Methodology to Heighten Resilience in Critical Maritime Infrastructure

1st Manuel Schaefer
Institute for the Protection of Maritime Infrastructures
German Aerospace Center - DLR
Bremerhaven, Germany
manuel.schaefer@dlr.de

2nd Arto Niemi
Institute for the Protection of Maritime Infrastructures
German Aerospace Center - DLR
Bremerhaven, Germany
arto.niemi@dlr.de

3rd Frank Sill Torres
Institute for the Protection of Maritime Infrastructures
German Aerospace Center - DLR
Bremerhaven, Germany
frank.silltorres@dlr.de

***Abstract*—This paper proposes a methodology that combines proven techniques from business continuity management and resilience concepts, to enhance resilience in critical maritime infrastructure. Initially, a vulnerability analysis process is implemented through the utilization of a Business Impact Analysis (BIA) and a comprehensive risk assessment. BIA detects critical business processes, single points of failure, and the interconnections among these vulnerabilities. The risk assessment identifies and appraises risks. It takes into account both their likelihood of occurrence and their prospective severity. Following the vulnerability analysis, a resilience plan is established in order to define adequate resilience measures. To address the diverse domains of resilience, our strategy is compartmentalized into preventive measures, damage mitigation measures, crisis management, and a restoration plan. In this manner, all distinct stages can be systematically addressed.**

***Index Terms*—resilience, critical maritime infrastructure, Business Continuity Management, EU CER**

I. Introduction

In recent times, global uncertainty has grown back to an almost forgotten extent, while Europe is witnessing a significant increase in hybrid warfare attacks. Especially in the offshore area, like the destruction of Nord-Stream in Germany [1], the increased military presence of Russia in the North Sea [2] or the cuttings of multiple seabed cables [3]. These threats demand enhanced resilience of Critical Maritime Infrastructure (CMI) to protect socio-economic safety and security. The EU recognized this need in the EU Critical Entity Resilience (CER) Directive (EU 2022/2557) [4], enacted in 2022. The directive obliges critical-infrastructure operators to implement extensive resilience measures. We propose a framework for CMI operators that integrates established Business Continuity Management (BCM) and resilience-engineering methods, moving beyond purely risk-based resilience.

In this paper, we consider the following classes of CMI: Seabed Power-Cables, Seabed Data-Cables, Pipelines, Shipping Lanes, Offshore Wind Farms and Ports. Maritime infrastructure as a whole contains multiple classes of different infrastructure types. The criticality of the infrastructure is defined within the national execution of the CER directive. For example in Germany, energy infrastructure is considered critical, if its capacity reaches a defined threshold [5].

Our framework is composed of a vulnerability analysis (section II) and a resilience plan (section III). The vulnerability analysis, in turn, is composed of two basic components: a business impact analysis and a risk assessment. That way, critical processes and resources can be detected in the first step. Possible risks can be identified and assessed in the second step. After assessing the threats, adequate measures are defined in the resilience plan. These resilience measures are subdivided into preventive measures, damage mitigation measures, crisis management, and restoration plan. By defining adequate measures in all four of those stages, a comprehensive resilience plan is created. That way, the methodology proposed in this paper can heighten resilience in critical maritime infrastructure. However since this is a brief proposal, not all details are included here. The limitations, as well as the work that still needs to be done to refine this methodology, are discussed in the outlook in section IV.

II. Vulnerability Analysis

The first phase of the proposed methodology, comprising a Business Impact Analysis (BIA) and a Risk Assessment, evaluates critical processes. It also identifies and assesses risks.

A. Business Impact Analysis

The BIA is an established BCM technique that identifies time-critical processes, single points of failure, bottlenecks, and their interconnections. Here we give a brief summary of the BIA. ISO 22301 [6] provides a detailed rationale for the BIA. Comprehensive guidance is available in ISO 22317 [7] and a book [8]. For CMI, the emphasis should shift from purely monetary risk to socio-economic risk because operators have a societal duty to maintain everyday functions.

