Applied Computing and Informatics 14 (2018) 17–27

Contents lists available at ScienceDirect

Applied Computing and Informatics

journal homepage: www.sciencedirect.com

Interdependencies and reliability in the combined ICT and power system: An overview of current research

Inger Anne Tøndel [a], Jørn Foros [b], Stine Skaufel Kilskar [c], Per Hokstad [c], Martin Gilje Jaatun [a,*]

[a] SINTEF Digital, Strindveien 4, Trondheim, Norway
[b] SINTEF Energy Research, Norway
[c] SINTEF Technology and Society, Norway

ARTICLE INFO

Article history:
Received 18 October 2016
Revised 18 January 2017
Accepted 20 January 2017
Available online 3 February 2017

Keywords:
Interdependencies
Smart grid
Power system
ICT
Reliability
Cyber-security

ABSTRACT

The smart grid vision implies extensive use of ICT in the power system, enabling increased flexibility and functionality and thereby meeting future demands and strategic goals. Consequently, power system reliability will increasingly depend on ICT components and systems. While adding functionality, ICT systems also contribute to failures, such as hidden failures in protection systems, as has been exemplified by recent power outages. It also brings new threats, such as that of cyber-attacks. To ensure effective power system reliability, the interdependencies between power and ICT systems need to be properly understood. This paper provides an overview of main interdependency categories, as well as methods that can be used to identify and study interdependencies. Based on a study of recent papers in major archival journals, we conclude that appropriate methods for identification of interdependencies between power and ICT systems seem to be lacking. In addition, current methods seem unable to both cover the power system at large, and at the same time take into account the full array of intentional and accidental threats. Based on these findings, we make recommendations for future research in this field.

Contents

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

* Corresponding author.
E-mail address: martin.g.jaatun@sintef.no (M.G. Jaatun).

http://dx.doi.org/10.1016/j.aci.2017.01.001
2210-8327/

1. Introduction

Information and communication technology (ICT) systems are an increasingly important part of power systems. Traditionally, it is primarily the office systems that have been regarded as ICT systems, but there are an increasing number of systems for automation, control and protection that utilize ICT and are tightly integrated with the power system. Power systems with extensive ICT and smart components are often termed smart grids. Smart grids promise increased flexibility and functionality, both in normal operation and for handling of failures and unwanted incidents in the grid, and are expected to be the future power system of choice, enabling both future demands and national and international strategic goals to be met [1].

While adding functionality, ICT systems also contribute to failures, such as hidden failures in protection systems, as has been exemplified by recent power outages [2–4]. The increased complexity and use of ICT in smart grids can affect the reliability of power supply negatively in ways that are not presently fully known or understood. Technical and organizational interdependencies between the power and ICT systems cause new potential vulnerabilities, as well as common cause failures and other interdependent failures, and supply interruptions. The interdependencies also imply that power systems are more susceptible to cyber-attacks, also when such attacks do not target the power systems directly. Cyber threats are constantly advancing in sophistication, and there is a variety of measures one may take to make the ICT system more robust and to prepare in case an attack should be successful. Many of the measures available are, however, best suited for more traditional ICT systems, such as those used in office environments, and may be more difficult to apply to ICT components closely connected to the power network. Thus, it is important to identify and analyse the nature of the interdependencies between the power and ICT systems, in order to ensure system reliability and facilitate incident handling in case of failures and attacks.

Assessment of reliability of supply in traditional power systems has long been a topic of study (see, e.g., Allan et al. [5]). Likewise, for ICT systems, the knowledge on traditional security subjects such as information security, network security and network resilience is vast (see, e.g., Bishop [6]). There are also recent advances in reliability assessment of specific ICT systems used in power systems [7,8]. Most of these studies deal with the power and ICT systems more or less separately, without much focus on interdependencies between them and the causal relationship between failures in the power and ICT systems. With the evolution of smart grids, more studies of interdependencies have however started to emerge [9–11].

Within the wider subject of critical infrastructures, to which power and ICT systems belong, the literature on interdependencies is vast. There are a number of papers that review and classify modelling approaches for quantitative analysis of risk and interdependencies in critical infrastructures [3,12–18]. Ouyang [15] also lists several other references to modelling approaches. We have however not been able to find any review of advances in the study of interdependencies and reliability in the combined power and ICT system.

This paper contributes to the body of knowledge of interdependencies and reliability specifically in the combined power and ICT system. This is done by presenting an overview of papers addressing interdependencies and their effects on reliability in this system, based on a literature search in selected major archival journals during the last five years (see Section 4.1 for details on the literature search). We categorize the papers in terms of the type of interdependencies that they consider, and the methods they employ to analyse these interdependencies. By limiting the overview to the last five years we emphasize the current focus of the research community.

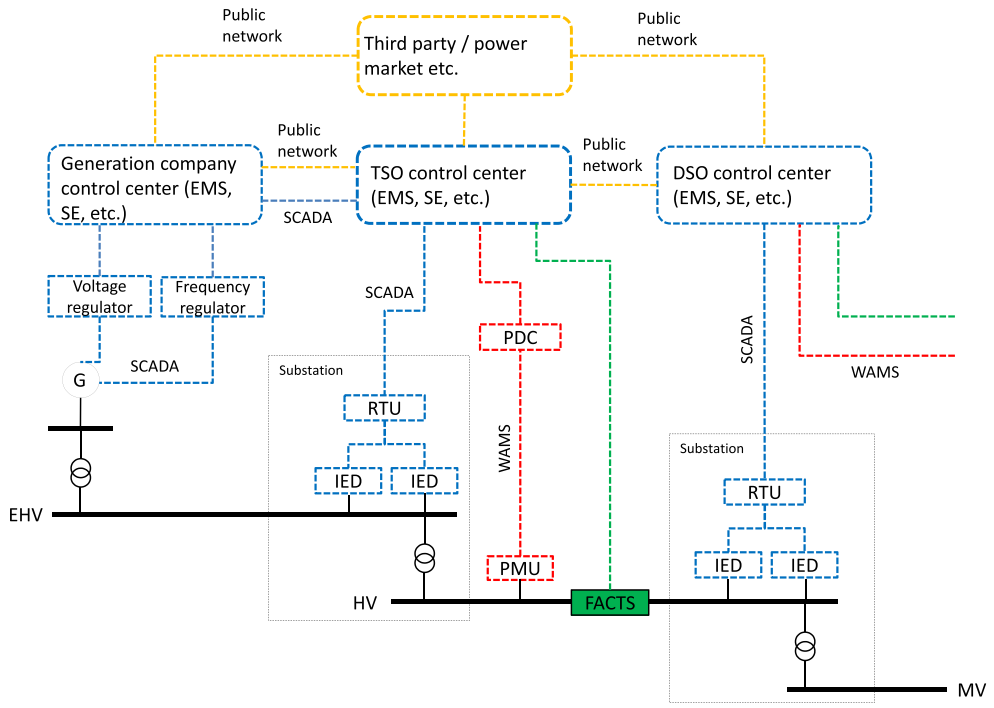
There are several suggested definitions of reliability, security, risk and related terms in the literature, and the definitions vary with the field of study. For power systems, suggested definitions of reliability and security have been provided by, e.g., the North American Electric Reliability Council (NERC) [19]: *"Reliability, in a bulk power electric system, is the degree to which the performance of the elements of that system results in power being delivered to consumers within accepted standards and in the amount desired*". Security is *"the ability of the power system to withstand sudden disturbances such as electric short circuits or non-anticipated loss of system components*". Furthermore, reliability is understood to be the aggregate of security and adequacy, where the latter is linked to long-term supply capacity and defined as *"the ability of the power system to supply the aggregate electric power and energy requirements of the customer at all times, taking into account scheduled and unscheduled outages of system components*". The terms security and reliability are used differently in the ICT community. To illustrate, the use of the term security in the context of ICT implies the protection of the system from adversaries that may perform various types of attacks in order to harm the system. The terms have yet other alternative definitions in more general risk research, see e.g. Rausand [20]. In this paper, we use the power system definitions of the terms security and reliability.

