The threat of Intentional Electromagnetic Interference to Maritime Vessels

F R Arduini[a*], CJJ van der Ven[b*], M Lanzrath[a*], Dr, M Suhrke[a*], Dr.

[a]*Fraunhofer Institute for Technological Trend Analysis INT, Germany;* [b]*RH Marine, Netherlands*

*Corresponding author. Email: fernando.Ribeiro.Arduini@int.fraunhofer.de

Synopsis

Known as Intentional Electromagnetic Interference (IEMI), perpetrators employ electromagnetic sources to intentionally disrupt, deceive or damage electronic devices by broadcasting or injecting disturbance signals. Modern ships are vulnerable to IEMI as they increasingly rely on electronic devices for their power, control, communication, and navigation systems. The prolonged disruption of the Global Positioning System (GPS) would bring huge financial losses to the maritime sector, for example. Given the wide range of attack possibilities employing electromagnetic interference, this paper discusses and contrasts different IEMI threats for the maritime application, divided here into jamming, spoofing, and use of high-power electromagnetic (HPEM) sources. For the case of HPEM, this paper proposes a simplified model to estimate the field strength at targeted electronics part of ships for HPEM weapons located in vicinities. Finally, this paper also presents guidelines oriented for stakeholders in the maritime sector on how to increase the IEMI security level of their assets.

Keywords: IEMI; Security; Jamming; Spoofing; HPEM; Maritime vessels; Ships; Critical Infrastructure

1 Introduction

The increased penetration and reliance on Smart Electronic Devices (SEDs) in Critical Infrastructures (CIs) have raised the number of potential gateways for attacks intended to cause service interruption. Under this scope, a threat that is growing in concern by experts and entities worldwide is the use of Intentional Electromagnetic Interference (IEMI). In this threat, perpetrators employ electromagnetic interference to disrupt, deceive or damage electronics of critical assets LANZRATH, SUHRKE and HIRSCH (2019). Considering the power and communication system onboard ships, electromagnetic disturbance can affect a vessel by two coupling means. On the one hand, IEMI attacks can be front-door, where the electromagnetic disturbance signals use ports especially made to propagate Radiofrequency (RF) signals between devices and the external environment (e.g., antennas). On the other hand, the attacks can be back-door, where the electromagnetic disturbance signals employ coupling paths not intended for communication with the external environment (e.g., power and communication cables, drain and ventilation openings, and shielding structure imperfections) BÄCKSTRÖM (2006).

From the perspective of front-door IEMI attacks, the Global Navigation Satellite System (GNSS) is one of the most relevant attack points. The Position, Navigation, and Timing (PNT) information provided by GNSS has been crucial to many critical systems on board ships, allowing receivers to determine a vessel's location accurately. As an example of its importance, an investigation by the UK government in 2017 found that a five-day GNSS outage would cost the British maritime economy over a billion pounds, highlighting the fundamental value of this system in the maritime sector LE (2017). The forms of front-door IEMI attacks on GNSS signals are typically divided into jamming and spoofing. A jamming attack intentionally directs electromagnetic waves towards a victim GNSS receiver to disrupt its function. On the other hand, a spoofing attack transmits false GNSS-type signals to produce a false position perceived by the target receiver without interrupting its operation HU et al. (2018).

Besides spoofing and jamming, another IEMI threat to maritime vessels is High Power Electromagnetic (HEPM) sources. HPEM attacks can be both front-door and back-door. In the front-door form, HPEM can affect GNSS receivers and other onboard electronics through antennas, and represents a jamming threat involving higher power sources. In back-door form, HPEM can affect the internal components of any electronic through cables, apertures and shielding imperfections within a vessel. The HPEM weapons have several technology variations and are flexible to be mounted on different means of transport, such as a suitcase, a car, or even a maritime vessel MORA et al.

Authors' Biographies

Fernando Ribeiro Arduini (MSc) works as an associate researcher at Fraunhofer INT and is a PhD student at Leibniz University Hannover. His research interests include smart grid technologies, power systems, security of critical infrastructures and risk management of cyber and electromagnetic threats.

Jan-Kees van der Ven graduated in Mechanical Engineering with Energy Science as main subject. He has worked for various railway related companies as an EMC specialist and has been an Technical Consultant for RH Marine Netherlands for 16 years now. He is an active member of IEC – TC 18 (Electrical installations of ships and of mobile and fixed offshore units) and chairman of the Dutch EMC-ESD society.

Marian Lanzrath (Phd) is the head of the business unit electromagnetic effects and threats at Fraunhofer INT in Euskirchen, Germany. His research interests include the HPEM vulnerabilities of electronic devices and complex systems as for example critical infrastructures especially power grids.

