Safe and Resilient Control for Marine Power and Propulsion Plants

Kougiatsos, N.

DOI
10.4233/uuid:9f85e2ff-f994-4682-a7e8-cca91c3e2e5a

Publication date
2024

Document Version
Final published version

Citation (APA)
Kougiatsos, N. (2024). *Safe and Resilient Control for Marine Power and Propulsion Plants*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:9f85e2ff-f994-4682-a7e8-cca91c3e2e5a

Safe and Resilient Control for Marine Power and Propulsion Plants

Kougiatsos, N.

Publication date
2024

Document Version
Final published version

Citation (APA)
Kougiatsos, N. (2024). *Safe and Resilient Control for Marine Power and Propulsion Plants*. [Dissertation (TU Delft), Delft University of Technology]. TRAIL Research School.

Safe and Resilient Control for Marine Power and Propulsion Plants

Nikos KOUGIATSOS

Safe and Resilient Control for Marine Power and Propulsion Plants

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft
op gezag van de Rector Magnificus prof.dr.ir. T.H.J.J. van den Hagen,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op dinsdag 07 november 2024 om 10:00 uur

door

Nikos KOUGIATSOS
Master of Naval Architecture and Marine Engineering
National Techical University of Athens, Athens, Greece
geboren te Athens, Greece

Dit proefschrift is goedgekeurd door de promotoren:
Prof.dr. R.R. Negenborn
Dr. V. Reppa

Samenstelling promotiecommissie:

Rector Magnificus	voorzitter
Prof. dr. R. R. Negenborn	Technische Universiteit Delft, promotor
Dr. V. Reppa	Technische Universiteit Delft, copromotor

Onafhankelijke leden:

Prof.dr. R. Babuska	Technische Universiteit Delft
Prof. dr. ir. M. van Koningsveld	Technische Universiteit Delft
Dr. M. Lützen	University of Southern Denmark
Prof. dr. C. Panayiotou	University of Cyprus
Prof.dr. N. P. Ventikos	National Technical University of Athens, Greece

The research described in this thesis was supported by the Dutch Research Council (NWO) under the research programme "Topsector Water & Maritime: the Blue route" (Grant Agreement no. TWM.BL.019.002)

TRAIL Thesis Series no. T2024/12, the Netherlands TRAIL Research School
TRAIL, P.O. BOX 5017, 2600 GA Delft,The Netherlands, E-mail: info@rsTRAIL.nl
ISBN: 978-90-5584-351-0
Published and distributed by: N. Kougiatsos

Keywords: Marine Power and Propulsion Plants (PPPs), Resilient control, Maritime safety, Decision-support systems, Quantitative and Qualitative modelling techniques

Printed in the Netherlands

“Τὰς ἰδέας νοεῖσθαι μὲν, ὁρᾶσθαι δ’ οὐ”

Πολιτεία, Πλάτωνας (Republic, Plato)

Preface

It has now been almost four years since I first came to TU Delft to pursue my PhD. Surely, it was one of the most wonderful, brave and challenging decisions I have ever made. At the end of this journey, I would like to acknowledge everyone who inspired, helped, encouraged, trusted, and made my days here a little brighter.

First, I would like to thank my promoter, Prof. Dr. Rudy R. Negenborn. Rudy gave me the chance to join a lively and supportive department at TU Delft, while turning my dream of working towards the vision of intelligent and autonomous marine vessels into reality. His critical reviews of my papers and during the writing of this thesis helped improve the quality of my research. I am also thankful that he supported me during my supervisor's maternity leave by organizing more meetings and encouraging collaborations.

I owe much of my development throughout these years to my supervisor, Dr. Vasso Reppa. Coming from a marine engineering background, I was eager to learn more about systems and control, as well as fault diagnosis. Vasso was always there to support me through thorough discussions, provide materials, and suggest courses. Our discussions helped improve my critical thinking, presentations, manuscripts, and she also gave me the opportunity to act as a reviewer for well-known conferences and high-ranking journals. Most importantly, I would like to thank her for helping me maintain a clear mindset during the PhD cycle and for trusting me to make independent decisions.

A big thanks also goes to my colleagues at TU Delft. It was delightful to be part of the Safe-NET research group with Abhishek Dhyani, Andrea Caspani, Tasos Tsolakis, Zhe Du, and Pablo Segovia Castillo. I am fortunate to have met and befriended Adrien Nicolet, Apostolos Souflis-Rigas, Nikos Vasilikis, Semina Karadima, Nicole Charisi, Jesper Zwaginga, Evelien Scheffers, Zacharias Oikonomou, Xiaohuan Lyu, Estelle Meyer, Çiğdem Karademir, Alejandro Latorre Correa, Marcel van Benten, Kostas Kiouranakis, Kostantinos Zoumpourlos, Marco Borsotti, and Sana Lateef. It was delightful to work with Pan Fang, Ana Azevedo Vasconcelos, Sankarshan Durgaprasand, Ahmed Hadi, Jayvee Ramos, Foivos Mylonopoulos, Jake Walker, and so many others. To Timon Kopka and Rafael Leite Patrão, mine and Adrien's successors in organizing the TEL PhD meetings, I wish you the best of luck in your work. Finally, a big thanks goes to my office mates Hao Shi, Aaron Chen, and Simeon

Slagter.

Thanks to the Netherlands Organisation for Scientific Research (NWO) for sponsoring and supporting my research, and to all the industrial partners involved. I was very fortunate to spend a two-month secondment period at SINTEF Digital, Trondheim, Norway, under the supervision of Dr. Marialena Vagia.

My biggest thanks, however, goes to my family and friends from Greece. Without your continuous support and visits, I would not have been able to complete this PhD. To my sister Marialena and my friend Spyros, you really are my wings in every new adventure I embark upon, and I cherish having you in my life. To my parents, Sofia and Stathis, I owe much of who I am at the moment, and I always appreciate your unconditional love, support, and advice. To my grandparents, Maria, Eleni, Nikos, and Giorgos, whether with us or forever in our hearts, I dedicate this thesis mostly to you. You will always be my heroes and greatest inspirations. Last but not least, to my friends Vaggelis, Dimitris, Thodoris, and Thomas, thank you for the countless joyous hours we spend together and for bearing with me at times. Let us enjoy our summer vacation!

Thanks a lot for everything! Σας ευχαριστώ πολύ για όλα!

Nikos Kougiatsos,
Delft, June 2024

Contents

Chapter 1

Introduction

This thesis focuses on the development of safe and resilient control architectures for marine vessels that can handle control system adaptations while increasing their operational safety. This chapter introduces the main challenges tackled in this thesis and outlines the methodologies used to address those challenges. More specifically, Section 1.1 provides the research background, basic definitions and relevant challenges in the maritime industry. Section 1.2 then further motivates the problem using similar project examples from both industry and academia, while the research questions addressed in this thesis are outlined in Section 1.3. Finally, the main contributions of this thesis are presented in Section 1.4, followed by the overall structure of the thesis in Section 1.5.

1.1 Background

Realising the vision of the "Blue Route"-call (NWO, 2019) raises tremendous challenges including guaranteeing low environmental impact and safety of marine vessels. The maritime industry is mainly challenged at two fronts: reducing its environmental impact and increasing autonomy (Felski &Zwolak, 2020).

Previous calls from the *International Maritime Organisation* (*IMO*) in 1997 and 2008 demanded that NOx, SOx and particle emissions are cut down substantially in the following years. So far marine vessels are able to cope with the requirements by developing new engine technologies (Tier II, Tier III) or by retrofitting older systems with exhaust gas treatment technologies such as scrubbers, *Selective Catalytic Reduction* (*SCR*) and *Exhaust Gas recirculation* (*EGR*) systems (Wärtsilä, 2024a,b,c). In recent years, IMO regulations also aim for a reduction in CO_2-emissions of 40% by 2030 and a simultaneous reduction of 70% carbon emissions and of 50% *Green House Gas* (*GHG*) emissions, by 2050 (IMO, 2018). This is expected to be accomplished using more sustainable energy carriers such as methanol, biofuels or even

ammonia, or by taking advantage of other energy sources (e.g., batteries, supercapacitors, fuel cells). However, what technologies will prevail for each type and size of vessel is still greatly uncertain.

Meanwhile, the vision for maritime transport includes autonomous shipping (Felski &Zwolak, 2020). As marine vessels are a valuable asset, a large number of cyberdevices will need to be added on-board and more sophisticated monitoring, control and coordination algorithms will need to be implemented. This will enable remote operation in the short term and fully autonomous navigation in the longer term. Moreover, reliable communication and computation mechanisms will need to be designed to facilitate the processing, storage and transferring of information between the various cyberdevices on-board vessels. Nonetheless, the number, the type and the connections between the physical and cyberdevices on-board a vessel is greatly uncertain both at the initial design stage and during design adaptations. As a result, the control systems' design should account for this uncertainty.

Vessels can be considered as a large network of subsystems interconnected with physical interconnections (e.g., pipes, ducts, cables) and cyber interactions (e.g., communication network). Both in the initial design phase and during their lifecycle, it is the responsibility of the vessel designers (e.g., marine engineers) to select the components based on the specifications of the ship owner and the existing regulations. As a result of this process, there are more than one *Power and Propulsion Plant* (*PPP*) topology design options satisfying the power requirements of the vessel, such as the ones shown in Figure 1.1. The designers also manually draft the connection graphs of the selected components (i.e., without using automated generation software), based on their expert knowledge, and are expected to re-iterate the design until all specifications are met. Design adaptations affecting marine *PPP*s are mainly initiated by the operators (i.e., on-board crew, on-shore control centers) in three cases; **(i)** under changes in the regulatory framework and available technologies in the industry for emission control (Papanikolaou, 2018), **(ii)** when the mission characteristics change (van Benten, 2022), and **(iii)** under the occurrence of unexpected events such as faults and attacks during the power and propulsion plant operation (Wu et al., 2006). In all the aforementioned scenarios, modifications upon the vessel will eventually be required such as replacements of outdated equipment and switching machinery, actuators, and sensors either online (during operation) or offline (between operations). The required topology design adaptations to satisfy new regulations, missions and/or updated safety requirements could be extensive such as an adaptation from the system architecture shown in Figure 1.1a to to the one shown in 1.1b.
As a result, a useful concept for the design of marine vessels is that of modularity, defined as:

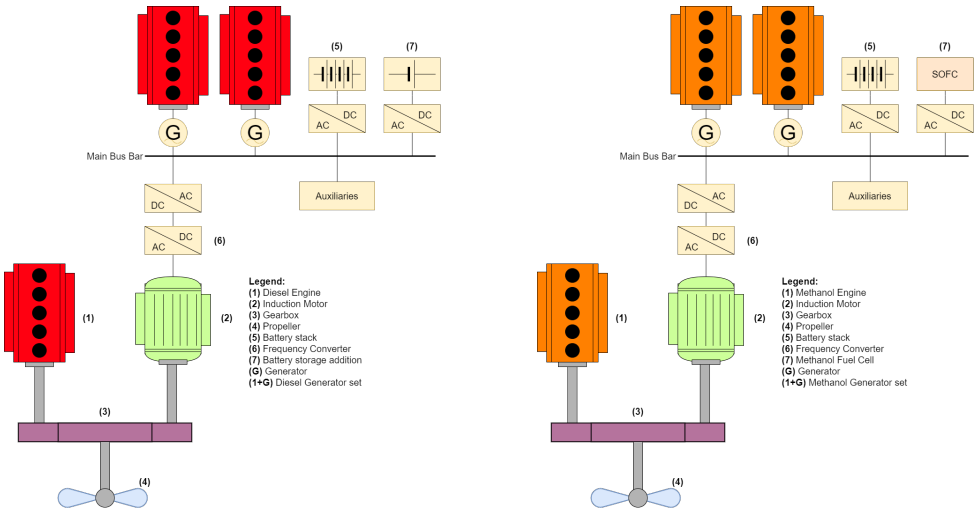


Figure 1.1: Examples of topology choices of marine PPP*s considering different fuels and energy storage choices; (a) use of carbon fuels and battery energy storage, (b) use of methanol and addition of Solid Oxide Fuel Cells (SOFC) to energy storage*

Definition 1.1 Modularity (Choi, 2018)
From a systems perspective, modularity is a strategic approach to handle complexity, whether this complexity is structural, behaviorial, contextual, perceptual or temporal. This is achieved by dividing a system into manageable and self-contained parts. □

Definition 1.2 Modular vessel design (Papanikolaou, 2018)
Modular vessel design is an approach to handling contextual uncertainty in ship design. This considers modularity in operation, which enables a ship to be changeable. Thus, equipment can be retrofitted and different missions can be taken to maximize the value throughout the lifecycle of the vessel. □

The aforementioned system modifications will need to be accompanied by appropriate controller modifications in order to maintain the interoperability between components sourced from different manufacturers. However, nobody can guarantee the compatibility of the new controllers and the seamless operation of the whole system. As seen in the literature, marine vessels mostly employ a multi-level control scheme, where the different drive-train modules are controlled by a single agent at a higher layer (Geertsma et al., 2017b). Taking into account the design complexity of marine power and propulsion plants, the effects of structural modifications upon

(a) *(b)*

Figure 1.2: (a) Seavigour vessel blocks the Suez Canal traffic after engine failure (2023) (Magdy, Samy, 2023), (b) Loss of propulsion power lead to a collision between a vessel and the Baltimore bridge, US (2024) resulting in excessive damage and human casualties (Meredith, Sam, 2024).

the control design are in most cases unknown a priori. The current control system design does therefore not offer the needed flexibility for handling uncertain future modifications. This flexibility can be expressed in terms of modularity built-in the multi-level control system.

Even if the deployed multi-level architecture is efficient under healthy system operation, it does not allow for seamless reconfiguration of the system when malfunctions occur. Maritime safety is indeed a prerequisite for current vessels and a basic pillar for the development of future ships (de Vos et al., 2021). By recognising this important role, the *International Convention for the Safety of Life at Sea* (*SOLAS*), created in 1914 (aftermath of the Titanic disaster), is continuously evolving, including amendments, to adapt to technological advancements and emerging challenges in the maritime domain (IMO, 1974). This convention encompasses, amongst others, the regulatory framework for the design, construction, and operation of ships to minimize safety risks to ships and the environment. Concerning control systems, safety can be defined as follows:

Definition 1.3 Safety in control systems (Blanke et al., 2016)
Safety describes the absence of danger. A safety system is a part of the control equipment that protects a technological system from permanent damage. It enables a controlled shutdown, which brings the technological process into a safe state. To do so, it evaluates the information about critical signals and activates dedicated actuators to stop the process if specified conditions are met. The overall system is then called a fail-safe system. □

The consequences of flawed decision making by the *PPP* control systems could be severe, like the two vessel cases shown in Figure 1.2. Malfunctions such as engine failures and loss of propulsion can potentially lead to block of traffic, damage

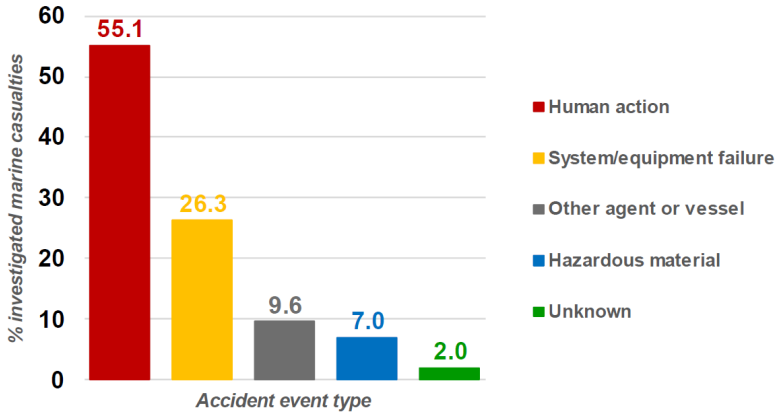


Figure 1.3: Distribution of marine casualties / accidents for the period 2014-2022 (23.814 total casualties). Marine casualties / accidents (y-axis) can be attributed to more than one accident events, which are more generally categorised in accident event types / categories (x-axis). (European Maritime Safety Agency, 2023).

to the vessel and other infrastructure (e.g., bridges, waterway structure) and human casualties. Despite the importance of maritime safety, recent reports from the European Maritime Safety Agency indicate certain alarming results about the distribution of marine accidents and casualty events (European Maritime Safety Agency, 2023). In Figure 1.3, the distribution of vessel accidents per cause of accident is presented for the years 2014-2022. As can be seen, almost 26% of all maritime casualties/accidents for this time period are attributed to system/equipment failure. As for the casualty events, Figure 1.4 shows the distribution of vessel casualty events per year and per cause for the same years. It was found that almost 7% of all ship casualties are attributed to loss of control events. The reliability of the equipment monitoring modules is indeed questionable when single sensor values are considered to perform fault diagnosis (Li &Marden, 2010; Wu et al., 2006).

For determining the course of actions after a fault has been diagnosed, resilience against faults needs to be built in the control systems. Resilience is a term that appears in a wide range of engineering disciplines, including control, and can be defined as follows (Woods &Hollnagel, 2017):

Definition 1.4 Resilience
Resilience is the ability of systems to prevent or adapt to changing conditions in order to maintain control over a system property. □

In the context of this thesis, the property we are concerned about is safety. To ensure safety, the control system must be resilient in terms of avoiding failures and losses,

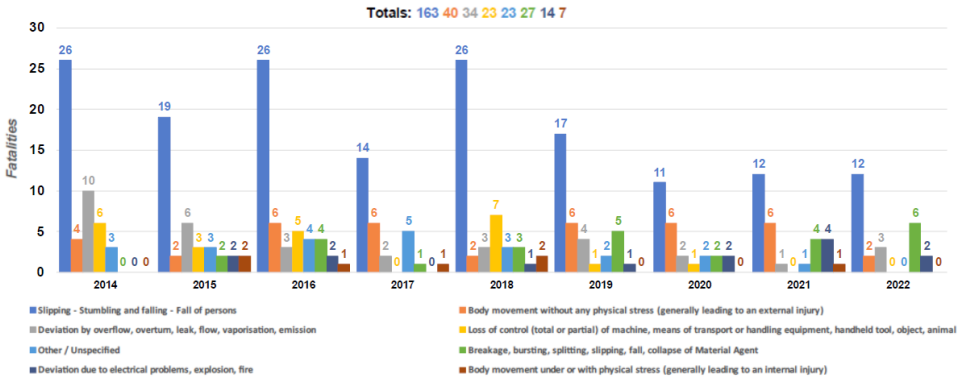


Figure 1.4: Yearly distribution of vessel casualty events for the years 2014-2022 (European Maritime Safety Agency, 2023). The loss of control events are shown with yellow.

as well as responding appropriately after the fact. Using the concept of resilience in Definition 1.4, resilient control can be defined as follows (Rieger et al., 2009):

Definition 1.5 Resilient control
A resilient control system is one that maintains state awareness and an accepted level of control stability in response to disturbances, including threats of an unexpected and malicious nature, such as faults. □

The concept of resilience is able to encompass control modularity in cases of faults affecting the vessel's systems, where online switching between physical and/or cyber devices will be initiated in order to maintain safe operation. For this reason, in the context of this thesis, resilience is deemed as a broader property than modularity for vessel control.

In marine literature and in practice, there are many cases when no distinction is made between a sensor fault or an actual system malfunction (MACSEA, 2012). Under the occurrence of sensor faults, utilizing hardware redundancy has been proposed in literature, meaning that multiple copies of a sensor are installed in the physical plant (Wu et al., 2006). This approach is also followed in many cases in practice due to the existing design regulations of some safety-critical vessel systems such as the Dynamic Positioning System (DNV, 2012). However, the physically redundant sensors can potentially fail as a unit due to the same cause (e.g., manufacturing defects). Alternatively, the vast availability of heterogeneous sensors onboard the vessel and the model information can be combined to construct virtual sensors instead (Blanke et al., 2016; Darvishi et al., 2021). Hardware and virtual sensors can then be combined to create a multi-sensory monitoring and control architecture. In this way, the operational awareness inside the ship can be improved

Figure 1.5: ZES battery pack (ING, 2020)

significantly.

1.2 Research motivation

The emerging technologies, changes in emission-related regulations and the increasing importance of operational safety for marine vessels motivate the need for safe and resilient control technologies. Currently, the future of the maritime industry is greatly uncertain regarding the fuels that will be used, the required equipment modifications to support these new fuels and the impeding digitalization of operations. Even though the existing regulatory guidelines prescribe the specification criteria for new system design concepts and technologies, they do not elaborate on their application in a wide variety of operational conditions (e.g., use of alternative fuels, operational profiles, faults). Moreover, considering the importance of maritime safety, more research effort should be placed in the development of reliable performance indicators that take into account a wide range of operational contexts (Negenborn et al., 2023). In order for vessels to remain competitive in face of uncertain future modifications, modularity is required to be built-in the vessel design in two ways: (a) by allowing quick and reliable topology adaptations using intelligent tools, and (b) by integrating resilient control techniques to enable seamless topology adaptations during operation under the effects of faults. Here, the design aspect of topology incorporates the selection of components and the associated diagrams showing their connections. The increase in operational safety will in turn be achieved by employing more sophisticated fault diagnosis techniques and by utilising the available knowledge in models, expressing the analytical redundancy of the system to increase the situational awareness of vessels under both healthy and faulty conditions. These concepts form the basis for safe and resilient control of marine vessels.

In industry, earlier projects investigated resilient solutions to make on-board control more flexible to equipment modifications. As an example, the creation of

modular drive trains which would allow easier retrofit for new vessel missions was previously investigated (IHC, 2020). The proposed *Drive & automation Integrated Vessel Automation* (*DIVA*) platform enables modular drivetrain designs during the vessel's lifecycle while increasing operational safety, system stability and reliability. Despite this, the platform mainly addresses the navigation and dynamic positioning processes of marine vessels and lacks the monitoring aspect, that is the detection and isolation of potential vulnerabilities. In addition, a modular battery project under the name ZESpacks aimed to use batteries having the form of containers, with an available capacity able to propel a barge 50 to 100 km, and with zero emissions (ING, 2020). The battery containers were also interchangeable from port to port and do not need to be recharged onboard the vessel. However, the application of swappable batteries was accompanied by challenges related to the integration aspects and availability of components. Considering previous related research, the HORIZON 2020 STRIKE3 project aimed to increase the safety and security of *Global navigation satellite system* (*GNSS*) technologies in ships and other infrastructures (GSA, 2016). Project ORCAS aimed to increase autonomous vessels' situational awareness and apply reconfiguration to the system when needed (NTNU, 2018). Nonetheless, both projects focused on the motion control technologies, excluding the underlying systems and sensors (e.g., power plant systems, shaft torque sensor). The performance and efficiency of those systems, under variations in power profile characteristics, were investigated in the *Dutch Research Council* (*NWO*) project ShipDrive without explicit considerations for safety (Geertsma, 2019; Haseltalab, 2019).

The READINESS project was launched in 2020, investigating, among others, ways to handle the uncertainty in automation modifications for marine vessels (READINESS, 2020). This thesis focuses on safe and resilient control of marine *PPP*s. In the next section, the main research question and subquestions addressed in this thesis are formulated, while the basic research approach is outlined.

1.3 Research questions and approach

The overall research question of this thesis is:

Q: *How to design safe and resilient autonomous control systems to handle the uncertain future adaptations in ship automation and to compensate for malfunction effects without human intervention?*

To address this main question, the following sub-questions are formulated:

Q1: *What are the state-of-the-art, state-of-practice and research gaps regarding*

the monitoring and resilient control of marine power and propulsion plants?

As briefly outlined in Section 1.1, the multi-level control scheme typically encountered in marine vessels, like in the case of marine power and propulsion plants, needs to be revisited to allow for increased safety and to allow for adaptations offline and during operation (resilience). A systematic literature review is, thus, required to determine the research gaps, state-of-the-art and state-of-practice in monitoring and resilient control of marine *PPP*s. The review should also include approaches from other fields facing similar problems and the feasibility of applying these solutions to marine vessels should be examined.

Q2: *How to derive models of marine power and propulsion systems for monitoring and resilient control purposes?*

An abundance of quantitative models for the most common ship power and propulsion systems is available in literature (e.g., Hansen et al. (2013)). These models are translated in a nonlinear state-space form, in this thesis, considering their Differential-Algebraic nature. Considering modularity, and more specifically the facilitation of the humans in the loop (designers, vessel operators) in seamlessly performing adaptations to the topology and control design, this thesis also explores the use of qualitative models. In particular, the qualitative modelling technique used is that of semantics (Milis, 2018). The use of either quantitative or qualitative models or both is then examined per case, depending on the research question.

Q3: *How to design and verify the performance of a sensor fault diagnosis architecture for marine propulsion systems?*

Due to the limited research works found in literature considering sensor faults and the lack of distinction between sensor faults and system malfunctions, the health of sensors should be questioned (MACSEA, 2012). Proper monitoring systems for sensor health should, thus, be developed and verified in an effort to increase operational safety.

Q4: *How to switch between hardware and virtual sensors during operation for enhanced fault resilience in marine propulsion plants?*

The occurrence of sensor faults during the propulsion plant operation will most likely compromise safety if left unattended. Whenever model information is available, such as the case of marine *PPP*s (Hansen, 2000), and one or multiple faults are diagnosed, the faulty measurement signals can be reconstructed (Isermann, 2006).

The analytical redundancy of the system can be employed in the form of virtual sensors, which can be combined with the onboard hardware sensors in a multi-sensory framework. Switching between those sensor types is required to enhance the resilience of marine power and propulsion plants against sensor faults. In addition, more attention should be placed in how this switching is applied in order to maintain the stability of the control systems applied to the power grid.

Q5: *How to optimise the fault diagnosis capabilities and the required hardware redundancy for safe operation of marine* PPP*s?*

The utilisation of analytical alongside of hardware redundancy has the potential to reduce both component installation and maintenance costs by loosening the extra hardware requirements. Meanwhile, the way the information extracted from hardware and virtual sensors is combined in the monitoring scheme plays a pivotal role in determining the isolability of sensor faults. The optimisation of sensor fault diagnosis should thus be examined.

Q6: *How to design a resilient control scheme to facilitate the adaptation of the power and propulsion systems to changes in operational requirements?*

During the typical 30-year lifecycle of a marine vessel, system adaptations are inevitable due to changes in regulations and mission specifications, the need for maintenance or the availability of new technologies. For the past few years and until 2050 the maritime industry is expected to operate under uncertainty regarding the fuels to be used and increasing autonomy. In order to facilitate design adaptations, intelligent tools should be built, focusing, amongst others, on the connection between the topology (i.e., network architecture) and control aspects of the design and on promoting resilience against unexpected events such as sensor faults during operation. This question, as a result, aims at the exploration of the control system technologies that will enable the seamless adaptation of vessels to changing operational requirements.

1.4 Contributions

The contributions of this thesis are as follows:

(1) Inspiration from semantic modelling techniques (Milis, 2018) and adaptation for marine multi-level control systems. The semantic models concern both physical and cyber plant components in the context of this thesis. Moreover, quantitative models stemming from First Principles are transformed in a

Differential-Algebraic state-space representation for the purposes of this thesis. This contribution has been published in (Kougiatsos et al., 2023, 2024a).

(2) The design of virtual sensors using both Differential and Algebraic modelling representations, in an effort to use the available analytical redundancy to increase situational awareness. This contribution has been published in (Kougiatsos &Reppa, 2022; Kougiatsos et al., 2024b).

(3) The optimisation of fault isolation using virtual sensors and the trade-off between hardware and analytical redundancy are both explored in the context of this thesis. This contribution has been published in (Kougiatsos &Reppa, 2024b).

(4) Design and performance analysis of model-based techniques for the sensor fault diagnosis of marine power and propulsion plants and for online reconfiguration purposes. In more detail, the reconfiguration entails the switching between hardware and virtual sensors or between controllers during operation to promote resilience against unexpected events such as sensor faults and system unavailability. This contribution has been published in (Kougiatsos et al., 2022b,a; van Benten et al., 2022; Kougiatsos et al., 2024b).

(5) The technical aspects that will enable the application of virtual sensors and non-centralised controllers in actual installations are also explored, boosting the intelligence of marine vessels. This contribution has been published in (Kougiatsos &Reppa, 2024a; Kougiatsos et al., 2024a).

1.5 Thesis outline

This thesis is structured in 8 chapters. A graphical representation of the outline is given in Figure 1.6. The contents of each chapter are briefly explained next:

- In **Chapter 1** we introduce the research subject, questions, approach and the outline for the following of this thesis;
- **Chapter 2** addresses question **Q1** by reviewing the available literature regarding the monitoring and control capabilities of the multi-level control schemes typically encountered in marine vessels. Moreover, the feasibility of implementing solutions from other fields for similar problems is assessed;
- In **Chapter 3**, question **Q2** is addressed. We describe the system models used for the remainder of this thesis. Both quantitative and qualitative models are considered and applied in a per case basis. The first rely on a state-space representation of the Differential-Algebraic First Principle models commonly

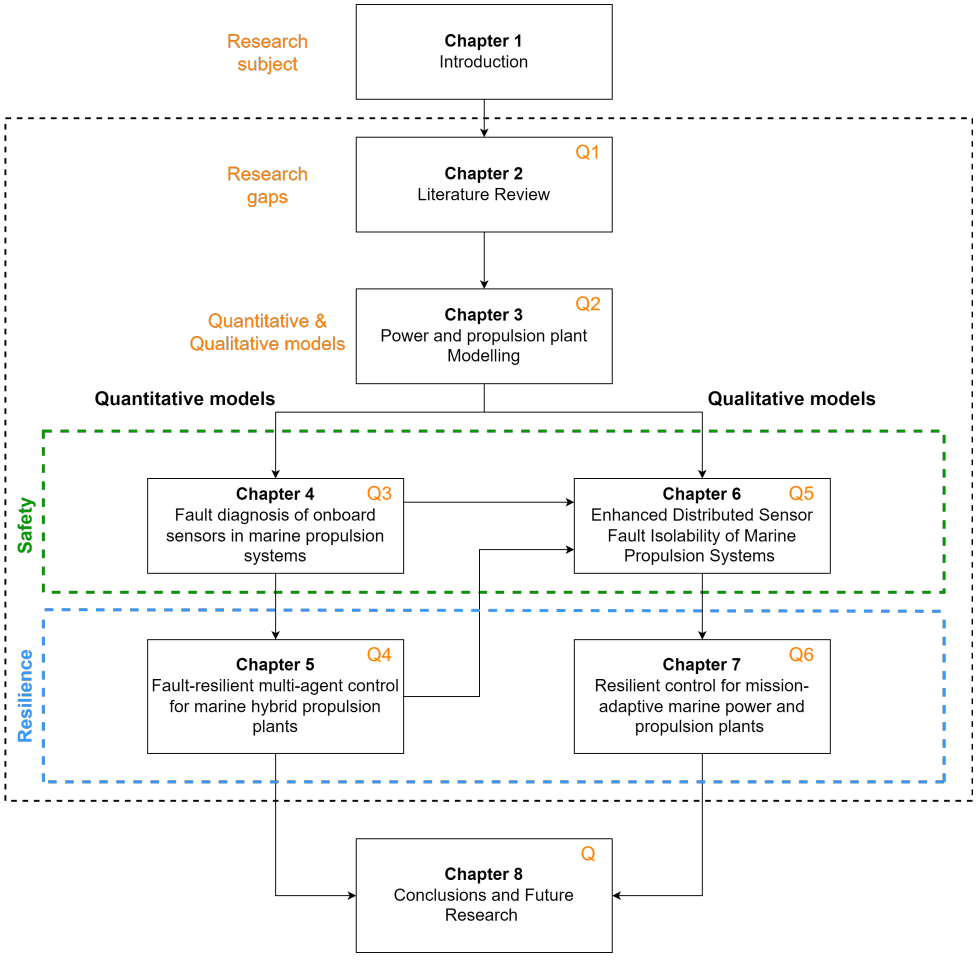


Figure 1.6: The outline of this thesis

found and used throughout the maritime literature. The latter are formulated using semantic representation techniques;

- **Chapter 4** follows up with question **Q3** and contains the design and performance analysis of a distributed sensor fault diagnosis scheme applied to marine internal combustion engines. The Differential-Algebraic nature of the system is considered in both fault detection and isolation processes and the possibility of false alarms is mitigated using model-based adaptive thresholds. Moreover, the monitoring scheme is assessed considering both sensor fault detectability and isolability performance metrics;

- **Chapter 5** then addresses question **Q4**, by introducing the design of virtual sensors, again considering the Differential-Algebraic nature of marine vessel systems. The virtual sensors are also assessed in terms of fault estimation accuracy and the time required for convergence to the healthy measurement. Hardware and virtual sensors are then combined in a multi-sensory control scheme and a logic is developed to switch between the two types of sensors, when the former are affected by sensor faults;

- In **Chapter 6** we address question **Q5** through the optimisation of the fault isolation property by tweaking the grouping between hardware and virtual sensors. In addition, the effect of using the analytical redundancy of the system (virtual sensors) in reducing the required hardware redundancy is explored. For both of these objectives, semantic modelling techniques are used;

- The final research question **Q6** is addressed in **Chapter 7**. This Chapter focuses on the integration of the topology and control design aspects in an intelligent framework to enable the adaptability of vessels to varying missions with different power requirements. The intelligent characterisation refers to the exploration of technical aspects that will enable these adaptations, stemming from the field of *Computational Intelligence* (*CI*). In this Chapter, the Differential-Algebraic and semantic modelling are both utilised for different purposes. The latter enable the use of CI tools while the former are used for simulation purposes, to enable the switching between hardware and virtual sensors or between controllers in cases of sensor faults or Denial-of-Service events respectively;

- **Chapter 8** concludes the thesis and provides directions for future research. As a result, the overall research question is addressed.

Chapter 2

Literature Review

The research topic of this thesis is the safe and resilient control of marine power and propulsion plants. This chapter addresses the first research question (**Q1:**) *"What are the state-of-the-art, state-of-practice and research gaps regarding the monitoring and resilient control of marine power and propulsion plants?"*. The chapter is organised as follows. Section 2.1 introduces the state-of-the-art of monitoring and control approaches for *Cyber-Physical System*s (*CPS*s) and motivates the need for resilience against design adaptations. Section 2.2 further categorises the factors concerning the design adaptations for marine *PPP*s. The available literature regarding the multi-agent low-level control scheme that is frequently encountered in marine *PPP*s is examined in Section 2.3, focusing on the ability for control design adaptations. Section 2.4 then introduces the vulnerabilities present in marine *PPP*s while the state-of-the-art in monitoring methods found in marine literature is presented in Section 2.5. Section 2.6 evaluates the available resilient control mechanisms in marine literature, and concluding remarks are provided in Section 2.7

2.1 Monitoring and control of adaptive Cyber-Physical Systems

The monitoring and control of *CPS*s is a typical research problem in the control systems field. A *CPS* is composed of a combination of physical/hardware systems (e.g., plant, actuators, sensors) and certain cyber/software systems (e.g., cloud capabilities, communication network). Their design allows for flexibility under changing conditions while reducing the necessary system wiring, installation and maintenance costs (Rajkumar et al., 2010).

Automation design adaptations will be required in a *CPS* in two cases; **(i)** when one or more structural changes affect the system design (Kougiatsos et al., 2024a), and **(ii)** under the occurrence of malfunctions affecting either the physical (e.g.,

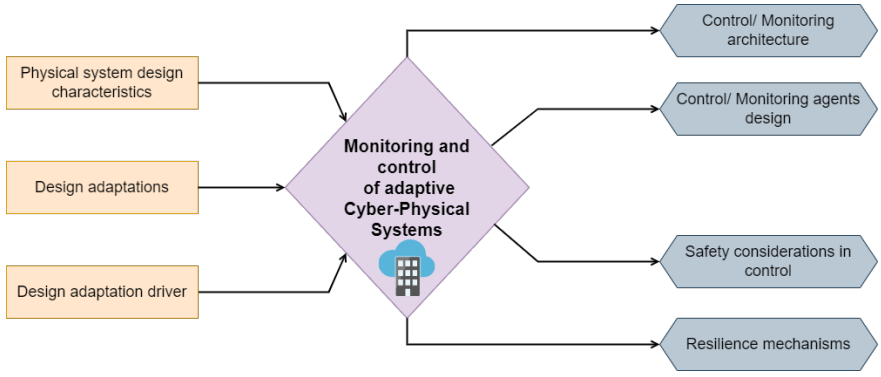


Figure 2.1: Classification of the monitoring and control of CPSs, under the influence of design adaptations.

hardware sensors) or cyber components (e.g., control agents) and/or connections during operation (Kougiatsos et al., 2024b). In both cases, the topology of the system (i.e., number and type of subsystems, redundancy, interconnections between subsystems), the physical subsystem characteristics (e.g., scale) and the employed control approach greatly affect the feasibility for seamless automation design adaptations. The basic inputs and outputs for the classification of the monitoring and control problems encountered in the *CPS* literature, under the effects of structural adaptations or malfunctions, are summarised in Figure 2.1.

2.1.1 State-of-the-art in monitoring and control approaches

Typically, multiple control and monitoring agents are involved in the safe and resilient control of *CPS* at different levels (Jilg &Stursberg, 2013). Figure 2.2 shows an example of a multi-agent monitoring and control system for *CPS*s, employing two control levels. For each subsystem $\Sigma^{(I)}$, $I = 1, \cdots, N$, a local control agent $C^{(I)}$ is designed to satisfy the control objectives of this subsystem. Each local controller $C^{(I)}$ belonging to this primary control level receives a reference input stemming from the secondary level controller, responsible to satisfy a global control objective for the *CPS*. Regarding the control agent design, centralised architectures have been extensively discussed in literature. This means that instead of having multiple control agents $C^{(I)}$, a single agent is used to satisfy the control objectives. However, under the effect of system adaptations (e.g., physical component addition), a redesign of the control agent will be required. Alternatively, the use of non-centralised control approaches for *CPS*s, as shown in the primary control level of Figure 2.2, has recently gained interest in literature (Cómbita et al., 2015).

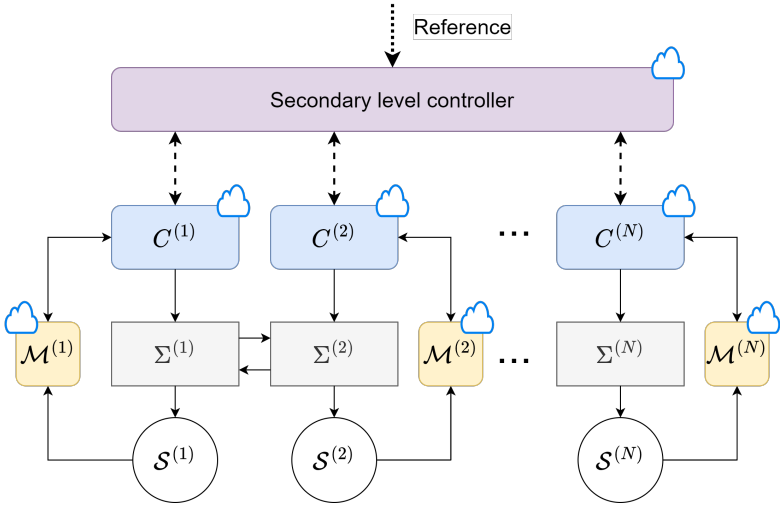


Figure 2.2: Multi-agent monitoring and control of CPSs. The cyber parts are indicated with a "cloud" icon. Control occurs at two different levels indicated by purple and blue respectively. The monitoring agents are shown in yellow.

In case a distributed/ decentralised[1] control approach is followed in one of the control levels, there are mainly two aspects where the control architecture differs:

- Partitioning: This determines the decomposed subsystems based for which local agents are designed
- Communication: If and how the exchange of information will take place (time-based, event-based etc.)

Partitioning is the first step to achieving either decentralised or distributed control. The decision factor is, in most cases, the level of interaction between the different subsystems. The physical partitioning of the plant can be derived from the mathematical modelling or, in more complex systems, a decomposition algorithm can be employed (Vu et al., 2018; Chen et al., 2020; Jiang &Yang, 2024). A simple example is the ϵ-decomposition where couplings with a given weight smaller than an arbitrarily chosen quantity are neglected. In (Jilg &Stursberg, 2013), a distributed two-level feedback control structure is proposed using the Hierarchical Lower Block Triangular decomposition algorithm. At the lower level, subsystems with strong dependence with each other form clusters. The weaker interactions are then inserted at a higher level. This way, communication can occur at a higher frequency in the bottom level (strong interactions) and at a lower frequency in the upper level (weak

[1]Decentralised control only involves partitioning

interactions). The computational effort is also claimed to be reduced due to the optimisation of communication topology used. Graph theory is also employed in many cases to deduce the interaction level using the drawn edges and weights, often alongside other algorithms (Xinsheng et al., 2018; Pierer von Esch et al., 2024).

Communication is regarded as a safety-critical process since information can be propagated, exposed or even altered during its broadcast between the monitoring and/or control agents . A standard way of information broadcast is time-based, meaning that the agents communicate at specified intervals (Xinsheng et al., 2018; Pierer von Esch et al., 2024; Jiang &Yang, 2024). The advantage is that regulating when the exchange of information occurs is a simple task. However, this approach can lead to unnecessary high communication cost (Panagi &Polycarpou, 2013). Concerning this issue, an enhancement of this option is proposed in (Jilg &Stursberg, 2013) where the frequency of communication differs in the lower and upper levels. An alternative in most cases is an event-based communication protocol where information broadcast occurs only when certain conditions are met (Pullaguram et al., 2018; Deng et al., 2021). In (Panagi &Polycarpou, 2013), the authors propose a coordinated event-based scheme where two agents work together when both their local tracking errors are off-bounds. The key idea is that when one control subsystem follows the reference very accurately, the connected controllers can instead continue their operation by assuming the reference is followed exactly in that subsystem. Thus, the agents normally work in a decentralised scheme and enter the distributed configuration only when needed. A higher level coordinator is responsible for the assessment of the interactions and the formation of clusters according to a specified logic. The authors of this paper also account for a possible failure of the coordinator and propose to fall back on the one subsystem off-threshold approach in those cases. Concerning the decentralised configuration, (Nayyar et al., 2013) discusses a stochastic control model in which the controllers share part of the information with one another. An updatable shared memory serves the communication purposes between the agents. Special cases of errors are also examined such as **(1)** delayed sharing of Information, **(2)** periodic sharing of information, **(3)** absence of shared memory, and **(4)** one-way information sharing.

Aside from the followed control approach, *CPS*s are exposed to both hardware and cyber vulnerabilities, such as faults and cyber-attacks, respectively (Cómbita et al., 2015). Safety is embedded to the *CPS*, using one or more monitoring agents $\mathcal{M}^{(I)}$, $I = 1, \cdots, N$ to diagnose these vulnerabilities, as can be seen in Figure 2.2. Each monitoring agent is designed to monitor the health of the system components belonging to $\Sigma^{(I)}$ and/or the health of the respective hardware sensors, denoted as $\mathcal{S}^{(I)}$. Similar to the control agents, the design of monitoring agents can be classified as centralised, decentralised or distributed (Reppa et al., 2016).

In the centralised configuration, the measurement information of the sensor sets

$\mathcal{S}^{(I)}$, $I = 1, \cdots, N$ and the available control actions $u^{(I)}$ is processed by a single monitoring agent, composed by one or more internal monitoring modules. The decentralised and distributed configurations include more than one monitoring agents, each with their respective monitoring modules, with the only difference being the existence or lack of communication between the monitoring agents respectively. The diagnosis of vulnerabilities such as faults and attacks is performed in two steps in the monitoring agents; the detection and the isolation process.

