American Journal of Information Science and Technology
2020; 4(1): 1-16
http://www.sciencepublishinggroup.com/j/ajist
doi: 10.11648/j.ajist.20200401.11
ISSN: 2640-057X (Print); ISSN: 2640-0588 (Online)

Micro Smart Micro-grid and Its Cyber Security Aspects in a Port Infrastructure

Monica Canepa[1, *], Giampaolo Frugone[2], Riccardo Bozzo[2, 3], Stefan Schauer[4]

[1]World Maritime University, Malmö, Sweden

[2]Electrical, Electronics and Telecommunication Engineering and Naval Architecture Department (DITEN), University of Genova, Genova, Italy

[3]Italian Centre of Excellence on Logistics, Transport and Infrastructures (CIELI), Genova, Italy

[4]Center for Digital Safety & Security Austrian Institute of Technology GmbH, Vienna, Austria

Email address:

moc@wmu.se (M. Canepa), frugone.xng@gmail.com (G. Frugone), Stefan.Schauer@ait.ac.at (S. Schauer)

[*]Corresponding author

To cite this article:

Monica Canepa, Giampaolo Frugone, Riccardo Bozzo, Stefan Schauer. Micro Smart Micro-grid and Its Cyber Security Aspects in a Port Infrastructure. *American Journal of Information Science and Technology*. Vol. 4, No. 1, 2020, pp. 1-16. doi: 10.11648/j.ajist.20200401.11

Received: October 16, 2019; **Accepted**: February 21, 2020; **Published**: March 24, 2020

Abstract: Maritime ports are intensive energy areas with a plenty of electrical systems that require an average power of many tens of megawatts (MW). Competitiveness, profits, reduction of pollution, reliability of operations, carbon emission trading are important energy related considerations for any port authority. Current technology allows the deployment of a local micro-grid of the size of tenths of MW, capable of islanded operation in case of emergency and to grant an increasing energy independency. Ownership of the grid permits a large flexibility on prices of energy sold inside the port, trading on local electric market and reduction of pollution. Renewable energy generation has a large impact on costs since features a low marginal cost. Unfortunately the smart grid is a critical asset within the port infrastructure and its intelligence is a high-level target for cyber-attacks. Such attacks are often based on malicious software (malware), which makes use of a controlling entity on the network to coordinate and propagate. In this document, we will outline some features of a port smart grid and typical characteristics of cyber-attacks including potential ways to recognize it and suggestion for effective countermeasures.

Keywords: Smart Grid, Ports, Energy Efficiency, Cyber-attacks

1. Introduction

The purpose of this paper is twofold; on one side it highlights advantages of upgrading or deploying a smart micro smart grid in a port and on the other side the importance of a proper extension of cybersecurity concepts to the operation of the port smart micro grid. Being smart micro-grids heavily dependent on a distributed intelligence, they are exposes to a number of possible targeted attacks. Port operators, ships, and port infrastructure target of an attack may be the vehicle to propagate these attacks to other organizations. Furthermore extensive communication capabilities may increase vulnerabilities.

Energy in a port is distributed through a local electrical grid connected to an external utility via a point of connection and often to internal more and more renewable generation. Upgrading to a smart microgrid instead of using a dumb micro-grid offers advantages in terms flexibility of utilization, dependability, possible revenues coming from services paid from its internal users, savings deriving from better contracts that can be stipulated with the utility, returns from trading of services.

A smart micro-grid is commanded and controlled by a relatively small SCADA and DMS (Distribution Management System). This small SCADA plays a very critical role in operations of the smart microgrid and due to its pervasiveness, richness in communications, smartness available at all levels, connection to non-secure subsystems and organizations is vulnerable to attacks.

A smart microgrid properly sized, configured and used means efficient and cost effective internal generation and utilization of energy, i.e. important issues for port authorities

and port operators due to impacts on operational cost, business continuity, compliance to emission regulations, satisfaction for operators and in last instance its competiveness [1].

Distributed intelligence, adaptive protection and control, strong user involvement, load and generation programmability and effective management of electric fleets are sources of effective benefits to stakeholders and users [2].

The resiliency of the microgrid is of utmost importance due to the reliance of port infrastructure on continuity and quality of its operations. Resiliency "is the ability to bounce back, to mitigate the effects of an attack, or recover quickly after getting a hit" [3].

The cyber security issues of smart grid infrastructures have been addressed by several research papers in order to improve the cyber security of the smart grid by using different methodologies and techniques.

Rawat et al. [4] they explored the challenges for the smart grid security, classifying the attacks based on the type of network: home network (HAN), neighborhood area network (NAN) and wide area network (WAN). Starting from the fact that information security is based on three known principles such as confidentiality, integrity and availability (CIA) have shown the impacts deriving from attacks on information security.

Shapsough et al. [5] presenting some security challenges in the smart grid system and possible solutions, recommends a new security conceptual model based on the Internet of Things paradigm. Development of standards, conceptual models is crucial to increase a secure design of a micro smart grid.

Another study, conducted by Liu et al. [6] pointed out the importance of the identification of the relevant IT security and privacy problems in order to create a reliable intelligent grid. With reference to IT security problems, especially in relation to privacy problems, the differences between IT networks and networks of networks were highlighted. intelligent.

Wang et al. [7] have developed a study on IT security on surveys and challenges in the smart grid, which shows that due to the complexity of the network architecture, the delay limits on different time scales, the scalability and the diversified capacity of the built-in devices, the most viable solutions are those on a large scale shaped on the needs for different network applications.

Bedi et al. [8] with a Review of internet of things (IoT) in electric power and energy systems, have analyzed the use of IoT technologies in electricity and energy systems. It highlights how the effective use of IoT technologies can represent an opportunity for a rapid development in smart grid applications but with some challenges represented by aspects related to communication Digitization brings significant benefits but a safe use of IoT technologies in smart grid applications is necessary.

Kimany et al. [9] analyze Cyber-security issues capturing the development of IoT-based smart grid, highlighting how the use of IoT-based technologies in smart grid applications represents one of the biggest challenges in terms of IT security, in the development of this system.

Eder et al. [10] in order to predict future types of malware, it develops a cyber attack model for detecting malware-based communications derived from existing technologies.

With reference to electrical networks, given that existing malware attacks can have significantly destructive impacts, it is important to provide adequate description of the generic phases of cyber attacks carried out by means of malware.

Thanks to the generic life cycle model that formalizes the phases of malware-based cyber attacks, you can be able to analyze existing malware by fragmenting it into recurring cycles, thus allowing a detailed comparison of the characteristics of existing malware and constituting a finalized basis to predict future developments.

Therefore the impact of cyber-attacks on power systems has been a primary issue of research in recent years [11]. Smart grids depend significantly on data transfers, with higher quality of service (QoS),]. Due to their highly integrated nature, smart grids are also more vulnerable to cyber threats and attacks.

Most of the existing research has explored either cyber system or power system vulnerabilities, but not both in a comprehensive and truly integrated manner. Sridhar et al [12] presented the impact of data integrity attacks on voltage control loop. The impact of cyber-attacks on transient stability of smart grids with voltage support devices is analyzed by Chen et al. [13]. A framework that models a class of cyber-physical switching vulnerabilities in smart grid systems is found in Liu et al. [14].

2. Port Organization

Two key figures are present in a port: the port authority and port operators. Operators are entity/organization working in a port that use and/or generate energy, own infrastructures, plants and buildings and provide services to their customers. The port authority, within its institutional role, can decide to operate as an energy aggregator of internal energy resources, establishing a virtual power plant, scheduling operations according to optimality criteria agreed with operators and stakeholders. As an aggregator it can trade energy and capacity services and respond to signals (generally prices) coming from the external utility.

Of course port operators and port authorities look for profits [15] and competitiveness, from different point of view. Most of them have a growing focus on reduction of emissions, energy efficiency and energy saving,

According to Theodoropoulos [16], Energy efficiency and reduction of emissions is achieved by:

a. Effective use of energy mix of internal traditional and renewables generation.
b. Adjusting demand and generation of energy by flexible management, instantaneous load shedding or curtailment and intelligent utilization of battery storage.
c. Maximum priority given to renewable energy as primary resource.

d. Constantly moving generation and utilization of equipment to the their respective high efficient operating points.
e. Having operators with greater awareness on micro-grid status and current/forecasted prices in order to permit to them the correct planning of their own technical and economic operations.
f. Maximize the use of electric transportation within the port area.