The first BIA step identifies time-critical processes. Examples for time-critical processes in CMI are data or energy transportation, monitoring and identification of faults, maintenance, repair and communication.

Next, infrastructure dependencies are mapped, revealing additional critical processes, resources, components, and hidden bottlenecks that can be addressed later. The final identification step detects single points of failure for future mitigation.

Subsequent to the definition of the vulnerabilities, their criticality is evaluated. To do so, first, the Maximum Tolerable Period of Disruption (MTPD) is defined for each hazard. This indicates the duration of a failure of the associated vulnerability, that can be endured without causing considerable harm.

Deriving from the MTPD, the Recovery Time Objective (RTO) must be defined. This establishes a quantifiable objective for the longest possible time to fix the malfunction. The harm potential of the corresponding failure should be taken into account when calculating the safety buffer between RTO and MTPD. It is also necessary to specify the emergency mode level, which guarantees a certain amount of productivity throughout the RTO period.

B. Risk Assessment

After the BIA, a risk assessment must be conducted in order to find and assess as many risks as possible. The risk assessment can be conducted in accordance to the general information provided in ISO 31000 [9]. At large, the risk assessment consists of three parts. The risk identification, the risk evaluation, and the risk treatment.

In the risk identification, as many risks as possible are collected, irrespective of their probability of occurrence or their severity. Many time-proven methods for risk identification can be found in the literature. Some of which are discussed by Chartres et al. [10], and can be used to give structured guidance on how they can be conducted. For risk identification of CMI, the exact method can be freely chosen depending on the case. However, we propose to classify the risks within the chosen method into 7 categories:

- environment (weather / heavy seas, erosion)
- technical failure (corrosion, wear)
- malicious intent (espionage, drone attack, cut cables)
- environmental protection (contamination, noise pollution)
- human failure (maloperation, negligence)
- accidents (transfer accident, person in water)
- third-party error (delayed services, damage from fishing)

In the evaluation, every risk is rated in terms of its specific probability of occurrence as well as its severity. To assess the severity of all the collected risks accurately, the results of the BIA have to be taken into consideration in the risk evaluation.

The outcome of the risk evaluation is a list of all the considered risks that are ranked by their severity and probability of occurrence.

$$\text{Risk} = \text{Severity} * \text{Likelihood} \tag{1}$$

In more complex methods, other factors, like their exposure rate [11] or cascading effects [12] can also be included.

Depending on the conclusion of the risk evaluation, an adequate risk treatment must be conducted. For the purpose of the methodology presented in this paper, the risk treatment will be conducted through a resilience plan as described in section III.

III. Resilience Plan

In order to appropriately treat the risks in complex systems, a mere risk prevention tactic is insufficient. In a resilience-based risk treatment, the reality of disturbances that will occur in a sometimes unpredictable manner is recognized. As a result, instead of solely focusing on risk prevention, the categories of damage mitigation, crisis management, and a restoration plan (including a continuous improvement process) must be considered as well [13]. Installing those resilience measures can meet the minimum requirements of the CER directive [4], and reduces harm in future disturbances.

A short overview of the content of those categories is given below. In addition, some examples specific to CMI to showcase their ability to heighten resilience are also shown.

A. Preventive Measures

Preventive measures aim to stop disturbances from occurring at the facility. A key guiding concept for these measures is Safety and Security by Design [14], [15]. In short, it describes the importance of already thinking about safety and security during the planning process of the infrastructure facility. Thus, safety and security measures can be built in from the get-go, rather than added in post activation. Embedding safety and security from the start, allows the facility to be built around these concepts, enhancing overall protection. Examples of safety and security by design include built-in fire-safety systems, deeper burial of seabed cables, anti-drone barriers (fences, nets, reinforced concrete), and robust cyber-security.

In addition, a testing plan and a staff-education program must be implemented and continuously refined. Testing identifies weaknesses, trains personnel, and validates existing preventive measures. The ongoing education program prepares employees and raises awareness of safety and security issues, which proves invaluable to facility managers.

