Failure Modes and Effects Analysis (FMEA) for Smart Electrical Distribution Systems

Alexandre Neves Silvestre Baleia, MSc. Student in Instituto Superior Técnico, Lisboa, Portugal. November 2018

***Abstract*—Reliability assessment in traditional power distribution systems has played a key role in power system planning, design and operation. Recently, new information and communication technologies have been introduced in power systems automation and asset management, making the distribution network even more complex. In order to achieve efficient energy management, the distribution grid has to adopt a new configuration and operational conditions that will change the paradigm of the actual electrical system which has to face numerous technical and economic challenges. The emergence of the smart systems concept to face future energetic needs requires alternative approaches for evaluating the reliability of modern distribution systems, especially in the smart grids environment. In this thesis, a reliability approach that makes use of failure modes of power and cyber network main components will be proposed to evaluate risk analysis in smart electrical distribution systems. This dissertation introduces the application of Failure Modes and Effects Analysis (FMEA) method in future smart grid systems in order to establish the impacts of different failure modes on smart grid performance. A smart grid test system is defined and failure modes and their effects on the system are scrutinized. Preventive maintenance tasks are enumerated to minimize the impact of high-risk failures and to increase reliability of the proposed test system.**

Keywords: failure mode, failure rate, FMEA, Reliability, risk analysis, smart grid.

I. Introduction

It is undeniable that electrical energy plays a crucial role in today's society. It is the most versatile and easily controlled form of energy and welfare, comfort and health of world communities depends on the delivery of electricity. It is involved in almost all aspects of society's daily routine.

Nowadays, it urges the necessity to introduce new ways of generating electrical energy from renewable resources in an effort to decrease the impact of world's climate changes by decreasing the dependence from conventional and pollutant energy resources [1], [2]. Associated with the growth of mobile loads and the increasing number of energy storage equipment [3], [4], new technological applications will be integrated in robust and complex cyber-physical systems in order to provide energy management in a more reliable, effective and sustainable way.

However, new problems arise: the increased complexity of the electrical system creates a considerable number of barriers that can difficult the development of such system, regarding technical and non-technical challenges: several failures can occur, compromising system's performance and the correct delivery of energy [5]–[11].

It is important to evaluate reliability and security of a smart system through alternative reliability approaches. The relevance of these tools in such complex systems like future smart grids allows not only the development of maintenance strategies to create a more authentic, safe and secure system but also the optimization of installation and maintenance costs, in order to create a high-reliable system with low-risk failures.

When considering reliability tools, Reliability Centered Maintenance (RCM) arises as one of the most important ones.

A few studies concerning RCM techniques in energy systems had been developed throughout the years.

In [5] a first attempt for an RCM application in a transmission system was presented. The Turkish National Power Transmission System was decomposed into sub-systems and failures of each sub-system was held individually to attain a reasonable maintenance program for the transmission system.

In [6], RCM methodologies are applied in more than 90 high-voltage stations operated by a generating and transmission company in Brazil. Several power system performance indexes and results were modeled and compared with the company operating data. In another survey, reference [7] proposes a reliability model based on a combination of fault tree analysis and FMEA combined with dynamic power system simulations as used for probabilistic analysis of power system reliability in the Finnish 400kV transmission system.

A method based on condition-based maintenance (preventive maintenance) and system reliability assessment was proposed in [8] to model the quantitative relationship between monitoring data of overhead lines and failure rates as well as system reliability in overhead lines in a 182-bus, considering 5474 MW of the transmission system in southwest China.

Authors in [9] use Markov state model for reliability analysis of various substation automation system architectures. A new approach for power system reliability analysis using the fault tree analysis approach was also developed in [10].

In [12] and [13], FMEA was used to analyse failure modes, their causes and effects in power equipment. Reliability Block Diagram (RBD) and Monte-Carlo simulation methods were applied in [11] as proposed reliability estimation methods in an UPS.

Related to an introduction in reliability studies in future smart grids, [14] presented an extensive study based on analytic and probabilistic reliability procedures under various scenarios. In this turn, authors in [15] analyse reliability performance of smart grids with demand-side management, distributed generation and storage technologies using adapted Monte-Carlo procedures.

In sum, several studies focused on RCM and alternative approaches to evaluate their viability in reliability assessment in energy systems, but few have considered FMEA as a reliable tool for risk assessment.

The main purpose of this dissertation is to conduct a risk analysis in a smart electrical distribution grid applying FMEA, an RCM technique which emphasizes failure modes impact on the grid.

In chapter II, a general characterization of the concept of a smart grid is presented, setting the current energy panorama in the need for technological evolution of the electrical grid. Chapter III gives a special focus to the FMEA methodology that will be used to address the problem. The basics of FMEA, including its fundamental concepts, development, implementing procedure and basic terminology, are herein introduced. Chapter IV describes the implementation of FMEA in a test system in order to evaluate FMEA methodology in a smart grid reliability study. In chapter V, it will be presented the most relevant results obtained through the employment of FMEA in a smart grid environment. FMEA methodology and its viability in a complex system such as a smart electrical distribution system are discussed. Finally, chapter VI summarizes the main conclusions of this dissertation.

II. Smart Grid Definition

The interest in local connection of distributed electrical resources at the distribution network has gained lots of attention of the industry. Hence, small, modern and interconnected distribution systems – designated microgrids – have been integrated in the traditional distribution network [16].

A microgrid is defined as an interconnected network of distributed energy systems (loads and resources) that can function whether it is connected to or separate from the electricity grid – interconnected or islanded operation mode, respectively.

In the long run, future smart grids are expected to emerge as a well-planned integration of microgrids that will be interconnected through dedicated highways for command, data and power exchange.

A. Smart Grid Bried Description

Smart grid, also known as ”intelligent grid”, ”modern grid” or ”future grid”, is a cyber-physical system capable of integrating an information and communication technology (ICT) network with the existing power system infrastructure. A smart grid is a smarter version of its predecessor, the traditional power grid, which has to face the increased use of digital information and control technologies to improve reliability, security and efficiency of the grid [17].