The paper is organized as follows. Section 2 gives an introduction to the combined power and ICT system and defines interdependency categories in terms of failure types. Section 3 discusses and classifies methods that are judged as useful for identifying and analysing interdependencies, based on methods for risk analysis and methods that have previously been applied to model critical infrastructures. Section 4 describes the literature study, and classifies the papers in terms of the interdependency and method categories that have been introduced. Section 5 summarizes the paper in terms of our recommendations, before the conclusion is presented in Section 6.

2. Power and ICT interdependencies

2.1. Overview of the combined power and ICT system

The basic constituents of a power system are generation units, transformers, transmission and distribution lines, and consumers. As produced and consumed power must balance at all times, supervision and operation of power systems is an essential and complicated task. A simplified sketch of a national power system and its control and protection functions is shown in Fig. 1. The figure, which is based on the Norwegian power system, shows from left to right the generation, transmission and distribution parts of the power system. Solid lines represent power lines and equipment while dashed lines represent communication lines and equipment for monitoring, control, protection and management (ICT components).



DSO	Distribution system operator	PDC	Phasor data concentrator
EHV	Extra high voltage	PMU	Phasor measurement unit
EMS	Energy management system	RTU	Remote terminal unit
FACTS	Flexible alternating current transmission system	SCADA	Supervisory control and data acquisition system
G	Generator	SE	State estimation
HV	High voltage	TSO	Transmission system operator
IED	Intelligent electronic device	WAMS	Wide area measurement system
MV	Medium voltage		

Fig. 1. Sketch of integrated power/ICT system.

The figure includes generation and transmission/distribution from extra high voltages (EHV, >300 kV) via high voltages (HV, 36–300 kV) to medium voltages (MV, 1–36 kV). For simplicity, only one generator and single EHV-, HV- and MV-lines are shown. Low voltage (LV, <1 kV) distribution lines have been excluded, as has distributed generation that may be connected directly to e.g. HV power lines.

Supervision and operation of the system and its components are carried out from control centres using supervisory control and data acquisition systems (SCADA). The national transmission system operator (TSO) has the overall responsibility for the power system, and generation companies and distribution system operators (DSO) have control centres responsible for their parts of the system. For clarity, only one generation company (control centre) and one DSO (control centre) are included in the figure, and regional TSO control centres are omitted.

In general, power systems include automatic as well as manual functions used for both system operation and system protection in case of failures. Generation companies utilise e.g. automatic voltage and frequency regulators to control generator power output, and their SCADA systems enable supervision and manual intervention if necessary. This may include automatic input from the TSO SCADA system for maintaining a stable transmission system frequency (load frequency control). The TSO and the DSOs utilize control and protection functions located in substations to e.g. regulate transformers and operate circuit breakers in case of overload or short circuits. These functions are typically automatically carried out by intelligent electronic devices (IED). Connection by communication lines directly to the control centre or via remote terminal units (RTU) enables supervision and manual intervention as needed. Additional advanced monitoring, control and protection methods are becoming more common, such as synchronised phasor measurements, adjustment of load flow through flexible AC transmission (FACTS) devices, and numerical and communication based protective gear. Phasor measurement units (PMU) are connected to the control centre via phasor data concentrators (PDC) that collect the data. Such data networks are often called wide area measurement systems (WAMS). Future power systems will even include monitoring and control functions down to the consumer level, such as smart meters and load control.

Automatic component control functions as described above handle system regulations on a short time scale, i.e. within seconds or minutes. At a higher level, the market for buying and selling power is instrumental for the regulation of the power system on longer time scales (i.e. hours or days). In the control centres, available information from monitoring and component control functions, as well as market information, is used for short and long-term management using, e.g., power system state estimation (SE) and energy management systems (EMS).

Communication between voltage/frequency regulators, IEDs and RTUs and the control centres, and communication from the TSO to generation companies for load frequency control, are typically over dedicated private communication networks. Communication between generation companies, the TSO and the DSOs, and between these companies and third parties, such as service companies and other power market participants, may take place over public networks. The ICT components directly connected to the power system, such as the SCADA, RTUs and IEDs, have traditionally been special purpose components with proprietary software and protocols. They have also been completely

disconnected from more general-purpose systems and networks, as used in the administrative ICT systems of the power companies. At the same time, as the amount of ICT is increasing in the power system, the nature of ICT is also changing with the use of more standard software components and general-purpose protocols. Increasingly, the ICT components of the power system are connected to other ICT systems, either for administrative purposes or for vendor support.

From the above, it is clear that ICT is integrated with modern power systems and that ICT in the future will increase in use and become more deeply integrated with the power system on multiple levels. In this article, we use the definition of ICT by Tornqvist et al. [21]: *"The technology involved in acquiring, storing, processing and distributing information by electronics means (including radio, television, telephone, and computers)."* With this in mind, and with respect to Fig. 1, we define the ICT part of the power system as the SCADA and WAMS systems including voltage/frequency regulators, IEDs, RTUs, PMUs, PDCs, control centres, and private and public communication networks, but excluding the primary power components for voltage and power flow control, such as transformers and FACTS (power electronics) devices.

2.2. Interdependency categories

The power system is clearly dependent on the ICT system, but the ICT system is also dependent on the power system to operate, i.e. the systems are interdependent. In general, a power system is heavily affected by various dependencies that exist within the system itself, between the power system and ICT, and between the power system and other critical infrastructures or its environment. The focus of this paper is on the power/ICT interdependencies.

