Issue 24
2022
ISSN: 2241-438X

NMIOTC

Maritime Interdiction Operations Journal

NATO OTAN

NATO
OTAN

NMIOTC/ΚΕΝΑΠ

NATO
Maritime Interdiction Operational Training Centre

SAVE THE DATES

14th NMIOTC Annual Conference
7 - 8 June 2023

7th Conference on Cyber Security in the Maritime Domain
27 - 28 September 2023

CONTENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Commodore Ch. Thymis GRC (N)
Commandant NMIOTC

Executive Director
Commander G. Finamore ITA (N)
Director of Training Support

Editor
Captain P. Pantoleon GRC (N)
Head of Transformation Section

Layout Production
Lieutenant I. Giannelis GRC (N)
Journal Assistant Editor

Cover Photo: Lt I. Giannelis GRC (N)

You may send your comments to:
pantoleonp@nmiotc.nato.int

A Holistic Approach for the Dependability Enforcement of Cyber & Power Systems on future MVDC Ships

by Massimiliano Chiandone, CDR Marco Merola, Andrea Vicenzutti, Giorgio Sulligoi, CDR Gianluca Maria Marcilli

Abstract — Modern shipboard power systems are complex systems that rely on automation for their correct operation. The power and the control layers are strictly interrelated, and the data infrastructure is as critical as the power one. Future power systems exploiting resilient architectures (like the zonal medium voltage dc one) will rely more and more on controlled components (e.g., power electronics converters) to achieve their operational advantages, thus increasing the integration among data and power infrastructure. In such a context, the cyber security of the data infrastructure constitutes a critical point for the correct operation of the ship. Existing approaches mostly focus on enforcing the dependability on the cyber infrastructure, taking the power infrastructure as a given. However, ensuring the dependable operation of the power system means ensuring the supply of the onboard critical loads, which directly depends on the power system architecture, its design, and how it is operated. Therefore, it is critical to evaluate the effect on the power system of the malicious actions performed on the data infrastructure, and consider the possibility of acting on the power system itself to avoid or react to the threats (i.e., designing a dependable power system). In this paper such a holistic approach for the dependability enforcement of integrated cyber & power systems on ships is presented, discussing some of the solutions for the actual power systems and presenting an overview in regards to future medium voltage dc power systems.

Keywords—component, formatting, style, styling, insert

I. INTRODUCTION

In modern ships, the Integrated Power System (IPS) is a core component because it supplies both onboard loads and propulsion (either in full electric or hybrid configuration). Fig. 1 depicts a notional IPS of a cruise ship, which is at present, one of the most complex examples of shipboard power systems. In such an IPS, two separable main switchboards operating at medium voltage (MV) are powered by a total of four generators. The MV distribution directly supplies the higher power loads, such as propulsion variable frequency drives, while low voltage busbars fed through transformers are used for the low power users. Being the IPS an islanded system with high installed power (tens of MW), ensuring Power

Quality (PQ) and Quality of Service (QoS) is a demanding task [1]. Therefore, proper system design and control are capital. Regarding the latter, a multilayered hierarchical control system is used, which relies on several devices and automation channels to correctly operate. Nowadays, IPSs are evolving due to the introduction of more demanding requirements (e.g., mission and payload related ones for naval vessels, or pollutant emissions related ones for merchant ones), pushing towards the use of new architectures and innovative subsystems. The most performing architecture actually conceived it based on the Zonal Electrical Distribution System (ZEDS) approach, using MV direct current (MVDC) [2].

The modern implementation of control architecture in power systems (IPS included) is made using digital systems. Indeed, from analog controls technology has moved on, rewriting/redesigning them in discrete time and implementing them digitally on controllers specifically dedicated to automation. The increase of the computational capacity in these devices allows to implement more and more control functions, and to integrate more and more sophistication in a single device. The resulting increase in complexity in developed control software implies that low-level programming languages are practically no longer usable, and there is a standardization in high level development languages and platforms. Specifically, the tendency is to use Central Processor Units (CPU) with standard 32- and 64-bit architectures, to allow for great flexibility, offering virtual memory management and multitasking. These platforms require a real-time operating system (RTOS) for proper management of hardware and timing requirements, which enables using standard software platforms (e.g., cryptographic suites, communication protocols, software for hardware management)

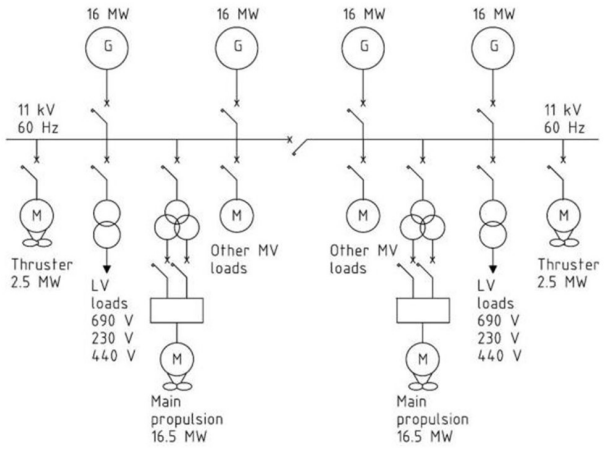

Fig. 1. All-Electric Ship: Integrated Power System layout [1]

[3]. On the other hand, the complexity of the IPS control software architecture poses security and reliability issues. In this paper, a unified approach to dependability of complex system that contemplates the hardware and software structures in a single model is presented.

