Why Dealing with Electrical Faults for Smart Microgrid is not Enough?

Pragya Kirti Gupta[1], Sai Shibu Narayanan Babu[2], Anjana Mohandas Sheeladevi[2], and Venkatesh Pampana[1(✉)]

[1] fortiss GmbH, Munich, Germany
{gupta,pampana}@fortiss.org
[2] Center for Wireless Networks and Applications, Amrita Vishwa Vidyapeetham, Amritapuri, India
{saishibunb,anjanams}@am.amrita.edu

Abstract. With increasing use of Information and Communication Technologies (ICT) in smart grids, the need to study the faults induced by software and communication systems is important towards realizing stable operation of microgrids. Since the effect of faults in the electrical, communication and software systems is different, the impact of these faults in each other system, the knowledge of their effects and causes is necessary to design appropriate recovery actions. In this paper, we study the faults and their impact on the microgrids. We emphasize on the necessity of software and communication fault handling in order to create resilient microgrids. This paper highlights the effects of software and communication faults on electrical system and vice-versa. A detailed study of the commonly occurring faults in a microgrid and their cascading effects is presented. Towards this a cause-and-effect analysis of the commonly occurring faults on the performance of the microgrid is carried out. Finally, we identify potential research areas where the fault handling approaches can be included and improved to make the microgrid more resilient.

Keywords: Faults · Failures · Microgrid challenges · Cause-effect analysis · Fishbone analysis · Cascading faults · Resilience · Self-healing

1 Introduction

The 2019 massive power outage in Latin American countries affecting Argentina, Uruguay, Paraguay, Chile and Brazil is the perfect example of a fault occurring in one part of the distribution system and cascading to the extent of a partial power outage in these five countries [1]. As the cause of the outage is still being investigated, it illustrates the failure of the automatic protection system of the grid. In this instance, a well-planned automatic protection system that could either isolate the fault or switch to backup power resources was already operational. However, the protection system failed to control the power fluctuation leading to further power outage and damage to the devices. This example illustrates that the failure (observed as the power outage) could have been caused

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 55–74, 2022.
https://doi.org/10.1007/978-3-031-06371-8_5

by multiple faults (physical damage to the grid lines or cyber-attack). Once the failure of power supply occurred, it further induced faults (short-circuits) that led to the breakdown of the electrical system for 24 h affecting millions of people. Even though the use of automatic switches to isolate the faults are installed, their synchronized operation needs coordination.

Towards the automation of complex decisions and to operate complex microgrid systems, fault handling is a crucial aspect that engineers, designers and researchers need to deal with. In fact, a significant feature of microgrids is its ability to automatically handle faults, which is often referred to as self-healing. In general, self-healing systems include two aspects: self and healing. The term 'self' refers to the system's ability to observe its own behavior. In the context of faults and failures, this information also includes the knowledge of abnormal behavior that is specifically identified as faults. The healing actions are the recovery measures designed to counter the effects of the faults. Towards the objective of defining and designing healing actions, knowledge about the faults and failures is necessary. However, there are several questions surrounding faults and fault handling in a microgrid that need to be investigated. The bigger research question that should be investigated is *why dealing with electrical faults for smart microgrids is not enough?* To answer this, we focus on the following questions in this paper: - RQ1: *What are the effects of electrical faults on the ICT system and viceversa?* Faults from the electrical systems may cause either power disruptions or power disturbances. However, the effect of software and communication faults and their impact on the electrical distribution system are still unclear. - RQ2: *What are the commonly occurring faults in a microgrid and their impact?* Not all faults can be observed and handled by the microgrid controller. Therefore, an estimation of the fault space and the scope of faults for designing recovery actions are necessary. This estimation helps in identifying the appropriate recovery mechanisms for self-healing microgrids.

This paper is organized into six sections. In the Sect. 2, the concept of microgrid is discussed along with the basic concept and layout of an islanded microgrid. In the Sect. 3, some of the scenarios are presented to highlight the effect of faults on each other leading to cascading effects. Section 4 describes various faults and fault handling techniques, highlighting the gap in the on-going research for resilient microgrid. Section 5 deals with the commonly occurring faults in a microgrid and their impact. Finally, in the Sect. 6, we highlight some of the emerging solutions and future trends in fault handling.

2 Concept of Microgrid

In 2017, IEEE encompassed the vision for microgrids and provided a specific definition of microgrid in the IEEE Standard for Microgrid Controllers [2]. *A microgrid is a group of interconnected loads and distributed energy resources with clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid and can connect and disconnect from the grid to enable it to operate in both grid-connected or island mode.* A typical microgrid is composed of

three systems: electrical, software and communication. This standard essentially provides three distinct characteristics for microgrids, namely *a) clearly defined electrical boundaries, b) a control system to manage and dispatch resources as a single controllable entity and c) installed generation capacity that exceeds the critical load; this allows the microgrid to be disconnected from the main grid, i.e., to operate as an entity in islanded mode, and supply local loads.* The conceptual model of the microgrid considered in this work is shown in Fig. 1. Conceptually a microgrid is comprised of three individual domains: electrical, software and communication. A typical microgrid has: 1) consumers, which are the energy consumption units, 2) generators, which are the renewable energy sources, 3) storage units such as batteries, 4) controller, which is the energy management system and 5) grid connectors, which provide the ability to connect or disconnect from the grid. The power distribution and communication distribution in the microgrid are also shown in Fig. 1. Power supply from the grid is distributed to the consumers (including controller) and storage units. Power supply from the generators is supplied to consumers, storage unit or fed into the grid. Communication distribution is further shown in terms of the data generated by each component.

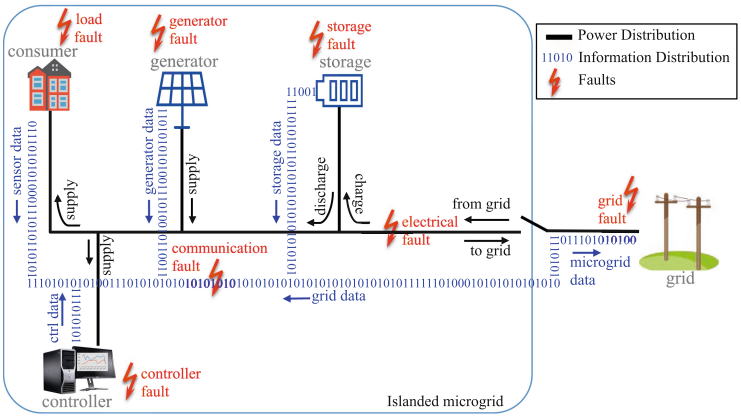

Fig. 1. Microgrid with components, faults, power and information flow.