From Rinaldi et al. [22], interdependency may be defined as "a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other". Interdependencies can be classified in various ways. Ouyang [15] gives an overview of different classifications proposed in the literature. Rinaldi et al. [22] propose an elaborate classification scheme in which interdependencies are described by six dimensions, i.e. infrastructure characteristics, state of operation, types of interdependencies, environment, coupling and response behaviour, and type of failure. A simpler classification scheme is used by Hokstad et al. [12], in which interdependencies are classified into geographical, functional and impact interdependencies. These are linked to the interdependency failure types proposed by Rinaldi et al. [22]; that is, they correspond to common cause, cascading, and escalating failures, respectively. A common cause failure is simultaneous failures in two systems due to a single common cause. Cascading failure is a failure in one system that causes a failure in another system. Escalating failure is a failure in one system that is worsened by the occurrence of a failure in another system, or by a failure that already has occurred in the other system. Interdependencies causing cascading and escalating failures are also named direct and indirect interdependencies, respectively, by some scholars [23].

In this paper we build on the classification schemes of Rinaldi et al. [22] and Hokstad et al. [12] and adapt them to classify power and ICT system interdependencies. The interdependency categories used can be found in Table 1. These categories emphasize the paper's focus on reliability, as they are defined in terms of failure type. A failure can be defined as "the termination of the ability to perform a required function" [20]. Note that although the interdependency categories are defined in terms of failure, we include malicious attacks as a possible cause of failure. This is reflected in some of the examples given in the table. The examples illustrate deterministic interdependencies, but the interdependencies may also be stochastic in nature.

3. Available methods for identifying and analysing interdependencies

General methods for identifying and analysing interdependencies in the combined power and ICT system are described and classified in the following. As we focus on the effect of interdependencies on reliability, we emphasize generally accepted methods used in reliability and risk analysis, but also include methods that have been used to model and simulate critical infrastructures. Most of the methods are not specifically designed for identifying or analysing interdependencies, but are capable of and useful for this.

We divide available methods into the following general categories, based on the key purposes of the methods (see Table 2): Hazard identification methods, causal analysis methods, consequence analysis methods, topological analysis methods, and dynamic analysis methods. The first three categories contain traditional methods for reliability and risk analysis, the fourth category contains methods that have been used to model complex systems such as critical infrastructures, and the last category includes methods from both of these areas of research. The categories are not mutually exclusive; some categories overlap partially, and some methods have properties that could place them in more than one category. Also, hybrid models that combine two or more methods are commonly used, as will be seen in Section 4 (see Table 6).

It is not possible to include all methods that can be used for identifying and analysing interdependencies. Some methods that

Table 1
Interdependency categories.

Nr.	Interdependency category	Explanation/example
I1	Common cause/geographical	Components within both systems fail due to a common cause. The reason could be that the systems are geographically close. Example: Power and communication lines located at the same place, both damaged in a storm
I2	Cascading/functional	Commonly referred to as "domino effect" failures, as they occur when a failure in one system causes a failure in the other system. A cascading failure typically occurs when the function of one system (e.g. the power system) depends on the functioning of the other system (e.g. ICT system)
	a Power failure causes ICT failure	Example: Lack of power for ICT components
	b ICT failure causes power failure	Example: An attacker gets access to the control system, and can send unauthorized commands to interrupt power
I3	Escalating/impact	Characterized by an existing failure in one system exacerbating an independent failure in the other system. The failure that has already occurred can e.g. increase the severity of the second failure or the time for recovery or restoration of the second failure
	a Power failure exacerbates an independent ICT failure	Example: Repair time of ICT component increases due to blackout
	b ICT failure exacerbates and independent power failure	Examples: Monitoring not available at a time when a power failure occurs (reduces situational awareness). Or, a failure occurs in the power system and its protection system fails to operate. In this case, the backup protection will clear the failure, but the result is worsened consequences in the power system

Table 2
Methods for identification and analysis of interdependencies.

Category	Description	Example methods
M1: Hazard identification methods	Methods for identifying threats, hazards and hazardous events, which can be used also for identifying interdependencies	HAZID, HAZOP, SWIFT, FMECA
M2: Causal analysis methods	Methods for identifying or analysing failure causes, with the possibility of including or exploring interdependencies	Ishikawa cause and effect diagram, risk influence diagram, fault tree analysis, reliability block diagram, attack tree, Bayesian network, probabilistic relational model, STEP diagram, why-because graph
M3: Consequence analysis methods	Methods for assessing failure consequences, including revealing or analysing interdependencies such as cascade and escalation	Event tree, power flow simulation methods, communication network simulation, cascade diagram
M4: Topological analysis methods	Methods for describing or modelling system topology, including interactions and interdependencies between components and systems	Network theory/graph theory
M5: Dynamic analysis methods	Methods for analysing dynamic (time-dependent) aspects or effects, with the possibility of including or exploring interdependencies	Markov process, Petri net, agent-based methods, system dynamics, dynamic control system theory

have been omitted in Table 2 are input-output models (see, e.g., Ouyang [15]), high level architecture (see, e.g., Kröger and Zio [13]), and human reliability analysis (see, e.g., Kröger and Zio [13]).

3.1. Hazard identification methods

There are a number of general methods for identification of threats, hazards and hazardous events, which can be used also for identifying hazardous interdependencies. Most of these are based on brainstorming or checklists, and require a group of experts on the system at hand to meet and discuss. Well-known examples are HAZID (“Hazard identification”), HAZOP (“Hazard and operability study”) [24] and SWIFT (“Structured What-If Technique”) (see, e.g., Rausand [20]). HAZID is used for a multitude of installations and operations, whereas HAZOP is commonly used for risk assessment of process plants. SWIFT utilizes a set of what-if questions, and can be used as a simplified HAZOP.

There are also hazard identification methods that are based on analysis of system components or functions rather than brainstorming and checklists. A prime example is FMECA (“Failure mode, effect and criticality analysis”) (see, e.g., Rausand [20]). Whereas HAZOP looks for the impact of anomalies on a system, FMECA is commonly used to systematically assess failures of system components as part of system reliability analyses. FMECA is an extension of the Failure Mode and Effects Analysis (FMEA) standard [25].

3.2. Causal analysis methods

Causal analysis methods identify and describe causes of system failures, including relations and dependencies between causes. These methods can therefore be used for both identifying and examining system interdependencies, such as failures in one system due to underlying causes in another system.

Causal analysis is a basic part of risk analysis, and there are several methods available, as listed in Table 2. The analyses can be performed at a varying level of detail, ranging from simple qualitative methods to more comprehensive quantitative methods. The Ishikawa cause and effect diagram is an example of a qualitative method. This is a structured graphical way to identify, sort and describe causes of failures or hazardous events. Risk influence diagrams and fault tree analysis may be used for both qualitative and quantitative analyses. The risk influence diagram describes factors/conditions that may influence the occurrence of failures or hazardous events, but do not directly cause them. The most common method for causal analysis is fault tree analysis, which illustrates the combinations of “basic events” (failures) that can cause a system failure. A fault tree can be converted to a reliability block diagram, which instead of illustrating a system failure illustrates combinations of components needed to perform a system function. Fault trees have also been used as a basis for attack trees [26] that are capable of describing possible attack strategies in order to achieve an attacker goal (e.g. some kind of system failure).