Michael Suhrke (Phd) holds a PhD in Physics (1985, Humboldt University Berlin) and Habilitation in Physics (1997, University Regensburg). Until his retirement in 2022, he was the head of the business unit Electromagnetic Effects and Threats at Fraunhofer INT, which he joined in 2002. He is a Senior Member of IEEE and an HPEM Fellow of the US-American SUMMA foundation.

 https://doi.org/10.24868/10723

(2014). Therefore, the risk management process is particular for each sector to be evaluated since the threat scenarios may vary accordingly to the different HPEM sources and the target environment. In the context of offshore CIs, such as energy and airport infrastructures, the risk of HPEM has been investigated in recent years LANZRATH, SUHRKE and HIRSCH (2019); KRETH et al. (2012). However, there is no evidence in the scientific literature of studies covering this threat to maritime vessels.

Given the possibilities of exploiting electromagnetic interference to target CIs, this paper discusses and contrasts the different IEMI threats to the maritime application. These threats are here divided into jamming, spoofing, and the use of HPEM sources. Under this scope, they are described by enlightening information regarding the technological levels of each threat, the potential attack gateways on a vessel, and the expected effects on target systems. For the case of HPEM, the contribution of this paper is extended to propose a simplified model to estimate the field strength at critical electronic systems belonging to maritime vessels from HPEM weapons located in the vicinity. Finally, once the potential risks of jamming, spoofing, and HPEM sources are described, this paper presents basic guidelines oriented to maritime stakeholders on protective measures to ensure the security of their assets to IEMI.

2 IEMI Risk Management Approach

The risk of electromagnetic attacks on CIs can only be recognized and mitigated if a risk management process is applied. The International Organization for Standardization (ISO) specifies a risk management process that can be applied to any risk, regardless of its nature. Therefore, under the ISO 31000:2009 standard ISO (2009), this process follows a set of tasks, as shown in Figure 1. Detailed information on each step of this process can be found in SABATH (2017).

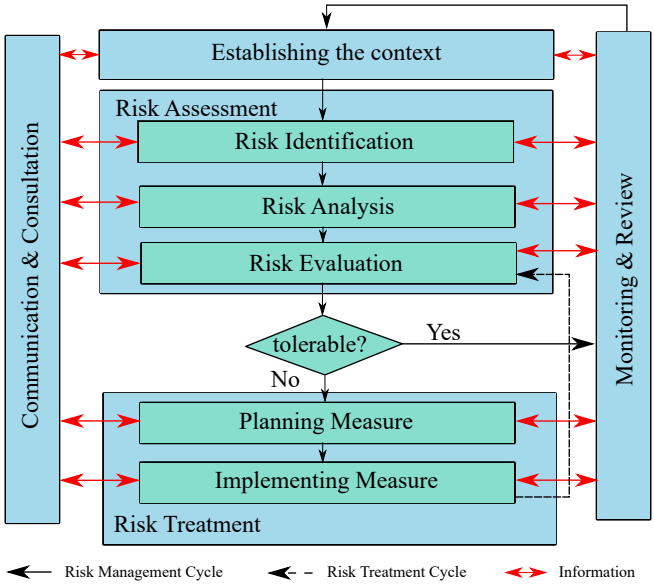

Figure 1: Risk Management Process SABATH (2017).

The IEMI risk to the ship can arise in several forms depending on the sector considered. This paper aims to describe these forms for the application of maritime vessels as a way to contribute to the *Risk Identification* step. Furthermore, possible mitigation approaches for these threats are outlined as an input for the *Risk Treatment step*.

3 IEMI Threats to Maritime Vessels

The intentional use of electromagnetic interference to affect maritime systems can be accomplished in three ways: jamming, spoofing, and deployment of High-Power Electromagnetic (HPEM) sources. Jamming and spoofing generally employ low-power interference sources, while HPEM attacks involve high-power means. The following subsections detail each IEMI threat with a particular focus on maritime vessels.

3.1 Jamming

Today's maritime vessels rely heavily on Global Navigation Satellite System (GNSS) for safe operations. While GPS (USA) is the most prevalent GNSS within the maritime and other sectors, other nations have their own systems to provide complementary and independent PNT capability. The other main GNSSs include Galileo (EU), GLONASS (Russia), and BeiDou (China). Under the scope of ship applications, GNSS is employed for open

 https://doi.org/10.24868/10723

sea navigation, harbor approaches, vessel positioning monitoring, and situational awareness involving obstructions and other vessels at sea. This high dependency, however, has raised concerns about the vulnerability of these satellite-based systems to electromagnetic interference.