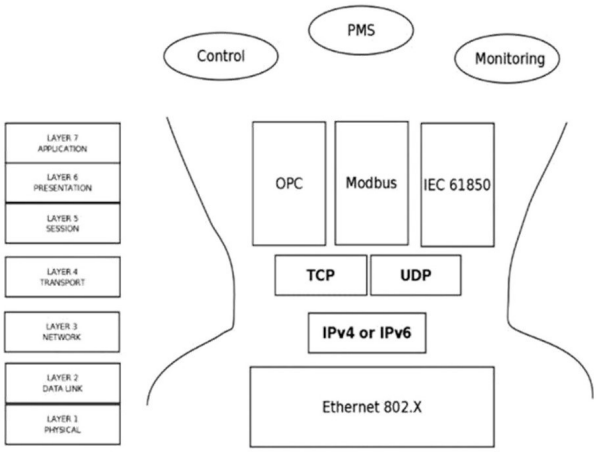

Fig. 2. Protocols used for control and energy transactions. The central role of IP stack.

The paper is organized as follow: in Section II common aspects between hardware and software errors are detailed, Section III deals with some security issues related to protocols communication in naval systems. In section IV the holistic approach is presented, and in Section VI is shown the help of simulations in the application of the holistic approach is presented.

II. HARDWARE AND SOFTWARE FAILURES

Due to the increasing pervasiveness of power converters in modern IPSs, their operation depends less and less on the physical laws of electricity and more and more on the control system algorithms. The latter are performed by dedicated CPUs and exchanged data through a communication infrastructure. Thus, two main components of a shipboard power system can be recognized: the power (physical) infrastructure and the cyber infrastructure. The latter consists of all the software that implements the algorithms and protocols to transmit data among devices. All this can be summarized generically as continuous growth in the digitalization of IPSs. In such highly digitalized systems, the software component assumes a role comparable (due to the effects it has on the plant) to those of the hardware component. In both these elements, events may occur that lead to system degradation. Suppose only the malicious events due to an intentional fraudulent action are considered. In that case, the cyber part can be subjected to errors due to malware, errors in the code, cyber-attacks, intentional actions on controls or on communication channels, and fraudulent actions on sensors and actuators. Intentional malicious events on hardware components are essentially physical damage to equipment or control actions that bring the devices to an operating point outside the physical limits of the device. Both kinds of events generally lead to a failure that causes abnormal behavior of the IPS and, therefore, to a degradation of its performance and Quality of Service (QoS). In such a context, it is clear that cyber infra-

structure security constitutes a critical point for the correct operation of a ship. Existing approaches mostly focus on enforcing the dependability of the cyber infrastructure, taking the power infrastructure as a given. However, ensuring the dependable operation of the power system means ensuring the supply of the onboard critical loads, which directly depends on the power system architecture, its design, and how it is operated. Therefore, it is critical to evaluate the effect on the power system of the malicious actions performed on the data infrastructure and consider the possibility of acting on the power system itself to avoid or react to the threats (i.e., designing a dependable power system). In this paper, such a holistic approach for the dependability enforcement of integrated cyber & power systems on ships is presented, discussing some of the solutions for the existing power systems and presenting an overview in regards to future medium voltage dc power systems.

III. CYBER SECURITY INFRASTRUCTURE IN IPSs

A. Communication protocols in actual and future IPSs

Communication protocols have been standardized on a few models, one of the most used is TCP/IP, which has also entered the field of automation systems [4]. The convergence of General Purpose Processors (GPP) and IP-based communication protocols has also given way to the use of different software platforms (an example is the use of IoT platforms also in the field of automation [5]). As regards the communications between the different subsystems, in the last 20 years, there has been a convergence towards the Internet Protocol (IP), which has become the most used transport layer. In physical levels 1 and 2 of the ISO-OSI model [6], there has been a proliferation of different physical media for the various domains currently standardized in one of the many Ethernet protocols of the IEEE802 family. Different specific protocols have been adopted for each domain in the higher application levels. Modbus, IEC61850 and OPC are perhaps the most common protocols used for ship automation and are used mainly over IP. IP version 4 does not have any security mechanisms, thus, data encryption is adopted at the application level, where deemed necessary, possibly through public key infrastructures and with the Transport Layer Security (TLS) protocol. Power Management System (PMS), hierarchical control and monitoring of the IPS are implemented on top of those protocols.

