Krivohlava *et al. Energy Informatics* (2022) 5:33
https://doi.org/10.1186/s42162-022-00218-3

Energy Informatics

REVIEW Open Access

Failure and fault classification for smart grids

Zuzana Krivohlava, Stanislav Chren* and Bruno Rossi

*Correspondence:
chren@mail.muni.cz

Faculty of Informatics, Masaryk University, Brno, Czech Republic

Abstract

Smart grid (SG) has been designed as a response to the limitations of traditional power grids caused by growing power supply demands. SG is considered a critical infrastructure in which dependability plays a crucial role and manifestation of failures can lead to severe consequences. Architecture-wise, SGs can be decomposed in several layers comprising variety of physical, software, communication and business components, each representing a potential point of failure determined by their underlying faults. In this paper, we present a systematic literature review surveying 30 different faults and failures which can occur in the SG infrastructure. The discovered faults and failures are investigated to extract details about their causes, impacts, detection techniques and counter-measures. Based on the collected information, the faults and failures are classified and mapped to Smart Grid Reference Architecture Model (SGAM), providing a useful frame of reference for practitioners and researchers dealing with hardware and software dependability in this complex domain.

Keywords: Smart grid, Reliability engineering, SGAM, Systematic literature review

Introduction

Smart Grids (SG) represent an evolution of the concept of traditional power grids. While traditional power grids were centralized power systems, modern SGs represent two-way IT-supported communication between energy providers and customers, which allows the delivery of electricity in a more efficient, reliable, sustainable way (Fang et al. 2011). An SG is composed of several components that can include: Advanced Metering Infrastructure (AMI) and smart meters, Supervisory control and data acquisition (SCADA), sensors and a multitude of network communication protocols (Gao et al. 2012; Yu et al. 2011; Chren et al. 2016). The complexity of the SG infrastructure is reflected in the multitude of faults and failures that can emerge from different components and their interrelations, leading often to complex failure scenarios with potential cascading and disruptive effects (Rivas and Abrao 2020; Mousa et al. 2019; Otuoze et al. 2018). Thus, an important aspect is to be able to classify and determine the possible faults and failures that can impact SGs, to look at the causes for preventive measures and at consequences and countermeasures to counteract the effects of failures.

The goal of this paper is to review and classify existing faults and failures in SGs to provide a summary view of all the causes, consequences, and countermeasures that can be applied. To review the existing SG failures and faults we adopt the Systematic Literature

Review (SLR) approach, collecting and classifying information from 50 articles that were filtered during the process. The types of faults/failures and their belonging to specific categories in the SG system were synthesised primarily from the causes, impacts and descriptions that were collected from the articles. Synthesised data was then examined and summarised to provide information concerning the most common types of faults and failures. Afterwards, we looked at common detection techniques and methods for countermeasures. From the list of all determined impacts, we uncovered the most recurrent general consequences and connected them to the causing faults/failures—building also chains of faults and failures that can be represented as graphs.

The main contribution of this paper is the collection of 30 faults/failures from 50 articles in the context of Smart Grids. Such faults/failures were defined, categorized, and then linked to the areas and domains of the Smart Grid Conceptual Model and the Smart Grid Architecture Model (SGAM) (Bruinenberg et al. 2012). Among others, we cover aspects such as causes, countermeasures, impacts, and faults/failures chains. Unlike some of the similar studies surveying the fault or security issues in SG (Rivas and Abrao 2020; Otuoze et al. 2018), we do not aim to propose new fault classification and architecture schemes for SGs. Instead, we map the extracted faults and failures to an established dependability taxonomy (Avizienis et al. 2004) as well as the SGAM model (Bruinenberg et al. 2012). The final classification can be useful for both practitioners and researchers dealing with dependability engineering in the context of Smart Grids.

The paper is structured as follows. In "Related work" section we discuss existing previous reviews about faults and failures in SGs: covering power, security faults and failures and giving classifications of different faults/failures types and detection techniques. In "Background" section, we review the concept of SG, in particular the SGAM model, and provide the main concepts related to reliability engineering that will be used in the remaining parts of the paper. In "Literature survey" section, we define the research questions and propose the methodology that has been applied for building the catalogue of faults / failures. In "Faults and failures in smart grids" section we answer the main research questions of the study, determining major faults and failures in SG, their classification by type, causes, impacts, consequences, fault chains, and countermeasures. In "Conclusions" section we conclude the paper.

Related work

To the best of our knowledge, there are not many papers dealing with the provision of a summary view of faults and failures types in SGs. We collected the major previous studies in Table 1. With the ongoing interest for SG cybersecurity, several studies providing a list of main attack types against SGs including countermeasures were published, such as Mathas et al. (2020); Wang and Lu (2013)—in some cases dealing with security threats leading to SG failures (Otuoze et al. 2018). Other reviews are more focused on power faults (Mousa et al. 2019), and on faults classification and detection (Sarathkumar et al. 2021; Rivas and Abrao 2020).

Mathas et al. (2020) classify attacks to Smart Grids in confidentiality, integrity, and availability attacks. Confidentiality attacks such as passive eavesdropping, man-in-the-middle, and spoofing attacks can be detected and mitigated with countermeasures such as cryptographic signatures and inspection of network packets. Integrity attacks such as

Table 1 Related works

Year	Article	Focus	Results
2021	Sarathkumar et al. (2021)	Faults Classification	15 SG faults with causes, effects, and diagnosis
2020	Rivas and Abrao (2020)	Faults Detection	65 faults detection and location approaches
2020	Mathas et al. (2020)	Security Failures	Faults related to confidentiality, integrity and availability cyber-attacks
2019	Mousa et al. (2019)	Power Faults	Classification of power faults and techniques for monitoring and detection
2019	Hlalele et al. (2019)	Faults Classification and Identification	16 types of faults in power distribution, photovoltaic and wind turbine categories.
2018	Otuoze et al. (2018)	Security Failures	Classification of security threats leading to SG failures
2013	Wang and Lu (2013)	Security Failures	Detection and mitigation of failures derived from cyber-attacks

false data injection attacks can relate to tampered data packets of false measurements. They can be counteracted with machine learning models and software infrastructure taking into account cryptographic techniques. Availability attacks such as Denial of Service (DoS) happening at different layers (physical, MAC, network and transportation layer) can be detected and mitigated by means of several monitoring and self-healing approaches.

Wang and Lu (2013) extensive survey identifies several challenges for the detection and mitigation of security threats. Challenges go in the direction of proactive countermeasures for DoS attacks, cryptographic measures for Smart Grids, and the design of secure network protocols and architectures.

Otuoze et al. (2018) provide a review of various security threats and challenges that do not represent specifically failures but may result in a failure being the outcome. Authors distinguish between technical and other sources of SG threats. Technical sources deal with infrastructure security (such as Advanced Metering Infrastructure (AMI), Smart meters and power theft), technical operational security, and system data management security. Non-technical sources of security threats are related to environmental threats (e.g., earthquakes), and governmental regulatory policies.

In Mousa et al. (2019) different types of power faults, impacts, and countermeasures are presented. Power faults can be classified into short circuits and open circuit faults with incipient, abrupt and intermittent categories. These faults can be detected by means of several monitoring techniques, such as using wavelet transforms to detect the duration of disturbances in the power signal.

A brief summary of faults in smart grid infrastructure is provided by Hlalele et al. (2019). They distinguish between faults related to power distribution, photovoltaic and wind turbines and outline possibilities of the fault identification.

The most comprehensive summaries of faults similar to the current review were found in both (Rivas and Abrao 2020; Sarathkumar et al. 2021) that deal with the classification of faults and the discussion of countermeasures.

Rivas and Abrao (2020) mostly focuses on monitoring and detection techniques, dividing Smart Grids faults in physical devices, communication and hardware/software faults. Sensors and monitor capabilities can be adopted to provide self-healing mechanisms. The authors provide 65 faults detection and location approaches that were discussed

in previous research (e.g., real-time anomaly detection of smart meter data). Methods for fault detection location are divided into impedance-based methods (e.g., waveform measurements to detect power disturbances), analytical methods (e.g., signal processing techniques), learning-based methods [(e.g., forecasting with Artificial Neural Networks (ANN)].

Sarathkumar et al. (2021) provide 15 common types of faults which are discussed according to causes, effects and diagnosis methods. The faults are collected and reported from previously published research papers. Similarly to previous reviews (e.g, Mousa et al. (2019)), faults are classified into incipient, abrupt, and intermittent faults.

Compared to previous reviews, our surveys of faults and failure has the following main contributions:

1. the provision of a list of 30 faults/failures in the context of Smart Grids that are linked to the areas and domains of the SGAM model (Bruinenberg et al. 2012) as well as to one of the main dependability taxonomies (Avizienis et al. 2004) (in "Faults and failures in smart grids" section). Unlike the related work (e.g. Rivas and Abrao (2020); Sarathkumar et al. (2021)) that proposed their custom taxonomies, we believe that grounding our classification in the already established taxonomies would be more beneficial for the practitioners as they could find the context more familiar;
2. the first review attempting to provide a linkage in form of graphs for the most common consequences and chaining of faults and failures (in "Causes and impacts (RQ4)" section);
3. to the best of our knowledge, this is the first of this kind of reviews conducted as a Systematic Literature Review (SLR), tracing the sources throughout the process;

Background

Smart grids

In this study, we use SGAM (Bruinenberg et al. 2012) when referring to smart grid elements as shown in Fig. 1. The SGAM is a three-dimensional, multi-layered framework that consists of the interoperability layers that are mapped on the smart grid pane. The smart grid pane is spanned by physical electrical domains and information management zones. The purpose of this model is to indicate which zones of information management interactions between domains take place. It allows the presentation of the current state of implementations in the electrical grid, and also depict the evolution to future smart grid scenarios.