Smartness in the microgrid is not limited to load balancing or meeting the demand. It also includes the ability to detect and recover from the faults and failures, which may arise due to factors such as environmental changes, weather or climatic conditions and hardware malfunctions. This aspect of faults originating in different parts in the microgrid is also shown in Fig. 1. Faults that affect the device operations at consumer level are shown as load faults. These faults can also be induced by generators or storage units. Faults in the generators are labeled as generator faults. Similarly, the storage units faults are mentioned as storage faults. A microgrid can be affected by grid faults and faults in the power

distribution infrastructure like wires and relays. These are labeled as electrical faults. In a microgrid, faults are not limited to devices or electrical infrastructure. Software faults in the controller also affect microgrid performance, which are referred here as controller faults. Therefore, microgrids should be resilient towards the disturbances in power supply, communication channel and software faults using various fault handling approaches.

3 Effect of Faults

In this section, we investigate the RQ1 on the effects of faults originating in one system and their effect on the other parts of the microgrid. In the existing microgrids, fault handling techniques are designed considering the other systems as a black-box [3]. There are many fault handling techniques in the individual systems. This narrow approach of dealing with faults in individual systems is not sufficient to introduce self-healing in the microgrid. A complete microgridcentric approach to fault handling should encompass not only individual faults, but also their effect on the other compositional systems. For the above mentioned reasons, a self-healing microgrid should be able to detect and recover from the following classes of faults:

1. Errors and failures occurring in any of electrical, software or communication systems. Here, the electrical system includes power system components, smart devices (Photovoltaic, batteries, sensors, actuators etc.). Software includes the microgrid controller and communication includes all types of communication channels relevant to the microgrid.
2. Faults that have a cascading effect on other systems. For example, a software fault leading to incorrect commands can induce short-circuit faults [4].
3. Faults that have similar symptoms, but have different effects. For example, according to Table A.20 in IEEE Guide to Classification for Software Anomalies [5], a wrong input accepted by the software could lead to wrong decision-making, whereas the wrong input accepted as command/signal by the hardware can lead to incorrect actuation of the hardware. The same input problem leads to logical fault in software and wrong controlling in the hardware.

Table 1 shows fault sources and their effects in the originating system and in other compositional systems. Here ◯ denotes the effect of the fault affecting only the individual system, while × denote faults in one individual system cascading into other systems. There are faults that occur within the individual system, but do not affect other systems. Although such faults are observable by other systems, they affect only the system in which they occur. For example, voltage fluctuations occurring while transitioning from island mode to grid-connected mode is observable by the controller, but does not impact the functioning of the controller. These faults are generally accounted for while designing the microgrid and are shown as *circles* in Table 1. On the other hand, there are faults which occur in one system, but can induce faults in other systems. For example, high voltage spike due to environmental factors can affect the functioning of the

Table 1. Fault affecting an individual system and their cascading effects

	Software	Electrical	Communication
Software	O	X	X
Electrical	X	O	X
Communication	X	X	O

sensors connected with the power network. The wrong values from the sensors can induce software faults (out of range or garbage values). Such faults are shown with a *cross* symbol in Table 1. The cascading effect is discussed only for faults that are observable and not hidden. The occurrence of fault in one system adversely affects another system in the following ways:

1. *Software faults inducing fault in electrical system:* A fault in the microgrid controller leads to failure/fault in the electrical system. For example, logical faults in the software lead to wrong commands, which result in short circuit faults in the electrical network. The outcome of the short circuit fault could be power outage or further damaging the devices connected with the network.
2. *Software faults inducing fault in communication system:* Software faults can also flood the network traffic to an extent that the communication system either crashes or stops responding. For example, errors messages from the software application can clog the communication network resulting in the denial-of-service.
3. *Electrical faults inducing software failure:* Any fault in the electrical system can lead to disruption of software application. For example, an unbalanced network or frequent power spikes in the electrical network can cause long disruptions in power supply. This power outage can affect the hardware platform on which software is running resulting in crash of the software.
4. *Electrical faults inducing communication failure:* Similar to the previous case, electrical faults may not directly affect the communication, but they can break down the hardware (router, switch) resulting in network crash. It should be noted that in case of Power Line Communication (PLC), harmonic distortions directly affect the communication network as well.
5. *Communication faults inducing software failure:* In complex systems like microgrids, the software system depends heavily on the communication system. Interactions with other software and hardware entities depend on a robust communication channel. A heavy data rate and loss of data in an unstable communication network result in wrong inputs to the software. This results in either software crash or wrong computation in decision-making.
6. *Communication faults inducing electrical failure:* A highly robust communication system aids in the reliable data sharing that in turn helps in smart operations. The faults induced due to the lack of communication can lead to cascading effect. The dependency of loss of communication and power loss are also topics of research [6]. For example, the power outage in September 2011 in US (Arizona, Southern California, and Baja California, Mexico) started

with the tripping of a single power line and led to cascading blackout in the neighboring regions. Since the grid operators of the affected regions were unaware of the power outage, any coordination or controlling of the outage at the initial stage could not be carried out [7].

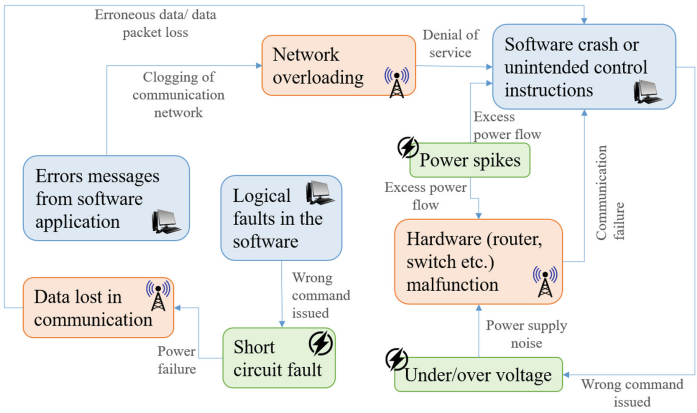

Fig. 2. Fault effecting an individual system and cascading into other systems.