In the new power distribution architectures, including MVDC ZEDS, the power flows are even more dependent on the controls of the converters. Therefore, there is a direct relation with the behavior of the CPUs transmitting data and commands through the data protocols. More sophisticated hierarchical controls can be implemented in this type of IPS, such as zonal control. Nevertheless, the communication architecture still relies on the Fig. 2 structure.

B. Cyber security of the data infrastructure

The growing use of distributed controls and communication protocols (in cyber interactions within the electrical system) leads to greater control over its operation. However, it can also lead to a general weakening of the system against software errors, communications errors, or fraudulent actions taken against the system through its cyber infrastructure. The security by design paradigm must become preeminent with respect to generic prevention of every possible type of cyber-attack. Two types of problems can be considered in an IPS: software problems (due to software malfunction and errors in data transmission) and hardware problems (therefore, the fault of a physical device). For each of these two types, non-voluntary (due to errors and misconfigurations, aging of components or breakage) and voluntary events can be considered. Concerning the cyber infrastructure, the software problems can be caused by the insertion of malicious code or the fraudulent insertion of incorrect data capable of affecting the correctness of the operation of the entire system or part of it. All types of errors can lead to

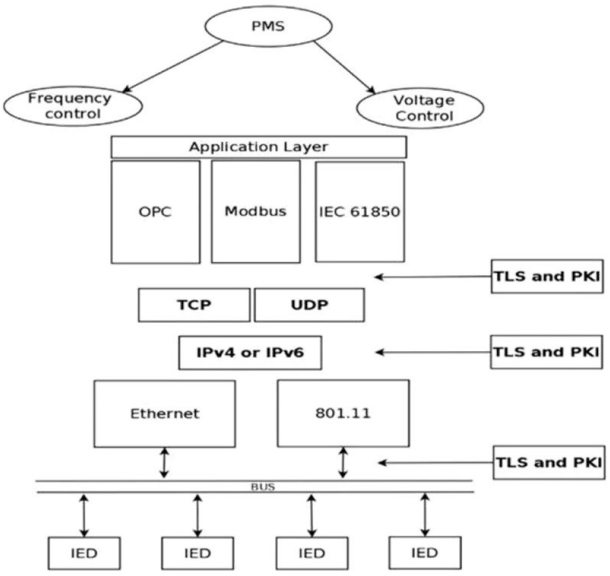

Fig. 3. Data management architecture for the grid control with three different levels where cryptography can be applied.

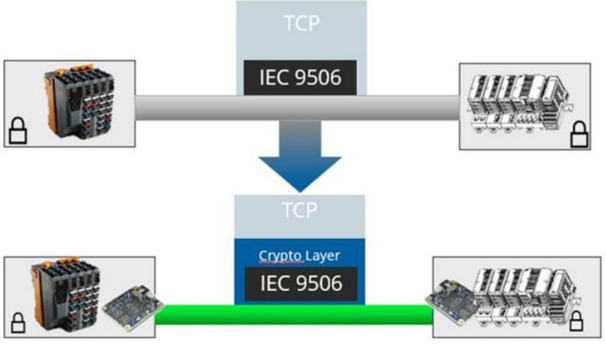

Fig. 4. Crypto layer for real-time comms.

a failure that causes an incorrect operation which in turn can lead to a lowering of the quality of the service offered by the system.

C. Approaches to increasing the security of cyber infrastructure and related critical points

An increase of security level in communication channels can be achieved using the encryption of transmissions. The encryption can be implemented at different levels (Fig. 3), but the most common are: at the physical layer, at the network level or, more generally, at the application level.

At the application level, message encryption can be implemented directly on the CPUs that control the static converters that interface with the PMS or secondary controls. Provided the processors support this possibility, encryption should be done using standard encryption software suites.

Some aspects of this infrastructure have effects on the vulnerability of the system:

• the use of standard libraries and protocols brings the system at the state of the art but only if it is reg–ularly updated (by constantly applying all the necessary patches). In the absence of an update, you are exposed to known and well-documented attacks;

• the use of modern cryptographic suites has a computational cost that effectively excludes some proces–sors (i.e., microcontrollers) from being usable;

• the addition of a software component increase es the complexity of the system (and therefore affects its safety) in the same way as adding a new hardware component.

The increased complexity and the computational cost due to the cryptography layer can be considered non-sustainable by the existing OT devices (e.g. PLC, RTU), especially in near real-time and mission-critical applications. Dedicated crypto devices (Fig. 4) could represent an affordable solution: principal design requirements are low latency encryption-decryption processes for real-time coms, filtering IP and ARP messages, and easy setup over existing systems. The crypto-layer must protect from external, extraneous or compromised OT/IT devices connected to the control network, preventing spoofing, tampering and other malicious activity. Combined with a behavioural Intrusion Detection System that analyses network traffic and software and firmware configuration, the complexity of an effective cyber attack increase dramatically.

In general, a perfectly secure system cannot be built; hence it is always necessary to consider a possible failure in the cyber section of the system. However, such failure can or cannot affect the IPS operation depending on its design, making it necessary to study both the cyber and the physical sections of the system as a whole.

