Cyber-Security Aspects for Smart Grid Maritime Infrastructures

Monica Canepa
World Maritime University
Malmö, Sweden
e-mail: moc@wmu.se

Stefan Schauer
Austrian Institute of Technology
GmbH Vienna, Austria
e-mail: Stefan.Schauer@ait.ac.at

Giampaolo Frugone
University of Genova,
Genova, Italy
e-mail: frugone.xng@gmail.com

Riccardo Bozzo
DITEN, University of Genova
Genova, Italy
e-mail: riccardo.bozzo@unige.it

***Abstract*— Maritime ports are intensive energy areas with plenty of electrical systems that require an average power of many tens of megawatts (MW). Competiveness, profits, reduction of pollution, reliability of operations, and carbon emission trading are important considerations for any port authority. Current technology allows the use of a local micro-grid of the size of tens of megawatts, capable of isolated operation in case of emergency and moving toward a large energy independency. Ownership of its grid permits a large control on the prices of energy services and operation either on local electric market or generally on dangerous emission. Renewable energy generation has a large impact on costs since it features a low marginal cost, but it is random in nature. Since the smart grid is a critical asset within the port infrastructure, it 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 paper, we examine the characteristics of a port smart grid and the typical characteristics of cyber-attacks. Furthermore, the potential ways to recognize these cyber-attacks and suggestion for effective countermeasures are also discussed.**

Keywords-Smart grid; maritime ports; energy efficiency; cyber attacks.

I. INTRODUCTION

The aim of this paper is to describe advantages of utilization of smart micro-grids in port areas and the requirements to protect them effectively from cyber-attacks. The paper stresses the advantages of this approach as a key factor of port competitiveness. Typical features of cyber-attacks against smart grid infrastructures are illustrated to suggest possible foundations for development of future research regarding mitigation and protection actions.

Efficient utilization of energy and sustainability of generation are critically important for port authorities and port operators due to obvious impacts on operational cost, business continuity, compliance to emission regulations, satisfaction for operators, attractiveness of the port and in last instance its competiveness [1].

In this paper, an operator is defined as an entity/organization active inside the port area that owns infrastructures, plants and buildings that is; an operator can perform simultaneously any of the following energy related operations: use of energy, generation of energy or storage of energy and change of generation /demand profile. Furthermore, the port authority can assume the role of market operator and consequently trade energy and services internally and externally.

Port electrical demand originates by:

- Civil and mechanical structures for shipbuilding activities and industrial installations, etc.
- Cruise ship terminals.
- Conveying systems, transfer towers, cranes, lighting and stockyards, refrigerated container, terminals to accommodate the movement of container
- Lighting systems for parking areas, roads, railway sidings, industrial shipbuilding yard
- Conditioning and heating system
- Electrical vehicles

From different points of view, port operators and port authorities look for competitiveness and also for profits, with a strong focus on energy efficiency and energy saving, which are related but different concepts (as efficiency implies savings but the vice versa is not necessarily true). Demand and generation have a flexible pattern in relation to the growth of port activities.

As per Theodoropoulos [2], energy efficiency and reduction of emissions is achieved by:

- Effective use of energy coming from traditional and renewables generations
- Enforce a general policy aimed to achieve the main energy objectives of the port
- Adjusting demand and supply of energy by flexible demand management, instantaneous load shedding or curtailment (both directions) and intelligent battery storage [3]
- Giving priority to renewable energy as primary resource
- Constantly moving generation and utilization of equipment to the their respective high efficient operating points

 ISBN: 978-1-61208-661-3

- Maximizing the use of electric transportation within a port
- Providing all operators with greater awareness on micro-grid status and current/forecasted prices in order to permit to anybody the correct planning of its own technical and economic operation

Protection of a smart micro-grid from cyber-attack is essential. A smart micro-grids is characterized by a set of distinctive aspects (extended geographical distribution, unmanned sub-systems, strong interaction between logical and physical level, strong requirements on service continuity, use of Internet communication services) that make traditional ICT defense techniques weaker or some time ineffective.