Given the high dependency on satellite-based systems, concerns have been raised about the vulnerability of GNSS to electromagnetic interference. The strength of GNSS signals transmitted from satellites to the earth's surface reaches receivers at very weak levels. According to IDC-GPS-200 FYFE, KOVACH and NAVSTAR (1991), the transmission power of the main GPS carrier signals, L1 (1575.42MHz) and L2 (1227.6 MHz), is guaranteed at the earth's surface with minimum power levels below - 166 dBW. Thus, GNSS receivers of maritime vessels can suffer Denial of Service (DoS) by in-band interference signals that overpower the legitimate signals coming from the satellites. Such RF interference is generally unintentional but can also be deliberately generated by individuals with criminal intent.

The probability of detecting GPS signals is proportional to the carrier-to-noise ratio C/N0. The goal of an intentional jammer is to increase the noise level at the operational frequency of the GPS in order to prevent that the GNSS receiver detects the intended signal LUBBERS (2015). Figure 2 illustrates a scenario where a vessel carrying a GPS-based system is targeted by a jammer located on a smaller vessel. In this case, prior to the attack, the vessel navigates according to GPS coordinates. However, it stops acquiring GPS signals once the jammer on the perpetrator's boat overpowers the legitimate signals coming from the satellites. In this scenario, the jamming source is mounted on a small mobile boat located close to the target system on the high seas. However, a static jammer could also be located several kilometers away (e.g., coastline, cliff) and still affect the vessel.

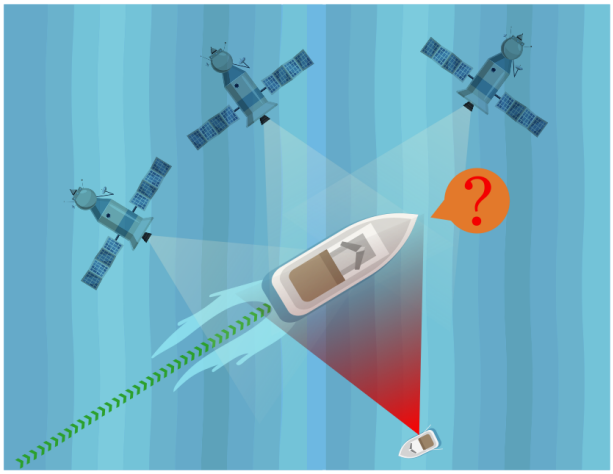

Figure 2: Jamming as an IEMI threat.

The results of the GILMORE and DELANEY (1994) experiments indicated that a 1 W power jammer could disturb the GPS receivers located within a distance of 85 km. Similarly, the same jamming attack attempt could affect multiple vessels. In recent years, North Korea has been accused of producing jamming signals near its border with South Korea in order to affect South Korean naval and air traffic. As a result, although many vessels and aircraft had their navigation units exposed, most were only indirectly affected, given they had other means of navigation not vulnerable to jamming, such as the Inertial Navigation System (INS). Even so, at least 70 fishing vessels were forced to go back into port due to GPS navigation problems JANJEVIC (2016).

In addition to satellite-based systems, naval vessels have other means of navigation to ensure safer navigation. In addition to INS, these include techniques free of jamming effects such as dead reckoning and echo sounders. However, given the greater reliance on satellite navigation and accuracy, the inability of a vessel's crew to identify a jamming attack and fall back on traditional means of navigation can make DoS of GNSS signals a safety issue. In the occurrence of GPS signal interruption, alarms linked to the failure of different functions dependent on GPS coordinates can sound simultaneously and create a stressful situation in the crew, as shown in the study of GRANT et al. (2019). In these conditions, a significant impact on the crew's safety can arise, especially if the attack occurs when the vessel is performing a highly precise maneuver, such as docking in poor light and visibility conditions (e.g., during a storm or foggy night). Thus, although the vessels have redundant navigation aids, the impact of disrupted satellite navigation aids can have significant consequences.

A basic jammer consists of a signal generating source, a power amplifier, an RF signal transmitter, and an antenna. However, there are also more robust devices, such as those containing frequency sweep features, that prevent many standard GNSS receiver interference mitigation techniques from working GAO et al. (2016). In general, bandwidth-based GPS jammers technologies are classified into three types, represented by continuous

 https://doi.org/10.24868/10723

wave, narrowband and broadband WANG (2022). Internet searches for these devices show that they are widely available on online marketplaces. On the other hand, there are several online tutorials on how to build self-made jammers with basic components, which any individual with minimal knowledge of electronics can run. Some websites indicate that the purchase and use of these devices violate federal law, but other websites do not even mention this information IET (2016).