IV. A HOLISTIC APPROACH TO THE DEPENDABILITY ENFORCEMENT OF CYBER-PHYSICAL SYSTEMS

A. Effect of the cyber infrastructure on the physical one

Existing approaches mostly focus on enforcing the dependability of the cyber infrastructure, taking the power infrastructure as a given. However, it should be considered that not all possible attacks can be faced only by increasing the security of the HW and SW architecture of the former. Given the complexity of present control systems used in electrical power systems, it must be assumed that some security flaws are always present. If they are not found during system construction, they could be discovered during their useful life. In critical systems, a continuous security assessment and a system update activity must therefore be envisaged for the cyber infrastructure (e.g., updating the software whenever new exploits are discovered), as happens with their physical part with predictive maintenance. Despite the preventive corrective actions, the possibility of fraudulent actions must be always taken into account. Thus, the evaluation of their effect on the physical part of the system is needed, considering not only the single affected subsystem, but all the system as a whole. This is a complex task, due to the several interrelations between cyber and physical parts, which are already complex by themselves.

Following a cyber-attack (for example, an attack that modifies the power system control layer by injecting false data into it), actions on the hardware must be taken to mitigate its effects. In a power system a cyber-attack can tamper with the references in the automatic voltage regulator of one or more generators, bringing them to a point outside the safety values and causing their disconnection. The result is equal to a physical fault, leading to the failure of the power system if this has not been correctly designed to manage such an event. Malicious actions of this type can thus be represented by using their final effect on the power system modeled as a fault of one component or subsystem, and then assessing the capability of the system to resist such fault. Through this approach it is possible to enforce the dependability of these systems, by applying an integrated methodology that acts both on the cyber and the physical sections.

B. Applying dependability theory to IPS analysis

The dependability theory consists of a set of definitions and concepts for analyzing and managing the origin of faults, errors, and failures, determine their effects on a system, and set appropriate countermeasures, using a systematic approach. The general theory corpus originated from the computing and communication systems area, and is consistently and exhaustively depicted in literature (e.g., [7][8]). Thanks to its generality,

it is possible to extend its application to systems aimed at performing different tasks, like ships' IPSs [9],[10]. This can be done because the latter are complex systems, i.e., a set of components that, once assembled, function as a single entity with a given functionality. In fact, an IPS is a set of electrical, mechanical, and control components that are designed and built to provide power to the onboard loads with a specified QoS (defined by the design requirements). Given the size of a ship's IPS, the complexity of designing it dependable and secure is evident. From a practical point of view, several tools have been developed to aid in this task, like Failure Mode and Effects Analysis (FMEA) or Fault Tree Analysis (FTA), to mention two of the most famous only [10]. Although all the tools aimed at evaluating dependability or its specific attributes (reliability, maintainability, availability, etc.) are useful, the ones capable of providing a quantitative evaluation (i.e., calculate numerical indexes) are the most powerful ones. As an example, FTA method allows building failure-trees of specific failure events, and apply simple mathematical equations to evaluate numerical indexes starting from failure data (e.g., failure rate, MTTF, MTTR, etc.) [11].

By considering cyber originated events by means of their effect on the power system hardware, it is possible to include cyber-attacks in the dependability analysis of a power system. Thus, the evaluation of the overall IPS performance is enabled, not only in respect to physical faults, but also in respect to cyber originated events. It is relevant to notice that different types of cyber-attack and related countermeasures can lead to the same physical effect. As an example, a cyber-attack may be aimed at a generator, and its success leads to protection intervention, uncontrolled behavior, or the machine stopping producing power. In either case, at some point at least one electrical protection (possibly the ones in the main switchboard, if the generator's ones are compromised by the cyber-attack) intervene, disconnecting the generator from the power system. On the contrary, the cyber-attack may not be directed immediately to the generator, but a loss of security in the data communication infrastructure is identified by a suitable method. In such a case a possible solution is to stop relying on the compromised equipment, thus stopping the generator as a preventive measure. In either case, from the electrical point of view the effect is a stopped generator, which is considered as a fault in the power station. From this point onwards, it becomes possible to consider the effect of the cyber-attack on IPS operation with different tools, using either an estimate of the cyber-attack probability of occurrence (calculated through a vulnerability assessment) or setting a 100% probability to evaluate the worst case.

It is relevant to notice that the evolution of a power system towards a failure is a dynamic process, and not a Boolean one. Thus, it is possible to act on the failure process (to stop it) not only before its occurrence, but also during it and at different time instants. This can be properly highlighted by means of mathematical modeling and simulation of the physical system. Focusing on IPSs, suitable power system dynamic simulators can be built, at different levels of detail depending on the specific power system and the analysis goal. Then, the simulation results, in conjunction with the considered critical events, can be used to define enforcing techniques to the system, as fault prevention, tolerance, or removal. The result of this process is the modification of the IPS design, so that the problems discovered are solved and a more dependable system is obtained. The latter can be done changing the system design, if possible, or introducing modification to an existing system [11]. For a given identified critical event, the modifications can be done on the physical part of the IPS, on the cyber part, or on both of them.