The detection process aims to determine the presence of one or more vulnerabilities and to estimate their instant of occurrence (Reppa et al., 2016). Considering model-free approaches, detection is often achieved using fault trees (Li et al., 2016; Kherif et al., 2021; Knežević et al., 2020), rule-based systems (Cai et al., 2020; Liu et al., 2020; Aimiyekagbon et al., 2021), *Support Vector Machine* (*SVM*) (Zhang et al., 2019; Zhou et al., 2020), principal component analysis (Lin et al., 2017) and neural network methods (Cai et al., 2020). However, a considerable amount of data is required both from healthy and faulty component conditions to perform model-free analyses. In addition, the generalisation ability of the results is considered low, especially in applications lacking standardization, such as marine power and propulsion plants. From the model-based perspective, the use of parity equations (Pop et al., 2020) or observer (Rojas et al., 2022) approaches for state estimation and the comparison of the state estimation error to one or more thresholds is commonly used for detection purposes. The choice of threshold(s) is of particular significance for the exclusion of false alarms and the minimisation of missed detections. To this end, adaptive threshold design (i.e., based on dynamical system models) methods are being developed in recent years (Papadopoulos, 2020; Tan &Zhang, 2023; Kougiatsos &Reppa, 2024a), instead of fixed thresholds widely used in literature. Aside from the chosen threshold, the missed detection rate highly depends on the accuracy of the used models. Nonetheless, most papers in the fault detection and isolation (FDI) literature only consider simplified system representations, composed by *Ordinary Differential Equations* (*ODE*) .

The isolation process follows the detection process with the aim of determining the components that were exposed to one or more vulnerabilities, or at least of excluding certain component cases (Reppa et al., 2016). To this end, the decisions of the monitoring agents are collected in vectors and compared against predefined binary *Signature Matrices* (*SM*), constructed based on the system structure. The comparison can be accomplished using either the rows or the columns of the matrices and this consists the main difference between the *Artificial Intelligence Diagnostic* (*DX*) and the *Fault Detection and Isolation* (*FDI*) communities. Combinatorial approaches between the two communities have also been proposed in literature (Reppa et al., 2018; Kougiatsos &Reppa, 2024a), while other research articles include more information in the matrices such as the sequence of activation of the different moni-

toring modules/agents for each fault case (Puig et al., 2005), in an effort to enhance fault isolation.

Other critical factors for isolation are the monitoring architecture under consideration (centralised, decentralised, distributed), the placement of sensors and the decomposition of sensors in sensor sets $\mathcal{S}^{(I)}$. In the case of a distributed monitoring architecture, the effects of faults can be propagated between the monitoring agents and thus, an extra level of fault isolation is required to distinguish between fault effects that have been propagated between monitoring agents and actual faults. The sensor placement problem consists in determining the optimal set of measuring devices such that a selection of faults can be detected and isolated (Rosich et al., 2007). The objective function considered in these problems is often related to the assumed cost of sensors (purchase, installation, maintenance) (Sattarzadeh et al., 2021) or simply the required number of sensors (Raju et al., 2022). Moreover, fault distinguishability requirements (Jung et al., 2020) may also be incorporated to the constraints besides the detectabilty and isolability targets. Finally, the sensor set decomposition problem aims to determine the optimal number and composition of sensor subsets, stemming from the starting sensor set, in order to enhance the isolation of multiple sensor faults (Reppa et al., 2016). This is especially necessary in large networks of cyber-physical interconnected systems, as in the case of marine propulsion systems, where the isolation of multiple sensor faults is really difficult or even infeasible with a single monitoring module. The objective function in these problems is based on nonlinear observer stability and fault isolability objectives rather than cost. In addition, applications on centralised monitoring architectures are mostly discussed in literature (Reppa et al., 2016), which would however result in high computational burden for large-scale applications such as marine vessels.

Metrics to characterize the performance of the fault diagnosis process are mostly related to the detectability such as the minimum detectable fault magnitude, the missed detection rate and the detection delay (Ding, 2013; Reppa et al., 2016). The performance of the ability to isolate faults has attracted less attention especially considering multiple sensor faults and interconnected differential-algebraic systems.

Further cyber functionalities can then be built in the monitoring agents for redundancy (Kougiatsos &Reppa, 2022) and/or online reconfiguration purposes (Kougiatsos et al., 2024a; Kougiatsos &Reppa, 2024b). Using such functionalities in coupling with the local control agents $C^{(I)}$, we can accomplish resilient control of complex CPSs.

2.1.2 The need for resilience against design adaptations

While non-centralised control approaches enable the adaptability of *CPS*s to structural changes and malfunctions, the stability after system adaptations is not guaranteed. The addition, removal and replacement of system components (e.g., sensors,

actuators, subsystems) requires the use of resilient control techniques. These capabilities are a necessity especially in case of multi-level complex systems such as marine vessels, which are often subject to structural modifications for e.g., retrofitting.

Resilience in control of complex CPSs requires the timely and effective capture of structural adaptations and/or malfunctions, so that their effects can be properly identified and mitigated. In (Riverso et al., 2016), a control reconfiguration strategy is proposed after detecting a fault in one of the plant's subsystems. The faulty module is disconnected from the system leading to an automated reconfiguration of the interconnected subsystems' controllers and monitoring modules. After its replacement, an automated plugging-in procedure restores normal operation. The application of the method is highlighted using two examples, one of coupled Van der Pol Oscillators and another one of a power network system. The authors of (Riverso et al., 2013), propose a decentralised *Model-Predictive Control* (*MPC*) scheme with resilient capabilities in case of subsystem additions or decommissions. When a new subsystem is plugged in, its local controller is designed while those of its neighbours are redesigned according to a specified algorithm. The algorithm also assesses the feasibility of the plug-in operation. However, since the configuration is decentralised, the controller redesign only aims to improve performance and may not affect other subsystems' stability. At the same time, there might also be cases where we would like to retain the ability to switch back to a previous trustworthy control design when the new configuration proves non-satisfactory in practical operation. In (Bendtsen et al., 2013), this situation is addressed using two approaches; a sensor fusion method that modifies the inputs to an existing controller when new measurements are available and a Youla-Kucera based controller parametrization method. Youla Kucera is an affine parametrization of all stabilising controllers for a given plant based on certain design parameters. This method is also applied in (Luo et al., 2017) for a DC motor network. On the other hand, (Stoustrup, 2009) also highlights a controller reconfiguration technique through terminal connections. In case of a system addition or replacement, instead of redesigning the controller, a new compensator controller could be plugged upon the terminals of the old one to modify the actuation command.

Furthermore, many works in literature have investigated the use of resilient control for adding new sensors and actuators to an existing system. In (Bendtsen et al., 2008), the authors propose a sensor fusion filter as a method to incorporate new sensor measurements in an existing subsystem without the need for controller reconfiguration, either using a model of the initial plant or in the case where only data is available. The "online" switching of sensors,under the effects of sensor faults, is also discussed in the control literature. In (Seron et al., 2008), a multi-sensory switching control strategy is proposed with the stability guarantees during switching being based on the state estimation error. A similar approach is used in (Kodakkadan

Table 2.1: Summary of literature studies on adaptive CPS*s, their resilient control methods and the adaptation drivers (N/D: not discussed).*

		Resilience Method		***CPS* adaptation driver**	
Article(s)	**Application**	Accommodation	Reconfiguration	Structural adaptation	Malfunction
(Bendtsen et al., 2008)	N/D	✓		✓	
(Riverso et al., 2013, 2016)	N/D		✓	✓	
(Stoustrup, 2009; Bendtsen et al., 2013; Luo et al., 2017)	N/D	✓	✓	✓	
(Milis et al., 2018)	Smart buildings		✓	✓	
(Kodakkadan et al., 2016)	N/D		✓		✓
(Stoican et al., 2014)	Process control		✓		✓
(Adamczyk &Orlowska-Kowalska, 2019)	Automotive	✓			✓

et al., 2016), where however a Youla-Kucera parametrization of all stabilizing controllers is used to ensure stability. The authors of (Stoican et al., 2014) on their end, ensure stability during switching using a pre-calculated dwell-time. Nonetheless, these papers only consider linear system dynamics, an *ODE* system representation and only hardware redundancy.

In (Milis et al., 2017), the concept of Semantic Mediation is introduced. It is composed of two parts; (1) the semantic database which stores information about different and possibly heterogeneous components and (2) an ontological knowledge model that can form relations between different components. A component can be a controller, a sensor, an actuator or even intermediary blocks (e.g., to transform the units of a sensor quantity). Thus, instead of providing a fixed system configuration with specific components and implicit knowledge about their characteristics, the Semantic Mediation Framework could reconfigure the plant as needed in case of a fault and better use the available equipment resources. A main advantage of the approach is its ability to encompass wired, wireless and digital components in a common framework. Moreover, it can also be used online, a useful characteristic for marine vessels, as they are on voyage most of their lifecycle. However, high computational load is associated with its deployment when the plant rapidly changes and new components need to be entered manually in the database. Table 2.1 summarises the previously reviewed literature on resilient control methods for adaptive CPS, depending on the adaptation driver.

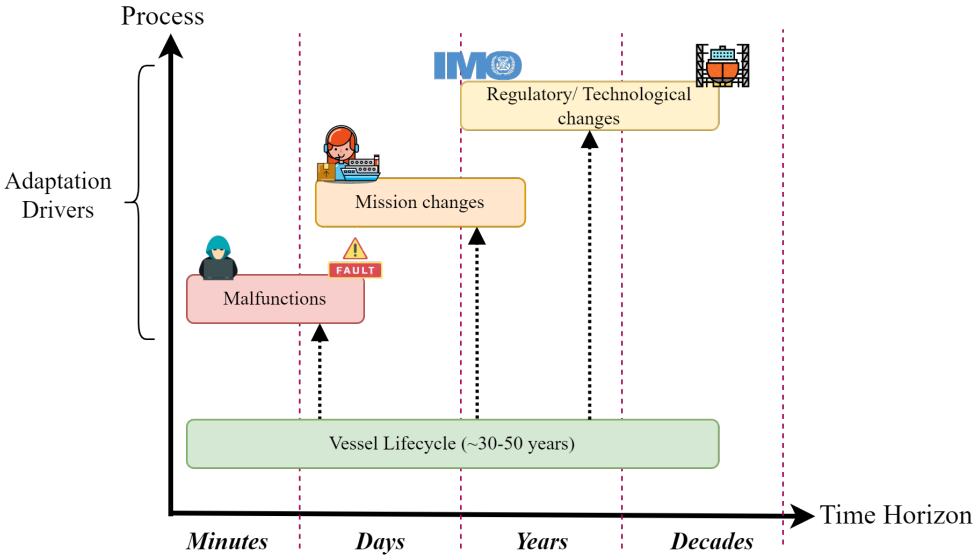


Figure 2.3: Relative time horizon for the design adaptation drivers of marine PPP*s compared to the vessel's lifecycle*

2.2 Design adaptations of marine power and propulsion plants

Marine power and propulsion plants can be considered as a large network of subsystems with physical interconnections (e.g., pipes, ducts, cables) or cyber interactions (e.g., communication network), comprising a large *CPS*. Design adaptations are required in such systems in the following cases; **(i)** due to changes in the regulatory and/or technological framework supervising their operation (IMO, 2018), **(ii)** under changes in the vessel mission characteristics (i.e., required power, time of operation etc.) (Vu et al., 2015; van Benten et al., 2022; Kougiatsos &Reppa, 2024b) and **(iii)** during operation, due to the occurrence of malfunctions (e.g., faults, attacks) affecting the vital subsystems of the *PPP* (Kougiatsos et al., 2024b). A main difference between these adaptation drivers is their time horizon which can range from a few decades to a few minutes accordingly, as can also be seen in Figure 2.3.

The *PPP* design can be also analyzed in three different perspectives; topology, size and control (Qin et al. (2018)). Both at the initial design phase and during the vessel's life cycle, it is the responsibility of the vessel designers (e.g., marine engineers) to select the components based on the specifications (e.g., emissions, produced power, attainable speed), manually draft their connection graph using expert knowledge and reiterate the design until the specifications are met. There are three possible propulsion configurations; mechanical, electric and hybrid. In the hybrid

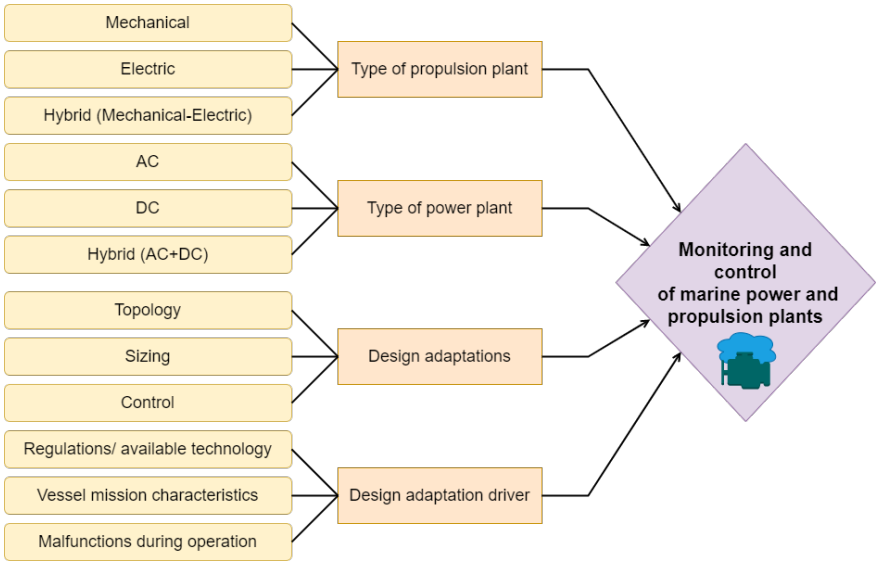


Figure 2.4: Analysis of the types of power and propulsion plants, potential design adaptations and drivers for design adaptations considered in marine literature.

design, the electric motors although present are used only when needed (Geertsma et al., 2017b; Planakis et al., 2021), thus coupling or decoupling the propulsion and the power system. In a mechanical propulsion configuration, the two systems are always decoupled while in an electric configuration, the two systems are always coupled. Similarly, there are three main power plant configurations, *Alternating current* (*AC*), *Direct Current* (*DC*) and hybrid, based on the types of the onboard power plant systems (e.g., batteries, generators, fuel cells). Reconfiguration of the topology is usually initiated by the operators (e.g., onboard crew, on-shore control centres) in case of maintenance, malfunctions or changes in mission specifications. As a result, considerable time and human labour are required both at the initial design stage and during the life cycle of the vessel to keep the topology of the *PPP* updated to be consistent with existing regulatory and technological frameworks.

The second perspective of system analysis, that is the sizing of the components belonging to a specific *PPP* topology, is investigated extensively in marine literature. In many cases, the size of components (e.g., power output, dimensions and other component characteristics) is determined by benchmarking different options in terms of operational efficiency, fuel savings and the reduction of the running hours for generators (Skjong et al. (2017)). Optimisation approaches are also proposed in literature, where operational data like power profiles is used to tune the sizing of the energy storage devices and generators. The objective functions are usually re-

lated to the system installation and management costs (Boveri et al. (2018); Letafat et al. (2020)), fuel usage efficiency (Haseltalab et al. (2021)), and lifetime carbon emissions or a combination of those (Bolbot et al. (2020)).

Control systems are, in most cases, designed for a specific iteration of the topology and take into consideration the chosen sizing (Geertsma (2019); Planakis et al. (2021)). However, in case of topology adaptations, control needs to be redesigned from scratch to avoid problems such as inefficient use, or overloading of the *PPP* equipment, or even the inability to carry out new vessel missions with different power requirements. The control agents are often designed for a specific *PPP* topology and sizing, thus being inflexible for design adaptations. Alternatively, Zhang et al. (2023) consider swapping battery energy storage between stations on inland waterways. The voyage scheduling and energy management are both optimised in a joint optimisation problem. Another approach includes the design of multiple energy management strategies based on known iterations of the *PPP* topology to adapt to new missions and a digital supervisor installed to switch between these strategies during operation (Sørensen (2011); Bertaska &von Ellenrieder (2018)). Nevertheless, so far in the marine literature, the technical aspects regarding the implementation of the digital supervisor and the occurrence of anomalies such as sensor faults during operation have not been investigated. Figure 2.4 summarises the types of power and propulsion plants, potential design adaptations and drivers for design adaptations considered in marine literature.

2.3 Multi-agent low-level control of marine power and propulsion plants

Most papers dealing with low-level control of marine power and propulsion plants define one or more global objectives such as the minimisation of fuel consumption (Kalikatzarakis et al., 2018), emissions (Nielsen et al., 2017, 2018), propeller cavitation (Vrijdag et al., 2007) or engine overloading (Planakis et al., 2021)) and the drivetrain modules are controlled in order to satisfy these objectives. Furthermore, some papers only discuss a single level of control (Nielsen et al., 2018; Planakis et al., 2021), while others deal with a multi-level control architecture (Haseltalab et al., 2016; Geertsma et al., 2017c; Haseltalab et al., 2018; Hou et al., 2018; Geertsma et al., 2018; Haseltalab &Negenborn, 2019). A comprehensive review of the multi-level power and propulsion architectures can be found in (Geertsma et al., 2017a). This Section will instead focus on showcasing the research gaps from the control agent design perspective in the different control levels and focusing on design adaptations.

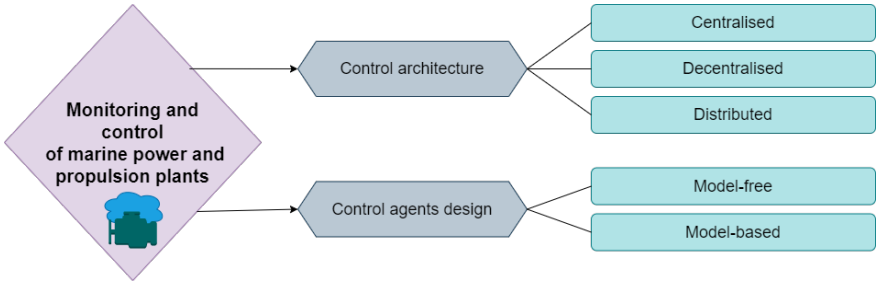


Figure 2.5: Classification of the control approaches employed for marine power and propulsion plants.

2.3.1 Primary control level

The primary level incorporates the local control agents of the systems present in the *PPP*. So far in marine literature, mostly model-free *Proportional–integral–derivative* (*PID*) agents are used for the Governors (Nielsen et al., 2017, 2018; Geertsma et al., 2017b,c, 2018), Electric motor controllers (Haseltalab et al., 2016, 2018; Haseltalab &Negenborn, 2019) and Energy storage controllers (Hou et al., 2018). However, in case of design adaptations and due to the low robustness level of the *PID* control agents, the control reconfiguration task will be tedious, increasing the costs and manual labor. Instead, the use of model-based approaches like *MPC* (Planakis et al., 2021) control agents or feedback linearisation techniques (Xinsheng et al., 2018) allows more flexibility for control reconfigurations. The model-based design also facilitates the expression of control stability guarantees, which can be of paramount importance during design adaptations. The efficiency of the control agents in this case depends on the accuracy of the considered models. However, in the majority of literature works, only simplified representations of the involved systems are considered, either excluding part of the dynamics (Haseltalab et al., 2018) or considering low order models (Zhang et al., 2020b).

Similar to other *CPS* applications, three types of control architecture are considered in the primary level: centralised, decentralised and distributed. From these three architectures, the majority of papers consider a decentralised configuration, with partitioning based on the physical system decomposition (Kalikatzarakis et al., 2018; Geertsma et al., 2018; Ni et al., 2019; Zhang et al., 2020b). Centralised approaches have also been extensively used, requiring though a complete control redesign in case of system adaptations. Regarding distributed approaches, in (Bidram et al., 2013), a distributed cooperative control of marine *AC* generators is performed. The generators' agents exchange information through the use of one-way communication links in a specified communication graph. However, the reference is known only to the first generator and no control sequence can be initiated without includ-

Table 2.2: Classification of existing literature on multi-agent primary control of marine power and propulsion plants based on the number of control agents, their design and the employed control architecture.

		Control agent design		**Control Architecture**			
Article(s)	**Number of agents**	Model-based	Model-free	Centralised	Decentralized	Distributed	**Stability guarantees**
(Nielsen et al., 2017; Haseltalab et al., 2018; Li et al., 2018; Vafamand et al., 2019; Planakis et al., 2021)	1	✓		✓			
(Geertsma et al., 2017c; Hu &Shi, 2021)	1		✓	✓			
(Geertsma et al., 2017b, 2018; Nielsen et al., 2018; Ni et al., 2019)	2		✓		✓		
(Kalikatzarakis et al., 2018)	3		✓		✓		
(Bidram et al., 2013)	4	✓				✓	
(Zohrabi &Abdelwahed, 2017)	2	✓				✓	
(Xinsheng et al., 2018)	3	✓				✓	
Zhang et al. (2020b)	2	✓			✓		
Contributions of this thesis							
Chapter 4 *(Kougiatsos et al., 2022a; Kougiatsos &Reppa, 2024a)*	1		✓	✓			
Chapter 5 *(Kougiatsos et al., 2024b)*	2	✓				✓	✓
Chapter 7 *(Kougiatsos et al., 2024a)*	6	✓	✓		✓		

ing it. The deviation from the nominal values of frequency and voltage given by the reference is restored using distributed control. As for the loads, these are assumed known. In the case of *DC* power networks, (Zohrabi &Abdelwahed, 2017) examines a distributed control scheme. The authors consider the use of a high level coordinator, responsible for the transmission of information amongst the different subsystems. In the low level, MPC control is used with the objective to maintain the bus voltage close to the specified value. An optimisation problem is solved at the high level which outputs the interactions between the different subsystems in the form of Lagrange multipliers. The low-level MPC controllers utilise this information and try to regulate the voltage with minimum control output fluctuation. In (Xinsheng et al., 2018), a distributed control approach is implemented for a vessel's power system. Two control strategies are employed; the voltage distributed cooperative control aiming to stabilise the generator voltages and the frequency distributed cooperative control aiming to stabilise the generator frequencies to the voltage and frequency reference values. The generators communicate with each other according to a specified connected graph again defining a leader node. In addition, (Vu et al., 2018) proposes a distributed MPC strategy for the energy management of a 4-zone sea vessel power system using the *Alterating Direction Method of Multipliers* (*ADMM*). The information exchanged between the agents consists of the neighbors' current and voltage values.

Table 2.2 classifies the existing literature on primary control of marine power and propulsion plants. Compared to the majority of the reviewed papers, in Chapter 5, we present a multi-agent distributed control scheme for a marine hybrid propulsion plant, composed of two model-based agents. Moreover, control stability guarantees are provided under healthy and faulty sensor conditions. Chapter 7 discusses a decentralised configuration for the control agents, mostly composed of PID controllers. However, a higher total number of control agents is considered compared to other relevant papers and model-based agents are introduced for the energy storage (battery constraint modules).

2.3.2 Secondary control level

The secondary level typically consists of a single centralised control agent providing the reference values for the primary level's agents. This can be accomplished either through an optimisation process based on the aforementioned global plant control objectives or using static curves, constraining the output values.

In both cases, the objectives are related to the minimisation of fuel consumption with the use of an *Equivalent fuel Consumption Minimisation Strategy* (*ECMS*) (Kalikatzarakis et al., 2018) or the maximisation of the energy performance of the *PPP* (Çetin &Sogut, 2021; Liang et al., 2022). However, the secondary control strategy often becomes specific to a selected topology and sizing and is thus unfit for

adapting to missions with different power requirements. Considering all-electric[2] power and propulsion plants, the secondary control level is represented by an energy management module (Haseltalab et al., 2016, 2018; Haseltalab &Negenborn, 2019). This module typically consists an *MPC* controller used to split the energy demand to the different power sources while minimising the fuel consumption. Power system losses and non-propulsive loads can also be taken into account in the optimisation process. In case of a design adaptation, the cost function should be modified with subsequent changes in the low-level controllers. Furthermore, the moderation of the plant and the flow of information to a single secondary control agent constitutes a single-point of failure which can further endanger safety onboard.

Mechanical and hybrid propulsion vessels most commonly employ strategies such as fuel consumption minimisation strategies and pitch control. A common secondary control strategy in this kind of vessels is the *ECMS* (Kalikatzarakis et al., 2018; Bassam et al., 2017). In this case, the centralised control agent solves an internal optimisation problem with the objective to minimise the fuel consumption. For electrical power sources (e.g., batteries), an equivalence factor is derived between the produced electrical energy and a certain quantity of fuel. The secondary level's outputs are the reference values to the main engines, batteries and generator sets. However, when uncertainties in the operational conditions exist in the plant, using a constant equivalence factor can lead to sub-optimal solutions. Thus, Kalikatzarakis et al. (2018) propose using an adaptive factor derived from historical data for the operational conditions, resulting in an *Adaptive Equivalent fuel Consumption Minimisation Strategy* (*A-ECMS*). The main issue with both *ECMS* and *A-ECMS* is that they consider a known operational profile, while this is not always available in practice. A-ECMS does not rely on this assumption but only uses information from a limited past time horizon. As a result, the quality of the decisions made by both strategies is limited.

For mechanical and hybrid vessels using *Controllable Pitch Propeller*s (*CPP*s), pitch control is often discussed, which controls the reference values to both the Fuel engine and the Propeller. Combinator curve control is commonly employed (Geertsma et al., 2017b,c). These curves correlate the needed engine angular speed and propeller pitch setpoints according to the speed lever setpoint of the vessel commanded by the operator. The purpose of the combinator curves is to provide a static operating point that is optimal for criteria like fuel efficiency, engine loading and propeller cavitation (Geertsma et al., 2017b). However, their limitation is that they are designed for a specific operational mode with specific environmental disturbances and hull fouling. As a result, the derived operation point which is optimal for the design conditions might be suboptimal for other modes and environments. Many

[2]All-electric signifies the use of electric propulsion. The power plant can be either AC, DC or Hybrid.

Table 2.3: Classification of existing literature on multi-agent secondary control of marine power and propulsion plants handling adaptations based on the design type, drivers to instigate control adaptations and control objectives (N/A: non applicable). Performance control objectives refer to energy performance.

	Design		**Adaptation driver**			**Control Objectives**	
Article(s)	Fixed	Adaptive	Regulations/ Technology	Mission	Malfunction	Fuel consumption	Performance
(Haseltalab et al., 2016; Zhang et al., 2020c; Vu et al., 2015)	✓		N/A	N/A	N/A	✓	✓
(Kalikatzarakis et al., 2018)	✓		N/A	N/A	N/A	✓	
(Geertsma et al., 2018; Vu et al., 2018; Zhang et al., 2020b; Çetin &Sogut, 2021; Liang et al., 2022)	✓		N/A	N/A	N/A		✓
(Zhang et al., 2023)		✓		✓			✓
(Kerrigan &Maciejowski, 1999)		✓			✓		✓
Contributions of this thesis							
Chapter 5 *(Kougiatsos et al., 2022b, 2024b)*		✓			✓		✓
Chapter 7 *(Kougiatsos et al., 2024a)*		✓		✓	✓	✓	✓

workarounds have been proposed on this matter such as using multiple combinator curves (Geertsma et al., 2017c) instead of one for the different operational modes of the vessel and pitch reduction to prevent engine overloading (Vrijdag et al., 2007). However, in case the engine or the propeller should be replaced, the combinator curves must be derived from scratch. Even if no change occurs, the fouling of the hull will gradually alter the service conditions for which combinator curves are derived leading to poor performance. The authors in (Geertsma et al., 2018) have also proposed an adaptive pitch controller that does not use static combinator curves while outperforming in multiple measures of efficiency. This is accomplished again in a centralised configuration that produces also an extra output, the estimated hydrodynamic pitch angle.

Considering an adaptive design of the *PPP*, Zhang et al. (2023) consider swapping battery energy storage between stations on inland waterways. The voyage scheduling and energy management are both optimised in a joint optimisation problem. Another approach includes the design of multiple energy management strategies based on known iterations of the *PPP* topology to adapt to new missions and a digital supervisor installed to switch between these strategies during operation (Sørensen, 2011; Bertaska &von Ellenrieder, 2018). Nevertheless, so far in marine literature, the technical aspects regarding the implementation of the digital supervisor have not been explored. Moreover, the authors of (Kerrigan &Maciejowski, 1999) considered system malfunctions as an adaptation driver in a single engine/ propeller model and designed the secondary control agent using an *MPC* approach. However, only simplified linearised models based on lookup tables were considered for the controller design.

Figure 2.5 summarises the different control approaches, while Table 2.3 classifies the reviewed papers on secondary control of marine power and propulsion plants and showcases the additional contributions of this thesis. In contrast to the majority of literature works, Chapters 5 and 7 consider an adaptive design for the *PPP*, subject to one or multiple adaptation drivers respectively. Finally, Chapter 7 defines the secondary control agent using both fuel consumption and energy performance objectives, in contrast to the majority of papers only considering a single control objective.

2.4 Consideration of vulnerabilities

The digitalization of on-board systems, the integration of novel sensors and the development of more sophisticated control architectures towards greater degrees of autonomy, gradually leads to cyber-enabled ships. As a result, similar to other CPSs, marine power and propulsion plants are becoming more and more susceptible to numerous vulnerabilities. The operational and condition-based monitoring

Table 2.4: Summary of the physical quantities measured and used for the monitoring and control of marine power and propulsion plants

System	Measured quantities	Sources
*Internal Combustion Engine*s (*ICE*s)	Fuel injection; Emissions; Temperature; Pressure; Torque; Shaft angular speed	(Jones &Li, 2000; Zhang et al., 2008; Li et al., 2012b; Hu et al., 2018; Qi et al., 2020)
Electric Motors	Temperature;Air gap flow; Current; Sound emissions; Torque; Shaft angular speed;	(Ostojic &Stinson, 2013; Djagarov et al., 2019)
Generators	Voltage; Current; Frequency; Rotation angle of the crankshaft; Shaft angular speed	(Gasparjan et al., 2015)
Batteries	Temperature; Current; Voltage	(García et al., 2019)

task, thus, becomes more and more important for vessel-wide resiliency (Kougiatsos &Reppa, 2024a). The vulnerabilities can be either intentional (cyber-attacks) or non-intentional (sensor faults; process faults).

Current literature on marine power and propulsion systems has addressed the diagnosis of process faults while sensor faults have mostly been overlooked. However, one or more sensors reporting erroneous information could result in masking of process faults, unneeded maintenance and flawed decision making by operators (MACSEA, 2012). A misstep in the onboard decision making during voyage will in turn affect the lives onboard the vessel, the transported cargo and possibly the environment. In addition, due to the larger size of engines, limited operator access as well as the highly uncertain sea environment, the consequences of a wrong decision regarding faults are in most cases greater in a marine system than a land-based system (Wang et al., 2017).

The fault diagnosis of marine *Internal Combustion Engine*s (*ICE*s) typically takes into account only single sensor values (MACSEA, 2012) while a marine ICE can incorporate 15-17 sensors (Raptodimos et al., 2016). Table 2.4 summarises the physical quantities that are usually measured and used for control and monitoring purposes in literature. Making use of the complete sensor network has been proven useful in effectively supporting decision making onboard marine vessels (Zhang et al., 2022). Moreover, the occurrence of multiple sensor faults has become a significant problem to tackle, due to the large number of sensors distributed in marine systems (Jones &Li, 2000). Although more realistic, this problem has not yet received much attention in the relevant literature.

Cyber-attacks are also a growing concern especially for control networks be-

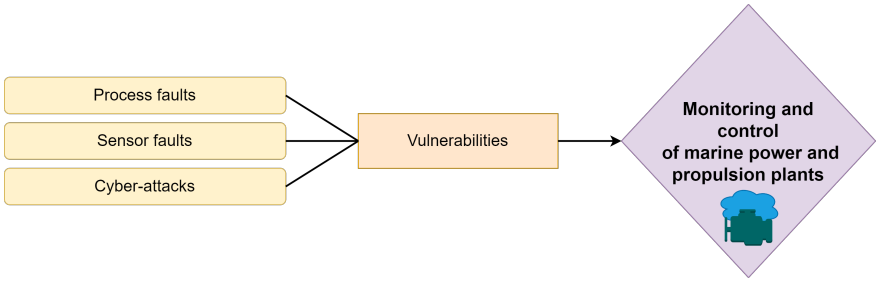


Figure 2.6: Summary of the considered vulnerabilities examined in marine literature and affecting marine power and propulsion plants.

cause they are at the core of many critical infrastructures (Amin et al., 2009). Some of the consequences that cyber-attacks will have on a *PPP* include component failures, loss of propulsion, power blackouts, temporarily or permanently damaged systems or the disruption of operation. From all the different categories of attacks examined in the Cyber-security literature (Ferrari &Teixeira, 2021), false data injection attacks and *Denial-of-Service* (*DoS*) attacks are considered most common in marine power and propulsion plants (Caprolu et al., 2020; Bolbot et al., 2022). A summary of the considered vulnerabilities in marine *PPP*s is shown in Figure 2.6.

2.5 Monitoring methods for marine power and propulsion plants

2.5.1 Fault Detection & Isolation

The monitoring of marine *PPP*s is attracting increasing interest in literature . Most papers use quantitative methods for their approach based on observers, parity equations and neural networks to perform the monitoring and a centralised monitoring approach. Regarding process faults, in (Sonandkar et al., 2020), the diagnosis is based on parity equations and a fixed threshold value arbitrarily chosen by the authors. The authors of (Cai et al., 2017; Wang et al., 2020) instead rely on a data-driven approaches based on *SVM*s and back propagation neural networks, respectively, to diagnose process faults on marine diesel engines. In (Zhou et al., 2018), the authors also apply a *SVM* method to diagnose process faults in a simplified ship propulsion system. In data-driven approaches, classification of system components as healthy or faulty mostly occurs using fixed classes. Nevertheless, in (Li et al., 2019; Listou Ellefsen et al., 2020; Liu et al., 2021) adaptive thresholds are proposed for the classes based on the vessel's operational characteristics. In addition, the data-driven methods require a substantial amount of data from the system under healthy conditions as well as under several faulty conditions for training purposes.

Regarding sensor faults, the authors of (Mesbahi, 2001; Zhang et al., 2019) apply neural network or *SVM* techniques, respectively, to validate the coherence of sensor measurements, isolate faulty sensors and recover the lost information from other measurements for marine *ICE*s. However, only single faults are considered and again a substantial amount of data is required for training purposes, including both healthy and faulty conditions. The authors of (Perera, 2016) in their work propose fault detection in two levels regarding sensors used for ship performance analysis (e.g., shaft speed, fuel consumption sensors). The first level's purpose is to detect faults like repeated data points and data points outside selected fixed thresholds. Using fixed thresholds may increase the conservativeness of the approach and careful selection is essential to minimise false alarms. Then the second level's aim is to detect in-range sensor faults by using localised models constructed by the data and Principal Component Analysis. The models though only describe three regions of operation for the engine. In (Yang &Shi, 2018), the authors develop a particle swarm optimisation neural network algorithm for diagnosis purposes but omit the performance analysis of the monitoring approach. (Tsaganos et al., 2018) focuses on the diagnosis of faults related to multiple sensors (e.g., shaft speed, pressure, temperature sensors) of marine *ICE*s. To this end, data from an engine simulator are used based on different fault scenarios and multiple model-free algorithms are tested and compared to these data-sets. The results showcase performance-wise superiority of the AdaBoost Algorithm with a Simple Cart base classifier. The limitation in this case is that the algorithm requires more time for classification. Hu et al. (2018) perform temperature sensor fault detection for a selective catalyst reduction system built upon an *ICE* using a suitable temperature model and an observer based on the Extended Kalman Filter. In the decision-making process though, the authors choose an arbitrary threshold to perform fault detection, which may lead to missed detection of sensor faults or false alarms if it is not well selected. In (Wohlthan et al., 2021), a model-based sensor fault diagnosis method is proposed for engine test beds using a multi-stage geometric analysis of the extracted residuals. However, this method considers static models and single sensor fault occurrence. Finally, (Stoumpos &Theotokatos, 2022) discusses a Unified Digital System for diagnosis and health management for dual fuel marine engines by combining a thermodynamic model with data driven methods to diagnose sensor faults and compensate for their effects. More precisely, a feed-forward neural network approach is used, enhanced by expert knowledge to improve isolation while considering two case studies where faults occur at two engine sensors simultaneously. This work lacks the performance analysis or experimental validation of the proposed approach.

Table 2.5 summarises the reviewed literature on monitoring methods currently employed for marine power and propulsion plants. In contrast to the majority of

Table 2.5: Summary of the employed monitoring methods against the effects of faults for marine power and propulsion plants (SF: sensor faults; PF: process faults)

			Threshold design		**Monitoring architecture**			
Article(s)	**Method**	**Fault scenario**	Adaptive	Fixed	Centralised	Decentralised	Distributed	**Validation**
(Li et al., 2019; Listou Ellefsen et al., 2020; Liu et al., 2021)	Model-free	PF, Single faults	✓	✓	✓			
(Cai et al., 2017; Wang et al., 2020)	Model-free	PF, Multiple faults		✓	✓			✓
(Zhou et al., 2018)	Model-free	PF, Multiple faults		✓	✓			
(Sonandkar et al., 2020)	Model-based	PF, Single faults		✓	✓			
(Mesbahi, 2001; Perera, 2016; Zhang et al., 2019)	Model-free	SF, Single faults		✓	✓			
(Tsaganos et al., 2018; Yang &Shi, 2018)	Model-free	SF, Multiple faults		✓	✓			
(Wohlthan et al., 2021)	Model-based	SF, Single faults		✓	✓			
(Hu et al., 2018; Stoumpos &Theotokatos, 2022)	Model-based	SF, Multiple faults		✓	✓			
Contributions of the present thesis								
Chapters 4, 6 *(Kougiatsos et al., 2022a; Kougiatsos &Reppa, 2024a)*	Model-based	SF, Multiple faults	✓				✓	✓

papers employing a centralised monitoring architecture, this thesis explores a distributed architecture in Chapters 4 and 6. This consideration is particularly useful in large scale applications such as marine power and propulsion plants for isolation purposes. The use of adaptive thresholds instead of fixed ones allows for reducing the conservativeness in decision making of the monitoring agents, ensuring the absence of false alarms and minimising the rate of missed sensor fault detections. Compared to the model-based monitoring literature, Chapter 4 includes the performance analysis of the proposed monitoring scheme, in terms of both detectability and isolability characteristics, which can prove useful for certification purposes. Finally, Chapter 6 proposes an optimisation algorithm for sensor fault isolability in marine power and propulsion plants.

2.5.2 Cybersecurity algorithms

The topic of cybersecurity is relatively new in marine literature and associated with many additional issues and challenges (Caprolu et al., 2020). Despite this, certain approaches described for other applications such as networks of systems or microgrids are also promising for marine applications. In (Velarde et al., 2018), a secure

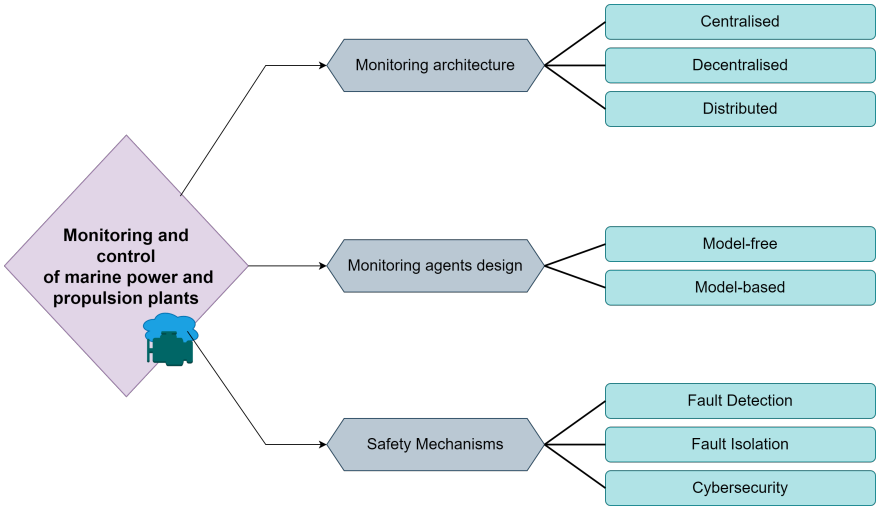


Figure 2.7: Classification of the monitoring approaches employed for marine power and propulsion plants.

dual-decomposition-based distributed MPC algorithm is proposed in case of one local controller attack to the distributed network. The agent tries to benefit from the negotiation process by altering its own cost function to steer the negotiation process. The proposed strategy, on the other hand, tries to prevent the agent from doing so by finding it and ignoring its participation in the rest of the negotiation process. This task is accomplished by having each agent ignore the largest and the smallest interconnection values received by its neighbors, a resilient method proposed in fault tolerant distributed algorithms literature. Kurt et al. (Kurt et al., 2018) on their side deal with the detection of false data injection and denial of service attacks in a distributed framework. To this end, observer-based attack detectors are designed in a distributed configuration and benchmarked using several numerical case studies. A similar observer-based attack detection approach is also used in (Gallo et al., 2018) for distributed DC Microgrids while in other works such as (Cui et al., 2020) machine learning techniques are employed for the detection purposes. The classification of monitoring approaches can be seen in Figure 2.7.

2.6 Resilience against system adaptations

2.6.1 Redundancy considerations

In the presence of vulnerabilities affecting the on-board systems or sensors, additional hardware redundancy in the design has been extensively proposed as a way to recover operation, both in literature and in practice (Wu et al., 2006; DNV, 2012).

This design philosophy, however, translates to greater installation and maintenance costs assumed by the shipowner. Alternatively, the availability of multiple heterogeneous systems and sensors in the *PPP* can be utilised in coupling with model information to construct virtual/ software-based components, also referred to as the analytical redundancy of the system. The use of analytical redundancy has not been properly investigated yet for maritime applications, with only a small amount of papers referring to virtual thrusters (Fu et al., 2011; Lin &Du, 2016; Zhang et al., 2020a) or virtual sensors (Kerrigan &Maciejowski, 1999; Darvishi et al., 2021). However, other fields like induction motor control (Adamczyk &Orlowska-Kowalska, 2019), process control (Stoican et al., 2014) and smart buildings (Reppa et al., 2014) have more efficiently integrated these technologies.

The efficiency of the virtual component design highly depends on the accuracy of the considered training data or models. Considering data-driven approaches, in (Campa et al., 2008), a sensor validation scheme for heavy-duty diesel engines is proposed using a hybrid scheme composed of Adaptive Linear Neural Networks for linear engine operating conditions as well as Minimal Resource Allocating Networks for non-linear engine conditions to create virtual sensors. In (Li et al., 2019), the values of various hardware heterogeneous sensors are used as inputs to a neural approximator for the temperature forecast of marine propulsion plants. The forecast is then compared to the actual sensor measurement to identify sensor faults. Moreover, the authors of (Darvishi et al., 2021) propose a machine-learning-based framework for sensor validation considering a multi-layer perceptron neural network architecture for vessels. The virtual sensor design is validated in their work in terms of the probability density function of the error signals on each of the used data-sets, considering ranges for the number of network nodes and hidden layers. However, the proposed model-free approaches often require a high number of neurons to calculate the output due to the high system nonlinearity. The produced results are also characterized by low generalization ability due to the lack of standardization in the propulsion plants of different vessels.

Regarding model-based approaches, the authors of (Li et al., 2012a) combine the information of multiple hardware vibration sensors with vibration and wear particle analysis models for the diagnosis of the tribo-system of marine ICEs. In (Kerrigan &Maciejowski, 1999), the authors deal with both process and sensor faults in marine propulsion plants. For the latter, a Kalman estimator technique is used to reconstruct the measurements of the faulty sensors. However, only simplified models with linear dynamics or representing part of the involved processes have been used so far in the existing literature to design the virtual sensors (Blanke et al., 2016). The validation of the virtual sensor design through the use of *Key Performance Indicator*s (*KPI*s) is also currently lacking from model-based approaches.