3.2 Spoofing

Transmitting false GNSS-type signals to cause receivers to wrongly compute positions required expensive hardware and could only be performed by RF specialists. Nevertheless, following the introduction of low-cost, software-defined RF signal generators, widespread concern about spoofing attacks on GNSS-dependent systems has been flagged as a security threat. Although there are highly sophisticated military-grade GNSS spoofing sources, low-cost spoofers can nowadays be assembled by perpetrators with minimum RF knowledge. For example, a basic spoofer, consisting of a Software-Defined Radio (SDR) device, a mobile phone battery, and an antenna, can be built for less than 220 euros. For this purpose, tutorials on how to mimic satellite signals with SDR devices are publicly available online GITHUB (2016).

Assuming that a vessel follows a route set by the GPS in automatic mode, Figure 3 illustrates a scenario where a spoofing attack targets a vessel. In this scenario, a spoofer is located on a small boat, which follows the navigation course of the target vessel. The attack starts when the perpetrator transmits counterfeit signals initially synchronized with the genuine GPS signals acquired by the target GNSS antenna. At a certain point, the power of the spoofed signals is gradually increased until the GNSS receiver acquires them instead of the legitimate signals. Once the receiver is taken over, the perpetrator applies small increments to the target's positioning, causing the vessel to drift off its planned course. This form of spoofing is termed "carry-off". Its consequences include collisions, blocked navigation routes, and even piracy attempts. Nevertheless, despite the high risk, "carry-off" attack spoofing attempts require a high technical level of expertise to be accomplished without being detected by the basic anti-spoofing algorithms found in some GNSS receiver technologies MADRY (2015).

Meaconing is another type of spoofing that requires less technological challenge for the perpetrator. In this form of spoofing, GPS signals are not created with manipulated information but only re-transmitted from a receiver located elsewhere, which could be, for example, another vessel nearby. To this end, the broadcast signals are generally amplified to reach the target GNSS antenna with adequate power levels for acquisition. Although unintentional, there has already been one recorded incident of meaconing that has raised concerns about this threat. In this instance, GPS repeaters used in indoor aircraft hangars unintentionally transmitted their signals to the outside and triggered ground proximity warnings during aircraft take-offs APPEL, HORNBOSTEL and HÄTTICH (2014).

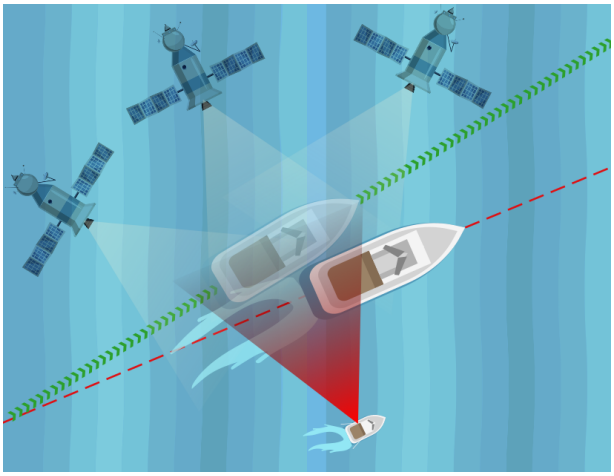

Figure 3: Spoofing as an IEMI threat.

Although jamming and spoofing target GNSS systems, the technical complexity and motivation behind these IEMI threats differ. On the one hand, if the attacker aims to avoid discontinuity in a spoofing "carry-off" attack, he must synchronize the spoofed signal with the genuine signal. To achieve this, the attacker must find a satisfactory way to ascertain and track the location of the target receiver. On the other hand, a jamming attack does not necessarily need information about the target and reaches its ultimate goal only by overpowering the genuine GPS signals. Therefore, coordinating and carrying out a spoofing attack demands a much higher technical grade and engagement from the perpetrator than a jamming attack, especially in an intentional covert context. In light of this,

 https://doi.org/10.24868/10723

an additional characteristic of spoofing is that its effects are less evident than jamming attacks, which can delay the possible detection of an attack.

3.3 HPEM

High-power electromagnetic weapons (HPEM) pose a greater threat to maritime vessels in the sense that there are more attack gateways within a vessel. Unlike jamming and spoofing, where targets are mainly GNSS systems, the HPEM threat can compromise any electronic device in a vessel's power, communication, and automation systems. From a CI perspective, although attacks involving HPEM weapons have a relatively low probability of occurrence, the consequences of such attacks can be highly severe for two main reasons. First, the consequences can vary from interference, DoS, to destruction of electronic devices that perform mission-critical functions SABATH (2010). Second, a single attack attempt can affect multiple devices, whose simultaneous failures can trigger adverse system-level effects. Even so, the HPEM threat is still commonly overlooked in CI security plans. One reason for this decision is that there are few publicly disclosed incidents of HPEM attacks, which makes stakeholders believe that this threat is not a priority security issue for their CIs.