V. MATHEMATICAL MODELING AND DIGITAL TWINS FOR CYBER SECURITY TESTING AND DEPENDABILITY ENFORCEMENT

The use of software simulators has become an established practice in design. Through the implementation of mathematical models of physical systems, it is possible to calculate with great precision the system's dynamic response to various inputs to define a design capable of complying with the relevant requirements before its construction [12]. This possibility is useful in the design phase, since it can reduce the risk and the need of relying on expensive experimental phases. As an example, it is possible to check the correct coordination between control system and protections of an IPS, and plan actions to face emergency situations or to increasing flexibility, defining the correct control system's parameters and support crew training [13]. The physical system modeling can include a section of the cyber infrastructure, to provide an integrated assessment tool to test the security of a power system. Moreover, the mathematical model can be compiled in a real-time environment and executed in parallel with the real system continuously exchanging data with it, constituting the so-called digital twin. If properly built and managed, the latter can be a critical asset for enforcing system's dependability. Indeed, it can be used to identify cyber-attacks and other malicious actions by comparing the real component behavior and the expected one given by the digital twin.

In the following, two examples of how the proposed approach works are given, considering actual and future IPSs architectures.

A. Actual IPS example

To provide an example in regards to an actual IPS, it is possible to refer to [11]. While in such paper

only the physical components' faults where applied, it is still possible to use such a case by considering a cyber-attack that leads to a component or subsystem fault. Then, the same process for the analysis and dependability enforcement can be applied. E.g., it is possible to assume a cyber-attack affecting the data communication infrastructure of the ship, causing a loss of security in the data channel between the PMS and one generator. The result (either by the attack itself or as a security measure after the attack is identified) is the shut off of the compromised generator. From this point onwards the cyber section of the system is not concerned anymore with the resulting physical system behavior, until specific actions by the PMS are to be adopted to maintain the system operation. Depending on the power system design and operation, the effect of the generator shut off may or may not be critical.

In the [11] case study, the power system fails after a short amount of time due to overloading of the remaining generators. Specifically, Fig. 5 and 6 show frequency and active power output of the remaining DG

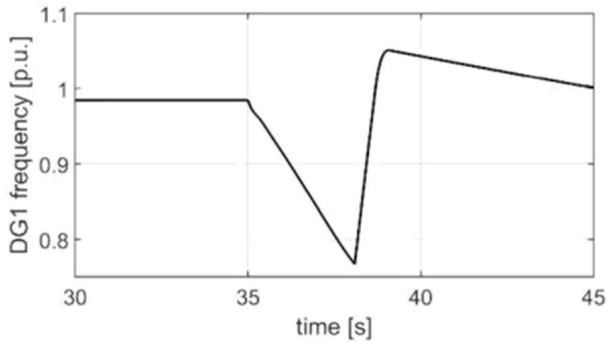

Fig. 5. Frequency of a running generator [11]

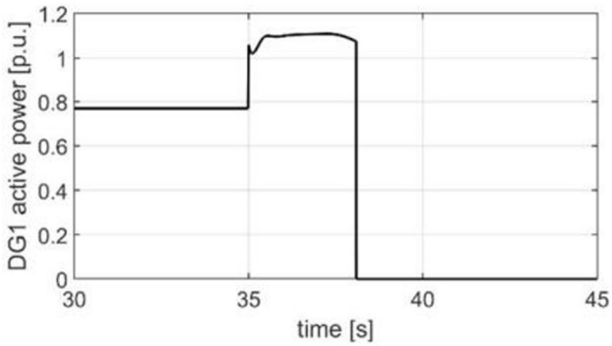

Fig. 6. Power of a running generator [11]

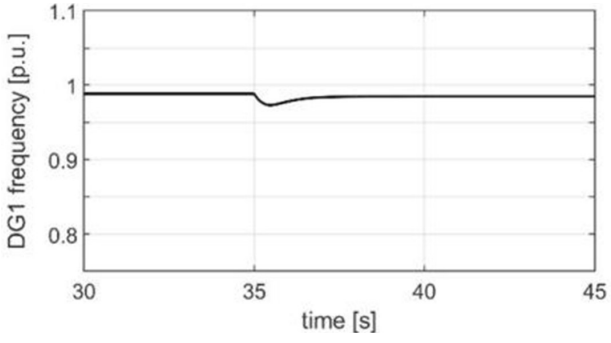

Fig. 7. Frequency of a running generator, with one more active DG [11]