Smart grid is envisioned to take advantage of all available modern technologies in transforming the current grid to one that functions more intelligently, meaning it has to face some requirements to meet the challenges of the 21st century needs. According to [4], a smart grid should:

- enable active participation by consumers in demand response;
- be self-healing;
- provide quality power that meets current needs;
- operate resiliently against both physical and cyberattacks;
- accommodate all generation and storage options;
- enable new products, services and markets;
- optimize asset utilization and operating efficiency.

In short, the grid will be more dynamic in its configuration and operational conditions, which will present many opportunities for optimization but also many new technical challenges, such as [3]:

- integration of renewable energy: energy from diverse renewable sources, in addition to traditional ones, must be combined to serve customer needs while minimizing the impact on the environment and maximizing sustainability; renewable sources will be found distributed in the grid;
- proliferation of energy storage: numerous energy storage centers must be used to buffer the impact of sudden load changes and fluctuations in renewable resources;
- growth of mobile loads and resources: the increase viability of electric vehicles means many loads and resources will no longer be stationary, which will represent both mobile loads and potential sources of power;
- the smart consumer and the grid-friendly appliance: end-user interactive and intelligent appliances will be able to interact with the grid by collecting and monitor information about consumption patterns, modulating power consumption to reduce stress on the system and to help preventing service disruptions;
- real-time distributed intelligence and a new level of controllability: advanced grid-monitoring, optimization and control applications will continuously monitor the operating conditions of grid assets and determine the best control strategies to maximize energy delivery efficiency and security in real time.

Figure 1 depicts a smart grid's typical cyber-physical structure as a set of correlated interacting layers. At the bottom level, the physical layer incorporates physical systems and devices which participate in the generation, transmission, distribution and consumption sectors of the grid. At the top level, the cyber layer manages and operates the physical layer, providing local control and computation capabilities through cyber systems and enabling intra and inter-communication between physical and cyber systems [18].

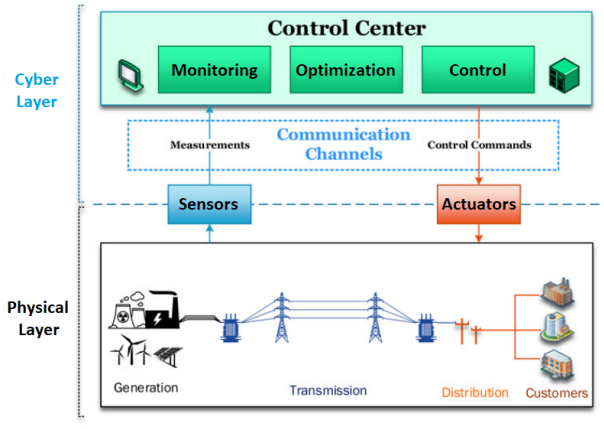

Fig. 1. Typical cyber-physical structure in a smart grid (adapted from [19])

1) Power Network: The electrical network is an interconnected physical network responsible for delivering electricity

from producers to consumers. A power network is usually divided into three hierarchical levels: generation, accountable for electrical power production; transmission, responsible for carrying power from distant sources to demand centers; and distribution, taking charge of connecting individual customers.

A power grid has its own physical laws and limitations due to its inherence. For instance, the power balance at each node and the relation between voltage and power through each line are two fundamental sets of equations that must be considered in a power study. Overloads and abnormal voltages must be avoided to preserve physical network integrity and to guarantee user's security, delivering reliable and stable electricity to customers [20]. Otherwise, possible destructive effects on power network could collapse the system, compromising society's comfort and welfare.

2) Cyber Network: The cyber network is an ICT network accountable for performing a wide variety of tasks in order to successfully operate the power system. These tasks consist in monitoring, protecting and controlling the power system, making use of every kind of data collected in all devices.

The cyber network is usually divided into two sub-layers: the communication layer, in which grid-status data are gathered in real-time synchronization and information is exchanged between devices; and the control layer, responsible for power system automation and other widespread control systems.

The typical communication framework of a smart grid is usually categorized in three levels: Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide-Area Network (WAN).

Communication is essential to support different smart grid functions such as self-healing, asset management and wide area integrity. The International Electrotechnical Commission (IEC) 61850 standard allows high-speed Ethernet communication at electrical substations and offers an international standardized configuration language and data model, providing interoperability, reliability and agility in the communication system [21] and [22].

Besides that, IEC 60870 standard defines communication protocols used for telecontrol – Supervisory Control And Data Acquisition (SCADA) control center application –, which in turn is used for power system automation and other widespread control systems, suiting the requirements for communication between control centers and substations [22].

Along with several benefits communication networks offer to smart grids, they bring the private power control systems to the public communication networks and associated security vulnerabilities [23]. Such a substantial dependence on ICT, alongside with the increasing complexity of the cyber network, require cybersecurity techniques in order to meet cybersecurity requirements.

3) Cyber-Power Network: Communication networks connect power and cyber layers with robust communication links, which perform two way communication between smart grid domains as shown in Figure 2. Electrical flows are also illustrated between power layer's domains.

The cyber-power network is known as an interconnected network with interdependences. Interdependency means that

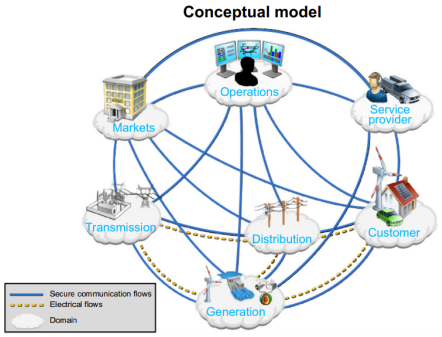

Fig. 2. Conceptual model for smart grid (from [24])

the correct and appropriate operation of one element of the grid depends on the existence and proper function of some other elements, whether or not they are part of the same network [25] and [26]. Actual interdependencies inherent to the smart grid operation cover element-element and network-element interdependencies, as recognized in [25].