In Fig. 2 specific fault cases are shown, where faults originating in an individual system lead to cascading effect in other systems. One of the fault case shown in Fig. 2 is the software crash. Software crashes at the controller leads to unintended control instructions issued to the switches. Wrong control of the switches may lead to under- or over-voltage situations that leads to hardware damage. Hardware damage can further lead to power spikes in the overall distribution grid. Another fault case shown is the logical fault in the controller where the incorrect analysis is carried out. Due to the logical mistake, more than one switch is open or closed simultaneously leading to short circuit faults. This can also lead to loss in the communication network, ultimately resulting in the loss of data at the controller. Existing fault handling approaches in the microgrids do not focus on the cascading effects of faults, especially the faults from the microgrid controller affecting the protection system. These specific fault cases are foreseeable and counter actions can be included at the design and planning stage. These specific fault cases conclude that the system experts from multiple domains should be involved in design phase, standards from different domain must be referred to develop system specifications and testing strategies for system conformance should also be established.

4 Faults and Fault Handling: A Survey

In Fig. 3 a generic understanding of faults, errors and failures is presented. Faults are the adjudged or hypothesized cause of an error [8]. In other words, fault

causes error, which is observed when the system exhibits failure. Error is that part of the system state that may cause a subsequent failure [8]. Failures are the indicators of fault, without knowing the cause. A failure occurs when an error reaches the service interface and alters the service. A failure is a transition from correct service to incorrect service, where correctness of a service is described as the service performing the intended system functions [8].

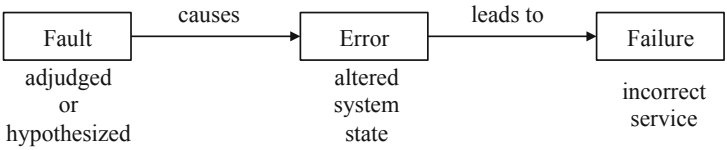

Fig. 3. Generic understanding of fault, error and failure.

4.1 Faults in a Microgrid

We now discuss faults in the compositional system of microgrid, namely faults in electrical, communication and software control system.

Faults in Electrical Systems in Microgrids. Faults in the electrical system can be caused due to several factors such as varying environment, operation or aging of infrastructure. In the electrical system, the classical fault categories are shown in Fig. 4. An electrical fault occurring in a circuit or device causes deviation in the voltage and current values from their nominal ranges. This deviation may result in over-current, under-voltage, unbalance of the phases, reversed power or high voltage surges. As a result, the normal operation of the network is interrupted, equipment failure or fire in the electrical connection occurs. Electrical system faults shown in Fig. 4 are mainly classified into two types, namely open and short circuit faults. Short-circuit faults can be further categorized as symmetrical or unsymmetrical faults. A considerable part of fault detection and identification is towards handling short-circuit or open-circuit faults. Fault location detection in electrical systems is a well-established research area, which focuses on the localization and identification. To handle the electrical system faults within a microgrid, major focus is on the power supply stabilization and grid protection. Since the inception of the microgrid concept, one particular fault scenario that remains the focus of researchers is the intentional switching to island mode operations to protect the grid from any damage caused by the electrical faults. Most research work follows the vision of Lasseter [9] to protect the grid by considering the basic structure of the microgrid as having local microsource controllers, system optimizer and distributed protection. He defined the protection process as *when the fault is on the utility grid, the desired response may be to isolate the microgrid from the main utility as quickly as possible to protect the microgrid loads. In case the fault is within the microgrid, the protection coordinator must isolate the smallest possible section of the radial feeder to*

eliminate the fault. He did not mention the kind of faults that must be handled, but only used electrical system faults that the microgrid controller must handle. High Voltage DC (HVDC) grid is becoming popular especially in transportation sector and microgrids. Yi Wang and his team investigated pole to ground faults in HVDC transmission lines [10]. They simulated HVDC system to study the system behaviour in case of fault. Their results show that during a pole to ground fault, the system can be under damped condition when the impedance between the ground and the line is small. If the impedance is large, the system is in a over damped condition. Investigation on the existing approaches for faults in microgrids shows that faults are mainly restricted to the following categories; balanced, unbalanced, line-to-line, single-line to ground, double-line to ground and three-phase faults [11–15]. Most of the fault detection techniques are focused on detecting the maximum and minimum deviation values of current and voltage.

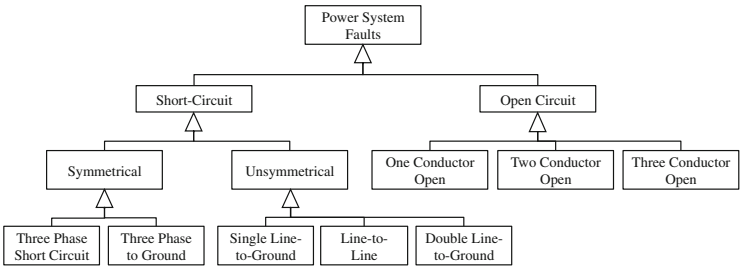

Fig. 4. Overview of the electrical system faults.

Faults in Communication Systems in Microgrids. The increased use of communication technologies in the microgrid also mean that the faults from communication system can affect the functioning of the electrical system. Faults in the communication channels can lead to the erroneous controlling of electrical infrastructure. Since the use of wireless communication network is foreseeable in the future, a quick overview of faults in communication network will help in understanding the need for handling communication faults to increase the resilience of the microgrids. Krings and Ma [16] studied the faults in the wireless communication network based on the earlier work by Thambidurai and Park [17]. They classified faults into several categories like benign and malicious, as shown in Fig. 5.