Bayesian networks and probabilistic relational models are examples of more complex and comprehensive models that can be used for causal analysis. The Bayesian network is a directed acyclic graph that includes nodes describing system states, conditions or events, and directed arcs describing relations or dependencies between them, together with a set of probability tables. The probabilistic relational model is used, e.g., by König et al. [27], and combines a Bayesian network with a model of the system architecture.

There are also several approaches and models that are used to analyse failure events and their causes through the utilization of empirical information. Two examples are the STEP (sequentially timed events plotting) diagram and the why-because graph. These are both designed to investigate a particular accident or incident, and thus also reveal possible system interdependencies. The STEP diagram [28] is a frequently applied graphical presentation of the flow of events as a function of time; it will include actors (i.e., persons and objects/systems involved), and the focus is on the interaction and interdependencies between these actors. The main objective of the why-because graph, is to identify all contributing causes to an actual accident/event.

An introduction to most of the above mentioned methods can be found in Rausand [20]. The methods are generally not well suited for analysing dynamic effects (the STEP method being a possible exception). Methods suitable for treating time-dependent effects are described in Section 3.5.

3.3. Consequence analysis methods

Consequence analysis methods assess consequences of system failures, e.g., in terms of power interruptions, loss of communication, loss of other critical societal functions, or hazards to personnel due to e.g. fire or explosions. These methods can therefore be used for revealing or analysing interdependencies such as failure cascade and escalation within or between systems.

Consequence analysis is a basic part of risk analysis, together with hazard identification and causal analysis. The most common method for consequence analysis is event tree analysis, which illustrates possible hazardous events (contingencies) that may

follow a failure, and may be used for both qualitative and quantitative analyses (see e.g. [20]). Additionally, power flow and communication network simulations are commonly used for calculating the resulting power and ICT system state following a failure [29].

There are also consequence models specifically made for analysing interdependencies. An example is cascade diagrams [12], which provide a graphical overview of cascading of failures and resulting loss of critical societal functions in critical infrastructures. In quantitative calculations, these diagrams allow inclusion of escalating failures in addition to cascading failures.

3.4. Topological analysis methods

Many critical infrastructures exhibit properties that are characteristic of complex systems, and there are a number of methods that have been used to understand the behaviour of such systems. Some of these describe and model the system topology. These methods are suitable for analysing interdependencies, as physical interactions and interdependencies within or between systems are explicitly included. Prime examples of such methods are network theory and graph theory. As network theory is based on graph theory, and these are similar methods, we do not distinguish between them here. Network/graphs consist of nodes and links, where the nodes represent the physical system components and the links represent their connections or interactions.

There are a number of papers that review these and other modelling approaches for risk and interdependencies in critical infrastructures, such as Kröger et al. [13], Landegren et al. [14], and Ouyang [15].

3.5. Dynamic analysis methods

Dynamic analysis methods can be used for identifying and analysing interdependencies that emerge in time dependent processes.

There are several methods available for analysis of dynamic aspects or effects. Within risk analysis, examples of common methods are Markov processes and Petri nets. Within critical infrastructure modelling, examples of methods are agent-based methods, system dynamics, and dynamic control system theory. A Markov process is a stochastic process with discrete states and continuous time, suitable for analysing systems with redundancy, interdependencies and dynamic properties. Petri nets are based on graph theory, and include two types of nodes describing system states and transitions, and directed arcs describing relations or dependencies between the nodes. Agent-based methods utilize dynamically interacting and interdependent agents that act based on specific rules; agents may represent physical components as well as human operators. System dynamics utilizes the three concepts feedback, stock, and flow to dynamically analyse complex systems with interdependencies and emergent and adaptive behaviour. Dynamic control system theory applies traditional control system theory and transfers functions to dynamic analysis of critical infrastructures with interdependencies.

An introduction to Markov processes and Petri nets can be found in Rausand [20]. There are a number of papers that review agent-based methods, system dynamics, dynamic control system theory, and/or other modelling approaches for risk and interdependencies in critical infrastructures, such as Kröger et al. [13], Landegren et al. [14], Ouyang [15], Pederson et al. [16], Rinaldi [17] and Eusgeld et al. [18].

4. Literature review

In order to study the current state of research on power and ICT interdependencies and their impact on power system reliability, we performed a literature review. This review aimed to provide answers to the following research questions:

- What types of power and ICT system interdependencies that may impact power system reliability are covered in existing work?
- What types of methods are used to identify and/or analyse the interdependencies and their impact on power system reliability?

In this section we present the method used in identifying and analysing relevant research papers, as well as the main results from the review.

4.1. Method

Due to resource constraints, a full systematic review could not be performed. Instead we selected three major archival journals and went through all materials published in 2010 or later. The selected journals were the International Journal of Critical Infrastructure Protection, IEEE Transactions on Smart Grid and IEEE Transactions on Power Systems. By studying recent papers in major journals we identify a significant portion of high-quality research in this domain, and also emphasise current focus in the research community. The three journals were selected to include one journal targeted towards smart grid research, one journal that considers power system research without particular focus on the smart grid aspects, and one more general critical infrastructure journal. We acknowledge that by restricting our search to only three journals we cannot claim to be comprehensive, but we maintain that this selection still gives a good overview of the focus of current research.

An overview of the process for selecting papers for inclusion in the study can be found in Table 3. The selection of papers was performed according to the following selection criteria:

- The papers should address both power and ICT components, and their relation or interdependencies.
- The papers should consider power system reliability impacts of interdependencies.

In mid-October 2014, one researcher went through the relevant issues of the three journals, and selected papers based on title and

Table 3
Overview of the paper selection process.

Stage	Description	Number of papers included for further analysis
Stage 1: Initial selection of papers, mid-October	One researcher went through the selected journals, and included papers based on title and abstract	48
Stage 2: Initial reading, October/November	Each paper read by one researcher	26
Stage 3: Second reading, December	Each paper read by one additional researcher. Borderline-papers, as well as all papers that were excluded at this stage were discussed in the full group of researchers.	14

abstract. In total 48 papers were selected for more detailed analysis: six from the International Journal of Critical Infrastructure Protection, thirty from the IEEE Transactions of Smart Grid and twelve from the IEEE Transactions on Power Systems. In this first stage, papers concerned with the relation between ICT and power systems were included, also when interdependencies were not particularly mentioned in the title or abstract. However, papers clearly concerning the development of new or improved ICT technology for use in power systems were excluded, unless its impact on power system reliability was also considered. When in doubt, the paper was included.

In stage 2, each of the papers selected based on title and abstract was read by at least one researcher. Four researchers cooperated on reading the papers. Papers clearly not meeting the selection criteria were excluded, but when in doubt the papers were read by one additional researcher in stage 3. A total of 22 papers were excluded in stage 2, leaving 26 papers for stage 3. Five researchers took part in this stage. Each paper was read by at least one additional researcher. Papers that were considered borderline papers, and papers that were considered not to meet the selection criteria, were discussed in the full group before a decision on whether or not to include or exclude the paper was made. In the end, 14 papers were included in the study.