The sensitivity towards potential cyber-attacks increases in proportion to the growth of the complexity of micro grid control and intelligence, and is amplified by:

- Increasing interconnection also based on public networks between networks and micro grids, end users and power generation parks
- Increasing adoption of COTS (Commercial) Off-the-Shelf products in control (operating systems, DBMS, application software, etc.), and introduction of new technological paradigms of the ICT sector (virtualized systems)
- Extensive use of Internet based communication networks
- Data volume growth available and coming from non-homogeneous sources [4].

Technological evolutions introduce new vulnerabilities and criticalities of security and require accurate verification of compatibility with the requirements specified for the management of critical infrastructures.

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

Taking into account that the infrastructures of the electrical micro-grid generate a high dependence of almost all the other critical infrastructures and vital functions of the port, it is evident the possible impact that could have for a port a cyber-attack aimed at making these infrastructures not operational.

In this scenario, characterized by 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, more needs arise, especially in field of attack prevention such as:

- the acquisition of feedback regarding the level of security of the physical infrastructure
- the correlation of information coming from the ICT security domain, physical security and Supervisory Control and Data Acquisition (SCADA).
- requirement of very low reaction times

In this scenario, an attacker could design malicious activities based on the contemporary perturbation of the SCADA and of physical equipment, but it could also operate a coordinated series of actions that could cause unexpected behavior of the micro-grid.

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

II. WHY A SMART MICRO-GRID

A smart micro-grid is not a new concept since many large industrial areas and some ports are already operating an internal electrical grid powered by internal generation and connected to an external utility.

Irrespective of its smartness, a micro-grid consists of two major parts: on the one hand, the electrical infrastructure, i.e. the smart assets that generate, deliver, transform, protect and use energy and, on the other hand, communication and control systems, i.e., bidirectional communication and control system (SCADA) that operates the whole electrical smart micro-grid [5].

Most ports still use “dumb” micro-grids at certain marginal cost, rigidity of operations, level of reliability and resiliency. This implementation has a number of shortcomings, such as:

- Difficulty to fully exploit the potential of internal generation resources (often renewables such that large arrays of Photo Voltaic (PV) modules, biogas gas fired turbines, wind turbines, storage batteries, etc.)
- Difficulty to establish a customizable tariff policy that meets reward and economic and technical expectation of operators and remunerate them without tantalizing micro-grid performance and violating contractual requirements with the utility
- No easy way to support different control and regulations services required by external utility and by internal continuous activity related requirements, a fact that has an economic impact
- Difficulty to establish a customizable tariff policy that meets reward and economic expectation of operators without tantalizing grid performance and exceed contractual requirements
- Limited flexibility to server changing operators’ needs
- Less reliability and resilience of dumb micro-grid
- Small possibility to trade services and actuate policies such as “Demand Response” (DR) and exploit “Time of Usage Tariff” (TOU).

 ISBN: 978-1-61208-661-3

A smart micro-grid generally overcomes these shortcomings, provides many other benefits [6] and therefore is a sensible solution to make a port an efficient and competitive infrastructure from the energy point of view.

Last but not least, a smart micro-grid provides a significant contribution to the process of generating revenues for port authority and operators. These revenues compensate some or all of the capital and operating costs incurred by operators during the micro-grid life cycle.

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" [7].

As stated in the "Micro-grid technology white paper" written by Muni-Fed – Antea Group Energy Partners, LLC in 2016, micro-grids are designed to allow delivering of excess energy into the incumbent utility grid as well as to import energy from the utility grid [11]. A micro-grid is a small-scale version of the traditional utility grid designed to optimize energy services through its intelligent pervasive controls, they can operate completely separated (that is islanded) from the utilities outside grid if properly sized internal generation and storage is provided.

Therefore, economic and technical objectives are enabling factors for a smart micro-grid deployment. Economic objectives aim to reach cost reductions and to stream revenues coming from operations of the smart micro-grid, specifically arbitrage/trading, minimization of cost associated to procurement of energy (including supply and bilateral contracts), correct definition of procurement contracts, avoiding penalties due to non-compliance with contractual terms (peaks, valleys, supply of services, emissions, etc.). Regarding the technical aspects, the fundamental objective is to deploy a stable, resilient, cyber-secure and reliable smart micro-grid capable of delivering high quality energy at the best prices to operators in relation to their past, present and forecasted behavior. These objectives are a function of availability of functionality, such as:

- Control at different levels capable to provide a cost effective, reliable durable, sustainable electric system able to serve efficiently its operators
- Enable independent (off the grid) operations in case of external adverse electrical conditions
- Reduce risk of general electrical collapse of micro-grid and permit faster detection, identification, isolation/clearing of fault and fast restoration to a normal state of operations
- Mitigate of the consequences of energy fluctuations through dispatching energy storage and switchable loads
- Improve energy-related operational efficiencies and coordinated use of energy storage systems
- Ensure continuous delivery of energy
- Face the stochastic nature of renewable generation
- Reduce peak load exposed to the utility
- Enable cranes with independent (often diesel) generation to inject excess of their generation, if economically viable and technically reasonable, into the micro-grid.
- Enable Vehicle to Grid (V2G) and Vehicle to Building (V2B) operations for port fleet of electrical vehicles
- Enable deployment and sound utilization of a Virtual Power Plant (VPP)
- Use energy normally wasted owing to braking operation through regenerative breaking.

III. MICRO-GRID DESIGN

Micro-grid design starts from specific port specifications like size of initial load and generation, its evolution as well mode of utilization of external energy supplies, operation schedules, and economic investment. Design Analysis is supported by some forecasting methods (e.g., it is possible to use spatial load forecasting, Support Vector Machine (SVM), time series analysis, Kernel Auto-Regressive Model with Exogenous Inputs (KARX), etc.

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

Design Analysis is performed under various scenarios including the worst conditions, synchronization capability in connected and disconnected mode. Finally, risk analysis techniques like FMEA (Failure Mode and Effect Analysis) and FMECA (Failure Mode and Effect and Criticalities Analysis) are carried out as well to complete the preliminary project and permit an objective evaluation. These analyses are prerequisite for micro-grid risk management.

The smart micro-grid is also 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 reducing the risk of temporarily downgrading of the service. While the micro-grid planning criteria may come from a variety of sources, the most common is the need for high grid resilience to maintain active critical services during extended utility outages; other criteria include the increasing use of renewables, reducing emissions, managing energy costs and improving energy self-reliance, leading to state government regulations and incentives. (See figure 1).

 ISBN: 978-1-61208-661-3

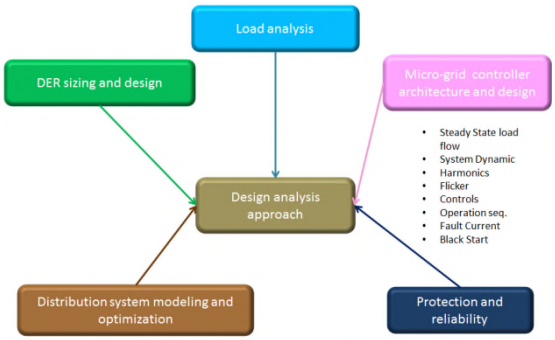

Figure 1. Micro-grid Design

Critical (that is must serve), no-critical loads and generating and storage farms are assigned to different feeders. Critical feeders are powered by dedicated generators and backed by their own storage so that 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 controllability, capability to respond to outside request to adjust load and/or generation profile and finally level of local intelligence. Design adheres to a general form of control that is hierarchical and decentralized, that means

- Each controllable operator can operate according to its own objective, preferences and policy
- Policy and objectives of the whole micro-grid are established by the controller at the highest level of the hierarchy
- A set of coordination principles takes into account the interaction of the processors (i.e. the fact they operate on their own according to a specific policy).

IV. CYBER-SECURITY ASPECTS OF SMART GRIDS

The cyber information security plays a fundamental role in management of smart micro-grids due to their strategic nature, since they represent the basis for the operation of several critical port infrastructures [11]. Because of this strategic role and considering the massive presence of intelligent components in the smart grid sector, the cyber-security of the smart micro grids (which includes attack prevention, detection, mitigation and resilience) represents a challenge for the future at the base of the research to be carried out. It is useful to reach the definition of models that are able to quantify potential consequences of a cyber-attack on the electricity grid, and this in terms of pressure drops, stability violations, and damage to equipment and / or economic losses.