As long as numerous power applications rely upon increasingly complex cyber networks, the probability of failure in a smart grid also increases, and their impact on the power system become a serious concern. In general, the impact of non-ideal communication in the operation of the power grid can be categorized as follows [27]:

- Failure to send the correct control signal to a dispatchable energy resource;
- Failure to send the correct demand response signal to a controllable load;
- Failure to send the correct open/close command to breakers or tie-switches;
- Failure to send the correct measurement values (e.g. voltage, current, active power, reactive power, power factor, etc.) to the control center or any distributed function using those measurements;
- Failure to send the correct status data (e.g. breaker status, capacitor banks status, etc.) to the control center or any distributed function using those data.

In short, wrong operation and deficiency in cyber network applications, such as in control, monitoring and protection tasks, are decisive factors for the degradation of the power grid's stability and efficiency, which ultimately may cause massive outages.

B. Smart Grid Security

The vulnerability of future smart grids has been illustrated in today's electric grids, such as recent incidents in the USA and in Ukraine: in PG&E Metcalf Transmission Substation, in 2013, a sniper attack fired on 17 substation's transformers resulting in $15 million worth of equipment damage [28], luckily with little impact on energy supply in Silicon Valley; in this turn, in Ukraine power grid, in 2016, malware was injected from the communication channels and allowed the attacker to obtain illegal access to the control center. With the collected information, the attacker was able to determine critical lines

in the regional grid leading to a widespread power blackout affecting 225,000 customers [29].

This clearly shows that knowledgeable attackers can directly exploit vulnerabilities of communication and control systems to exert immediate and significant impacts in the smart grid.

The security issues of a cyber-physical smart grid comprise the following issues: the physical components of the smart grid; control centres and control applications; the cyber infrastructures for stable, reliable, and efficient operation and planning; the correlation between cyber-attacks and the resulting physical system impacts and protection measures to mitigate risks from cyber threats.

1) Physical Security: Power systems have inherent physical vulnerabilities. Besides that, the increase of the number of equipment strictly necessary for the correct operation of future smart grids enlarge insecure physical locations, making them vulnerable to physical access. An equipment could be damaged or even destroyed in an attempt to make the service unavailable.

2) Cybersecurity: The increasing complexity of the communication network and ICT strictly necessary for the control of a smart grid create new weaknesses in the cyber network. A great number of intelligent devices represents several points for external access in the cyber system, making the smart grid more vulnerable to different types of attacks which can compromise the correct operation of the grid.

There are many possible schemes for cyber-attacks, which according to the authors in [27] they can be defined in device attacks, privacy attacks, data attack and network availability attacks.

Such attacks can occur by malware spreading, false data injection or control system network access through database links. Communication equipment may be compromised, in the sense it can be directly damage or used as a backdoor to launch future attacks. Hence, sensitive information can be obtained and network availability is in danger, since attackers might attempt to delay, block or corrupt information transmission (and affect SCADA for instance) in order to make smart grid resources unavailable.

3) Cyber-Physical security: One general aspect recognized in every cybersecurity study is the importance of developing strategies to ensure several security requirements in order to protect a smart grid against cyberattacks or at least mitigate their actions. These requirements are listed in [27]:

- Privacy: a customer load data from smart meters should be maintained confidential;
- Availability: attackers cannot perform a denial of service attack or its impact must be mitigated;
- Integrity: data must not be manipulated by unauthorized users;
- Authentication: the identity of communication users must be validated;
- Authorization: unauthorized users cannot access the cyber system;
- Audibility: a system must record all kinds of actions made in the system (keep track of actions history for useful further investigations);
- Non-repudiability: a system must provide irrefutable proof to a third party on who started an action in the system.

If some of the previous security requirements are violated, adverse impacts in power supply can occur, and system's reliability drastically decreases.

On the one hand, data modified from smart meters in LAN communications can usurp collected data tripping the circuit breakers and leading to inadvertent operations in power grid [30] and [31].

On the other hand, in MAN and WAN communications, sensor data could be missed or misrepresented, or external control commands could be injected; data delay could compromise the effectiveness of SCADA, exchanged data between different cyber equipment could be modified and illegal access to price and cost information can occur.

This actions could cause adverse impacts in power system, such as false alarms, Energy Management Systems (EMS) applications failure – like state estimation and contingency analysis – shifting power transmission and distribution system from its optimal running point (non-optimal planning and asset management). The system can run exceeding its own limits and in the worst cases malicious actions leads to system outage and personnel injuries or death [30] and [31].

Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient security strategies must be incorporated in the smart grid system to reduce the risks to an acceptable secure level. They must ensure the availability of uninterrupted power supply according to user requirements, the integrity of communicated information and confidentiality of user's data in order to make a smart grid more reliable.

III. Reliability Assessment

A. The RCM Approach

The RCM methodology is a systematic approach which determines maintenance requirements of a system or equipment in its operation with the aim of increasing cost effectiveness, reliability and a greater understanding of the level of risk of the analyzed system [32] and [33].

First adopted in 1978 in *Reliability-Centered Maintenance* to determine the optimum maintenance requirements in the aeronautic industry, F. Stanley Nowlan and Howard F. Heap took a different approach from maintenance methodologies at that time by developing a maintenance strategy based on system functions, consequence of failure and failure modes, in addition to the existing preventive maintenance techniques. This new approach combined proactive maintenance techniques, based on preventive maintenance in order to avoid the failure of an equipment or system or at least to decrease its probability of failure, and reactive techniques, related to maintenance techniques implemented after a failure occurs.