1. Transmissive symmetric: a single erroneous message is delivered to all receiving nodes. The messages, even faulty, are all identical. This indicates that the error has occurred due to the fault in the sender. Therefore the node can be identified

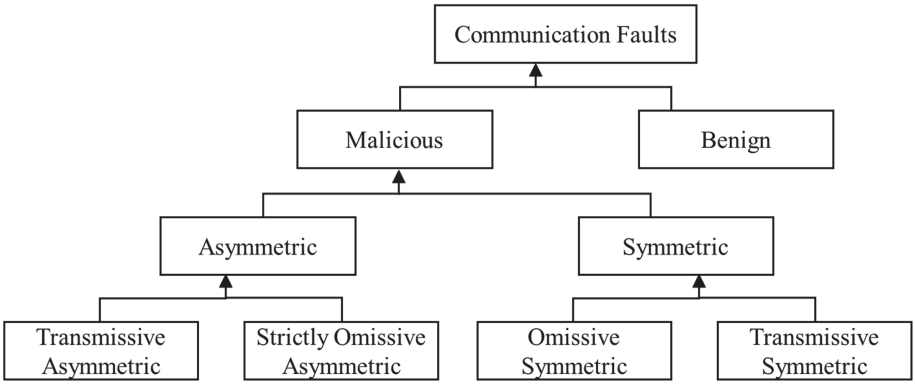

Fig. 5. Classification of the communication faults as proposed by Thambidurai and Park [17].

2. Omissive symmetric: no message is delivered to any receiving node. As before, all nodes are affected the same, however, the omissive behavior results in the destination nodes to most likely take different action as if the message had been received.
3. Transmissive asymmetric: this fault can exhibit any form of arbitrary asymmetric behavior, capable of delivering different erroneous messages to different receivers. This fault will need special attention to find which node has failed, whether it is the receiver or sender or in the communication link.
4. Strictly omissive asymmetric: a correct message is delivered to some nodes and no message is received by other nodes. Here, the omissions have the capability of affecting the system in an asymmetric way, since those nodes which have not received the message, will most likely react differently. In this case the sender or the receiver or some of the communication links get failed.

In addition to the faults, the communication system faces threats from cyber-attacks and malicious data injection due to the insecure networking. Peter Eder-Neuhauser [18] describes about the smart grid attack model, smart grid security model and the classification of existing malware types. Bo Chen [19] also discussed about different cyber-security issues in smart grids and conducted a study on modification of cyber-attacks, providing transient stability to the smart grids with voltage support devices. For a wide area monitoring, Shang Li [20] developed a distributed sequential cyber-attack detector using an adaptive sampling technique, to detect the false data injection. These works gave insight into the importance of addressing cyber-attack along with the communication faults in smart grids.

Faults in Software Systems in Microgrids. Microgrid Controller monitors and controls the electrical infrastructure within a microgrid can also encounter

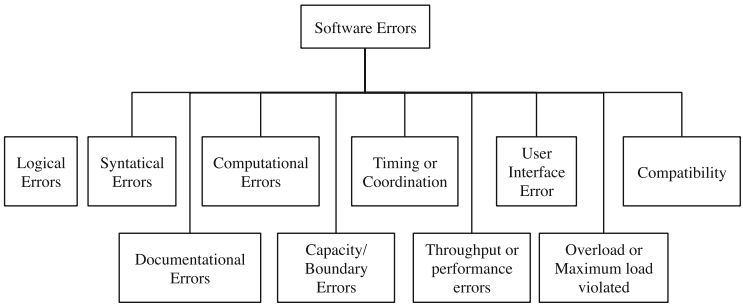

Fig. 6. Overview of software errors as proposed by Sommervile [21].

faults. The cause of the faults may vary from design time to run time. Few software faults are shown in Fig. 6. Some of the causes are described below:

1. Incomplete requirements: Many times the requirement elicitation for the target system is inconsistent, wrong or missing.
2. Incomplete communication: The lack of communication between the clients, designers and the software developers lead to a wrong interpretation of the requirements.
3. Incomplete documentation: Important documents like user manuals, operator manuals and design documents are written at different stages of the development. When these documents are not well written, incomplete or consistent, then the probability of faults increases.
4. Logical design flaws: These include incorrect computations, process definitions and unclear boundary conditions.
5. Weak testing: Once the coding is complete, incomplete test plans and insufficient error detection during software testing can also lead to fault during runtime.

Above mentioned causes can induce software faults, which can lead to the adverse effect on the operations of the microgrid. Authors found very limited focus on the effects of software faults in the microgrid fault handling research. In most cases, it is assumed that the microgrid controller follows prescribed safety standards and use standard protocols like SCADA etc.

From the above review of the existing literature, it can be concluded that the faults and their causes exist in each of the individual compositional system, but not in coordination (when coupled together).

4.2 Fault Handling Approaches in Microgrid

In this section, we review the widely used fault handling approaches in three different areas i.e. electrical, communication and software system.

Electrical Faults Handling: In a conventional grid, fault location, identification and restoration are carried out manually as they are time consuming. In the event of power outage, the rescue team has to manually travel throughout the transmission line path and check the condition at every pole. The operation turns out worse at night or during rainy season. The modern electrical fault handling techniques are listed below:

- The arc fault detection device [22] designed for household protection is a circuit breaker that isolates the power terminals when it detects an arc fault. This will prevent the house from catching fire. Surge protection devices protect the electrical and electronics equipment from lightning strike [23]. Residual Current Devices protect people from electric shock by isolating the power supply when earth leakage is detected [24].
- At substation level, air circuit breakers and vacuum circuit breakers are employed to isolate high voltage supplies. They provide protection against short circuit and over current and couples feeders within the distribution network [25]. Automatic Voltage Regulators (AVR) provide protection against burnouts and over-voltage in small factories and residential loads. AVR conditions the incoming power supply by using power electronic devices to protect devices against over voltage, harmonics, and surge [26].
- Khandare et al. [27] explored the possibilities of using numerical relay in microgrids to detect faulty lines, isolate the fault line and protect electronic loads. They designed the numerical relay and simulated it in different fault conditions to validate the design. Their findings concluded that in addition to primary fault protection devices like numerical relays, a secondary system is mandatory for added protection.
- Pilaquinga et al. [28] proposed a protection scheme for a 3-bus radial microgrid with a static compensator and storage system. They developed a bidirectional over-current relay as a primary protection system and frequency relays as secondary protection system. The proposed system was capable of detecting most of faults occurring in the microgrid during grid connected mode as well as islanded mode.
- On-line and off-line fault detection techniques for inverter based islanded microgrid proposed by Kuthsav Thattai, et al. [29] used Park's Vector Trajectory (PVT) and Hilbert-Huang Transform (HHT) and analyzed transient faults in load current at the point of common coupling (PCC).