In the first reading of the papers (stage 2), the researcher reading the paper made a written summary of the scope of the paper, the method used to identify or analyse interdependencies, as well as any interdependencies identified in the paper. In the second reading of the papers (stage 3), the reader of the paper made a categorization of the paper according to the interdependency categories in Table 1 as well as the method categories in Table 2. In both stages, the reader of the papers could provide additional comments if necessary.

4.2. Results

An overview of the included papers can be found in Table 4, with two papers from the International Journal of Critical Infrastructure Protection (IJCIP), ten papers from IEEE Transactions on Smart Grid and two papers from the IEEE Transactions on Power Systems. There are three to four papers from each year, except from 2010 where none are included. The papers can be broadly divided into the following subjects:

- *General approaches that include both ICT and power aspects (1 paper):* Chen et al. [30] propose strategies for hierarchical construction of petri net models by different experts for various parts of the system. The combined petri net models attacks in the smart grid and may include multiple coordinated attackers as well as a combination of physical and cyber-attacks.
- *General approaches in order to combine ICT and power models (1 paper):* Lin et al. [31] present a simulation framework that allows power and ICT simulations to be synchronized.
- *Studying ways the power system may be attacked via the ICT system (2 papers):* Zonouz et al. [32] propose a framework for evaluating potential contingencies due to remote cyber-attacks, as a complement to traditional power system contingency analysis that analyses accidental failures. Srivastava et al. [33] provide ways of estimating how an attacker may determine which relays to attack in an Aurora like attack, taking into account attack feasibility as well as power system consequences.
- *Studying power system reliability impact of failures of specific ICT functions or components (5 papers):* Both Aminafar et al. [34] and Panteli et al. [35] study impact of situational awareness on power system reliability, though with varying methods and scope. Aminafar et al. [34] study the impact of wide-area measurement system (WAMS) malfunction, while Panteli et al. [35] emphasize the human aspect of situational awareness, where ICT systems influence the human operator's perception of the current system state. Both König et al. [27] and Lei et al. [36] address reliability of substation automation and protection systems, and Lei et al. [36] also propose how the result of such a reliability analysis can be used as input to broader reliability analysis of the overall power system. Jiang and Singh [37] propose ways to include protection system failure and repair rates as input to power system reliability evaluations.
- *Studying power system reliability impact of ICT failures at a general level (4 papers):* Falahati et al. [23] and Falahati and Fu [38] provide quantitative calculations of power system reliability indices such as "loss of load probability" and "expected energy not served" due to failures in the ICT system. Chiaradonna et al. [39] model the combined power and ICT system using the stochastic activity network (SAN) formalism, which is based on Petri nets. The usefulness of the approach is demonstrated through modelling and analysing cases where the communication network performance is reduced at the same time as a failure has happened in the power network. Beccuti et al. [40] extend the work of Chiaradonna et al. [39], using the SAN formalism primarily to model the power grid, while stochastic well-formed nets (SWN) are used to model a denial of service (DoS) attack in the communication network.
- *Combining power and ICT aspects in order to better identify critical components of the combined ICT and power system (1 paper):* Nguyen et al. [41] present an approach to detect critical nodes in the power network, taking into account also the communication network and ways in which failures may cascade from one network to the other.

As illustrated in Fig. 2, most papers put effort into including both ICT and power aspects in the modelling. As examples, Beccuti et al. [40] (P2) create one model of the ICT part of the system, and another for the power part, and then combine these in the analysis, whereas Lin et al. [31] (P7) present a framework for co-simulation of a power system and an ICT network. In some cases, both ICT and power aspects are included, but there is a slight emphasis on one of the aspects. Zonouz et al. [32] (P14), one the one hand, put more emphasis on the ICT part in the paper, as malicious attacks through the ICT part of the system are the new addition to the contingency analysis; Chiaradonna et al. [39] (P4), on the other, put a slight emphasis on power aspects in their model, something that is put forward as a motivation for the work of Becutti et al. [40] (P2).

Some of the papers are, however, mainly concerned with either the ICT or the power part of the system, and treat the other part more superficially. Either the main emphasis is on the power system, but the failure rates of ICT components such as protection systems (P8) or PMUs (P1) are taken into account, or the main emphasis is on the ICT part of the system, but the failure rates of power components (P9), or the consequences for the power system (P10, P13), are taken into account. For the more focused papers, it varies to what extent they suggest ways in which the results from the targeted models or analysis they suggest can be used in additional analysis that covers a larger part of the system.

No papers aim to cover all relevant threats or failures. The majority of the papers only consider accidental failures, and a few exclusively consider attacks, as illustrated in Fig. 3. There are only two papers (P2 and P4) that clearly cover both, but then in a limited fashion – considering communication network performance problems either due to failures or attacks,[1] as well as the loss of a line in the power grid either due to an accidental failure

[1] And of these two papers, one (P2) primarily focuses on Denial of Service (DoS) attacks.

Table 4
Overview of included papers, alphabetically ordered based on author name.

Nr.	Author and title	Journal, Year	Paper topic
P1 [34]	Aminifar et al.: Impact of WAMS Malfunction on Power System Reliability Assessment	IEEE smart grid, 2012	Understand the impact of situational awareness and controllability on power system reliability assessments
P2 [40]	Beccuti et al.: Quantification of dependencies between electrical and information infrastructures	IJCIP, 2012	Investigate the consequences of a denial of service (DoS) attack on the communication network when the grid has just experienced a failure. Build upon paper P4
P3 [30]	Chen et al.: Petri Net Modelling of Cyber-Physical Attacks on Smart Grid	IEEE smart grid, 2011	Use of Petri-net to model attacks on Smart Grid, focusing on multiple attacks (timing dependent attacks)
P4 [39]	Chiaradonna et al.: Definition, implementation and application of a model-based framework for analysing interdependencies in electric power systems	IJCIP, 2011	Propose a model-based framework for quantitatively analysing propagation and impact of malfunctions in the combined power and ICT system, with an emphasis on the impact of communication network performance problems when the grid experiences a failure
P5 [23]	Falahati et al.: Reliability Assessment of Smart Grids Considering direct Cyber-Power Interdependencies	IEEE smart grid, 2012	Provides quantitative calculation of reliability indices such as "loss of load probability" and "expected energy not served" due to cyber failures cascading to the power system. Only consider cascading failures (*direct* interdependencies)
P6 [38]	Falahati and Fu: Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies	IEEE smart grid, 2014	Provides quantitative calculation of reliability indices such as "loss of load probability" and "expected energy not served" due to cyber failures cascading to the power system. Only consider escalating failures (*indirect* interdependencies)
P7 [31]	Lin et al.: GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network	IEEE smart grid, 2012	Presents a framework for co-simulation of a power system and an ICT network, including control functions. The performance/speed of relay protection is evaluated for two failures as an example
P8 [37]	Jiang et al.: New Models and Concepts for Power System Reliability Evaluation Including Protection System Failures	IEEE power systems, 2011	Presents a Markov model for incorporating protection system failures into overall power system reliability calculations, including both spurious trips in the protection system and escalating power failures due to protection system failure on demand
P9 [27]	König et al.: Reliability Analysis of Substation Automation System Functions Using PRMs	IEEE smart grid, 2013	Present and test the application of a probabilistic framework for reliability analysis of substation automation systems
P10 [36]	Lei et al.: Reliability Modelling and Analysis of IEC 61850 Based Substation Protection Systems	IEEE smart grid, 2014	Present a reliability modelling and analysis methodology for modern substation protection systems, as well as a cyber-physical interface matrix that ease further reliability analysis of large-scale systems
P11 [41]	Nguyen et al.: Detecting Critical Nodes in Interdependent Power Networks for Vulnerability Assessment	IEEE smart grid, 2013	Identifying critical nodes in an interdependent power network. These are the nodes whose removals maximally destroy the power network's functions, due to malfunction of these nodes and cascading failures of its interdependent communication network
P12 [35]	Panteli et al.: Assessing the Impact of Insufficient Situation Awareness on Power System Operation	IEEE power systems, 2013	Presents a general multi-state model based on Markov modelling for analysing escalating power failures due to lack of situational awareness, including lack of situational awareness due to ICT failures
P13 [33]	Srivastava et al.: Modelling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information	IEEE smart grid, 2013	Model how an attacker can determine (based on incomplete information) which generators to attack in an Aurora-like event in order to cause maximum adverse impact to the grid
P14 [32]	Zonouz et al.: SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures	IEEE smart grid, 2014	Introduce a cyber-physical contingency analysis framework for analysing the physical impacts resulting from compromise in the cyber network. Analysis is performed based on measurements already present in modern control centres