From a more technical perspective, a continuous maintenance plan is essential for every facility's long-term success. In the field of CMI, there are special challenges related to repair and maintenance. Required specialized equipment often has long rental lead times and can only be used during good weather conditions [16]. Precautions should ensure rapid, privileged equipment access or, at a minimum, prepare adequate damage-mitigation measures, which are discussed in section III-B. Similarly, measures must be taken to ensure the quick availability of spare parts, safety equipment, emergency power, emergency fuel, and so on.

Furthermore, recent incidents of apparently intentional maritime-infrastructure destruction [1], [2], and [3] require

increased resources for prevention. Threats include ship collisions, anchor-induced cable cuts, data-cable interception, and airborne drone espionage. Preventive actions may involve exclusion zones for unauthorized vessels and drones, facility access controls, personnel background checks, and additional safeguards.

Finally, robust supply-chain management is needed to avert large-scale harm. The COVID-19 container crisis [17] and the 2021 Suez Canal blockage [18] showed that high inter-connectivity allows small events to cause global repercussions. The Suez Canal blockage was caused by a ship blocking the Suez Canal and therefore disrupting global supply chains. The container crisis was a global supply chain crisis caused by a container accumulation in particular ports. Therefore causing worldwide shipping blockage through missing containers in other parts of the world. Consequently, CMI supply chains must be analyzed, understood, and reinforced with resilience measures. Because of its complexity, supply-chain management is beyond the scope of this brief paper. More extensive information on that topic can be found in [19] and [20].

B. Damage Mitigation Measures

Damage mitigation measures acknowledge that even the best preventive measures cannot fully prevent incidents. Therefore they focus not only on mitigating damages of foreseen risks, but also on minimizing the damage after an unforeseen or underestimated incident occurs. Effective mitigation measures should be based on the risk assessment outcome, as well as the BIA outcome [21]. Because the assessment detects and ranks many risks according to their need for attention. While the BIA detects the business processes and bottlenecks that need to be protected the most regardless of the nature of the incident.

Risk can be reduced by real-time monitoring of critical processes [22]. Early detection enables automated shutdown or slowdown to prevent a collapse. For example, it could prevent transformer overheating. It could also detect a pipeline crack before rupture or identify unauthorized tapping of a data cable. Because the marine environment is highly sensitive, monitoring water and air pollution around the infrastructure is necessary. This provides data on the plant's environmental impact and informs response measures. Furthermore, oil spill-response equipment must be mandatory on all offshore infrastructure.

In addition to mitigating known major risks, it is important to acknowledge that not all relevant risks can be identified and treated. Therefore, modern resilience approaches should include measures that mitigate damage from unforeseen incidents. These measures focus on critical facility processes defined in the BIA. Those measures will be highly specific to the facility that is treated. In general, redundancy options and emergency operations must be established. They secure all major processes regardless of the failure cause.

Passive protective measures should also be employed. They mitigate damage during incidents without activation. Examples include fire-resistant doors and walls that compartmentalize the plant, preventing fire spread. Similarly, watertight compartments in a ship prevent flooding. Other examples are lightning arresters, earthquake-resistant construction, and drip pans that prevent hazardous substances from entering the sea.

C. Crisis Management

Crisis management must define every organisational process that enables a rapid, orderly response. In general, that means that clear definitions of roles and responsibilities, as well as communication-ways and communication-substances are determined [23]. Additionally, with critical infrastructure, a clear, quick, and transparent communication towards the public and media needs to be defined for major incidents as well as environmentally damaging incidents. This is needed because infrastructure failures can provoke public fear. Which may turn into frustration with operators and politicians. This frustration can be dangerous because it can jeopardise future infrastructure projects and erode trust in democratic institutions. The potential for negative public response further increases critical infrastructure attractiveness as a hybrid warfare target. The effect of public outrage despite adequate crisis management has been described by Foussard et al. on the example of a large scale fire in 2019 [24].

Since the exact crisis management is highly dependent on the organizational structure of the individual plant rather than the type of CMI, no concrete examples will be given in this paper. Instead, more information can be found in [23].