Communication Faults Handling: Communication faults affect the performance of the system. A fault is detected when there is a delay or loss of information in the network. Time out and frequent monitoring processes can help to detect the faults. The two methods of handling these types of faults are fate sharing and the principle of optimality. The fate sharing principle [30] states that it is fine to lose the information from a node if the node itself is down at the same time. A node is a data point from where data is being transmitted. It can be a single sensor point or an aggregated point in which multiple sensor

data are aggregated. The principle of optimality states [31] that network protocol should be designed to operate in two different modes: failure free mode and failure mode. The cause of communication faults can be a communication link failure, node failure etc. The protocols to handle such failures depend on the number of nodes, network topology and geographical placement of node. Towards fault management by the microgrid controller, cyber-attacks resulting in denial-of-service (DoS) [32] have been looked into. Danzi et al. looked into the software-defined microgrid control model, where data exchange and control information are shared over the power-line communication.

Software Fault Handling: Increased synergy between electrical grid and ICT in a microgrid has resulted in additional complexity of fault detection and identification techniques. A fault could manifest itself differently in the system. For example, faults in ICT may lead to faults in electrical system, or multiple faults may have the same effect on the system due to the dynamic nature of the grid. The challenge is in the identification of faults accurately. In the survey conducted by Medeiros et al. [33], they emphasized that 48% failures occur in the middleware and 43% in the microgrid application. They also highlighted that the software faults are still harder to deal with due to several reasons like unknown failure semantics, use of proprietary applications etc. Fault handling approaches for software systems holds unique importance in the functioning of microgrid control system. In software systems, the topic of fault handling is studied as one of the aspects of ensuring dependability [8]. Fault handling in software systems is defined as the process that prevents faults from being activated again. It involves four steps: fault diagnosis, fault isolation, system reconfiguration and system re-initialization. Two popular fault handling approaches are by designing fail-safe or fail-operational systems. Fail-safe system are the ones that switch to a safe mode when failure is encountered. Fail-operational systems can still operate after a failure, with a reduced functionality.

Another fault handling approach fitting into the vision of future grids is *self-healing* capability. Self-healing properties have often been described as one of the core properties of autonomic computing. In the technology and automation context, the essence of autonomic computing [34,35] lies in the self-management of the system, which includes self-configuration, self-optimization, self-healing and self-protection.

Research towards making fault-tolerant systems exist in abundance [36–39]. Various fault analysis techniques and dependability issues in the software systems have also been studied [8,40]. Specifically with respect to smartgrids, advanced fault detection and handling techniques in electrical network [41–43], in software systems [44,45] and in the communication networks [46,47] are already in use.

From the above review of the existing fault handling literature, it can be concluded that there is hardly any focus on the faults induced by the software in distribution network. Study on the impact of software bug in the microgrid controller leading to errors and impacting the operations of microgrids is largely missing.

5 Fault Classification

In this section we investigate the commonly occurring faults in a microgrid and their impact. To investigate and systematically analyze potential causes of faults that lead to microgrid not performing any of its prescribed functions, a cause and effect analysis is carried out. A problem-solving tool also known as *fishbone analysis* is used. The benefit of doing the cause and benefit analysis of faults is that it helps in the deciding the scope of fault handling. Based on such analysis the microgrid controller can be designed in such a manner that the fault handling mechanisms are put in place at the design stage. The possibility of handling specific faults can also be extended during the operational stage. The fishbone diagram shown in Fig. 7, also known as Ishikawa model, is an effective tool to identify and classify the cause of faults that lead to lower performance situation in the microgrid. Ishikawa proposed generic categories for causes of fault as: environment, materials, machine, measurement, man, and method [48]. The low performance could be power outage situation, software error or communication network problem. The cause of the lower performance can originate from: i)instrumentation and control ii) communication network iii) electrical network iv) user v) environments and vi) microgrid control system. In this work, these categories are modified. For instance, the *machine* refers to the *instrumentation and control* category that helps in capturing the measurable values of the environment. The *measurement* refers to the power supply indicators listed under the *electrical* category. The *man* is indicated by the user/people interacting with the system. The *method* is the way data is collected, manipulated and analyzed, which are listed in the *communication and microgrid control system* categories. Finally, the *environment* category represents the impact of the climate on the micrgorid.

A detailed description of each category is as following:

- Faults in *instrumentation and control* category are the faults in the hardware devices, including smart sensors that capture the observable parameters from the environment like temperature, humidity, movement etc. Small power generation units like Photovoltaic and smart power backups like smart batteries. These devices provide data to build intelligence in the microgrid. For example, energy efficient consumption, optimized use of local power generation etc. These smart devices could also fail. This may lead to sensors sending incorrect values, which results in wrong decisions. Other kind of hardware damages include relay malfunctions that lead to recording noises and incorrect data reading.
- Faults in the *communication* category relate to the faults in the communication distribution. The primary objective of the communication network is message forwarding. If the data that is transmitted doesn't reach the receiver's end in a certain specified format, the primary objective is not fulfilled. Faults in the communication network are diverse and are discussed in Sect. 4. Network coverage issues, varying bandwidth, data losses, unsecured data transfer and time synchronization issues are few issues that an unstable communication network might experience. Clock synchronization issues

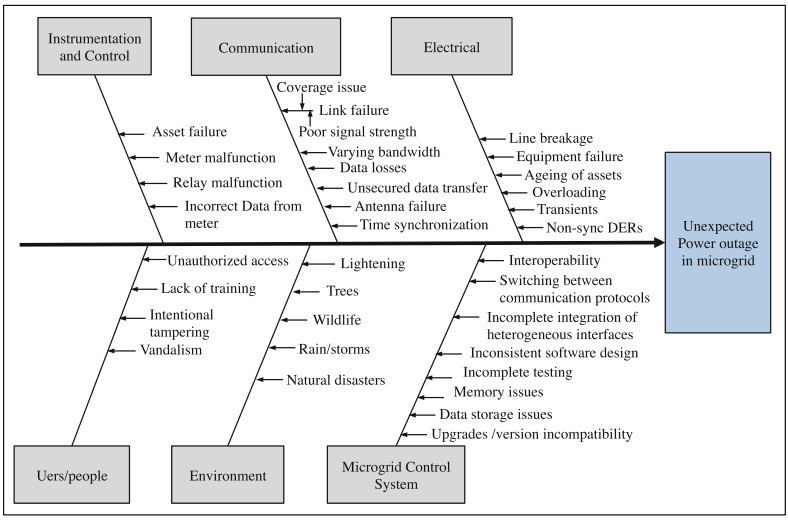

Fig. 7. Fishbone analysis of faults and failures from various sources in a microgrid, which are a mix up of design and runtime faults.

between the distributed entities may lead to a delay in controlling the switches in the specified order, which can generate unbalanced power supply in the electrical network, leading to power outage situation. Faults in the communication network vary from no data transmission to wrong response received as acknowledgment.