Nowadays, RCM integrates Preventive Maintenance (PM), Predictive Testing and Inspection (PTI), Repair (also called Reactive Maintenance (RM)) and Proactive Maintenance (PrM) to increase the probability a system or component will

function in the desired manner over its design life-cycle with a minimum amount of maintenance and downtime [33].

A technique for risk analysis and for proactive maintenance that can be implemented in RCM is FMEA, which is a qualitative technique for reliability assessment and risk analysis.

B. FMEA methodology

Failure Mode and Effect Analysis (FMEA), first developed in the 1960s by aerospace industry, is a systematic methodology designed to identify known and potential failure modes, their causes and effects on system performance [34] and [13].

In other words, FMEA is a proactive procedure for evaluating a process by identifying where and how it might fail and assessing the relative impact of different failures [12].

This methodology allows the identification of parts of the process that are most in need of repair and maintenance so that it is possible to carry out corrective actions for the most serious issues to enhance the reliability and safety of the analyzed system. FMEA aims to mitigate risk of a failure mode through a recommended action, without necessary elaborating a maintenance task. FMEA can be performed in the design phase of a project, in the hope of assessing risks and improving the reliability of the asset by optimizing the design of the system.

FMEA assigns a numerical value, in a qualitative way, to each risk associated with a causing failure, taking into account the risk factors for occurrence (OCC), severity (SEV) and detection (DET), and subsequently prioritizes the actions needed to counteract or avoid these failures. The line-up of failure modes in FMEA is determined by a risk priority number (RPN), made by the arithmetic product of the previous risk factors, as expressed in (1):

$$RPN = OCC \times SEV \times DET. \tag{1}$$

The higher the RPN of a failure mode, the greater the risk is for the system reliability. Proper actions should be preferentially taken on the high-risk failure modes so that the system should increase its performance.

In order to carry out an FMEA effectively, a systematic approach should be followed. The general procedure for conducting an FMEA is briefly explained in the following steps [34]:

- step 1: determine the scope of FMEA analysis in order to define boundaries approaches that are to be considered during the analysis;
- step 2: assemble the FMEA team in order to be cross-functional and multi-disciplined, forming a line-up of subject matter experts from a variety of disciplines with knowledge of the problem to be discussed;
- step 3: understand the problem to be analyzed by dividing the system into subsystems and/or assemblies and use schematics and flowcharts to identify components and relations among components;
- step 4: brainstorm failure modes that could affect the system quality and identify their causes and potential effects on the system;
- step 5: determine OCC, SEV and DET for failure modes and calculate their RPN;
- step 6: prioritize failure modes by ranking them in terms of the RPNs for preventive actions and recommend actions for the high-risk failure modes in order to eliminate them, increasing failure detectability and minimizing losses in the event a failure occurs;
- step 7: prepare FMEA report by summarizing the analysis results;
- step 8: calculate the revised RPNs as the failure modes are reduced or eliminated once the recommended actions have been taken to improve the system.

Some of the terms commonly used in FMEA are introduced below. The definitions of terms used herein are in accordance with the definitions used in [34]:

- **Function:** task that the system, process or component must perform.
- **Failure mode:** manner in which a failure occurs.
- **Failure cause:** cause or sequence causes that initiate a process that leads to a failure mode over a certain time.
- **Failure effect:** adverse consequence of a failure in terms of the operation, function or status on a system. It can be addressed from two points of view: the first one is local, in which the failure is isolated and does not affect anything else so that it is considered the impact on a system element under consideration; the second one is global, in which the entire system is considered for the effect analysis.
- **Occurrence:** frequency that a root cause is likely to occur.
- **Severity:** magnitude of the end effect of a system failure.
- **Detection:** likelihood of detecting a root cause before a failure can occur.
- **Recommended actions:** specific actions that can be implemented to reduce or eliminate the risk associated with a potential cause of each failure mode.

Ratings of OCC, SEV and DET are divided in a numerical representation, in a ranking system usually from 1 to 10, in order to represent the risk level of a given failure, according to the respective rating. The higher the risk level, the higher the rating. In this dissertation, ratings are classified according to [34].

C. Failure Rate

Failure rate, denoted by λ, is the frequency in which an engineering system or component fails, expressed in failures per unit of time. The failure rate of a system usually depends on time, with the rate varying over the life cycle of the asset. The failure rate λ is expressed as in equation 2, where Nf is the number of failures and Δt is the period of time:

$$\lambda = \frac{\text{Nf}}{\Delta t}. \tag{2}$$

Failure rate is often reported in Mean Time Between Failures (MTBF), whose value is denoted by equation 3, which is valid when the failure rate is assumed to be constant (see III-C1).

$$\lambda = \frac{1}{\text{MTBF}} \tag{3}$$

Sometimes, failure rate is indicated in annual failure rate (AFR) in order to illustrate the expected number of failures in one calendar year. This way, failure rate can be defined as in equation 4:

$$\lambda = \text{AFR}[\%] \times 100. \tag{4}$$

1) The Bathtub Curve: The bathtub curve is the most common term used in reliability engineering to describe a particular evolution of the failure rate of a engineering system or component over time. The term "bathtub" is used due to the shape of a bathtub form, which is a combination of a decreasing hazard of early failures, a constant hazard of random failures and an increasing hazard of wear-out failures. This way, this type of hazard function can be characterized by three distinct parts, as presented in Figure 3:

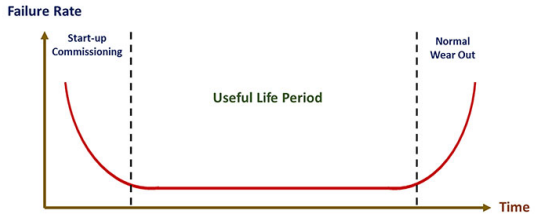

Fig. 3. The bathtub curve [35]

Note that equation 3 is only valid for the flat region of the bathtub curve (as explained in section III-C).