D. Restoration Plan

While damage-mitigation and crisis-management measures reduce incident effects, structured plans are also required. One plan ensures short-term business continuity (emergency-response plan). Another restores processes to normal operation (restoration plan) [25]. To develop both plans, it helps to classify scenario categories. Examples are acute damage, malfunction, or breakdown, wear-induced damage, danger to personnel, environmental damage, economic uncertainty, societal damage, malicious acts, and resource shortages. Classification after that sort enables the plant operators to prepare for a broad range of incidents without the need to anticipate the actual event in great detail. However, the resulting measures are often generic. Such generality can lead to sub-optimal preparation for specific incidents.

To minimize that drawback, more specific standard scenarios can be defined. The scenarios should reflect incidents with high likelihood or high risk. They are derived from the risk assessment and the BIA. Typical CMI standard scenarios include energy outage, fire or explosion, oil leakage of varying scale, ship collision, and cable damage caused by an anchor or fishing net. The distinction between standard categories and scenarios is not binary. It represents a spectrum: one end offers broad, low-accuracy measures; the other provides narrow, high-accuracy measures.

As noted above, the emergency-response plan provides a rapid reaction to incidents. It aims to raise business processes to the emergency mode defined in the BIA as quickly as

possible. It prioritises high-importance processes to maintain partial plant productivity and to limit secondary impacts. A more detailed guide to an emergency response plan can be found in [26] and [27]. Alternatively, a business continuity plan, as defined in ISO 22301 [6], can replace an emergency response plan.

Conversely, the restoration plan restores all processes to normal operating capacity. To achieve this as quickly as possible, the restoration plan must start immediately after the incident, concurrently with the emergency-response plan. But due to the different target (quality instead of reaction time), its implementation takes significantly longer than the restoration plan, making both plans vital components. A more detailed guide for a restoration plan can be found in the BSI Standard-204 [25].

Besides restoring normal process levels, the restoration plan incorporates a continuous-improvement process. Due to the newfound information that can be gathered from a real-world incident, a lessons-learned-process can be conducted, which enhances future plant resilience. The process reflects on mistakes, defines improvements, and documents the incident in detail for future reference. Conclusions from continuous improvement are used to upgrade personnel training and regular performance reviews. An extensive guide to a lessons-learned-process can be found in [28].

IV. Outlook

This paper proposes a general methodology to enhance resilience in critical maritime infrastructure. The proposal can guide actions to improve resilience, but it is not a standalone guide. Implementing the methods requires knowledge beyond what is presented here. Also, many details specific to the actual type of plant have been left out.

To address this, the methodology should be detailed for each CMI type listed in section I. Tailoring the proposed methodology towards one specific type of plant will allow the choice of specific methods at every step. Rather than, for example, just stating that a risk evaluation needs to be conducted. That way, a specific guide for every type of CMI can be created. Those guides can be used by actual plant operators without the need for a comprehensive knowledge of current risk and resilience science.

Additionally, the specialisation on one type of CMI will allow us to define concrete methods for the supply chain management, as well as for the crisis management, which have been left out of this paper.

Lastly, by focusing on specific types of CMI, concrete resilience measures can be developed that can be used for every plant. Those measures could further be collected in a repository which would be sufficient in fulfilling all requirements that are stated in the CER directive [4].

References

[1] N. Adomaitis and J. Ahlander, "What is known about the Nord Stream gas pipeline explosions?" Reuters, news article, 2025.

[2] E. Cook, "North Sea 'Very Unprotected' Against Russia—NATO Admiral," Newsweek, news article, 2025.

[3] I. Kottasova, "Finland detains ship and its crew after critical undersea cable damaged," CNN, news article, 2025.

[4] European Union, "Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC," *Off. J. Eur. Union*, vol. 65, pp. 164 – 198, 2022.

[5] Federal Ministry of the Interior and Community, "Zweite Verordnung zur Änderung der BSI-Kritisverordnung," in *Bundesgesetzblat Teil I*. Bundesanzeiger Verlag, 2021, no. 63, pp. 4163 – 4187.