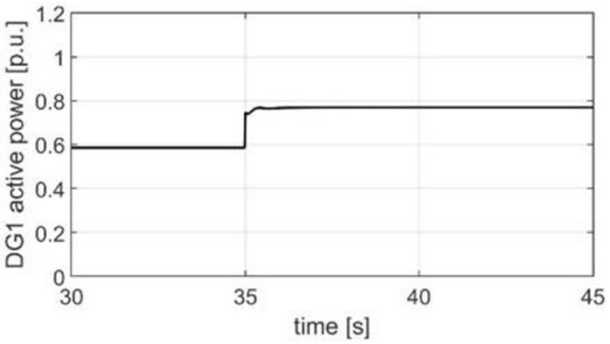

Fig. 8. Power of a running generator, with one more active DG [11]

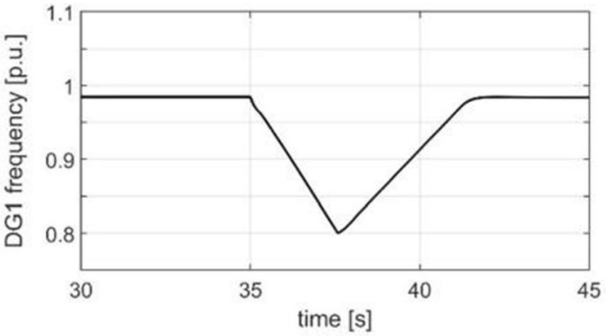

Fig. 9. Frequency of a running generator, with load-shedding [11]

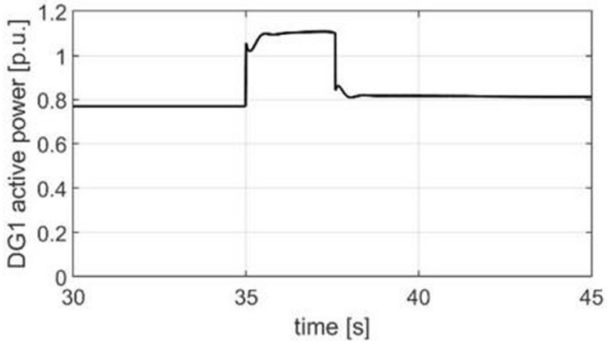

Fig. 10. Power of a running generator, with load-shedding [11]

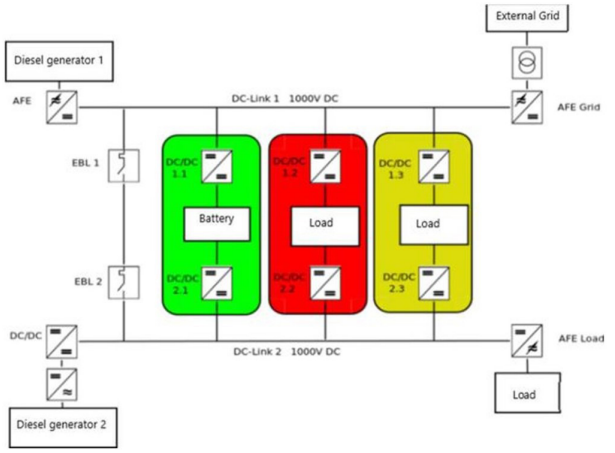

Fig. 11. Zonal DC electrical distribution under study.

after the shut-off of one running DG at t = 35s, and it is evident the failure of the latter due to the intervention of the under-frequency protection (caused by the overload). However, if an additional DG was operating prior to the event (operational-based solution, Fig. 7 and 8), or if a

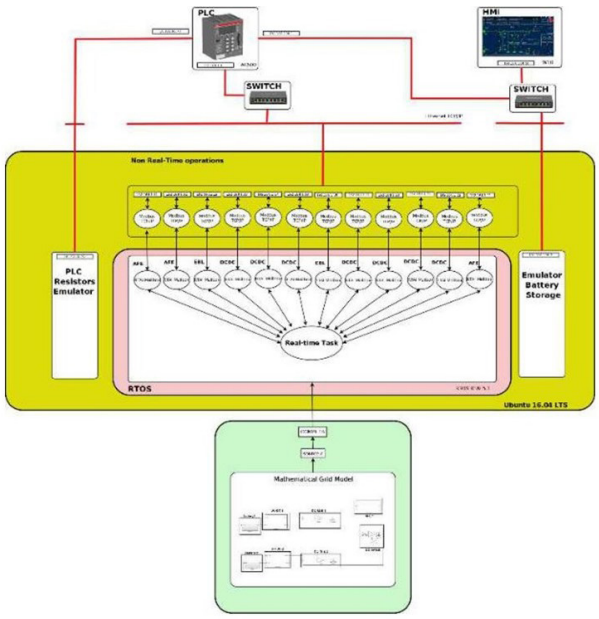

Fig. 12. HIL communication layout: each converter in the mathematical model has its own modbus interface task.

load-shedding function was implemented (control-based solution, Fig. 9 and 10), the system would have survived. It is worth noticing that the former solution does not require any additional action by the PMS, thus being possible also in presence of a fully compromised data communication system. However, it has a significant impact on the physical section, because it leads to increased fuel consumption and running hours for the generators. This example demonstrates how the same cyber-attack can lead to different outcomes depending on the physical system design and operational condition. Moreover, it demonstrates how the use of mathematical modeling can be useful to address the intertwined nature of modern