– Faults in the *electrical* category are the faults that affect power supply in the microgrid. Line breakages could be due to adverse conditions such as tree felling(in case of overhead lines) or erroneous digging of the ground (in case of underground lines). Extreme changes in weather such as floods, heavy rain, increased thunderstorms, could lead to heating up of wires, melting of fuses, short-circuiting etc. Loose connections of the electrical wires and connected peripherals can cause fire or could lead to sudden voltage variations. Transient currents due to sudden release or withdrawal of power can result in instabilities in the distribution network. With increased inclusion of renewable energy generators into the microgrid this situation is expected to occur frequently. The overload situations, where several high energy consumption devices are simultaneously connected, leading to a sudden deficit of power could also induce instabilities.
– Faults can also be introduced by humans. The *Users/people* category deals with faults occurring due to human interaction. Users interacting with microgrids range from common household habitants to the system operator. Various roles are defined for users based on the extent of their interaction with the microgrid. Faults could be caused due to lack of training amongst the users. There could be unauthorized users who access microgrid information in order to shut down the system or steal sensitive data. Intentional tempering of

smart meters and sensors could also lead to faults. Other issues include vandalism with the intention to break or interrupt smart monitoring and control processes.
- *Environment* category represents the surroundings in which the system under the observation operates. Weather conditions play a big role in the functioning of devices and communication. During peak summers, sensors are prone to burn or melt due to high heat. During storms, communication network often fails to function as desired.
- Faults in the *microgrid control system* category deal with the faults in the controller. These faults may emerge during the operational stage due to various reasons such as insufficient requirements, design defects, and errors in coding, testing and maintenance. Insufficiency in requirements could be due to incomplete and inconsistent description of the target system. Design defects arise due to the incorrect design specifications or the inconsistent translation of requirements etc. The choice of programming paradigm used for the implementation and implementation of logic for the software controllers may also lead to wrong control actions. Some other examples of coding errors include incorrect configurations, uninitialized variables, invalid file path, wrong interface specification, version issues with standard libraries etc. During testing and maintenance phases, if the software is either not tested thoroughly or changes in the software are not tracked and maintained, then the microgrid controller will not be able to monitor and control as required.

The faults in the microgrid are also context-specific, based on the geographical setting, devices in use, etc. However, fishbone analysis reveals the enormity of the fault in microgrid environment. It emphasises that focusing on the faults and failures from the electrical domain is not sufficient to create a resilient microgrid, as there are multiple systems operating simultaneously. This fishbone analysis helps the developers and designers of microgrid to plan recovery and observe the effects of the faults. Such analysis of commonly occurring faults helps in identifying the dependencies at the design stage.

6 Promising Solutions and Future Directions

With the fault cases and survey presented in the previous sections, it is clear that fault detection and recovery in the microgrids are highly desirable. The existing methods that exist individually in electrical, software and communication system must be brought together in the microgrid. As much as data capturing and analysis is required, the design of the application and platform to handle enormous data is equally important. A generic fault handler should be part of each microgrid controller, so that the cascading effects of faults can be observed. The underlying architecture of the microgrid controller has to be generic to include fault profiles and fault detection based on the domain-specific models and data analytics. A generic fault handler and the design helps in the recovery related decisions. Data analytics based fault handling provides capabilities such as anomaly detection and predictive maintenance. During the survey conducted,

we found some of the promising solutions used for fault detection and recovery, resulting in improved resilience of the microgrid. Following are the few of the approaches:

- **Multi-Agent System (MAS):** Application of MAS in the electrical engineering for design and distributed controls is explored by many researchers [49,50]. Autonomous independent agents interact and coordinate with each other to fulfil both individual and system goals. Howell et al. [51] argued that in the smart grid system each individual microgrid can be considered as an autonomous agent such that the intelligence and decision making can be distributed among agents. Plenty of research articles exist on the local and global goals of agents such as storage management within a microgrid and local balancing by the negotiating agents [52,53].
- **Architectures:** In the conventional grid, power flow is in one direction only, hence the system architecture is also layered with decisions executed in a top-down manner. In microgrids, distributed decision and coordination require system architectures to also be distributed. Existing approaches of Service-Oriented Architecture (SOA), MAS and Holonic Systems provide distributed decision and definition of different levels of automation [51]. Hybrid approaches also exist that combine these system architectures for fine-grained control within a microgrid and better coordination among each other [54,55]. An Agent based architecture is proposed and demonstrated for fault location isolation and supply restoration (FLISR) application in electrical system automation by Zhabelova et al. [56]. A survey on software architectures by Ramesh et al. [57] provides an overview of the use of software technologies in the legacy systems like power grids. They have also presented the list of existing reference architectures for smartgrids.
  Towards fault-tolerance embedded in the design, agent based systems are used [58,59], where the model-based approach is used to define the communication between agents to define the internal behaviour of agents and resolve conflicts among agents in the electrical grid.
- **Data Analytics based fault handling:** In the last five years, there has been an exponential growth of Artificial Intelligence (AI) based approaches from anomaly detection to power stabilization. In case of reconfiguration of the electrical network to stabilize voltage in the network, approaches like genetic algorithm [60,61], reinforcement learning [62] and deep reinforcement learning [63] are widely popular. Apart from this, anomaly detection, uncertainty quantification and predictive maintenance are some of the areas where data analytics is being used to handle faults at the operational stage.