HPEM sources can couple electromagnetic disturbances in two modes known as radiated and conducted coupling. In the first mode, the disturbance signal is radiated over the air to reach the internal electronics of a target system. In contrast, in the second mode, the propagation of the disturbance signal is carried out through wires connected to the target system. Regarding bandwidth, the most common types of HPEM sources are narrowband, Ultra-Wideband (UWB), and damped sinusoidal. Apart from the features mentioned above, they can also have different degrees of technological challenge directly related to the assembling technical complexity and component availability. Moreover, depending on the components' arrangement, they can be big enough to require transportation by truck or small enough to fit in a briefcase LUGRIN (2013). An example of a commercial HPEM source is the suitcase-shaped DS110 produced by DIEHL from Germany. It consists of a High Voltage (HV) power supply, a MARX generator, and an adjustable self-resonant antenna. The DS110 has a peak power of 250 MW and emits field strengths of 125 kV/m at 1 meter from the antenna EREN (2021). Therefore, even if the DIEHL was used at a great distance from target onboard electronics, it could still cause interference given many of those electronics are typically designed to withstand field strengths of only 10 V/m.

Figure 4 exemplifies a scenario of a radiated HPEM attack on a maritime vessel. The HPEM source is mounted on a small boat and employs an antenna to interfere with the target vessel. In this case, the perpetrators could manually direct the antenna towards the system to be hit. The target could be, for example, the communication antennas located on the deck, the main switchboard protection system on the lower deck, the bridge on the upper deck, among other points of attack. In contrast to the numerous possibilities of radiated HPEM attack gateways, assuming the perpetrator never gets access inside the vessel, conducted attacks are limited to a single scenario. This scenario is represented when the vessel is charging with shore power and an perpetrator injects disturbance signals into the vessel's cabling, which is connected to the power station. For this case, the risk is generally considered low as most vessels have isolation transformers between their internal circuits and the shore installation, which is a great attenuating medium for electromagnetic interference.

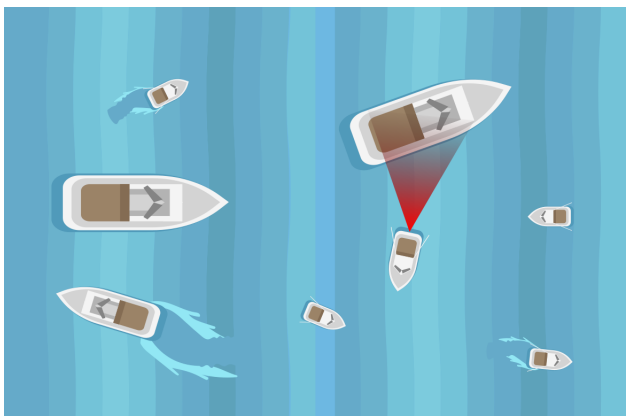

Figure 4: HPEM as an IEMI threat.

3.4 HPEM propagation model

The model *Source* $\Rightarrow$ *Coupling Path* $\Rightarrow$ *Protection* $\Rightarrow$ *Receiver* represent the process of an HPEM attack. The aforementioned items can be detailed as follows:

 https://doi.org/10.24868/10723

1. *Source*: Emitter of radio frequency (RF) signals.
2. *Coupling Path*: Propagation medium of radiated or conducted RF signals between the source and the receiver.
3. *Protection*: EMC countermeasures to attenuate the undesired RF signals between the source and the receiver.
4. *Receiver*: Electronic device affected by the RF signals coming from the source

The field strength at a target system inside a vessel originated from a radiated HPEM source can be estimated based on all relevant influences in the path of the interference signal. Figure 5 presents an adaptation of the generic power substation model proposed by LANZRATH, SUHRKE and HIRSCH (2019) for the application of maritime vessels. In the given scenario, a car-mounted HPEM source is located near a harbor where a target ship is docked. The source irradiates the vessel targeting sensitive critical electronic systems placed in the lower deck control room. The ship has a hull, walls, and surrounding objects that reduce the attenuation of the electromagnetic interference to the target system. As the arrangement of components and the ship layout vary widely, the distance from the HPEM source to the target system varies accordingly. Hence, the expected field strength at the target system position (E_T^{rad}) according to the peak field strength of an emitting source (E_S^{rad}) is given by Equation 1 in logarithmic scale.