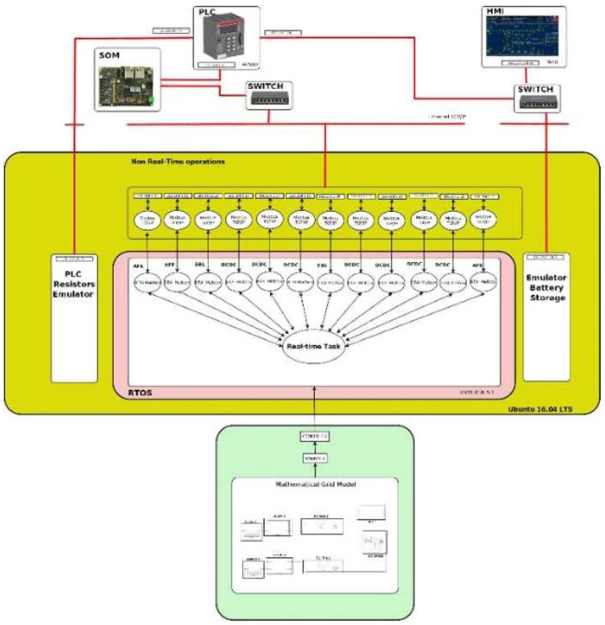

Fig. 13. HIL communication layout with a System on Module attacking in Man in The Middle configuration.

IPSs.

B. Future IPS example

The same approach applied to the actual IPS can be used to study, design, and manage future shipboard power systems. To provide an example, in Fig. 11 a MVDC ZEDS is shown. It consists of two dc buses connected by Electronic Bus Link (EBL), and interfaced with batteries, an electronic load, generators, and an external AC network by means of twelve static converters. A complete mathematical model of the grid has been developed in Matlab Simulink environment, has been translated into a C++ source, and then has been compiled for real-time execution. Each component is simulated by coupling its mathematical model (running in real-time) with a software interface for connecting it to the control system. In the case shown here the latter is a real PMS (implemented by a CPU with suitable onboard software), which communicates using a standardized protocol (e.g., Modbus/TCP or IEC 61850) over an IP network. Each converter therefore has its own IP address and exchange data with the PMS. The simulator scheme is shown in Fig. 12. The built simulator allows applying a classic Man-In-The-Middle attack, as described in [14]. The insertion of a fraudulent device into the network is assumed, and the possibility of manipulating the data is considered, leading to incorrect system operation. The attacking device is implemented with a System on Module (SOM) having two appropriately configured Ethernet cards. The scheme of the attacking action is in Fig. 13. The model allows to evaluate the effect of the attack on the entire physical system, by modifying the data sent from/to the PMS and analyzing the consequent power system behavior for evaluating the various options for enforcing its dependability.

The work towards using the Fig. 13 simulator is in progress, and case studies results will be provided in future publications.

VI. CONCLUSIONS

In this paper an integrated approach for enforcing the dependability of shipboard integrated power system is proposed. By considering both the cyber and physical infrastructures as interrelated, it is possible to determine the performance of the system as a whole. In particular, the cyber originated events are modeled as faults of the physical components, thus enabling their evaluation through power system analysis and simulation tools. Such an approach enables additional degrees of freedom in counteracting malicious actions, being the failure process of the power system a dynamic one. Indeed, the IPS evolution towards a failure takes a variable amount of time (depending on the operating point of the system and on

the specific failure), which can be used to apply corrective measures. Thus, by means of the dynamic simulation results it is possible to determine enforcing actions for the system. These actions can then be focused on the cyber infrastructure, on the physical infrastructure, or on both at the same time.

Additionally, dynamic models of the cyber and physical infrastructures can be used to build a digital twin of the system, which enables continuous system surveillance by providing a tool to identify malicious actions (comparing real system and digital twin behavior in real time).

Massimiliano Chiandone graduated from University of Udine (M.Sc.) in Computer Science and from University of Trieste (B.Sc.) in Electrical Engineering and received a Ph.D. in Electrical Engineering from University of Padua (Italy) in 2012. He has been working for several years at MSC Software Corporation and at the Synchrotron Light Laboratory in Trieste as system administrator and software developer.
His main research interests are in real time control systems.
Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (mchiandone@units.it)

Giorgio Sulligoi (Senior Member, IEEE) received the M.Sc. degree (Hons.) in electrical engineering from the University of Trieste, Trieste, Italy, in 2001, and the Ph.D. degree in electrical engineering from the University of Padua, Padua, Italy, in 2005. He is the Founder and the Director of the Digital Energy Transformation & Electrification Facility, Department of Engineering and Architecture, University of Trieste. He is a Full Professor of Electric Power Generation and Control and an appointed Full Professor of Shipboard Electrical Power Systems. He is the author of more than 100 scientific papers in the fields of shipboard power systems, all-electric ships, generators modeling, and voltage control.
Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (gsulligoi@units.it)