In this section, we briefly present the three SGAM dimensions that are used to organize the survey results and classification.

The SGAM domains represent a set of roles and services involved in the energy industry:

- *Generation* generators of electrical energy in bulk quantities (e.g. fossil, nuclear and large-scale hydropower plants), that are connected to the transmission system.
- *Transmission* infrastructure and organization responsible for carrying bulk electricity over long distances.

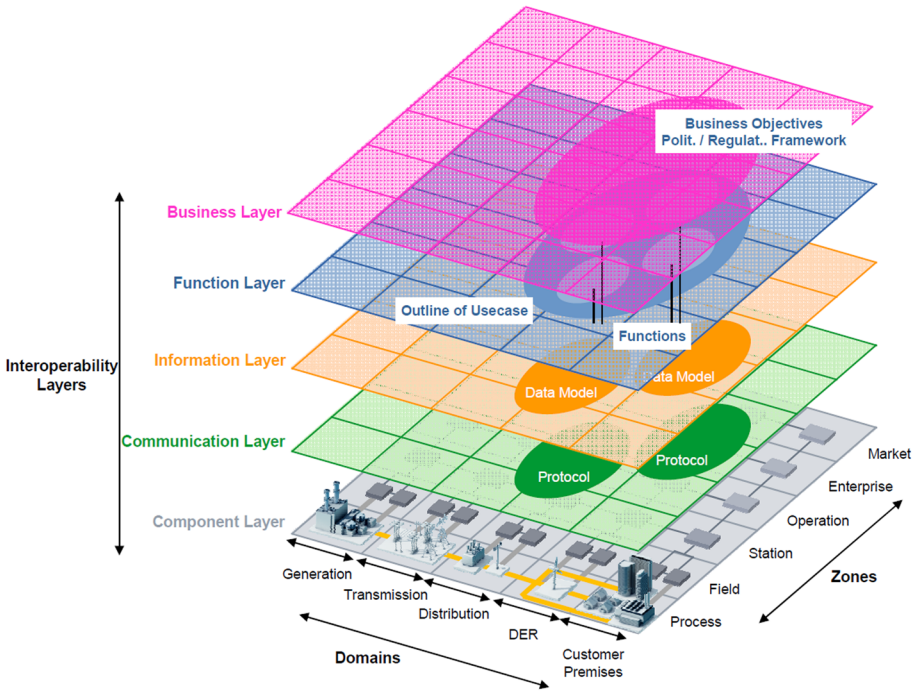

Fig. 1 The SGAM framework (Bruinenberg et al. 2012)

- *Distribution* infrastructure and organization responsible for delivering electricity to and from customers.
- *DER* small-scale distributed resources connected directly to the distribution system. May also include energy storage devices.
- *Customer premises* industrial, commercial and residential end-users of electricity managing their use of energy, they may also act as producers or storage of energy.

Smart grids largely depend on the interconnection and information exchange between different systems. Within SGAM, such interoperability is described by the five layers (Bruinenberg et al. 2012):

- *Business layer* includes regulatory and economic structures and policies, business models, business portfolios of market parties involved. Business capabilities and business processes are also part of this layer.
- *Function layer* represents functions and services provided by SG and their relationships from an architectural viewpoint. Functions are described as extracted use case functionalities separated from actors.
- *Information layer* deals with the format and semantics of information exchanged between functions, services and components to ensure interoperable exchange of information during communication. It includes information objects and data models.
- *Communication layer* is responsible for interoperable communication by describing appropriate protocols and mechanisms.

- *Component layer* encompasses all the components of the SG and their physical distribution.

Finally, the SGAM zones represent the hierarchical levels of power system management, aggregation and functional separation. The aggregation can be on a data level or spatial level. The former deals with aggregating the data from the field zone to the station zone in order to reduce the volumes of data to be sent to and processed by the operation zone. The latter represents, for example, aggregation from distinct locations to wider areas or the aggregation of data from customers' smart meters by data concentrators in the neighbourhood, as there are many data analysis techniques that can be applied in the context of SGs (Rossi and Chren 2019).

- *Process zone* represents all the primary power grid equipment designed for energy generation, transmission and distribution (e.g. generators, transformers, circuit breakers, overhead lines, cables, electrical loads). Physical energy conversion is also part of this zone (electricity, solar, heat, water, wind).
- *Field zone* consists of equipment to protect, control and monitor the process of the power system (e.g. protection relays, bay controllers and intelligent electronic devices (IEDs) which receive and utilize power system process data)
- *Station zone* describes the aggregation level for fields, e.g. for data concentration, substation automation.
- *Operation zone* consists of all sorts of management systems controlling different parts of the grid such as distribution management systems, energy management systems in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle fleet charging management systems etc.
- *Enterprise zone* refers to the commercial and organizational processes, services and infrastructures for enterprises (e.g. asset management, staff training, customer relation management, billing and procurement).
- *Market zone* includes operations of the market domain such as energy trading, mass market, retail market.

Reliability engineering

For the classification of faults and failures, we adopt the general taxonomy proposed by Avizienis et al. (2004)—failures can be classified by four criteria:

- *Failure domain* recognises failures of content and timing failures. *Content failure* represents information delivered by the service, that differs from the desired (implemented) form. *Timing failure* occurs when the service is delivered at the incorrect time or for the wrong duration. Timing failure can be further classified as *early* or *late*, depending on the system being delivered too soon or too late. *Content and timing failure* is a combination of the two aforementioned failures. If the system's activity is no longer perceptible, it is called a *halt failure*. It can be also labelled as an *erratic failure* when the service is delivered, but its content and timing are off.

- *Consistency* considers the view of different users. *Consistent failure* is observed equally by all users, whereas an *Inconsistent failure* is perceived variously by different users.
- *Detectability* determines whether a failure was signalled to the user. *Signalled failure* is detected and a signal warning is sent. Otherwise, it is an *Unsignalled failure*.
- *Consequences* determine the severity of failure's impact. Failures span the range from *minor* to *catastrophic consequences*.

Additionally, besides the service failures, there are also *Dependability (or security) failures* which relate to more frequent or severe service failures of the system than it is acceptable and *Development failures* which occur when the development process is terminated before the system is placed into service.

Faults can be classified into eight categories (Avizienis et al. 2004):

- *Phase of creation* determines when the fault occurred. it can occur either during system development and maintenance *Development fault*) or during the system's operation phase (*Operational fault*)
- *System boundaries* show where the fault originates from. It can arise within the system *Internal fault* or from the outside of the system boundary (*External fault*)
- *Phenomenological cause* depends on whether there were human activities involved and it can be caused by natural phenomena (*Natural fault*) or as a result of human actions (*Human-made fault*).
- *Objective* can be specified in case of human-made faults and we distinguish faults induced with the intention of causing harm (*Malicious fault*) or without a malignant purpose (*Non-malicious fault*)
- *Intent* refers to the intention of non-malicious human-made faults. They can be an outcome of a harmful decision (*Deliberate fault*) or caused without awareness (*Non-deliberate fault*)
- *Capability* considers competence of non-malicious human-made faults. *Accidental fault* happens by mistake and *Incompetence fault* results from lack of professional competence.
- *Dimension* distinguishes between *Hardware fault* affecting physical components and *Software fault* occurring in programs or data.
- *Persistence* considers the duration of faults which can remain continuous in time (*Permanent fault*) or its presence can be bounded in time (*Transient fault*)

Apart from the classification of faults and failures we further investigate their details that could be helpful for smart grid stakeholders. In accordance with the reliability engineering goals and inspired by the failure mode and effects analysis (FMEA) (Stamatis 2003), we extract information about faults and failures causes, impacts, detection techniques and counter-measures.

Literature survey

We adopted the Systematic Literature Review (SLR) (Keele 2007) methodology. An SLR provides a structured method to conduct detailed surveys of a given topic and can be considered a suitable approach for the goals of this article, as the identification of fault/

failure types requires detailed research among all published research to gather information about faults/failures as determined in the context of Smart Grids.

To carry out the SLR, we followed the SLR guidelines (Keele 2007) for the planning, execution, and reporting of the review. We next describe the SLR process and provide the review protocol. First, we mentioned pre-existing studies that related to the topic in a previous part of the paper ("Related work" section). After that, we define research questions ("Research questions (RQs)" section) and specify the search strategy ("Search strategy" section) to clarify what information will be searched and how. Results of the search need to be examined and filtered with respect to a set of chosen selection criteria ("Study selection criteria" section).

Research questions (RQs)

With respect to the aim of the review, the following questions were considered:

RQ1 *What **faults** and **failures** occur in smart grids?* The aim of this RQ is to provide an extensive list of all the different faults and failures that are reported by SG research.

RQ2 *In what **component** of smart grids are the faults/failures involved?* The goal of this RQ is to classify the failures and faults into SGAM domains, layers, and zones to see how many failures and faults are propagating in these different contexts.

RQ3 *What is the **type** of a particular discovered fault/failure?* The goal of this RQ is to provide the types of failure and faults in SG according to an orthogonal classification (e.g., hardware/software related, operational, etc...).