3. Smart Micro Grid and Vulnerability

A smart micro-grids is characterized by a set of distinctive aspects (small geographical distribution, distributed presence of intelligence, smart sub-systems, extensive interaction between logical and physical level, strong requirements on service continuity, resilience, extensive use of INTERNET communication services [17], access by many users and organization) that make traditional mechanism for ICT defense techniques weaker or some time ineffective.

The weakness towards potential cyber-attacks increases in proportion to the growth of the complexity of microgrid control [18, 19] is amplified by:

a. Increasing interconnections with public networks, end users and IT organizations.
b. Extensive use of INTERNET based communication among all customers of the microgrid.
c. Increasing adoption of COTS (Commercial Off-the-Shelf products in control) such as operating systems, DBMS, application software, etc.
d. Introduction of new technological paradigms of the ICT sector (e.g. virtualized systems, clouds).
e. Big growth of data volume coming from non-homogeneous and non-secure sources.
f. Smart metering (Automatic metering infrastructure).
g. Technological evolution that is introducing new security related vulnerabilities and criticalities.

Security context finds an additional interpretation in the analysis of the level of danger of potential attackers and their motivations, objectives and technical capabilities.

Preventing malicious events arising from well-organized attackers with strong financial resources, technical skills and the availability of state-of-the-art technological tools is a critical issue in a port and maritime organization.

Operators and stakeholders need to identify their specific threats and estimate their risks, to protect their business assets, minimize costs in case of failures and recover as quickly as possible. Taking into account that the infrastructure of the electrical micro-grid generates a high dependence of almost all the infrastructures and vital functions of the port on it, it is evident the disastrous impact that might have for a port a cyber-attack aimed at forcing these infrastructures out of service.

Beyond traditional attacks and exploitation of "zero-day" vulnerabilities that bypass signature-based attack detection systems, an attacker could design malicious activities based on the contemporary perturbation of information coming from the SCADA and physical equipment, what would trigger of actions that could cause unexpected behavior of the micro-grid.

This situation greatly complicates the micro-grid security monitoring practices and the degree of applicability of the technologies available today in ICT field.

The combination of relevant factors, such as the logical-physical nature of the infrastructure, the need to guarantee a high level of continuity of service and the threat of technically competent and well-organized attackers, makes apparent the need of sophisticated counter-measures for attack prevention, identification and quick response.

Operations such as:

a. acquisition of feedback regarding the level of security of the physical infrastructure.
b. correlation of information coming from the ICT security domain, physical security and SCADA (Supervisory Control and Data Acquisition).
c. minimization of reaction and recovery times are very critical in relation to security.

Analysis and design support in relation to vulnerability is based on cyber security testbed platforms. It permits to investigate security issues and countermeasures. Different network attack scenarios can be simulated. Most of the testbeds consider security and privacy as a priority [20]. Typical attack scenarios [21] are:

a. Unauthorized access to a PLC, RTU, PMU, IED device;
b. Blocking field sensors from reporting false data or events;
c. Spoofing;
d. Message relay;
e. Request tampering;
f. Injection of malicious function;
g. Denial of service (DoS) attack.

It is a good practice to have all micro-grid customers and micro-grid owners equipped with their own cyber protections at hardware and software level including communication and training of operators or concerned people (awareness).

According to Larkin M [22], game theory is a good reply to issues posed by cyber security; in particular three points are to be examined:

Point 1.

Methods to evaluate resiliency of a cyber system employing game theory and stochastic modeling.

Point 2.

Given the current state the grid and potential actions of an attacker, how is it possible to evaluate the likelihood of success or failure of defensive countermeasures?

Point 3.

Validate methods to perform a cost analysis to decide about upgrade or replacement of cyber defense hardware and software taking into account the effects on the system.

4. Why a Smart Micro-grid

A micro-grid is not a new concept since many large industrial areas and many ports are using an internal electrical

grid connected to an external utility and partially powered by internal generation. The micro-smart grid add pervasive intelligence, smart devices and an ubiquitous communication system [23] to an otherwise traditional micro-grid.

The U.S. Department of Energy (DOE) defines a micro grid as: "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 to and disconnect from the grid to enable it to operate in both grid-connected or island-mode [24].

As indicated in the White paper developed by Muni-Fed – Antea Group Energy Partners, LLC [25], smart micro-grids are also designed to allow delivering of excess energy into the incumbent utility grid as well as to import energy from the utility grid. A smart micro-grid is a small-scale version of the traditional utility grid designed to optimize energy services through its extensive use of decentralized flexible, user oriented control.

Irrespective of the level of its smartness, a micro-grid consists of two major parts:

a. The electrical infrastructure, i.e. the smart assets that generate, deliver, transform and use energy.
b. Communication and control systems, i.e., bidirectional communication and control system that operates the whole electrical smart micro-grid.

The most of ports are still using "dumb" micro-grids operating at significant marginal cost, rigidity of operations and a level of reliability and resiliency that would be helpful to be improved.

A traditional dumb micro-grid shows a number of shortcomings, like:

a. Difficulty to fully exploit the potential of internal generation resources, often random and not dispatchable (frequently renewables such that large arrays of PV modules, biogas fired turbines, wind turbines, storage batteries, etc.) and transform them into an opportunity by remunerate stakeholders without tantalizing micro-grid performance and violating contractual terms with any part connected to the microgrid;
b. Difficulty to meet price expectations from operators by establishing a customizable and flexible tariff policy that fits well with their operational needs. And;
c. Limited possibility to provide support to requests coming from external supplier and achieve revenues by contractualizing this support;
d. Inadequate capability to trade services, actuate policies such as "Demand Response" (DR) and exploit "Time of Usage Tariff" (TOU);
e. Less reliability and resilience compared to a smart micro-grid.

A smart micro-grid is able to work out these shortcomings [26] and therefore is a sensible solution to help a port to increase its operational capabilities, its efficiency and eventually competitiveness.

Revenues and savings generated by a smart micro grid compensate some or all of the capital and operating costs incurred by port authority to upgrade to a smart micro-grid and to operate it.

5. Enabling Objectives

Economic and technical objectives are enabling factors that justify deployment of a smart micro-grid.

a. Economic objectives include cost reductions and streaming revenues coming from grid mode of operations like arbitrage/trading, reduction of cost of procurement of energy by virtue of flexible procurement (for base and time varying supply) contracts that may be stipulated, minimization of risks to incur into penalties due to non-compliance with contractual terms (peaks, valleys, supply of services, emissions, etc.), opportunity get rewards by responding positively to signal coming from the supplying utility.
b. Technical objectives include the deployment of a stable, resilient, cyber-secure and reliable smart micro-grid capable of delivering high quality energy at the best prices to its users considering to their past, present and forecasted behavior.

These objectives [26] translate themselves into specifications that highlight characteristics that are required or desirable:

a. Control of the micro-grid available at different layers of a hierarchy. It permits to pursue the individual optimization objectives of single users within the general optimization scheme of the smart microgrid.
b. Capability of "off the grid" operations when necessitated by external adverse electrical conditions.
c. Face the stochastic nature of renewable PV and Wind generation.
d. Increase reliability, availability and resiliency through coordinates operation of reconfiguration after an evaluation of possible alternatives and associated technical costs.
e. Mitigate the consequences of energy fluctuations through dispatching energy storage, controlling of switchable loads, changing of import of energy, re-dispatching of activities.
f. Operate the smart micro-grid (i.e. its generation, storage, loads import/export) to ensure continuous quality delivery of energy Reduce or shift peak load exposed to the external utility on the basis of contractual conditions.
g. Enable Vehicle to Grid (V2G) and Vehicle to Building (V2B) operations for port fleet of electrical vehicles.
h. Enable organization and sound utilization of a Virtual Power Plant (VPP) based on the available generation sources.