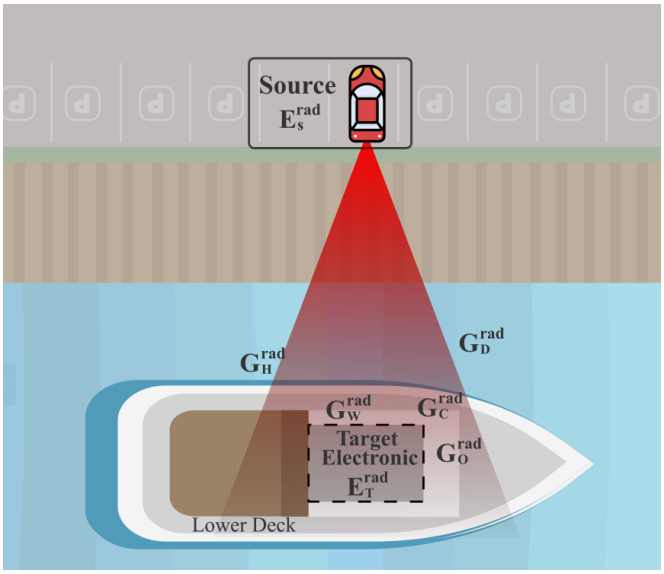

Figure 5: RF propagation model.

$$E_T^{rad} = E_S^{rad} - G_D^{rad} - G_H^{rad} - G_W^{rad} - G_O^{rad} - G_C^{rad} \tag{1}$$

where the subtracted elements in 1 represent the attenuation of the emitted signal from the source to the receiver inside the ship. Under far-field conditions, the EM field decreases with 1/r along the propagation path, so G_D^{rad} represents the attenuation due to distance. The attenuation of the vessel's hull is represented by G_H^{rad}. The EM shielding provided by the internal walls is represented by G_W^{rad}. In the G_0^{rad} term, the attenuation of engines and other objects is summarized. EM protections, in turn, are represented by G_C^{rad}.

Based on this model and assuming direct coupling on the target electronics, a first insight into the risk of radiated HPEM attacks on maritime vessels can be provided quickly and economically. For this purpose, E_T^{rad} has to be compared with the failure thresholds of the targeted electronic device. Moreover, different HPEM sources can be considered in the analysis. Information of E_S^{rad} for some HPEM sources can be found in MORA et al. (2014).

4 Mitigation measures

Table 1 represents some measures to protect maritime vessels against IEMI. Some of them apply to more than one IEMI threat (e.g. jamming and spoofing), others are unique to a particular type. The criteria of which measures should be applied, as well as their technical specifications, are directly related to the ship being considered in the risk management process. For each strategy, a bibliographic reference is provided for further information.

 https://doi.org/10.24868/10723

Table 1: Countermeasures against jamming, spoofing and HPEM.