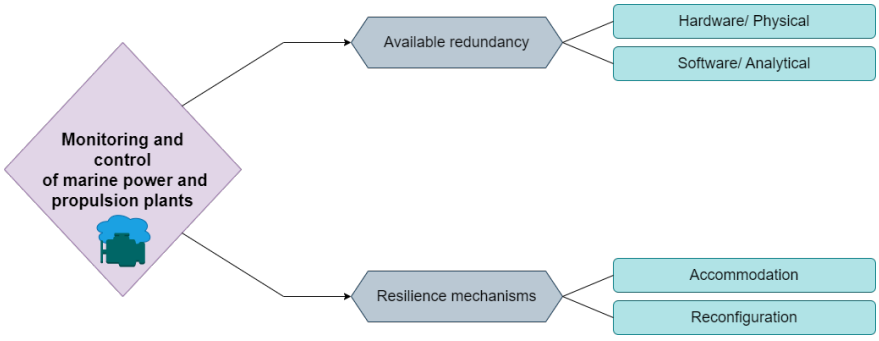


Figure 2.8: Summary of the considered redundancy and resilience mechanisms in marine power and propulsion plants.

Table 2.6: Classification of the resilient control methods found in the marine literature based on the considered control levels, adaptation driver(s), employed resilience mechanism and available type(s) of redundancy (SF: sensor faults; PF: process faults; CA: cyber-attacks)

			Resilience mechanism		**Redundancy**	
Article(s)	**Control level**	**Adaptation driver(s)**	Accommodation	Reconfiguration	Hardware	Analytical
(Bo &Johansen, 2013)	Multi-level	PF		✓	✓	
(Kerrigan &Maciejowski, 1999)	Secondary	PF, SF	✓	✓		✓
(Li et al., 2017)	Multi-level	CA		✓	✓	
(Sonandkar et al., 2020)	Primary	PF		✓	✓	
(Darvishi et al., 2021; Stoumpos &Theotokatos, 2022)	Primary	SF	✓			✓
(Vu et al., 2015)	Secondary	Mission		✓	✓	
Contributions of the present thesis						
Chapter 5 *(Kougiatsos &Reppa, 2022; Kougiatsos et al., 2022b, 2024b)*	Multi-level	SF	✓	✓		✓
Chapter 7 *(Kougiatsos et al., 2023, 2024a)*	Multi-level	Mission, SF, CA		✓	✓	✓

2.6.2 Resilience mechanisms

By employing both hardware and analytical redundancy, the safety and resilience of the *PPP* will be augmented. For instance, when sensors are affected by faults, system and control stability can be ensured by switching between hardware and virtual sensors.

Nowadays, an increasing number of resilience mechanisms are developed to

ensure the safe operation of marine vessels, optimise their *PPP* topology and reduce costs. The authors of (Sadjina et al., 2019) propose a co-simulation platform (coupling of simulators) that will enable fast and reliable testing and optimisation of vessel system and automation designs before construction, and that can also be used for training purposes of crews during the vessel's life cycle. However, they excluded closed-loop control systems from the case studies while the applicability of the method requires the machinery models the manufacturers are willing to provide for the platform. In (Vu et al., 2015), adaptations of the *PPP* to known and unknown power profiles is investigated. To this end, a secondary level control strategy with prediction abilities over unknown profiles is developed for a hybrid plant and bench-marked against a conventional rule-based approach. Nevertheless, only hardware redundancy was assumed and the occurrence of faults during the operational phase of the vessel was not explored as an additional adaptation mechanism for the installed system configuration during operation.

Under the occurrence of faults, the authors of (Kerrigan &Maciejowski, 1999) considered both process and sensor faults for a ship propulsion system case study with accommodation and reconfiguration strategies used in each case, respectively. Accommodation is made possible through the use of an *MPC* controller while virtual sensors based on Kalman estimators were utilised against sensor faults. The design of the *MPC* was based, though, on a rather simplistic propulsion model expressed by lookup tables. Stoumpos &Theotokatos (2022), on their end, propose a Unified Digital System to accommodate the effects of sensor faults after their diagnosis, for a marine dual fuel engine, based on a low order engine model (zero-dimensional/one-dimensional). A similar accommodation approach from the data-driven perspective is presented in (Darvishi et al., 2021), with virtual sensors being designed to estimate the sensor fault magnitude. However, in both cases the effects of other vulnerabilities such as process faults and cyberattacks are excluded from the analysis. The control reconfiguration under the effects of process faults are investigated in (Sonandkar et al., 2020) considering an electric motor application with process faults affecting one of the motor's phases. To mitigate the fault effects, the phase current references are subsequently reconfigured. Even so, the ability for reconfiguration is limited by the fault magnitude and the available hardware redundancy in the motor's phases. In addition, only a single level of control was assumed in all of the above papers, following a centralised configuration. A multi-level control application is instead considered in (Bo &Johansen, 2013; Li et al., 2017), but only assuming hardware redundancy and a single type of vulnerability.

Table 2.6 classifies the aforementioned resilient control approaches in marine literature based on the considered control levels, adaptation driver(s), employed resilience mechanism and considered type(s) of redundancy. Moreover, the contributions of the present thesis are highlighted. As can be seen, in both Chapter 5 and 7,

a multi-level control scheme is considered with control reconfiguration capabilities, in contrast to the majority of the reviewed papers. The analytical redundancy of the system, expressed through the model-based design of virtual sensors is explored in both chapters, and combined with the available hardware redundancy in the systems of the *PPP* in Chapter 7. Moreover, the virtual sensors are also used for accommodation considering the monitoring task in Chapter 5. Finally, a major contribution compared to the existing literature is the consideration of multiple change mechanisms affecting the same hybrid *PPP*, such as offline changes in mission characteristics and the online occurrence of vulnerabilities (sensor faults and cyberattacks), in Chapter 7. A summary of the considered redundancy and resilience mechanisms in marine power and propulsion plants is provided in Figure 2.8.

2.7 Conclusions

This chapter reviews the existing works on the monitoring and resilient control of marine *PPP*s. It addresses the first research question (**Q1:**) *"What are the state-of-the-art, state-of-practice and research gaps regarding the monitoring and resilient control of marine power and propulsion plants?"*

Inspired by the relevant literature in the field of adaptive *CPS*s, the different control and monitoring approaches for marine *PPP*s were classified based on the drivers leading to design adaptations, the types of adaptations and the physical system characteristics. The control and monitoring architectures were then classified in three categories: centralised, decentralised and distributed. For each architecture, its definition and basic steps for its construction were discussed in detail. It was found that in the multi-agent control architecture, mostly centralised or decentralised control agents were involved. In the primary control level the control agents mostly followed a model-free *PID* design, offering little flexibility for control adaptations. Despite the existence of certain model-based techniques, the majority of relevant papers only consider simplified system representations of marine *PPP*s. Moreover, the secondary level control agent is usually designed for a fixed *PPP* layout and only considers one type of objective, either energy performance or fuel consumption.

The available literature on vulnerabilities affecting *PPP*s was also analyzed and it was found that sensor fault and cyberattack scenarios are mostly omitted in marine literature. The state-of-the-art in monitoring methods for safe control were discussed, distinguishing between approaches used for faults and those employed for cyberattacks. Mostly centralised monitoring approaches are so far discussed in marine literature, while the performance analysis of the monitoring scheme is omitted. In addition, most relevant papers propose the use of fixed and arbitrarily set thresholds for detection purposes, a design choice that increases the conservativeness in decision making and can potentially lead to false alarms and missed detections.

Considering the available resilience of marine *PPP*s against design adaptations, the relevant literature was extensively discussed in terms of the considered redundancy for fail-safe operation and the proposed resilience mechanisms. We found that, in most cases, hardware redundancy is considered while only few papers consider analytical redundancy. The majority of marine literature considers adaptations based on either faults, cyberattacks or changes in the vessel's mission and only a single level of control. Thus, control adaptations due to more than one adaptation drivers and concerning a multi-level control scheme has been so far mostly overlooked. The complete classification of available literature on the monitoring and resilient control of marine *PPP*s can be seen in Figure 2.9.

Based on the above findings, to handle the complexity of the *PPP*, quantitative and qualitative models are developed in Chapter 3 and used for the remainder of this thesis. A distributed model-based monitoring approach for marine *ICE*s applications is developed in Chapter 4 to facilitate adaptations, and its performance analysis is presented based on detectability and isolability-based *KPI*s. The isolability of the distributed approach is optimised in Chapter 6, including the addition of an induction motor in the system architecture. Finally, the utilisation of analytical redundancy and further resilience mechanisms for marine *PPP*s, such as a multi-sensory switching framework and an intelligent automation supervisor, are presented in Chapters 5 and 7.

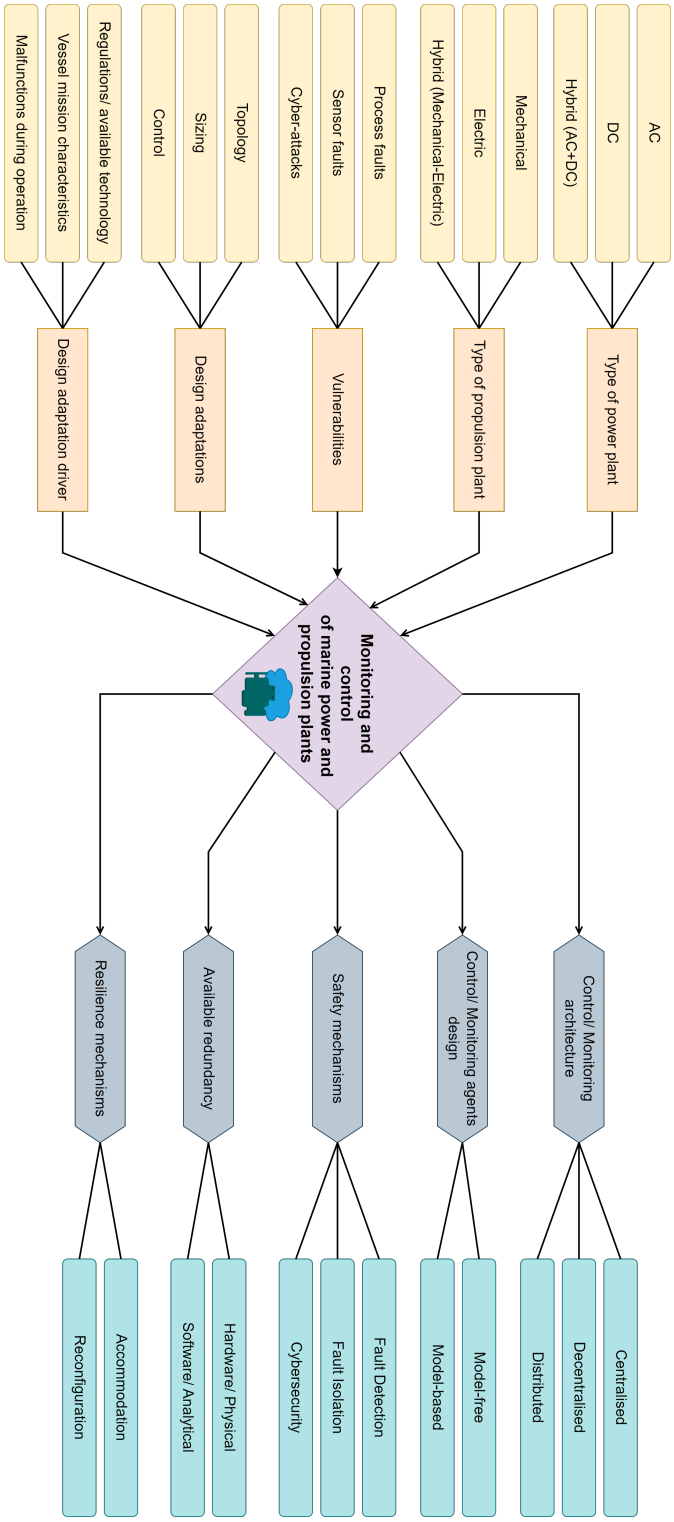


Figure 2.9: A detailed review outline regarding the monitoring and control of marine power and propulsion plants

Chapter 3

Power and propulsion plant modelling

In this chapter, we address the second research question, that is (**Q2:**) *"How to derive models of marine power and propulsion systems for monitoring and resilient control purposes?"*. This chapter is organised as follows. In Section 3.1, the general description of Differential-Algebraic systems is formulated. This description is then used in all of the considered *PPP* systems in Sections 3.2-3.6. Qualitative models, using semantics, are then provided for use in marine *PPP*s in Section 3.7, followed by concluding remarks in Section 3.8.

The contents of this chapter have been partially included in two journal publications (Kougiatsos et al., 2024a) [1], (Kougiatsos et al., 2024b)[2]

3.1 Differential-Algebraic modelling

Marine *PPP*s can be decomposed in multiple interconnected subsystems $\Sigma^{(I)}$, $I = 1, \cdots, N$, characterized by high complexity. The first principle models of each subsystem $\Sigma^{(I)}$, stemming from literature and used in the context of this thesis, are formulated using the formulation shown in (3.1), (3.2) and presented in Sections 3.2-3.6. The subsystem models are used for the development of safe and resilient control approaches. In order to handle tasks like the derivation of adaptive thresholds (Chapter 4), subsystem output approximation and nonlinear control (Chapter 5) , it is useful to distinguish between the linear, nonlinear and interconnection dynamics of the different subsystems (Reppa et al., 2016; Farrell &Polycarpou, 2006).

[1] **N. Kougiatsos**, E.L Scheffers, M.C. van Benten, D.L. Schott, P. de Vos, R.R. Negenborn, and V. Reppa, "An intelligent topology and control design framework for mission-adaptive marine power and propulsion plants," submitted to a journal, 2024.

[2] **N. Kougiatsos**, M. Vagia, R.R. Negenborn, and V. Reppa, "Fault-resilient multi-agent control for marine hybrid propulsion plants," submitted to a journal, 2024.

The Differential-Algebraic dynamics of each subsystem $\Sigma^{(I)}$, $I = 1, \cdots, N$ are, thus, mathematically described as (Vemuri et al., 2001):

$$\Sigma^{(I)} : \begin{cases} \dot{x}^{(I)}(t) = A^{(I)}x^{(I)}(t) + \gamma^{(I)}(x^{(I)}(t), z^{(I)}(t), u^{(I)}(t)) + h^{(I)}(x^{(I)}(t), z^{(I)}(t), \chi^{(I)}(t), u^{(I)}(t)), & \text{(3.1a)} \\ 0 = \xi^{(I)}(x^{(I)}(t), z^{(I)}(t), \chi^{(I)}(t), u^{(I)}(t)), & \text{(3.1b)} \end{cases}$$

where $x^{(I)} \in \mathbb{R}^{n_I - r_I}$ is the state variable vector, $z^{(I)} \in \mathbb{R}^{r_I}$ is the algebraic variable vector, $\chi^{(I)} \in \mathbb{R}^{k_I}$ are the interconnection variables from the neighbouring subsystems, $u^{(I)} \in \mathbb{R}^{l_I}$ is the control input vector, $\gamma^{(I)} : \mathbb{R}^{n_I - r_I} \times \mathbb{R}^{l_I} \mapsto \mathbb{R}^{n_I - r_I}$ represents the known nonlinear system dynamics, $h^{(I)} : \mathbb{R}^{n_I - r_I} \times \mathbb{R}^{r_I} \times \mathbb{R}^{k_I} \times \mathbb{R}^{l_I} \mapsto \mathbb{R}^{n_I - r_I}$ represents the known interconnection dynamics with the neighbouring subsystems, $\xi^{(I)} : \mathbb{R}^{n_I} \times \mathbb{R}^{k_I} \times \mathbb{R}^{l_I} \mapsto \mathbb{R}^{n_I - r_I}$ is a smooth vector field. The term $A^{(I)}x^{(I)}$ represents the linear part of the system's $\Sigma^{(I)}$ dynamics, where $A^{(I)} \in \mathbb{R}^{(n_I - r_I) \times (n_I - r_I)}$ is assumed known.

Each subsystem $\Sigma^{(I)}$, $I = 1, \cdots, N$ incorporates a set of hardware sensors $\mathcal{S}^{(I)} = \bigcup_{k=1}^{m_I} S^{(I)}\{k\}$ described as (Reppa et al., 2016):

$$S^{(I)} : y^{(I)}(t) = C^{(I)} \cdot \begin{bmatrix} x^{(I)}(t) \\ z^{(I)}(t) \end{bmatrix} + d^{(I)}(t) + f^{(I)}(t), \tag{3.2}$$

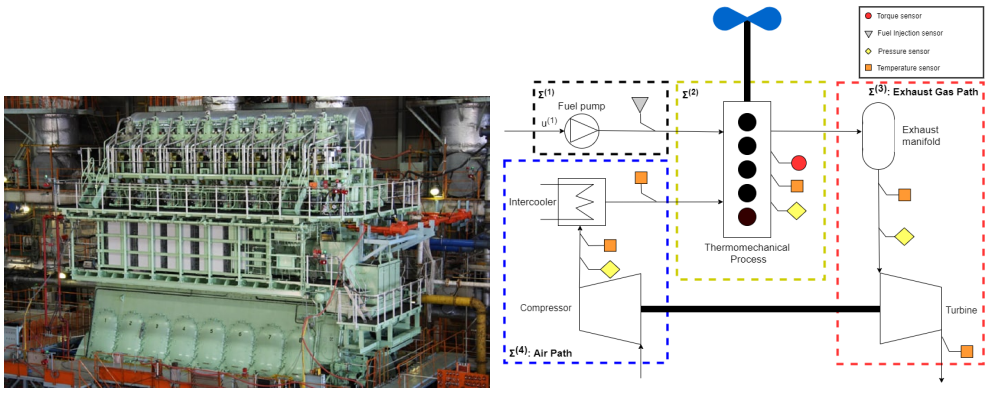
where $y^{(I)} \in \mathbb{R}^{m_I}$ denotes the hardware sensor measurements, $C^{(I)} \in \mathbb{R}^{m_I \times n_I}$ is the observability matrix, $d^{(I)} \in \mathbb{R}^{m_I}$ are the measurement noise vectors and $f^{(I)} \in \mathbb{R}^{m_I}$ are the sensor fault vectors. Each fault vector is given by $f^{(I)}(t) = [f_1^{(I)}(t), \cdots, f_{m_I}^{(I)}(t)]^\top$, where $f_k^{(I)}(t), k \in \{1, \cdots, n_I\}$ denotes the change in the output due to a fault in the k-th hardware sensor. Permanent abrupt faults can be modelled as follows Reppa et al. (2016):

$$f_j^{(I)}(t) = \begin{cases} 0, & t < T_{f_j}^{(I)} \\ \hat{\phi}_j^{(I)}(t), & t \geqslant T_{f_j}^{(I)} \end{cases}, \tag{3.3}$$

where $T_{f_j}^{(I)}$ is the time instant of occurrence of the j-th fault and $\hat{\phi}_j^{(I)}$ is its fault magnitude. The subsystem models in Sections 3.2-3.6 are presented in order to highlight the involved non-linearities and to assist in the reproducibility of the obtained results with the proposed methods in Chapters 4-7.

3.2 Marine *ICE* models

Marine *ICE*s are complex systems incorporating components characterised by heterogeneous dynamics and inherent interconnections. In Fig. 3.1b a simplified representation of a marine ICE is shown, where the different parts are grouped in four



(a) *(b)*

Figure 3.1: (a) Real-scale example (Group, 2024) and (b) 2-D Schematic representation of a typical marine ICE *(Kougiatsos &Reppa, 2024a).*

distinct subsystems and a total of ten sensors are deployed for condition monitoring. Subsystem 1 ($\Sigma^{(1)}$) incorporates the fuel pump, used to supply fuel to the engine's cylinders and its output fuel injection sensor. Subsystem 2 ($\Sigma^{(2)}$) is the thermomechanical process which refers to both the thermal and mechanical processes occurring inside the engine. As fuel oil, air and exhaust gases are all present in this block, it is characterised by heterogeneous dynamics. One pressure, one temperature and one torque sensor are considered for this subsystem. Subsystem 3 ($\Sigma^{(3)}$) consists of the exhaust manifold and the turbine, both handling the exhaust gas, having therefore similar dynamics. As for the sensors, a pressure sensor after the exhaust manifold and two temperature sensors before and after the turbine are considered. Finally, subsystem 4 ($\Sigma^{(4)}$) includes the compressor and the intercooler of the engine, both dealing with the air supply. A pressure sensor is considered after the compressor as well as two temperature sensors before and after the intercooler.

3.2.1 Fuel Pump

Subsystem 1 is expressed as (Geertsma et al., 2017c):

$$\Sigma^{(1)} : \dot{x}^{(1)}(t) = -\frac{1}{\tau_X} x^{(1)}(t) + \frac{x^{(1)}_{nom}}{\tau_X} u^{(1)}(t), \tag{3.4}$$

sec where $x^{(1)}(t) \in \mathbb{R}$ is the amount of fuel injected per cylinder per engine cycle in $[kg]$, $x^{(1)}_{nom} \in \mathbb{R}$ signifies the same quantity under nominal engine conditions, $u^{(1)}(t) \in \mathbb{R}$ is the fuel injection setting in $[\%]$, and $\tau_X = \frac{1}{4n^{nom}_{fe}}$ is the fuel injection time delay

in [*sec*]. The nominal fuel injection amount $x_{nom}^{(1)}$ is expressed as:

$$x_{nom}^{(1)} = \frac{SFC^{nom} P_{fe}^{nom} k_e}{i_e n_{fe}^{nom}}, \tag{3.5}$$

where n_{fe}^{nom} is the nominal rotational engine speed in [rps], SFC^{nom} is the nominal fuel consumption of the engine in [kg/Wh], P_{fe}^{nom} denotes the nominal power output of the engine in [W], i_e is the number of engine cylinders and k_e denotes the number of crank revolutions per engine cycle ($k_e = 1$ for a 2-stroke engine and $k_e = 2$ for a 4-stroke engine). The output of the fuel injection sensor $y^{(1)} \in \mathbb{R}$ is described by:

$$\mathcal{S}^{(1)} : y^{(1)}(t) = x^{(1)}(t) + d^{(1)}(t) + f^{(1)}(t). \tag{3.6}$$

3.2.2 Thermomechanical process

This subsystem has 3 algebraic variables, namely the pressure ($z_1^{(2)}(t)$) in [Pa] and the temperature ($z_2^{(2)}(t)$) in [K] inside the engine's cylinders and the engine's shaft torque ($z_3^{(2)}(t)$) in [Nm]. The mathematical representation of the system is:

$$\begin{aligned} \Sigma^{(2)} : 0 &= \begin{bmatrix} z_1^{(2)} - \xi_{z1}^{(2)}(x^{(1)}, x^{(4)}, z_1^{(4)}) \\ z_2^{(2)} - \xi_{z2}^{(2)}(x^{(1)}, x^{(4)}, z_1^{(4)}) \\ z_3^{(2)} - \xi_{z3}^{(2)}(x^{(1)}, z_3^{(2)}, x^{(4)}, z_1^{(4)}) \end{bmatrix} \\ &= \xi^{(2)}(x^{(1)}, z^{(2)}, x^{(4)}, z_1^{(4)}), \end{aligned} \tag{3.7}$$

where the functions $\xi_{z1}^{(2)}, \xi_{z2}^{(2)}, \xi_{z3}^{(2)} \in \mathbb{R}$ can be modelled using the Seilinger thermodynamic cycle as follows Geertsma et al. (2017c):

$$\begin{aligned} \xi_{z1}^{(2)} =& x^{(4)} r_c^{\kappa_a} \left(1 + \frac{\frac{1}{c_{v,a}} \left(X_{cv} \frac{\eta h_L R_a}{v_1} \frac{z_1^{(4)}}{x^{(4)}} x^{(1)} \right)}{z_1^{(4)}(t) r_c^{(\kappa_a - 1)}} \right) \cdot \\ & \left(\frac{r_{eo} r_c}{1 + \frac{(1 - X_{cv} - X_{ct}) \frac{\eta h_L R_a}{v_1} \frac{z_1^{(4)}}{x^{(4)}} x^{(1)}}{\left(z_1^{(4)}(t) r_c^{(\kappa_a - 1)} + \frac{X_{cv} \frac{\eta h_L R_a}{v_1} \frac{z_1^{(4)}}{x^{(4)}} x^{(1)}}{c_{v,a}} \right) c_{p,a}}} \right)^{-n_{exp}} \cdot \\ & e^{- \frac{(n_{exp} - 1) X_{ct} \frac{\eta h_L}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)}}{1 + \frac{X_{cv} \frac{\eta h_L R_a}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)}}{c_{v,a}} + \frac{(1 - X_{cv} - X_{ct}) \frac{\eta h_L R_a}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)}}{c_{p,a}}}}, \end{aligned} \tag{3.8}$$

$$
\begin{aligned}
\xi_{z2}^{(2)} =& \left(1 + \frac{\frac{\eta h_L R_a}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)} \left(c_{p,a} X_{cv} + c_{v,a}(1 - X_{cv} - Xct) \right)}{c_{v,a} c_{p,a}} \right) \cdot \\
& \left(\frac{r_{eo} r_c (z_1^{(4)} r_c^{(\kappa_a - 1)})^{(n_{exp}-1)}}{1 + \frac{(1-X_{cv}-X_{ct}) \frac{\eta h_L R_a}{v_1} \frac{z_1^{(4)}}{x^{(4)}} x^{(1)}}{\left(z_1^{(4)}(t) r_c^{(\kappa a - 1)} + \frac{X_{cv} \frac{\eta h_L R_a}{v_1} \frac{z_1^{(4)}}{x^{(4)}} x^{(1)}}{c_{v,a}} \right) c_{p,a}}} \right)^{1-n_{exp}} \cdot \\
& e^{\frac{(n_{exp}-1) X_{ct} \frac{\eta h_L}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)}}{1 + \frac{X_{cv} \frac{\eta h_L R_a}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)}}{c_{v,a}} + \frac{(1-X_{cv}-X_{ct}) \frac{\eta h_L R_a}{v_1} \frac{r_c^{(1-\kappa_a)}}{x^{(4)}} x^{(1)}}{c_{p,a}}}},
\end{aligned}
\tag{3.9}
$$

$$
\begin{aligned}
\xi_{z3}^{(2)} =& \frac{v_1 i_e x^{(4)}}{2\pi k_e} \left(\frac{r_c^{(\kappa_a - 1)} - 1}{\kappa_a - 1} + \frac{(1 - X_{cv} - X_{ct})}{c_{p,a}} \frac{\eta h_L}{v_1} \frac{R_a}{x^{(4)}} x^{(1)} \right. \\
& - \frac{r_c^{(\kappa_a - 1)} + \frac{\frac{\eta h_L R_a}{v_1 x^{(4)}} x^{(1)} \left(c_{p,a} X_{cv} + c_{v,a}(1 - X_{cv} - Xct) \right)}{c_{v,a} c_{p,a}}}{n_{exp} - 1} \\
& \left. + \frac{X_{ct} \eta h_L R_a x^{(1)}}{x^{(4)} v_1} + \frac{\xi_{z2}^{(2)}}{z_1^{(4)}(n_{exp} - 1)} \right) - Q_{loss}^{nom} \left(1 + Q_{loss}^{grad} \right. \\
& \left. \cdot \frac{n_{fe}^{nom} - n_{fe}}{n_{fe}^{nom}} \right),
\end{aligned}
\tag{3.10}
$$

where $X_{cv} = X_{cv}^{nom} + X_{cv}^{grad} \frac{n_{fe} - n_{fe}^{nom}}{n_{fe}^{nom}}$, $X_{ct} = X_{ct}^{nom} \frac{x^{(1)}}{x_{nom}^{(1)}}$, X_{cv}^{nom} is the nominal constant volume portion, X_{cv}^{grad} is the gradient of the constant volume portion, X_{ct}^{nom} is the nominal constant temperature portion, η is the thermal efficiency incorporating both the combustion and heat release processes, h_L is the lower heating value of fuel at ISO conditions in [J/kg], R_a is the gas constant of air in [J/kgK], v_1 is the cylinder volume at start of compression in $[m^3]$, r_c is the effective compression ratio determined by the inlet valve timing,κ_a is the specific heat ratio of the air, r_{eo} is the ratio of the volume at Seiliger point 6, n_{exp} is the polytropic exponent for expansion, $c_{p,a}$ is the specific heat at constant pressure for the scavenge air in [J/kgK], $c_{v,a}$ is the specific heat at constant volume for the scavenge air in [J/kgK], Q_{loss}^{nom} denotes the nominal mechanical losses of the engine in [Nm], Q_{loss}^{grad} denotes the gradient of mechanical losses of the engine in [Nm] and c is a constant.

The output values of the subsystem's pressure, temperature and torque sensors $y^{(2)} \in \mathbb{R}^3$ are described by:

$$
\mathcal{S}^{(2)} : y^{(2)}(t) = z^{(2)}(t) + d^{(2)}(t) + f^{(2)}(t). \tag{3.11}
$$

Solely for the purposes of Chapter 7, system $\Sigma^{(2)}$ will be alternatively defined as follows. The dynamic operation of the diesel engine is expressed as a first-order differential equation (Haseltalab &Negenborn (2019)):

$$\Sigma^{(2)} : \dot{x}^{(1)}(t) = \gamma^{(2)}\left(x^{(2)}, u^{(2)}\right) + h^{(2)}\left(x^{(2)}, \chi^{(2)}, u^{(2)}\right), \tag{3.12}$$

where

$$\begin{cases} \gamma^{(2)}\left(x^{(2)}, u^{(2)}\right) = k_{ICE} \cdot u^{(2)}(t), \\ h^{(2)}\left(x^{(2)}, \chi^{(2)}, u^{(2)}\right) = -\frac{i_{ICE}}{0.9} \cdot x^{(6)}(t) \cdot x^{(2)}(t), \end{cases} \tag{3.13}$$

,$x^{(2)} \in \mathbb{R}$ denotes the torque of the internal combustion engine [Nm], $\chi^{(2)}(t) = x^{(6)}(t)$ is the propeller speed [rps] and serves as the interconnection state between $\Sigma^{(2)}$ and $\Sigma^{(6)}$, k_{ICE} is the torque constant, i_{ICE} is the gearbox ratio of the diesel engine and $u^{(2)}(t)$ is the control input and expresses the fuel index [kg of fuel]. The engine is equipped with a torque hardware sensor, mathematically expressed as:

$$\mathcal{S}^{(2)} : y^{(2)}(t) = x^{(2)}(t) + d^{(2)}(t) + f^{(2)}(t), \tag{3.14}$$

where $d^{(2)}(t)$, $f^{(2)}(t) \in \mathbb{R}$.

3.2.3 Exhaust Gas Path

This subsystem has 1 state-variable, the exhaust receiver pressure ($x^{(3)}(t)$) in [Pa] and 2 algebraic variables, the temperature before ($z_1^{(3)}(t)$) and after ($z_2^{(3)}(t)$) the turbine in [K]. This subsystem is represented as follows in state-space, based on the physical model equations in (Geertsma et al., 2017c):

$$\Sigma^{(3)} : \begin{cases} \dot{x}^{(3)}(t) = & -\frac{1}{\tau_{p_d}} x^{(3)}(t) + h^{(3)}(x^{(3)}(t), z^{(3)}(t), \chi^{(3)}(t)) \\ 0 = & \xi^{(3)}(x^{(3)}(t), z^{(3)}(t), \chi^{(3)}(t)), \end{cases} \tag{3.15}$$

where $\chi^{(3)} = [x^{(1)}, z^{(2)}, x^{(4)}, z^{(4)}]^\top$ are the interconnection variables. The interconnection dynamics are described by:

$$h^{(3)}(x^{(3)}, z^{(3)}, \chi^{(3)}) = \frac{1}{\tau_{p_d}} \sqrt{p_{ex}^2 + \frac{z_1^{(3)}(n_{fe}^2 \left(\psi_1 \frac{x^{(4)}}{z_1^{(4)}} + \frac{i_e}{k_e} x^{(1)}\right)^2}{a_Z^2 A_{eff}}}, \tag{3.16}$$

where $\psi_1 = \psi_1(x^{(3)}, x^{(4)}, z^{(4)}, n_{fe}) = \frac{\sqrt{R_g} i_e v_1 s_{sl}(x^{(3)}, x^{(4)}, z^{(4)}, n_{fe})}{R_a k_e}$. The algebraic part is expressed as

$$\xi^{(3)}(x^{(3)}, z^{(3)}, \chi^{(3)})) = \begin{bmatrix} z_1^{(3)} - \frac{\psi_2 T_{sl} + \bar{\psi}_3 z_2^{(2)}}{\psi_2 + \psi_3} \\ \\ z_2^{(3)} - \psi_4 z_1^{(3)} \end{bmatrix}, \tag{3.17}$$

where

$$\psi_2 = \frac{c_{pa} v_1 s_{sl}(x^{(3)}, x^{(4)}, z^{(4)}, z^{(2)}) \frac{x^{(4)}}{z_1^{(4)}}}{R_a}, \tag{3.18}$$

$$\psi_3 = c_{pg}\left(x^{(1)} + \frac{v_1}{R_a}\frac{x^{(4)}}{z_1^{(4)}}\right), \tag{3.19}$$

$$\widetilde{\psi_3} = \psi_3(t)\left(\frac{1}{n_{bld}} + \frac{n_{bld}-1}{n_{bld}}\tau_{p_d}\frac{h^{(3)}}{z_1^{(2)}}\right), \tag{3.20}$$

$$\psi_4 = 1 + \eta_{tur}(x^{(4)})(\Pi_{tur} - 1), \tag{3.21}$$

$$\Pi_{tur} = \Pi_{tur}(x^{(3)}) = \left(\frac{p_{ex}}{x^{(3)}}\right)^{(\frac{\kappa_g - 1}{\kappa_g})}, \tag{3.22}$$

$$\eta_{tur}(x^{(4)}) = a_{tur} + b_{tur}x^{(4)} + c_{tur}(x^{(4)})^2, \tag{3.23}$$

τ_{p_d} is the time delay for filling the exhaust receiver in [sec], p_{ex} is the pressure after the turbocharger in [Pa] assumed equal to the atmospheric pressure, a_Z is the Zinner turbine area decrease factor assumed 1 for a constant pressure turbocharger, A_{eff} is the turbine's effective area in $[m^2]$, R_g is the gas constant of the exhaust gas in [J/kgK], n_{bld} is the polytropic expansion coefficient of the blowdown process, c_{pg} is the specific heat at constant pressure for the exhaust gas in [J/kgK], s_{sl} denotes the total slip ratio of the engine expressed in (Geertsma et al., 2017c), T_{sl} is the temperature of the air slip during scavenging in K, $a_{tur}, b_{tur}, c_{tur}$ are the polynomial coefficients of the isentropic turbine efficiency and κ_g is the specific heat ratio of the exhaust gas.

The output values of the subsystem pressure and temperature sensors $y^{(3)}(t) \in \mathbb{R}^3$ are described by:

$$\mathcal{S}^{(3)} : y^{(3)}(t) = \left[x^{(3)}(t)\, z^{(3)}(t)\right]^\top + d^{(3)}(t) + f^{(3)}(t). \tag{3.24}$$

3.2.4 Air Path

This subsystem has 1 state-variable, the charge air pressure after the compressor ($x^{(4)}(t)$) in [Pa] and 2 algebraic variables, the temperatures before ($z_1^{(4)}(t)$) and after ($z_2^{(4)}$) the intercooler in [K]. This subsystem is represented as follows in state-space:

$$\Sigma^{(4)} : \begin{cases} \dot{x}^{(4)}(t) = & -\frac{1}{\tau_{TC}}x^{(4)}(t) + h^{(4)}(x^{(4)}(t), z^{(4)}(t), \chi^{(4)}(t)) \\ 0 = & \xi^{(4)}(x^{(4)}(t), z^{(4)}(t), \chi^{(4)}(t)), \end{cases} \tag{3.25}$$

Figure 3.2: Real-scale turbocharger for marine ICE *applications. The turbocharger is compossed by the compressor and the turbine coupled to the same shaft. As a result, it serves as the interconnection between* $\Sigma^{(3)}$ *and* $\Sigma^{(4)}$ *(Image credits: ABB)*

where $\chi^{(4)} = [x^{(1)}, z^{(2)}, x^{(3)}, z^{(3)}]^\top$ are the interconnection variables. The interconnection dynamics are expressed as:

$$\begin{aligned} h^{(4)}(x^{(4)}, z^{(4)}, \chi^{(4)}) &= \frac{p_{amb}}{\tau_{TC}} \cdot \\ &\left(1 + \chi_g \delta_f \eta_{TC}(x^{(4)}) r_{TC}(z^{(3)})(1 - \Pi_{tur})\right)^{\left(\frac{\kappa_a - 1}{\kappa_a}\right)}, \end{aligned} \tag{3.26}$$

where

$$\delta_f = \delta_f(x^{(4)}, z^{(4)}, \chi^{(4)}) = 1 + \frac{x^{(1)}}{\left(1 + \frac{v_1}{R_a} s_{sl} \frac{x^{(4)}}{z_1^{(4)}}\right)}, \tag{3.27a}$$

$$\eta_{TC}(x^{(4)}) = a_\eta + b_\eta x^{(4)} + c_\eta (x^{(4)})^2, \tag{3.27b}$$

$$r_{TC}(z^{(3)}) = \frac{z_1^{(3)}}{T_{amb}}, \tag{3.27c}$$

$$\chi_g = \frac{c_{pg}}{c_{pa}}. \tag{3.27d}$$

The algebraic part is described by

$$\xi^{(4)}(x^{(4)}, z^{(4)}, \chi^{(4)})) = \begin{bmatrix} z_1^{(4)} - \xi_{z1}^{(4)} \\ z_2^{(4)} - \xi_{z2}^{(4)}(x^{(3)}, z^{(3)}) \end{bmatrix}, \tag{3.28}$$

where

$$\xi_{z1}^{(4)} = T_c - \epsilon_{inl}(T_{inl} - T_c), \tag{3.29a}$$

$$\xi_{z2}^{(4)} = T_{amb} + \chi_g \eta_{tur}(\delta_f(t) + \eta_{com}) x^{(3)} \left(z_2^{(3)} - z_1^{(3)}\right), \tag{3.29b}$$

τ_{TC} is the compressor time delay in [sec], p_{amb} is the ambient pressure in [Pa], T_{amb} is the ambient temperature in [K], a_η, b_η, c_η are the polynomial coefficients of the turbocharger for estimating its efficiency, η_{com} is the mechanical efficiency of the compressor which can be considered constant, T_c is the charge air temperature after the intercooler in [K], ϵ_{inl} is the parasitic effectiveness of the heat exchange between inlet duct and the air and T_{inl} is the temperature of the inlet duct that heats the inducted air in [K].

The output values of the subsystem pressure and temperature sensors $y^{(4)}(t) \in \mathbb{R}^3$ are described by:

$$\mathcal{S}^{(4)} : y^{(4)}(t) = \left[x^{(4)}(t)\, z^{(4)}(t)\right]^\top + d^{(4)}(t) + f^{(4)}(t). \tag{3.30}$$

3.3 Induction motor

The operation of the induction motor can be described as (Wildi (2002)):

$$\Sigma^{(5)} : z^{(5)} = \xi^{(5)}\left(\chi^{(5)}, u^{(5)}\right) = \frac{p}{4\pi i_{gb} x^{(6)}} \frac{\left(u^{(5)}\right)^2}{\left(\frac{R_s}{s}\right)^2 + \left(\frac{i_{gb} x^{(6)}}{2\pi}(H_s + H_r)\right)^2} \frac{R_r}{s}, \tag{3.31}$$

where p denotes the number of poles, $\chi^{(5)} = x^{(3)} \in \mathbb{R}$ is the rotational speed of the propeller shaft in [rps] and serves as the interconnection state between $\Sigma^{(5)}$ and $\Sigma^{(6)}$, $u^{(5)}$ is the control value expressing the input voltage, s is the slip, R_r is the rotor resistance in [Ω], R_s is the stator resistance in [Ω] and H_s, H_r are the stator and rotor reluctance in [H] respectively. The output of the induction motor torque sensor $y^{(5)} \in \mathbb{R}$ is described by:

$$S^{(5)} : y^{(5)} = z^{(5)} + d^{(5)} + f^{(5)}. \tag{3.32}$$

3.4 Gearbox, shaft, and propeller

The shaft dynamics of the gearbox, shaft and propeller, are expressed as (Haseltalab &Negenborn (2019)):

$$\Sigma^{(6)} : \dot{x}^{(6)}(t) = \gamma^{(6)}\left(x^{(6)}(t)\right) + h^{(6)}\left(x^{(6)}(t), \chi^{(6)}(t)\right), \tag{3.33}$$

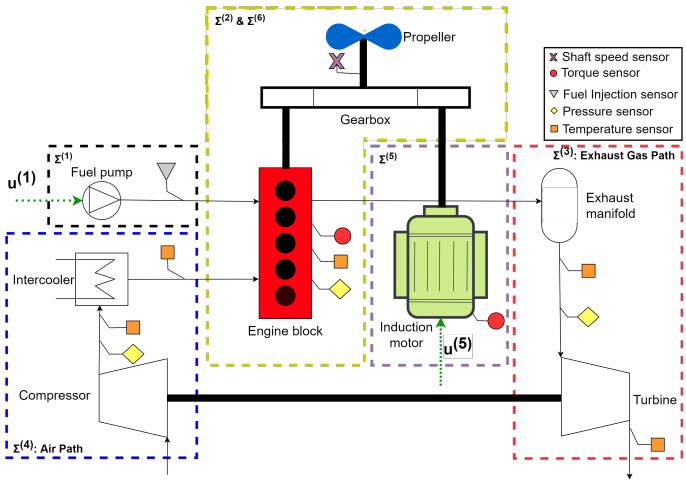


Figure 3.3: 2-D Schematic representation of a typical marine hybrid propulsion plant configuration incorporating systems $\Sigma^{(1)}$-$\Sigma^{(6)}$ (Kougiatsos et al., 2024b).

where

$$\begin{cases} \gamma^{(6)}\left(x^{(6)}(t)\right) = -\frac{C_p}{J_{tot}} \cdot (x^{(6)}(t))^2, \\ h^{(6)}\left(x^{(6)}(t), \chi^{(6)}(t)\right) = \frac{\eta_T}{J_{tot}}\left(i_{gb} \cdot z_3^{(2)}(t) + i_{gb} \cdot z^{(5)}(t)\right), \end{cases} \tag{3.34}$$

$x^{(6)}(t) \in \mathbb{R}$ denotes the propeller shaft rotational speed [rps], $\chi^{(6)}(t) = [z_3^{(2)}(t); z^{(5)}(t)]^\top \in \mathbb{R}^2$ are the interconnection states between $\Sigma^{(6)}$ and $\Sigma^{(2)}, \Sigma^{(5)}$, J_{tot} is the total inertia of the engines, shaft, gearbox and propeller $[kg \cdot m^2]$, induction machine and the diesel engine together and η_T denotes the efficiency of the transmission system. Aside from its differential model description in (3.33), the shaft speed ($x^{(2)}$) can be calculated using the following algebraic equation:

$$x^{(6)} = \frac{1}{i_{gb}}\left(\frac{2\pi}{c}(z_3^{(2)} + z_1^{(5)})\right)^{1/2}. \tag{3.35}$$

A shaft speed sensor is installed in this system and expressed as follows:

$$S^{(6)} : y^{(6)} = x^{(6)} + d^{(6)} + f^{(6)}, \; with \; d^{(6)}(t), f^{(6)}(t) \in \mathbb{R}. \tag{3.36}$$

Solely for the purposes of Chapter 5, system $\Sigma^{(6)}$ will be incorporated in $\Sigma^{(2)}$. As a result, slight notation changes will occur (e.g., $x^{(6)} \rightarrow x^{(2)}$). The sensor set of $\Sigma^{(2)}$ will then be represented as follows:

$$\mathcal{S}^{(2)} : y^{(2)}(t) = \left[x^{(2)}(t)\, z^{(2)}(t)\right]^\top + d^{(2)}(t) + f^{(2)}(t). \tag{3.37}$$

where $d^{(2)}(t)$, $f^{(2)}(t) \in \mathbb{R}^4$.