According to a joint study by Iowa State University and the University of Illinois at Urbana-Champaign, after an appropriate risk assessment, the next step should be the development of an integrated set of security algorithms that can protect the network from multiple forms of cyber-attacks, such as denial of service attacks, malware-based attacks, etc. Such algorithms should take into consideration very sophisticated attacking modeled that could potentially cause a maximum level of damage. According to this study algorithms to mitigate the risk of an ICT attack should be developed through real-time correlation of the data streams and registers obtained from substations and control centers, algorithms that can prevent, detect and tolerate as well as mitigate cyber-attacks [8].

The 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) [9], IEC 61850, Distributed Network Protocol 3 (DNP3) [10] (derived by GE-Harris from IEC 60870-5), if not properly protected, could potentially be used as carriers to launch cyber-attacks. This requires secure versions of these protocols.

A. *Kinds of Cyber- Attacks to Smart Grids*

A first type of attacks on the grid is represented by the "Intrusions": this type refers to exploiting the vulnerabilities of software and communication between the network infrastructures that then provides access to critical elements of the system. The "Malware" instead consists of malicious software that aims to exploit the existing vulnerabilities in the software system, programmable logical controllers, or protocols. Once the malware has gained access, it will try to cause damage in the system using the self-propagation mechanism.

The "Denial of service attacks aim to make services or resources managed by an organization 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 operation of the attack lens.

Further, "Insider threats" are considered a great danger, by virtue of the privileged position that the potential attacker has, as it can operate from within the organization. Finally, "Routing attacks", in which cyber-attacks occur on internet routing infrastructures, should not be underestimated. Although this type of attack is not directly related to grid operations, it could have consequences on power system applications. Generally, it includes the following:

- Spear-phishing emails (from compromised legitimate accounts),
- Watering-hole domains,
- ICS infrastructure targeting and credential gathering
- Host-based exploitation,
- Industrial control
- Open-source reconnaissance

 ISBN: 978-1-61208-661-3

B. *Electrical Supply System: Vulnerability of Control Systems*

From a functional point of view, the micro-grids divided into: generation and storage, transmission and distribution.

Each functional division corresponds to systems whose task is the control of specific machines/devices. Each functional division has systems that control specific machines/devices and operate using dedicated communication signals and protocols. In this perspective, it is clear that each control system is subjected to specific vulnerabilities; in fact, they could constitute vectors of threats with a consequent potential impact on the operations of the whole supply system. Figure 2 shows a typical cyber-physical system.

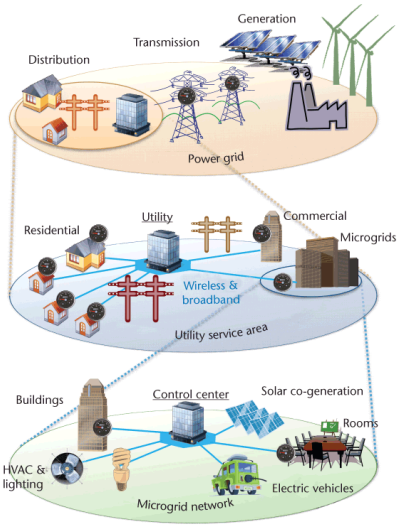

Figure 2. A typical cyber-physical system [12]

Resilience features of micro-grid control systems, includes

- Minimization of the occurrence of outages
- Mitigation of any unwanted incidents
- Minimization of the impact of outages
- Restoration of the normal working conditions of the grid in short time.

C. *Smart and Micro- Grid: Cyber- Security Aspects*

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

Therefore, in the specific case instead of investigating and proposing new technologies, we try to improve the process of defining the appropriate and measurable requirements of cyber-security for the micro-grid in order to define a realistic, efficient and scalable solution.

Computer security is an essential feature for the reliability of any control system today and is to be considered from the beginning of any project and not as an additional final component, as it sometimes happens. On the other hand, Cyber-Security for a smart micro-grid must be "smart" by itself, based on cost benefit and risk analysis, with negligible effect, if any, on performances. In this context, it is reasonable to recommend analysing from the beginning the specific needs of electrical equipment and the interconnections of data exchange [13].

Nowadays, the dedicated technology for ICS (Industrial control system) Cyber-Security consists mainly in analysis of network traffic at connection points relevant to the distributed control system. Current solutions range from easily configurable systems, which require traffic rules explicit and simple to self-learning machines that can separate autonomously normal and abnormal traffic, after a period of unsupervised training.