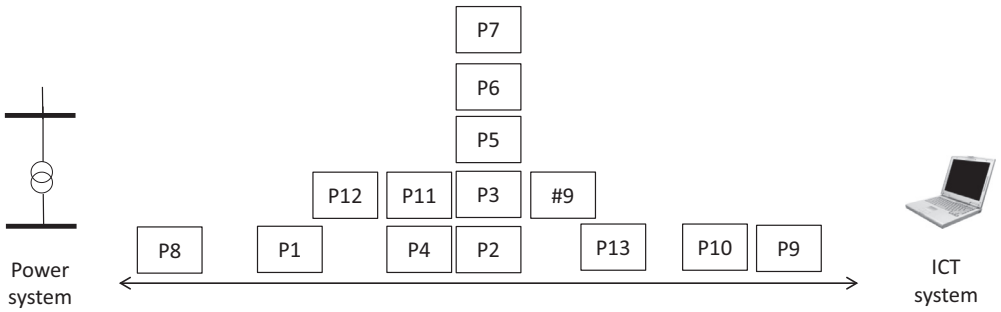


Fig. 2. Included papers differ in their emphasis of power or ICT aspects.

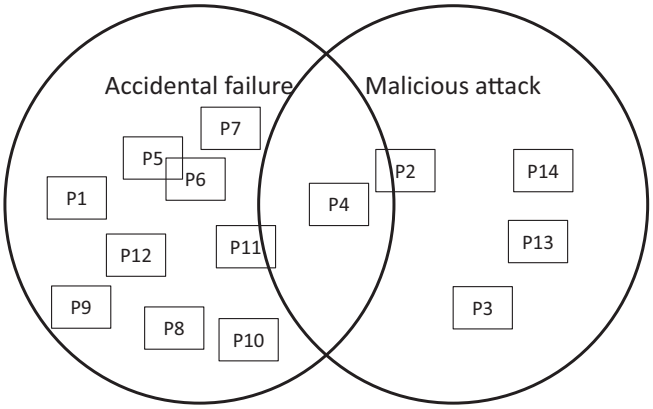


Fig. 3. Coverage of accidental failures and malicious attacks in the included papers.

or an attack. One paper (P11) mentions both failures and attacks, but seems to focus only on accidental failures.

In Section 2.2, a set of interdependency categories was defined. Table 5 provides an overview of the main interdependency types that are considered in the included papers. As can be seen from the table, the majority of the papers covers escalating interdependencies, where the consequences of a power failure are made worse due to a failure or attack in the ICT system at the same time (interdependency category I3b). This is due to the role ICT systems play in achieving situational awareness and sending commands (P1, P2, P4, P6, P10, P12), as well as in performing automatic actions to limit power consequences of a failure (e.g. protection systems) (P7, P8). Several of the papers consider cascading failures, where ICT systems cause failures in the power systems (interdependency category I2b). This can be due to attacks (P13, P14) or due to failures, where power components rely on ICT components to function (P5, P11). Lack of situational awareness may result in operator actions that endanger power system stability (P12). Protection system malfunctions may also cause power failures, in case of undesired tripping (P7, P8). A few of the papers consider cascades from the power system to the ICT system, through including power component failures when considering reliability of ICT systems (P9), or by taking into account that ICT components of the power system may rely on power components to function (P11). None of the papers specifically address escalating interdependencies where a failure in the power system may increase the consequences of an ICT failure (interdependency category I3a), although Chiaradonna et al. (P4) discuss the possibility that repair rates of control system components may increase due to a large blackout. None of the papers address common cause interdependencies. One paper (P3) does not emphasize any of the interdependency categories, but rather aims at including all types of attacks in the model.

The methods used in the included papers vary greatly. Nearly half of the papers (P1, P5, P6, P10, P11, P13) present tailor made methods to model or analyse particular aspects of the combined power and ICT system. One paper (P3) uses Petri Nets, and two more (P2, P4) use models that are based on the Petri Net formalism. Markov models are used in three of the papers (P8, P12, and P14). One of these (P12) uses fault trees to estimate probabilities that are needed as input to the Markov model. One paper (P9) uses Probabilistic Relational Models (PRM), and one paper (P7) uses the simulation frameworks Network Simulator 2 (NS2) and Positive Sequence Load Flow (PSLF) to simulate the communication and power network respectively. An overview of the main methods used in the papers is given in Table 6, in terms of the method categories defined in Section 3.

As can be seen from Table 6, dynamic methods are used in half of the papers included. These are able to deal with time dependencies, but at the cost of complexity. Consequence methods are also used in half of the papers, in some cases in combination with causal methods. Topological analysis methods are used in three of the papers.

From the table it can be seen that none of the papers use hazard identification methods that in Section 3 was discussed as a possible mean for identifying interdependencies. This may be due to the limitations of such simple models when applied to complex systems. In the papers it is either unclear how interdependencies are identified, or it seems to be assumed that the interdependencies are already known. In one of the papers (P14), identification seems to be done rather automatically, based on information available in the systems. In many of the papers, the interdependencies are often related to the topology. Power and ICT components are connected to each other, and this leads to interdependencies. These interdependencies are however represented in various ways. Some papers create matrices that capture important aspects of the interdependencies (such as changes in availability (P5, P6) or failure probabilities (P10)). Failure and repair rates are influenced by the interdependencies in several of the papers (e.g. P4, P8, P12). In some papers the interdependencies are included through inclusion of power and ICT aspects in the same model (e.g. P3), or are taken into account in the formulas used (P4, P1). In the paper on co-simulation

Table 5
Main interdependency categories covered by the papers.