Power and cyber equipment are usually characterized by failure rates which behave in accordance with the bathtub curve.

For the purpose of this thesis, and bearing in mind the equipment which will be used in this dissertation for the FMEA analysis, future references of failure rate values will only refer to the useful life period of an equipment, thus when failure rate remains constant in time [36].

IV. FMEA Implementation

A case study is developed in order to demonstrate the application of FMEA in reliability analysis in a smart grid. The aim is to evaluate the impact in the reliability analysis by identifying the source of failure of each equipment.

A. Test System Description

Figure 4 presents the model of smart grid, where a 30kV simplified power distribution network is integrated with a communication-ring network topology.

Related to power test system, bus bars, cables (aerial lines), circuit breakers and transformers are considered for reliability analysis. Storage facility and generation stations were not regarded into this reliability analysis, since it was considered that their failures don't compromise system's operation.

The cyber-control network is a bus topology LAN-Ethernet and WAN-optical fiber network consisted of human-machine interfaces (HMIs), Ethernet switches (SWs), servers (SVs), energy boxes (EBs) – also designated as smart meters –, intelligent electronic devices (IEDs) and Ethernet and optical fiber links.

Failure rates for each component have been collected from different sources. Power and cyber components' reliability data can be found in Tables I and II.

Note that related to aerial cables, and for simplification purposes, it was defined different substations are equally distanced between each other – about 2,5km.

TABLE I
Power Equipment's Reliability Data

Equipment	Failure rate [(f/yr)/km]	Length [km]	Failure rate [f/yr]
Bus bar	-	-	0,01
Cable	0,054	2,5	0,135
Circuit Breaker	-	-	0,023
Transformer	-	-	0,01

TABLE II
Cyber-control Equipment's Reliability Data

Equipment	MTBF [h]	AFR [%]	Failure rate [f/yr]
IED	166.440	-	0,0526
SW	390.190	-	0,0225
SV	-	2,07	0,027
HMI	50.000	-	0,172
EB	-	0,5	0,005
Ethernet Link	-	-	$\leq$1E-6
Optical fiber Link	-	-	0,0044

IEDs, acting as interface devices between power and communication network, include measuring units, protective relays and controllers. Each IED is responsible for monitoring, controlling and optimizing the effective utilization of energy between generation and load. It also applies the commands received from HMIs.

Cyber-power links between individual IED controllers and their corresponding power elements are given in table III.

TABLE III
Cyber-power links between power and cyber network

Link	equipment
1	IED1:B1, IED1:CB2, IED1:CB3
2	IED2:B2, IED2:CB5, IED2:CB6
3	IED3:B3, IED3:CB8, IED3:CB9
4	IED4:B4, IED4:CB12, IED4:CB13
5	IED5:CG, IED5:CB1
6	IED6:WE, IED6:CB4
7	IED7:ES, IED7:CB11
8	IED8:PV, IED8:CB15

The application of the FMEA technique comprises the definition of failure modes that can be triggered in a given system, in order to evaluate their causes of failure and their impacts on the system. Failure rates of Tables I and II must be distributed accordingly to each failure mode and each failure cause.