3.5 Generator sets

Each generator set is modeled as follows (Cheong et al. (2010); Haseltalab &Negenborn (2019)):

$$\Sigma^{(7)}: \begin{cases} \dot{x}^{(7)}(t) = \gamma^{(7)}\left(x^{(7)}(t), z^{(7)}(t), u^{(7)}(t)\right) \\ 0 = \xi^{(7)}\left(x^{(7)}(t), z^{(7)}(t)\right) \end{cases}, \tag{3.38}$$

where

$$\gamma^{(7)}\left(x^{(7)}(t), z^{(7)}(t), u^{(7)}(t)\right) = \begin{bmatrix} -\frac{10}{9} \cdot x_1^{(7)}(t) \cdot x_2^{(7)}(t) + k_{GS} \cdot u^{(7)}(t) \\ \frac{1}{J_{GS}}\left(x_1^{(7)}(t) - z_1^{(7)}(t)\right) \end{bmatrix}, \tag{3.39}$$

$$\xi^{(7)}\left(x^{(7)}(t), z^{(7)}(t)\right) = \begin{bmatrix} \frac{(a_{G,1} \cdot I_X(t) + a_{G,0}) \cdot Re(z_2^{(7)}(t))}{2\pi} - z_1^{(7)}(t) \\ \frac{(a_{G,1} \cdot I_X(t) + a_{G,0}) \cdot x_2^{(7)}(t)}{2\pi(R_{GS,int} + j \cdot L_{GS} \cdot \omega_{GS}(t) + R_{GS}(t)} - z_2^{(7)}(t) \end{bmatrix}, \tag{3.40}$$

$x^{(7)}(t) = [x_1^{(7)}(t); x_2^{(7)}(t)]^\top \in \mathbb{R}^2$, $z^{(7)}(t) = [z_1^{(7)}(t); z_2^{(7)}(t)]^\top \in \mathbb{R}^2$, $x_1^{(7)}$ denotes the torque of the internal combustion engine driving the generator set $[Nm]$, $x_2^{(7)}$ is the rotational speed of the generator's shaft $[rps]$, $z_1^{(7)}$ denotes the torque of the generator part in the generator set$[Nm]$, $z_2^{(7)}$ is the generator output current $[A]$, k_{GS} the torque constant, $m_{f,GS}$ $[kg\ fuel]$ is the fuel index (regulated by a PI controller), I_X $[A]$the excitation current, $a_{G,1}$ and $a_{G,0}$ are constants, $R_{GS,int}$ $[\Omega]$ the internal resistance, L $[H]$ the inductance, j the imaginary number, and J_{GS} $[kg \cdot m^2]$ the generator inertia. In this work, the load resistance R_{GS} $[\Omega]$ is assumed to be purely resistive, and determined with the assigned power P_{GS} $[W]$ (given by the secondary level controller) and the reference-voltage $V_{GS,ref}$ $[V]$ as follows:

$$R_{GS}(t) = \frac{V_{GS,ref}^2(t)}{P_{GS}(t)}. \tag{3.41}$$

The engine is equipped with two torque sensors (one for the engine output and one for the generator input), a shaft speed sensor installed on the generator set shaft and a current sensor measuring the output current. The aforementioned hardware sensors are mathematically expressed as:

$$\mathcal{S}^{(7)}: y^{(7)}(t) = \begin{bmatrix} x^{(7)}(t) \\ z^{(7)}(t) \end{bmatrix} + d^{(7)}(t) + f^{(7)}(t), \text{ with } d^{(7)}(t),\ f^{(7)}(t) \in \mathbb{R}^7. \tag{3.42}$$

3.6 Batteries and constraint modules

Batteries can be mathematically described as follows Kularatna &Gunawardane (2021):

$$\Sigma^{(8)}: \begin{cases} x^{(8)}(t) = \gamma^{(8)}\left(z^{(8)}(t)\right) \\ 0 = \xi^{(8)}\left(x^{(8)}(t), z^{(8)}(t), u^{(8)}(t)\right) \end{cases}, \tag{3.43}$$

where

$$\gamma^{(8)}\left(z^{(8)}(t)\right) = -\frac{z_1^{(8)}}{C_0} \tag{3.44}$$

$$\xi^{(8)}\left(x^{(8)}(t), z^{(8)}(t), u^{(8)}(t)\right) = \begin{bmatrix} z_1^{(8)} - \frac{u^{(8)}}{z_2^{(8)}} \\ \alpha_{B,1}x^{(8)}(t) + \alpha_{B,0} - R_B z_1^{(8)} - z_2^{(8)} \end{bmatrix}, \tag{3.45}$$

$x^{(8)}(t) \in \mathbb{R}$ is the *State of Charge* (*SOC*) of the battery [%], $z^{(8)}(t) = [z_1^{(8)}(t); z_2^{(8)}(t)]^\top \in \mathbb{R}^2$, $z_1^{(8)}(t)$ [A] is the battery current, $z_2^{(8)}(t)$ [V] expresses the battery output voltage, $u^{(8)}(t)$ [W] is the requested power from the battery (determined by the secondary control level), $a_{B,0}$ and $a_{B,1}$ are constants, C_0 [$A \cdot h$] is the capacity of the battery, and R_B [Ω] denotes the resistance of the battery. Each battery comes equipped with a battery constraint module. The main goal of the constraint module is to provide a window $[\underline{u}^{(8)} \ \ \bar{u}^{(8)}]$ for $u^{(8)}$ to the secondary level, such that $x^{(8)}$ and $z^{(8)}$ are kept within their pre-described limits. Based on the work of (Kalikatzarakis et al. (2018)) the following constraints are prescribed:

$$\bar{u}_V^{(8)} = \frac{\left(\alpha_{B,1}x^{(8)}(t) + \alpha_{B,0}\right) \cdot \underline{z}_2^{(8)} - \left(\underline{z}_2^{(8)}\right)^2}{R_B} \tag{3.46}$$

$$\underline{u}_V^{(8)} = \frac{\left(\bar{z}_2^{(8)}\right)^2 - \left(\alpha_{B,1}x^{(8)}(t) + \alpha_{B,0}\right) \cdot \bar{z}_2^{(8)}}{R_B} \tag{3.47}$$

$$\bar{u}_{SOC}^{(8)} = \frac{x^{(8)} - \underline{x}^{(8)}}{\Delta t} \cdot C_0 \cdot \left(\alpha_{B,1}x^{(8)}(t) + \alpha_{B,0}\right) \tag{3.48}$$

$$\underline{u}_V^{(8)} = \frac{x^{(8)} - \bar{x}^{(8)}}{\Delta t} \cdot C_0 \cdot \left(\alpha_{B,1}x^{(8)}(t) + \alpha_{B,0}\right) \tag{3.49}$$

$$\underline{u}^{(8)} = max\left(\underline{u}_V^{(8)}, \underline{u}_{SOC}^{(8)}\right) \tag{3.50}$$

$$\bar{u}^{(8)} = min\left(\bar{u}_V^{(8)}, \bar{u}_{SOC}^{(8)}\right) \tag{3.51}$$

where $\underline{z}_2^{(8)}$, $\bar{z}_2^{(8)}$, $\underline{x}^{(8)}$, and $\bar{x}^{(8)}$ are the minimum and maximum bounds of the terminal voltage $z_1^{(8)}(t)$ and the SOC $x^{(8)}(t)$ of the battery, respectively, and are provided by the battery manufacturer. Δt is a discrete timestep, which can be tuned to alter the power constraints related to the SOC of the battery. The hardware sensors that are used to monitor the operation of the battery are a terminal voltage sensor and

a battery current sensor, while the state of charge is not measured (can only be estimated). Thus, the battery sensors are defined as follows:

$$\mathcal{S}^{(8)} : y^{(8)}(t) = [0\ 1] \cdot \begin{bmatrix} x^{(8)}(t) \\ z^{(8)}(t) \end{bmatrix} + d^{(8)}(t) + f^{(8)}(t), \textit{with } d^{(8)}(t),\ f^{(8)}(t) \in \mathbb{R}^2. \quad (3.52)$$

3.7 Qualitative modelling of marine power and propulsion plants

In literature, many models are available describing the dynamics of the various subsystems encountered in marine power and propulsion systems (Hansen et al. (2013); Geertsma et al. (2017c)). These models are often characterised by high nonlinearity and complexity with their details being more of value in the operational stage (e.g. control, emissions prediction, fault diagnosis) rather than the vessel design phase. For this reason, the basis of the integrated life cycle decision and automation support system presented in Figure 7.3, which enables the use of intelligent functions, is a qualitative modelling technique based on semantics. The semantic database is composed of the following parts; **(a)** the semantic database $\mathcal{F}$ where the semantic information about the system components is stored; **(b)** the knowledge graph G, a tool that helps visualize the connections between the different hardware and cyber components based on their semantic information, and; **(c)** multiple Quality of Service (QoS) criteria that are used for topology and control design assessment purposes.

The semantic database is enriched by semantic information provided either by the designer (e.g., the propeller needs torque from the power and propulsion system to produce thrust for the vessel) or by system manufacturers (e.g., fuel engine operational maps). Using the semantic information of the vessel components (knowledge provided by experts/designers and manufacturers), an automated algorithm is proposed to construct a knowledge graph (G). Finally, the *Quality of Service* (*QoS*) criteria are mostly set by the operators and can include new mission descriptions, power profiles, combinator curves etc. (quantitative data).

3.7.1 Semantic database

In this research work, multi-level control system architectures are considered, such as those often encountered in marine *PPP*s. As can be seen in Figure 3.4. In order to handle design uncertainty regarding both topology and control aspects, we propose a qualitative modelling technique based on semantics. To this end, the physical and cyber *PPP* components are described as follows:

"System": Systems $\Sigma^{(I)}, I = 1, \cdots, N$ each have necessary input and output

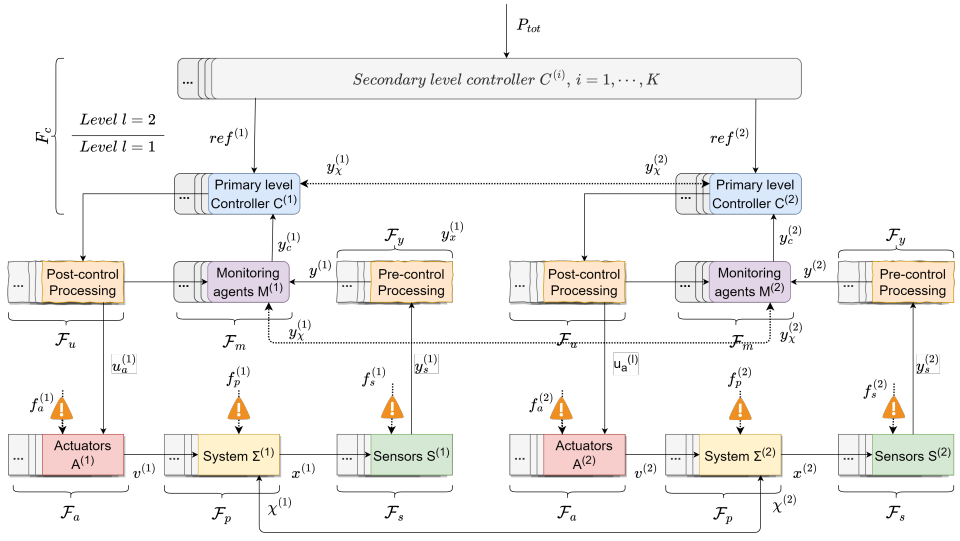


Figure 3.4: Semantic representation of a typical multi-level control system with two "systems" comprising the plant in the semantic database $\mathcal{F}$. The database is composed of two parts, the system topology modules $\mathcal{F}_p$ and the automation modules $\mathcal{F}_A$.

mediums. Therefore, system components are added to the database including input and output information for the specific medium (e.g. water, air, etc.). For instance, the fuel pump(s), electric motors, internal combustion engines, batteries, and propellers found inside marine vessels can be considered as system components.

"Controller": In a multi-level control scheme (such as those frequently encountered in marine vessels), multiple "Controllers" at different levels are needed to coordinate the system operation. A "Controller" at the level l, $l = 1, \cdots, L$ of the control system can be generally expressed as $u(k) = f_c\left(y(k), ref(k), \hat{x}(k), \hat{g}_p(k); \zeta_c, l\right)$ where $u(k)$ is the control decision signal, f_c describes the algorithm for deciding on which action to take next, $y(k)$ represents the plant feedback, $ref(k)$ is the reference trajectory of the system state, $\hat{x}(k)$ is the estimated system state, $\hat{g}_p(k)$ denotes the estimation of possible unknown system dynamics, and ζ_c are parameters used by the controller implementation (e.g. controller gains).

"Monitoring agent": The monitoring agent $\mathcal{M}^{(I)}$ is used to oversee the health of sensors $\mathcal{S}^{(I)}$ belonging to system $\Sigma^{(I)}$, $I = 1, \cdots, n_I$. Due to the complexity associated with marine systems, each "monitoring agent" is typically composed of one or more "monitoring modules" $\mathcal{M}^{(I,q)}$, $q = 1, \cdots, q_I$ (Reppa et al. (2016)). The decision vector resulting from this comparison is then compared to certain binary

sensor fault signature matrices at two levels of isolation, as already described in (Kougiatsos &Reppa (2024a)). The result of the diagnosis is a mapping $R^{(I)} \rightarrow \mathcal{S}_F^{(I)}$ with $R^{(I)}$ denoting the set of residuals and $\mathcal{S}_F^{(I)}$ denoting the faulty sensor set, as a result of the diagnosis process.

"Virtual sensor": Each "virtual sensor" instance leverages the analytical redundancy of the system in order to create virtual and fault-free measurements and is part of a "monitoring agent". It is activated after the detection and isolation of sensor faults by the respective "monitoring module", thus increasing computational effectiveness. A "virtual sensor" is described by the equation $\hat{x}^{(I)}(k) = f_v^{(I)}(\hat{x}^{(I)}[k-1], y^{(I)}[k], u^{(I)}[k], \hat{x}^{(I)}[k]; \zeta_s^{(I)}, \mathcal{S}_F^{(I)})$, where $\zeta_s^{(I)}$ denotes the design parameters of the virtual sensor. In previous work (Kougiatsos et al. (2024b)), two types of "virtual sensors" have been defined for Differential-Algebraic systems and may be used under this module label; differential and algebraic virtual sensors.

The previously described "system" semantic modules are denoted as $\mathcal{F}_p$. We then express the "automation" semantic database, denoted by $\mathcal{F}_A$, as:

$$\mathcal{F}_A = \mathcal{F}_a \cup \mathcal{F}_c \cup \mathcal{F}_s \cup \mathcal{F}_e \cup \mathcal{F}_y \cup \mathcal{F}_u \cup \mathcal{F}_m \cup \mathcal{F}_v, \tag{3.53}$$

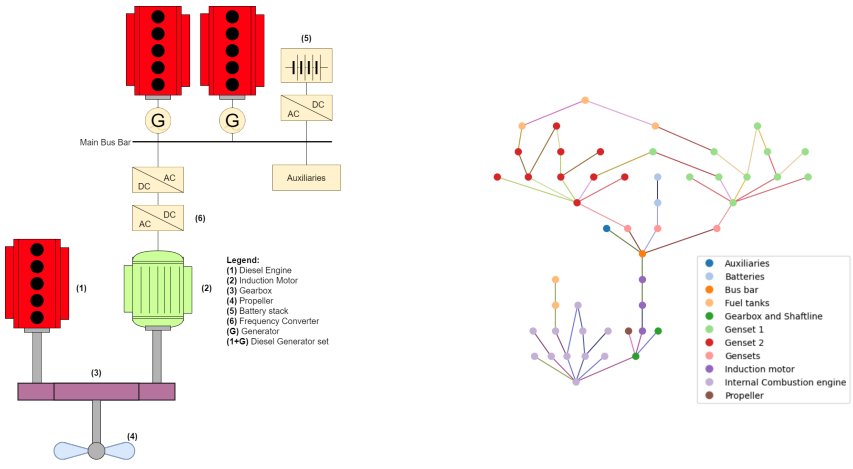
where $\mathcal{F}_a, \mathcal{F}_c, \mathcal{F}_s, \mathcal{F}_e, \mathcal{F}_y, \mathcal{F}_u$ denote the set of "actuators", "controllers", "sensors", "state-estimators", "pre-control functions" and "post-control functions" respectively. The novelty of this thesis regarding the semantic module database resides in a richer description of the "system" and its associated set $\mathcal{F}_p$ and the addition of module sets for "monitoring agents" and "virtual sensors" denoted as $\mathcal{F}_m, \mathcal{F}_v$, respectively.

In the context of one or more candidate topologies i, $i = \{0, \cdots, N_t\}$, multiple "system" databases $\mathcal{F}_{p,i}$ are formed each corresponding to a different candidate topology. Finally, the complete semantic database is defined as:

$$\mathcal{F} = \mathcal{F}_p^{(s)} \cup \mathcal{F}_A, \tag{3.54}$$

where $\mathcal{F}_p^{(s)}$ denotes the selected topology semantic description (e.g. $\mathcal{F}_{p,1}$, $\mathcal{F}_{p,2}$,$\cdots$,$\mathcal{F}_{p,N_t}$).

For instance, the *PPP* topology, such as the one shown in Figure 3.5a, can be semantically described using the above description and expert knowledge on the additional components needed for operation, such as coolers, fuel tanks, etc. An excerpt of this information used to construct the system database $\mathcal{F}_p$ is shown in Table 3.1. Similar representation techniques are also considered from the control design perspective.



(a) *(b)*

Figure 3.5: (a) Typical hybrid PPP *topology used in marine vessel applications. The hybrid characterisation denotes the use of both mechanical (internal combustion engine) and electric (induction motor) power for propulsion and the use of both AC (generators) and DC (batteries) components for power generation; (b) Representation of the hybrid* PPP *shown in (a), using semantic knowledge $\mathcal{F}_p$ such as the one seen in Table 3.1 and the automated knowledge graph algorithm (Algorithm 3.1). The vertices V of the graph (topology components) are coloured based on the subsystem of this component while the edges E between vertices are also shown in multiple colours, each signifying the use of a different medium Υ.*

Table 3.1: Excerpt of Semantic Information for a hybrid PPP *example*

System	Inputs	Outputs
Gearbox	Cool air Motor Power Engine Power	Hot air Propeller Power
Fixed Pitch Propeller	Propeller Power	Thrust
Induction Motor	Converted Motor Voltage (AC)	Motor Power
Bus bar	Generator 1 power Generator 2 power Converted Battery power (AC)	Bus bar voltage

3.7.2 Knowledge Graph

The knowledge graph of the plant is a graph representation of the plant's components (e.g. systems, controllers, sensors) formed using the available semantic knowledge specified by experts, such as designers and manufacturers in the semantic database $\mathcal{F}$. In particular, the connections between the different types of components are based on matching semantic inputs to semantic outputs. This process can take place both in the topology design phase of the plant, where information about the systems is solely prescribed, and in the control design phase where the semantic information of the physical and control components is also relevant. The knowledge graph G serves as a map for identifying the dependencies of each component and for visualising the complexity and modularity of the design layout.

In this research work, we develop an algorithm (see Algorithm 3.1) to generate the knowledge graph G based on the semantic information about the plant, included in the semantic database $\mathcal{F}$. The resulting knowledge graph is expressed as $G\{V, E, \Upsilon\}$ where: **(1)** vertices **(V)** are the entries of the semantic database (e.g., electric motor, internal combustion engine, shaft speed sensor), **(2)** edges **(E)** express the connections between vertices (e.g. the induction motor is connected to the DC/AC converter) and **(3)** mediums **(Υ)** specify the information carried by the connection (e.g. AC voltage is used as the medium between the induction motor and the DC/AC converter). In the topology design phase, the knowledge graph generation algorithm (Algorithm 3.1) begins with a list of "systems" that are considered by the designer for each candidate topology adaptation required to support new missions. The algorithm then starts, for instance, from a propeller (see vertex v_1 in line 3) and connects the system components (vertices v_2) that are necessary for the propeller to be operational in lines 4-11. When multiple systems have the same input or output, graphs are duplicated. The aforementioned lines of the Algorithm 3.1 are run for each different topology consideration, resulting in the knowledge graph for each topology $G_{p,i},\ i = \{0, \cdots, N_t\}$ in line 12.

A decision is made on which topology to use based on the resulting knowledge graphs. Thus, the set $\mathcal{F}_p^{(s)}$ is obtained (line 14). To make the chosen configuration operational, the addition of automation components is required. In the control design phase, the algorithm starts by connecting the automation components (excluding "monitoring agents"), as shown in lines 15-16. Moreover, the information about the grouping of hardware sensors is used to generate the "monitoring agents" (belonging to set $\mathcal{F}_m$) and their connections in lines 17-27. A "monitoring agent" requires the output of relevant hardware sensors and controller(s) to provide decisions on the occurrence of faults. Moreover, its output (fault decision) can be used as input to the controller(s) it is associated with in a fault-tolerant control scheme (Kougiatsos et al., 2022b). Finally, the complete cyber-physical knowledge graph is generated based on the prescribed vertices, edges, and mediums, as shown in line

28.

Algorithm 3.1 Automated function for the generation of Knowledge graphs using semantic information

Input: $\mathcal{F}_{p,0}, \cdots, \mathcal{F}_{p,N_t}, \mathcal{F}_A - \mathcal{F}_m$ ▷ Databases
Output: G ▷ Knowledge Graph

1: **for** $i = 0 : N_t$ **do**
2: $V \leftarrow \mathcal{F}_{p,i}$; $E \leftarrow \emptyset$; $\Upsilon \leftarrow \emptyset$ ▷ **Topology**
3: **for** v_1 in V **do** ▷ Physical plant connections
4: **for** v_2 in V **do**
5: $y \leftarrow v_2.output \cap v_1.input$ ▷ y: medium
6: **if** $y \neq \emptyset$ **then** ▷ Components can be connected
7: $E \leftarrow E \cup \{v_2, v_1\}$
8: $\Upsilon \leftarrow \Upsilon \cup \{y\}$
9: **end if**
10: **end for**
11: **end for**
12: $G_{p,i} \leftarrow \{V, E, \Upsilon\}$ ▷ Physical plant knowledge graph
13: **end for**
14: **Intelligent topology decision support module**: $\mathcal{F}_{p,i} \mapsto \mathcal{F}_p^{(s)}$ by assessing $G_{p,i}$, $i = 1, \cdots, N_t$ ▷ (Kougiatsos et al., 2024a)
15: $V \leftarrow \mathcal{F}_p^{(s)} \cup \{\mathcal{F}_A - \mathcal{F}_m\}$; $E \leftarrow \emptyset$; $\Upsilon \leftarrow \emptyset$ ▷ **Control**
16: **Execute lines 3-11**
17: $s_g \leftarrow \mathcal{F}_s\{sensor\_groups\}$ ▷ Sensor grouping information
18: **for** i=1:length(s_g) **do** ▷ Monitoring agents generation
19: $V \leftarrow V \cup \{M\_i\}$
20: $S \leftarrow \{s \in \mathcal{F}_s \cap s_g[i]\}$ ▷ Connect sensors
21: $C \leftarrow \{c \in \mathcal{F}_c \cap S.edges\}$ ▷ Connect controllers
22: $E \leftarrow E \cup \{\{S, M\_i\},\ \{C, M\_i\}\}$ ▷ Update edges
23: $\Upsilon \leftarrow \Upsilon \cup \{S.output,\ C.output\}$ ▷ Update mediums
24: $E \leftarrow E \cup \{M\_i, C\}$ ▷ Update edges
25: $\Upsilon \leftarrow \Upsilon \cup \{M\_i.output\}$ ▷ Update mediums
26: **end for**
27: $\mathcal{F}_m \leftarrow \{M_1, \cdots, M_{s_g}\}$
28: $G \leftarrow \{V, E, \Upsilon\}$ ▷ Multi-level system and automation knowledge graph (cyber-physical)

3.7.3 Quality of Service (QoS) criteria

The Quality of Service (QoS) criteria are quantitative criteria employed in addition to the qualitative models described in the semantic database $\mathcal{F}$ and the knowledge graph G, in order to enable the use of the intelligent topology and control design framework. On the one hand, from the perspective of system topology, criteria based on graph theory are used to quantify the complexity and modularity measures of the extracted knowledge graphs from a set of candidate topologies. On the other hand, quantified power profiles based on the description of different missions (see Section 7.1) are used on the control side. Moreover, the components belonging to the hardware ($\mathcal{F}_s$) and the virtual ($\mathcal{F}_v$) sensor set are to be used interchangeably by the system when one or more hardware sensors fail during operation. Considering control system performance, switching to the sensor with the minimum reference tracking error is preferable. However, certain types of virtual sensors require a long time for convergence, so choosing a sensor with a higher convergence rate but moderate reference tracking error to avoid danger is also a reasonable option. The time to switch is also taken into consideration as multiple consecutive switches may compromise control stability. The aforementioned criteria have already been explained in detail in Kougiatsos et al. (2022b).

3.8 Conclusions

This chapter introduced the system models used for monitoring and control purposes for the remainder of this thesis. It addresses the second research question, that is (**Q2:**) *"How to derive models of marine power and propulsion plants for monitoring and resilient control purposes?"*

In general, two types of models have been derived:quantitative/differential-algebraic and qualitative/ semantic models. Regarding quantitative models, Section 3.1 presented the general notation followed in a *Differential-Algebraic Equations* (*DAE*) mathematical representation. The *Mean Value First Principle* (*MVFP*) models of the different systems were then adapted to this general mathematical description, as can be seen in Sections 3.2-3.6. The quantitative models will be used in Chapters 4, 5 and 7.

On the other hand, qualitative modelling methods can also prove useful especially when considering design adaptations and the complexity of the considered *PPP* increases. These models, presented in Section 3.7, are composed of a semantic database, storing input/output information for all the system and automation components, an automated knowledge graph tool that is able to generate the system graph for different iterations of the topology and Quality of Service (QoS) criteria in which resilience mechanisms can be built. The qualitative models will be used in Chapters 6 and 7.

Chapter 4

Fault diagnosis of onboard sensors in marine propulsion plants

As presented in Chapter 3, the systems of marine power and propulsion plants are described by *Differential-Algebraic Equations*s (*DAE*s). In this chapter, we propose a methodology for the detection and isolation of multiple, permanent sensor faults for nonlinear *DAE* interconnected subsystems described by (3.1) and (3.2). This answers the third research question (**Q3:**) *"How to design and verify the performance of a sensor fault diagnosis architecture for marine propulsion systems?"*. This Chapter is organised as follows. Sections 4.1-4.3 present the theoretical aspects of the proposed distributed *Sensor Fault Diagnosis* (*SFDI*) methodology, while Section 4.4 is dedicated to the performance analysis of the monitoring scheme. Simulation results using MATLAB are shown in Section 4.5, followed by some concluding remarks in Section 4.6.

The contents of this chapter have been published in the form of one conference (Kougiatsos et al., 2022a)[1] and one journal article (Kougiatsos &Reppa, 2024a)[2].

4.1 Distributed sensor fault diagnosis architecture

In this section, the architecture of the proposed sensor fault diagnosis methodology is described. As can be seen from Figure 4.1, for each subsystem $\Sigma^{(I)}, I = 1, \cdots, N$,

[1] **N. Kougiatsos**, R.R. Negenborn, and V. Reppa,"Distributed model-based sensor fault diagnosis of marine fuel engines," IFAC-PapersOnLine, 55(6), 347-353, 2022.

[2] **N. Kougiatsos**, and V. Reppa, "A Distributed Cyber-Physical Framework for Sensor Fault Diagnosis of Marine Internal Combustion Engines," IEEE Trans. Control Syst. Technol. SI Resilient Control Cyber Phys. Power Energy Syst., pp. 1–12, 2024.

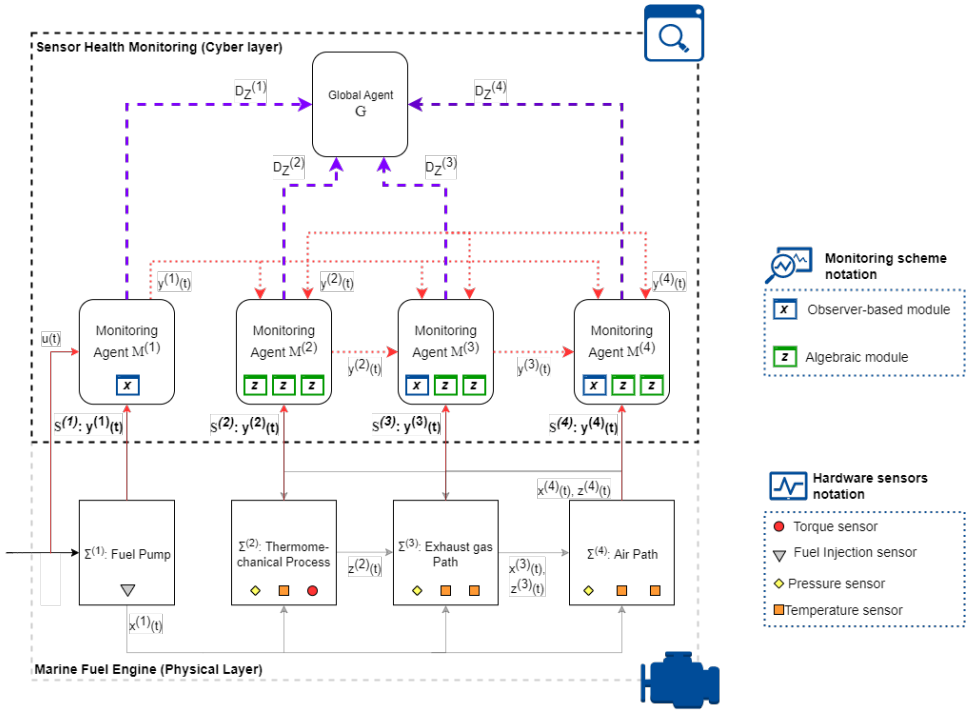


Figure 4.1: Distributed SFDI architecture for marine ICE*s. The distributed aspect is due to the communication between monitoring agents, imitating the interconnections in the physical layer. The interconnection variables between the agents, denoted as $y_{\chi}^{(I,q)}$, are shown with red, dotted lines*

a monitoring agent $\mathcal{M}^{(I)}$ is designed to monitor the health of the sensor set $\mathcal{S}^{(I)}$ belonging to the specific subsystem. Internally, each agent is composed by q_I monitoring modules denoted as $\mathcal{M}^{(I,q)}$, $q = 1, \cdots, q_I$ ($q_1 = 1$, $q_2 = q_3 = q_4 = 3$).The q-th local sensor subset, denoted as $\mathcal{S}^{(I,q)} \subseteq \mathcal{S}^{(I)}$ is assigned to be monitored by the module $\mathcal{M}^{(I,q)}$ and, similar to (Papadopoulos, 2020), is expressed as :

$$\mathcal{S}^{(I,q)} : y^{(I,q)}(t) = C^{(I,q)} \begin{bmatrix} x^{(I)}(t) \\ z^{(I)}(t) \end{bmatrix} + d^{(I,q)}(t) + f^{(I,q)}(t), \tag{4.1}$$

where $y^{(I,q)}$, $d^{(I,q)}$, $f^{(I,q)} \in \mathbb{R}^{m^{(I,q)}}$, $m^{(I,q)} \leq n_I$ denotes the cardinality of the sensor subset $\mathcal{S}^{(I,q)}$. Each monitoring module $\mathcal{M}^{(I,q)}$, $q = 1, \cdots, q_I$ internally compares certain residuals to adaptive thresholds, with the design of both being discussed in Section 4.2. Communication of sensor values, denoted as $y_{\chi}^{(I,q)}$, between the agents is essential in the calculation of the various adaptive thresholds. Thus, a distributed monitoring architecture is implemented. Given the Differential-Algebraic formulation (3.1) of systems considered in this chapter, a mixed Differential-Algebraic

diagnosis scheme is proposed.

The isolation of sensor faults is then realised in two steps. First, a local decision logic is used to indicate the presence of one or more faults, locally affecting the sensors $\mathcal{S}^{(I)}$ monitored by the agents $\mathcal{M}^{(I)}$. A global agent is also implemented to enhance the decision process by providing information on whether sensor faults have been propagated from or to the agent $\mathcal{M}^{(I)}$ from the neighboring agents. The isolation process applies a combinatorial decision logic and diagnostic reasoning between the local and global levels and is described in Section 4.3.

4.2 Distributed sensor fault detection

4.2.1 Residual generation

A residual is most commonly defined as the difference between the expected $\hat{y}^{(I,q)}$ and the measured signal $y^{(I,q)}$ signals for *ODE* systems (Reppa et al., 2016). Considering the *ICE* system description in Section 3.2, it can be inferred that $\hat{y}^{(I,q)} = \hat{x}^{(I,q)}$, since $C^{(I,q)}$ is the unity matrix. The residual vector of the module $\mathcal{M}^{(I,q)}$ is, thus, defined as:

$$\epsilon_y^{(I,q)}(t) = \begin{bmatrix} y_x^{(I,q)}(t) - \hat{x}^{(I,q)}(t) \\ y_z^{(I,q)}(t) \end{bmatrix} = \begin{bmatrix} \epsilon_{y_x}^{(I,q)}(t) \\ \epsilon_{y_z}^{(I,q)}(t) \end{bmatrix} \in \mathbb{R}^{n_I}, \tag{4.2}$$

where $\hat{x}^{(I,q)}$ denotes the estimation of the differential state $x^{(I)}$ involved with the module $\mathcal{M}^{(I,q)}$ and is calculated using a standard nonlinear Luenberger estimator as follows (Papadopoulos, 2020):

$$\begin{aligned} \dot{\hat{x}}^{(I,q)}(t) =& A^{(I)}\hat{x}^{(I,q)}(t) + \gamma^{(I)}(\hat{x}^{(I,q)}(t), y_z^{(I,q)}(t), u^{(I)}(t)) + h^{(I)}(\hat{x}^{(I,q)}(t), y_z^{(I,q)}(t), y_\chi^{(I,q)}(t), u^{(I)}(t)) \\ &+ L^{(I,q)}(y_x^{(I,q)}(t) - \hat{x}^{(I,q)}(t)), \end{aligned} \tag{4.3}$$

where $L^{(I,q)} \in \mathbb{R}^{(n_I - r_I)\times(n_I - r_I)}$ is chosen such that the matrix $A_L^{(I,q)} = A^{(I)} - L^{(I,q)}$ is Hurwitz. Substracting (3.1) from (4.3) and substituting from (3.2) yields (Papadopoulos, 2020):

$$\dot{\epsilon}_x^{(I,q)} = A_L^{(I,q)}\epsilon_x^{(I,q)} + \tilde{\gamma}^{(I,q)} + \tilde{h}^{(I,q)} + \eta_x^{(I)} - L^{(I,q)}d_x^{(I,q)}, \tag{4.4}$$

where $\epsilon_x^{(I,q)} = x^{(I)} - \hat{x}^{(I,q)}$ is the state estimation error, $\tilde{\gamma}^{(I,q)} \triangleq \gamma^{(I)}(x^{(I)}(t), z^{(I)}(t), u^{(I)}(t)) - \gamma^{(I)}(\hat{x}^{(I,q)}(t), y_z^{(I,q)}(t), u^{(I)}(t))$ and $\tilde{h}^{(I,q)} = h^{(I)}(x^{(I)}(t), z^{(I)}(t), \chi^{(I)}(t), u^{(I)}(t)) - h^{(I)}(\hat{x}^{(I,q)}(t), y_z^{(I,q)}(t), y_\chi^{(I)}(t), u^{(I)}(t))$. The residual $\epsilon_{y_x}^{(I,q)}$ can then also be expressed as $\epsilon_{y_x}^{(I,q)} = \epsilon_x^{(I,q)} + d_x^{(I,q)}$.

4.2.2 Computation of adaptive thresholds

The design of adaptive thresholds takes into account the need for them to bound the respective residuals under healthy sensor conditions. Mathematically, the aforementioned design principle can be expressed as:

$$\left|\epsilon_{y_{x_j}}^{(I,q)}(t)\right| \leq \bar{\epsilon}_{y_{x_j}}^{(I,q)}(t),\ j = 1,\cdots,n_I - r_I \tag{4.5}$$

$$\epsilon_{y_{z_j}}^{(I,q)}(t) \in [\underline{\epsilon}_{y_{z_j}}^{(I,q)}(t), \bar{\epsilon}_{y_{z_j}}^{(I,q)}(t)],\ j = 1,\cdots,r_I \tag{4.6}$$

The following assumptions are made:

Assumption 1: The measurement noise of each sensor is unknown but uniformly bounded, meaning: $\left|d_j^{(I)}\right| \leqslant \bar{d}_j^{(I)}, \forall\, j \in 1,\cdots,n_I$ where $\bar{d}_j^{(I)}$ is known.

Assumption 2: The nonlinear vector fields $\gamma^{(I)}, h^{(I)}$ are locally Lipschitz in $x \in \mathcal{X}$, $z \in \mathcal{Z}$ for all $u \in \mathcal{U}$ and $t \geqslant 0$ with Lipschitz constants λ_{γ_I}, λ_{h_I} respectively.

Under the Assumptions 1 and 2 and after some mathematical manipulations of (4.4) the adaptive thresholds for the state-based residuals $\bar{\epsilon}_{y_{x_j}}^{(I,q)}(t)$ shown in (4.5) can be computed as (Reppa et al., 2015):

$$\begin{aligned}\bar{\epsilon}_{y_{x_j}}^{(I,q)}(t) =& E^{(I,q)}(t) + \rho^{(I,q)}\Lambda_I \int_0^t E^{(I,q)}(\tau) e^{-\xi^{(I,q)}(t-\tau)}\, d\tau \\ &+ \bar{d}_{x_j}^{(I,q)},\end{aligned} \tag{4.7a}$$

$$\begin{aligned}E^{(I,q)}(t) =& \rho^{(I,q)} e^{-\xi^{(I,q)}t}\bar{x}^{(I,q)} + \frac{\rho_d^{(I,q)}\bar{d}_x^{(I,q)}}{\xi_d^{(I,q)}}(1 - e^{-\xi_d^{(I,q)}t}) \\ &+ \frac{\rho^{(I,q)}\lambda_{h_I}\bar{d}_\chi^{(I)}}{\xi^{(I,q)}}(1 - e^{-\xi^{(I,q)}t}),\end{aligned} \tag{4.7b}$$

$$\Lambda_I = \lambda_{h_I} + \lambda_{\gamma_I}, \tag{4.7c}$$

where $\rho^{(I,q)}, \xi^{(I,q)}, \rho_d^{(I,q)}, \xi_d^{(I,q)}$ are positive constants such that $\left|e^{A_L^{(I,q)}t}\right| \leqslant \rho^{(I,q)} e^{-\xi^{(I,q)}t}$ and $\left|e^{A_L^{(I,q)}t} L^{(I,q)}\right| \leqslant \rho_d^{(I,q)} e^{-\xi_d^{(I,q)}t}$.

The thresholds corresponding to the algebraic residuals $\underline{\epsilon}_{y_{z_j}}^{(I,q)}, \bar{\epsilon}_{y_{z_j}}^{(I,q)}$ shown in (4.6) are computed using *Set Inversion via Interval Analysis* (*SIVIA*) (Jaulin et al., 2001). This numerical method benefits from the property of monotonic convergence. Hereafter, the notation $[\cdot]$ will be used to denote the interval of potential values of the variable $(\cdot)$. Under Assumption 1 and using (3.1b) with $x \in \mathbb{X}^{(I,q)}$, $z \in \mathbb{Z}^{(I,q)}$, $\chi^{(I,q)} \in \mathcal{X}^{(I,q)}$, $u^{(I)} \in \mathbb{U}^{(I,q)}$, the following algebraic estimator can be constructed:

$$\Xi^{(I,q)} = \xi^{(I,q)}(\mathbb{X}^{(I,q)}, \mathbb{Z}^{(I,q)}, \mathcal{X}^{(I,q)}, \mathbb{U}^{(I)}), \tag{4.8}$$

where $\mathbb{X}^{(I,q)} = y_x^{(I,q)} + [d_x^{(I,q)}] = [y_x^{(I,q)} - \bar{d}_x^{(I,q)}, y_x^{(I,q)} + \bar{d}_x^{(I,q)}]$, $\mathcal{X}^{(I,q)} = y_\chi^{(I,q)} + [d_\chi^{(I,q)}] = [y_\chi^{(I,q)} - \bar{d}_\chi^{(I,q)}, y_\chi^{(I,q)} + \bar{d}_\chi^{(I,q)}]$, $\mathbb{U}^{(I,q)} = [u^{(I)}] = [\underline{u}^{(I)}, \bar{u}^{(I)}]$ are known intervals and $\mathbb{Z}^{(I,q)}$

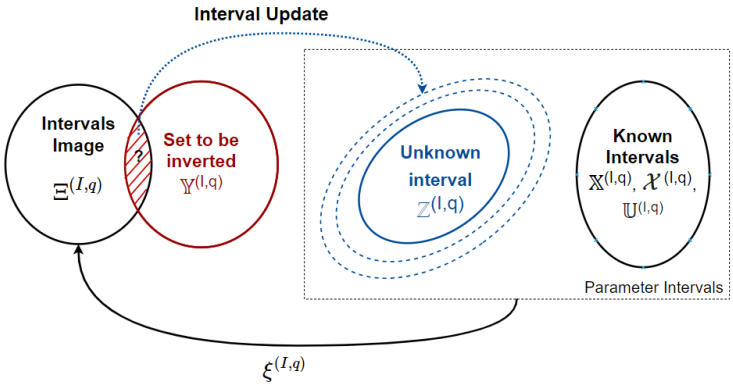


Figure 4.2: Algebraic variables' interval ($\mathbb{Z}^{(I,q)}$) estimation using Set Inversion via Interval Analysis *(*SIVIA*), based on known intervals $\mathbb{X}^{(I,q)}, \mathcal{X}^{(I,q)}, \mathbb{U}^{(I,q)}$ of the state, interconnection and control variables. $\mathbb{Z}^{(I,q)}$ is updated until the obtained image $\Xi^{(I,q)} \subseteq \mathbb{Y}^{(I,q)}$, where $\mathbb{Y}^{(I,q)} = \{0\}$ according to* (3.1b).

is unknown. According to (3.1b), the inversion set (Jaulin et al., 2001) is defined as $\mathbb{Y}^{(I,q)} = \{0\}$. The target of the numerical method is to estimate the unknown interval box $[z^{(I,q)}] = \mathbb{Z}^{(I,q)}$ so that $\Xi^{(I,q)} \subseteq \mathbb{Y}^{(I,q)}$. *SIVIA* is used to dynamically update the unknown interval estimation, starting from an initial estimation $\mathbb{Z}_0^{(I,q)}$, as can be seen in Figure 4.2. The high nonlinearity of the *ICE*'s systems is amended by using forward-backward propagation contractors integrated with *SIVIA* (Jaulin et al., 2001). Then, based on (3.2), (4.2) and some mathematical manipulations, the residual interval under healthy sensor conditions can be calculated as follows:

$$[\epsilon_{y_z}^{(I,q)}] = [z^{(I,q)}] + [d_z^{(I,q)}]. \tag{4.9}$$

Thus, the adaptive thresholds $\underline{\epsilon}_{y_{z_j}}^{(I,q)}, \bar{\epsilon}_{y_{z_j}}^{(I,q)}$ are computed as:

$$\left[\underline{\epsilon}_{y_{z_j}}^{(I,q)}, \bar{\epsilon}_{y_{z_j}}^{(I,q)}\right] = \left[\min[\epsilon_{y_{zj}}^{(I,q)}], \max[\epsilon_{y_{zj}}^{(I,q)}]\right] \tag{4.10}$$

4.2.3 Detection logic

Sensor fault detection in $\mathcal{S}^{(I,q)}$ by the monitoring modules $\mathcal{M}^{(I,q)}$ occurs by comparing the previously defined residuals to the designed adaptive thresholds, based on a set of *Analytical Redundancy Relation*s (*ARR*s). The j-th *ARR* can be defined as:

$$\mathcal{E}_j^{(I,q)} : \left|\epsilon_{y_{x_j}}^{(I,q)}(t)\right| - \bar{\epsilon}_{y_{x_j}}^{(I,q)}(t) \leqslant 0, \; j = 1, \cdots, n_I - r_I \tag{4.11}$$

for the monitoring modules using the residual expression $\epsilon_{y_x}^{(I,q)}$ defined in (4.2) and the threshold expression of (4.7a). Otherwise, the j-th *ARR* is defined as follows:

$$\mathcal{E}_j^{(I,q)} : \epsilon_{y_{z_j}}^{(I,q)}(t) \in [\underline{\epsilon}_{y_{z_j}}^{(I,q)}(t), \bar{\epsilon}_{y_{z_j}}^{(I,q)}(t)],\ j = 1, \cdots, r_I \tag{4.12}$$

The set of *ARR*s based on which the module decides on the presence of local sensor faults is defined as $\mathcal{E}^{(I,q)} = \bigcup_{j \in \mathcal{J}^{(I,q)}} \mathcal{E}_j^{(I,q)}$, where $\mathcal{J}^{(I,q)}$ is an index set, defined as $\mathcal{J}^{(I,q)} = \{j : S^{(I)}\{j\} \in S^{(I,q)}\}$.