[6] "Security and resilience – Business continuity management systems – Requirements (ISO 22301:2019)," International Organization for Standardization, Geneva, CH, Standard, June 2020.

[7] "Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA) (ISO/TS 22317.2021)," International Organization for Standardization, Geneva, CH, Standard, November 2021.

[8] P. Sikdar, *Practitioner's Guide to Business Impact Analysis*. Auerbach Publications, 2017.

[9] "Risk management — Guidelines (ISO 31000:2018)," International Organization for Standardization, Geneva, CH, Standard, October 2018.

[10] N. Chartres, L. A. Bero, and S. L. Norris, "A review of methods used for hazard identification and risk assessment of environmental hazards," *Environment international*, vol. 123, pp. 231–239, 2019.

[11] P. K. Marhavilas and D. Koulouriotis, "A risk-estimation methodological framework using quantitative assessment techniques and real accidents' data: Application in an aluminum extrusion industry," *Journal of loss prevention in the process industries*, vol. 21, no. 6, pp. 596–603, 2008.

[12] V. Cozzani, G. Antonioni, and G. Spadoni, "Quantitative assessment of domino scenarios by a GIS-based software tool," *Journal of Loss Prevention in the process industries*, vol. 19, no. 5, pp. 463–477, 2006.

[13] D. D. Woods, "Four concepts for resilience and the implications for the future of resilience engineering," *Reliability Engineering & System Safety*, vol. 141, pp. 5–9, 2015, special Issue on Resilience Engineering.

[14] I. Van de Poel and Z. Robaey, "Safe-by-design: From safety to responsibility," *Nanoethics*, vol. 11, no. 3, pp. 297–306, 2017.

[15] A. Lunkeit and W. Zimmer, "Security by Design," *Berlin, Heidelberg*, 2021.

[16] M. Scheu, D. Matha, M. Hofmann, and M. Muskulus, "Maintenance Strategies for Large Offshore Wind Farms," *Energy Procedia*, vol. 24, pp. 281–288, 2012.

[17] R. Mahmud, F. Zheng, I. B. Løff, and Z. H. Munim, "The container shipping crisis during COVID-19 disruption: consequences and lessons learned from news analysis," *Journal of Shipping and Trade*, vol. 10, no. 1, p. 29, 2025.

[18] M.-A. Russon, "The cost of the Suez Canal blockage," BBC, news article, 2021.

[19] "Security and resilience — Security management systems — Requirements (ISO 28000:2022)," International Organization for Standardization, Geneva, CH, Standard, November 2022.

[20] D. Weiß, T. Hajduk, and J. Knopf, *Step-by-step guide to sustainable supply chain management: a practical guide for companies*. Federal Ministry for the Environment, 2017.

[21] J. B. Leite and M. Kezunovic, "Risk mitigation approaches for improved resilience in distribution networks," in *2020 IEEE PES Transmission & Distribution Conference and Exhibition - Latin America (T&D LA)*, 2020, pp. 1–6.

[22] S. Bas and N. Catbas, *Bridge Failures and Mitigation Using Monitoring Technologies*. Cham: Springer International Publishing, 2021, pp. 43–52.

[23] E. L. Quarantelli, "Disaster crisis management: A summary of research findings," *Journal of management studies*, vol. 25, no. 4, pp. 373–385, 1988.

[24] C. Foussard, W. Van Wassenhove, and C. Denis-Rémis, "Taking Public Concerns into Account as a Risk Management Criterion. A Case Study," in *European Safety and Reliability Conference*, August 2022.

[25] *Business continuity management : BSI-Standard 200-4*. Bundesamt für Sicherheit in der Informationstechnik, 2023.

[26] E. S. Devlin, *Crisis management planning and execution*. Auerbach Publications, 2006.

[27] D. E. Alexander, "Disaster and emergency planning for preparedness, response and recovery." Oxford University Press, 2015.

[28] N. Milton, *The lessons learned handbook: Practical approaches to learning from experience*. Chandos Publishing, 2010.