6. Design of Smart Micro-grid

Successful deployment of a smart microgrid (or upgrading from an existing micro-grid) requires a proper design in rode

to achieve technical and economic results. Design of micro-grid [16] starts from specifications that include size of initial load and generation, early economic investment, forecasted evolution and upgradability, mode of utilization of external energy supplies, expected operation schedules, stipulated contracts. Main points of specifications include:

a. Energy Security – Ability to improve power supply to critical facilities. Routing of available energy to predetermined critical facilities is computer controlled.
b. Energy Resiliency – Ability to provide power during utility grid outages and to recover more quickly if outages occur. "Resiliency" is the capability to operate through utility disturbances/disasters and or recover from them quickly.
c. Power Quality – Ability to mitigate the impact of power quality fluctuations including harmonic content on the utility grid.
d. Reduced Electric Load On The Utility – use of micro-grid has an important role in reducing costs. For example, net-zero energy consumption could be achieved at the primary metering point due to optimized local energy production and consumption.
e. Energy Savings – Savings are achieved through control of loads and energy consumption. For example, the energy normally wasted during a large crane's braking operation could be captured and managed through regenerative breaking.
f. Lower Electricity Costs – Enables best use of controllable loads and distributed generation resources, including renewables.

Electrical design of electric micro-grid is carried out using network analysis packages such as loads and power flow, state estimation, stability and transient stability, voltage profiles, contingency analysis, etc.

Design study is performed under various scenarios including the worst conditions, operations and synchronization capability in "on" and "off" the grid mode.

Finally, risk analysis techniques like FMEA (Failure Mode and Effect Analysis) and FMECA (Failure Mode and Effect and Criticalities Analysis) are used either to complete the preliminary project or to permit an objective evaluation of the design. In this stage an exhaustive fault tree is established, it will be helpful to analyze alarms (root and trees) in phase of detection of a cyber-attack.

The smart micro-grid is generally designed to support a "plug in type" approach to allow an easy horizontal and vertical upgrade as well as a seamless addition and integration of new equipment or replacement of existing one with a minimum of reconfiguration of existing configuration and with the reduction of the risk of temporarily downgrading of the service.

On another side there are design criteria deriving from the need for high grid resilience to maintain active critical services during extended utility outages, maximize the potential utilization of renewables and reducing emissions.

Critical (that is "must serve"), no-critical loads and generating and storage farms are assigned to different feeders. Critical feeders are often powered by dedicated generators and backed by their own energy storage so that their required level of operability is always ensured.

For design purposes operators are categorized as active controllable or uncontrollable being the difference represented by the level of dispatchability, capability and flexibility of their equipment to respond to exogenous requests to adjust load and/or generation profile and finally level of local intelligence.

Design adheres to a general organization of control that follows a hierarchical and decentralized scheme i.e.:

a. Any effort is done to allow each port operator to operate according to its own objective, preferences, schedule and policy. Available local controls are referred as *action space* of the controller.
b. Policy and objectives of the whole micro-grid are established at the highest level of the control hierarchy.
c. Coordination principles take into account the interaction among controllers (i.e. the fact they operate on their own horizon according to a specific policy without knowing operations of other controllers at the same level).

Finally from a cyber point of view the design of smart micro grid must depend also on communication and information infrastructures. Integration enhances capabilities and is useful of the most of grid operations, but on the other hand increases vulnerabilities. Therefore domain specific approaches and solutions are necessary [27]. It is important [11] to understand the complex relations between cyber and grid domains, and the possible impacts of cyber events on the smart micro grid.

7. Organization of Control

Two possible control modes are considered.

7.1. Centralized Control

Centralized control architecture implies that all tertiary control functions (forecasting, economic optimization, etc.) are located on a computer server at one site, preferably within the microgrid.

Remote monitoring and control from an off-site location can also be accommodated in this control scheme.

7.2. Distributed Control

A distributed control approach has no central controller. Instead, there are multiple distributed controllers located within the microgrid.

Each distributed controller operates locally and communicates with one another through a peer-to-peer communication and with the master hierarchically.

A port has a pyramidal structure centered on a authority and many underlying organizations and operators. For these reasons an adequate criteria is the selection of a decentralized hierarchical mode of control and structure.

Two types of controller are generally employed:

a. Master controller at the highest level of the hierarchy (let we say the port authority).
b. Local controllers at organization and user level. Each of them interacts directly with people and the local equipment.

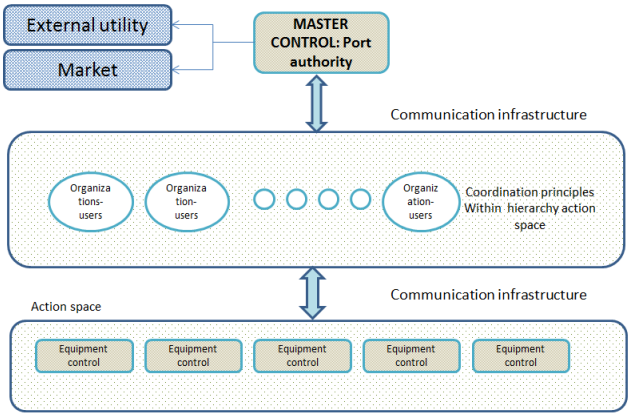

Figure 1. *General control organization.*

From a logical point of view it is used a set of agents (decision-makers, controllers, actors) and for each agent a preference ordering (utility function, performance criterion, pay-off function, reward function, etc.).

It is defined a set of permissible decisions (action space A_i and a probability φ on state space for the decision set) for each agent and a command information structure for the entire structure.

Each agent makes observation of the environment (state-of the world from its point of view) in which the agent is operating, and then performs a mapping from the state into the underlying structure,

Each agent has a description or model of the smart microgrid i.e., the way in which the known state and the combined actions of the agent will affect the operations.

Local controllers do not act passively on sole the basis of their data and policy instructions, but operate also on the basis of specific policy generated by the master controller constrained by coordination principles and within their action space A_i.

The master controller devises an optimal policy based on the knowledge of the general state and identifies the targets of each local controllers.

Any local controller looks to achieve its objectives in the best way but may be in conflict with the operations of other controllers and the general optimum computed by the master controller. In such a case an economic technique based on fees and rewards is used to work out the rising conflicting situation.

8. Strategies to Counteract Deviations from Expected Profiles

The master controller decides on the actions to take when significant events happen in the smart microgrid domain. The events that may require actions to bring the deviating user back to its reference are:

a. A significant deviation in the pattern of consumption/generation.
b. Deviations that may happen due to changes of the scheduled operations conditions respect to previously entered or forecasted.
c. The reception of request from external stakeholders (Utilities, retailers).

The decision on a policy change required to remediate the situations is decided by the master controller, it might decide on making a new plan by requesting the activation of a new short term planning or requesting the modification of operations of users.

Once the calculation of the new policy and associated plan is finished the low level controllers will be informed about the new consumption patterns to follow.

9. Forecasting of Consumption and of Generation

The importance of integrating a forecasting mechanism for energy consumption and generation depends on the possibility of devising proper strategies to operate efficiently in the energy market. The idea is to establish the basic energy behavior of users so that information on their attitude, flexibility, response to prices and other parameters can be instrumental to forecast their future behavior in order to make bids on dispatching services, capacity markets, reserve markets and to stipulate better economic conditions with the electrical utility at the time of negotiation of the contract. This forecasting mechanism relies on the knowledge of the past behavior of users, data about energy utilizations vs schedule of activities.

The basis of forecasting is a set of predictors used for the identification procedure; they are employed to elaborate the historical behavior of users as a function of the main variable of interest (i.e., the inputs of the identified model).

These variables of interest describe the scheduling of operations together with the "properties" of the day of the week (i.e., working day, holiday, day of week).

By elaborating this information, it is possible to develop a model able to provide a good dynamical description of the expected energy consumption/generation behavior of the grid and it can be used to predict the amount of energy that will be generated and-or utilized in a specified time interval (e.g., next day, week, next 2 weeks).

Since the identified model relies on past information it is possible to keep track and capture changes in the habits of the users. Clearly, several time-horizons (next week, next two weeks) can be used depending on the particular need. It is obvious that a very long term prediction (next month) will be inaccurate because the principal pattern inputs are not available. Instead it would be possible to have a very long term prediction using only the past outputs (time series), but this policy is usable only if the signals trends are regular.

10. Photovoltaic Energy Generation

Port generation is a mix of many assets like micro CHP (Combined heat plant), diesel gen set, gas turbines, off shore wind generation farms, but the really green generation is based on photovoltaic generation and in some case of wind farms (where possible and allowed). The photovoltaic generation depends on the day of the year, on geographical position and on the cloudy factor, a parameter that indicates the cloudy intensity in a determinate place in a determinate time.