RQ4 *What are the **causes** and **impacts** of the faults/failures?* The goal of this RQ is to provide a graphical representation linking the faults and failures to their usual causes and consequences.

RQ5 *What **detection techniques** and **countermeasures** are used in connection with a given fault/failure?* The goal of this RQ is to provide an extensive list of any detection techniques that are commonly adopted for the detection of faults/failures and then common countermeasures put into place to respond to the critical situation.

Search strategy

The search for the review was conducted within three different digital libraries, namely ACM Digital Library, IEEExplore and Elsevier ScienceDirect. With regard to search terms, the following three variants were considered: after the definition of the best combination of terms, following the Patient, Intervention, Comparison and Outcome (PICO) suggestions to build the query (Frandsen et al. 2020), we adopted the following query:

- ("smart grid" AND fault) OR ("smart grid" AND failure) OR ("power grid" AND fault) OR ("power grid" AND failure)

As we needed very specific types of papers to collect faults and failures, we adopted a specific search strategy: collecting first a set of core relevant papers and then looking at the referenced papers that could provide more relevant results [(so-called *snowballing* in SLR terminology (Wohlin 2014)]. We run the search query in each repository and we shortlisted 20 studies for each of the repositories that were considered relevant after

reviewing the abstracts (Fig. 2). This led to a core-set of 60 papers. From this core-set of papers, we reviewed the reference list and we added additional papers that were considered relevant from the titles. All included papers were then refined by looking at the abstracts.

Study selection criteria

To determine which papers to accept or deny, inclusion and exclusion criteria were formulated. The inclusion criteria list consists of:

- IC1 studies that include a description of a fault/failure in a smart grid and possibly its causes and consequences,
- IC2 studies published in journals and conference proceedings,
- IC3 year of publication in the range of 2010 - 2021,
- IC4 English language only.

As for the exclusion criteria, we defined the following:

- EC1 studies that do not concern faults/failures in smart grids,
- EC2 studies discussing only faults in general (e.g. fault tolerance, fault detection etc.) that do not mention any specific fault/failure.

Study selection process

Since the review was targeted at the identification of specific failures and faults, we followed a search approach that was attempting to include the largest amount of papers and then filtering based on the most relevant references. For this reason, due to the extensive number of search results, the results were sorted by relevance and thoroughly examined the most relevant papers in every digital library along with their promising references. The total number of examined studies was 189 (20 from each digital library, 129 relevant references). The primary resulting studies often did not provide sufficient findings, but they provided many potentially relevant references.

Thereafter, all the full texts of the chosen papers were read and checked for the fulfilment of the remaining criteria: only the papers containing a description of a fault/failure with at least a brief mention of its causes or consequences were included in the review's results. Ultimately, 50 papers were selected out of which 30 different faults or failures types were extracted. During the whole review, a list of all examined papers was maintained with notes about their acceptance or rejection. The list of all papers surveyed

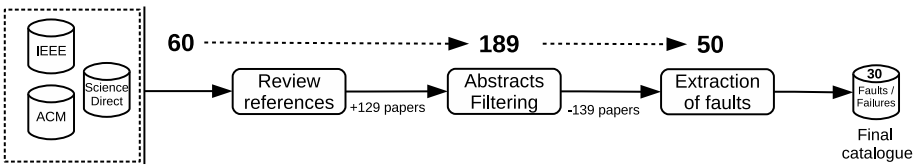

Fig. 2 The SLR process with # of articles in each phase

and the final table with all the failures and faults collected is available in a downloadable dataset (Authors 2022).

Data extraction and synthesis

Data extracted from selected studies encompass following information about a fault or failure:

- name,
- description,
- type,
- causes,
- detection techniques,
- involved components,
- impacts,
- countermeasures.

While data items such as name, description, cause, detection, impact and countermeasures were usually extracted directly from a study, involved components and the type of a fault/failure had to be often determined from the context using the SGAM model of domains, layers and zones (Fig. 1) and types of faults and failures collected during the review.

Faults and failures in smart grids

In the next sections we answer the five research questions (set in "Research questions (RQs)" section) by building a catalogue of SG faults and failures, mapping them to the SGAM levels, and extracting information about causes, consequences, detection techniques and countermeasures.

Overview of faults and failures (RQ1)

In the list below, we provide answers to question RQ1 by reporting 30 found faults and failures as well as their brief description. We also list a total of 50 references to the studies from which the data about specific faults/failures were extracted.

F1 **Connection loss between the smart meter and local controller**—Wireless communication between the smart meter and the controller is disrupted because the particular communication channel is unavailable due to a channel jamming attack (Alohali and Vassilakis 2017; Mathas et al. 2020; Wang and Lu 2013; Liu et al. 2017).

F2 **Connection loss from all IEDs to the substation gateway**—IEDs are responsible for monitoring and controlling automated devices in distribution and they can perform operations such as tripping circuit breakers if they sense voltage, current, or frequency anomalies. If their connection to the substation is lost, those operations cannot be performed correctly (Mathas et al. 2020; Wang and Lu 2013).

F3 **Collision in a Wireless Sensor Network (WSN)**—Collisions can occur when a large number of messages are sent (possibly premeditatedly by an attacker), that

can interfere with normal protocol communication (Alohali and Vassilakis 2017).

F4 **Maliciously forged identities in a WSN**—A single malicious node can forge many identities and therefore mislead the legal nodes (Alohali and Vassilakis 2017; Najafabadi et al. 2013).

F5 **Data aggregator's buffer overflow**—The event buffer of a data aggregator is filled, and therefore is unable to buffer critical alerts (Mathas et al. 2020; Wang and Lu 2013; Jin et al. 2011).

F6 **Black hole in the network**—In a communication network a node can drop a certain portion (possibly all) of packets instead of forwarding them further (Kaplantzis and Şekercioğlu 2012).

F7 **Software Defined Network (SDN) controller failure**—With the use of software-defined networking in SG communications, SDN controllers can be seen as a single point of failure, as it is solely responsible for flow control in a network (Ghosh et al. 2016).

F8 **Desynchronized measurements**—Measurements like consumption and production values have to be synchronized, often with the use of GPS for obtaining a time stamp. If a GPS signal is forged, then measurements are sent to the WAMS (wide-area monitoring system) with wrong timestamps and therefore not synchronized (Mathas et al. 2020; Gong et al. 2012).

F9 **False state estimate**—A key function in building a real-time network model in the energy management system in the state estimation, based on data periodically collected from remote meters. False state estimates can be a consequence of random errors in measurements or bad data injection attacks (Liu et al. 2013; Mathas et al. 2020; Wang and Lu 2013; Cui et al. 2012; Liu et al. 2013).

F10 **Programmable logic controller (PLC) hijacked**—During the Stuxnet worm attack on Iran's nuclear facilities discovered in 2010, the PLCs were hijacked by inserting a rogue code into the controllers. Thereafter, the controllers were monitored and eventually, the rogue code took control without the legitimate controller code noticing (Langner 2011; Trellix 2021).

F11 **Inconsistent energy consumption reports**—Data concerning energy consumption can be tampered with locally or remotely either before being sent to smart meters, inside the smart meters or over the communication links. For example, the reported energy consumption can be smaller than the actual one which is done in order to pay less than the real price for the consumed energy (an energy theft) (Jokar et al. 2016).

F12 **Privacy leakage**—Malicious users can access smart meters to obtain collected fine-grained power usage data and therefore invade customers' privacy (Birman et al. 2015; Federal Office for Information Security (BSI) 2013; Wang and Lu 2013; McDaniel and McLaughlin 2009).

F13 **Compromised price signals**—The real-time prices advertised to smart meters are compromised by a scaling factor (so that the meters will use the wrong prices) or by corrupted timing information (so that the meters will use old prices) (Tan et al. 2013).

F14 **Inconsistent state messages**—In a distributed energy routing, nodes inform each other how much energy they request or supply. In addition, correct energy link

state information is also needed for the energy routing process. Spreading incorrect information can disrupt the energy distribution process (Lin et al. 2012).

F15 **Frequency variation**—A stable frequency synchronized throughout the whole electrical grid is required for the grid's stability. Frequency pushed outside the 47-52Hz range (50Hz being the optimal value in Europe) can cause instability of the electrical grid possibly leading to a total blackout (Costache et al. 2011; Samarakoon and Ekanayake 2009).

F16 **Voltage variation**—Tolerance limits for voltage variation are +10 % and -15 % around the optimal value (230V in Europe). Manifestations of voltage variations include short interruptions, flickers, voltage dips, supply voltage variations and harmonic disturbances (Costache et al. 2011).

F17 **Transformer failure**—Transformers are crucial constituents of electrical transmission and distribution systems and they can fail due to many different causes (Bhatt et al. 2014).

F18 **Series fault**—Also known as an open circuit fault, occurs when one or more conductors (phases) open in the system due to a broken line. It can be further divided into unsymmetrical and symmetrical series faults (Mousa et al. 2019; Gururajapathy et al. 2017; ElectronicsHub 2015).

F19 **Shunt fault**—Alternatively called a short circuit fault, represents an abnormal connection of very low impedance between two points of different potential, whether made intentionally or accidentally. There are different types of shunt faults, such as Single line to ground fault (most common, least severe); Line to line fault (second most common, less severe); Double line to ground fault (less common, more severe); Three-line to ground fault or Three line to ground fault (Mousa et al. 2019; Gururajapathy et al. 2017; ElectronicsHub 2015).