Interdependency category	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
I1 (common cause)			(x)											
I2a (cascading P → ICT)			(x)						x		x			
I2b (cascading ICT → P)			(x)		x		x	x			x	x	x	x
I3a (escalate ICT consequences)			(x)											
I3b (escalate P consequences)	x	x	(x)	x		x	x	x		x		x		

Table 6
Main method categories used in the papers.

Method	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
M1 (hazard identification)														
M2 (causal)					x	x			x			x		
M3 (consequence)	x				x	x	x					x	x	x
M4 (topological)											x		x	x
M5 (dynamic)		x	x	x				x		x		x		x

of power and ICT networks (P7), the interdependencies are dealt with by a common event queue.

All papers present results from evaluations of the suggested approach, by using a test case (in some cases a very small example system) to demonstrate the feasibility of the approach.

5. Discussion and recommendations for further research

In this paper, we have studied how recent research results published in three major archival journals identify and analyse interdependencies between the power and ICT systems. As we did not aim to cover all research in this field, but limited the study to three journals, there are relevant research results that are not covered by our literature review. However, as we took a systematic approach to studying the literature, we claim that the results are able to say something about the state of the research field, as well as the main research focus.

As shown in Section 4.2, the included papers vary in scope and methods used. As such, it seems that the current research on power and ICT interdependencies is at a relatively early stage where a large number of approaches are suggested. The suggested approaches are evaluated using test cases, but none of them is evaluated in a real-life setting.

Identification of interdependencies between power networks and ICT is a research area that is given close to no attention in the journals that we have studied. In the included papers, it seems to be assumed that these interdependencies are already known by the analyst. However, both the power network and the ICT system are highly complex systems. In smaller test cases, it is likely that such interdependencies can be identified relatively easily, and that the analyst is able to have a sufficient overview of the combined system. In real cases, this is however likely to be much harder to achieve. In Section 3.1, we identified a few methods that we consider useful for identifying interdependencies at a high level. There is a need for research on how adequate these methods are in addressing power and ICT interdependencies and in providing input to analysis of interdependencies. New or adapted methods may be needed.

When addressing interdependencies between power networks and ICT, there is a need for competence on both the power system and the ICT system, as well as on methods for identifying and analysing interdependencies. To ease interdisciplinary collaboration, it seems wise to use models that are as simple as possible. Traditional risk analysis methods, such as fault trees, reliability block diagrams and event tree analysis, have gained much of their success from their ease of use and understanding. In contrast, many of the approaches suggested in the papers are quite complex to understand and use, and may thus be a poor choice as a basis for interdisciplinary communication.

As both the power and ICT systems are complex, simple models are however unlikely to cover all system aspects at a level of detail necessary to understand the reliability impact of the interdependencies. This is likely to be difficult also for complex models. None of the papers presents models that are able to fully include the combined power and ICT system and a wide array of threats. Thus, there is a need to understand how models can be used together, and in particular how simple models can be used together with complex models in order to achieve both interdisciplinary understanding and the necessary detail. In some of the papers it is explained how the work can be used as input to other analysis. One example is the cyber-physical system interface matrix suggested by Lei et al. [36] that makes it possible to include ICT failures in more traditional power analyses.

In the papers, it is not clearly stated who are considered potential users of the suggested approaches, and what the user requirements are. The needs of TSOs and DSOs for identifying and understanding the interdependencies in their systems should be understood. This aspect is currently lacking in the journal papers studied.

Also related to the needs of the DSOs and TSOs are considerations of what type of input is required in the models. A few of the papers mention the difficulties of obtaining reliable data on ICT components. In particular, König et al. [27] discuss the difficulty of obtaining failure rates for control and protection systems. Most papers are however mainly concerned with presenting models that can be used for analysis, and less concerned with addressing whether or not relevant data are available. Zonouz et al. [32] are however concerned with the ease of building the model, and present an approach that builds a model automatically. A model of the ICT system is generated by utilizing data that are already measured and present in modern control centres. This model is then connected to a state-based model of the power network, in an online manner.

The papers mainly cover cascading and escalating interdependencies, in particular in terms of incidents in the ICT system that causes or escalates failures in the power systems. Of the interdependency categories in Table 1, these are the most important ones in order to understand how the integration of more ICT in the power network influences power system reliability. However, of the included papers, the majority is concerned only with accidental failures, and only a few papers take intentional attacks into account. With the use of more ICT in the power network, and increased connectivity among ICT components, the malicious threat from remote attackers is becoming more and more real. There is a need to understand the implications of the risks associated with cyber-attacks for power system reliability. The traditional models for power system reliability analysis are however concerned with accidental failures. Extending or complementing these to deal with ICT component failures is thus easier than to aim for also dealing with attacks. If including attacks in the models, the concept of failure rates will be different since the models need to take into account an intelligent adversary rather than accidental failures. In addition, there are limited data available related to probabilities, consequences and propagation of cyber-attacks in power systems; thus, the problem of obtaining the necessary input data for the models is even more difficult when including cyber-attacks in the analysis.

None of the papers we have studied use empirical data to identify or analyse interdependencies, although there have been relevant incidents that could be used as a basis for analysis. This may be due to confidentiality issues. However, failures, and also near misses, are an important source for learning and are likely to be useful in understanding how the power and ICT systems depend on and influence each other.

In summary, we recommend that future research addresses the following research topics:

- Methods for identification of interdependencies between power networks and ICT systems.
- Methods targeted towards easing interdisciplinary communication among power and ICT experts, in particular the feasibility of more easy-to-understand methods when analysing power and ICT interdependencies.
- Approaches to using simple and more complex methods in combination, to achieve ease of understanding as well as the necessary detail.
- Understanding DSO and TSO needs when it comes to identifying and understanding interdependencies in their systems.
- Evaluate and suggest approaches to ease modelling and obtain necessary input data to the model.
- Understand the risk associated with cyber-attacks for the power grid.

- Use information from historical failures and near-misses to improve understanding of interdependencies, and the role interdependencies may play in case of failures.

6. Conclusion

Interdependencies between the power and ICT systems already have an impact on the reliability of the power system. With the ongoing transition towards a smarter grid, this will increase in the future. In this paper, we have presented the results of a literature review of the current state of research on power and ICT interdependencies and their impact on power system reliability. In particular, we have reviewed which interdependency types that are covered in existing work, as well as which methods that are used to identify and analyse interdependencies. We found that research on interdependencies in the combined power and ICT system is at an early stage. Cascading and escalating interdependencies are covered, in particular in terms of incidents in the ICT system that causes or escalates failures in the power systems. The methods presented in the papers are however not yet able to provide an overview of interdependencies in the power system at large, and at the same time take into account a wide array of both intentional and accidental threats. Methods for identification of interdependencies seem to be lacking. We recommend that future research addresses these limitations of the current methods, and puts more attention on identifying the needs of TSOs and DSOs for identifying interdependencies and understanding their impacts.