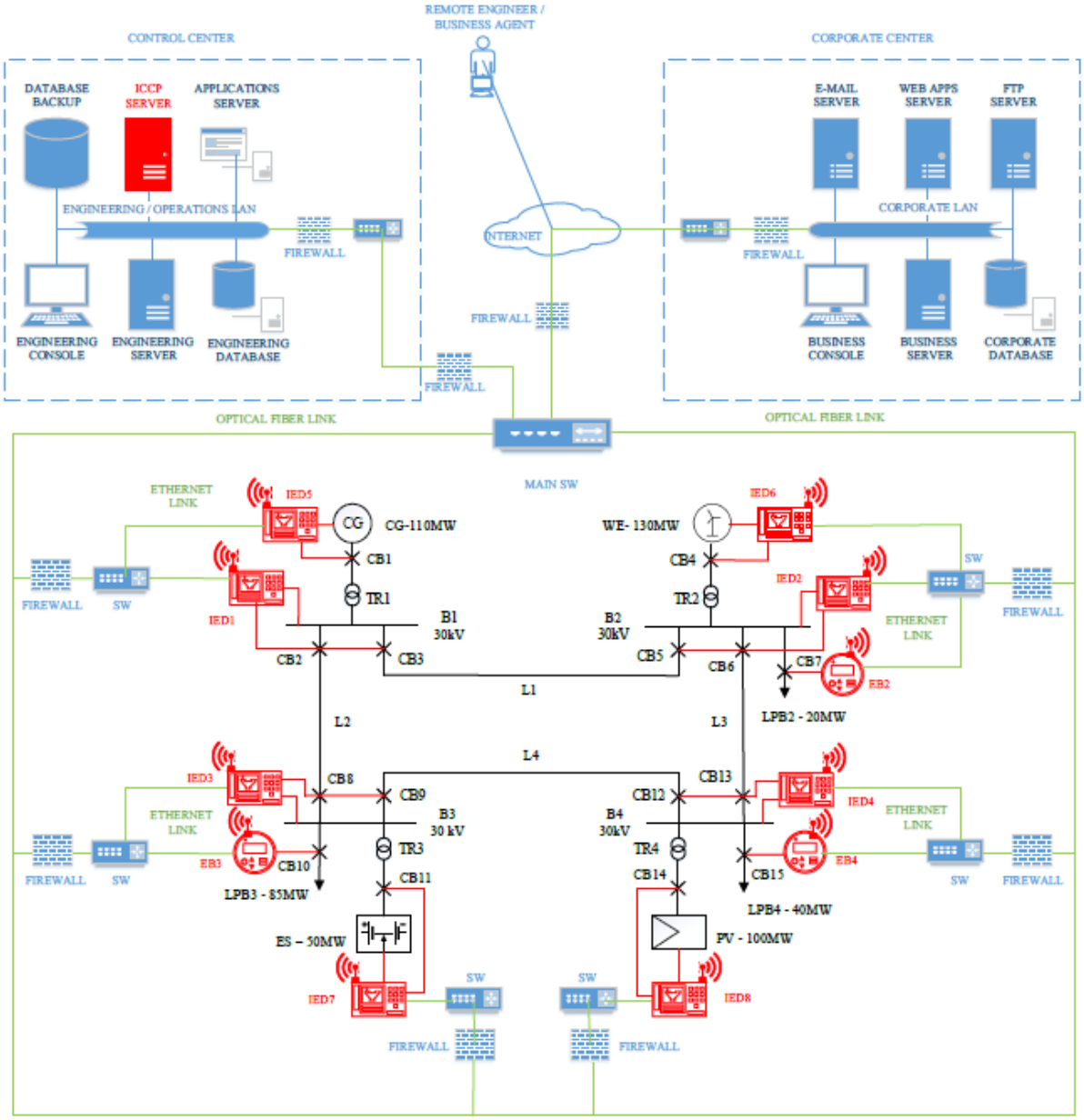

Fig. 4. Cyber-Power network test system

Then, an analysis of predictable impacts on the system as an effect of identified failure causes is evaluated.

Failure consequences are measured in: a local perspective, where the impact of a failure is locally evaluated considering the impact on the system element under consideration; in a system's perspective, where the implications of given failures are globally inspected at the entire system.

In order to evaluate the likelihood of detecting a root cause, detection methods are enumerated for each specific cause of failure.

In order to evaluate risk analysis in the presented study, RPN for each failure cause is calculated. As a result, final RPN for failure modes corresponds to the highest RPN obtained between its respective failure causes.

V. Results

A. Risk analysis

The final FMEA analysis is presented in Table IVin which are highlighted the fifteen failure modes with the highest RPN. Failure modes are prioritized according to their RPN value, and high-risk failure modes for the present case study are identified.

From Table IV, it is possible to conclude SVs and transformers are the equipment with the most critical failure modes, meaning that their respective high-risk causes of failure compromises the correct grid operation as pretended. Bus bars failure modes are also identified as critical, in the sense that their impact of failure in the grid is significant.

TABLE IV
FIFTEEN FAILURE MODES WITH THE HIGHEST RPN

Rank	Equipment	Failure Modes	Failure Causes	OCC	DET	SEV	RPN
1	SV	Hardware crash	Hard drive crash	6	10	8	480
2	Transformer	Transformer explosion	Internal short circuit	5	10	9	450
3	HMI	Operational failure	Human error	8	10	5	400
4	IED	Control failure	Defective data processing (software error)	7	7	8	392
5	Bus bar	Loss of structural integrity	Break of the support insulators	6	9	7	378
6	Cable	Electrical operation failure	Short circuits transients	6	10	6	360
7	SW	Operational failure (SW blackout)	SW is locked up	6	10	6	360
8	Bus bar	Loss of electrical continuity	Arc flash	4	10	8	320
9	Bus bar	Electrical disturbances	Short circuits between bus bars	4	10	8	320
10	Transformer	Distortion, loosening or displacement of the windings	Short circuits	5	9	7	315
11	CB	Bushing breakdown	External short circuit	5	10	6	300
12	SV	Data errors	Software malfunction	5	10	6	300
13	Transformer	Winding overheating	Overload	6	7	7	294
14	Cable	Cable integrity defect	Lightnings	7	5	8	280
15	CB	CB contacts degradation	Electrical treeing (partial discharges)	5	9	6	270

Related to cyber equipment, failure modes with the highest RPNs are those which express themselves as operational failures, verified in equipment like HMIs, SWs or IEDs. Concerning to power equipment, failure modes that tease unstable behaviors in system's power supply, possibly causing partial or total (less frequent) power outages in the grid, are also classified with high RPNs.

Table IV also indicates Ethernet links, optical fiber links and EBs as the less critical equipment.

In the domain of cyber equipment, failure modes concerning security reasons, despite the enormous impacts cyberattacks can cause in the system, are not considered as high-risk failure modes in the applied FMEA methodology. It can be explained due to low OCC ratings, in the sense that in spite of the expected increase of cyberattacks attempts in future years, they will not be necessarily successful.

In this turn, power outages in each cyber equipment's power supply are expected to be less frequent, thus expressing themselves also with lower RPNs.

In general, it is possible to infer a pattern in high-risk failures, which are mainly determined by high DET and SEV ratings.

In fact, besides all ratings are treated as equals, one can see OCC rating remains with low variations between different failure modes with high and low RPNs, not being a decisive rating with impact on high-risk failures.

In its turn, failure modes characterized by high levels of unpredictability are more likely to be more critical, since these modes of failure occurs without early warning and are difficult to prevent, while strong negative impacts on the smart grid operation have also a repercussion in high SEV ratings.

Finally, a conclusion regarding human interference in future smart grids must be pointed out. In fact, HMI's operational failure due to human error proves to have negative impacts on the grid. This human error is unintentional, and its high probability of occurrence and unpredictability (as seen in Table IV) makes it an high-risk failure cause.

This way, it is expected main weaknesses in future smart grids are related to some tasks that demand human interference.

B. Discussion

In order to obtain the final result of FMEA, one has to take into account important information is lost during FMEA procedure. This situation can compromise final conclusions concerning high-risk failure modes and their impact on the reliability of the system.

As a matter of fact, Table IV presents the final result of FMEA in the system, giving prioritization of the fifteen high-risk failure modes with their respective high-risk causes of failure. This means that, according to FMEA, maintenance strategies should be prioritized from the highest RPN to the lowest in order to increase smart grids reliability. This implies it will be the origin of the failure which will receive special attention in its maintenance tasks in order to decrease or eliminate its risk of failure in the system and to reduce failure mode impact on the system. This is established with the aim of decreasing the number of times in which the respective failure manifests itself so that system reliability increases as pretended.