Using the historical generation data, the historical day's number data, the historical month data and the historical cloudy factor data is possible to generate an identification and prediction model (ARX model) for the electrical energy generation.

The inputs of this model is the information about the months for next period, the numbers of the day for the next period (from 1 to 365) and the cloudy factors for the next period. The output is the predicted electrical energy generation.

Equally important is storage capability for its fast reacting capability to support the microgrid.

11. Micro-grid Resilience

Resilience is the ability to maintain acceptable electrical service levels notwithstanding severe disruptions to equipment, critical control processes, communications and the IT systems.

The distributed control of micro-grid aims to achieve resilience in terms of:

a. Minimization of the occurrence of outages.
b. Mitigation of any incidents.
c. Minimization of the impact of outages.
d. Reconfiguration.
e. Quick restoration of the normal working conditions of the grid.

12. Cyber-security Aspects of Smart Grids

Cyber information security plays a fundamental role in operation of smart micro-grids due to their strategic nature; smart micro grids represent the basis for the activities of the most port infrastructures. Cybersecurity is a major concern in the operations of a micro smart grid.

Because of this strategic role and the massive presence of intelligent components, cyber-security policy for smart micro grid (which includes attack prevention, detection, target deception, mitigation and resilience) represents a big challenge. To study effect of attacks, weakness and possible countermeasures it is useful to define models that are important to quantify potential consequences of a cyber-attack in terms of dangerous orders, misconfigurations, stability violations, and damage to equipment and economic losses.

According to a joint study by Iowa State University and the University of Illinois at Urbana-Champaign, after completion of an appropriate risk assessment, a key design step is the development of an integrated set of security algorithms to protect the network from multiple forms of cyber-attacks, such as denial of service attacks, malware-based attacks, etc.

Such algorithms take into consideration very sophisticated attacking modeled that potentially might cause a maximum level of damage. Algorithms to mitigate the risk of an ICT attack needs to be developed through real-time correlation of the data streams obtained from substations and control centers, these algorithms are designed to prevent, detect and mitigate cyber-attacks.

Mechanisms that correlate multiple, advanced detection techniques are useful to manage cyber threats and process risks.

Within available and developing techniques the ones identified as "Run-time security monitoring" [28] are a good starting point, they include:

a. Definition and support of metrics to measure the distance deviation of the current state / behavior of the grid from those defined by the security policy.
b. Verification of compliance with behavior-based security policies (dynamic evolution) and not only on the state of the grid.
c. Extension to probabilistic / stochastic models to support run-time risk assessment, manage countermeasures according to appropriate priorities and reduce the risk of late responses. The goal is to identify optimal protection in a set of predefined scenarios, without making any assumptions about the current situation or the attack strategy.
d. Assessment of the worst case scenario to be faced.

Finally it is worth to note that protocols used in the SCADA, such as the inter-Control Center Communications Protocol ICCP also known as International Electro-technical Commission (IEC)/60870-6/Telecontrol Application Service Element 2 (TASE.2), IEC 61850, Distributed Network Protocol (DNP3) (derived by GE-Harris from IEC 60870-5), if not properly protected, may be used as carriers to launch cyber-attacks. Secure versions of these protocols and continuous surveillance of information networks are required.

12.1. Cyber - Attacks to Smart Grids

The infrastructure of the electricity sector generate a high dependence of almost all the other critical infrastructures and of vital functions, it is evident the dangerous impact that a cyber-attack might have by forcing these infrastructures to be non-operational or even not available.

Escalation of cyber-attacks against industrial control systems has been reported. These attacks are targeted toward systems and apparatuses responsible for monitoring and controlling critical infrastructures (for example equipment for the production and distribution of electricity) [29]. These

systems are characterized by peculiar aspects (geographical distribution, unmanned sub-systems, strong interaction between logical level and physical level, strong requirements on service continuity) that make traditional defense techniques weaker or ineffective.

The sensitivity towards potential cyber-attacks on the infrastructures, in addition to increasing in proportion to the growth of the complexity of these systems, is amplified, as already noted, by increasing interconnection, growing use of COTS and increasing use of new technological paradigms in the ICT sector (virtualized systems).

It is a fact that any new technological development introduces secu interconnection rity vulnerabilities and criticalities and needs accurate compatibility checks with the requisites typical of the management of critical infrastructures such as: high performance, ease of, redundancies, responses in the time required by process dynamics and high level of reliability (continuity of the electricity service).

The security context finds a further dimension of interpretation in the analysis of the level of danger of potential attackers and of the related motivations, objectives and technical capabilities. The need to prevent events deriving from well-organized attackers, often with strong financial capabilities, technical skills and the availability of state of the art technological tools is widely shared. These attackers often have the possibility of using "zero-day" vulnerabilities, bypassing the detection systems of attacks based on "signature" and most of the current Prevention solutions / Detection of attacks.

The perception of risk of the concerned parties and stakeholders of critical infrastructures has grown to such an extent that is widely recognized that the adoption of industrial control solutions cannot be separated from an assessment of defense capabilities against cyber-attacks [1].

In this context, characterized by the combination of relevant factors, such as the logical-physical nature of the infrastructure, the need to guarantee a high level of service continuity and the threat of technically competent and well-organized attackers the prevention needs to be addressed by multiple concurring techniques. Among them:

a. The collection of feedback regarding the security level of the physical infrastructure.
b. The correlation of information coming from the domain of ICT security, physical security and process logic.
c. The security of technologies installed in unmanned environments due to peculiar distribution of the infrastructures.
d. Very short reaction times required for reaction and implementation of countermeasures.

Game theory is becoming a promising solution for cyber security context. Attacks and countermeasures can be evaluated by assessing the strategies and payoffs for each side.

12.2. Vulnerability of Control Systems

As known basic building blocks of a micro-grid are:

a. Generation and storage,
b. Distribution,
c. Delivery and exchange of energy.

Each block includes sub-systems whose task is the control of specific machines/devices and operate using dedicated communication signals and protocols. Each control sub-system is subjected to specific vulnerabilities; they could constitute vectors of threats with a consequent potential impact on the operations of the whole supply system. Figure 2 shows a conceptual figure of a cyber-physical system.

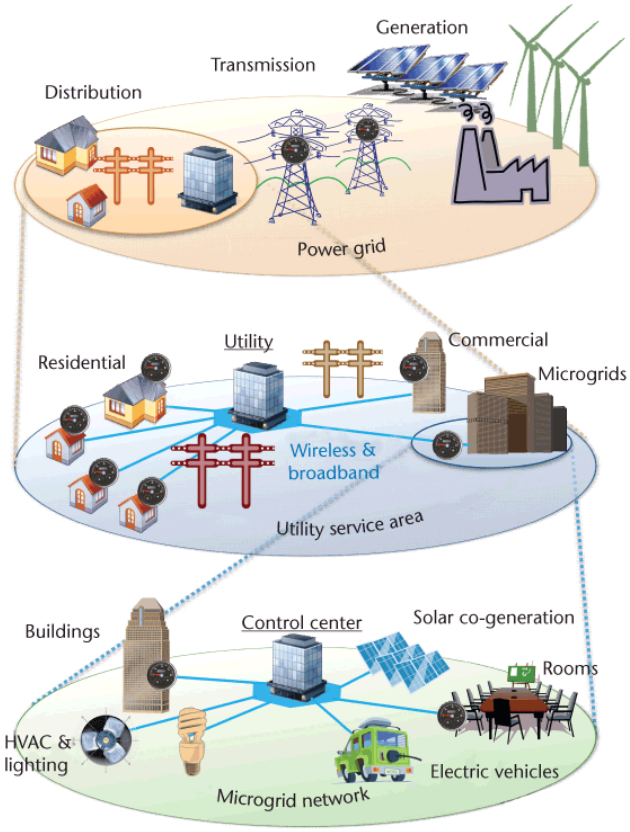

Figure 2. *Grid structure, Simmhan et al. (2013).*

12.3. Game Theory Support

Game theory provides a mathematical model of the interactions between players and has gained increased prevalence due to its logical applicability to a vast range of topics as well as gaining additional traction in cyber security research [30, 31].