Countermeasure	Description	Reference	Threat		
			Jamming	Spoofing	HPEM
Inertial Measurement Units (IMUs)	The use of IMUs represents one approach to promoting PNT backup. A basic IMU is composed of accelerometers, gyroscopes, and magnetometers. These devices measure the motion of a vessel without any external reference and can fill gaps from seconds to a few minutes in case of a GNSS outage. However, this strategy should not be used alone because IMU measurements drift over time and become inaccurate quickly.	ROGNE et al. (2016)	✓	✓	
Multi-constellation receivers	Multi-constellation receivers that can simultaneously track GPS and other GNSS systems, such as GLONASS, Galileo, and BeiDou, can hinder jamming and spoofing attempts. A successful attack would be extremely difficult in such a case since the perpetrator would have to jam or spoof all GNSS signals simultaneously.	STENBERG (2019)	✓	✓	
Adaptive Array Antenna	Controlled Receive Pattern Antennas (CRPAs) employ intelligent signal processing algorithms to mitigate all types of electromagnetic interference. These antennas can distinguish the direction from which an interfering signal is coming and create a lower gain receiving pattern in that direction. In this way, a receiver can be protected from disturbances coming from the perpetrator's location, even if the interfering signals are within the target system's frequency band.	SPIRENT (2019)	✓	✓	✓
External PNT software	Flywheel algorithms can be employed to alert the crew and forbid immediate jumps in the location and time information captured by a GNSS receiver.	INTERTANKO (2019)		✓	
E-Loran	Enhanced LORAN, also known as eLORAN, is a low-frequency radio navigation system operating in the 90 to 110 Hz frequency range. Since it is a station-based system, transmission power levels are much higher than GNSS, making this navigation system less susceptible to interference and spoofing. However, unlike GPS, eLoran does not offer global coverage. In this case, for vessels navigating solely in areas covered by eLoran, combining both systems could increase PNT resilience.	SON (2020)	✓	✓	
Filters	One of the most classical approaches against any kind of electromagnetic interference is filtering power and communication lines entering cabinets, as well as received signals from antennas. However, this approach is only effective for filtering out-of-band signals. As an example, in case an interference signal falls directly in-band, it might still overpower a GNSS receiver in case of a jamming attack.	OZENBAUGH (2000)	✓	✓	✓
RF shielding	Isolated critical electronics can be shielded in fully enclosed, highly conductive, grounded metal racks. Alternatively, a set of critical electronics can be concentrated in a fully shielded room.	RADASKY (2015)			✓
Control of apertures and vents	Shielding-based measures should be aligned with adequate control of apertures and penetrations to ensure that interfering signals from the vessel's external environment reach the internal environment with negligible power levels. For windows, the countermeasures include thin conductive coatings and wire mesh embedded in glass. For vents, mesh screens and honeycomb panels are recommended.	KUNKEL (2020); FENICAL (2006)			✓
Electromagnetic resilience approaches	Several approaches established by IEEE Standard P1848 to increase electromagnetic resilience could be applied to the power system of vessels. Some of these include: Employment of different hardware backup systems; Data transmission via multiple channels; Different sensors measuring the same parameter; Providing independent power supplies to critical electronics.	IEEE (2020)	✓	✓	✓
Constructional measures	One of the most economical and simple measures to prevent HPEM attack attempts is to increase the distance between potential HPEM sources and critical electronics. Aligned to this, it is known that ships naturally have natural obstacles that can attenuate electromagnetic radiation. While these obstacles cannot guarantee professional RF shielding, they can provide additional attenuation to critical electronics. At the design phase of maritime vessels, it is therefore desirable that critical electronics are arranged considering the vessel's natural obstacles and as far as possible from the vessel's hull.	PUSCH, LANZRATH, SUHRKE (2019)			✓
Crew's training	Awareness of IEMI attacks can facilitate the vessel's crew to identify attack attempts and make quick and accurate decisions in case the vessel is successfully targeted. In general, such training should provide an overview of the types of IEMI sources, how jamming, spoofing, and HPEM attacks can be carried out, the likely effects on onboard systems, and the countermeasure plans to be implemented in the event of such incidents.	PUSCH, LANZRATH, SUHRKE (2019)	✓	✓	✓

 https://doi.org/10.24868/10723

5 Conclusion

Successful IEMI attacks on maritime vessels can cause massive economic losses and compromise the safety of individuals onboard ships. This paper discussed the different forms of the IEMI threat to ships to raise awareness of the maritime community. Under these different forms, jamming signals can overpower GNSS signals, resulting in a DoS of PNT information. In spoofing attacks, transmitting GNSS-like signals can result in the vessel's false perception of position and divert its intended course. In HPEM attack attempts, high-power interference can covertly cause interference, DoS, or even damage to critical onboard electronics.

Given these threats, IEMI attacks should be treated as a relevant security issue in the maritime sector. The risk of such attacks is not only related to the perpetrator's intention but also to the different types of IEMI weapons and the particularities of each vessel. These particularities include, for example, the attenuation levels offered by a ship, as shown in the proposed RF propagation model. In order to ensure the safety of maritime vessels, IEMI risk management processes should be carried out. As a contribution to the risk treatment step, this paper summarized different possibilities of mitigation measures that maritime stakeholders could implement to protect their assets.

Acknowledgement

The research leading to these results has received funding from the European Union´s Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 812790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

References

SABATH, Frank. A Systematic Approach for Electromagnetic Interference Risk Management. IEEE Electromagnetic Compatibility Magazine, v. 6, n. 4, p. 99-106, 2017.

LANZRATH, Marian; SUHRKE, Michael; HIRSCH, Holger. HPEM-based Risk Assessment of Substations Enabled for the Smart Grid. IEEE Transactions on Electromagnetic Compatibility, v. 62, n. 1, p. 173-185, 2019.

FYFE, Peter; KOVACH, Karl. Navstar GPS Space Segment/Navigation User Interfaces (public release version). RESEARCH CORP FOUNTAIN VALLEY CA, 1991.

WANG, Jia et al. Impacts of GPS Spoofing on Path Planning of Unmanned Surface Ships. Electronics, v. 11, n. 5, p. 801, 2022.

LUBBERS, Barend et al. A Study on the Accuracy of GPS Positioning during Jamming. In: 2015 International Association of Institutes of Navigation World Congress (IAIN). IEEE, 2015. p. 1-6.

GILMORE, S. W.; DELANEY, W. Jamming of GPS Receivers: A stylized analysis. Project Report, Lincoln Laboratory, 1994.

JANJEVIC, D. (2016, Abril 4). Pyongyang Jams GPS signal Over South Korea. DW. https://www.dw.com/en/pyongyang-jams-gps-signal-over-south-korea/a-19157414.