F20 **Geomagnetically Induced Currents (GIC) in the power grid**—Geomagnetic storms induce GIC in the power grid, that then flows through the power transformer causing half-wave saturation of the iron core and generating a large amount of reactive power loss, possibly resulting in cascading failures and large-scale blackouts (Kang et al. 2019).

F21 **Flashover fault in a transmission line**—Various natural phenomena like forest fires can cause an electric discharge - a flashover in a transmission line (Yue et al. 2017).

F22 **Transmission line break off**—A transmission line can break off due to weather factors like ice or wind that can increase the mechanical stress of the line (Jin et al. 2017).

F23 **Lightning stroke trip-out of a transmission line**—Lightning stroke presents an important threat to the power grid infrastructure, specifically, transmission lines are often exposed to lightning (Li et al. 2016; Bakar et al. 2013).

F24 **Cascading failure**—The effect of one or a few component (typically transmission line) failures, leading to the failure of a sequence of interconnected components in a networked system (Chen et al. 2014; Min and Varadharajan 2016; Bernstein et al. 2012, 2012; Wang et al. 2017; Eppstein and Hines 2012; Wei et al. 2019).

F25 **Fault current**—The rising integration of renewable energy sources in the smart grid increases the fault current level of the system (Reddy and Chatterjee 2017;

Jangale and Thakur 2017; Liu et al. 2019; Rajaei et al. 2014; Rajaei and Salama 2015).

F26 **Hurricane damage**—Hurricanes can have devastating consequences on a power grid's generation, transmission and distribution, like in the case of Hurricane Maria in Puerto Rico, 2017 (Kwasinski et al. 2019; Menasché et al. 2014).

F27 **Supply uncertainty in DERs power generation**—Uncertainty comes from perturbation of the amount of energy generated by the DERs from the generation schedule due to factors like the change of the wind speed and the sunlight intensity or equipment failure (Yang and Walid 2014).

F28 **Tripping of a distributed generator in a microgrid**—Due to the intermittent nature of its distributed generators, a microgrid in an islanding mode can suffer from severe frequency deviation during the post-fault condition that can eventually lead to tripping of the generators (Mousa et al. 2019; Kabir e al. 2014; Arif and Aziz 2017).

F29 **DC series arc fault in photovoltaic (PV) systems**—The rising of PV systems and the trend toward higher DC voltage levels may potentially create DC arc faults. DC arcing appears across small gaps in connections (Lu et al. 2017).

F30 **Wind turbine gearbox failure**—Wind turbine gearbox transmits mechanical energy into the generator with high speeds. It is one of the most fragile components since it is responsible for 59 % of total wind turbine failures (Wang et al. 2017).

From the list of discovered faults and failures, it becomes apparent that the faults and failures are largely varied in the literature. However, half of them is referenced from multiple sources with F24, F25, F1, and F12 being the most referenced ones. Additionally, the literature covers faults and failures on different levels of abstraction ranging from general faults and failures, such as F24 to very specific ones, such as F7 or F20.

Domain, layer and zone classification (RQ2)

The faults and failures were mapped into SGAM domains, layers and zones as defined in "Background" section based on their characteristics. In the case of zones and domains, one fault/failure could be assigned to more domains depending on their origin and the range of their impact. The resulting mapping is shown in Fig. 3.

All SGAM domains were covered by at least two faults or failures. The most frequent domain was the Transmission with 18 distinct faults and failures closely followed by the Distribution domain with 16 results.

In terms of SGAM zones, we were able to map faults and failures to Process, Station, Operation and Market zones. We did not find any suitable fit for the Enterprise and Field zones. In the latter case, they seemed to be close enough to the Field zone but after careful examination, we attributed them to the Operation and Station Zones. The most frequent were the Process and Operation zones with 11 and 10 faults and failures respectively, spread across all the domains.

From the SGAM layers perspective, the Component and Communication layers were the most prominent with 16 and 9 faults and failures respectively. The Information and Function layers were rarer with only two findings for each. Additionally, we did not discover any faults and failures related to the Business layer. An interesting observation can

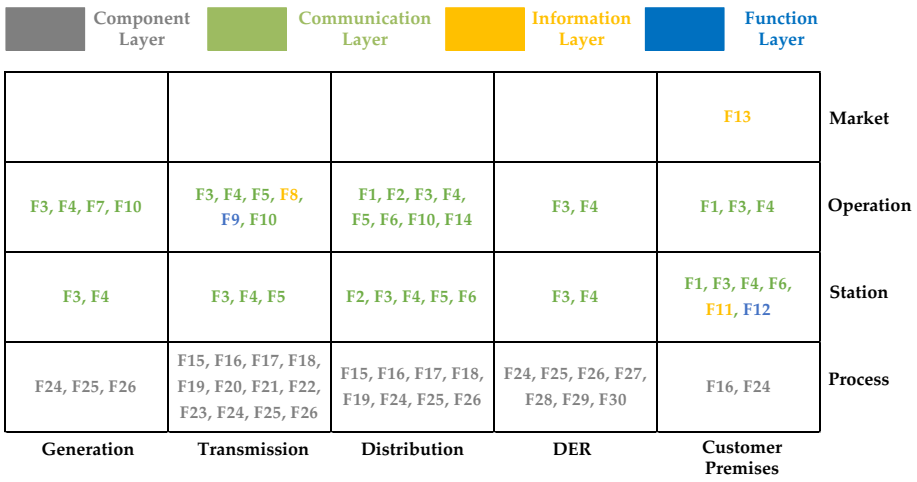

Fig. 3 RQ2. Mapping of faults and failures to SGAM domains, zones and layers

be made about the relation between the layers and zones. All Component layer faults and failures are present only in the Process zones. The Communication layer faults and failures are distributed between Operation and Station zones with frequent overlaps especially for F3, F4. On the other hand, there are no Communication layer faults and failures in Process and Market zones.

Classification of faults and failures (RQ3)

The classification of faults and failures described in "Reliability engineering" section was applied to the findings listed earlier in "Overview of faults and failures (RQ1)" section. The findings were classified based on the Tables 4 and 7. Additionally, full texts of the related papers were consulted for better comprehension of the fault/failure's characteristics.

First of all, we divided the findings into faults and failures. However, some failures could also be considered faults, since they may lead to another failure. As a result, some findings are labelled both as a fault and a failure.

The Table 2 includes 27 faults classified by 12 attributes. All faults were operational, nevertheless, 3 of them (F7, F17, F19) could also be identified as development faults depending on the circumstances. A similar situation appears also in other categories like internal-external, HW-SW etc. because one particular fault can have multiple different causes (more in "Causes and impacts (RQ4)" section) and therefore fall in different categories. External faults appeared more frequently than internal ones. the Same amount of natural and human-made faults was found, although malicious faults significantly outweighed non-malicious ones (deliberate and non-deliberate). The capability category (accidental and incompetence faults) was not taken into consideration as the available information about the faults was not sufficient to determine this category. Hardware faults were slightly more common than software faults and the persistence category was divided more or less equally.

Regarding failures, Table 3 presents 17 different failures categorized by failure domains and consistency. On top of that, failure F24 is assigned to a special category of

Table 2 RQ3 (Types of faults according to taxonomies defined in "Reliability engineering" section)

Fault	Operational	Development	Internal	External	Natural	Malicious	Non-deliberate	Deliberate	Hardware	Software	Transient	Permanent
F1	✓			✓		✓			✓		✓	
F2	✓			✓		✓				✓		✓
F3	✓		✓	✓		✓	✓			✓	✓	
F4	✓			✓		✓				✓	✓	✓
F5	✓		✓	✓		✓				✓	✓	
F6	✓			✓		✓				✓		✓
F7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
F8	✓			✓		✓				✓	✓	
F9	✓		✓	✓	✓	✓				✓	✓	
F10	✓			✓		✓				✓		✓
F11	✓		✓			✓			✓	✓		✓
F13	✓			✓		✓				✓	✓	✓
F14	✓			✓		✓				✓	✓	
F15	✓		✓		✓	✓			✓		✓	
F16	✓		✓		✓	✓		✓	✓		✓	
F17	✓	✓	✓	✓	✓		✓	✓	✓			✓
F18	✓		✓		✓				✓			
F19	✓	✓	✓	✓	✓	✓	✓	✓	✓			
F20	✓			✓	✓				✓		✓	
F21	✓			✓	✓				✓		✓	
F22	✓			✓	✓				✓			✓
F23	✓			✓	✓				✓			✓
F25	✓		✓		✓				✓		✓	
F26	✓			✓	✓				✓			✓
F28	✓		✓		✓				✓			✓
F29	✓		✓		✓				✓			
F30	✓		✓	✓	✓				✓			✓
Total	27	3	14	20	16	16	4	4	17	12	13	12

Dependability failures, because it presents a very serious threat due to its severe consequences. Out of all the failures, 15 were also mentioned as faults. As for the domain category, most of the failures were designated as halt failures, in addition, some content and late timing failures also appeared. The consistency category ended up balanced. Just like in the case of faults, some failures were assigned to more types within a category.

After careful consideration, one finding F27 was marked as neither fault nor failure, but an error, more specifically a content, inconsistent error. The supply uncertainty is caused by the perturbation of the amount of generated energy that could be perceived as a fault, and it may lead to a failure such as a power outage.