7 Conclusion

In this paper, we explained faults and failures from different compositional systems and then presented the fault scope in a microgrid. With the help of fault cases and their cause-effect analysis, the cascading effect of faults was analyzed. The categories considered in the analysis were: electrical system, smart devices,

communication network, data handling, users, microgrid control system. We found that not just the electrical faults, but faults occurring in the software and the communication systems affect the microgrid operations. We further studied the cascading effects of faults in the microgrid, which highlights the need for including fault detection and diagnosis in the design of the microgrid control system. By reviewing the existing fault handling strategies, we found that interdependency and cascading effects of faults require further research. Authors suggested some areas of research, where fault handling methods can be combined with the existing methods such as architecture designing, agent based systems and data analytics. In conclusion, authors emphasize that to make grid resilient and stable, approaches of design(architectures) should be combined with the faults handling using data analytics.

Acknowledgement. The authors would like to thank Dr. Markus Duchon, Dr. Maneesha V Ramesh, Dr. Aryadevi R D, Mr. Sudharsan V C and Shri Mata Amritanandamayi Devi for supporting the research work. This work was partly done under the Project "Smart Services and Optimization for Microgrids (SSOM)" in the scheme of Project-based Personnel Exchange Program with Indo-German (DST-DAAD) Joint Research Collaboration.

References

1. Guardian, T.: Millions across South America hit by massive power cut (2019). https://www.theguardian.com/world/2019/jun/16/millions-across-south-america-hit-by-massive-power-cut-argentina-uruguay-paraguay-brazil
2. IEEE Power and Energy Society. IEEE Standard for the Specification of Microgrid Controllers, IEEE STD 2030.7-2017. IEEE (2017)
3. Dinkel, M., Stesny, S., Baumgarten, U.: Interactive self-healing for black-box components in distributed embedded environments. In: 2007 ITG-GI Conference on Communication in Distributed Systems (KiVS), pp. 1–12 (2007)
4. Friedman, A.: Diagnosis of short-circuit faults in combinational circuits. IEEE Trans. Comput. **100**, 746–752 (1974)
5. Zubrow, D., Baldwin, M.: IEEE Guide to Classification for Software Anomalies. IEEE STD 1044.1-1995, p. i (1996)
6. Parandehgheibi, M., Turitsyn, K., Modiano, E.: Modeling the impact of communication loss on the power grid under emergency control. In: 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 356–361 (2015)
7. Ferc, N.: Arizona-southern California outages on 8 September 2011: causes and recommendations. FERC and NERC (2012)
8. Avizienis, A., Laprie, J., Randell, B.: Fundamental concepts of dependability. University of Newcastle upon Tyne, Computing Science (2001)
9. Lasseter, R.: Microgrids. In: 2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 02CH37309), vol. 1, pp. 305–308 (2002)
10. Wang, Y., Zhang, Z., Fu, Y., Hei, Y., Zhang, X.: Pole-to-ground fault analysis in transmission line of DC grids based on VSC. In: 2016 IEEE 8th International Power Electronics and Motion Control Conference (IPEMC-ECCE Asia), pp. 2028–2032 (2016)

11. Laaksonen, H., Kauhaniemi, K.: Fault type and location detection in islanded microgrid with different control methods based converters. In: 19th International Conference on Electricity Distribution (CIRED), Vienna, Austria (2007)
12. Nikkhajoei, H., Lasseter, R.: Microgrid fault protection based on symmetrical and differential current components. In: Power System Engineering Research Center, pp. 71–74 (2006)
13. Zhou, Y., Xu, G., Chen, Y.: Fault location in power electrical traction line system. Energies **5**, 5002–5018 (2012)
14. Hong, Y., Wei, Y., Chang, Y., Lee, Y., Liu, P.: Fault detection and location by static switches in microgrids using wavelet transform and adaptive network-based fuzzy inference system. Energies **7**, 2658–2675 (2014)
15. Sadeghkhani, I., Golshan, M., Guerrero, J., Mehrizi-Sani, A.: A current limiting strategy to improve fault ride-through of inverter interfaced autonomous microgrids. IEEE Trans. Smart Grid **8**, 2138–2148 (2017)
16. Krings, A., Ma, Z.: Fault-models in wireless communication: towards survivable ad hoc networks. In: MILCOM 2006–2006 IEEE Military Communications Conference, pp. 1–7 (2006)
17. Thambidurai, P., Park, Y.: Interactive consistency with multiple failure modes. In: Proceedings [1988] Seventh Symposium on Reliable Distributed Systems, pp. 93–100 (1988)
18. Eder-Neuhauser, P., Zseby, T., Fabini, J., Vormayr, G.: Cyber attack models for smart grid environments. Sustain. Energy Grids Netw. **12**, 10–29 (2017)
19. Chen, B., Mashayekh, S., Butler-Purry, K., Kundur, D.: Impact of cyber attacks on transient stability of smart grids with voltage support devices. In: 2013 IEEE Power and Energy Society General Meeting, pp. 1–5 (2013)
20. Li, S., Yılmaz, Y., Wang, X.: Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans. Smart Grid **6**, 2725–2735 (2014)
21. Sommerville, I.: Software Engineering. Addison-Wesley, New York (2010)
22. Electrical Safety. Arc Fault Detection Devices reduce the risk of electrical fire (2019). https://www.se.com/in/en/home/renovation/home-protection.jsp
23. Electrical Safety. Surge protection devices: your best defence (2019). https://www.se.com/in/en/home/renovation/electronic-equipment-protection.jsp
24. Electrical Safety. Protect your family with Residual Current Devices (2019). https://www.se.com/in/en/home/renovation/people-protection.jsp
25. Electrical Safety. Circuit Breakers and Switches (2019). https://www.se.com/ww/en/product-category/4200-circuit-breakers-and-switches/
26. Generator System. Working Principle of Automatic Voltage Regulator (2019). https://medium.com/@dieselgenerator/working-principle-of-automatic-voltage-regulator-1ff1275f5495
27. Khandare, P., Deokar, S., Dixit, A.: Advanced technique in micro grid protection for various fault by using numerical relay. In: 2017 2nd International Conference for Convergence in Technology (I2CT), pp. 803–807 (2017)
28. Pilaquinga, D., Pozo, M.: Novel protection schema for a radial microgrid system. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America), pp. 1–6 (2017)
29. Thattai, K., Sahoo, A., Ravishankar, J.: On-line and off-line fault detection techniques for inverter based islanded microgrid. In: 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), pp. 1–6 (2018)
30. Clark, D.: The design philosophy of the DARPA Internet protocols. In: Symposium Proceedings on Communications Architectures and Protocols, pp. 106–114 (1988)