The first time instant that (4.11) or (4.12) is invalid for at least one $j \in \mathcal{J}^{(I,q)}$ signifies the time instant of fault detection $T_{D_j}^{(I,q)}$ by the local SFDI module $\mathcal{M}^{(I,q)}$, defined as $T_{D_j}^{(I,q)} = \min\{t : \left|\epsilon_{y_{x_j}}^{(I,q)}(t)\right| - \bar{\epsilon}_{y_{x_j}}^{(I,q)}(t) > 0\}$ or $T_{D_j}^{(I,q)} = \min\{t : \epsilon_{y_{z_j}}^{(I,q)}(t) \notin [\underline{\epsilon}_{y_{z_j}}^{(I,q)}(t), \bar{\epsilon}_{y_{z_j}}^{(I,q)}(t)]\}$ accordingly. Until this instant, the local sensing subsystem $\mathcal{S}^{(I,q)}$ is considered non-faulty meaning that either no fault exists or that faults exist but remain undetected.

The output of $\mathcal{M}^{(I,q)}$ is denoted by $D^{(I,q)}$ and in the case of permanent sensor faults, it can be defined as:

$$D^{(I,q)}(t) = \begin{cases} 0 & , t < T_D^{(I,q)} \\ 1 & , t \geqslant T_D^{(I,q)} \end{cases} \tag{4.13}$$

with $T_D^{(I,q)} = \min\{T_{D_j}^{(I,q)} : j \in \mathcal{J}^{(I,q)}\}$.

4.3 Distributed sensor fault isolation

4.3.1 Local decision logic

From the detection logic step, a binary decision vector $D^{(I)} = [D^{(I,1)}, \cdots, D^{(I,q_I)}]$ can be obtained for the monitoring agent $\mathcal{M}^{(I)}$ and compared to the columns of a binary *Fault Signature Matrix* (*FSM*) $F^{(I)}$, consisting of N_I rows and $N_{C_I} + 2$ columns where $N_{C_I} = 2^{n_I} - 1$. The design of this matrix will be described in the simulation results section for the easiness of the analysis. While $D^{(I)}(t) = 0_{N_I}$, the diagnosis set $\mathcal{D}_s^{(I)}$ is empty. In addition, if $D^{(I,q)} = F_{qi}^{(I)}\ \forall q \in 1, \cdots, N_I$, then the observed pattern $D^{(I)}(t)$ is said to be consistent with the theoretical pattern $F_i^{(I)}$ and the diagnosis set is defined as $\mathcal{D}_s^{(I)}(t) = \{\mathcal{F}_{ci}^{(I)} : i \in \mathcal{I}_{\mathcal{D}}^{(I)}(t)\}$ where $\mathcal{I}_{\mathcal{D}}^{(I)}(t)$ is the consistency index set defined as $\mathcal{I}_{\mathcal{D}}^{(I)}(t) = \{i : F_i^{(I)} = D^{(I)}(t), i \in \{1, \cdots, N_{C_I}\}\}$.

4.3.2 Global decision logic

Together with the local diagnosis set $\mathcal{D}_s^{(I)}$, the agent $\mathcal{M}^{(I)}, I \in \{1, \cdots, N\}$ also provides a decision on the propagation of sensor faults from the interconnected subsystems,

denoted as $D_{\chi}^{(I)}(t)$ with

$$D_{\chi}^{(I)}(t) = \begin{cases} 0 & \text{, if } f_{\chi}^{(I)} \notin \mathcal{D}_s^{(I)}(t) \text{ and } f_p^{(I)} \notin \mathcal{D}_s^{(I)}(t) \\ 1 & \text{, otherwise} \end{cases} \tag{4.14}$$

where $f_p^{(I)} \in \mathbb{R}^{n_I^*}, n_I^* \leqslant n_I$, collectively amounts for the sensor faults that are propagated from the agent $\mathcal{M}^{(I)}$ to its neighbouring agents due to the exchange of sensor information and $f_{\chi}^{(I)}$ corresponds to the sensor faults propagated to the agent from the neighbouring agents. The global decision logic serves to isolate sensor faults propagated through the interconnections between the monitoring agents. As shown in Fig.4.1, a global agent $\mathcal{G}$ collects the decisions on the propagation of sensor faults from the N local agents $D_{\chi}(t) = [D_{\chi}^{(1)}(t), \cdots, D_{\chi}^{(N)}(t)]$ and compares them with the columns of a global binary sensor fault signature matrix F^{χ} consisting of N rows and $N_C = 2^p - 1$ columns ($p \leqslant \sum_{I=1}^{N}\{p_I\}$, p_I is the length of $f_{\chi}^{(I)}$). A (*) is used in F^{χ} instead of 1 in case the sensor fault is propagated to the agent $\mathcal{M}^{(I)}$ from the other agents $\mathcal{M}^{(J)}$, $J \in \{1, \cdots, N\}$, $J \neq I$ to indicate that a set of *ARR*s is less sensitive to this fault. The attenuated sensitivity may be due to the propagation effects of sensor faults or the algebraic nature of *ARR*s.If $\mathcal{D}_{\chi}(t)$ is consistent with the k-th column of F^{χ} (F_k^{χ}), meaning that $D_{\chi}(t) = F_k^{\chi}$, the diagnosis set of propagated sensor faults (propagation through communicated measuring signals) is defined as $\mathcal{D}_s^{\chi}(t) = \{\mathcal{F}_{ck}^{\chi} : k \in \mathcal{I}_{\chi}(t)\}$, where $\mathcal{I}_{\chi}(t)$ is an index set defined as $\mathcal{I}_{\chi}(t) = \{k : F_{Ik}^{\chi} = D_{\chi}^{(I)}(t), k \in \{1, \cdots, N_C\}, \forall I \in \{1, \cdots, N\}\}$.

The isolation of sensor faults in $\mathcal{S}^{(I,q)}$ requires the combination of the local and global decision logic levels. More precisely, the output $\mathcal{D}_s^{\chi}(t)$ of the global agent is used to update the diagnosis sets $\mathcal{D}_s^{(I)}(t)$ of the local monitoring agents $\mathcal{M}^{(I)}$. The occurrence of $f_{\chi}^{(I)}$ and its combinations can be excluded from the local diagnosis sets, if $f_{\chi}^{(I)} \notin \mathcal{D}_s^{\chi}(t)$. Moreover, the intersection of the updated sets is considered the diagnosis results. The formal mathematical expression of the resulting global diagnosis set is the following:

$$\mathcal{D}_s^{\mathcal{G}}(t) = \mathcal{D}_s^{\chi} \bigcap_{\substack{I=1 \\ \mathcal{D}_s^{(I)} \neq \emptyset}}^{N} \mathcal{D}_s^{(I)} \tag{4.15}$$

The isolated faulty sensors set is then denoted as $\mathcal{S}^{\mathcal{F}} = \{\mathcal{S}^{(I)}\{j\}, I = 1, \cdots, N\, j = 1, \cdots, n_I | f_j^{(I)} \in \mathcal{D}_s^{\mathcal{G}}\}$ and is a superset of the actual faulty sensors set $\mathcal{S}_0^{\mathcal{F}}$.

4.4 Fault resilience quantification metrics

The performance analysis of the proposed distributed monitoring scheme in this chapter concerns the detectability and ability to isolate sensor faults. This section

provides the definitions of the Key Performance Indicators (KPIs) based on which the fault resilience of the proposed monitoring scheme is assessed.

4.4.1 Distributed sensor fault detectability

Having designed the adaptive thresholds according to (4.7a),(4.10), the occurence of false alarms is excluded. Thus, the KPIs of interest for sensor fault detectability include:

Minimum Detectable sensor fault magnitude

The minimum detectable sensor fault magnitude for each of the local monitoring modules $\mathcal{M}^{(I,q)}$ can be expressed as:

$$MDF_j^{(I)} = \min \quad \{\hat{\phi}_j^{(I)}\} \text{ s.t.} \qquad \neg\mathcal{E}^{(I,q)} \tag{4.16}$$

Missed detection rate

In comparison to existing literature (Ding, 2013), (Papadopoulos, 2020), the missed detection rate metric is assessed both locally (local monitoring modules) as well as globally (interconnected monitoring modules). According to (Ding, 2013), the missed detection rate (MDR) for each of the local monitoring modules $\mathcal{M}^{(I,q)}$, $I = 1,\cdots,N_I$, $q = 1,\cdots,q_I$ is expressed as:

$$MDR^{(I,q)} = prob(D^{(I,q)} = 0 | f_j^{(I)} \neq 0,\ j \in \mathcal{J}^{(I,q)}) \tag{4.17}$$

Following a similar rationale, the MDR concerning the propagation of sensor faults will be defined as follows:

$$\begin{aligned} MDR = prob(D^{(K)} = \emptyset | \quad & f_j^{(I)} \neq 0,\ j \in \mathcal{J}^{(I)},\ I \in [1,N], \\ & \forall K \neq I,\ K \in [1,N]) \end{aligned} \tag{4.18}$$

Detection delay

The detection delay for each of monitoring modules $\mathcal{M}^{(I,q)}$ is expressed as:

$$DL^{(I,q)} = T_D^{(I,q)} - T_{f_j}^{(I)} \tag{4.19}$$

Thus, taking into consideration the aforementioned KPIs, good monitoring performance regarding distributed architectures would be associated with low values for all $MDF^{(I,q)}$, $MDR^{(I,q)}$, MDR and $DL^{(I,q)}$.

4.4.2 Ability to isolate sensor faults

Considering the existing literature on fault diagnosis, no clear metrics on the ability to isolate sensor faults have been proposed so far. In this chapter, we define the uncertainty $U_{\mathcal{G}}$ and the exoneration efficiency $E_{\mathcal{G}}$ of the global diagnosis set as follows:

$$U_{\mathcal{G}}(t) = |\mathcal{S}^{\mathcal{F}}|(t) - |\mathcal{S}_0^{\mathcal{F}}|(t), \tag{4.20}$$

$$E_{\mathcal{G}}(t) = |\cup_{I=1}^{N} \mathcal{S}^{(I)}| - |\mathcal{S}^{\mathcal{F}}|(t), \tag{4.21}$$

where $|\cdot|$ denotes the cardinality of the set $(\cdot)$. The isolation ($P^{U_{\mathcal{G}}}$) and exoneration ($P^{E_{\mathcal{G}}}$) performance of the sensor fault isolation process can be then quantified as follows:

$$P^{U_{\mathcal{G}}} = \frac{100}{T - T_{D0}} \int_{T_{D0}}^{T} \Big(1 - \frac{U_{\mathcal{G}}(t)}{|S^{\mathcal{F}}|(t)}\Big) dt, \tag{4.22}$$

$$P^{E_{\mathcal{G}}} = \frac{100}{T - T_{D0}} \int_{T_{D0}}^{T} \Big(\frac{E_{\mathcal{G}}(t)}{|\cup_{I=1}^{N} S^{(I)}|}\Big) dt, \tag{4.23}$$

where T is the running time of the system and $T_{D0} = \min\{T_D^{(I,q)} : I = 1, \cdots, N,\ q = 1, \cdots, q_I\}$ is the time the first sensor fault gets detected.

4.5 Simulation results

In this section, the Distributed sensor fault diagnosis architecture described in Sections 4.1-4.3 is applied on the marine *ICE* model, described in Chapter 3. The data needed for the model and the controller are extracted from (Geertsma et al., 2017c) while the noise bound of each sensor is assumed to be equal to 5 % of the amplitude of the sensor value.

The sensor subsets are defined as follows (sensor descriptions in Chapter 3): $\mathcal{S}^{(1,1)} = \{\mathcal{S}^{(1)}\{1\}\}$, $\mathcal{S}^{(2,1)} = \{\mathcal{S}^{(2)}\{1\}\}$, $\mathcal{S}^{(2,2)} = \{\mathcal{S}^{(2)}\{2\}\}$, $\mathcal{S}^{(2,3)} = \{\mathcal{S}^{(2)}\{2\}, \mathcal{S}^{(2)}\{3\}\}$, $\mathcal{S}^{(3,1)} = \{\mathcal{S}^{(3)}\{1\}, \mathcal{S}^{(3)}\{2\}\}$, $\mathcal{S}^{(3,2)} = \{\mathcal{S}^{(3)}\{1\}, \mathcal{S}^{(3)}\{2\}\}$, $\mathcal{S}^{(3,3)} = \{\mathcal{S}^{(3)}\{1\}, \mathcal{S}^{(3)}\{2\}, \mathcal{S}^{(3)}\{3\}\}$, $\mathcal{S}^{(4,1)} = \{\mathcal{S}^{(4)}\{1\}, \mathcal{S}^{(4)}\{2\}\}$, $\mathcal{S}^{(4,2)} = \{\mathcal{S}^{(4)}\{2\}\}$, $\mathcal{S}^{(4,3)} = \{\mathcal{S}^{(4)}\{2\}, \mathcal{S}^{(4)}\{3\}\}$. Each module $\mathcal{M}^{(I,q)}$ is then used to monitor the sensors in $S^{(I,q)}$. The modules $\mathcal{M}^{(1,1)}$, $\mathcal{M}^{(3,1)}$ and $\mathcal{M}^{(4,1)}$ use an *ARR* expression as given in (4.11) while all the other modules use an *ARR* expression as given in (4.12).

The engine is operated at constant and nominal load, corresponding to the maximum continuous rating (MCR) point of the engine. The residual generation (Section 4.2.1) and the computation of adaptive thresholds (Section 4.2.2) processes within each monitoring module are then set up with the following design parameters: $L^{(1,1)} = 1.16$, $\rho^{(1,1)} = 1$, $\xi^{(1,1)} = 25$, $\rho_d^{(1,1)} = 2$, $\xi_d^{(1,1)} = 20$, $L^{(3,1)} = 900$, $\rho^{(3,1)} = 0.05$, $\xi^{(3,1)} = 600$, $\rho_d^{(3,1)} = 900$, $\xi_d^{(3,1)} = 1000$, $L^{(4,1)} = 499.98$, $\rho^{(4,1)} = 0.03$, $\xi^{(4,1)} = 500$,

Table 4.1: Part of the Sensor Fault signature matrix of $\mathcal{M}^{(2)}$ (single faults)

	$f_1^{(2)}$	$f_2^{(2)}$	$f_3^{(2)}$	$f_1^{(1)}$	$f_1^{(4)}$	$f_2^{(4)}$
$\mathcal{E}^{(2,1)}$	*	0	0	*	*	0
$\mathcal{E}^{(2,2)}$	0	*	0	*	*	*
$\mathcal{E}^{(2,3)}$	0	*	*	*	*	*

Table 4.2: Part of the Sensor Fault signature matrix of $\mathcal{M}^{(3)}$ (single faults)

	$f_1^{(3)}$	$f_2^{(3)}$	$f_3^{(3)}$	$f_1^{(1)}$	$f_1^{(2)}$	$f_2^{(2)}$	$f_3^{(2)}$	$f_1^{(4)}$	$f_2^{(4)}$
$\mathcal{E}^{(3,1)}$	1	*	0	*	0	0	*	*	*
$\mathcal{E}^{(3,2)}$	*	*	0	*	*	*	*	*	*
$\mathcal{E}^{(3,3)}$	*	*	*	0	0	0	0	0	0

$\rho_d^{(4,1)} = 320$ and $\xi_d^{(4,1)} = 450$. The initial estimations $\mathbb{Z}_0^{(I,q)}$ for the algebraic modules are deduced based on logic and physical laws. For the simulation scenario, three permanent, abrupt and offset sensor faults are assumed to affect the sensors $\mathcal{S}^{(2)}\{3\}$, $\mathcal{S}^{(3)}\{1\}$, and $\mathcal{S}^{(4)}\{2\}$, described by (3.3), and with their magnitudes chosen as $\widehat{\phi}_3^{(2)} = -3.8 \cdot 10^4 Nm$, $\widehat{\phi}_1^{(3)} = 5 \cdot 10^4 Pa$ and $\widehat{\phi}_2^{(4)} = 8K$. The sensor faults are initiated at the time instances $T_{f3}^{(2)} = 20\ sec$, $T_{f1}^{(3)} = 45\ sec$ and $T_{f2}^{(4)} = 70\ sec$ respectively.

The simulation results for the specified scenario are shown in Figure 4.3. Each row of graphs $I \in \{1,2,3,4\}$ represents the internal structure of each of the local monitoring agents $\mathcal{M}^{(I)}$, composed by one or more monitoring modules $M^{(I,q)}$. Each subplot then portrays the residuals (blue line), adaptive thresholds (green/magenta lines) and decision function (red line) used by the respective module.

Tables 4.1, 4.2, 4.3, 4.4 represent the local and global sensor fault signature matrices. In Table 4.1 the three first columns provide the theoretically expected local sensor fault patterns while the rest of the columns are showing the propagated sensor fault patterns. For brevity purposes, only the single sensor fault columns are shown while this chapter deals with multiple sensor faults. In order to obtain the multiple fault columns, logical conjuction between the respective single fault columns needs to be applied. As for the rows of this matrix, each of them corresponds to a local module $\mathcal{M}^{(2,q)}$ making use of the set of *ARR*s $\mathcal{E}^{(2,q)}$, $q = \{1,2,3\}$. A similar approach is also followed for the creation of the Tables 4.2, 4.3. The reason of having two modules $\mathcal{M}^{(3,1)}, \mathcal{M}^{(3,2)}$ monitoring the same set of sensors ($\mathcal{S}^{(3,1)} = \mathcal{S}^{(3,2)}$) is to improve the ability to isolate sensor faults. For instance, a local decision vector $D^{(3)} = [D^{(3,1)}\ D^{(3,2)}\ D^{(3,3)}]^\top = [0\ 1\ 0]^\top$ would exclude the occurrence of sensor faults $f_1^{(3)}, f_2^{(3)}$. In the case that there were 2 modules e.g. $\mathcal{M}^{(3,1)}$ and $\mathcal{M}^{(3,3)}$ then an observed pattern $D^{(3)} = [D^{(3,1)}\ D^{(3,3)}]^\top = [1\ 0]^\top$ would include $f_1^{(3)}$ in the diagnosis set.

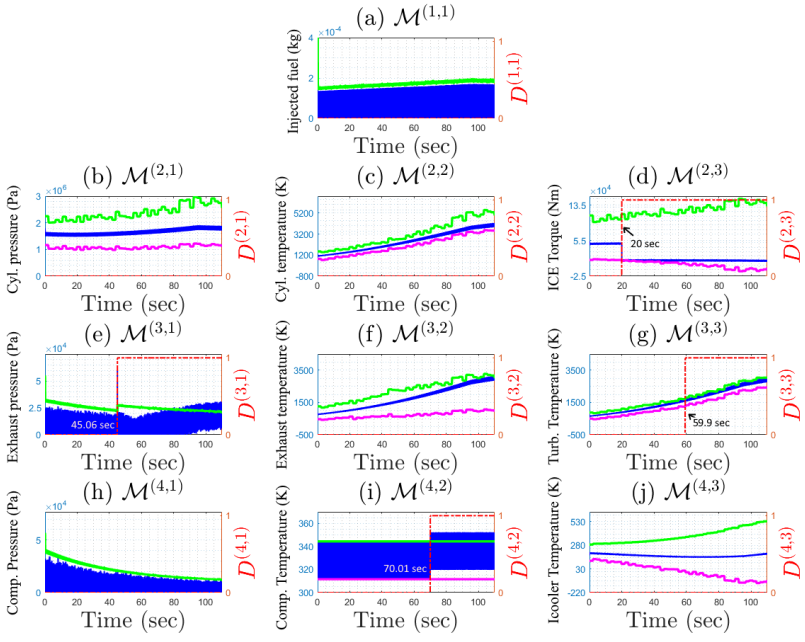


Figure 4.3: Simulation results of the Distributed SFDI methodology for the specified fault scenario (red/ dash-dotted line: decision logic, blue/ continuous line: residual, green and magenta/ continuous lines: adaptive thresholds). The respective detection times in [sec] are also indicated on the subfigures.

Table 4.3: Part of the Sensor Fault signature matrix of $\mathcal{M}^{(4)}$ (single faults)

	$f_1^{(4)}$	$f_2^{(4)}$	$f_3^{(4)}$	$f_1^{(1)}$	$f_3^{(2)}$	$f_1^{(3)}$	$f_2^{(3)}$
$\mathcal{E}^{(4,1)}$	1	*	0	*	*	*	*
$\mathcal{E}^{(4,2)}$	0	*	0	0	0	0	0
$\mathcal{E}^{(4,3)}$	*	*	*	*	*	*	*

Table 4.4: Part of the Global sensor fault signature matrix (single faults)

	$f_1^{(1)}$	$f_1^{(2)}$	$f_2^{(2)}$	$f_3^{(2)}$	$f_1^{(3)}$	$f_2^{(3)}$	$f_3^{(3)}$	$f_1^{(4)}$	$f_2^{(4)}$	$f_3^{(4)}$
$\mathcal{E}^{(1)}$	1	0	0	0	0	0	0	0	0	0
$\mathcal{E}^{(2)}$	*	1	1	1	0	0	0	*	*	0
$\mathcal{E}^{(3)}$	*	*	*	*	1	1	1	*	*	0
$\mathcal{E}^{(4)}$	*	0	0	*	*	*	0	1	1	1

From the simulation results shown in Figure 4.3, the diagnosis process proceeds as follows. For $t < 20$ *sec*, the diagnosis set is empty ($\mathcal{D} = \{\}$), as all detection decisions are zero. For $20 \leqslant t < 45.06$ *sec*, the second monitoring agent $\mathcal{M}^{(2)}$ outputs the decision vector $D^{(2)}(t) = [0\ 0\ 1]^\top$ as can be seen in Figures 4.3(b)-(d). Since, $D^{(1)}(t) = 0$, $D^{(3)}(t) = D^{(4)}(t) = [0\ 0\ 0]^\top$ the sensor faults $f_1^{(1)}$, $f_1^{(3)}$, $f_1^{(4)}$ are excluded from the diagnosis sets. Comparing $D^{(2)}$ with Table 4.1, the resulting local diagnosis set is $\mathcal{D}_s^{(2)}(t) = \left\{f_2^{(2)}, f_3^{(2)}, f_2^{(4)}, \{f_2^{(2)}, f_2^{(4)}\}, \{f_3^{(2)}, f_4^{(2)}\}\right\}$. The global decision vector for this time interval is $D_\chi(t) = [0\ 1\ 0\ 0]^\top$ and when compared to Table 4.4, results in the diagnosis set on fault propagation $\mathcal{D}_s^\chi(t) = \left\{f_1^{(2)}, f_2^{(2)}, f_3^{(2)}\right\}$. As a result, the global diagnosis set is $\mathcal{D}_s^\mathcal{G}(t) = \mathcal{D}_s^\chi \cap \mathcal{D}_s^{(2)} = \left\{f_2^{(2)}, f_3^{(2)}\right\}$.

Then, for $45.06 \leqslant t < 59.9$ *sec* the decision vector for the monitoring agent $\mathcal{M}^{(2)}$ remains the same, thus resulting in the same local diagnosis set $\mathcal{D}_s^{(2)}(t)$. The rest of the local agent decision vectors are $D^{(1)} = 0$, $D^{(4)} = [0\ 0\ 0]^\top$, therefore excluding the sensor faults $f_1^{(1)}$, $f_1^{(4)}$ from the diagnosis sets. However, the decision vector for agent $\mathcal{M}^{(3)}$ is now equal to $D^{(3)} = [1\ 0\ 0]^\top$, also seen in Figure 4.3(e)-(g) and comparing that to Table 4.2, the resulting local diagnosis set is $\mathcal{D}_s^{(3)} = \left\{f_1^{(3)}, f_2^{(3)}, f_3^{(2)}, f_2^{(4)}, \{f_1^{(3)}, f_1^{(2)}\}, \{f_1^{(3)}, f_2^{(2)}\}, \{f_1^{(3)}, f_3^{(2)}\}, \cdots\right\}$. The decision vector on the propagation of sensor faults is now $D_\chi(t) = [0\ 1\ 1\ 0]^\top$ and comparing with Table 4.4, we obtain the diagnosis set on fault propagation $\mathcal{D}_s^\chi(t) = \left\{f_1^{(2)}, f_2^{(2)}, f_3^{(2)}, \{f_1^{(2)}, f_1^{(3)}\}, \{f_1^{(2)}, f_2^{(3)}\}, \cdots\right\}$. The global diagnosis set is $\mathcal{D}_s^G(t) = \mathcal{D}_s^\chi \cap \mathcal{D}_s^{(2)} \cap \mathcal{D}_s^{(3)} = \left\{f_3^{(2)}, \{f_1^{(3)}, f_2^{(2)}\}, \{f_1^{(3)}, f_3^{(2)}\}, \{f_2^{(3)}, f_2^{(2)}\}, \{f_2^{(3)}, f_3^{(2)}\}\right\}$. For $59.9 \leqslant t < 70.01$ *sec*, only the decision vector of agent $\mathcal{M}^{(3)}$ changes to $D^{(3)} = [1\ 0\ 1]^\top$ as can be seen in Figure 4.3(e)-(g). Following the same approach, the resulting global diagnosis set changes to $\mathcal{D}_s^G(t) = \left\{\{f_1^{(3)}, f_2^{(2)}\}, \{f_1^{(3)}, f_3^{(2)}\}, \{f_2^{(3)}, f_2^{(2)}\}, \{f_2^{(3)}, f_3^{(2)}\}\right\}$.

Finally, for $t \geq 70.01$ *sec*, the local decision vector of agent $\mathcal{M}^{(4)}$ is $D^{(4)} = [0\ 1\ 0]^\top$ and when compared to Table 4.3, results in the local diagnosis set $\mathcal{D}_s^{(4)} = f_2^{(4)} \cup \left\{\{\}, f_3^{(4)}, f_3^{(2)}, f_1^{(3)}, f_2^{(3)}, \{f_3^{(4)}, f_3^{(2)}\}, \{f_3^{(4)}, f_1^{(3)}\}, \cdots\right\}$. Comparing the decision vector on fault propagation $D_\chi(t) = [0\ 1\ 1\ 1]^\top$, outputs the diagnosis set on fault propagation $\mathcal{D}_s^\chi(t) = \left\{f_3^{(2)}, f_1^{(4)}, f_2^{(4)}, \{f_3^{(2)}, f_1^{(3)}\}, \{f_3^{(2)}, f_2^{(3)}\}, \{f_3^{(2)}, f_1^{(4)}\}, \{f_3^{(2)}, f_2^{(4)}\}, \{f_3^{(2)}, f_1^{(2)}\}, \cdots\right\}$.
The global diagnosis set is then given by the expression $\mathcal{D}_s^G(t) = \mathcal{D}_s^\chi \cap \mathcal{D}_s^{(2)} \cap \mathcal{D}_s^{(3)} \cap \mathcal{D}_s^{(4)} = f_2^{(4)} \cup \left\{f_1^{(3)}, f_2^{(3)}, f_3^{(3)}, \{f_1^{(3)}, f_2^{(2)}\}, \{f_1^{(3)}, f_3^{(2)}\}, \{f_2^{(3)}, f_2^{(2)}\}, \{f_2^{(3)}, f_3^{(2)}\}, \{f_3^{(3)}, f_2^{(2)}\}, \{f_3^{(3)}, f_3^{(2)}\}\right\}$.
Based on the above analysis, the proposed methodology managed to isolate sensor faults in $S^{(4)}\{2\}$ and combinations of the sensors $S^{(2)}\{2\}$, $S^{(2)}\{3\}$, $S^{(3)}\{1\}$, $S^{(3)}\{2\}$, $S^{(3)}\{3\}$. It is also useful to note that the the resulting diagnosis set managed to include the sensors with simulated faults in our scenario.

In order to investigate the effectiveness of the proposed distributed SFDI scheme, the KPIs mentioned in Section 4.4 were calculated. Uniform noise bands

Table 4.5: Minimum detectable sensor fault magnitudes by respective local monitoring modules (noise bound 5%)

$MDF_j^{(I)}$	$j=1$	$j=2$	$j=3$
$I=1$	5.06%	-	-
$I=2$	20.36%	14.06%	63.68%
$I=3$	5%	50.8%	11.37%
$I=4$	4.88%	0.03 %	68.97%

for all sensors were chosen to provide a common point of reference for the analysis. Regarding the minimum detectable sensor fault magnitudes, defined in (4.16), the respective results for a noise bound of 5% are given in Table 4.5. The algebraic modules $\mathcal{M}^{(2,1)}$, $\mathcal{M}^{(2,2)}$, $\mathcal{M}^{(2,3)}$, $\mathcal{M}^{(3,2)}$, $\mathcal{M}^{(3,3)}$, $\mathcal{M}^{(4,2)}$ and $\mathcal{M}^{(4,3)}$ exhibit an $MDF_j^{(I)}$ value according to the complexity of the model equations and the number of interconnection variables $\chi^{(I)} \in \mathbb{R}^{k_I}$. For instance, the system dynamics of (3.7), (3.10) or (3.29b), used by the modules $\mathcal{M}^{(2,3)}$, $\mathcal{M}^{(4,3)}$ respectively, are more complex and include more interconnections than the dynamics of (3.29a) used by the module $\mathcal{M}^{(4,2)}$. As a result, the $MDF_j^{(I)}$ indicator has a substantially higher value for those modules. Regarding the rest of the modules that use observer based *ARR*s, the $MDF_j^{(I)}$ is comparable to the noise level as can be seen in Table 4.5. The results regarding the missed detection rates and detection delays are given for two fault cases affecting the following sensors, namely (a) the fuel mass sensor $f_1^{(1)} \neq 0$ and (b) the engine torque sensor $f_3^{(2)} \neq 0$. This particular choice of sensors was made taking into consideration the criticality of these two sensors for control of marine *ICE*s. Extensive simulation was used to obtain the data points for ten levels of sensor noise affecting all system sensors $(1-10\%)$ (Papadopoulos, 2020). At each noise level, the simulation is run for 100 times, with varying seed. The simulations were carried out using TU Delft's Blue Supercomputer (Delft High Performance Computing Centre , DHPC). The simulated faults in each of the two different scenarios occur at the time instant $T_{f_1}^{(1)} = T_{f_3}^{(2)} = 20sec$ and are again considered permanent, abrupt and offset. As for the magnitudes of the sensor faults, in scenario (a) we consider a fault magnitude of $\hat{\phi}_1^{(1)} = 7\% x_{nom}^{(1)}$ while in scenario (b) a sensor fault magnitude $\hat{\phi}_3^{(2)} = 65\% z_{3,nom}^{(2)}$. Moreover, as both $MDR^{(I,q)}$ and MDR are defined as probabilities in expressions (4.17), (4.18), aside from the mean values found by simulation for these indicators, the respective confidence intervals for the mean value are also depicted in Figure 4.4 using a shaded area representation (95% confidence level). As illustrated in Fig. 4.4(a),(b), both MDR and $MDR^{(I,q)}$ are increasing or remain constant as the variance of the sensor noise is increasing as well. Moreover, $MDR^{(I,q)} \leq MDR$, which indicates the persistency of the local module design to detect the sensor fault. In addition, Figure 4.4(b) suggests that between a noise

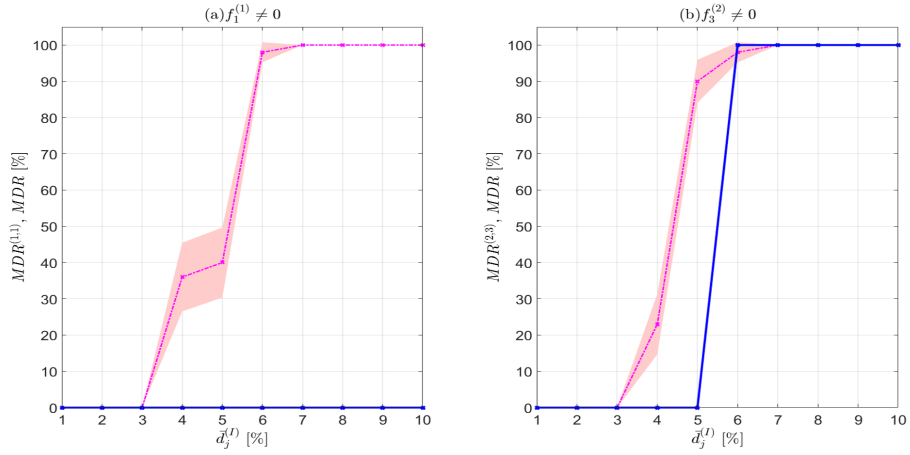


Figure 4.4: Missed detection rates with respect to increasing sensor noise levels $\bar{d}_j^{(I)}$ for all sensors. Results for two single sensor fault scenarios are shown (blue/continuous line: $MDR^{(I,q)}$, magenta/ dash-dotted line: MDR). Each point on the curves corresponds to the times that the corresponding diagnosis agent failed to detect the presence of the sensor fault out of the 100 simulations obtained for each sensor noise variance $d_j^{(I)}(t)$. The confidence intervals are also shown as a shade (95% confidence level)

Table 4.6: Detection delays $DL^{(I,q)}$ for two cases of sensor faults and ascending sensor noise level (min-max and [mean] values are provided, - is used to denote undefined values due to $MDR^{(I,q)}$ or MDR being greater than zero)

Noise level	**2%**	**4%**	**6%**	**8%**	**10%**
	(a) $f_1^{(1)} \neq 0$				
$DL^{(1,1)}$ **[mean value]**	0-0.01 sec **[0 sec]**				
$\min(DL^{(I,q)}), (I,q) \neq (1,1)$ **[mean value]**	0-32.81 sec **[10.52 sec]**	>59.04 sec **[-]**	>89.36 sec **[-]**	-	
	(b) $f_3^{(2)} \neq 0$				
$DL^{(2,3)}$ **[mean value]**	0-0.01 sec **[0 sec]**		-		
$\min(DL^{(I,q)}), (I,q) \neq (2,3)$ **[mean value]**	0.15-59.67 sec **[14.83 sec]**	>59.11 sec **[-]**	>74.48 sec **[-]**	-	

level of 6-7%, although the local module misses the fault ($MDR^{(2,3)}$=100%), the interconnected agents manage to still detect the fault effects through propagation. This strength of the distributed architecture is particularly useful for the diagnosis process. As for the detection delay, the values of the indicator $DL^{(I,q)}$, defined in (4.19), are given for the same fault scenarios in Table 4.6 both for the local monitoring modules and the interconnected modules. The local module detection delays are relatively small, indicating a solid design of the residual and adaptive thresholds.

Again, as the noise level increases so does the detection delay as can be seen in both scenarios.

Regarding sensor fault isolation, the initial scenario with three sensor faults described at the beginning of this Section was used. Using TU Delft's Blue supercomputer, the simulation was run for 100 times with a noise level of 5% affecting all system sensors and a varying seed. Based on the acquired results, implementing the metrics defined in (4.22), (4.23) yields $P^{U_{\mathcal{G}}} = (51.16 \pm 0.81)\%$ and $P^{E_{\mathcal{G}}} = (57.83 \pm 2.93)\%$ (95% confidence level) suggesting a fair isolation performance for the three consecutive faults scenario.

4.6 Conclusions

In this chapter, we illustrated a Distributed Cyber-physical framework for isolating sensor faults in marine *ICE*s. The goal of the proposed methodology was the isolation of sensor faults affecting multiple sensors of the engine using the information exchanged between its different subsystems. We thus replied to the following research question (**Q3:**) *"How to design and verify the performance of a sensor fault diagnosis architecture for marine propulsion systems?"*

The core of the diagnosis approach consisted of two cyber layers; one based on a bank of local monitoring agents monitoring specific sensor sets and a global decision logic layer which decided on the propagation of faults between the different subsystem. Each monitoring agent was composed of one or more monitoring modules. Fault detection was carried out by the different modules using differential or algebraic residuals and comparing them to designed adaptive bounds. Sensor faults were isolated by comparing the decisions of the various monitoring agents to combinations of sensor faults and by applying diagnostic reasoning.

The resilient control strategies that are able to handle the occurrence of one or multiple sensor faults, after their diagnosis, are explored in Chapters 5 and 7. Moreover, Chapter 6 addresses the optimisation of sensor fault isolability, in an effort to improve the relevant fault resilience quantification metrics from a design point of view.

Chapter 5

Sensor fault-resilient multi-agent control for marine hybrid propulsion plants

Through the use of the *SFDI* methodology described in Chapter 4, multiple sensor faults can be diagnosed and safety is improved. However, the decisions for recovery purposes after the diagnosis, related to the available redundancy and resilience mechanisms, are not yet discussed.

The objective of this chapter is to design a fault-resilient control architecture that is able to compensate for the multiple sensor fault effects in the marine hybrid propulsion plant (see Figure 3.3). In doing so, the following research question is addressed (**Q4:**) *"How to switch between hardware and virtual sensors during operation for enhanced fault resilience in marine propulsion plants?"*. The chapter is structured as follows. In Section 5.1 the Cyber-Physical control scheme for marine hybrid propulsion plants is discussed. Section 5.2 provides the details for a model-based control design in the primary control level considering feedback linearization controllers. The design of the virtual sensors and the multi-sensory switching logic to guarantee fault resilience are discussed in Sections 5.3 and 5.4. Simulation results showcasing the applicability and efficiency of the method are shown in Section 5.5, followed by some concluding remarks in Section 5.6.

The contents of this chapter have been published in two conference (Kougiatsos &Reppa, 2022; Kougiatsos et al., 2022b) [1] [2] and one journal (Kougiatsos et al.,

[1] **N. Kougiatsos** and V. Reppa, "A distributed virtual sensor scheme for marine fuel engines," IFAC-PapersOnLine, vol. 55, no. 31, pp. 333–338, 2022

[2] **N. Kougiatsos**, R. R. Negenborn, and V. Reppa. "A Multi-Sensory Switching-stable Architecture for Distributed Fault Tolerant Propulsion Control of Marine Vessels." Proceedings of the 2022 International Ship Control Systems Symposium, Delft, the Netherlands. Vol. 16. 2022.

2024b)[3] publications.

5.1 Sensor fault-resilient multi-agent control architecture

The overall scheme proposed in the context of this chapter to promote resilience against sensor faults is depicted in Figure 5.1 and is composed by two control levels, the physical system and sensor level and the monitoring level. The secondary control level is responsible for splitting the power requirements dictated by the power profile P_D $[W]$ to the shaft speed and torque reference signals n_{ref} $[rps]$ and Q_{ref} $[N \cdot m]$, respectively, communicated to the primary level controllers. As this control level is not the main focus of this chapter, for simplicity, a rule-based power split strategy (Sciberras &Norman, 2012) is enforced.

For propulsion loads less or equal than the maximum rated power of the *Induction Motor* (*IM*), only the *IM* will be used. For loads that exceed however the rating of the *IM*, the internal combustion engine's used is prioritized instead and the *IM* is only used to support excess power loads. Mathematically, the previously described rule-based design is expressed as follows:

$$n_{ref}(t) = \left(\frac{P_D(t)}{c \cdot \eta_T} \right)^{\frac{1}{3}}, \tag{5.1}$$

$$Q_{ref}(t) = \begin{cases} \frac{P_D(t)}{2\pi n_{ref}(t)\eta_T} & , P_D \leq \bar{P}_m \\ \max\left\{0, \frac{P_D(t)-\bar{P}_i}{2\pi n_{ref}(t)\eta_T}\right\} & , P_D > \bar{P}_m \end{cases}, \tag{5.2}$$

where $\bar{P}_m$ $[W]$ corresponds to the maximum rated power of the *IM* and $\bar{P}_i$ $[W]$ denotes the maximum rated power of the internal combustion engine.

In the primary control level, a parallel control strategy is employed (Geertsma et al., 2017b) using two control agents operating in a distributed configuration, as shown in Figure 5.1. In contrast to the majority of marine literature where model-free PI controllers are used (e.g., Geertsma et al. (2017b)), in this chapter model-based controllers are designed for the parallel control of the internal combustion engine and the *IM*. The specifics of the nonlinear model-based design of the primary level control agents are discussed in Section 5.2.

As shown in Figure 5.1, the monitoring level includes the monitoring agents $\mathcal{M}^{(1)}, \cdots, \mathcal{M}^{(5)}$, the virtual sensors and the switching logic. For each subsystem $\Sigma^{(I)}, I = 1, \cdots, N$, a monitoring agent $\mathcal{M}^{(I)}$ is designed to monitor the health of the hardware sensor set $\mathcal{S}^{(I)}$. Each monitoring agent is composed by one or more monitoring modules, denoted as $\mathcal{M}^{(I,q)}$, with $q \in \{1, \cdots, q_I\}$ ($q_1 = 1$, $q_2 = 4$, $q_3 = 3$, $q_4 = 3$,

[3] **N. Kougiatsos**, M. Vagia, R.R. Negenborn, and V. Reppa, "Sensor fault-resilient multi-agent control for marine hybrid propulsion plants," submitted to a journal, 15 pp.,2024

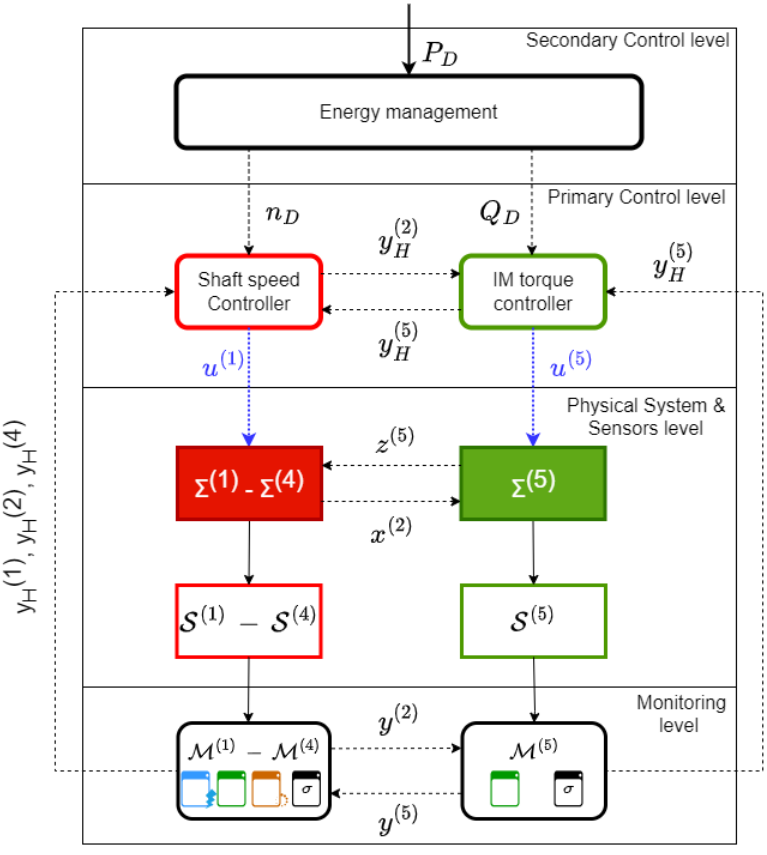


Figure 5.1: Multi-level and fault-resilient control scheme for marine hybrid propulsion plants. The physical, cyber and control connections are shown with continuous, dashed and blue/ dotted lines respectively.