Causes and impacts (RQ4)

We report the findings for RQ4 in Tables 4 and 7, introducing every cause and impact of found faults/failures that we were able to extract from the reviewed studies. Here, we report only the causes and impacts that have been extracted from the literature associated with SGs as a result of SLR. However, it is possible for the individual faults and failures that other causes and impacts exist, especially when the fault or failure is more generic and can occur in different domains.

We identified the most common consequences of the found faults or failures:

- Power outage (14 causes)
- Financial loss (9 causes)
- Equipment damage (8 causes)
- Loss of network connectivity (5 causes)

These consequences are pictured in Fig. 4 along with the faults/failures that may cause them.

Table 3 RQ3 (Types of failures)

Failure	Dependability	Content	Late timing	Halt	Inconsistent	Consistent
F1				✓		✓
F2				✓	✓	
F3			✓	✓	✓	
F5			✓	✓	✓	
F6				✓	✓	✓
F7			✓	✓	✓	✓
F9		✓				✓
F11		✓			✓	
F12		✓			✓	
F13		✓	✓		✓	
F14		✓			✓	
F17				✓		✓
F22				✓		✓
F23				✓		✓
F24	✓					
F28				✓		✓
F30				✓		✓
Total	1	5	4	11	9	9

Table 4 RQ4 (Impacts of found faults and failures)

F/F	Impacts	F/F	Impacts
F1	• Impaired network performance of power substation systems can cause delayed delivery of time-critical messages or DoS • preventing the local controllers from receiving complete data samples for state estimation • undermined demand-respond system	F16	• Major physical and economical damage to the customer • customers and the electrical company may lose money • damage to the electrical appliances
F2	• After shutting down the connections, an attacker can masquerade itself as a monitoring IED and send false close/open messages to switches • loss of both availability and integrity • mess-up status of the protection system • potential loss of power supply for customers	F17	• Power outages • personal and environmental hazards • expensive re-routing or purchase of power from other suppliers
F3	• Node exhaustion • consumption of valuable limited resources	F18	• Increase of frequency and voltage • current reduction • unbalance of voltages and currents can cause equipment damage • increased voltage levels may lead to insulation failures and short circuit faults
F4	• Interferes with many network operations including routing voting, data aggregation and reputation evaluation	F19	• Current's increment can cause equipment overheating: reduced life span of insulation • fall in voltage and frequency • fire and explosion in equipment (e.g. transformers, circuit breakers) • limited power flow
F5	• Negative impact on the control station's situational awareness • significant loss of real events	F20	• Half-wave saturation of transformer iron core • temperature rise and vibration of transformer • reactive power demand and active power loss • voltage collapse • inadequate reactive power capacity, that can lead to destructive accidents, e.g., the damage of power grid equipment
F6	• Decline in network connectivity and packet delivery	F21	• Can lead to block faults of transmission lines
F7	• Delays of data packets • network congestions • packet losses • packet retransmissions	F22	• Power outage
F8	• Negative impact on the accuracy and effectiveness of many SG functions, e.g., event localization, monitoring voltage stability and fault detection on transmission lines	F23	• Damage to the transmission line • power outage
F9	• Wrong control decisions and sending false commands conceivably leading to large-scale malfunction • financial losses • increase in reported consumption of some nodes, decrease of other nodes	F24	• From local impact to a large blackout • customer electricity service disturbance • damage to the power grid (e.g. unstable voltage) • benefiting the attacker (e.g. lower power rates)
F10	• At the time of attack, legitimate code is halted and isolated from real I/O • destruction of HW equipment	F25	• Exceeding the rating of existing circuit breakers and damaging SG equipment • voltage sags • malfunction of protective devices
F11	• Financial loss to the utility company caused by unpaid energy usage	F26	• Complete power outage, possibly long lasting • damage to power plants, transmission lines, substation components or distribution
F12	• Potential leakage of customer information • using private data to deduce personal habits and behaviours of the home's occupants	F27	• Outage of the power grid • poor power quality
F13	• Monetary losses for individual victims • system's instability leading to price and demand fluctuations • regional blackouts	F28	• Dropped loads • disconnection of utility power at consumer ends
F14	• Wasted energy • increased transmission cost • energy outages • imbalance of energy supply • invalid energy links • isolation of nodes from the grid in terms of energy supply and demand)	F29	• The heat energy generated over long time duration could lead to serious damage to system components • serious threats to system stability and human safety

Table 4 (continued)

F/F	Impacts	F/F	Impacts
F15	• Destabilization of the electrical network leading to a complete blackout • large areas without electrical energy • lack of communications • lack of heating in the winter • significant economic losses	F30	• Unexpected downtime • economic losses

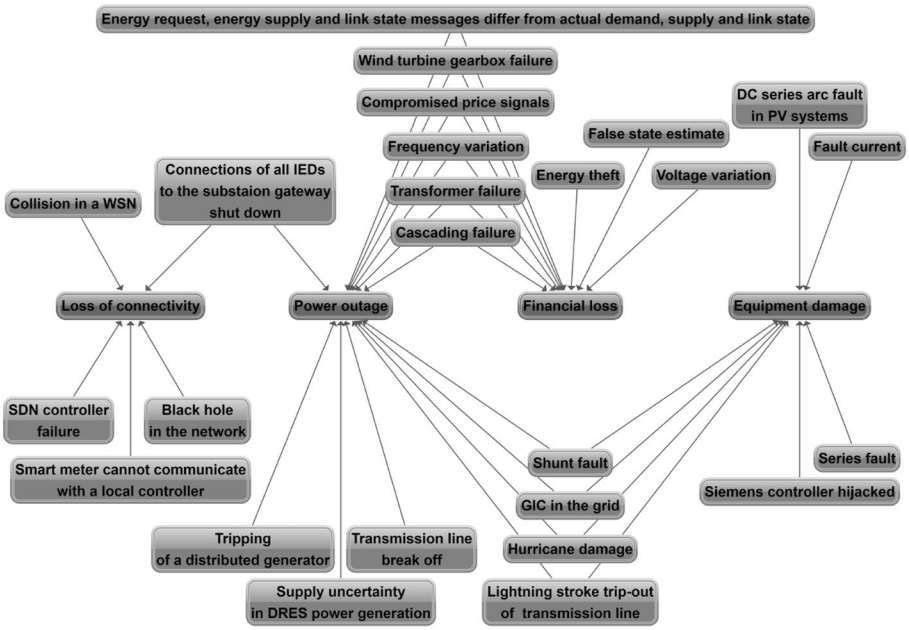

Fig. 4 RQ4. Most common consequences and their causes

Furthermore, we present the results of the efforts to assemble representative faults and failures into a chronological sequence based on their causes and impacts. The goal is to graphically depict how a fault/failure can lead to another, eventually forming a chain of subsequent faults/failures, similar to the concept of fundamental chain of dependability and security threats described by Avizienis et al. (2004).

The outcome is presented in Fig. 5, which consists of two separate groups. The major group encompasses 15 faults or failures and 20 associations among them, where arrows point to the consequent event. In particular, it is worth mentioning the cascading failure F24, since it is associated with many others as a consequence. We can also notice the cyclic relationship with voltage variation F16, meaning that a fluctuation of voltage levels can cause a cascading failure, which may lead to further voltage variation. Additionally, the minor group contains a simple relationship of lost communication to smart meter F1 with false state estimate F9.

Detection and countermeasures (RQ5)

Concerning question RQ5, we report in Tables 5 and 6 detection techniques and countermeasures if they are available in the reviewed articles. Only 9 of the reported faults/failures include both detection techniques and countermeasures, on the other side two

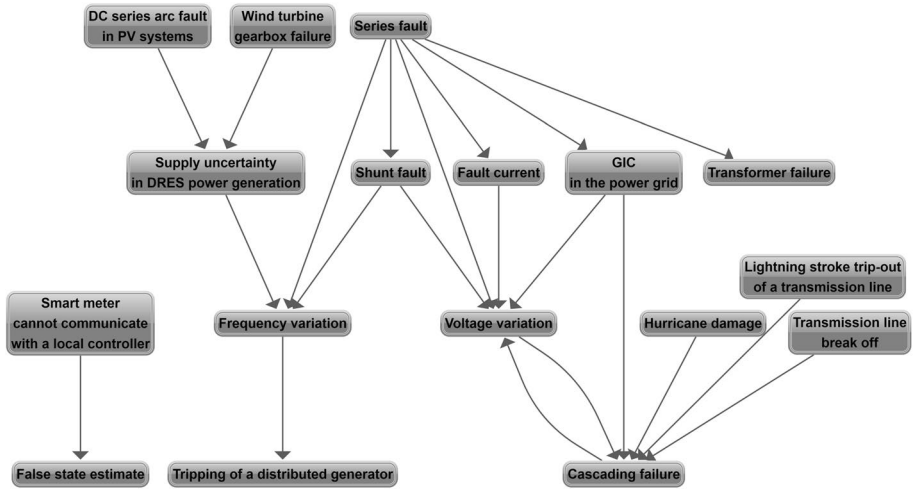

Fig. 5 RQ4. The fault chain

Table 5 RQ5 (Detection techniques for SG faults and failures)