However, this also means numerous failure causes are herein discriminated as long as high-risk causes of failure of each failure mode are not taken into account for final FMEA analysis. In fact, critical failure causes, sometimes with bigger RPN than certain failure causes and modes herein identified in Table IV, see their maintenance strategies being ignored.

In fact, critical failure causes, sometimes with bigger RPN than certain failure causes and modes, see their maintenance strategies being ignored.

Table V shows some failure modes with some high-risk failure causes that are not considered for final FMEA analysis.

From here, one can conclude that maintenance tasks are not efficiently applied in terms of risk decrease, therefore with implications in maintenance costs/risk-decrease ratio, bearing in mind the aim to execute a cost-effectiveness maintenance strategies.

TABLE V
HIGH-RISK FAILURE CAUSES

Equipment	Failure Mode(s)	Failure Cause(s)	OCC	DET	SEV	RPN
Bus bar	Loss of structural integrity	Fracture of the copper bar	5	9	7	315
		Break of the support insulators	6	9	7	378
		Cracking of connection welds	5	9	7	315
Bus bar	Electrical disturbances	Short circuits between bus bars	4	10	8	320
		Harmonics	4	8	8	256
SW	Operational failure (SW blackout)	SW is locked up	6	10	6	360
		Module failure	5	10	6	300
IED	Communication failure	Poor communication between IED and remaining cyber network	5	8	6	240
		Signal processing error (corrupted data)	4	8	6	192
		Network/Cyber storm	5	7	6	210

Besides that, FMEA methodology itself should be criticized for a wide variety of reasons.

In the first instance, the relative importance among OCC, SEV and DET is not taken into account. The three risk factors are treated as equals, with the same weight in RPN calculation, and this may not be the case when considering a practical application of FMEA in this dissertation.

As an illustration, as seen in Table IV, software errors in IEDs control applications have a larger negative impact in system performance (thus in terms of severity), when compared to unintentional human error in HMI operations (SEV rating is assigned with 8 and 5, respectively). However, one can see HMI operational failure due to human error is an higher-risk failure mode instead of IEDs control failure. The severity of the failure seems to be herein neglected.

Likewise, different combinations of OCC, SEV and DET may produce the same RPN rating, but their hidden risk implications may be different.

The mathematical form adopted for calculating RPN is also strongly sensitive to the variation of risk factor evaluations. Small variation in one rating may lead to vastly different effects on the RPN value.

This clearly shows FMEA is limited in the prioritization of maintenance tasks. FMEA is not able to assign different weights for its ratings, leading to some misreadings concerning the risk of a failure mode.

In the literature, it was verified the lack of failure rates information discriminated for each failure mode, either for power and cyber equipment. This hinders the viability of FMEA in the present system. In this dissertation, failure mode's rates where subjectively discriminated from equipment's failure rates, which may have led to some errors in RPN final calculation.

Therefore, for a deeper understanding on the criticality of a certain failure, the collection of data on the frequency of failure for each power and cyber equipment, by specifying failure rates for each failure mode and their causes, would be profitable for reliability purposes. Knowing the frequency of a certain failure, as long as bearing in mind the real impact that failure triggers in the smart grid, would make FMEA more efficient (more reliability of OCC rating) and maintenance strategies more precise (strategies based on maintenance frequency adjustments are improved).

Finally, in order to ensure system's high reliability level, a cost-effectiveness maintenance strategy must be achieve by prioritizing failure modes from the most critical to the lowest, as long as one has to take into consideration maintenance costs for each equipment and each failure mode.

VI. CONCLUSION

RPN calculation considers risk factors mainly in terms of criticality and other important risk factors such as economical impacts are ignored. Besides that, criticality of a failure mode depends on its penetration level on the system, and the manner in which a failure occurs could be seen in different perspectives, depending on the complexity of the system and where and how it expresses itself.

In a nutshell, FMEA is very successful in assemble failure modes and their causes of a given smart system. However, for a better reliability assessment and risk analysis of a smart grid using FMEA, one needs to adopt possible adjustments in FMEA technique in order to improve risk prioritization so that maintenance strategies can be efficiently applied.

REFERENCES

[1] J. A. Peças Lopes, N. Hatziargyriou, J. Mutale, P. Djapic, and N. Jenkins. Integrating Distributed Generation into Electric Power Systems: A Review of Drivers, Challenges and Opportunities. *Electric Power Systems Research*, 77(9):1189–1203, July 2007.

[2] S. Bilgen. Structure and Environmental Impact of Global Energy Consumption. *Renewable and Sustainable Energy Reviews*, 38:890–902, October 2014.

[3] Khosrow Moslehi and Ranjit Kumar. A Reliability Perspective of the Smart Grid. *IEEE Transactions on Smart Grid*, 1(1):57–64, June 2010.

[4] E. Santacana, G. Rackliffe, L. Tang, and X. Feng. Getting Smart. *IEEE Power & Energy Magazine*, 8(2):41–48, March 2010.

[5] A. Ozdemir and E. D. Kuldasli. RCM Application for Turkish National Power Transmission System. In *2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems*, Singapure, Singapure, July 2010. IEEE.

[6] I. P. de Siqueira. Measuring the Impacts of an RCM Program on Power System Performance. In *IEEE Power Engineering Society General Meeting*, San Francisco, CA, USA, June 2005. IEEE.

[7] L. Pottonen and F. Oyj. A Method for Analysing the Effect of Substation Failures on Power System Reliability. In *Proc. 15th Power Syst. Comput. Conf*, Liege, Belgium, August 2005. IEEE.

[8] Dabo Zhang, Wenyuan Li, and Xiaofu Xiong. Overhead Line Preventive Maintenance Strategy Based on Condition Monitoring and System Reliability Assessment. *IEEE Transactions on Power Systems*, 29(4):1839–1846, July 2014.