As pointed out in the already quoted paper [22], game theory provides an interesting potential solution for cyber security issues and allows evaluating effects of the actions between attackers and defenders in cyberspace by assessing the strategies and payoffs for each side. Often it is assumed that there exist perfect information and the attacker and the defender have complete knowledge of the strategies and capabilities of the opposing player.

It is an approach that contributes to a simplification of the problem and allows for a more tractable solution, but it may be not realistic in application to real-world scenarios. In fact

while each side may know their respective capabilities, intent, and strategies, there is a degree of uncertainty about the attacker. Even if less mathematically tractable an approach based on imperfect game is more realistic.

12.4. Examples of Attacks

An attacker could design malicious activities based on the contemporary perturbation of both the control and physical systems, but it could also cause a coordinated series of commands and data that might cause an unexpected behavior of the infrastructure.

As another example [22] an attack may modify data collected from the grid or other devices and subsystems (an attack known as “false data injection”). This type of attack is difficult to identify, it is a situation where “bad data detection” algorithms may fail even in presence of redundant and correlated measurements and known probability distribution of measurement errors.

This situation greatly complicates the systems security monitoring and the applicability of the technologies that are currently available in this field, with the consequence of making more difficult to achieve an overall vision of the evolution of the security of the micro-grid and an understanding complete with all the events that are acquired.

13. Cybersecurity on Smart and Micro-grid

As observed in many ongoing projects, recommendations and standards, in particular in the United States by NIST (National Institute of Standards and Technology) and within the EU by ENISA (European Network and Information Security Agency) Cyber-security plays a very important role. Unfortunately there is currently no common approach and technology for applications in SCADA and EMS and this is even truer for the Smart Grids.

Therefore instead of investigating and proposing new technologies, we try to clarify the process of defining the appropriate and measurable requirements of cyber-security to define realistic, efficient and scalable solutions.

Today computer security is an essential block for the reliability of any control system and is to be considered from the beginning of any project and not as an additional final component, as it may happens. Having in mind cybersecurity it is reasonable to start analysing from the beginning the specific needs of microgrid and users / stakeholders and the interconnections of data exchange.

Cyber events [11] both intentional acts of sabotage and random hardware or software failures impact the proper operation of the wide-area closed-loop decision engine. These events are broadly categorized into four categories as follows:

a. Events that affect physical equipment;
b. Events that affect communication channels;
c. Events that affect applications;
d. Events that affect data.

Analysis of network traffic at connection points relevant to the distributed control system is a critical factor.

Protocols are exposed to attacks:

a. Lack of authentication.
b. Lack of encryption.
c. Backdoors.
d. Buffer overflow.
e. Tailored attacks for control physical components.

Current configurations range from easily configurable systems, which require traffic rules explicit to sophisticated self-learning machines that build data communication profile for each node of the control network profile can separate autonomously normal and abnormal traffic, after a period of unsupervised or supervised training.

A promising technology, i.e. "Defence in depth" is at the initial stage and it's more expensive than filtering traffic, but it increases security of the single control nodes, independently of interconnection topology.

Defence in depth is an approach to cybersecurity where a set of defensive mechanisms are layered on over the other in order to protect valuable data and information that are used by control applications. If one mechanism fails, another is immediately triggered to prevent an attack.

This approach may to become very valid, but in general it is justifiable only for new installations, while in other cases a mix between in-depth and more traditional filtering must be evaluated.

A good compromise for the choice has been proposed in the standard ANSI/ISA-99, based on security zones and connection gateways. The term "Zone" means a grouping of logical or physical assets that share common safety requirements, based on factors such as criticality or others. The gateway connects different zones, is able to resist Denial of Service (DoS) or the injection of malware via back doors and protects the integrity and privacy of traffic on the network. The techniques of encapsulating areas guarantee the protection of much more areas from public networks; the deeper the encapsulation of an area is, the greater is its security.

A sophisticated attacker can attempt to modify the behavior of a SCADA and PMU (phasor measurements units) and in particular to directly or indirectly influence the data (states, measures, alarms) and the commands (continuous and discrete) in such a way to mislead the supervision and control system, protection, dispatching and operators. This type of attack may trigger improper interventions that may be harmful to the integrity of the equipment and interfere with the continuity of the service.

An important type of attacks on the grid is represented by the "Intrusions": this type of attack refers to exploiting the vulnerabilities of software and communication along the network infrastructures that provide access to critical elements of the micro-grid and related control /data acquisition [33].

"Malware" instead consists of malicious software that aims to exploit the existing vulnerabilities in the software system, RTUs, programmable logical controllers, or protocols. Once

the malware has gained access, it tries to cause damage in the system using self-propagation mechanism.

The "Denial of service" attacks aim to make services or resources unavailable for an indefinite period of time, denying the possibility to legitimate users of access them. This type of attack can aim to submerge the communication network (or a single server) with high volumes of traffic or loads of work to inhibit the legitimate operation.

"Insider threats" are considered a serious danger, due to the privileged position that the potential attacker to operate from within the organization.

Finally, "Routing attacks", occur on internet routing infrastructures. Although this type of attack is not directly related to grid operations, it may have consequences on operations of software power applications.

13.1. Risk Assessment

A cyber security risk assessment consists of understanding, managing, controlling and mitigating cyber risk across an organization. It is a crucial part of any organization's risk management strategy and data protection efforts. (NIST) Indeed as a consequence of the diffusion of new technologies for the electricity distribution network, it is necessary to face new threats, vulnerabilities and security requirements; as consequence it emerges the need to carry out dedicated to risk analysis specific to the domain of intervention. Three questions are to be answered:

a. What is the threat?
b. How vulnerable is the system?
c. What is the reputational or financial damage if breached or made unavailable?

In the presentation of Tieghi [32] it is well explained that "assessing the consequences of industrial cyber-attack is not simply a case of assigning a financial value to an incident. Although there are obvious direct impacts which may be easily quantifiable financially other consequences may be less obvious. For most companies the impact on reputation is probably far more significant than merely the cost of a operation outage".

First intervention should be based on the study and application of risk assessment methodologies in the specific intervention scenario, being this activity ~~as~~ a necessary step for the definition of secure methods for infrastructure protection. An appropriate risk assessment methodology is essential to identify threats accurately and in all its aspects and to assess vulnerabilities even belonging to non-homogeneous technological categories.

13.2. List of Common Attacks

A basic list follows:

a. Spear-phishing emails (from compromised legitimate accounts),
b. Watering-hole domains,
c. ICS infrastructure targeting and credential gathering,
d. Host-based exploitation,
e. Industrial control,
f. Open-source reconnaissance,
g. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks,
h. Man-in-the-middle (MitM) attack,
i. Phishing and spear phishing attacks,
j. Drive-by attack,
k. Password attack,
l. SQL injection attack,
m. Cross-site scripting (XSS) attack,
n. Eavesdropping attack.

Assessment of the impact on the level of service is performed using risk management analysis taking into account the presence of peculiarities dependent on the use of the different technologies and the probability of the occurrence of these events.

13.3. Disruption Attacks

Attacks whose purpose is the overpressure of a service for a certain period of time, creating an unavailability of the same usefulness for the purposes of decision-making processes:

a. DDoS-attacks from outside targeting inside assets (Inbound attacks).
b. DDoS-attacks from inside targeting inside assets (Internal attacks).
c. DDoS-attacks from inside attacking targets outside (Outbound attacks).
d. DDoS-attacks on certain user groups (selective harassment).

13.4. Destruction Attacks

Unlike the disruption attacks that permit the service can be restored after the attack, in the case of destruction it is generally necessary to rebuilt the infrastructure: This type of attack is able to:

a. Disconnect households.
b. Destroy energy management system.
c. Influence critical electrical nodes in the grid.
d. Modify sensor data.
e. Tamper with clock synchro.

13.5. Theft of Information

Stealing a commodity such as information to reveal to competitors:

a. Espionage:
b. Ruin credibility of users:
c. Sell long term data:
d. Bill manipulation.

13.6. Extortion Schemes

This type of malware restricts access to the device it infects, requiring a ransom. It may include:

a. Commodity or service.
b. Threat of destruction.
c. Threat of DDoS.

d. Crypto-locker.