F/F	Detection techniques	F/F	Detection techniques
F1	• Signal-based and packet-based detection	F11	• Consumption pattern-based energy theft detector
F4	• SDTM (Sybil attack Detection using Traffic Monitoring) • Radio resource testing and registration approaches • RSSI-based and TDOA-based schemes	F14	• A node persistently claiming too much quantity of demanded energy (above established threshold)
F5	• Third bit of the second octet of the two-octet internal indications (IIN) field in an application response header a sniffer watching traffic	F18	• Voltage, current, and frequency signals during disturbance
F6	• Identifying 'quiet spots' in link utilization plots	F19	• Voltage, current, and frequency signals during a disturbance • phase-overcurrent relays • ground-overcurrent relays • fault clearing or limiting devices such as fuses and circuit breakers
F7	• Delays of data packets	F23	• Lightning Location System • flashover path monitoring detection • magnetic steel stick method for lightning observation
F8	• Detection of time synchronisation attack by the signal-to-noise-ratio of the correlation peak or by applying the direction of arrival discrimination	F25	• Protective devices, that check for exceeded rating of fault current
F9	• Data integrity check • checking data with the laws of physics • collating data from data channels and energy measurements • control center advanced signal processing techniques • Adaptive Partitioning State Estimation (APSE) for detection of false data injection • secure sequence number in packet payload to detect replay attacks	F29	• The arc noise intensity increase
F10	• Checking for changes in the controllers' configuration		

Table 6 RQ5 (Countermeasures for SG faults and failures)

F/F	Countermeasures	F/F	Countermeasures
F1	• Spread-spectrum technique • schemes using priority messages and lower duty cycles • channel hopping techniques • intelligent local controller switching while integrating a retransmission mechanism	F17	• Condition monitoring such as thermal modelling, dissolved gas analysis, frequency response analysis, partial discharge analysis in order to predict and prevent failures on transformers
F2	• Strong point-to-point authentication schemes to avoid spoofing attacks	F19	• Increment in the current that can cause equipment overheating leading to a reduced life span of their insulation • fall in voltage and frequency • limited power flow
F3	• Error-correction code	F20	• Identification of vulnerable links in power grid under geomagnetic storm conditions
F4	• Authentication and probing	F21	• Reduced voltage operation can effectively lower the possibility of flashover in case of forest fire (specifically voltage drop to 50)
F5	• Scheduling policies like round-robin, weighted round-robin or weighted fair queuing • strong authentication and filtering policies for incoming communication flows	F23	• Analysis of transmission line lightning trip-out fault • installation of line arresters
F8	• Using information from multiple layers (physical layer of the time-synchronized measuring devices and the whole grid level) • applying system stability analysis on a dynamic physical infrastructure model	F24	• Mitigation plans deployed for critical components • deploying Energy Storage Systems (ESSs) • shielding against EMP attacks or solar flares • increasing the capabilities of relevant lines • monitoring • prediction of the fault chains of cascading failures (e.g. using weighted fuzzy C-means algorithm) • balancing the reactive power locally and avoiding long-distance transmission of reactive power • load shedding
F9	• Cryptography signatures and strong authentication • support vector models, machine learning, game-theoretic techniques against load redistribution attack • mechanisms to detect and mitigate man-in-the-middle attacks • advanced measurement units such as PMUs	F25	• Suppressing the fault current within minimum cycles with the use of a superconducting fault current limiter (SFCL), more specifically resistive SFCLs • fault current hierarchical limitation to neutralize the effect of microgrid fault current on system total fault current when there is a fault in utility grid • inverter-based distributed generators
F10	• New product generation and replacement • digital code signing • monitoring of the controllers	F26	• Use of mobile transformers, temporary transmission poles • use of local means of power generation, gasoline and diesel generators • resilience studies
F12	• Keeping data and most of the computation on the consumer's device • combining peer-to-peer communications and elements of centralized control • gossip protocols combined with PKI • adding noise to the meter readings and using differential privacy techniques to mask the contributions of individual meters' measurements • strong data encryption and secret key management schemes • Byzantine fault-tolerant algorithms ensuring protection from malicious meters • establishing a regulatory regimen of consumer protection	F27	• Fast-response energy storage
F15	• Smart meter based load blocking scheme	F28	• Minimization of frequency deviation with the help of energy storage devices like a supercapacitor or a battery
F16	• Hardening the smart meters • installing voltage regulators at the customer's site • installing adaptable renewable generation facilities	F30	• Predictive maintenance with early identifications of wind turbine malfunctions • monitoring approaches based on vibration signals • monitoring wind turbine gearboxes with SCADA data (oil temperature, lubricant pressure) (e.g. with deep neural networks)

Table 7 RQ4 (Causes of found faults and failures)

F/F	Causes	F/F	Causes
F1	• Jamming attack—emission of signals within a designated spectrum range creating noise in order to interrupt wireless communication	F16	• Power injection into a grid • abrupt changes in consumption • voltage variation attack—turning off the energy consumption in some buildings in a neighbourhood, in turn damaging electric appliances in other buildings still connected to the network
F2	• Spoofing attack combined with broadcasting of forged ARP packets	F17	• Dielectric breakdown • winding distortion caused by short-circuit withstand • winding and magnetic circuit hot spots • electrical disturbances • deterioration of insulation • lightning • inadequate maintenance • loose connections • overloading • failure of accessories such as OLTCs (on-load tap changers) • bushings
F3	• Sending a large number of messages to which nodes are forced to respond	F18	• Joint failures of cables and overhead lines • failure of one or more phase of circuit breaker • melting of a fuse or a conductor in one or more phases
F4	• Sybil attack—presenting numerous identities to other nodes by either forging new identities or stealing legitimate ones	F19	• Breakdown of transmission lines or equipment • ageing of insulation • deterioration of insulation in generator, transformer and other electrical equipment • improper installations • overloading of equipment • mechanical damage by public • wind, falling trees or other incidents
F5	• Flooding a data aggregator with many (unsolicited response) data events from a spoofed or compromised relay in order to make buffering of legitimate critical alerts impossible	F20	• Driven by the geoelectric field induced by geomagnetic storms
F6	• Selective forwarding attack where an attacker incorporates themselves in the data flow path of interest and then controls whether the packets will be forwarded or dropped	F21	• During forest fire high-temperature gas, charged particles and ash particles cause significant decrease of the insulation strength of the wire to ground gap, that may lead to flashover of transmission line
F7	• Failure of hardware or software • excessive flow table requests that overload or crash the controller • injected malware into SDN controllers • failure of a connecting link or failure of the OpenFlow protocol • faulty application • programming errors of the controller • error in control messages • infinite loops • resource exhaustion	F22	• Icing disaster covering lines with ice • ice load together with wind load increase the stress of wires • ageing factor
F8	• Time synchronization attack—spoofing GPS signals that are used as a time source by misleading GPS receivers to acquire fake GPS signals	F23	• Back flash-over when the lightning strikes on a shield wire or tower and the resultant voltage is large enough to cause a flash-over from the tower to the line conductors • shielding failure when lightning strikes directly on the phase conductor
F9	• Random noises (nature e.g. weather conditions, faulty nodes) • false data injection attack • load redistribution attack • replay attack • man-in-the-middle attack	F24	• Transmission lines failures like excessive flow through transmission lines, leading to overheating and outage of the lines • natural disasters (earthquakes, hurricanes, floods, solar flares) • physical attacks (e.g. Electromagnetic Pulse (EMP) attack) • false control command, false feedback or false meter data injection • physical components in the power grid taken down • maintenance works at substations • relay failure • voltage collapse • dynamic instability • operator error
F10	• Distribution of the malware worm via USB sticks and local networks; if a targeted controller is found through a complex process of fingerprinting, the rogue code is loaded on the controller	F25	• Integration of DER power generations increases short circuit capacity and consequently increases fault current

Table 7 (continued)

F/F	Causes	F/F	Causes
F11	• Physical tampering (e.g. strong magnet causing interference, reversing or disconnecting the meters) • bypassing the meters by directly wiring high-consuming appliances to an external feeder • cyber-attacks (e.g. gaining privileged access to the meter firmware, tampering with the meter storage, interrupting measurements, intercepting the communication link)	F26	• Hurricanes including phenomena such as storm surge and flooding in coastal areas, torrential rains, very strong winds and fallen trees
F12	• Extracting the private data like time of use of individual electrical appliances from smart meters • compromising the user authentication data or shared secret values (examples of confidentiality attack with intention of privacy leakage are wiretappers and traffic analyzers)	F27	• Weather changes • forecast error • disconnection of a DRES such as a wind turbine and solar panel from the grid due to equipment failure
F13	• Scaling and delay attacks, where the adversary modifies price values or timestamps in data packets during transmissions in vulnerable communication networks •modification of the smart meters' internal clocks in case of the delay attack	F28	• Frequency deviation of distributed generators
F14	• Energy deceiving attack - injecting forged energy or link-state information into the energy request and response message among nodes	F29	• A decrease of the contact area of the cross-section due to bad joints causes higher resistance and heat loss leading to the deterioration of the connecting point, resulting to a loose connection. • Ageing effects also increase the risk of fault.
F15	• Variable loads and unpredictable power generation • an attack on frequency variation, where an attacker takes control of a substantial number of smart meters in a large geographical area	F30	• Heavy loads • transient impulses of brakes • dust corrosion

are not covered by both detection and countermeasures. Half of all the findings mentioned some detection technique or approach. The situation concerning countermeasures was considerably better, 22 faults/failures in the papers are reporting some sort of countermeasures like prevention, mitigation or recovery.