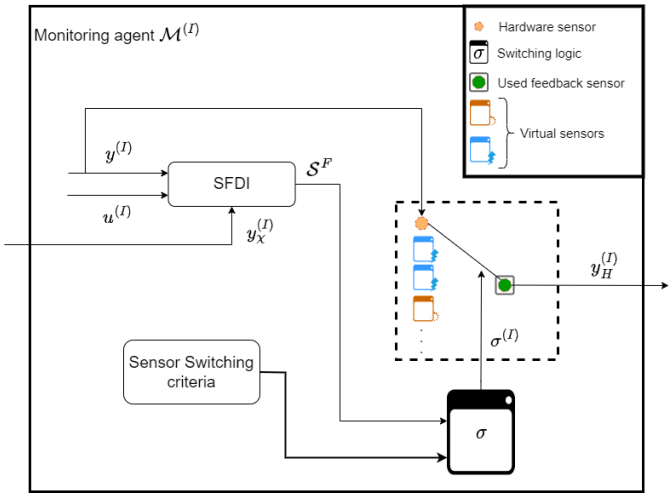


Figure 5.2: Internal structure of sensor monitoring agents. The sensor fault diagnosis (SFDI) block (Chapter 4) is responsible for indicating the sensors belonging to the faulty sensor set $\mathcal{S}^F$.

$q_5 = 1$). The monitoring agents can communicate with each other in a distributed configuration, sharing sensor information with one another. As can be seen from Figure 5.2, the sensor fault diagnosis block, already described in Chapter 4, determines the healthy $\mathcal{S}^H = \{s \in \mathcal{S}^{(I)} : s \notin \mathcal{D}_s^{\mathcal{G}}\}$, where $\mathcal{D}_s^{\mathcal{G}}$ is the resulting sensor fault diagnosis set, and faulty $\mathcal{S}^{\mathcal{F}} = \mathcal{S}^{(I)}/\mathcal{S}^H$ sensor sets by using model information, control values, local and interconnected hardware sensor measurements to form and compare residuals and adaptive thresholds. The virtual sensors are then implemented as part of the monitoring agents $\mathcal{M}^{(I)}$ as shown in Figure 5.2, with their design specifics discussed in Section 5.3.

The multi-sensory switching logic, denoted as σ in Figure 5.2, is designed to switch between hardware and virtual feedback sensors, when the former are affected by faults . The switching logic is a cyber tool, implemented as part of the monitoring agents alongside the sensor fault diagnosis (SFDI) block and the virtual sensors, as can be seen in Figure 5.2. The switching logic is able to make online decisions $\sigma^{(I)}$ on the sensor index to be used from a library of both hardware and virtual sensors using information on the faulty sensor set $\mathcal{S}^F$ and certain switching criteria. More specifically, both system and control stability criteria are formulated and used to switch between hardware and virtual sensors when one or multiple faults are diagnosed in the hardware feedback sensors. The result of this level are the selected feedback sensor signals $y_{1,s}^{(2)}$ and $y_{1,s}^{(5)}$, with further details of the employed criteria provided in Section 5.4.

The objective of this chapter is to design a fault-resilient control architecture that is able to compensate for the multiple sensor fault effects in the marine hybrid propulsion plant (see Figure 3.3). The proposed architecture is designed with three main goals; **(i)** to guarantee the stability of the control scheme, **(ii)** to maintain the optimal reference tracking error performance, and, **(iii)** to ensure the operation of the internal combustion engine within safety critical ranges.

5.2 Distributed model-based nonlinear control

In this Section,the nonlinear model-based design of the shaft speed control agent and the *IM* control agent in the primary control level is presented. Based on their successful application in similar problems (Haseltalab &Negenborn, 2019), feedback linearization techniques (Khalil, 2002) are used for the model-based design of the controllers in this level. The use of a model-based scheme also allows for the analytical computation of the closed-loop reference tracking error, which will enable event-based and stable switching of sensors in the distributed control scheme.

5.2.1 Shaft speed control agent

The main goal of the shaft speed control agent is to track a shaft speed reference signal $n_{ref}(t)$ by altering the fuel injection setting $u^{(1)}$, described in Chapter 3. As a result the main equations of interest are (3.4) and (3.33) as they contain the control value $u^{(1)}(t)$ and the shaft speed state $x^{(2)}(t)$ respectively. Furthermore, (3.33) requires the engine's torque state information $z_3^{(2)}(t)$ given by the same system using Eq. (3.10). The above equations can be summarised in the following form:

$$\dot{x} = f(x) + g(x)u^{(1)}(t), \tag{5.3}$$

where $x = [x^{(1)}, x^{(2)}]^\top$, $g(x) = \left[\frac{x_{nom}^{(1)}}{\tau_X}; 0\right]^\top$, $f(x) = \left[-\frac{1}{\tau_X}x^{(1)}; f_1(x^{(2)}) + g_1(x^{(1)}, x^{(2)}, z^{(2)})\right]^\top$, $f_1(x^{(2)}) = -\frac{c}{2\pi J_{tot}} \cdot (x^{(2)})^2$ and $g_1(x^{(1)}, x^{(2)}, z^{(2)}) = \begin{bmatrix} \frac{i_{gb}\eta_T}{2\pi J_{tot}} \frac{i_{gb}\eta_T}{2\pi J_{tot}} \end{bmatrix} \cdot \begin{bmatrix} z_3^{(2)} \\ z^{(5)} \end{bmatrix}$ and the rest of parameters defined in Chapter 3.

Based on (Khalil, 2002), the system (5.3) is feedback linearizable if and only if there is a domain $D_0 \subset D$ such that

(1) The matrix $G = [g(x), ad_f g(x)]$ has full rank for all $x \in D_0$ and

(2) the distribution $\mathcal{H} = span\{g(x)\}$ is involutive in D_0.

where $ad_f g(x)$ denotes the Lie bracket of function $g(x)$ with respect to function $f(x)$. Considering the representations of $f(x)$, $g(x)$ in (5.3):

$$ad_f g = \frac{\partial g(x)}{\partial x} f(x) - \frac{\partial f(x)}{\partial x} g(x) = \begin{bmatrix} -c_2 \frac{\partial g_1}{\partial x_2} \\ -c_1 c_2 \end{bmatrix}, \tag{5.4}$$

meaning that the matrix

$$G = [g(x), ad_f g(x)] = \begin{bmatrix} \frac{x_{nom}^{(1)}}{\tau_X} & -\frac{x_{nom}^{(1)}}{\tau_X} \frac{\partial g_1}{\partial x^{(1)}} \\ 0 & \frac{x_{nom}^{(1)}}{\tau_X^2} \end{bmatrix} \tag{5.5}$$

has full rank in the domain $D_0 = \{x = [x^{(1)}, x^{(2)}]^\top,\ x^{(1)} \in \mathbb{R}, x^{(2)} \in \mathbb{R} : \frac{\partial g_1}{\partial x^{(1)}} \neq 0\}$ and the distribution $\mathcal{H} = span\{g\}$ is involutive in D_0 since $g(x)$ represents a constant vector field.

In order to bring (5.3) to a feedback linearizable form, a change of variables $h(x)$ is required, satisfying the following conditions (Khalil, 2002):

$$\frac{\partial h}{\partial x} g(x) = 0, \tag{5.6a}$$

$$\frac{\partial L_f h}{\partial x} g(x) \neq 0, \tag{5.6b}$$

$$h(0) = 0, \tag{5.6c}$$

with $L_f g(x)$ denoting the Lie derivative. From the condition (5.6a), it is deduced that $h(x)$ must be independent from $x^{(1)}$, so $h(x) = h(x^{(2)})$. In addition,

$$L_f h(x) = \frac{\partial h}{\partial x^{(2)}} \left(f_1(x^{(2)}) + g_1(x^{(1)}, x^{(2)}, z^{(2)}) \right) \tag{5.7}$$

which means that condition (5.6b) is expressed as:

$$\frac{\partial L_f h}{\partial x} g(x) = c_2 \frac{\partial h}{\partial x^{(2)}} \frac{\partial g_1}{\partial x^{(1)}} \neq 0, \tag{5.8}$$

that is satisfied in the domain D_0 for any choice of h such that $\frac{\partial h}{\partial x^{(2)}} \neq 0$.

Based on the above conditions, a suitable transformation to make the system feedback linearizable is:

$$\begin{cases} \tilde{x}_1 = h(x) = x^{(2)} \\ \tilde{x}_2 = L_f h(x) = f_1(x^{(2)}) + g_1(x^{(1)}, x^{(2)}, z^{(2)}), \end{cases} \tag{5.9}$$

which, after differentiation, yields:

$$\begin{cases} \dot{\tilde{x}}_1 = \tilde{x}_2 \\ \dot{\tilde{x}}_2 = f_l(\tilde{x}) + g_l(\tilde{x}) u^{(1)}, \end{cases} \tag{5.10}$$

where $f_l(\tilde{x}) = \frac{df_1(x^{(2)})}{dt} + (g_1(x^{(1)}, x^{(2)}, z^{(2)}) + \frac{dg_1(x^{(1)}, x^{(2)})}{dt})x^{(1)}$ and $g_l(\tilde{x}) = \frac{x^{(1)}_{nom}}{\tau_X} \cdot g_1(x^{(1)}, x^{(2)})$.

In order to stabilize (5.10) and achieve the control objective of tracking the rotational speed signal n_{ref} the control law is designed as follows:

$$u^{(1)}(t) = \frac{1}{g_l(\tilde{x})}\left(-f_l(\tilde{x}) - k_1(\tilde{x}_1 - n_D) - k_2\tilde{x}_2\right), \tag{5.11}$$

where k_1, k_2 denoting the controller gains with $k_1, k_2 > 0$.

Substituting (5.11) in (5.10) and defining the state reference tracking error as $\epsilon^{(2)}_{\tilde{x}}(t) \triangleq \left[\tilde{x}_1(t) - n_{ref}(t);\ \tilde{x}_2(t)\right]^\top$ implies:

$$\dot{\epsilon}^{(2)}_{\tilde{x}}(t) = \begin{bmatrix} 0 & 1 \\ -k_1 & -k_2 \end{bmatrix} \cdot \epsilon^{(2)}_{\tilde{x}}(t), \tag{5.12}$$

meaning that the closed-loop reference tracking error dynamics of $\Sigma^{(2)}$ have been rendered linear under the nonlinear model-based design of $u^{(1)}$ in (5.11).

5.2.2 *IM* torque control agent

We design the *IM* torque control agent to track a *IM* torque reference signal $Q_{ref}(t)$ by altering the voltage input $u^{(5)}(t)$ of the *IM*. Taking into consideration the algebraic model of the *IM* torque in (3.31), the control law can be prescribed as follows;

$$u^{(5)}(t) = \sqrt{\left(\frac{R_s}{s}\right)^2 + \left(\frac{i_{gb}x^{(2)}}{2\pi}(H_s + H_r)\right)^2} \cdot \sqrt{\frac{4\pi s i_{gb}x^{(2)}}{pR_r}} \cdot \sqrt{z^{(5)}\exp(-k_3 t) + Q_{ref}(1 - \exp(-k_3 t))}, \tag{5.13}$$

where $k_3 > 0$ denotes the controller gain and the rest of parameters defined in Chapter 3. Substituting (5.13) in (3.31), defining the reference tracking error as $\epsilon^{(5)}_z \triangleq= z^{(5)}(t) - Q_{ref}(t)$ and considering that $\lim_{t\to\infty}\exp(-k_3 t) = 1$ yields:

$$\epsilon^{(5)}_z(t) = 0, \tag{5.14}$$

signifying that under the nonlinear model-based design of $u^{(5)}$ in (5.13), perfect tracking of the motor torque reference signal by the torque algebraic state $z^{(5)}$ is achieved.

During the propulsion plant operation, however, sensor information will be used as feedback instead of the actual states. This information can originate by either hardware or virtual (software-based sensors). The design of virtual sensors is presented in Section 5.3 while the sensor measurement reference tracking errors are formulated in Section 5.4.

5.3 Virtual sensor design

When the faults affecting the sensors of the system $\Sigma^{(I)}$ have been diagnosed, the analytical redundancy of the system can be employed in the form of virtual sensors to generate the required fault-free measurements. The virtual sensor instances are implemented as part of the monitoring agents in the cyber-layer and their design is accustomed to the Differential-Algebraic nature of the systems considered in this chapter. More specifically, two types of virtual sensors are designed; **(1)** differential virtual sensors for the parts of each system mathematically described by differential equations, and **(2)** algebraic virtual sensors for the parts of each system mathematically described by algebraic equations.

5.3.1 Differential virtual sensors

Nonlinear adaptive estimators are used for the dynamic virtual sensor design, as follows:

$$\begin{cases} \dot{\hat{x}}^{(I,q)} = A^{(I)}\hat{x}^{(I,q)} + \gamma^{(I)}(\hat{x}^{(I,q)}, y_{zH}^{(I)}, u^{(I)}) + \\ \qquad h^{(I)}(\hat{x}^{(I,q)}, y_{zH}^{(I)}, y_{\chi H}^{(I,q)}, u^{(I)}) + \\ \qquad L^{(I,q)}(y_x^{(I,q)} - \hat{y}_x^{(I,q)}) + \\ \qquad \Omega^{(I,q)}\dot{\hat{f}}_x^{(I,q)} & (5.15a) \\ \dot{\Omega}^{(I,q)} = A_L^{(I,q)}\Omega^{(I,q)} - L^{(I,q)} & (5.15b) \\ \hat{y}_x^{(I,q)} = \hat{x}^{(I,q)} + \hat{f}_x^{(I,q)} & (5.15c) \\ \dot{\hat{f}}_x^{(I,q)} = \Gamma^{(I,q)}(\Omega^{(I,q)} + 1)\mathcal{D}[\epsilon_{y_x}^{(I,q)}], & (5.15d) \end{cases}$$

where $\Gamma^{(I,q)}$ is the learning rate of the adaptive law in (5.15d) and $\Omega^{(I,q)}$ is a filtering term to ensure the stability of the state-equation adaptive scheme. Finally, $\mathcal{D}[\cdot]$ is the dead-zone operator, used to activate the sensor fault identification, given as:

$$\mathcal{D}[\epsilon_{y_x}^{(I,q)}] = \begin{cases} 0, & if\ D^{(I,q)}(t) = 0 \\ \epsilon_{y_x}^{(I,q)}, & if\ D^{(I,q)}(t) = 1, \end{cases} \tag{5.16}$$

where $\epsilon_{y_x}^{(I,q)} \triangleq y_x^{(I,q)} - \hat{x}^{(I,q)} - \hat{f}_x^{(I,q)}$ and $D^{(I,q)}$ denotes the binary decision of the monitoring module $\mathcal{M}^{(I,q)}$ on the occurrence of sensor faults as part of the diagnosis process.

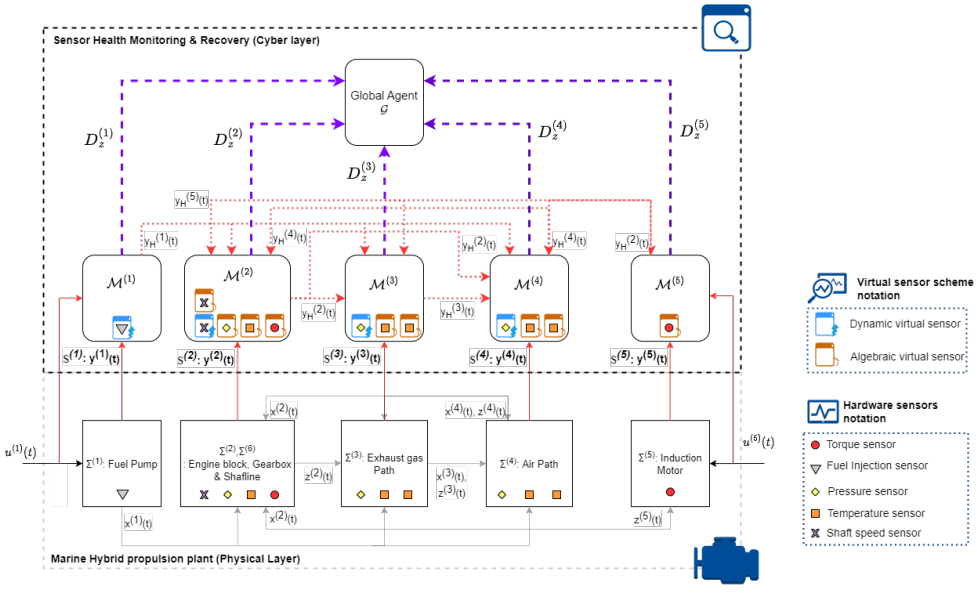


Figure 5.3: Distributed Sensor Fault Diagnosis scheme with the addition of virtual sensors for fault recovery. The distributed nature of the scheme is indicated by the communication between the monitoring agents, using the interconnection variables y_χ (shown as red,dotted lines). The virtual sensors are implemented as an extension of the monitoring agents.

5.3.2 Algebraic virtual sensors

If (3.1b) can be written in an explicit form $z^{(I)}(t) = \xi_z^{(I)}(x^{(I)}(t), \chi^{(I)}(t), u^{(I)}(t))$, the following nonlinear estimator can be used:

$$\begin{cases} \hat{z}^{(I,q)} = \xi_z^{(I)}(y_{xH}^{(I,q)}, y_{\chi H}^{(I,q)}, u^{(I)}) & \text{(5.17a)} \\ \hat{f}_z^{(I,q)} = (y_z^{(I,q)} - \hat{z}^{(I,q)}) D^{(I,q)}. & \text{(5.17b)} \end{cases}$$

For all other cases of algebraic equations, the use of *Set Inversion via Interval Analysis* (*SIVIA*) (Jaulin et al., 2001) is proposed. The rationale behind *SIVIA* is the identification of sets of nonlinear functions with the **guaranteed property of convergence**. Using (3.1b), the following nonlinear estimator can be constructed:

$$0 = \xi^{(I,q)}(x^{(I,q)}, \hat{z}^{(I,q)}, \chi^{(I,q)}, u^{(I)}) \tag{5.18}$$

From (3.2), the following intervals are known: $[x^{(I,j,q)}] = y_x^{(I,j,q)} - \hat{f}_x^{(I,j,q)} + [d_x^{(I,j,q)}]$ ($[x_j^{(I,j,q)}] = [y_{x_j}^{(I,j,q)} - \hat{f}_x^{(I,j,q)} - \bar{d}_{x_j}^{(I,j,q)}, y_{x_j}^{(I,j,q)} - \hat{f}_x^{(I,j,q)} + \bar{d}_{x_j}^{(I,j,q)}] = \hat{x}_j^{(I,j,q)} + [d_{x_j}^{(I,j,q)}]$, $j = 1, \cdots, n_I - r_I$), $[\chi^{(I,j,q)}] = y_\chi^{(I,j,q)} + [\hat{f}_\chi^{(I,q)}] + [d_\chi^{(I,q)}]$, $[u^{(I)}] = [\underline{u}^{(I)}, \bar{u}^{(I)}]$. The set to be inverted by *SIVIA* is expressed as $\mathbb{Y}^{(I,q)} = [\xi^{(I,q)}] = 0$. Using the above information, the unknown interval box $[\hat{z}^{(I,q)}]$ can be estimated based on an initial prediction interval $[\hat{z}^{(I,q)}]_0 \triangleq [\underline{\hat{z}}_0^{(I,q)}, \bar{\hat{z}}_0^{(I,q)}]$.

If the intervals of values for the parameters $x^{(I,q)}, \chi^{(I,q)}, u^{(I)}$ are known, *SIVIA* can calculate the unknown interval $[\hat{z}^{(I,q)}]_s \triangleq [\underline{\hat{z}}_s^{(I,q)}, \bar{\hat{z}}_s^{(I,q)}] = y_z^{(I,q)} + [\hat{f}_z^{(I,q)}] + [d_z^{(I,q)}]$ through numerical iterations with proved convergence (Jaulin et al., 2001). After some mathematical manipulations, the unknown interval $[\hat{f}_z^{(I,q)}] = [\underline{\hat{f}}_z^{(I,q)}, \bar{\hat{f}}_z^{(I,q)}]$ can be approximated as follows:

$$\begin{cases} \underline{\hat{f}}_z^{(I,q)} = y_z^{(I,q)} - \bar{d}_z^{(I,q)} - \bar{\hat{z}}_s^{(I,q)} \\ \bar{\hat{f}}_z^{(I,q)} = y_z^{(I,q)} - \bar{d}_z^{(I,q)} - \underline{\hat{z}}_s^{(I,q)}. \end{cases} \tag{5.19}$$

The estimates of the algebraic state and sensor fault are finally obtained as:

$$\begin{cases} \hat{z}^{(I,q)} = y_{zH}^{(I,q)} & \text{(5.20a)} \\ \hat{f}_z^{(I,q)} = \dfrac{\bar{\hat{f}}_z^{(I,q)} + \underline{\hat{f}}_z^{(I,q)}}{2} D^{(I,q)}. & \text{(5.20b)} \end{cases}$$

In the above formulations (5.15), (5.17) and (5.20), the healthy sensor measurements $y_{xH}^{(I,q)}, y_{\chi H}^{(I,q)}$ serve as the main outputs of the virtual sensors, alongside the estimations of the sensors faults $\hat{f}_x^{(I,q)}$, $\hat{f}_z^{(I,q)}$, $\hat{f}_\chi^{(I,q)}$, and are calculated as follows:

$$\begin{cases} y_{xH}^{(I,q)} = y_x^{(I,q)} - \hat{f}_x^{(I,q)} \\ y_{zH}^{(I,q)} = y_z^{(I,q)} - \hat{f}_z^{(I,q)} \\ y_{\chi H}^{(I,q)} = y_\chi^{(I,q)} - \hat{f}_\chi^{(I,q)}. \end{cases} \tag{5.21}$$

5.4 Multi-sensory switching logic

As previously discussed in Section 5.1, the multi-sensory switching logic included in each monitoring agent $\mathcal{M}^{(I)}, I = 1, \cdots, 5$ decides on which feedback sensor to use based on certain criteria. In the following subsections, the various proposed switching criteria for improved control tracking performance, safety and control stability, under the occurrence of sensor faults, are formulated.

5.4.1 Performance criteria

As previously stated, the switching logic decides on the shaft speed and *IM* torque feedback sensor indices to use, denoted as $\sigma^{(2)} \in \{1,2,3\}$ and $\sigma^{(5)} \in \{1,2\}$ respectively. In both cases, **an index value of 1 corresponds to the respective hardware sensors** whereas, **the virtual sensors receive indices greater than 1**. The performance criteria describe the switching law for achieving the minimum reference tracking error, leading to improved tracking performance; i.e.,:

$$\sigma^{(2)}(t) = \begin{cases} arg\min\limits_k \left| y_{(1,k)}^{(2)}(t) - n_{ref} \right|, & S^{(2)}\{1\} \in S^F \\ 1, & S^{(2)}\{1\} \notin S^F, \end{cases} \tag{5.22}$$

$$\sigma^{(5)}(t) = \begin{cases} arg\min\limits_k \left| y_{(1,k)}^{(5)}(t) - Q_{ref} \right|, & S^{(5)}\{1\} \in S^F \\ 1, & S^{(5)}\{1\} \notin S^F, \end{cases} \tag{5.23}$$

where $y_{(1,k)}^{(2)}, k \in \{1,2,3\}$ denotes the measurement value of the hardware sensor ($k = 1$) based on (3.36), differential virtual sensor ($k = 2$) based on (3.33) and (5.15a) and algebraic virtual sensor ($k = 3$) based on (3.35) and (5.17) that can be used for the shaft speed measurement and $y_{(1,k)}^{(5)}, k \in \{1,2\}$ denotes the measurement value of the hardware sensor ($k = 1$) based on (3.32) and algebraic virtual sensor ($k = 2$) based on (3.31) and (5.17) that can be used for the *IM* torque measurement.

5.4.2 *ICE*-specific Operational criteria

The operational criteria are mainly focused on safety of operation of the *ICE* systems ($\Sigma^{(1)}, \cdots, \Sigma^{(4)}$). For the specific engine model, the operational envelope is shown in Figure 5.4 and certain regions of performance can be seen in different colors, denoted as Ranges. The horizontal axis corresponds to the engine shaft speed measurement ($i_{gb} \cdot y_1^{(2)}$) in $[rpm]$ while the vertical axis is the produced power of the engine per cylinder ($i_{gb} \cdot y_1^{(2)} \cdot y_4^{(2)} / i_e$) in $[kW/cyl]$, where i_e is the number of cylinders and i_{gb} denotes the gearbox ratio. According to the project guide (SE, 2008), the engine operates in Range I under normal conditions. In case the operational point belongs to Range II, it is strongly advised to only operate the engine there for a maximum of 1 min and only for acceleration or manoeuvring operations. Finally, in Range III, operation is permitted up to 12 h. After this maximum allowable time durations have elapsed, the *ICE* can become unstable and multiple system failures can occur.

Regarding the design efficiency of virtual sensors, some preliminary results have already been extracted in (Kougiatsos &Reppa, 2022). More precisely, the use of differential virtual sensors produces relatively accurate results with minimal noise effect due to the combined filtering ability of the model-based controllers (controller gains k_1, k_2, k_3) and the adaptive observer (gain $L^{(2,1)}$). However, the adaptive nature of the underlying nonlinear observers entails a time-lag for the convergence of the fault estimation process. On the other hand, in the case of algebraic virtual sensors, convergence is fast, with the noise attenuation characteristics solely depending on the model-based design of the controllers (controller gains k_1, k_2, k_3).

As a result, the operational criteria dictate that, algebraic virtual sensors should be preferred in cases when the hardware shaft speed, $\mathcal{S}^{(2)}\{1\}$, and *ICE* torque, $\mathcal{S}^{(2)}\{4\}$, sensors indicate operation in Regions I or III and at least one of those sensors belong to $\mathcal{S}^F$.

5.4.3 Control stability criteria

Aside from the performance and operational criteria which are related to system tracking performance and stability considerations respectively, further criteria need to be specified regarding control stability between consecutive switching of sensors. These criteria can be expressed in terms of the reference tracking error for the different sensors. In order to analytically evaluate the criteria for control stability, both under healthy and faulty sensor operation, the following Lemma is used.

Lemma 5.1 *[Lyapunov stability] For linearized feedback systems with tracking error dynamics of the form*

$$\dot{\epsilon} = A \cdot \epsilon + B \cdot v, \tag{5.24}$$

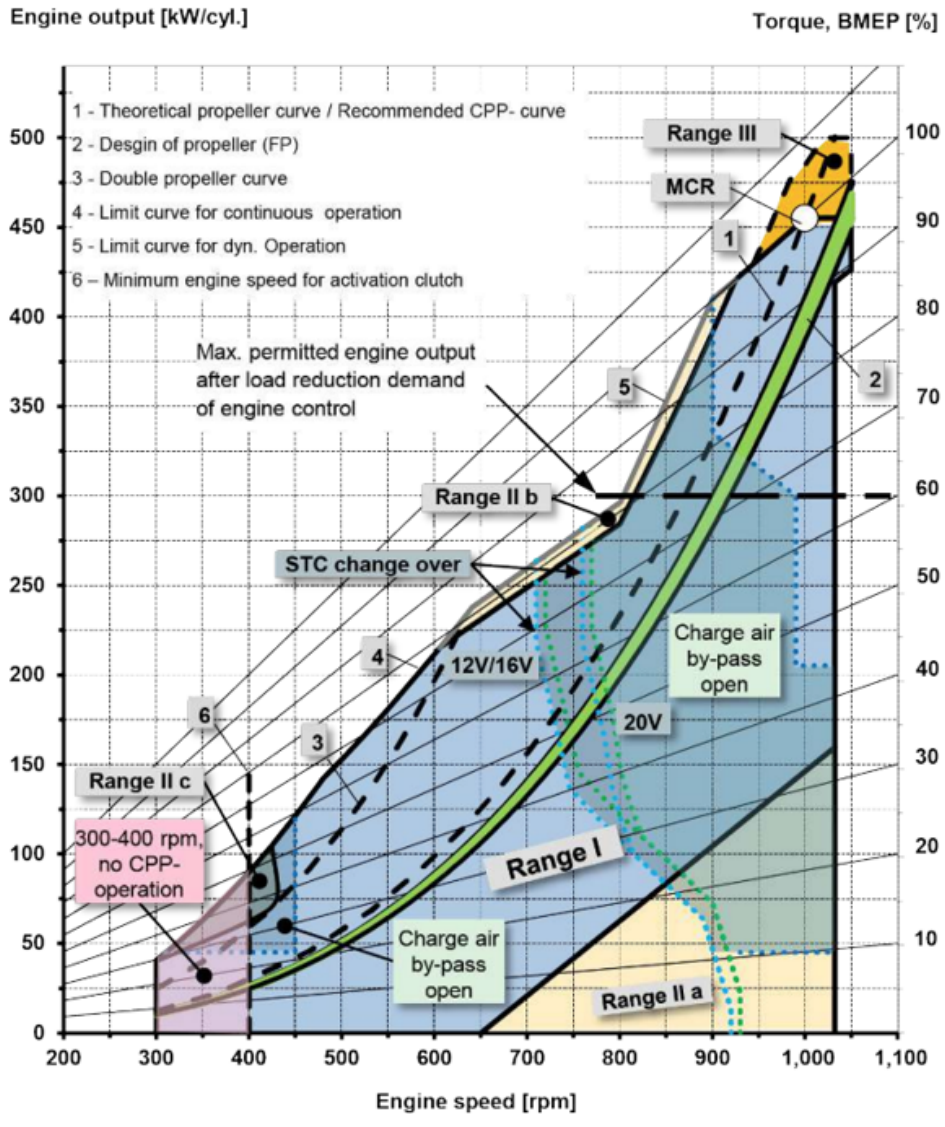


Figure 5.4: MAN V28/33D STC ICE *operational envelope (SE, 2008)*

where $\epsilon(t) \in \mathbb{R}^{(n-r)}$ denotes the tracking error and A, B are linear matrices, a candidate Lyapunov function based on the system (5.12) *is $V(\epsilon, v) = (1/2) \cdot \epsilon^\top \epsilon > 0$.*

Asymptotic control stability is satisfied if and only if $\dot{V}(t) < 0 \; \forall \epsilon \neq 0$, which after some algebraic manipulations yields:

$$\dot{V}(t) = \epsilon^\top \left(A^\top + A\right)\epsilon + v^\top B^\top \epsilon + \epsilon^\top B v < 0. \tag{5.25}$$

□

Under healthy sensor conditions ($f_1^{(2)} = 0, f_1^{(5)} = 0$), only hardware sensors are in use and the reference tracking errors are expressed by (5.29) and (5.31). For control stability, Theorem 5.2 applies.

Theorem 5.2 (Stability under healthy sensor conditions) *The feedback linearizable system* (5.10) *with control law* (5.11) *is stable under healthy sensor conditions of the sensors $\mathcal{S}^{(2)}\{1\}$ and $\mathcal{S}^{(5)}\{1\}$, if at least one of the following conditions is true:*

$$\tilde{x}_2 \geq \max\left\{0, \; \frac{(1-k_1)}{k_2}\left(y_1^{(2)} - n_{ref} + \bar{d}_1^{(2)}\right)\right\} = \underline{\tilde{x}}_2, \tag{5.26}$$

$$\tilde{x}_2 \leq \min\left\{0, \; \frac{(1-k_1)}{k_2}\left(y_1^{(2)} - n_{ref} - \bar{d}_1^{(2)}\right)\right\} = \bar{\tilde{x}}_2, \tag{5.27}$$

where $\tilde{x}_2$ is defined in (5.9)*, k_1, k_2 are positive constants and sufficing that the unknown sensor noise vectors $d^{(2)}, d^{(5)}$ are bounded; i.e. $\left|d_j^{(I)}\right| \leqslant \bar{d}_j^{(I)}, \forall j \in 1, \cdots, n_I$ where $\bar{d}_j^{(I)}$ is known.*

Proof : [Proof of Theorem 5.2] Using the reference tracking error expression in (5.12), Lemma 5.1 and some algebraic manipulations implies:

$$\epsilon_{\tilde{x}}^\top \begin{bmatrix} 0 & 1-k_1 \\ 1-k_1 & -2 \cdot k_2 \end{bmatrix} \epsilon_{\tilde{x}} \leq 0, \tag{5.28}$$

The next step is to mathematically express the reference tracking error for the shaft speed hardware sensor in comparison to $\epsilon_{\tilde{x}}$. Using (3.2), we denote the hardware sensor measurement tracking error as $\epsilon_y^{(2)}(t) \triangleq \left[y_1^{(2)} - n_{ref}; \tilde{x}_2(t)\right]^\top$, and mathematically associate it with $\epsilon_{\tilde{x}}^{(2)}(t)$ as follows:

$$\epsilon_y^{(2)}(t) = \epsilon_{\tilde{x}}^{(2)}(t) + \begin{bmatrix} d_1^{(2)}(t) \\ 0 \end{bmatrix}. \tag{5.29}$$

Substituting (5.29) in (5.28) and after some algebraic manipulations we obtain the following condition for stability:

$$\tilde{x}_2\left(\tilde{x}_2 + \frac{(k_1-1)}{k_2}\left(y_1^{(2)} - n_{ref} - d_1^{(2)}\right)\right) \geq 0 \tag{5.30}$$

where, however, $d_1^{(2)}$ is unknown. Using the assumption that $\left|d_1^{(2)}\right| \leqslant \overline{d}_1^{(2)}$ where $\overline{d}_1^{(2)}$ is known and exploring cases for the sign of $\tilde{x}_2$ (above or below zero), we are able to obtain the two conditions expressed in (5.26), (5.27).

Likewise, using (3.2), the reference tracking error for the hardware motor torque sensor, denoted as $\epsilon_y^{(5)}(t) \triangleq y^{(5)} - Q_{ref}$, is expressed as :

$$\epsilon_y^{(5)}(t) = d^{(5)}(t), \tag{5.31}$$

Taking again into account that $\left|d^{(5)}\right| \leqslant \overline{d}^{(5)}$ with $\overline{d}^{(5)}$ known, the *IM* closed-loop system is stable under healthy sensor conditions. □

When one or more hardware sensors used in the control feedback loop is affected by faults, the virtual sensors are switched in to compensate for the fault effects. In the case of the shaft speed controller, two candidate virtual sensors can be used for feedback purposes, the differential virtual sensor ($k = 2$) and the algebraic virtual sensor ($k = 3$). While the first proceeds to use the faulty hardware sensor ($k = 1$) to estimate the magnitude of the sensor fault and the fault-free measurement according to (5.15), the latter does not, according to (5.17). The control stability criteria under the occurrence of sensor faults are designed to ensure that the switching between the differential and algebraic shaft speed virtual sensor will not compromise stability. The necessary analytical conditions for control stability are, thus, described in the following theorem.

Theorem 5.3 (Stability under sensor faults) *The feedback linearizable system* (5.10) *with control law* (5.11)*, is stable under the influence of sensor faults affecting the sensor* $\mathcal{S}^{(2)}\{1\}$ *(see Eq. 3.36) by switching to either the differential or the algebraic shaft speed virtual sensors, described in* (5.15) *and* (5.17) *respectively, under the following conditions:*

(1) ***Condition 1:*** *When switching to the differential shaft speed virtual sensor, control stability is maintained, if and only if:*

$$\begin{aligned} 0 \leq & \left(k_2 + L_2^{(2)}\right)\hat{x}_2^2 - \hat{x}_2\left(\hat{x}_1 - n_{ref} + L_2^{(2)}\tilde{x}_2\right) + \\ & \left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)} + 1\right) - k_1\right)\left(\hat{x}_1 - n_{ref}\right)^2 - \\ & \left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)} + 1\right)\right)\left(\epsilon_y^{(2)} + \hat{f}_1^{(2)}\right)\left(\hat{x}_1 - n_{ref}\right), \end{aligned} \tag{5.32}$$

where $\hat{x}_1$ *denotes the estimation of the states* $\tilde{x}_1$ *in* (5.10)*,* $\hat{f}_1^{(2)}$ *is the estimation of the shaft speed sensor fault,* $\epsilon_y^{(2)} = y_1^{(2)} - n_{ref}$ *is the reference tracking error of the hardware shaft speed sensor,* $L^{(2)} \in \mathbb{R}_+^2$*,* $\Gamma^{(2)} \in \mathbb{R}_+$ *and* $\Omega^{(2)} \in \mathbb{R}$ *have already been introduced in* (5.15)*.*

(2) ***Condition 2:*** *When switching to the algebraic shaft speed virtual sensor, control stability is maintained, if and only if:*

$$\epsilon_{\hat{x}}^{\top}\begin{bmatrix} 0 & 1-k_1 \\ 1-k_1 & -2\cdot k_2 \end{bmatrix}\epsilon_{\hat{x}} \leq 0, \tag{5.33}$$

where $\epsilon_{\hat{x}} = \left[\hat{x}_1 - n_{ref}; \hat{x}_2\right]^{\top}$ *denotes the reference tracking error and* k_1, k_2 *are positive constants.*

Proof : [Proof of Theorem 5.3] Considering the dynamics in (5.10) and substituting (5.11) yields:

$$\begin{cases} \dot{\tilde{x}}_1 = \tilde{x}_2 \\ \dot{\tilde{x}}_2 = -k_1(\tilde{x}_1 - n_{ref}) - k_2\tilde{x}_2. \end{cases} \tag{5.34}$$

Using (5.15a), the differential virtual sensor is then expressed as follows:

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + L_1^{(2)}(y_1^{(2)} - \hat{x}_1 - \hat{f}) + \Omega\dot{\hat{f}} \\ \dot{\hat{x}}_2 = -k_1(\hat{x}_1 - n_{ref}) - k_2\hat{x}_2 + L_2^{(2)}(\tilde{x}_2 - \hat{x}_2), \end{cases} \tag{5.35}$$

which after substituting from (5.15) and some algebraic manipulations renders:

$$\begin{cases} \dot{\hat{x}}_1 = -\left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)}+1\right)\right)\hat{x}_1 + \hat{x}_2 \\ \qquad -\left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)}+1\right)\right)\hat{f}_1^{(2)} \\ \qquad +\left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)}+1\right)\right)\epsilon_y^{(2)} & (5.36a) \\ \dot{\hat{x}}_2 = -k_1(\hat{x}_1 - n_{ref}) - \left(k_2 + L_2^{(2)}\right)\hat{x}_2 + L_2^{(2)}\tilde{x}_2, & (5.36b) \end{cases}$$

where $\hat{x}_1, \hat{x}_2$ denote the estimations of the states $\tilde{x}_1, \tilde{x}_2$, $\hat{f}_1^{(2)}$ is the estimation of the shaft speed fault, $\epsilon_y^{(2)} = y^{(2)} - n_{ref}$ is the reference tracking error of the hardware shaft speed sensor, $L^{(2)} \in \mathbb{R}_+^2$, $\Gamma^{(2)} \in \mathbb{R}_+$ and $\Omega^{(2)} \in \mathbb{R}$. Defining the tracking error of the differential shaft speed sensor as $\epsilon_{\hat{x}} = \left[\hat{x}_1 - n_{ref}; \hat{x}_2\right]^{\top}$ results in a tracking error equation of the form (5.24) with:

$$A = \begin{bmatrix} -\left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)}+1\right)\right) & 1 \\ -k_1 & -\left(k_2 + L_2^{(2)}\right) \end{bmatrix},$$

$$B = \begin{bmatrix} \left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)}+1\right)\right) & 0 \\ 0 & L_2^{(2)} \\ \left(L_1^{(2)} + \Omega^{(2)}\Gamma^{(2)}\left(\Omega^{(2)}+1\right)\right) & 0 \end{bmatrix}^{\top},$$

and $v = \left[\epsilon_y^{(2)}; \tilde{x}_2; \hat{f}_1^{(2)}\right]^{\top}$. Using Lemma 5.1 and based on the aforementioned matrices, condition 1 is obtained, as formulated in (5.32).

Algorithm 5.1 Multi-sensory switching logic for marine propulsion plants (Shaft speed). This switching logic block is embedded in monitoring agent $\mathcal{M}^{(2)}$.

Input: S^F ▷ Faulty sensor set (from diagnosis)
Output: $\sigma^{(2)}$ ▷ Index of the selected shaft speed sensor

1: $y_1^{(2)} \leftarrow$Shaft speed measurement (rps)
2: $y_4^{(2)} \leftarrow$*ICE* torque measurement (Nm)
3: $y_1^{(5)} \leftarrow$*IM* torque measurement (Nm)
4: $i_e \leftarrow$Number of engine cylinders
5: $\mathrm{M} \leftarrow \left(i_{gb} \cdot y_1^{(2)}, i_{gb} \cdot y_1^{(2)} \cdot y_4^{(2)} / i_e\right)$ ▷ *ICE* operational point
6: $\sigma^{(2)} \leftarrow 1$ ▷ Hardware sensor
7: **while** True **do**
8: $\quad \sigma_p \leftarrow \sigma^{(2)}$
9: $\quad$ **if** $S^{(2)}\{1\} \in S^F$ **then**
10: $\quad\quad$ **if** $M \in$ Region II **and** Cond. (5.33) is True **then**
11: $\quad\quad\quad \sigma^{(2)} \leftarrow 3$ ▷ Operational criteria
12: $\quad\quad$ **else if** $M \in$ Region II **then**
13: $\quad\quad\quad \sigma^{(2)} \leftarrow \sigma_p$
14: $\quad\quad$ **else**
15: $\quad\quad\quad$ Compute $\sigma^{(2)}$ from (5.22) ▷ Performance criteria
16: $\quad\quad\quad$ **if** $\sigma^{(2)} = 2$ **and** Cond. (5.32) is True **then**
17: $\quad\quad\quad\quad$ **go to step** 24
18: $\quad\quad\quad$ **else if** $\sigma^{(2)} = 3$ **and** Cond. (5.33) is True **then**
19: $\quad\quad\quad\quad$ **go to step** 24
20: $\quad\quad\quad$ **else**
21: $\quad\quad\quad\quad \sigma^{(2)} \leftarrow \sigma_p$
22: $\quad\quad\quad$ **end if**
23: $\quad\quad$ **end if**
24: $\quad$ **end if**
25: **end while**

The reference tracking error definition for the shaft speed algebraic virtual sensor is the same as the differential virtual sensor case, that is $\epsilon_{\hat{x}} = \left[\hat{x}_1 - n_{ref}; \hat{x}_2\right]^\top$. However, in this case the reference tracking error dynamics obtain the form:

$$\dot{\epsilon}_{\hat{x}}^{(2)}(t) = \begin{bmatrix} 0 & 1 \\ -k_1 & -k_2 \end{bmatrix} \cdot \epsilon_{\hat{x}}^{(2)}(t). \tag{5.37}$$

The application of Lemma 5.1 in (5.37) yields condition 2, analytically expressed in (5.33), for switching to the algebraic shaft speed virtual sensor. □

Algorithm 5.2 Multi-sensory switching logic for marine propulsion plants (Motor torque). This switching logic block is embedded in monitoring agent $\mathcal{M}^{(5)}$.