[9] L. Andersson, K. P. Brand, C. Brummer, and W. Wimmer. Reliability Investigations for SA Communication Architectures based on IEC 61850. In *2005 IEEE Russia Power Tech*, St. Petersburg, Russia, June 2005. IEEE.

[10] Andrija Volkanovski, Marko Cepin, and Borut Mavko. Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering & System Safety*, 94(6):1116–1127, June 2009.

[11] Mohd Khairil Rahmat and Slobodan Jovanovic. Power Systems Reliability Estimation Method. In *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, Cambridge, UK, October 2015. IEEE.

[12] Mohsen Akbari, P. Khazaee, I. Sabetghadam, and P. Karimifard. Failure Modes and Effects Analysis (FMEA) for Power Transformers. In *28th Power System Conference*, 2013.

[13] A. Pourramazan, S. Saffari, and A. Barghandan. Study of Failure Mode and Effect Analysis (FMEA) on Capacitor Bank Used in Distribution Power Systems. *International Journal of Innovative R]esearch in Electrical, Electronics, Instrumentation and Control Engineering*, 5, February 2017.

[14] Mohd Ikhwan Muhammad Ridzuan, Ignacio Hernando-Gil, Sasa Djokic, Roberto Langella, and Alfredo Telsa. Incorporating regulator requirements in reliability analysis of smart grids. part 1: Input data and models and part 2: Scenarios and results. *IEEE PES Innovative Smart Grid Technologies, Europe*, February 2015.

[15] Ignacio Hernando-Gil, Irinel-Sorin Ilie, and Sasa Z. Djokic. Reliability performance of smart grids with demand-side management and distributed generation/storage technologies. In *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe*, Berlin, Germany, February 2012. IEEE.

[16] João Abel Peças Lopes, André Guimarães Madureira, and Carlos Coelho Leal Monteiro Moreira. A view of microgrids. *WIREs Energy Environ.*, 2(1):86–103, January 2013.

[17] K. C. Budka, J. G. Deshpande, and M. Thottan. *Communication Networks for Smart Grids*. Springer, 1st edition, 2014. ISBN 978-1-4471-6301-5.

[18] M. M. Farag, M. Azab, and B. Mokhtar. Cross-layer security framework for smart grid: Physical security layer. In *5th IEEE PES Innovative Smart Grid Technologies Europe*, Istanbul, Turkey, October 2016. IEEE.

[19] Haibo He and Jun Yan. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 1(1):13–27, 2016.

[20] Bamdad Falahati. *Reliability Assessment of Smart Grid Considering Cyber-Power Interdependencies*. PhD thesis, Faculty of Mississippi State University, August 2013.

[21] Bamdad Falahati and Eric Chua. Failure Modes in IEC 61850-Enabled Substation Automation Systems. In *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Dallas, TX, USA, May 2016. IEEE.

[22] S. Jaloudi, E. Ortjohann, A. Schmelter, P. Wirasanti, and D. Morton. General Communication Strategy for Control of Distributed Energy Resources in Smart Grids via International Standards. In *2011 16th International Conference on Intelligent System Applications to Power Systems*, Hersonissos, Greece, September 2011. IEEE.

[23] Danda B. Rawat and Chandra Bajracharya. Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives. In *Proceedings of the IEEE SoutheastCon 2015*, Fort Lauderdale, FL, USA, April 2015. IEEE.

[24] D. Markovic, I. Branovic, and R. Popovic. Smart Grid and Nanotechnologies: a Solution for Clean and Sustainable Energy. *Energy and Emission Control Technologies*, 3:1–13, January 2015.

[25] Bamdad Falahati, Yong Fu, and Lei Wu. Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies. *IEEE Transactions on Smart Grid*, 3(3):1515–1524, September 2012.

[26] M.A. Azarm, R. Bari, Y. Meng, and Z. Musicki. Electrical Substation Reliability Evaluation with Emphasis on Evolving Interdependence on Communication Infrastructure. In *2004 International Conference on Probabilistic Methods Applied to Power Systems*, Ames, IA, USA, September 2004. IEEE.

[27] Ricardo Siqueira de Carvalho and Salman Mohagheghi. Impact of Communication System on Smart Grid Reliability, Security and Operation. *Proc. IEEE North Amer. Power Symp.*, pages 1–6, 2016.

[28] Inovonics. Physical Security of the U.S. Electric Grid. Available at url: https://www.inovonics.com/wp-content/uploads/2017/12/Physical-Security-of-the-US-Electric-Grid.pdf, Accessed in 30/09/2018.

[29] ICS-CERT. Cyber-Attack Against Ukrainian Critical infrastructure. Available at url: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, Accessed in 30/09/2018.

[30] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rhode. Protecting Smart Grid Automation Systems Against Cyberattacks. *IEEE Transactions on Smart Grid*, 2(4):782–795, December 2011.

[31] Fadi Aloula, A. R. Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia, and Wassim El-Hajjb. Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*, 1(1), September 2012.

[32] Islam H. Afefy. Reliability-centered maintenance methodology and application: A case study. *Scientific Research Engineering*, pages 863–873, November 2010.

[33] The National Aeronautics and Space Administration. Reliability-Centered Maintenance Guide for Facilities and Collateral Equipment. Technical report, NASA, February 2008.

[34] Hu-Chen Liu. *FMEA Using Uncertainty Theories and MCDM Methods*. Springer, 1st edition, 2016. ISBN 978-981-10-1466-6.

[35] Pumps and Systems. The bathtub curve as applied to pumping systems. Available at url: https://www.pumpsandsystems.com/bathtub-curve-applied-pumping-systems, Accessed in 11/08/2018.

[36] Milena Krasich. How to estimate and use MTTF/MTBF would the real MTBF please stand up? In *2009 Annual Reliability and Maintainability Symposium*, Fort Worth, TX, USA, January 2009. IEEE.