13.7. Repurpose Attacks

They include the capability to reuse a vulnerability stolen or known in some way. Or alternatively used leaked offensive tools originally developed by other organizations:

a. Fake servers.
b. Proxies.
c. Distributed computing.

REMARK: A potential very specific growing risk is the possibility that the supervision and control system (SCADA) of the micro-grid is deceived by false data coming from compromised peripheral units (RTUs, PLCs, Smart Inverters and other smart equipment) or through interconnections with other systems that are the object of successful attack. It is essential to install tools able to distinguish between "genuine" data, incorrect data, whose error depends on malfunctioning of the peripheral instrumentation or the RTU "and data whose origin is dubious (potentially affected by malicious attacks).

13.8. Consequence of Communications Failure

It has been noted in Guo et al. [34] that problems on transmission line monitoring function may not cause direct changes on the physical system topology. But if communications is subject to transmission line monitoring function suffers from random failures due for example to cyber part of the physical system is unobservable to the operators / applications and therefore no remedial action can be taken.

14. Countermeasures

Consistently with the priority requirement of continuity service typical of electrical grid and the need to safeguard the integrity of the equipment, a strong focus is required on the adoption of technological solutions aimed at prevention of intentional attacks and characterized by a low degree of invasiveness on equipment and the systems (Like SCADA, EMS, DMS, smart protection system, etc.).

In response to these threats it is convenient to implement protection techniques in IT platforms and perform analysis of the data acquired by the various subsystems or transferred by other organizations in order to distinguish between “genuine, inclusive of real incorrect data, but whose error depends on malfunctioning of peripheral equipment or RTU” and data whose origin is doubtful (potentially invalidated by malicious attacks).

The integration of different technological approaches, namely IT protection, recognition of intrusions, etc. and analysis of data / commands leads to a higher level of security of supervision and control systems. It is advisable to focus on methods for continuous monitoring of the security status of the infrastructure, through the acquisition, analysis and correlation of relevant data.

The most important intervention areas deal with the use of attack identification techniques based on the continuous analysis of security events, integrity of messages, states, alarms, measurements and commands coming / sent to the remote control systems (SCADA), from the metering systems, from ICT systems, various users, from any external communication networks that connect to other systems (Electrical Utility, ships, service centers, port organizations, shipping companies, etc.) and from the protection systems of physical "assets".

A coordinate use of these techniques allows to evaluate the overall behavior of the grid, highlighting:

a. The presence of attacks (discriminating from really wrong information).
b. Changes in the level of risk that must be faced.

14.1. Modeling and Configuring

Activities need to be carried out for the identification of models appropriate to detect attacks and activating countermeasures, especially considering the heterogeneous nature of grid infrastructure.

The widespread diffusion of solutions for the centralization and correlation of information security events is instrumental to extend the capacity of current products including physical security solutions, and the search for event correlation capabilities across the different technological and organizational levels of the micro- grid.

These attempts that are now limited by the capabilities of the current implementations generally characterized by a limited scalability, only basic correlation functionalities (e.g. the normalization of the events and the related aggregation by categories) and a weak support of automatic analysis of events. Furthermore, these technologies generally have a low level of integration at process level.

In this area of work is necessary to define a technical reference architecture, which leveraging Open Source modules or COTS products, will help to develop the necessary functionalities to build a complete awareness of the changing dynamics of grid safety.

It is useful to strengthen the current state of the art in security monitoring systems, focusing particularly on the definition of methods to identify the dependencies of the grid's operational process towards all the technologies served to it. In particular, ad hoc functionalities are to be developed for:

a. Acquisition, normalization and correlation of security events coming from remote control systems, from ICT systems, from physical security systems.
b. Determination of the stability of the operational processes by evaluating the data acquired by the remote control systems.
c. Continuous monitoring of all the parameters describing security status of logical, physical structures and the level of regularity and stability of the operational process, in order to correlate them for more advanced and reliable cognition capability.

14.2. Monitoring of the State of the Grid

It is possible to use different methods for monitoring the state of the grid. They are based mainly on the comparison between different data sources using a dynamic model of the system and in the analysis of grid data patterns together with their classification. This comparison and analysis is used to identify data that differ from their expected value given:

a. The current network status,
b. The historical series of data,
c. The expected evolution of the micro-grid (generally derived from the past history and current data plus work schedule).

Analytical tools such as Vector Support Machines (SVM), Outlier analysis (OA), Principal component analysis (PCA), Precursor analysis (PA), Fault Tree Analysis (FTA) and the like are of great help, especially if used in mutual support.

The probable conditions in the next period of observation, helps to avoid that an attacker can compromise vital information.

Indeed equipment malfunctions, errors due to improper or incorrect configurations are inevitable during the operation of the electrical grid and unfortunately these are situations that can easily mask the initial phases of an attack. Therefore it is mandatory to identify them through analysis based on rules and peculiar characteristics of the entire electrical system.

The verification of data in search of anomalies inconsistent with the expected state of the system requires the analysis of network behaviors, incorporating information from a wide variety of sensors of different types, of the grid protections and information coming from the PMUs, PLCs and RTUs.

An attack can occur simultaneously in separate sections of the micro grid so that it is necessary to use specific analysis methods to evaluate the data coming from these areas with a single model. The detection of cascading effects and their precise temporal sequence in coherence with the collected data is used for the recognition of a true attack from an authentic malfunction and alarm.

Three phases are sequenced:

a. Statistical analysis and classification of data (which will be subsequently used by the control and supervision system) with the aim of preliminarily identifying the data that does not belong to the set of expected data. This phase should make it possible to identify suspicious data, eliminate them and activate the appropriate countermeasures. During this phase the alarms and events are examined through the execution of an active fault tree to verify that these events and alarms are correctly set based on the preventive FMEA analysis.
b. Verification of the coherence of data during the processing phase through analytical and heuristic models.
c. Replacement of "suspicious" data with internally generated pseudo-data. These data allow the normal course of operations and are associated with a flag that identify them as replaced data.

14.3. Identify Attacks

A defense system must identify complex attacks, using analysis of events (or example via fault tree, simulation, normal grid status, etc.) and predicted status using historical series and the current status.

Apart from traditional methods, physical assessment of the status of micro-grid is employed making confrontation between normal status (based on current situation) and status deriving from validated data that characterizes the "normal state".

This process includes:

a. Real-time analysis of information and state estimation including methods to understand deviation from normal state (due to real malfunctions or compromised data).
b. Identification of techniques to be used for the identification of attacks.
c. Surveillance of communications to locate attacks
d. Recognition of anomalies inside the "big" data characterizing the grid (outlier detection, SVM, anomaly detection, etc.).

14.4. State Estimation

It has been suggested [22] to work out the problem of failing of bad data detection tests by employing a hierarchical distributed state estimation not only on the grid but also for associated communication infrastructure and subsystem. This "augmented" estimation makes use of as many redundant measurements as possible. The "augmented" state solution makes easier and more reliable the identification of suspicious data before they are actually used by an attacker.

The information from the hierarchical state estimation includes therefore the results of state estimation of subsystems (often the micro-grid customers) in order to verify that there is a substantial coincidence. If there is no coincidence an alarm is raised and the suspicious piece of data or item is excluded from subsequent computation steps. If the control center is under attack, local state estimations can be used for control and supervision purposes. Measurements on one section of the micro-is employed to verify the consistency of data coming from another section.

14.5. Analysis of Alarms and Events with Fault Tree

Sequences of alarms and events can be altered by malicious interventions and lead to untimely interventions if not even harmful to the equipment and to impair the continuity and quality of the service.

Therefore it is crucial to verify the validity of these sequences through appropriate methodologies. A promising development line is to verify whether an alarm defined as "significant" (within the rules and a special dictionary associated to each grid) is confirmed by a set of events and alarms that should be generated according to correct sequences and over a certain time span. The Active Fault Tree approach is suitable to this purpose. It is necessary to verify from time to time that:

a. When a main alarm event is present, also related alarms / events are existent in the correct time sequence.
b. In the presence of secondary alarms (whose sequence and time window is verified) the main alarm actually exists.

This tool operates using information collected and made available to the SCADA by field acquisition systems and subsequently integrated, allowing the detection of equipment malfunctions, the causes of failure and the components fault discriminating the real failures from those that are considered faulty due to non-genuine information.

Analysis is time based and therefore the sequence of events that determine the start of an analysis must belong to a specific time interval.