Detection techniques cover a broad spectrum of approaches for the identification of faults and failures (Table 5). These techniques deal mostly with the identification of anomalies that can be linked to the presence of faults or the triggering of failures. For example, delays in data packets can be an indication of SDN controller failures (F7), consumption patterns analysis and anomaly detection of energy demand can be used for energy theft (F11), energy link-state information (F14). Other signal-based, and traffic monitoring detection can be used for smart meter communications with local controllers failures (F1), the presence of forged identities in a WSN (F4).

Countermeasures represent actions and techniques put in place to counteract the possible effects of faults and the impacts of failures (Table 6). For example, error correction codes can be used for communication collision in a WSN (F3), smart meter load blocking schemes can be used to counteract frequency variations of the grid (F15), adding noise and using differential privacy techniques to mask the individual contributions of smart meters to data aggregates sent to the utility can be used for potential privacy leakage (F12). Other more hardware-related countermeasures can be the utilization of energy storage devices for the minimization of frequency deviations for wind turbine

gearbox failures (F30) or the deployment of Energy Storage Systems (ESS) for cascade failures of interconnected networked components (F24). Many countermeasures are also related to the application of machine learning techniques that are commonly applied in the context of SGs (Rossi and Chren 2019), for example, using the weighted fuzzy-C means algorithms for the identification of faults chains and cascading failures (F24) (Table 7).

Conclusions

The goal of this paper was to review and classify existing faults and failures in SGs to provide a summary view of all the causes, consequences, and countermeasures that can be applied. Following the SLR approach, we collected and classified information from 50 articles arriving at the definition of a catalogue of 30 faults/failures. These were categorized and then linked to the areas and domains of the SGAM model (Bruinenberg et al. 2012) and to the general dependability taxonomy (Avizienis et al. 2004). Overall, the categorization provides an actionable catalogue that can be used by practitioners and researchers to pinpoint specific predictive activities and countermeasures with an indication of the sources where to gather additional knowledge about the proposed techniques.

The definition of clear categories of faults and failures and their characteristics can allow to better cope with such disruptive events and to enable self-healing capabilities of SG components, by having in place preventive measures for the detection and activities for the restoration of the impacted services. There are still many researchers that attempt at making SG systems more robust, secure, and resilient but they clash with the heterogeneity of the different devices and components involved in the different layers—as we have shown by mapping faults and failures to the SGAM levels. An overall and integrated view is necessary, however, most of the preventive measures are fine-grained techniques that need to be applied in a coordinated modality. The level of coverage is thus given by the combination of all these disparate techniques: simulation, optimization, analysis techniques all need to be combined with engineering methods to build self-healing components in the SG. If we want to reach such a level of coordination, categorizations as the one presented in this paper are of fundamental importance.

Abbreviations

AMI	Advanced metering infrastructure
DC	Direct current
DER	Distributed energy resource
DoS	Denial of service
GIC	Geomagnetically induced currents
GPS	Global positioning system
IED	Intelligent electronic devices
NIST	US National Institute of Standards and Technologies
PICO	Patient, intervention, comparison and outcome
PLC	Programmable logic controller
PMU	Phasor measurement unit
PV	Photovoltaic
SCADA	Supervisory control and data acquisition
SDN	Software defined network
SG	Smart grid
SGAM	Smart grid reference architecture mode
SLR	Systematic literature review
WAMS	Wide-area monitoring system
WSN	Wireless sensor network

Acknowledgements
Not applicable.

Author contributions
ZK performed the paper collection and conducted the systematic literature review. SCH designed the overall goals of the study and provided the necessary smart grid and reliability engineering background. BR refined the SLR process and investigated the related work. All authors read and approved the final manuscript.

Funding
The work was supported by ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

Availability of data and materials
The datasets generated and/or analysed during the current study are available in the Figshare repository: https://doi.org/10.6084/m9.figshare.19086593.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: 7 June 2022 Accepted: 2 October 2022
Published online: 20 October 2022

References

Alohali BA, Vassilakis VG (2017) Security of wireless sensor network (WSN) in smart grid. In: Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing. ICC '17, pp. 1–6. Association for Computing Machinery, USA. https://doi.org/10.1145/3018896.3056789. Accessed 2021-02-17

Arif S, Aziz T (2017) Impact of battery energy storage system on post-fault frequency fluctuation in renewable integrated microgrid. In: 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), pp. 594–598 . https://doi.org/10.1109/ECACE.2017.7912974

Krivohlava Z, Chren S, Rossi B (2022) Smart grids failure and faults classification dataset. https://doi.org/10.6084/m9.figshare.19086593. Accessed 28 Jan 2022

Avizienis A, Laprie J-C, Randell B, Landwehr C (2004) Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secure Comput 1(1):11–33

Bakar AHA, Talib DNA, Mokhlis H, Illias HA (2013) Lightning back flashover double circuit tripping pattern of 132kv lines in Malaysia. Int J Elect Power Energy 45(1):235–241. https://doi.org/10.1016/j.ijepes.2012.08.048

Bernstein A, Bienstock D, Hay D, Uzunoglu M, Zussman G (2012) Geographically correlated failures in power networks—survivability analysis. Submitted

Bernstein A, Bienstock D, Hay D, Uzunoglu M, Zussman G (2012) Sensitivity analysis of the power grid vulnerability to large-scale cascading failures. ACM SIGMETRICS Perform Eval Rev 40(3):33–37. https://doi.org/10.1145/2425248.2425256

Bhatt J, Shah V, Jani O (2014) An instrumentation engineer's review on smart grid: critical applications and parameters. Renew Sust Energ Rev 40:1217–1239. https://doi.org/10.1016/j.rser.2014.07.187

Birman K, Jelasity M, Kleinberg R, Tremel E (2015) Building a secure and privacy-preserving smart grid. ACM SIGOPS Oper Syst Rev 49(1):131–136

Bruinenberg J, Colton L, Darmois E, Dorn J, Doyle J, Elloumi O, Englert H, Forbes R, Heiles J, Hermans P, Uslar M (2012) CEN-CENELEC—ETSI: Smart Grid Coordination Group—Smart Grid Reference Architecture Report 2.0

Chen X, Yu W, Griffith D, Golmie N, Xu G (2014) On cascading failures and countermeasures based on energy storage in the smart grid. In: Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems. RACS '14, pp. 291–296. Association for Computing Machinery, USA. https://doi.org/10.1145/2663761.2663770. https://doi.org/10.1145/2663761.2663770 Accessed 2021-02-16

Chren S, Rossi B, Pitner T (2016) Smart grids deployments within eu projects: The role of smart meters. In: 2016 Smart Cities Symposium Prague (SCSP), pp. 1–5 . IEEE

Costache M, Tudor V, Almgren M, Papatriantafilou M, Saunders C (2011) Remote control of smart meters: Friend or foe? In: 2011 Seventh European Conference on Computer Network Defense, pp. 49–56 . https://doi.org/10.1109/EC2ND.2011.14

Cui S, Han Z, Kar S, Kim TT, Poor HV, Tajer A (2012) Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions. IEEE Signal Process Mag 29(5):106–115. https://doi.org/10.1109/MSP.2012.2185911

ElectronicsHub (2015) Types of faults in electrical power systems . https://www.electronicshub.org/types-of-faults-in-electrical-power-systems/ Accessed 2021-04-21