Input: S^F ▷ Faulty sensor set (from diagnosis)
Output: $\sigma^{(5)}$ ▷ Index of the selected motor torque sensor
1: $\sigma^{(5)} \leftarrow 1$ ▷ Hardware sensor
2: **while** True **do**
3: **if** $S^{(5)}\{1\} \in S^F$ **then**
4: Compute $\sigma^{(5)}$ from (5.23) ▷ Performance criteria
5: **end if**
6: **end while**

The various criteria mentioned in the above subsections will work together to enable switching decisions between the available hardware and virtual sensors. As a result, resilience under the presence of sensor faults affecting the hardware feedback sensors is promoted. The switching logic is composed of a total of two blocks, one included in the monitoring agent $\mathcal{M}^{(2)}$ and another one being part of monitoring agent $\mathcal{M}^{(5)}$. The switching logic block built in the monitoring agent $\mathcal{M}^{(2)}$ considers performance, operational and control stability criteria, analyzed in the above subsections. The switching logic of monitoring agent $\mathcal{M}^{(5)}$, however, only considers performance criteria. The content of each switching logic block is shown in Algorithms 5.1 and 5.2 respectively.

5.5 Simulation results

In this section, the multi-sensory switching logic presented in Section 5.4 is applied to the hybrid propulsion plant model, provided in Chapter 3 with parameters found in (Geertsma et al., 2017b). To this end, we assume a deceleration situation for the marine propulsion plant, with a gradual drop of power P_D from 9 MW to 6 MW, occurring for 30 $sec \leq t \leq 40$ sec. In order to track the reference signals n_{ref} and Q_{ref} (calculated using (5.1) and (5.2)) , we implement the control strategy presented in Sections 5.1 and 5.2, assuming the following gains for the model-based primary level controllers (see Section 5.2): $k_1 = 10$, $k_2 = 100$, $k_3 = 50$. The parameters of the employed models shown in Chapter 3 can be found in (Geertsma et al., 2017b). The initial conditions for the *ICE* are set to the maximum continuous rating (MCR) point while for the electric motor, a starting speed equal to the one at the MCR point of the *ICE*, $N_{MCR} = 16.7$ [rpm] is assumed.

We then assume that measurements of each sensor are corrupted by uniformly distributed noise with $\bar{d}_j^{(I)}$ being 3% of the amplitude of the noiseless measurements of the sensor. During the tracking of the power profile by the control agents, two

permanent abrupt offset sensor faults are simulated affecting the shaft speed sensor $\mathcal{S}^{(2)}\{1\}$ and the electric motor torque sensor $\mathcal{S}^{(5)}\{1\}$, at $T_{f_1}^{(2)} = 20\ sec$ and $T_{f_1}^{(5)} = 70\ sec$ respectively and with fault magnitudes of $\hat{\phi}_1^{(2)} = 2\ rps$ and $\hat{\phi}_1^{(5)} = 5 \cdot 10^4\ Nm$. The theoretical background behind the sensor fault diagnosis architecture has been already provided in Chapter 4. The design gains of the various monitoring modules corresponding to the marine *ICE* are selected as $L^{(1,1)} = 1.16$, $L^{(2,1)} = 10$, $L^{(3,1)} = 445$, $L^{(4,1)} = 319.98$ while the learning rates for the design of the differential virtual sensors are selected as $\Gamma^{(1)} = 0.5$, $\Gamma^{(2,1)} = 100$, $\Gamma^{(3,1)} = 8.7$, $\Gamma^{(4,1)} = 5$.

The simulation results are displayed in Figures 5.5-5.8. In Figures 5.5-5.7, the results related to the fault resilience provided by the monitoring agents $\mathcal{M}^{(2)}$ and $\mathcal{M}^{(5)}$ are displayed. More specifically, the time evolution of the sensor switching decisions $\sigma^{(2)}$ and $\sigma^{(5)}$ (blue/continuous line) is shown in Figure 5.5(a),(d) and related to the diagnosis process (red/dash-dotted line). As can be seen from these subfigures, the sensor faults are almost immediately diagnosed after their occurrence with the monitoring decisions $D^{(2,1)}$ and $D^{(5)}$ assuming the value of 1. Subsequently the sensor switching process is initiated, as shown with the blue/continuous lines.

As previously discussed in Algorithm 5.1, operational, performance and control stability criteria are all integrated in the sensor switching logic for $\mathcal{M}^{(2)}$. For the latter, analytical conditions have already been expressed in (5.32),(5.33) regarding switching to the differential and the algebraic virtual sensor respectively and are presented in Figures 5.5(b),(c). In both subfigures, the value of '0' is displayed with a red/dashed line while the evaluation of switching conditions 1 and 2, found in (5.32),(5.33), is shown with red/ continuous lines. As shown from Figure 5.5(b), Condition 1 is always satisfied (value '1' is assumed) after the diagnosis of the fault affecting sensor $\mathcal{S}^{(2)}\{1\}$ at $t = 20\ sec$, meaning that switching to the differential virtual sensor ($k = 2$) is always possible and only decided by the effects of performance criteria. In Figure 5.5(c), though, we notice that the same statement is not valid for the algebraic virtual sensor ($k = 3$). The evaluation of Condition 2 expressed in (5.33) alternates between '0' (invalid) and '1' (valid) after the diagnosis of the sensor fault at $t = 20\ sec$. Under the effects of the performance, operational and previously discussed control stability criteria, the switching result between hardware and virtual shaft speed sensors is that of rather frequent alternations between the differential ($k = 2$) and algebraic ($k = 3$) virtual sensors after the diagnosis of the shaft speed sensor fault at $t = 20\ sec$, also shown in Figure 5.5(a). As for the sensor fault affecting the *IM* torque sensor ($k = 1$), only performance criteria are used for sensor switching and Algorithm 5.2 is in use. The sensor switching process is less complicated in this case, as only an algebraic virtual sensor is available for the *IM* torque measurement ($k = 2$). As a result, after the diagnosis of this sensor fault, indicated by the shift of the decision $D^{(5)}$ of the monitoring agent $\mathcal{M}^{(5)}$ from 0 to 1 at $t = 70\ sec$, the decision of the used feedback sensor changes from $\sigma^{(5)} = 1$ (hardware

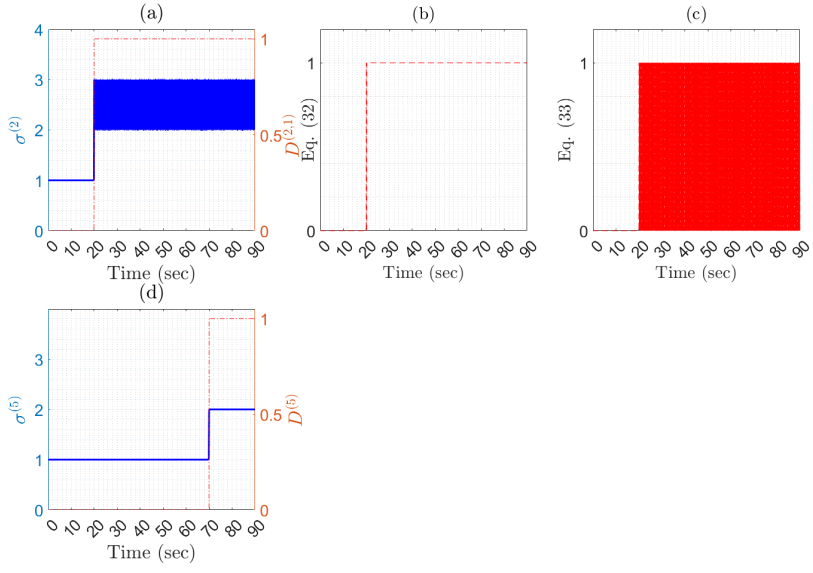


Figure 5.5: Sensor switching results and computation of analytically derived conditions (5.32),(5.33) *for each of the two monitoring agents* $\mathcal{M}^{(2)}$ *(subfigures (a)-(c)) and* $\mathcal{M}^{(5)}$ *(subfigure (d)). The diagnosis decisions are presented with a red/dash-dotted line in (a), (d) with the respective switching signals* $\sigma^{(2)}$ *and* $\sigma^{(5)}$ *shown with a blue/continuous line. The analytical conditions check is performed in (b),(c) with '1' signifying that the respective analytical condition is valid and '0' the otherwise. The evaluation of the analytical conditions starts after the diagnosis of the sensor fault.*

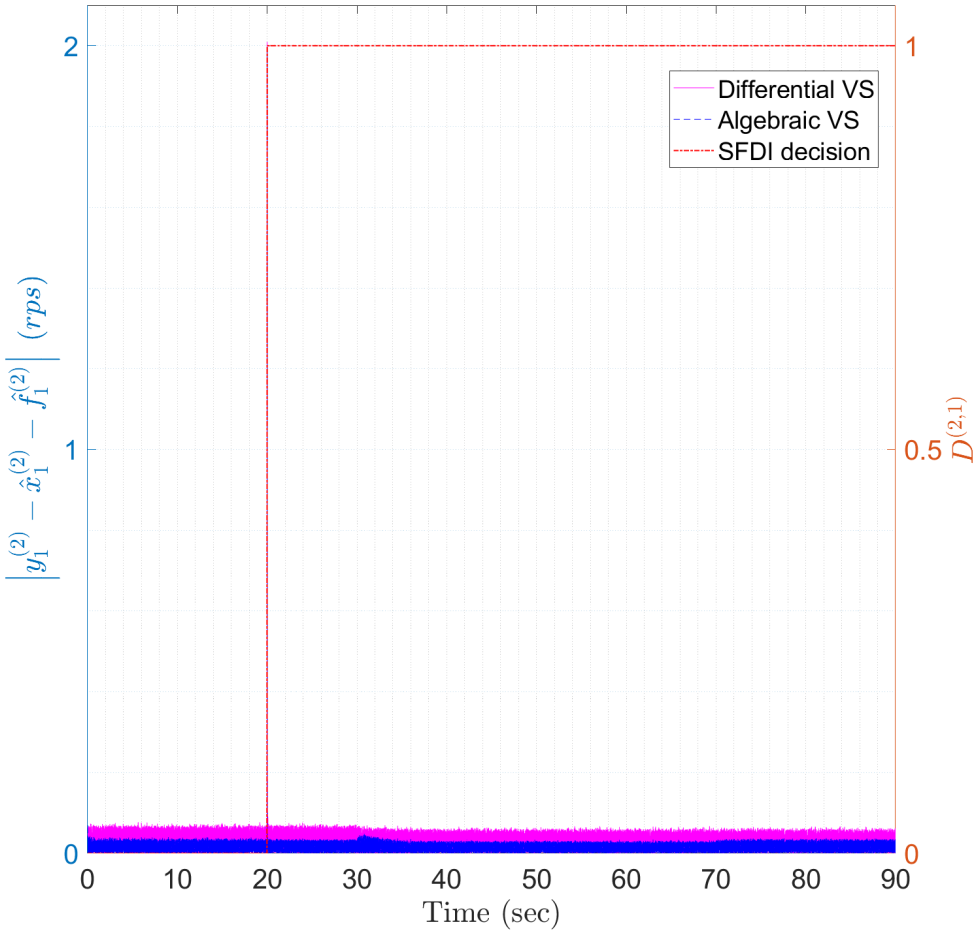


Figure 5.6: Performance of the differential and algebraic virtual sensor instances for the shaft speed measurement estimation. The SFDI decision is shown with a red/dash-dotted line while blue and magenta/continuous lines are used to showcase the estimation errors of the differential and the algebraic virtual sensor, respectively (left side y axis).

torque sensor) to $\sigma^{(5)} = 2$ (algebraic torque virtual sensor).

As already mentioned, the performance of the virtual sensor instances is highly dependent on the accuracy of the employed models. In this chapter, First Principle DAE models have been used and two types of virtual sensors have been proposed in Section 5.3. In order to assess the performance of virtual sensors, the estimation errors $|y_1^{(2)} - \hat{x}_1^{(2)} - \hat{f}_1^{(2)}|$ (in rps) and $|y_1^{(5)} - \hat{x}_1^{(5)} - \hat{f}_1^{(5)}|$ (in $N \cdot m$) have been calculated and shown in Figures 5.6 and 5.7 respectively, considering all available types of virtual sensors in each case. As can be seen from Figure 5.6, a satisfactory tracking

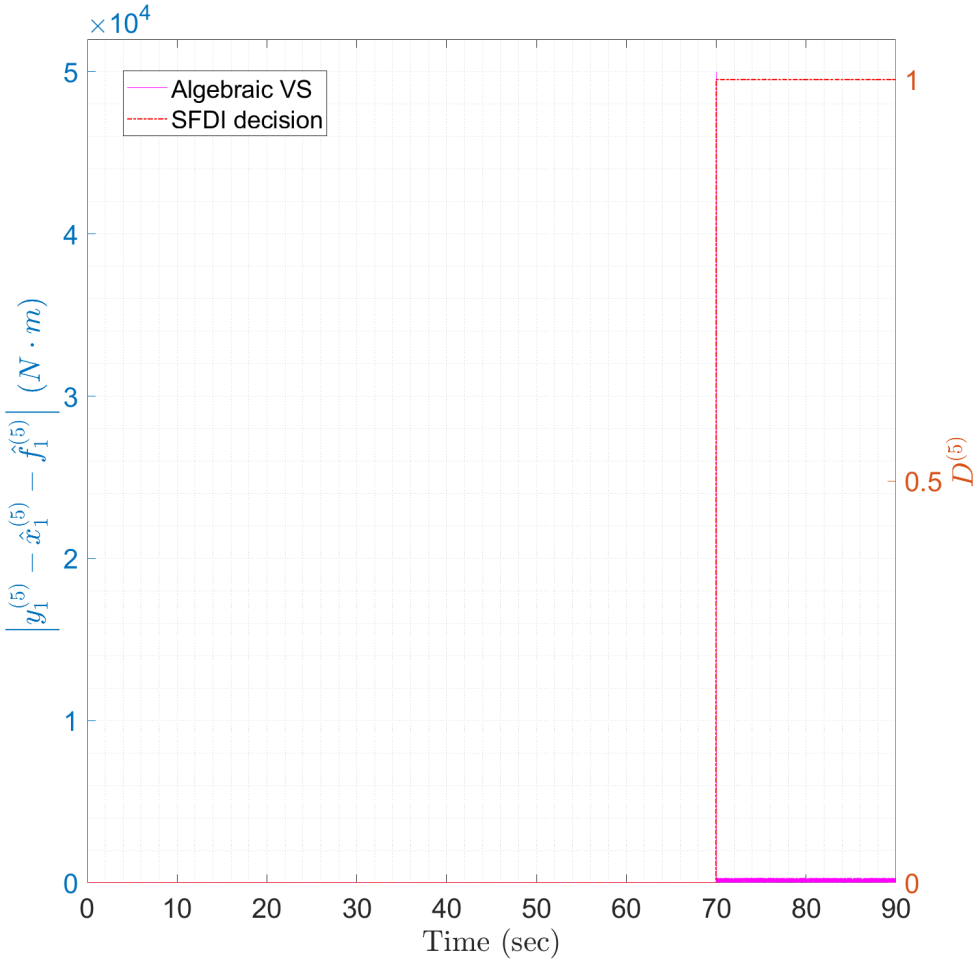


Figure 5.7: Performance of the algebraic virtual sensor instance for the motor torque measurement estimation. The SFDI decision is shown with a red/dash-dotted line while a magenta/continuous line is used to showcase the estimation error of the algebraic virtual sensor (left side y axis).

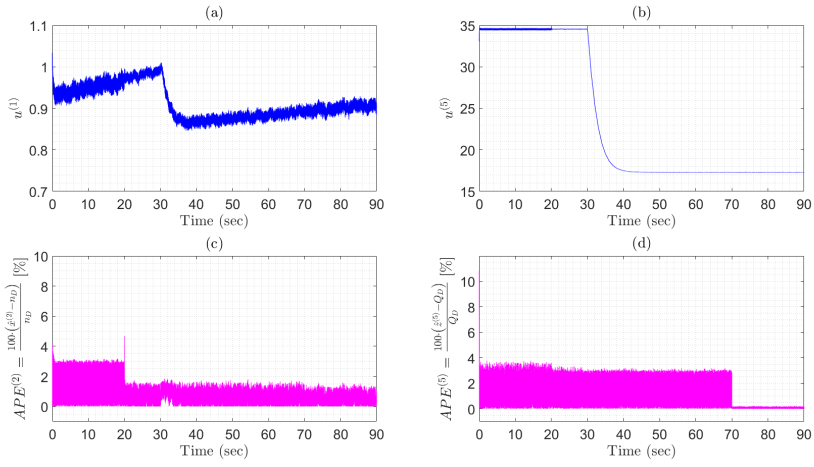


Figure 5.8: Performance results for the distributed primary level control scheme focusing on the control signals $u^{(1)}$, $u^{(5)}$ in (a),(b) and their absolute percentage reference tracking errors $APE^{(2)}$, $APE^{(5)}$ in (c), (d), respectively.

performance is achieved for both the differential (magenta line) and the algebraic (blue line) shaft speed virtual sensors, with a mean estimation error of 0.03 rps and 0.015 rps respectively. Similarly, as can be seen from Figure 5.7, a small estimation error is observed with a mean value equal to 33.4 Nm.

In Figure 5.8, the control agent perspective is presented, with the time history of control actions $u^{(1)}$ and $u^{(5)}$ displayed in Figures 5.8(a),(b) and the absolute percentage reference tracking errors (APEs), achieved using the designed controllers and sensor switching logic, displayed in Figures 5.8(c),(d), respectively. As seen from Figure 5.8(a), the control action $u^{(1)}$ is characterized by a mean value of 0.91 and a standard deviation of 0.04, indicating a small control effort despite the high nonlinearities considered in the shaft speed control agent design (see Section 5.2). A gradual change is noticeable at 30 $sec \leq t \leq 40$ sec due to the drop in the required power indicated by the reference power P_D in this time interval. Small changes in the noise of the control signal $u^{(1)}$ are also observed after $t = 20$ sec and $t = 70$ sec. This behavior is due to the switching between hardware and virtual sensors after those time instants. Considering the design of differential virtual sensors in (5.15), sensor noise is filtered using the gain $L^{(2)}$ and, thus, the control signal $u^{(1)}$ exhibits less noise after $t = 20$ sec. The noise of $u^{(1)}$ becomes, however, larger after $t = 70$ sec when the sensor switching decision of monitoring agent $\mathcal{M}^{(5)}$ becomes $\sigma^{(5)} = 2$ and the algebraic motor torque virtual sensor is activated. Due to the interconnection between the shaft speed and the motor torque controller, also seen in Figure 5.1, the

sensor switching effects are propagated to the control action $u^{(1)}$. A similar behavior is observed for the control signal $u^{(5)}$ of the *IM* torque controller in Figure 5.8(b). This control signal is characterized by a mean value of 23.83 V and a standard deviation of 8.13 V, indicating a higher control effort than the shaft speed controller and attributed to the employed secondary level control strategy. Again, the gradual change in control values is observed for 30 $sec \leq t \leq 40$ sec due to the drop in the required power. Moreover, at $t = 20$ sec, the change between the used shaft speed hardware $\sigma^{(2)} = 1$ and virtual sensors $\sigma^{(2)} \in \{2, 3\}$ is propagated to the *IM* torque controller through its interconnection with the shaft speed controller, resulting in a change of measurement noise in the control signal $u^{(5)}$.

In order to demonstrate the efficiency of the proposed fault-resilient architecture in tracking the reference power profile, Figure 5.8 is again examined. As seen from Figures 5.8(c),(d) the control signals result in relatively small APEs concerning the reference tracking errors of the primary level controllers, less than 4%. More specifically, the mean absolute percentage errors (MAPEs) equal to $MAPE^{(2)} = 2.77\%$ for the shaft speed reference signal and $MAPE^{(5)} = 0.05\%$ for the *IM* torque reference signal are achieved using the proposed control strategy. In both cases, the MAPE is less that the corresponding hardware sensor noise bound (3%), indicating a satisfactory tracking of the reference signals.

5.6 Conclusions

This chapter proposed a fault-resilient control architecture for marine hybrid propulsion plants. Thus, the following research question was addressed (**Q4:**) *"How to switch between hardware and virtual sensors during operation for enhanced fault resilience in marine propulsion plants?"*.

The control design considered two control levels, multiple control agents and was realised using model-based techniques. A switching logic was also developed to ensure efficient, safe and stable operation, under the occurrence of multiple sensor faults, employing a combination of control performance, operational and control stability criteria, respectively. Both hardware and virtual sensors were considered as subjects of the switching logic, with the latter designed using the hardware sensor measurements and model information. The simulation results showcased a stable and successful tracking of the control objectives with satisfactory performance metrics.

The use of virtual sensors alongside semantics for the optimisation of the sensor fault isolability performance will be explored in Chapter 6. Chapter 7 will then propose a resilient control targeted at both sensor faults and mission changes as adaptation drivers.

Chapter 6

Enhanced Distributed Sensor Fault Isolability of Marine Propulsion Systems

In Chapter 4, a distributed model-based *SFDI* methodology was proposed for marine *ICE*. The design of the monitoring agents was assessed using performance analysis tools. However, the isolability performance was not optimal. Moreover, the use of virtual sensors for control-related purposes was showcased in Chapter 5. Nonetheless, their use for optimising the monitoring capabilities was not explored.

This chapter addresses the following research question (**Q5:**) *"How to optimise the fault diagnosis capabilities and the required hardware redundancy for safe operation of marine* PPP*s?"*. This chapter is structured as follows. In Section 6.1 the use of semantics for the automated generation of the monitoring architecture is highlighted. The integrated optimization problem considering both isolation levels is then formulated in Section 6.2 and a greedy stochastic optimisation algorithm is proposed for its solution. The greedy optimiser is applied in a marine propulsion case study in Section 6.3 while some concluding remarks are provided in Section 6.4.

The contents of this chapter have been published in a conference publication (Kougiatsos &Reppa, 2024b) [1].

[1] **N. Kougiatsos** and V. Reppa, "Sensor Set Decomposition for Enhanced Distributed Sensor Fault Isolability of Marine Propulsion Systems," in: Proceedings of the 2024 IFAC SAFEPROCESS, Ferrara, Italy, pp. 55–60, 2024.

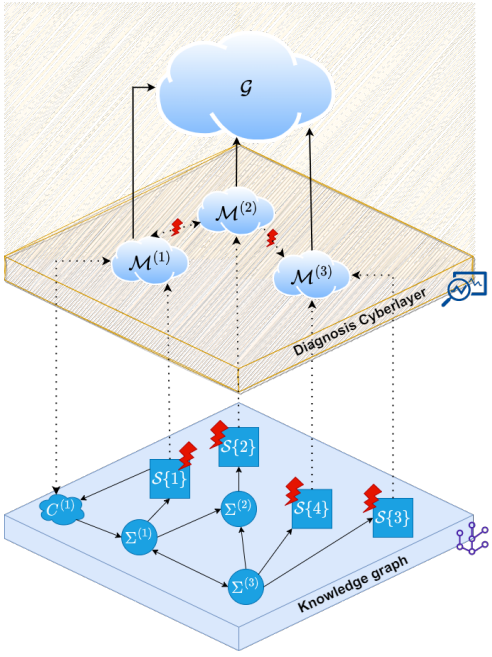


Figure 6.1: Sample design of a distributed sensor fault diagnosis scheme based on a known knowledge graph.

6.1 Semantics-based generation of monitoring architecture

Due to the large scale and complexity of marine propulsion installations, the application of a distributed monitoring architecture has already been proposed in [Kougiatsos et al. (2023)]. In this setup, monitoring agents $\mathcal{M}^{(I)}, I = 1, \cdots, N$ are designed, each consisting of N_I modules $\mathcal{M}^{(I,q)}$, $q = 1, \cdots, N_I$. Every agent $\mathcal{M}^{(I)}$ monitors a set of sensors $\mathcal{S}^{(I)}$, which is a subset of the global set of sensors denoted by $\mathcal{S}$. The sensors belonging to $\mathcal{S}$, the system components and controllers can be visualised in a knowledge graph as shown in Figure 6.1, where $\Sigma^{(I)}, C^{(I)}, \mathcal{S}\{I\}$ denote the subsystems, controllers and available sensors respectively. The number of monitoring agents is determined by the number of divisions of the available sensors set $\mathcal{S} \in \mathcal{F}_s$ into subsets $\mathcal{S}^{(I)}$, with one of those subsets assigned to each agent. Each module monitors the subset $\mathcal{S}^{(I,q)} \subseteq \mathcal{S}^{(I)}$.

The system interconnections included in the knowledge graph can be used to automatically configure the cyber connections between the monitoring agents in the distributed monitoring architecture, as indicated in Figure 6.1. For instance, the physical interconnection between $\Sigma^{(1)}, \Sigma^{(2)}$ indicates that a cyber connection should also exist between the monitoring agents $\mathcal{M}^{(1)}, \mathcal{M}^{(2)}$, using sensors $\mathcal{S}\{1\}$

and $\mathcal{S}\{2\}$ respectively. The information of the cyber connections between the monitoring agents are used for the generation of the theoretical FSMs $F^{(I)}$, F^{χ} in Section 6.2. The local multiple sensor fault isolability becomes complicated as the number of sensors in $\mathcal{S}^{(I)}$ increases. To handle this complexity, the objective of this chapter is to design an optimisation algorithm for the decomposition of the sensor set $\mathcal{S}$ in $\mathcal{S}^{(I)}, I = 1, \cdots, N$ subsets and the automated generation of the theoretical FSMs $F^{(I)}$, F^{χ} and agents' architecture $(\mathcal{M}^{(I)}, \mathcal{G})$ used in the distributed monitoring of marine propulsion systems, based on fault isolability criteria. To this end, we consider that each monitoring module $\mathcal{M}^{(I,q)}, I = 1, \cdots, N$ only uses one *Analytical Redundancy Relation* (*ARR*), meaning that $q = 1, \cdots, |\mathcal{S}^{(I)}|$.

6.2 Diagnostic system designer module

As previously discussed in Section 6.1, the design of the diagnosis cyberlayer depends on the decomposition of sensors in subsets $\mathcal{S}^{(I)}, I = 1, \cdots, N$ and their assignment to monitoring agents $\mathcal{M}^{(I)}$. In [Kougiatsos et al. (2023)], the sensors were grouped based on a physical decomposition of the system. However, the isolability performance of the monitoring scheme was not optimal. In this work, the physical system and its associated sensor set will be decomposed based on the maximisation of the ability to isolate sensor faults. This property can be expressed using the local $F^{(I)}$ and global F^{χ} theoretical fault signature matrices. The challenging part of the distributed architecture is the decision complexity introduced by the combinatorial decision logic. The fault signature of two faults might be the same in one FSM but different in another one, so these two faults can be isolated from one another. Moreover, sensor faults can be propagated between different local agents through their interconnections and multiple decisions are needed to exclude the possibility of certain fault combinations occurring. Thus, a different formulation of the sensor set decomposition problem is required to handle the challenges of the distributed monitoring architecture and will be presented next. The diagnostic system designer module presented in this Section is implemented as an additional utility of the semantic database. As a result, this tool can benefit from the semantic information (see Section 3.7) regarding the hardware sensors ($\mathcal{F}_s$), the virtual sensors ($\mathcal{F}_v$), the controllers ($\mathcal{F}_c$) and the knowledge graph (G) in order to automatically generate sensor set decompositions and the respective distributed monitoring architectures. (see Figure 6.1). The process of decomposing the original sensor set into subsets occurs offline.

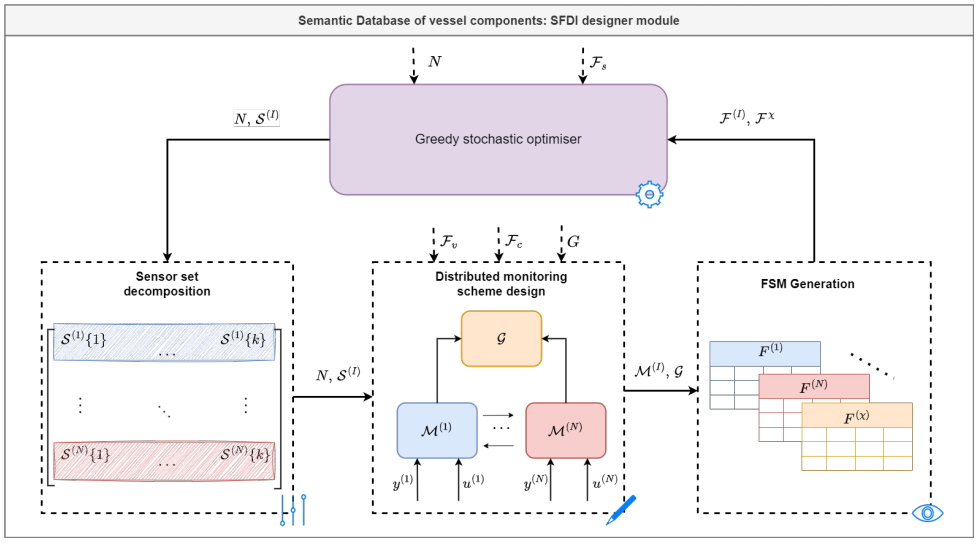


Figure 6.2: The greedy stochastic optimiser determines the composition of sensor sets $\mathcal{S}^{(I)}, I = 1, \cdots, N$ that maximises the isolability targets, as those can be expressed using the theoretical fault signature matrices $(F^{(I)}, F^{\chi})$. The inputs to the greedy stochastic algorithm in each different step are shown with dashed lines. The process described in this figure is implemented as a functionality of the semantic database. As such, the semantic information for hardware $(\mathcal{F}_s)$, virtual sensors $(\mathcal{F}_v)$ and controllers $(\mathcal{F}_c)$ can be used. In addition, the knowledge graph G is available.

6.2.1 Optimisation of sensor monitoring decomposition

The optimisation problem for the sensor fault diagnosis process, in a distributed monitoring architecture, can be expressed as follows:

$$\max_{N,S^{(I)}} \quad \rho\Big(\Phi(F^{(I)})\Big) + \rho\Big(F^{(\chi)}\Big) \tag{6.1}$$

$$\text{s.t.} \quad S^{(I)} \cap S^{(J)} = \emptyset \ \ \forall I \neq J, \tag{6.2}$$

$$\cup_{I=1}^{N} \mathcal{S}^{(I)} \subseteq S, \tag{6.3}$$

$$N \leq N_{max} \tag{6.4}$$

$$\mathcal{S}_R \subseteq \cup_{I=1}^{N} \mathcal{S}^{(I)}, \tag{6.5}$$

where the notation $\rho(A)$ signifies the rank of matrix A and $\Phi : F^{(I)} \mapsto F^{c}$ is a mapping transforming the local fault signature matrices to one equivalent sensor fault signature matrix with the total number of rows and the total number of columns of all local matrices $F^{(I)}$. **The objective function** (6.1) aims to

mathematically express the sensor fault isolability property of the (under design) distributed monitoring architecture in terms of the number of unique columns (or rank) of the matrices $F^{(I)}, F^{\chi}$. **Constraint** (6.2) signifies that each sensor can be assigned to only one monitoring agent, though its measurement may be transmitted between other agents as well. **Constraint** (6.3) is used so that sensors may not be used if they make no difference in the diagnosis process but they are selected from a limited pool of available hardware sensors. To implement the above constraints, the optimizer uses the available semantic information for hardware sensors ($\mathcal{F}_s$) as shown in Figure 6.2.

To implement the above constraints, the optimizer uses the available semantic information for hardware sensors ($\mathcal{F}_s$) as shown in Figure 6.2.

Moreover, **constraint** (6.4) aims to limit the size of the design space by keeping the number of created agents N bounded by a parameter N_{max}. In order to construct residuals in the graphs, the hardware sensor vertices ($\mathcal{F}^s$) belonging to the selected $\mathcal{S}^{(I)}, I = 1, \cdots, N$ need to be combined with similar "virtual sensor" vertices ($\mathcal{F}^v$) (e.g., if the shaft speed sensor is chosen, the virtual sensor for shaft speed needs to be coupled). Since virtual sensors require certain inputs from hardware sensors ($\mathcal{F}_s$) and controllers ($\mathcal{F}_c$) to be functional, **constraint** (6.5) aims to impose the selection of these hardware sensors in the designed division of sensors. The set of virtual sensor requirements $\mathcal{S}_R \subseteq \mathcal{F}_s$ can be defined as the semantic inputs of the virtual sensors and is also used to determine the interconnections between the monitoring agents $\mathcal{M}^{(I)}$ based on the knowledge graph G. Thus, the distributed monitoring architecture is automatically constructed, as shown in Figure 6.2. Finally, using the information about the interconnections between the agents $\mathcal{M}^{(I)}, \mathcal{G}$ and considering that each monitoring module $\mathcal{M}^{(I,q)}$ only employs one *ARR* (i.e., the number of modules of each agent $I \in [1, N]$ are $q = 1, \cdots, |\mathcal{S}^{(I)}|$), the local and global FSMs $F^{(I)}, F^{\chi}$ are also automatically generated.

6.2.2 Greedy stochastic optimisation algorithm

A heuristic search algorithm that can be used to solve the optimisation problem formulated in (6.1)-(6.5) is a greedy algorithm. This type of heuristic has been already used with success for a similar problem in [Jung et al. (2020)], proving a suitable candidate for our problem. However, the main issue associated with greedy algorithms is that they are deterministic and the solution greatly depends on the initial conditions of the search. As a result, the solution provided by the algorithm may be far from the global optimum. In order to mitigate this risk, in this research work, a greedy stochastic algorithm is used instead. The algorithm tunes the number of sensor subsets $\mathcal{S}^{(I)}$ ($\subseteq \mathcal{S} \subset \mathcal{F}_s$) and their hardware sensor composition, thus generating

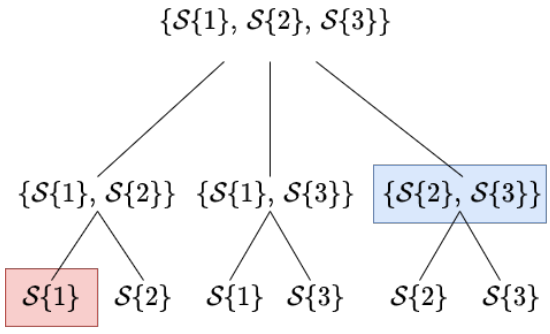


Figure 6.3: Lattice representation of the search space considering a sensor set $\mathcal{S} \in \mathcal{F}_s$ of three hardware sensors. An example of a sensor division (not necessarily optimal) between two monitoring agents that respects the constraints (6.2)-(6.5) *is also shown. The sensor sets $\mathcal{S}^{(I)}$, $I = 1, 2$ are shown with red and blue color boxes.*

different distributed monitoring architectures. The local and the global FSMs, $F^{(I)}$ and $F^{\mathcal{X}}$, are then derived and used for the calculation of the objective function in (6.1). The algorithm is repeated until convergence, as indicated in Fig. 6.2. In order to represent the search space of all possible sensor divisions in a structured manner, a lattice representation is used, such as the one shown in Figure 6.3. In every run of the algorithm, each monitoring agent is first assigned randomly a branch of the lattice tree, satisfying the constraints (6.2)-(6.5), similar to [Jung et al. (2020)]. The monitoring agents then sequentially make decisions on whether to drop, add, exchange a hardware sensor with another agent or do nothing. The objective of each agent at its decision step is the maximisation of the objective function in (6.1), considering the decisions of the previous agents and supposing that the following agents will opt to maintain their sensor sets as is [Konda et al. (2022)]. In order to assess the gains of the different options, 5 random removals, additions and exchanges of sensors are considered. The execution of the algorithm stops when all monitoring agents opt to maintain their sensor set division. The main improvements of our algorithm compared to the relevant literature [Jung et al. (2020)] are **(a)** its suitability for highly complex systems by combining quantitative and qualitative tools; and **(b)** the consideration of distributed monitoring architectures and associated challenges.

6.3 Simulation results

In this section we apply the diagnostic system designer module to a hybrid marine propulsion system, such as the one shown in Figure 3.3. The system is described

Algorithm 6.1 Sensor set decomposition algorithm using a greedy stochastic optimiser approach for distributed monitoring architectures (see Figure 6.2)

Input: $\mathcal{F}_s$, $\mathcal{F}_v$, G, N, total-runs
Output: $\mathcal{S}_{opt}^{(I)}$, F^{χ}, $F^{(I)}$, $\mathcal{M}^{(I)}$

Generate **Lattice** from F_s
for *run* = 1 : total-runs **do**
  $\mathcal{S}_0 \leftarrow$ Select N random valid subsets from Lattice
  Couple hardware ($\mathcal{S}_0$) and virtual sensors to generate **residuals**
  Generate the distributed monitoring scheme based on the residuals with local agents $\mathcal{M}^{(I)}$, $I = 1, \cdots, N$, each corresponding to the set $\mathcal{S}^{(I)}$, and the global agent $\mathcal{G}$
  Evaluate FSMs $F^{(I)}$, F^{χ} based on the knowledge graph G and the agent configuration $(\mathcal{M}^{(I)}, \mathcal{G})$
  $cost0 \leftarrow \rho\left(\Phi(F^{(I)})\right) + \rho\left(F^{(\chi)}\right)$ ▷ Eq. (6.1)
  $n \leftarrow 0$ ▷ Consensus metric
  while $n < N$ **do** ▷ Termination condition
    $n \leftarrow 0$
    for $I = 1 : N$ **do** ▷ Sequential agent decisions
      Determine valid potential additions, removals and exchanges in $\mathcal{S}_0^{(I)}$, based on (6.2)-(6.5)
      Determine $F^{(I)}$, F^{χ} for 5 random valid additions, removals and exchanges in $\mathcal{S}_0^{(I)}$ and evaluate the cost function (6.1)
      Store the sensor division $\mathcal{S}^{(I)}$ with the maximum **cost** value
      Update the distributed monitoring architecture $(\mathcal{M}^{(I)}, \mathcal{G})$ based on the updated $\mathcal{S}^{(I)}$
      if $cost = cost0$ **then**
        $n \leftarrow n + 1$
      end if
      if $cost \geq cost0$ **then**
        $\mathcal{S}_0^{(I)} \leftarrow \mathcal{S}^{(I)}$
        $cost0 \leftarrow cost$
      end if
    end for
  end while
end for

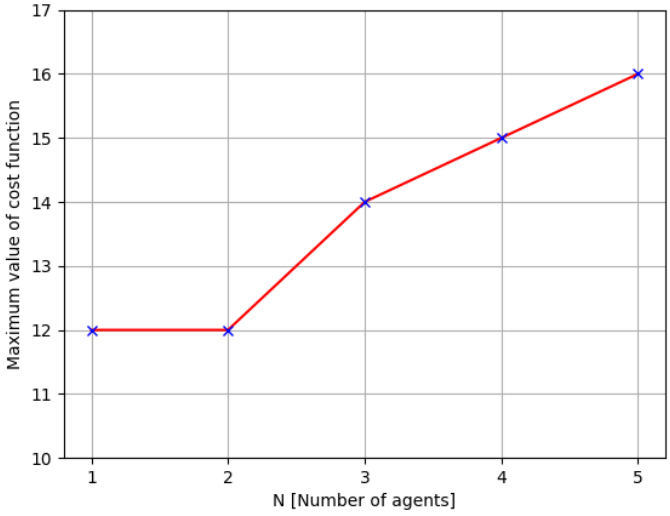


Figure 6.4: Depiction of optimal solution costs (shown in the y axis) per each value of N. The data points are shown with a blue x marker.

using semantic (qualitative) information such as the one discussed in Chapter 3. In total, 12 hardware sensors and 13 virtual sensors are available. For brevity purposes the sensors will be referred to using their IDs in the Semantic Database, shown in Table 6.1. In order to assess the optimal number of monitoring agents, the greedy stochastic algorithm is executed for $N \in \{1,2,3,4,5\}$. The optimal sensor set division per each number of agents N is defined as the one with the maximum cost value defined in (6.1) after running the algorithm 30 times. The implementation of the Algorithm is done in Python 3.9.

Table 6.1: Sensor IDs as vertices in the semantic database

ID	Sensor	ID	Sensor
18	Fuel injection	24	Turbine temperature
19	Cylinder pressure	25	Compressor pressure
20	Cylinder temperature	26	Compressor temperature
21	Engine torque	27	Intercooler temperature
22	Exh. manifold pressure	28	Shaft speed
23	Exh. manifold temperature	29	Motor torque

The results of the greedy stochastic optimisation algorithm are shown in Figure 6.4. In each run, the algorithm starts from a random sensor division with length

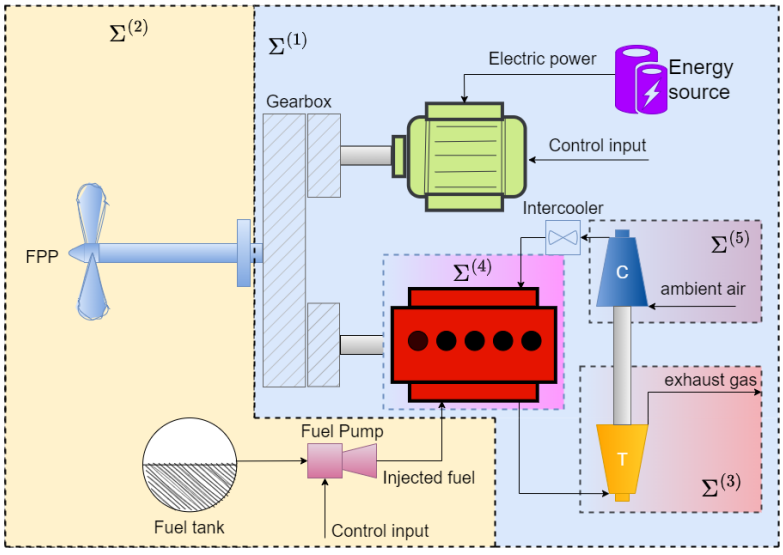


Figure 6.5: Marine hybrid propulsion system physical decomposition based on the optimisation of the sensor fault diagnosis. The 5 subsystems are shown with different colors. The subsystems $\Sigma^{(3)}$, $\Sigma^{(4)}$, $\Sigma^{(5)}$ are overlapping with subsystem $\Sigma^{(1)}$. For each subsystem $\Sigma^{(I)}$, $I = 1, 2, \cdots, 5$ a monitoring agent $\mathcal{M}^{(I)}$ is created.

equal to the number of monitoring agents. Lines 4-24 of Algorithm 6.1 are then executed until convergence to an optimal sensor set division. The solutions from each run are then collected and compared based on their achieved cost value. The blue points in Figure 6.4 then correspond to the maximum value of cost, meaning the maximum number of unique columns in the FSMs achieved by the integrated optimisation problem combining both isolation levels in (6.1), obtained for all the runs in a specified value of N. As observed, the centralised ($N = 1$) and distributed with two monitoring agents ($N = 2$) configurations result in the same maximum cost value. This is due to the high inter-connectivity of the physical system (marine hybrid propulsion system), which in the case of the two-agent configuration results in the monitoring agents being fully connected (the matrix F^{χ} has only one unique column). The cost value significantly increases when considering the $N = 3$ agent configuration while smaller increases are seen when $N = 4$ or $N = 5$. The maximum cost is encountered in the 5-agent distributed configuration. For this specific data point the optimal sensor divisions are the following: $\mathcal{S}^{(1)} = \{19, 20, 21, 23, 25, 27, 29\}$, $\mathcal{S}^{(2)} = \{18, 28\}$, $\mathcal{S}^{(3)} = \{24\}$, $\mathcal{S}^{(4)} = \{22\}$ and $\mathcal{S}^{(5)} = \{26\}$. The virtual sensors are realised in the monitoring agent that their hardware sensor counterpart has been assigned to. Suppose that we want to visualise the optimal sensor set decomposition

for $N = 5$ by extrapolating it as a decomposition of the physical plant shown in Figure 3.3 in multiple systems; the result is shown in Figure 6.5. As observed from Figure 6.5, some systems are overlapping ($\Sigma^{(1)}$, $\Sigma^{(3)}$, $\Sigma^{(4)}$, $\Sigma^{(5)}$) due to their hardware sensors being assigned to multiple non-overlapping sensor sets. Finally, the resulting local FSM for the first monitoring agent $\mathcal{M}^{(1)}$ can be seen in Table 6.2 while the global FSM F^{χ} is given in Table 6.3. In each matrix, every different column represents the theoretical signature of a fault on the sensor ID given in the header of the column. For brevity purposes, only single fault columns are shown. By using virtual sensors, the sensitivity of the resulting analytical redundancy relations is the same both for local and propagated sensor faults. As a result, no ambiguity is taken into consideration in the FSMs, as opposed to [Kougiatsos et al. (2023)].