Andrea Vicenzutti received the M.Sc. degree (Hons.) in electrical engineering at the University of Trieste, Trieste, Italy, in 2012, and the Ph.D. degree in industrial engineering from the University of Padua, Padua, Italy, in 2016.
He is currently an Assistant Professor on Power Systems Design with the Department of Engineering and Architecture (DIA), University of Trieste. His research interests include power systems design and dependability, for both marine and land power systems.
Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (avicenzutti@.units.it)

Commander Gianluca Maria Marcilli is graduated in Naval Engineering (M.Sc. Genova University) in 2003 and in Computer Science Engineering (BA - ECAMPUS University, Milan) in 2012. Commanded MARCILLI served aboard Italian Navy ships as Technical Officer and Chief Engineer until 2015. He serves as Specialist Technical Officer in the Italian Naval Directorate since 2015. His main research interests are in Naval Platform Automation, Human Centred Design, Digital Prototyping, Artificial Intelligence and Cyber Security.
CDR MARCILLI's education includes: Master in "Strategic-Military International Studies" (La Sapienza University, Rome - 2016); Master in "Strategic Studies and International Security"(Ca' Foscari University, Venice - 2019); Master in "Digital forensics and Cyber Technologies" (UNIMORE, Modena e Reggio Emilia - 2018). Post graduate courses in "Cyber Analyst" and "Penetration Tester" (UNIMORE 2021).
Directorate of Naval Armaments, Italian Navy, 00175 Roma, Italy (gianlucam.marcilli@marina.difesa.it)

References

[1] A. Vicenzutti, D. Bosich, G. Giadrossi, e G. Sulligoi, «The Role of Voltage Controls in Modern All-Electric Ships: Toward the all electric ship.», IEEE Electrification Mag., vol. 3, n. 2, pagg. 49–65, giu. 2015.
[2] Z. Jin, G. Sulligoi, R. Cuzner, L. Meng, J. C. Vasquez, e J. M. Guerrero, «Next-Generation Shipboard DC Power System: Introduction Smart Grid and dc Microgrid Technologies into Maritime Electrical Netowrks», IEEE Electrification Mag., vol. 4, n. 2, pagg. 45–57, giu. 2016.
[3] V. Arcidiacono; M. Chiandone; G. Sulligoi, "Voltage control in distribution networks using smart control devices of the Distributed Generators" 2011 International Conference on Clean Electrical Power (ICCEP)
[4] McClanahan, «SCADA and IP: is network convergence really here?», IEEE Ind. Appl. Mag., vol. 9, n. 2, pagg. 29–36, mar. 2003.
[5] M. Chiandone e G. Sulligoi, «Energy control in all-electric ship: State of the art and IoT perspectives», in 2017 AEIT International Annual Conference, 2017, pagg. 1–4.
[6] H. Zimmermann, «OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection», IEEE Trans. Commun., vol. 28, n. 4, pagg. 425–432, apr. 1980.
[7] A. Avizienis, J. C. Laprie, B. Randell, e C. Landwehr, «Basic concepts and taxonomy of dependable and secure computing», IEEE Trans. Dependable Secure Comput., vol. 1, n. 1, pagg. 11–33, gen. 2004.
[8] M. Al-Kuwaiti, N. Kyriakopoulos, e S. Hussein, «A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability», IEEE Commun. Surv. Tutor., vol. 11, n. 2, pagg. 106–124, Second 2009.
[9] G. Buja, A. da Rin, R. Menis, e G. Sulligoi, «Dependable design assessment of Integrated Power Systems for All Electric Ships», in Railway and Ship Propulsion Electrical Systems for Aircraft, 2010, pagg. 1–8.
[10] R. Menis, A. da Rin, A. Vicenzutti, e G. Sulligoi, «Dependable design of All Electric Ships Integrated Power System: Guidelines for system decomposition and analysis», in Railway and Ship Propulsion 2012 Electrical Systems for Aircraft, 2012, pagg. 1–6.
[11] A. Vicenzutti; R. Menis; G. Sulligoi "All-Electric Ship-Integrated Power Systems: Dependable Design Based on Fault Tree Analysis and Dynamic Modeling", IEEE Transactions on Trasportation Electrification Vol. 5, Issue 3, September 2019
[12] A. Boveri, F. D'Agostino, A. Fidigatti, E. Ragaini and F. Silvestro, "Dynamic Modeling of a Supply Vessel Power System for DP3 Protection System," in IEEE Transactions on Transportation Electrification, vol. 2, no. 4, pp. 570-579, Dec. 2016
[13] G. Sulligoi, D. Bosich, A. Vicenzutti, L. Piva, G. Lipardi and T. Mazzuca, "Studies of electromechanical transients in FREMM frigates integrated power system using a time domain simulator," in IEEE Electric Ship Technologies Symp., Arlington, USA, 22-24 April 2013
[14] H. Palahalli, M. Hemmati and G. Gruosso Analysis of Cyber Security Threat of using IEC61850 in Digital Substations involving DERMS