Eppstein MJ, Hines PDH (2012) A random chemistry algorithm for identifying collections of multiple contingencies that initiate cascading failure. IEEE Trans Power Syst 27(3):1698–1705. https://doi.org/10.1109/TPWRS.2012.2183624
Fang X, Misra S, Xue G, Yang D (2011) Smart grid-the new and improved power grid: a survey. IEEE Commun Surveys Tutorials 14(4):944–980
Federal Office for Information Security (BSI) (2013) Protection profile for the security module of a smart meter gateway (security module PP), 87
Frandsen TF, Nielsen MFB, Lindhardt CL, Eriksen MB (2020) Using the full pico model as a search tool for systematic reviews resulted in lower recall for some pico elements. J Clin Epidemiol 127:69–75
Gao J, Xiao Y, Liu J, Liang W, Chen CP (2012) A survey of communication/networking in smart grids. Futur Gener Comput Syst 28(2):391–404
Gong S, Zhang Z, Li H, Dimitrovski AD (2012) Time stamp attack in smart grid: physical mechanism and damage analysis . arXiv:1201.2578. Accessed 2021-03-19
Ghosh U, Dong X, Tan R, Kalbarczyk Z, Yau DKY, Iyer RK (2016) A simulation study on smart grid resilience under software-defined networking controller failures. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security. CPSS '16, pp. 52–58. Association for Computing Machinery, USA . https://doi.org/10.1145/2899015.2899020. https://doi.org/10.1145/2899015.2899020 Accessed 2021-02-15
Gururajapathy SS, Mokhlis H, Illias HA (2017) Fault location and detection techniques in power distribution systems with distributed generation: a review. Renew Sustain Energy Rev 74:949–958. https://doi.org/10.1016/j.rser.2017.03.021
Hlalele T, Sun Y, Wang Z (2019) Faults classification and identification on smart grid: part-a status review. Proc Manuf 35:601–606
Jangale M, Thakur KD (2017) Optimum positioning of superconducting fault current limiter for wind farm fault current in smart grid. In: 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA), vol. 2, pp. 312–316 . https://doi.org/10.1109/ICECA.2017.8212823
Jin D, Nicol DM, Yan G (2011) An event buffer flooding attack in DNP3 controlled SCADA systems. In: Proceedings of the 2011 Winter Simulation Conference (WSC), pp. 2614–2626 . https://doi.org/10.1109/WSC.2011.6147969. ISSN: 1558-4305
Jin P, Li Y, Guo K, Zheng Y (2017) Fault probability prediction of transmission lines under icing disaster. In: 2017 29th Chinese Control And Decision Conference (CCDC), pp. 6942–6947. https://doi.org/10.1109/CCDC.2017.7978433. ISSN: 1948-9447
Jokar P, Arianpoo N, Leung VCM (2016) Electricity theft detection in AMI using customers' consumption patterns. IEEE Trans Smart Grid 7(1):216–226. https://doi.org/10.1109/TSG.2015.2425222
Kabir S, Amin AA, Anayatullah M, Saha BK, Aziz T (2014) Impact of supercapacitor placement in renewable integrated microgrid to minimize post-fault frequency fluctuation. In: 2014 International Conference on Electrical Engineering and Information Communication Technology, pp. 1–5. https://doi.org/10.1109/ICEEICT.2014.6919063
Kang X, Zhang Y, Zhang X, Xu Y, Li X, Zhou H (2019) Identification of vulnerable links in power grid based on brittleness theory of complex system under geomagnetic storm conditions. In: 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), pp. 31–35 . https://doi.org/10.1109/APAP47170.2019.9225149
Kaplantzis S, Şekercioğlu YA (2012) Security and smart metering. In: European Wireless 2012; 18th European Wireless Conference 2012, pp. 1–8
Keele S et al (2007) Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, Ver. 2.3 EBSE Technical Report. EBSE
Kwasinski A, Andrade F, Castro-Sitiriche MJ, O'Neill-Carrillo E (2019) Hurricane Maria effects on Puerto Rico electric power infrastructure. IEEE Power Energy Technol Syst J 6(1):85–94. https://doi.org/10.1109/JPETS.2019.2900293
Langner R (2011) Stuxnet: dissecting a cyberwarfare weapon. IEEE Security Privacy 9(3):49–51. https://doi.org/10.1109/MSP.2011.67
Li X, Chen J, Gu S (2016) Study of lightning stroke trip-out fault analysis for transmission line. In: 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 2296–2300 . https://doi.org/10.1109/APPEEC.2016.7779901
Lin J, Yu W, Yang X, Xu G, Zhao W (2012) On false data injection attacks against distributed energy routing in smart grid. In: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, pp. 183–192 . https://doi.org/10.1109/ICCPS.2012.26
Liu T, Gu Y, Wang D, Gui Y, Guan X (2013a) A novel method to detect bad data injection attack in smart grid. In: 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 49–54. https://doi.org/10.1109/INFCOMW.2013.6562907
Liu Y, Liu J, Liu T, Guan X, Sun Y (2013b) Security risks evaluation toolbox for smart grid devices. In: Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM. SIGCOMM '13, pp. 479–480. Association for Computing Machinery, USA. https://doi.org/10.1145/2486001.2491693. https://doi.org/10.1145/2486001.2491693 Accessed 2021-02-18
Liu H, Chen Y, Chuah MC, Yang J, Poor HV (2017) Enabling self-healing smart grid through jamming resilient local controller switching. IEEE Trans Dependable Secure Comput 14(4):377–391. https://doi.org/10.1109/TDSC.2015.2479624
Liu X, Li C, Shahidehpour M, Gao Y, Zhou B, Zhang Y, Yi J, Cao Y (2019) Fault current hierarchical limitation strategy for fault ride-through scheme of microgrid. IEEE Trans Smart Grid 10(6):6566–6579. https://doi.org/10.1109/TSG.2019.2907545
Lu S, Phung BT, Zhang D (2017) Study on DC series arc fault in photovoltaic systems for condition monitoring purpose. In: 2017 Australasian Universities Power Engineering Conference (AUPEC), pp. 1–6 . https://doi.org/10.1109/AUPEC.2017.8282464. ISSN: 2474-1507
Mathas C-M, Grammatikakis K-P, Vassilakis C, Kolokotronis N, Bilali V-G, Kavallieros D (2020) Threat landscape for smart grid systems. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20, pp. 1–7. Association for Computing Machinery, USA. https://doi.org/10.1145/3407023.3409229. Accessed 2021-02-18
McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. IEEE Security Privacy 7(3):75–77

Menasché DS, Avritzer A, Suresh S, Leão RM, de Souza e Silva E, Diniz M, Trivedi K, Happe L, Koziolek A, (2014) Assessing survivability of smart grid distribution network designs accounting for multiple failures. Concurr Comput Pract Exp 26(12):1949–1974. https://doi.org/10.1002/cpe.3241

Min B, Varadharajan V (2016) Cascading attacks against smart grid using control command disaggregation and services. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing. SAC '16, pp. 2142–2147. Association for Computing Machinery, USA . https://doi.org/10.1145/2851613.2853128. https://doi.org/10.1145/2851613.2853128 Accessed 2021-02-17

Mousa M, Abdelwahed S, Kluss J (2019) Review of diverse types of fault, their impacts, and their solutions in smart grid. In: 2019 SoutheastCon, pp. 1–7 . IEEE

Najafabadi SG, Naji HR, Mahani A (2013) Sybil attack detection: improving security of WSNs for smart power grid application. In: 2013 Smart Grid Conference (SGC), pp. 273–278. https://doi.org/10.1109/SGC.2013.6733831

Otuoze AO, Mustafa MW, Larik RM (2018) Smart grids security challenges: classification by sources of threats. J Elect Syst Inf Technol 5(3):468–483

Rajaei N, Salama MMA (2015) Management of fault current contribution of synchronous DGs using inverter-based DGs. IEEE Trans Smart Grid 6(6):3073–3081. https://doi.org/10.1109/TSG.2015.2432759

Rajaei N, Ahmed MH, Salama MMA, Varma RK (2014) Fault current management using inverter-based distributed generators in smart grids. IEEE Trans Smart Grid 5(5):2183–2193. https://doi.org/10.1109/TSG.2014.2327167

Reddy JS, Chatterjee S (2017) Superconducting fault current limiter for smart grid application. In: 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–5 . https://doi.org/10.1109/ICECCT.2017.8118025

Rivas AEL, Abrao T (2020) Faults in smart grid systems: monitoring, detection and classification. Electric Power Syst Res 189:106602

Rossi B, Chren S (2019) Smart grids data analysis: a systematic mapping study. IEEE Trans Industr Inf 16(6):3619–3639

Samarakoon K, Ekanayake J (2009) Demand side primary frequency response support through smart meter control. In: 2009 44th International Universities Power Engineering Conference (UPEC), pp. 1–5

Sarathkumar D, Srinivasan M, Stonier AA, Samikannu R, Dasari NR, Raj RA (2021) A technical review on classification of various faults in smart grid systems. In: IOP Conference Series: Materials Science and Engineering, vol. 1055, p. 012152. https://doi.org/10.1088/1757-899X/1055/1/012152. IOP Publishing

Stamatis DH (2003) Failure mode and effect analysis: FMEA from theory to execution. Quality Press, USA

Tan R, Badrinath Krishna V, Yau DKY, Kalbarczyk Z (2013) Impact of integrity attacks on real-time pricing in smart grids. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. CCS '13, pp. 439–450. Association for Computing Machinery, USA. https://doi.org/10.1145/2508859.2516705. https://doi.org/10.1145/2508859.2516705 Accessed 2021-03-04

Trellix: What Is Stuxnet? | McAfee (2021). https://www.mcafee.com/enterprise/en-sg/security-awareness/ransomware/what-is-stuxnet.html Accessed 2021-03-16

Wang W, Lu Z (2013) Cyber security in the smart grid: survey and challenges. Comput Netw 57(5):1344–1371

Wang L, Zhang Z, Long H, Xu J, Liu R (2017) Wind turbine gearbox failure identification with deep neural networks. IEEE Trans Industr Inform 13(3):1360–1368. https://doi.org/10.1109/TII.2016.2607179

Wang M, Lu W, Wu S, Zhao C, Feng Y, Luo C, Xiao Y (2017) Vulnerability assessment model of power grid cascading failures based on fault chain and dynamic fault tree. In: 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 1279–1284 . https://doi.org/10.1109/CYBER.2017.8446361

Wei M, Lu Z, Tang Y, Lu X (2019) Cyber and physical interactions to combat failure propagation in smart grid: characterization, analysis and evaluation. Comput Netw 158:184–192. https://doi.org/10.1016/j.comnet.2019.05.006

Wohlin C (2014) Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, pp. 1–10

Yang K, Walid A (2014) Outage-capacity tradeoff for smart grid with renewables. ACM SIGMETRICS Perform Eval Rev 41(3):80–82. https://doi.org/10.1145/2567529.2567554

Yu X, Cecati C, Dillon T, Simoes MG (2011) The new frontier of smart grids. IEEE Ind Electron Mag 5(3):49–63

Yue Y-s, Zou Y-h, Huang F-y, Gong Z-x, Wang C (2017) Study on the flashover characteristics of 500kv DC transmission lines caused by forest fire under reduced-voltage operation. In: 2017 EPTC Power Transmission and Transformation Technology Conference, pp. 1–5. https://doi.org/10.1049/cp.2017.0567

Publisher's Note