GAO, Grace Xingxin et al. Protecting GNSS Receivers from Jamming and Interference. Proceedings of the IEEE, v. 104, n. 6, p. 1327-1338, 2016.

APPEL, Manuel; HORNBOSTEL, Achim; HÄTTICH, Christian. Impact of Meaconing and Spoofing on Galileo Receiver Performance. 2014.

IET. (2018, March) Jamming Radio Interference: Understanding the Impact. Instition of Engineering and Technology.https://www.theiet.org/media/8779/jamming-and-radio-interference.pdf.

GRANT, Alan, et al. GPS Jamming and the Impact on Maritime Navigation. The Journal of Navigation, 2009, 62. Jg., Nr. 2, S. 173-187

MORA, Nicolas et al. Study and Classification of Potential IEMI Sources. System design and assessment notes, v. 41, n. ARTICLE, 2014.

GITHUB. (2018, September) GPS-SDR-SIM.https://github.com/osqzss/gps-sdr-sim.

MADRY, Scott. National and International Governmental Policy Issues. In: Global Navigation Satellite Systems and Their Applications. Springer, New York, NY, 2015. p. 83-91.

EREN, Özge. (2021). Investigation and Design of Impulse Radiating Antennas Driven with Marx Generator (Master's thesis, Middle East Technical University).

LUGRIN, Gaspard et al. Overview of IEMI Conducted and Radiated Sources: Characteristics and Trends. In: 2013 International Symposium on Electromagnetic Compatibility. IEEE, 2013. p. 24-28.

LONDON ECONOMICS . (2017, Abril) The Economic Impact on the UK of a Disruption to GNSS .https://londoneconomics.co.uk/wp-content/uploads/2017/10/LE-IUK-Economic-impact-to-UK-of-a-disruption-to-GNSS-FULLredacted-PUBLISH-S2C190517.pdf

BÄCKSTRÖM, Mats G. The threat from intentional EMI Against the Civil Technical Infrastructure. In: Reprint from ESW2006, 3rd European Survivability Workshop. 2006. p. 16-19.

HU, Yanfeng et al. A Novel Array-based Spoofing and Jamming Suppression Method for GNSS Receiver. IEEE Sensors Journal, v. 18, n. 7, p. 2952-2958, 2018.

KRETH, Adrian et al. Identifying Electromagnetic Attacks Against Airports. In: 2012 ESA Workshop on Aerospace EMC. IEEE, 2012. p. 1-5.

SABATH, Frank. Classification of Electromagnetic Effects at System Level. In: Ultra-Wideband, Short Pulse Electromagnetics 9. Springer, New York, NY, 2010. p. 325-333.

ROGNE, Robert H. et al. MEMS-based Inertial Navigation on Dynamically Positioned Ships: Dead reckoning. IFAC-PapersOnLine, v. 49, n. 23, p. 139-146, 2016.

STENBERG, Niklas. Spoofing Mitigation Using Multiple GNSS-Receivers. Master's thesis. Linköping University. 2019.

INTERTANKO . (2019) Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

IEEE. 1848-2020 - IEEE Standard for Techniques and Measurement to Manage Functional Safety and Other Risks with Regards to Electromagnetic Disturbances , June 2020, pp. 1–164, 2020.

PUSCH, Thorsten; LANZRATH, Marian; SUHRKE, Michael. IEMI Resilience Assessment of Critical Infrastructures. In: 2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE. IEEE, 2019. p. 1132-1137.

KUNKEL, George M. Shielding of Electromagnetic Waves. Springer International Publishing, 2020.

FENICAL, Gary. New developments in Shielding Materials. In: 2006 IEEE Long Island Systems, Applications and Technology Conference. IEEE, 2006. p. 1-5.

RADASKY, W. A. The Role of Electromagnetic Shielding in Dealing with the Threat of Intentional Electromagnetic Interference (IEMI). In: 2015 International Conference on Electromagnetics in Advanced Applications (ICEAA). IEEE, 2015. p. 1145-1148.

SPIRENT . (2019) Characterising CRPAs and other Adaptive antennas. https://www.nubicom.co.kr/download/download.jsp?file_name=spirent/GNSS/39N.GSS9790.pdf

OZENBAUGH, Richard Lee; PULLEN, Timothy M. EMI filter design. CRC press, 2000.

SON, Pyo-Woong et al. eLoran: Resilient Positioning, Navigation, and Timing Infrastructure in Maritime Areas. IEEE Access, v. 8, p. 193708-193716, 2020.

ISO. ISO 31000: 2009: Risk Management: Principles and Guidelines. International Organization for Standardization, 2009.

 https://doi.org/10.24868/10723