The "Defence in depth" is still at the initial stage and it's more expensive than filtering traffic, but it increases security of the single control nodes, independently of their interconnected topology. This approach is expected to become very valid, but in general it is justifiable only for new installations, while in other cases a mix between in-depth and filtering must be evaluated.

A good compromise for the choice has been proposed in the standard ANSI/ISA-99 [14], 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.

There are several kinds of attacks to smart grids [15]:

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:

- DDoS-attacks from outside targeting inside assets (Inbound attacks)
- DDoS-attacks from inside targeting inside assets (Internal attacks)
- DDoS-attacks from inside attacking targets outside (Outbound attacks)

 ISBN: 978-1-61208-661-3

- DDoS-attacks on certain user groups (selective harassment)

Destruction attacks

Unlike the interruption where the service can be restored after the attack, with destruction very often the infrastructure must be rebuilt:

- Disconnect households
- Destroy energy management
- Influence critical electrical nodes in the grid
- Alteration of sensor data
- Tamper with clock synchro

Theft

Stealing a commodity such as information to reveal to competitors:

- Espionage
- Ruin credibility of users:
- Sell long term data:
- Bill manipulation

Extortion schemes

Extortion attempts for demanding ransom achieving the releasing a captured:

- Commodity or service
- Threat of destruction
- Threat of DDoS
- Crypto-locker

Repurpose attacks

- Fake servers
- Proxies
- Distributed computing

D. Cyber-Security Objectives: Functional Improvements and Processes

The objectives of cyber-security are divided into functional improvements of process:

- Customized off-the-shelf solution, integrated into nodes (such as firewalls, hardening mechanism, strong authentication) and communication channels (such as Virtual Private Network (VPN) and encryption);
- An event correlator based on an active fault tree and supported by symptom detection technique tools analyses incidents, identifies abnormal ones and searches for hidden patterns among them. This event correlator is often associated with a security console which can be seen as a "mini security operation centre", such as decision support for the management of physical and logical security of the whole system.

Furthermore, non-functional objectives are associated with the procedures, e.g.:

- A new approach to the priority of the security requirements of logical components of Smart Grids, based on a specific analysis of risk weighted by appropriate critical parameters in order to identify reasonable, effective and timely countermeasures;
- 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.

A potential growing danger 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 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). Methods 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 Metering and from ICT security systems. An appropriate use of these techniques allows to evaluate the overall behavior of the infrastructure, highlighting

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

A sophisticated attacker can attempt to modify the behavior of a SCADA 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 necessary to use techniques for the continuous monitoring of the safety of electrical infrastructures and to build identification of models to detect attacks.

It is useful 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:

- the acquisition, standardization and correlation of security events coming from SCADA systems, from ICT systems with these correlated, from physical security systems

 ISBN: 978-1-61208-661-3

- determination of the stability status of the micro-grid by evaluating the data acquired in real time by the PV, systems
- 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.

V. CONCLUSIONS AND FUTURE WORKS

The use of smart micro grid is to be promoted as a key element for port competitiveness and compliance with environmental regulations. Proper design of the micro-grid leads to benefits of port authority, port operators and external electrical utilities. It is important that the control and management structure reflects the organization and operation logics of port infrastructures, a fact that generally leads to a distributed hierarchical structure and a pervasive distribution of intelligence. Electrical and financial analysis supported by powerful forecasting tools is required to specify and deploy a micro grid that fit well with current and future requirements of the port. Modularity and upgradability is equally important as well as very friendly mode of operations.

Equally important is the cyber protection of the micro grids either in its smart equipment and control and information systems. This protection entails to points: defense of the information and control system as well as of communication infrastructure and recognition of electrical status that is not genuine and that would trigger dangerous control.

At the state of the art, in the face of a wide diffusion of solutions for the centralization and correlation of information security events it is possible to approach the problem using currently available technologies and planning developments aimed at extending the capacity of existing solutions.

Comprehensive control system with specialized optimizations tools needs to be developed together with sophisticated monitoring techniques. The role of forecasting and modeling cannot be neglected and its importance stems either or from management requirements or security model based constraints.