31. Gupta, A., Rothermel, K.: Fault handling for multi-party real-time communication. In: ICSI (1995)
32. Danzi, P., Angjelichinoski, M., Stefanović, Č, Dragičević, T., Popovski, P.: Software-defined microgrid control for resilience against denial-of-service attacks. IEEE Trans. Smart Grid **10**, 5258–5268 (2018)
33. Medeiros, R., Cirne, W., Brasileiro, F., Sauvé, J.: Faults in grids: why are they so bad and what can be done about it? In: Proceedings. First Latin American Web Congress, pp. 18–24 (2003)
34. Kephart, J., Chess, D.: The vision of autonomic computing. Computer **36**, 41–50 (2003)
35. Laster, S., Olatunji, A.: Autonomic computing: towards a self-healing system. In: Proceedings of the Spring, pp. 62–78 (2007)
36. Nelson, V.: Fault-tolerant computing: fundamental concepts. Computer **23**, 19–25 (1990)
37. Ericson, C., et al.: Hazard Analysis Techniques for System Safety. Wiley, Hoboken (2015)
38. Koren, I., Krishna, C.: Fault-Tolerant Systems. Morgan Kaufmann, Burlington (2010)
39. Lyu, M., et al.: Handbook of Software Reliability Engineering. IEEE Computer Society Press, California (1996)
40. Avižienis, A., Laprie, J.-C., Randell, B.: Dependability and its threats: a taxonomy. In: Jacquart, R. (ed.) Building the Information Society. IIFIP, vol. 156, pp. 91–120. Springer, Boston, MA (2004). https://doi.org/10.1007/978-1-4020-8157-6_13
41. Hwang, I., Kim, S., Kim, Y., Seah, C.: A survey of fault detection, isolation, and reconfiguration methods. IEEE Trans. Control Syst. Technol. **18**, 636–653 (2010)
42. Alwash, S., Ramachandaramurthy, V.: Novel fault-location method for overhead electrical distribution systems. IEEJ Trans. Electr. Electron. Eng. **8**, S13–S19 (2013)
43. Kezunovic, M.: Smart fault location for smart grids. IEEE Trans. Smart Grid **2**, 11–22 (2011)
44. Paradkar, A.: Case studies on fault detection effectiveness of model based test generation techniques. ACM SIGSOFT Softw. Eng. Notes **30**, 1–7 (2005)
45. Hall, T., Beecham, S., Bowes, D., Gray, D., Counsell, S.: A systematic literature review on fault prediction performance in software engineering. IEEE Trans. Software Eng. **38**, 1276–1304 (2012)
46. Pereira, E., Pereira, R.: Fault monitoring and detection of distributed services over local and wide area networks. In: 12th International Conference on Parallel and Distributed Systems, ICPADS 2006, vol. 2 (2006)
47. Krings, A., Ma, Z.: Fault-models in wireless communication: towards survivable ad hoc networks. In: Military Communications Conference, MILCOM 2006, pp. 1–7. IEEE (2006)
48. Ishikawa, K., Ishikawa, K.: Guide to quality control. Asian Productivity Organization Tokyo (1982)
49. McArthur, S., et al.: Multi-agent systems for power engineering applications-Part I: concepts, approaches, and technical challenges. IEEE Trans. Power Syst. **22**, 1743–1752 (2007)
50. Zhabelova, G.: Software architecture and design methodology for distributed agent-based automation of smart grid. University of Auckland (2014)
51. Howell, S., Rezgui, Y., Hippolyte, J., Jayan, B., Li, H.: Towards the next generation of smart grids: semantic and holonic multi-agent management of distributed energy resources. Renew. Sustain. Energy Rev. **77**, 193–214 (2017)

52. Brazier, F., et al.: Agents negotiating for load balancing of electricity use. In: Proceedings. 18th International Conference on Distributed Computing Systems (Cat. No. 98CB36183), pp. 622–629 (1998)
53. Vytelingum, P., Voice, T., Ramchurn, S., Rogers, A., Jennings, N.: Agent-based micro-storage management for the smart grid (2010)
54. Gupta, P., Gibtner, A., Duchon, M., Koss, D., Schätz, B.: Using knowledge discovery for autonomous decision making in smart grid nodes. In: 2015 IEEE International Conference on Industrial Technology (ICIT), pp. 3134–3139 (2015)
55. Gupta, P., Duchon, M.: Developing self-similar hybrid control architecture based on SGAM-based methodology for distributed microgrids. Designs **2**, 41 (2018)
56. Zhabelova, G., Vyatkin, V., Dubinin, V.: Toward industrially usable agent technology for smart grid automation. IEEE Trans. Industr. Electron. **62**, 2629–2641 (2014)
57. Ramesh, A., Karthikeyan, P., Padmanaban, S., Balasubramanian, S., Guerrero, J.: A Bibliographical Survey on Software Architectures for Smart Grid System. Preprints (2018)
58. Haqiq, A., Bounabat, B.: Towards integration of fault tolerance in agent-based systems. Procedia Comput. Sci. **127**, 264–273 (2018)
59. Haegg, S.: A sentinel approach to fault handling in multi-agent systems. In: Australian Workshop on Distributed Artificial Intelligence, pp. 181–195 (1996)
60. Tomoiagă, B., Chindriş, M., Sumper, A., Sudria-Andreu, A., Villafafila-Robles, R.: Pareto optimal reconfiguration of power distribution systems using a genetic algorithm based on NSGA-II. Energies **6**, 1439–1455 (2013)
61. Ebrahimi Moghadam, M., Falaghi, H., Farhadi, M.: A novel method of optimal capacitor placement in the presence of harmonics for power distribution network using NSGA-II multi-objective genetic optimization algorithm. Math. Comput. Appl. **25**, 17 (2020)
62. Gao, Y., Shi, J., Wang, W., Yu, N.: Dynamic distribution network reconfiguration using reinforcement learning. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7 (2019)
63. Yang, Q., Wang, G., Sadeghi, A., Giannakis, G., Sun, J.: Two-timescale voltage control in distribution grids using deep reinforcement learning. IEEE Trans. Smart Grid **11**, 2313–2323 (2019)