Specific tools are used to:

a. the formal definition of events and alarms.
b. the definition of the rules.
c. execution of the fault tree based on the rules.
d. presentation of the diagnosis.

This methodology is based on the "Executable Fault Tree" (EFT) structure that is a fault tree composed of the following elements:

a. "top event": final event produced by the analysis logic;
b. “intermediate events and conditions”: intermediate events / conditions generated by the execution of the related correlation logic and the logical operators;
c. "initiating events": events coming from the field and activating the correlation logic;
d. "gates": transformation operators (in the graph).

The Top Event of a Fault tree can be of two types: an event (typically an alarm) received from the field:

a. an event produced by the execution of the Fault Tree that is generated by specific processing.

In the first case the Fault Tree will deduce and verify the causes of the Top Event according to a TOP-DOWN approach: starting from the Top Event the conditions (Initiating Events) that should have triggered it will be verified. If the initiating events are not verified as correct or even existing it will be reasonable to assume that some information is not genuine.

In the second case, the Fault Tree is used to generate the TOP EVENT according to a bottom up approach: given the conditions (Initiating Events) the actual presence of the TOP Event is identified. If the processing does not lead to this event, again it could be in the presence of non-genuine data.

Through EFT it is possible to study how to formally model different scenarios / logics in a scalable manner depending on the characteristics of each grid. In particular, it is possible to model:

a. Combinatory Logics;
b. Relative Sequential Logics: i.e. the relative order of (expected) occurrence of events;
c. Absolute Sequential Logics: that is, items placed on a quantified time scale;
d. Mixed Logics: i.e. combination of the previous logics.

A Fault Tree (in particular an EFT that is "executable") is employed to model a behavior scenario identified by its Top Event, that is the root node of the fault tree and by the "Initiating Events", i.e. from the leaf nodes of the tree.

15. Statistical Analysis

15.1. Outlier

The validation / discrimination of data between genuine and non-genuine can be conducted through an analysis that identifies the presence of anomalous information (Outlier). The identification of outliers represents a crucial phase of the data verification process, as it can be considered that they represent an effective indication of anomalies or anomalous tendency on which to carry out further analyzes. Naturally it cannot be excluded that they represent a valid indication (due to the intrinsic variability of the investigated phenomenon; also in this case the identification of the outlier is important, at least from the electrical point of view).

Outliers can be univariate, that is, they have an extreme value for a single variable, or multivariate, so they present an anomalous combination of values on a certain number of variables. This means that a multivariate outlier will not necessarily present at least one extreme value on one of the variables, so all its scores could be perfectly admissible but they could represent an unlikely response pattern with respect to the rest of the subjects.

Multivariate outliers are specifically activated for:

a. Verify the conceptual validity of the use of the outliers for data validation and verification of their authenticity.
b. Identify the class of data with the best features in relation to their validation.
c. Select and possibly design methods for identifying multivariate outliers.

15.2. Principal Component Analysis (PCA)

The Principal Component analysis is often used as a data analysis tool and for the realization of predictive models. The PCA analysis is able to reveal the internal structure of the data in relation to their variance and allows obtaining a reduction in the complexity of the number of factors that explain a phenomenon.

The theoretical point of view the Principal component analysis (PCA) is a statistical procedure that uses an orthogonal transformation to convert a series of observations of potentially correlated variables into a set of values of linearly uncorrelated variables known as Principal Components where the number of main components is less than or equal to the number of original variables. This transformation is defined in such a way that the first main component has the largest possible variance (it is therefore characterized by the maximum possible variance), and each successive component has in turn the maximum possible variance under the constraint that is orthogonal to the previous components. The resulting vectors constitute an orthogonal set. The main components are orthogonal because they are the eigenvectors of the covariance matrix, which is symmetric.

Through the PCA it is possible to determine a certain number of "latent" variables (factors not directly measurable) that are more reduced and summarized with respect to the number of starting variables.

It is necessary to perform the validation of measurements and the possible identification of falsified data and therefore the search for a significant minimum set of latent variables weighted on the basis of their importance and characteristics of the system in question. In particular it is important to study the variance and its variation from the normally expected values. These variations take place in the case of modifications of a certain number of continuous variables and are traced to the latent variables whose number is lower and whose behavior can be analyzed more easily.

The criteria of discrimination is object of investigations linked to the way in which the falsified variables are reflected on the latent variables between variation of the variance due to real modifications of the measured data, compared to that obtained when some of these facts are modified by an intervention malevolent.

15.3. Anomaly Detection

The recognition of faults or anomalies is a fundamental activity in many situations, often linked to the problem of maintaining security within a grid. The concept of "anomaly" of for system derives from the definition of "normal" condition which represents the condition that the control seek to maintain in every area.

15.4. Support Vector Machine Prediction

The trend of variables and even better of a set of variables in a "normal grid" status can be predicted on the basis of the associated historical series, the better the greater the depth of the time series. The set or a subset of the variables can be classified as belonging to a normal or non-normal configuration. The methodology of Support Vector Machines (statistical supervised learning) is one of the methods that can be used effectively for classification and also for regressive analysis. Support vector machines (SVM) or kernel machines are a set of supervised learning methods for regression and pattern classification.

They belong to the family of generalized linear classifiers and are also known as maximum margin classifiers, since at the same time they minimize the empirical classification error and maximize the geometric margin. Support vector machines can be thought of as an alternative technique for learning classifiers, as opposed to classical neural network training techniques.

The SVM training technique solves both problems: it presents an efficient algorithm and is able to represent complex non-linear functions. The characteristic parameters of the network are obtained by solving a convex quadratic programming problem with equality or box constraints (in which the parameter value must be kept within an interval), which provides a single global minimum.

They are classification methods that guarantee a high accuracy of the prediction and do not require a large amount of data and are generally not affected by "overfitting".

The quality of the prediction (based on historical series containing both the trends of the manipulated variables and those that can be manipulated) makes it possible to evaluate the status of a variable following the previous measurements and the current acquisition cycle; if there was a significant deviation (that should be confirmed by the Anomaly detection analysis) an analysis will be performed to understand the reason for the deviation. Note that the cause and effect relationship is already implicit in time series and therefore it is not necessary to implement an analytical model.

16. Basic Solution Approach

The cyber-security solution for protection are divided into

a. Functional improvements of process,
b. Customized off-the-shelf solution, integrated into nodes (such as firewalls, hardening mechanism, strong authentication) and communication channels (such as VPN and encryption).

An event correlator based solution. It uses an active fault tree analysis supported by symptom detection technique tools. It analyses incidents, identifies abnormal ones and searches for hidden patterns among them. The event correlator is often associated with a security console that may be seen as a "mini security operation centre", such as decision support for the management of physical and logical security of the whole system.

Non-functional approaches are:

a. Exploitation of the priority of the security requirements of logical components of Smart Grids, it is based on a specific analysis of risk weighted by appropriate critical parameters in order to identify reasonable, effective and timely countermeasures;
b. A consequent logical partition of the smart or micro-grid in zones and communication channels that share security requirements homogeneous, allowing to customize cascade countermeasures.

Furthermore Tools for continuous monitoring of the security status of the infrastructure, through the acquisition, analysis and correlation of relevant data are key factors for security.

It is reasonable to use attack identification techniques based on the continuous analysis of safety events, states, alarms, measurements and commands coming / sent to the SCADA, from smart metering and from ICT security systems. An appropriate use of these techniques allows to evaluate the overall behavior of the infrastructure, highlighting:

a. Presence of attacks (discriminating from really incorrect, but genuine, information).
b. Changes in the level of risk.

In summary it is useful to work on:

a. the most suitable and reliable predictive methodologies in relation to grid reference.

b. the use of the prediction in the identification of anomalous cases that require further examinations.
c. the construction of derived (information increased) variables that have a greater meaning (physical) with respect to the identification of a possible manipulation.

17. Game Approach

Conceptually the game strategy is based on a virtual hacker and a virtual operator. Accurate model of the micro-grid is a prerequisite. The optimal strategy is identified by using game theory (Stakelberg competition and stochastic game for example).