It should be noted that early recognition (in the order of a few minutes) may be sufficient to undertake protective actions and to initiate the resumption of operations. For instance, it is important to design and develop monitoring techniques capable of assessing whether and to what extent the monitored system is deviating from the normal state due to causes not due to actual failures or malfunctions. Equally important is development of optimization methods that decouple high and low level of control (that is port authority and port operators) and compensate individual behavior in line with high level policy and objectives.

Finally, a powerful but easily usable modeling and evaluation techniques is recommended to help port authority and operator to devise the best and long lasting solutions.

REFERENCES

[1] G. Parise et al., “Wise port & business energy management: Portfacilities, electrical power distribution”, IEEE Transactions on Industry Applications, Vol. 52 , pp. 18-24, February 2016, doi: 10.1109/TIA.2015.2461176

[2] T . Theodoropoulos, “The port as an enabler of the smart grid”, retrieved: September, pp. 1-37, Inte-Transit training workshop in Valencia, Nov 2014, http://www.fundacion.valenciaport.com/docs/inte-transit/T_InteTransit_5TTheodoropoulos.pdf

[3] Y. Yang, S. Bremnera, C. Menictas, and M. Kaya, ”energy storage system size determination in renewable energy systems: A review', Renewable and Sustainable Energy Reviews” , vol. 91, August 2018, pp. 109 - 125, http://dx.doi.org/10.1016/j.rser.2018.03.047

[4] P. Bangalore, and L. B. Tjernberg, “Condition Monitoring and Asset Management in the Smart Grid” , Smart grids handbook 1, Wiely online library, August 2016, https://doi.org/10.1002/9781118755471.sgd061

[5] E. Lee, W. Shi, R. Gadh, and W. Kim, “Design and Implementation of a Microgrid Energy Management System”, Sustainability, Vol. 8, 2016, https://doi.org/10.3390/su8111143

[6] G. Morris, C. Abbey, G. Joss, and C. Marnay, “A framework for the evaluation of the cost and benefits of microgrids”, CIGRÉ International Symposium: The electric power system of the future, Lawrence Berkley National Laboratory, September 2011, https://building-microgrid.lbl.gov/publications/framework-evaluation-cost-and

[7] The US Department of Energy, Office of Electricity Delivery and Energy Reliability Summary Report , DOE Micro-grid Workshop Report, August 2011, California, https://www.energy.gov/sites/prod/files/Microgrid%20Workshop%20Report%20August%202011.pdf

[8] M. Govindarasu, A. Hann, and P. Sauer, “Cyber-Physical Systems Security for Smart Grid Future Grid Initiative”, Iowa State University February 2012, https://pserc.wisc.edu/documents/publications/papers/fgwhitepapers/Govindarasu_Future_Grid_White_Paper_CPS_Feb2012.pdf

[9] International Electrotechnical Commission, “Telecontrol equipment and systems”, IEC publication, April 2002, https://www.sis.se/api/document/preview/559181/

[10] International Electrotechnical Commission, “IEC Smart Grid Standardization Roadmap” , SMB Smart Grid Strategic Group (SG3) , June 2010, http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf

[11] Muni-Fed – Antea GroupEnergy Partners, LLC and The Port of Long Beach, Micro-grid Technology White Paper, August 2016, http://www.polb.com/civica/filebank/blobdload.asp?BlobID=13595

[12] Yogesh Simmhan et al., ” Cloud-based software platform for data-driven smart grid management”, University of Southern California, 2013,http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458.1106&rep=rep1&type=pdf

[13] S. Sridhar, A. Hahn, and M. Govindarasu, Jan 2012, “Cyber Physical System Security for Electric Power Grid,” Proceedings of the IEEE, Vol. 100, January 2012, http://powercybersec.ece.iastate.edu/powercyber/download/publications/11.pdf

[14] The International Society of Automation, ”ISA99-Industrial Automation and Control Systems Security”, retrieved: August, 2018, https://www.isa.org/isa99/

[15] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, “ Cyber attack models for smart grid environments. Elsevier-Sustainable Energy, Grids and Networks, Volume 12, December 2017, Pages 10-29, http://dx.doi.org/10.1016/j.segan.2017.08.002

 ISBN: 978-1-61208-661-3