Acknowledgements

This research has been performed as part of the AFTER project funded by the European Commission (grant nr. 267188), and the Flexnett project funded by the Norwegian Research Council (project nr. 245412). The authors would like to thank Gerd Kjølle for useful comments and suggestions when preparing this paper.

References

[1] European Technology Platform Smartgrids, SmartGrids SRA 2025, Strategic Research Agenda, Update of the SmartGrids SRA 2007 for the needs by the year 2035, 2012.
[2] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[3] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, P. Zhang, Risk assessment of cascading outages: methodologies and challenges, IEEE Trans. Power Syst. 27 (2012) 631–641.
[4] R. Zimmerman, Decision-making and the vulnerability of interdependent critical infrastructure. In: IEEE International Conference on Systems, Man and Cybernetics, IEEE, 2004, pp. 4059–4063.
[5] R. Allan, R. Billinton, Probabilistic assessment of power systems, Proc. IEEE 88 (2000) 140–162.
[6] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2012.
[7] R.J. Albuquerque, V.L. Paucar, Evaluation of the PMUs measurement channels availability for observability analysis, IEEE Trans. Power Syst. 28 (2013) 2536–2544.
[8] S. Zhang, V. Vittal, Wide-area control resiliency using redundant communication paths, IEEE Trans. Power Syst. 29 (2014) 2189–2199.
[9] J.-C. Laprie, K. Kanoun, M. Kaâniche, Modelling interdependencies between the electricity and information infrastructures, in: Computer Safety, Reliability, and Security, Springer, 2007, pp. 54–67.
[10] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, R. Setola, Modelling interdependent infrastructures using interacting dynamical models, Int. J. Crit. Infrastruct. 4 (2008) 63–79.
[11] D. Kirschen, F. Bouffard, Keeping the lights on and the information flowing, IEEE Power Energy Mag. 7 (2009) 50–60.
[12] P. Hokstad, I.B. Utne, J. Vatn, Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis, Springer, 2012.
[13] W. Kröger, E. Zio, Vulnerable Systems, Springer, 2011.
[14] F. Landegren, J. Johansson, O. Samuelsson, Review of computer based methods for modeling and simulating critical infrastructures as socio-technical systems, in: European Safety and Reliability Association Conference (ESREL2013).
[15] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Eng. Syst. Saf. 121 (2014) 43–60.
[16] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, Critical infrastructure interdependency modeling: a survey of US and international research, Idaho Natl. Lab. 1–20 (2006).
[17] S.M. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, in: Proceedings of the 37th Annual Hawaii International Conference on System Sciences, IEEE, 2004, p. 8.
[18] I. Eusgeld, C. Nan, S. Dietz, "System-of-systems" approach for interdependent critical infrastructures, Reliability Eng. Syst. Saf. 96 (2011) 679–686.
[19] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions, IEEE Trans. Power Syst. 19 (2004) 1387–1401.
[20] M. Rausand, Risk Assessment: Theory, Methods, and Applications, John Wiley & Sons, 2013.
[21] B. Tornqvist, M. Fontela, P. Mellstrand, R. Gustavsson, C. Andrieu, Overview of ICT components and its application in electric power systems, Distributed Intelligence for Distributed Energy Resources: Selected Publications from the CRISP Project, 2005.
[22] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Syst. 21 (2001) 11–25.
[23] B. Falahati, Y. Fu, L. Wu, Reliability assessment of smart grid considering direct cyber-power interdependencies, IEEE Trans. Smart Grid 3 (2012) 1515–1524.
[24] IEC, Hazard and operability studies (HAZOP studies) - Application guide, IEC 61882:2016, 2016.
[25] IEC, Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), IEC 60812:2006, 2006.
[26] B. Schneier, Attack trees, Dr. Dobb's J. 24 (1999) 21–29.
[27] J. Konig, L. Nordstrom, M. Osterlind, Reliability analysis of substation automation system functions using PRMs, IEEE Trans. Smart Grid 4 (2013) 206–213.
[28] K. Hendrick, L. Benner, Investigating Accidents with STEP, CRC Press, 1986.
[29] E. Ciapessoni, D. Cirio, A. Pitto, G. Kjolle, M. Sforna, An integrated framework for power and ICT system risk-based security assessment, in: PowerTech (POWERTECH) IEEE Grenoble, IEEE, 2013, pp. 1–6.
[30] T.M. Chen, J.C. Sanchez-Aarnoutse, J. Buford, Petri net modeling of cyber-physical attacks on smart grid, IEEE Trans. Smart Grid 2 (2011) 741–749.
[31] H. Lin, S.S. Veda, S.S. Shukla, L. Mili, J. Thorp, GECO: global event-driven co-simulation framework for interconnected power system and communication network, IEEE Trans. Smart Grid 3 (2012) 1444–1456.
[32] S. Zonouz, C.M. Davis, K.R. Davis, R. Berthier, R.B. Bobba, W.H. Sanders, SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures, 2014.
[33] A. Srivastava, T.H. Morris, T. Ernster, C. Vellaithurai, S. Pan, U. Adhikari, Modeling cyber-physical vulnerability of the smart grid with incomplete information, IEEE Trans. Smart Grid 4 (2013) 235–244.
[34] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, A. Safdarian, Impact of WAMS malfunction on power system reliability assessment, IEEE Trans. Smart Grid 3 (2012) 1302–1309.
[35] M. Panteli, P.A. Crossley, D.S. Kirschen, D.J. Sobajic, Assessing the impact of insufficient situation awareness on power system operation, IEEE Trans. Power Syst. 28 (2013) 2967–2977.
[36] H. Lei, C. Singh, A. Sprintson, Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems, 2014.
[37] K. Jiang, C. Singh, New models and concepts for power system reliability evaluation including protection system failures, IEEE Trans. Power Syst. 26 (2011) 1845–1855.
[38] B. Falahati, Y. Fu, Reliability assessment of smart grids considering indirect cyber-power interdependencies, IEEE Trans. Smart Grid 5 (2014) 1677–1685.
[39] S. Chiaradonna, F.D. Giandomenico, P. Lollini, Definition, implementation and application of a model-based framework for analyzing interdependencies in electric power systems, Int. J. Crit. Infrastruct. Prot. 4 (2011) 24–40.
[40] M. Beccuti, S. Chiaradonna, F. Di Giandomenico, S. Donatelli, G. Dondossola, G. Franceschinis, Quantification of dependencies between electrical and information infrastructures, Int. J. Crit. Infrastruct. Prot. 5 (2012) 14–27.
[41] D.T. Nguyen, Y. Shen, M.T. Thai, Detecting critical nodes in interdependent power networks for vulnerability assessment, IEEE Trans. Smart Grid 4 (2013) 151–159.