In the Stakelberg strategy hacker and the operator have a certain amount of resources while the grid is deemed to be in a known initial state. The attacker perform a number of attacks and he operator responds by activating a series of countermeasures. These operations cause an increase or loss of resources on both parties and the process goes on until one of the party has zero resources, that means the game is over. To be noted that during the competition the competing parties may choose different strategies to control transition of the micro-grid to a new state. Any migration implies an increase or loss of resources for both parties.

The Stackelberg game is played where one player acts as the leader and the other the follower. The leader is a dominant position as it can enforce strategies on the follower, giving the leader a first-mover advantage. In this instance, the leader and follower are defined as they are previously listed in their respective level. The cost functions for each level are represented with respect to the leader, where the first level seeks to minimize the cost of a false alarm for the IDS and the second seeks to maximize the amount of disturbance caused by the attacker.

A variation on the stochastic game, the Bayesian game, is used by Ouyang et al. [35] in order to evaluate a scenario in which there is asymmetric information amongst players and strategies are updated as the state of the system changes. Games with asymmetric information are those in which "agents have different information overtime.

18. Conclusions

Energy delivery in port infrastructures needs to be carried out in a safe and secure way, strongly protected, exploiting all the technological developments, providing favourable tariff, reducing cost and emissions, increasing revenues for port authority and internal operators.

A sophisticated attacker can attempt to modify the behavior of control and monitoring systems and, in particular, directly or indirectly influence data (states, measurements, alarms) and commands (continuous and discrete) in such a way as to mislead the supervision and control system, protection and operators; what would trigger improper interventions, that in turns may be detrimental to the integrity of the equipment and interfere with the continuity of the service.

It is appropriate to use techniques for the continuous monitoring of the safety of electrical infrastructures and to build identification of models to detect attacks.

From a general point of view it is beneficial to focus on the definition of methods for dynamically identifying the dependencies of the operational process of the micro-grid towards all the technologies served to it. In particular it necessary to study:

a. The acquisition, standardization and correlation of security events coming from SCADA systems, from ICT systems with these correlated, from physical security systems.
b. Determination of the stability status of the micro-grid by evaluating the data acquired in real time by the SCADA systems.
c. Check that the micro-grid is in the "normal state" and check alteration against measures that are deemed secure.
d. The continuous monitoring of all the parameters describing the safety status of the logical, physical structures and the level of regularity and stability of the operational process, with a view to their correlation.

References

[1] Parise G, Parise L, Martirano L, Chavdarian PB, Su CL, Ferrante A, (2014). Wise port & business energy management: Portfacilities, electrical power distribution.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[3] A. Wilner, "Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application, and Limitation," Comparative Strategy, vol. 36, no. 4, pp. 309–318, 2017.

[4] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in SoutheastCon 2015, 2015, pp. 1-6. (Conference Paper).

[5] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, A. R. A. AliSmart grid cyber security: Challenges and solutions. 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE) (2015), pp. 170-175, 10.1109/ICSGCE.2015.7454291.

[6] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen Cyber security and privacy issues in smart grids. IEEE Commun. Surv. Tutor., 14 (4) (2012), pp. 981-997, 10.1109/SURV.2011.122111.00145.

[7] W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges. Comput. Netw., 57 (5) (2013), pp. 1344-1371, 10.1016/j.comnet.2012.12.017.

[8] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, K. Wang, Review of internet of things (IoT) in electric power and energy systems. IEEE Internet Things J., 5 (2) (2018), pp. 847-870, 10.1109/JIOT.2018.2802704.

[9] K. Kimani, V. Oduol, K. LangatCyber security challenges for IoT-based smart grid networks. Int. J. Crit. Infrastruct. Prot., 25 (2019), pp. 36-49, 10.1016/j.ijcip.2019.01.001.

[10] P. Eder Neuhauser, T. Zseby, J. Fabini, G. VormayrCyber attack models for smart grid environments. Sustain. Energy Grid. Netw., 12 (Supplement C) (2017), pp. 10-29, 10.1016/j.segan.2017.08.002.

[11] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," in IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2444-2453, Sept. 2015.

[12] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts onvoltage control loop in power grid," in Proc. IEEE Power Energy Soc. Gen. Meeting, San Diego, CA, USA, Jul. 2011, pp. 1–6.

[13] B. Chen, S. Mashayekh, K. L. Butler-Purry and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, 2013, pp. 1-5. doi: 10.1109/PESMG.2013.6672740.

[14] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry,"A framework for modeling cyberphysical switching attacks in smartgrid," IEEE Trans. Emerg. Topics Comput., vol. 1, no. 2, pp. 273–285, Dec. 2013.

[15] Yeo G-T, Song D-W, Dinwoodie J, 2010. Weighting the competitiveness factors for container ports under conflicting interests, Journal of the Operational Research Society, Volume 61, Number 8, Page 1249.

[16] Theodoropoulos T. The port as an enabler of the smart grid, Inter transit project, MED Programme, Valencia, Spain, 2014.

[17] Department of Energy, Office of Electricity Delivery and Energy Reliability Summary Report (2012) DOE Micro grid Workshop.

[18] Eder-Neuhauser, Peter & Zseby, Tanja & Fabini, Joachim & Vormayr, Gernot. (2017). Cyber attack models for smart grid environments. Sustainable Energy, Grids and Networks. 12. 10.1016/j.segan.2017.08.002.

[19] MANIMARAN GOVINDARASU, ADAM HANN AND PETER SAUER "Cyber-Physical Systems Security for Smart Grid Future Grid Initiative White Paper" Iowa State University, 2012.

[20] M. H. Cintuglu, O. A. Mohammed, K. Akkaya and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446-464, Firstquarter 2017. doi: 10.1109/COMST.2016.2627399.

[21] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in Proc. IEEE PES Innov. Smart Grid Technol. (ISGT), Anaheim, CA, USA, 2011, pp. 1–7.

[22] Michael T. Larkin, A Stochastic Game Theoretical Model for Cyber Security", US Air Force Institute of Technology, 2019.

[23] Lee E., Shi W., Gadh R., KimW., 2016, Design and Implementation of a Microgrid Energy Management System, Sustainability 2016, 8, 1143.

[24] DOE (2011) DOE microgrid workshop report (trans: reliability OoEDaE). Smart Grid R&D Program. DOE, San Diego.

[25] Muni-Fed Antea Group Energy Partners, LLC and The Port of Long Beach. "Microgrid Technology White Paper-Port of Long Beach", August 2016.

[26] Morris g., Abbey c., Joss g., Marnay c., 2011. A framework for the evaluation of the cost and benefits of microgrids. Lawrence Berkley National Laboratory.

[27] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Draft Interagency Tech. Rep. NISTIR 7628, 2009.

[28] Coletta A. Armando A., Security Monitoring for Industrial Control System. The first Conference on Cybersecurity of Industrial Control Systems. Vienna, 2015.

[29] S. SRIDHAR, A. HAHN, M. GOVINDARASU, "Cyber Physical System Security for Electric Power Grid," Proceedings of the IEEE, Jan. 2012.

[30] M. Tambe, Security and Game Theory: Algorithm, Deployed Systems, Lessons Learned. New York: Cambridge University Press, 2011.

[31] Q. Wu, S. Shiva, S. Roy, C. Ellis, and V. Datla, "On Modeling and Simulation of Game Theory-Based Defense Mechanisms Against DoS and DDoS Attacks," Proceedings of the 2010 Spring Simulation Multiconference on - SpringSim '10, p. 10, 2010.

[32] "Why SCADA and Control Systems need a different Information Security approach?" of Enzo M. Tieghi Vision Automation srl, Cesano B. (MI). Retrieved from https://docplayer.net/602466-Integrating-electronic-security-into-the-control-systems-environment-differences-it-vs-control-systems-enzo-m-tieghi-etieghi-visionautomation.html.

[33] Ruchkin, Vladimir et al. "Smart monitoring of the emergencies by cyber-physical systems." 2018 ELEKTRO (2018): 1-5.

[34] Guo, Jia & Wang, Yifei & Guo, Chuangxin & Dong, Shufeng & Wen, Baijian. (2016). Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions. 1-5. 10.1109/PESGM.2016.7741899.

[35] Ouyang, Y., Tavafoghi, H., & Teneketzis, D. (2015). Dynamic Games With Asymmetric Information: Common Information Based Perfect Bayesian Equilibria and Sequential Decomposition. IEEE Transactions on Automatic Control, 62, 222-237.