Table 6.2: Part of the Sensor Fault signature matrix $F^{(1)}$ of $\mathcal{M}^{(1)}$

	18	19	20	21	22	23	24	25	26	27	29
$\mathcal{E}^{(1,1)}$	0	1	0	0	0	0	0	0	0	0	0
$\mathcal{E}^{(1,2)}$	0	1	1	0	0	0	0	0	1	1	1
$\mathcal{E}^{(1,3)}$	0	1	0	1	0	0	0	0	1	1	1
$\mathcal{E}^{(1,4)}$	0	1	1	1	0	1	1	0	1	1	1
$\mathcal{E}^{(1,5)}$	0	0	0	0	0	1	1	1	0	0	0
$\mathcal{E}^{(1,6)}$	0	0	0	0	0	0	0	0	0	1	0
$\mathcal{E}^{(1,7)}$	1	0	0	0	1	0	0	0	0	0	1

Table 6.3: Part of the Global Fault signature matrix of F^{χ} for a 5 agent distributed configuration

	18	19	20	21	22	23	24	25	26	27	29
$\mathcal{M}^{(1)}$	0	1	0	0	0	1	1	0	1	1	1
$\mathcal{M}^{(2)}$	1	1	1	1	1	1	1	1	1	1	1
$\mathcal{M}^{(3)}$	0	1	1	1	0	1	1	0	1	1	1
$\mathcal{M}^{(4)}$	0	1	0	0	1	0	0	0	1	1	1
$\mathcal{M}^{(5)}$	1	1	0	0	0	1	1	1	1	1	1

Based on the above results, a larger number N of decompositions of the sensor set $\mathcal{S}$ in $\mathcal{S}^{(I)}$, $I = 1, \cdots, N$ with an equally large amount of monitoring agents $\mathcal{M}^{(I)}$ seems to result in more isolable columns in the FSMs, at the cost of greater communication needed between the monitoring agents. Based on the automatically generated FSMs shown in Tables 6.2 and 6.3, we can see a large number of unique fault signatures. In particular, **9 out 11** unique columns are observed in Table 6.2 and **5 out of 11** in Table 6.3 considering the single faults case. Nonetheless, based

on the global FSM in Table 6.3, the monitoring agents are very interconnected with **4 out of 11** faults affecting all 5 monitoring agents, **6 out of 11** faults affecting at least three agents and at all cases of faults **(11 out of 11)** affecting at least two monitoring agents. Moreover, although the sensor sets are not overlapping by design (due to constraint (6.2)), if we choose to decompose the system based on the sensor set division, the resulting systems might be overlapping, as shown in Figure 6.5.

6.4 Conclusions

In this chapter, a distributed diagnostic system designer module was developed for the sensor set decomposition problem encountered in the distributed monitoring of marine hybrid propulsion architectures. This contributes to answering the following research question (**Q5:**) *"How to optimise the fault diagnosis capabilities and the required hardware redundancy for safe operation of marine* PPP*s?"*.

Due to its inherent modelling complexity, the propulsion system was modelled using a qualitative approach, based on semantic information about its components and a knowledge graph to visualise their interconnections. The problem was then expressed in sensor fault isolability terms and a greedy stochastic optimiser was proposed for its solution. The obtained results from the case study indicated the efficiency of the algorithm, provided valuable insights on the optimal sensor set decomposition and highlighted the feature of automatically constructing the binary FSMs (quantitative) using the semantics (qualitative) modelling method.

Chapter 7, like Chapter 5, again deals with resilient control. To this end, semantic models are again used, alongside their quantitative counterparts, to allow for the connection of the topology and control design aspects of marine vessels.

Chapter 7

Resilient control for mission-adaptive marine power and propulsion plants

In the previous chapters, sensor faults were considered as an adaptation driver, with a diagnosis approach presented in Chapters 4 and 6 and a fault-resilient control architecture discussed in Chapter 5. However, changes in mission characteristics were not considered as an adaptation driver.

This chapter addresses the research question (**Q6:**) *"How to design a resilient control scheme to facilitate the adaptation of the power and propulsion systems to changes in operational requirements?"*. It is structured as follows. Section 7.2 presents the overall proposed framework that integrates the topology and control system design perspectives, with the details of the designed automation supervisor discussed in Section 7.3. Section 7.4 discusses the mission adaptable marine *PPP* coupled with a modular control system. The proposed framework is applied to a tugboat case study facing different missions in Section 7.5, followed by concluding remarks in Section 7.6.

The contents of this chapter have been published in two conference (van Benten et al., 2022; Kougiatsos et al., 2023)[1][2] and one journal (Kougiatsos et al., 2024a)[3].

[1]M. C. van Benten, **N. Kougiatsos**, and V. Reppa. "Mission-oriented Modular Control of Retrofittable Marine Power Plants." in: Proceedings of the 2022 International Ship Control Systems Symposium, Delft, the Netherlands. Vol. 16. 2022.

[2]**N. Kougiatsos**, J. Zwaginga, J. Pruyn, and V. Reppa, "Semantically enhanced system and automation design of complex marine vessels," in: Proceedings of the 2023 IEEE Symposium Series on Computational Intelligence, Mexico City, Mexico, pp. 512-518, 2023.

[3]**N. Kougiatsos**, E.L Scheffers, M.C. van Benten, D.L. Schott, P. de Vos, R.R. Negenborn, and V. Reppa, "An intelligent agent-based resilient framework for marine vessel mission adaptations," submitted to a journal, 21 pp., 2024.

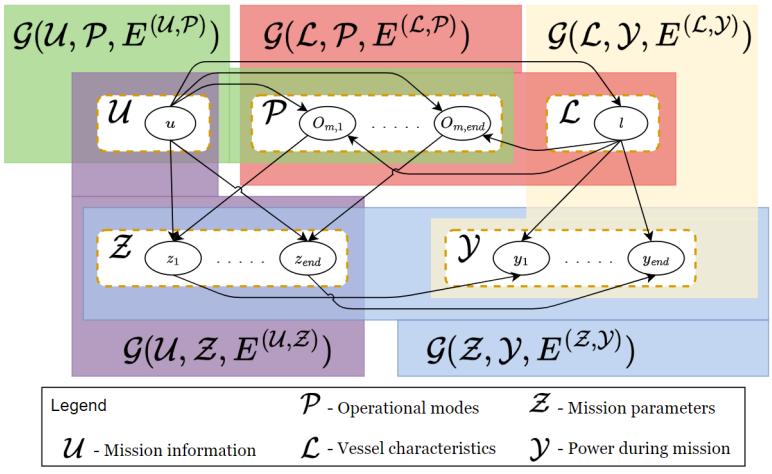


Figure 7.1: Graph depiction of the relations between the set of inputs from the mission definition 7.1 ($\mathcal{U}$), the vessel characteristics (features of interest $\mathcal{L}$ and capabilities P), the extracted mission characteristics $\mathcal{Z} = \{S_m, O_e, V_{O_m}, \nabla\}$ and the power demand output $\mathcal{Y} = \{P_D, P_{aux}, P_{tot}\}$.

7.1 Correlation between mission, power profile and design adaptations

In most marine vessel types found in practice the time scale needed for *PPP* component adaptations, and by association automation adaptations, is considered large. For that reason, most relevant papers in literature only consider a specific system layout when designing the automation systems. However, there are types of marine vessels for which the design of the *PPP* needs to be frequently adjusted to accommodate different missions (e.g., dredgers, patrol vessels). Let us define X as the cargo/passengers/vessel in need of transportation, and A, B, C, $D \in \mathbb{R}^2$ as the coordinates (i.e., [latitude,longitude]) of the locations visited. In this work, we define the mission as:

Definition 7.1 Mission
Transport X from A to B (optionally via C, D, etc.), leaving at t_0 (time and date), arriving at t_{end} (time and date). □

The correlation between the mission, the power profile and the required adaptations is depicted in Figure 7.1. Based on Definition 7.1, the input vector is expressed as $\mathcal{U} = \{X, A, B, t_0, t_{end}\}$. Using this vector, the type of vessel X_v (e.g., tugboat, Ro/Ro ferry) and the vessel characteristics such as the proportionality between the vessel speed and required power a, propeller diameter D, fouling f_h, torque coeffi-

cient K_Q, thrust coefficient K_T , and propulsive efficiency η_D can be derived. We refer to these characteristics as the features of interest $\mathcal{L} = \{X_v, a, D, f_h, K_Q, K_T, \eta_D\}$. The operational modes O_m of the vessel characterized by the set $\mathcal{L}$ and selected to meet the inputs from the mission $\mathcal{U}$ comprise the capabilities of the vessel $\mathcal{P} = \{O_{m,1}, O_{m,2}, \cdots, O_{m,end}\}$ where, for each $O_{m,i}$, the indices $i = 1, \cdots, end$ correspond to various time points $t_i \in [t_0, t_{end}]$ during the vessel's mission. Moreover, based on the input vector $\mathcal{U}$ and the capabilities of the vessel $\mathcal{P}$, the set of mission parameters $\mathcal{Z} = \{S_m, O_e, V_{0_m}, \nabla\}$ can be derived where S_m denotes the travel route , O_e are the parameters of the operational environment (waves s_s, currents c_s, wind w_s, ambient temperature T_a, water depth h, and waterway width w_w), V_{0_m} is the speed of the vessel during each operational mode O_m, and ∇ signifies the displacement of the vessel. Finally, the information from the features of interest $\mathcal{L}$ and the mission parameters $\mathcal{Z}$ is used to predict the power requirements of the vessel in propulsion (P_D), auxiliary (P_{aux}) and total power (P_{tot}), also denoted as the output vector $\mathcal{Y}$. The above defined sets and their relations are depicted in Figure 7.1 while the resulting equations of the power profile (P_D, P_{aux} and P_{tot}) are expressed as (van Benten et al. (2022)):

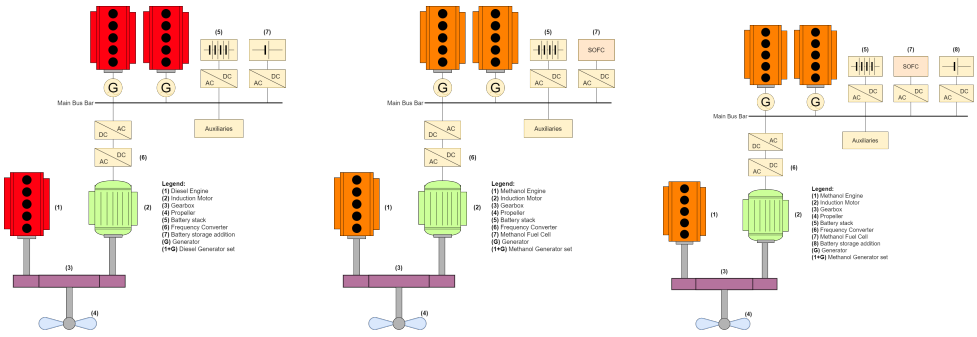
$$P_{aux}(t) = P_{aux,c}(X_v) + \Delta P_{aux}(O_m, T_a, X_v), \tag{7.1}$$

$$P_D(t) = \frac{f(s_s, w_s, c_s, h_i, w_w, f_h, \nabla) \cdot c \cdot {V_{O_M}}^a}{\eta_D} + |F_{tow}|^{\frac{3}{2}} \frac{2\pi K_Q}{\sqrt{\rho} D K_T^{\frac{3}{2}}}, \tag{7.2}$$

with F_{tow} denoting the towing force consideration in certain vessel types such as tugboats. The total power profile is then expressed as:

$$P_{tot}(t) = P_D(t) + P_{aux}(t), \tag{7.3}$$

Between two different missions (e.g., Mission 1, Mission 2), the difference in the required propulsion (ΔP_D), auxiliary (ΔP_{aux}) and total power (ΔP_{tot}) can be computed. Decisions can then be made on the necessary plant adaptations to adapt a specific vessel from Mission 1 to Mission 2. Nonetheless, considering the various component choices offered by the industry (e.g., batteries, fuel-cells, alternative fuels) to adapt to greater power requirements while making the vessel operation more sustainable, the optimality of the adaptation decision should be examined. Taking into account the different fuel choices, three candidate topology adaptations from the initial design layout seen in Figure 3.5a are considered, and the respective topologies are illustrated in Figure 7.2a-7.2c (Zwaginga &Pruyn (2022)). Candidate topology 1 (Figure 7.2a) assumes that more battery energy storage will be added. Candidate topology 2 (Figure 7.2b) suggests a change from fossil fuels to methanol and the addition of fuel cells aside the available battery storage. Finally, candidate topology 3 (Figure 7.2c) serves as a combination of the previous two candidate topologies.



(a) Candidate topology 1 ($\sigma_d = 1$) *(b) Candidate topology 2 ($\sigma_d = 2$)* *(c) Candidate topology 3 ($\sigma_d = 3$)*

Figure 7.2: Candidate topology alteration choices as a response to higher energy demands of the new mission 2 with (a) suggesting the addition of battery stack to the energy storage, (b) proposing the conversion to methanol and addition of Solid Oxide Fuel Cells (SOFC) to energy storage and (c) combining the conversion to methanol and addition of both battery stacks and fuel cells

The objective of this chapter is to develop a resilient control framework to support seamless design adaptation decisions made by designers and operators during the vessel's life cycle, in response to the change of operation from Mission 1 to Mission 2. From the topology perspective, a decision framework will be proposed based on qualitative graph-based KPIs to decide on the optimal candidate topology (1,2 or 3) to use for Mission 2. The use of an intelligent automation supervisor will also be introduced to enable modularity in the *PPP* control system in line with the updated power requirements. In addition, the intelligent supervisor will be designed to handle the occurrence of multiple sensor faults and Denial-of-Service events that can affect the operation of the marine *PPP*. The general framework we are proposing in this chapter can be seen in Section 7.2.

7.2 Intelligent Topology and Control Design Framework

In this section, an overview of the framework proposed to enable modularity in topology and control of marine vessels is presented. In Figure 7.3 the main human actors are the system designers/ integrators (i.e., marine engineers) and the vessel operators (i.e., crew members, remote control centres). In order to support life cycle seamless adaptation decisions the designer is aware of the initial layout of the *PPP* which translates into the semantic information of the system components, used to form the database $\mathcal{F}_p$, and the semantic information of the installed automation

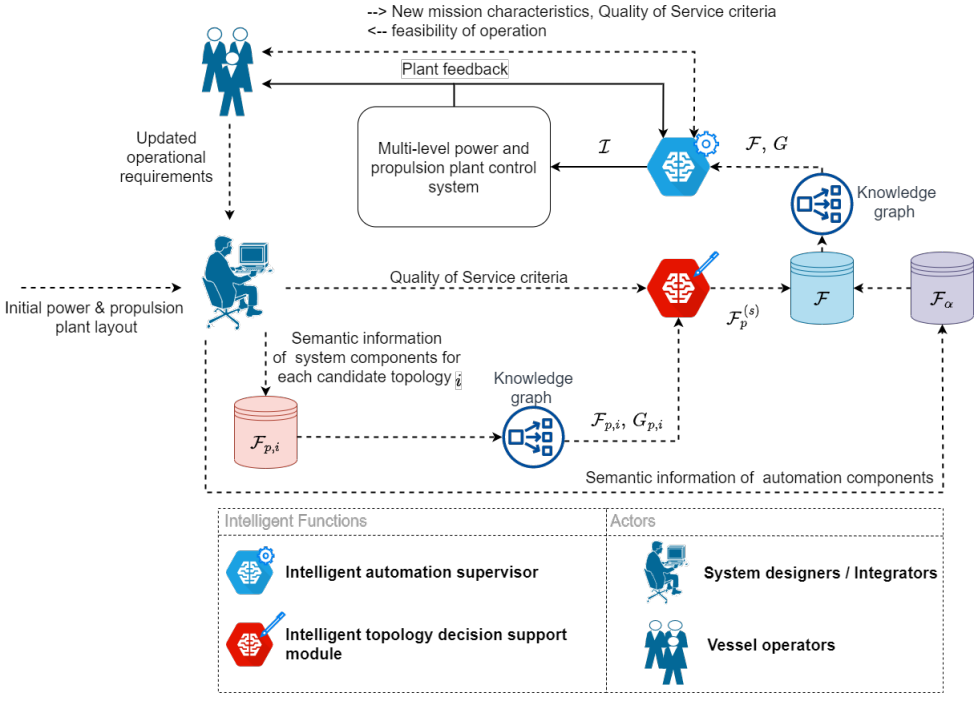


Figure 7.3: Intelligent topology and control design framework for mission-adaptive marine PPP*s. An intelligent automation supervisor is also designed to assist the vessel operators in monitoring the plant feedback, processing the new mission information, assessing the feasibility of handling the mission with the existing equipment and making decision on which energy management strategy and feedback sensors to use for stable operation. The details of the supervisor will be explained in Section 7.3. Continuous lines indicate synchronous/online flow of information during operation while dashed lines indicate asynchronous/offline flow of information.*

components, used to form the database $\mathcal{F}_A$. An automated algorithm to link the components included in the semantic database into knowledge graphs $G_p^{(s)}$ and G is also developed and used to support both topology and automation design decisions. The term knowledge graph will hereby refer to graphs automatically constructed using the knowledge available in the semantic database. During the vessel's life cycle, information of the mission characteristics is collected by an intelligent automation supervisor whose task is, in combination with the received plant feedback (e.g., diagnosis sets by monitoring agents, component availability), to make decisions on the secondary level controller to be used and the corrective actions to enforce in case of multiple sensor faults affecting the *PPP* operation. Thus, the intelligent automation supervisor supports the decisions made by the operators either by indicating that the operation for a specific mission is not feasible with the available equipment or by counteracting vulnerabilities such as sensor faults and *DoS* during the vessel operation, in an effort to promote onboard safety. The decision vector of the intelligent supervisor and its mapping to the active configuration $\mathcal{I}$ (output of the intelligent supervisor) will be further analyzed in Section 7.3.

In case the operation is declared infeasible by the intelligent automation supervisor, the operators will proceed to request a design update from the designer as a response to updated operational requirements (e.g., operation in harsh seas). Considering the current situation in emission regulations, technological developments, stock of components and financial targets, the designer decides on certain candidate topology adaptations to satisfy the new operational demand, such as the ones already shown in Figure 7.2. Another intelligent function, denoted as the intelligent topology decision support module, is then designed to assist the designer in choosing the optimal topology alteration, based on the semantic information stored in the system databases $\mathcal{F}_{p,i}$ and a ranking of the resulting graphs $G_{p,i}$, $i \in \{0, \cdots, N_t\}$, where N_t corresponds to the number of candidate topology considerations ($N_t = 3$), using graph complexity and modularity-related KPIs. The decision of the intelligent topology decision support module, denoted by σ_d is the "systems" that will be installed to handle the new mission and its mapping to the selected systems database $\mathcal{F}_p^{(s)}$ (output of the life cycle decision support module) is elaborated in (Kougiatsos et al., 2024a). The complete semantic database $\mathcal{F}$ to be used in the *PPP* operation is then formed and provided as input together with the complete knowledge graph G to the intelligent automation supervisor.

7.3 Intelligent automation supervisor

The decision on the optimal layout alteration σ_d, in terms of resulting "knowledge graph" modularity and complexity, and its mapping to the selected systems database $\mathcal{F}_p^{(s)}$ in (Kougiatsos et al., 2024a) as well as the database of automation components

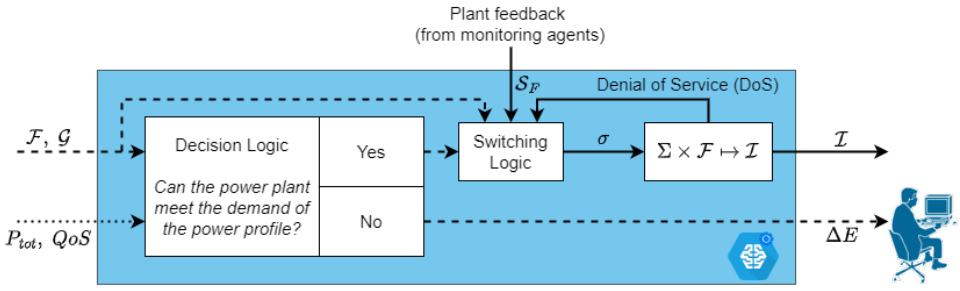


*Figure 7.4: Internal structure of the intelligent automation supervisor. A decision logic is implemented to match the power demand (power profile) with the onboard power supply (*PPP*) and potentially to initialise topology adaptations by the vessel designers. The specifics of the decision logic are provided Algorithm 7.1. A switching logic is then implemented with two degrees of freedom; switching between hardware and virtual sensors and switching between energy management controllers during the plant operation. The specifics of the switching logic are provided in Algorithm 7.2. Continuous lines indicate signals that get updated during operation and dashed lines indicate signals that get updated between missions.*

$\mathcal{F}_A$ are used to produce the semantic database $\mathcal{F}$ according to (3.54). The knowledge graph G corresponding to the multi-level control scheme can also be extracted using Algorithm 3.1. Using the available semantic knowledge, expressed by $\mathcal{F}$, G and the *Quality of Service* (*QoS*) criteria, and the power profile of the mission P_{tot}, defined in (7.3), an intelligent automation supervisor is designed to determine the power deficit needed to execute a new mission (offline calculation) and to switch between operating components in the multi-level control scheme during the *PPP* operation (online mapping). The logic behind the offline and online implementation of the supervisor is shown in Figure 7.4 and further detailed in Algorithms 7.1, 7.2. Section 7.3.1 will elaborate over the decision logic block of the supervisor and Section 7.3.2 will discuss the switching logic block, as seen in Figure 7.4.

7.3.1 Offline decision logic

As indicated in Figure 7.4, the goal of the decision logic block is **(i)** to determine whether the input power profile can be executed with the available power supply systems and **(ii)** otherwise, to determine the current deficit in the required power expressed as $\Delta E = E_{supply} - E_{demand}$, where E_{supply} denotes the available energy using the existing *PPP* topology and sizing and E_{demand} denotes the energy demand as indicated by the power profile. This deficit is then reported to the vessel operators and

used as input by the designers to determine certain candidate topology adaptations.

Algorithm 7.1 Decision logic of the intelligent automation supervisor (offline) drafted in Figure 7.4

Input: $P_{tot}(t)$, QoS, $\mathcal{F}$ ▷ Power profile, qualitative plant model (Chapter 3)
Design parameters: $\alpha \in [0, 1]$ ▷ Target generator sets utilisation factor
Output: ΔE ▷ Deficit in available power

1: $P_{tot}(t) \rightarrow P_D(t) + P_{aux}(t)$ ▷ Split power profile in propulsion and auxiliary power
2: $P_{D,elec}(t) = \frac{P_D(t)}{\eta_T \eta_{EM}}$ ▷ Propulsion power to electric power conversion
3: $P_{elec}(t) = P_{D,elec}(t) + P_{aux}(t)$ ▷ Total power demand of the power profile
4: $P_{ED}(t) = \sum_{i=1}^{I} P_{ED,i}(t)$ ▷ Total power demand of *Induction Motor*s (*IM*s)
5: $P_{GS}(t) = \sum_{n=1}^{J} P_{GS,j}^{opt}(t)$ ▷ Total genset power under optimal operation
6: $P_{demand}(t) = \mathbf{min}(0, \mathbf{max}(P_{elec}(t), P_{ED}(t)) - \alpha \cdot P_{GS}(t))$ ▷ Power for the electric power demand
7: $E_{demand} = \int_{t=0}^{T} P_{demand}(t)$
8: Detemine E_{supply} using the semantic information for the available *PPP* systems $\mathcal{F}$ and their sizing in QoS
9: $\Delta E = E_{supply} - E_{demand}$ ▷ Energy deficit calculation
10: **if** $\Delta E < 0$ **then** ▷ *PPP* can **not** match the desired power profile
11: **Output** $\leftarrow |\Delta E|$
12: **Output** is provided to the operators and then the vessel designers to proceed with topology adaptations.
13: **else**
14: No topology adaptation is needed. **Continue to operation in the specified mission.**
15: **end if**

Due to the hybrid nature of the propulsion system, the total power profile P_{tot} is expected to be served by both mechanical (e.g., *Internal Combustion Engine* (*ICE*)) and electrical (e.g., *Induction Motor* (*IM*), generator sets, batteries) energy systems. In order to make comparisons easier, the power profile is divided in two parts, the required propulsion P_D and auxiliary P_{aux} power profiles in line 1 of Algorithm 7.1 and a total - only electric- power profile is reformed in lines 2 -3. The required energy demand E_{demand} is calculated in lines 4- 7 and is based on a design parameter α, expressing the utilisation factor of the generator sets during operation in the requested power profile. A value of $\alpha = 0$ indicates high energy redundancy and sustainability targets in the design (both generator sets are in reserve) while a value of $\alpha = 1$ leads to less additional energy storage requirements and subsequently less retrofit costs (both generators are expected to be used at their optimal operation

point). Using this and information on the energy supply already present in the vessel topology (P_{supply} specified in the *QoS* criteria), the difference in energy ΔE is calculated in line 9. If $\Delta E < 0$, an energy deficit is indicated and adaptations on the *PPP* are requested by the vessel designers. In any other case, the installed *PPP* is considered sufficient to handle the mission and online operation is resumed. The aforementioned logic can also be seen in Algorithm 7.2.

7.3.2 Online switching logic

During the *PPP* operation, multiple vulnerabilities such as sensor faults or *DoS* events can negatively affect onboard safety. As a result, we design the logic of the intelligent automation supervisor to switch between hardware and virtual sensors, when one or more sensor faults affect the onboard energy storage devices, and between secondary level controllers, when access and control are denied to part of the energy storage. In lines 1-2 of Algorithm 7.2 the number of available batteries is determined using the component database $\mathcal{F}$. Considering that each energy storage device is equipped with one voltage and one current sensor, a switching vector is defined as $\sigma \in \mathbb{Z}_{+}^{2K+1}$, where K is the number of batteries. Using the feedback of the monitoring agents regarding the set of faulty sensors $\mathcal{S}^F$ the switching between hardware voltage and current sensors (index=1) and their virtual counterparts (index=2) is translated to adaptations in the respective elements of the switching vector σ in lines 3-12. The mapping of the switching vector space Σ ($\sigma \in \Sigma$) to the active automation configuration $\mathcal{I}$ using the semantic database $\mathcal{F}$ is attempted in lines 13-15 and is assumed to only be inhibited by *DoS* events. In this case, the supervisor determines the inaccessible part of the *PPP* through the knowledge graph G and updates the choice of secondary level controller in the switching vector σ in lines 16-18. The mapping to the active control configuration is re-attempted until the implementation of the switching decision vector σ is feasible, as is also seen in lines 19-20.

7.4 Multi-level power & propulsion plant control system

Marine vessel control systems are usually composed of two control levels; the primary and secondary control level. In Figure 7.5, a simplified control layout showing the interaction between the two control levels is provided, considering the hybrid *PPP* system architecture shown in Figure 3.5a.

The primary level includes the local controllers for the *ICE*, the *IM*, the generator sets and the batteries. Model-free PI controllers are designed while the batteries are controlled using battery constraint modules (van Benten et al., 2022). For propulsion, a parallel control approach is adopted with torque control designed

Algorithm 7.2 Switching logic of the intelligent automation supervisor (online) drafted in Figure 7.4

Input: $\mathcal{F}$, G, $\mathcal{S}^F$ ▷ semantic database, knowledge graph and faulty sensor set
Output: $\mathcal{I}$ ▷ Active control configuration

1: $K \leftarrow$ number of battery entries in $\mathcal{F}$
2: $\sigma \leftarrow [1_{2K}^{\top}; K]$ ▷ Each battery has one voltage and one current sensor (models in Chapter 3)
3: **for** voltage sensors $\in \mathcal{F}_s$ **do**
4: **if** voltage sensor of battery $\{k\} \in \mathcal{S}^F$ **then** ▷ $k = 1, \cdots, K$
5: $\sigma(2k-1) \leftarrow 2$ ▷ Switch to virtual voltage sensor with index 2
6: **end if**
7: **end for**
8: **for** current sensors $\in \mathcal{F}_s$ **do**
9: **if** current sensor of battery $\{k\} \in \mathcal{S}^F$ **then** ▷ $k = 1, \cdots, K$
10: $\sigma(2k) \leftarrow 2$ ▷ Switch to virtual current sensor with index 2
11: **end if**
12: **end for**
13: **try** ▷ Mapping to the active control configuration
14: $\Sigma \times \mathcal{F} \mapsto \mathcal{I}$ ▷ Σ: vector space of decisions σ
15: **Output**$\leftarrow \mathcal{I}$
16: **except** ▷ Denial-of-Service, mapping not feasible
17: Determine unavailable part of Graph G
18: $\sigma(2K+1) \leftarrow \sigma(2K+1) - 1$
19: **go to step** 13
20: **end try**

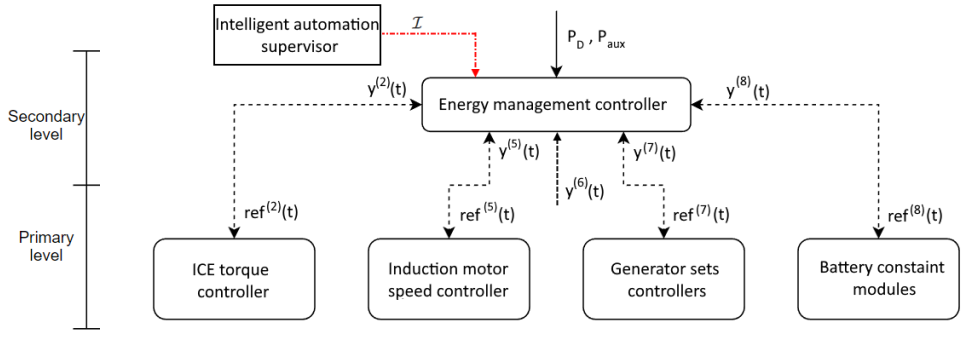


Figure 7.5: Multi-level PPP *control scheme overview*

for the *ICE* and speed control applied to the *IM* (Geertsma et al., 2017b).

In the secondary control level, an energy management controller is designed to handle the power split between the different systems and provide the appropriate reference signals to the primary level controllers, as can be seen in Figure 7.5. The input to this level is the propulsion and auxiliary power demand, as extracted by the power profile.

The intelligent automation supervisor we propose in this work has the ability to switch between different energy management controllers in case of *DoS* events affecting the *PPP* (e.g., a battery is not responding due to an attack or software issue). The relevant decision is included as the last element $\sigma(2K+1)$ of the decision vector of the supervisor and is implemented through the mapping $\Sigma \times \mathcal{F} \mapsto \mathcal{I}$. Finally, the communication from the primary to the secondary control level is enabled using the feedback measurement signals of the active, either hardware or virtual, sensors as these are determined by the switching logic of the intelligent supervisor.

For the sake of brevity, in this work we consider only sensor faults in the energy storage devices. As a result, monitoring agents and virtual sensors are generated only for the energy storage. The reader can find more information on the design of the design of the monitoring agents and virtual sensors in Chapters 4 and 5. Each secondary level controller is composed of an equivalent consumption minimisation problem with cost function and constraints described as follows, in cases only batteries are considered (van Benten et al., 2022):

$$\min\{\dot{m}_{T,K} | \mathcal{I}\}, \tag{7.4}$$

where

$$\begin{aligned}
\dot{m}_{T,K} = {} & a_1^{ICE} \cdot {P_{ICE}}^3 + a_2^{ICE} \cdot {P_{ICE}}^2 + a_3^{ICE} \cdot \omega_{ICE}^2 \cdot P_{ICE} \\
& + a_4^{ICE} \cdot \omega_{ICE} \cdot P_{ICE} + a_5^{ICE} \cdot {P_{ICE}}^2 + a_6^{ICE} \cdot P_{ICE} \cdot \omega_{ICE} \\
& + \underbrace{\sum_{j=1}^{2} \left(a_1^{g,j} \cdot \left(\frac{P_{g,j}}{\eta_{g,j}} \right)^3 + a_2^{g,j} \cdot \left(\frac{P_{g,j}}{\eta_{g,j}} \right)^2 + a_3^{g,j} \cdot \frac{P_{g,j}}{\eta_{g,j}} \right)}_{\text{Fuel consumption rate of fixed plant systems}} \\
& + \underbrace{\sum_{k=1}^{\sigma(2K+1)} \left(SFC^{nom} \cdot \eta_{FC} \cdot \eta_{IM} \cdot {\eta_{b,k}}^{sign(P_{b,k})} \cdot P_{b,k} \right)}_{\text{Fuel consumption rate of adapted systems according to } \mathcal{I}} ,
\end{aligned} \tag{7.5}$$

subject to the following constraints:

$$P_{ICE} \geq \frac{P_D}{\eta_T} - P_{IM,mec}, \tag{7.6}$$

$$\sum_{j=1}^{2} P_{g,j} \geq P_{aux} - \sum_{k=1}^{K} P_{B,k} + \frac{P_{IM,mec}}{\eta_{IM} \cdot \eta_{FC}}, \tag{7.7}$$

$$0 \leq P_{ICE} \leq \bar{P}_i, \tag{7.8}$$

$$0 \leq P_{IM,mec} \leq \bar{P}_m, \tag{7.9}$$

$$0 \leq P_{g,j} \leq \bar{P}_{g,j}, \qquad j \in [1,2], \tag{7.10}$$

$$\underline{P}_{b,k} \leq P_{b,k} \leq \bar{P}_{b,k}, \qquad k \in [1,\cdots,\boldsymbol{\sigma(2K+1)}], \tag{7.11}$$

$$P_{b,k} \geq P_{b,k-1}, \qquad k \in [2,\cdots,\boldsymbol{\sigma(2K+1)}], \tag{7.12}$$

$$P_{b,k} \cdot P_{b,1} \geq 0, \qquad \text{if } \boldsymbol{\sigma(2K+1)} \geq 2. \tag{7.13}$$

The term $\dot{m}_{T,K}$ is the fuel consumption rate for a *PPP* with K batteries in [kg/sec], $P_{ICE}, P_{IM,mec}, P_{g,j}$, and $P_{b,k}$ denote the power split regarding the *ICE*, *IM*, diesel generator set $j \in [1,2]$, and battery $k \in [1,...K]$, respectively, with limits $\bar{P}_i$, $\bar{P}_m$, $\bar{P}_{g,j}$, $\underline{P}_{b,k}$, and $\bar{P}_{b,k}$. Furthermore, a_i^{ICE} for $i \in \{1,2,3,4,5,6\}$, $a_i^{g,j}$ for $i \in \{1,2,3\}$ are constants to characterize the fuel consumption, SFC^{nom} is the nominal *ICE* fuel consumption, $\eta_{b,k}$ is the efficiency of battery k, and $\eta_{g,j}$ the j-th diesel generator set's efficiency. The effect of the active configuration $\mathcal{I}$ on the *Equivalent fuel Consumption Minimisation Strategy* (*ECMS*) controller is highlighted with a bold font. In addition, the intelligent supervisor ensures that only healthy measurements are given as feedback to the secondary level controller as can be seen in Figure 7.5 where the notation $y_H^{(I)}(t)$ is used to denote the healthy measurement of the quantity originally measured by $y^{(I)}(t)$, $I = 1,\cdots,N$.

Using the above optimization problem for the *ECMS*, the power for each component is found, at each moment during the mission. This can be used to derive the following reference signals for the primary level: torque of the *ICE* $ref^{(2)} \in \mathbb{R}$, rotor speed for the *IM* $ref^{(5)} \in \mathbb{R}$, voltage and shaft speed of each diesel generator set $ref_j^{(7)}(t) \in \mathbb{R}^2$, respectively for $j \in \{1, 2\}$, and the reference power of the K batteries, $ref_k^{(8)}(t) \in \mathbb{R}$, respectively for $k \in \{1, \cdots, K\}$. The reference signals are calculated as follows:

$$ref^{(2)}(t) = \frac{P_{ICE}}{ref^{(2)}(t)} \cdot \frac{i_{IM}}{i_{ICE}}, \tag{7.14}$$

$$ref^{(5)}(t) = i_{IM} \cdot \sqrt[3]{\frac{P_D}{c}}, \tag{7.15}$$

$$ref_j^{(7)}(t) = [V_{grid},\ f_{grid} \cdot \frac{4\pi}{p_{g,j}}]^\top,\ j \in \{1, 2\}, \tag{7.16}$$

$$ref_k^{(8)}(t) = P_{b,k},\ k \in \{1, \cdots, K\}, \tag{7.17}$$

where i_{IM} and i_{ICE} the *IM* and diesel engine gear ratios, V_{grid} and f_{grid} the required grid voltage and frequency, and $p_{GS,j}$ the number of poles of generator set j.

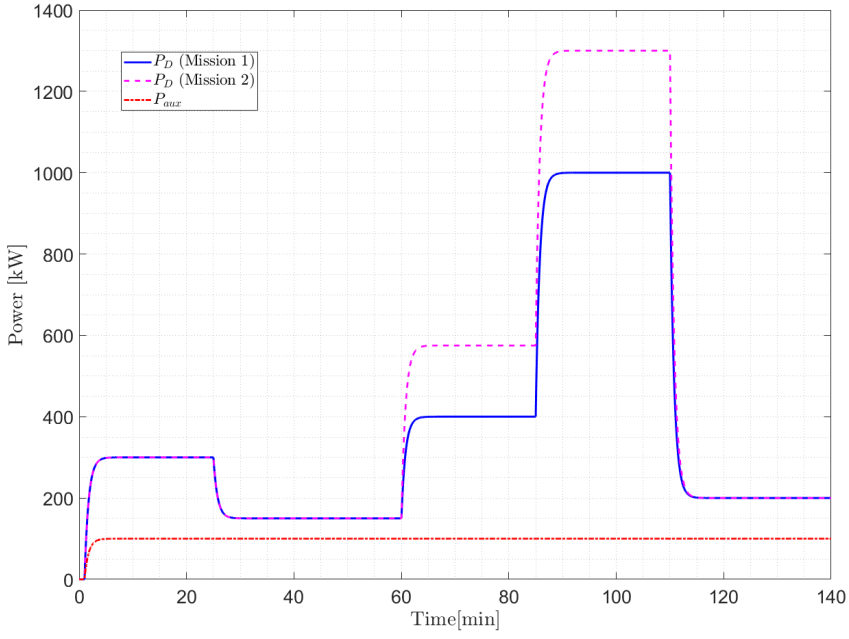
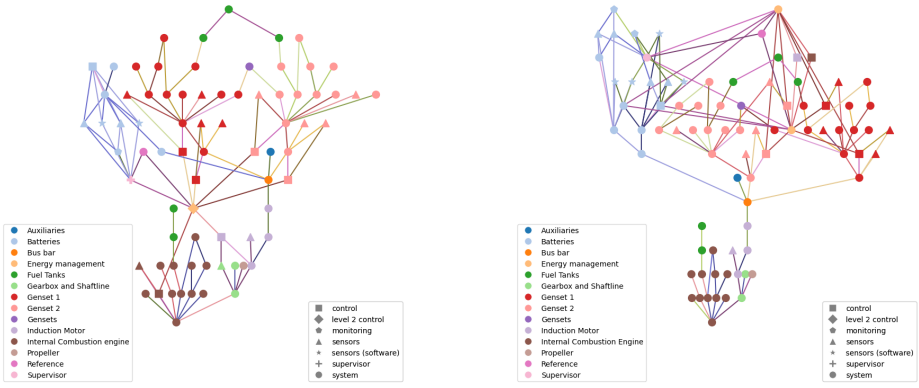


Figure 7.6: Power profiles of two missions with different power requirements

7.5 Case study and simulation results

For illustrating the efficiency of the developed framework to enable modularity in topology and control of marine vessels, we consider a tugboat application on the Smith Elbe vessel (Kalikatzarakis et al. (2018)). A typical mission for a tugboat consists of the following five operational modes: (i) Transit to the arrival location of the cargo vessel to be towed, (ii) remain standby at position until the cargo vessel arrives, (iii) assist-low, (iv) assist-high, in order to guide the cargo vessel into the harbour, and (v) transit back to a specific location in the harbour when finished. For this case study, a baseline mission, Mission 1, with an associated power profile, Power profile 1, is used for the vessel, found in (Yuan et al. (2016)) and shown in Figure 7.6. Based on the power requirements of this power profile (blue continuous and red dash-dotted curves in Figure 7.6), the initial *PPP* layout of the tugboat corresponds to the layout shown in Figure 3.5a with the associated "knowledge graph" as shown in Figure 3.5b.

For Mission 1, the initial multi-level control system is semantically described and incorporates one secondary level controller, the primary level controllers, monitoring agents, hardware and virtual sensors as seen in Figure 7.7a. Now, let's suppose that due to having a larger cargo vessel to assist and high demand for tugboats



(a) *(b)*

Figure 7.7: Complete knowledge graphs G including both the system and automation vertices V and edges E for (a) the initial PPP *layout and (b) the selected* PPP *topology using additional battery storage ($\sigma_d = 1$). The different colours of edges indicate the use of different mediums* Υ.

in port at a specific time period, the required propulsion power P_D increases. Using (7.2), the new propulsion power profile for Mission 2 can be estimated, resulting in Figure 7.6 with a magenta dashed line. For the sake of simplicity, we assume that the power demand for auxiliary power P_{aux} remains the same for the two missions. Using the decision logic of the intelligent automation supervisor between the two missions (Algorithm 7.1) with $\alpha = 0.5$ (only one generator set would be in use), it is deduced that the current *PPP* has a power deficit of $\Delta E = -1080\ MJ$ and as a result the topology of the *PPP* needs to be modified to handle Mission 2. From the analysis of the graphs related to the candidate topologies (Figures 7.2a-7.2c), the candidate topology with the highest modularity and lowest increase in complexity compared to the base knowledge graph is $\sigma_d = 1$ (battery addition).

After deciding on the optimal topology adaptation, the semantic database is updated with the additional automation components. More precisely, an additional energy management controller ($K = 2$) is designed to be able to utilise both the original ($\Sigma^{(5)}$) and the additional ($\Sigma^{(6)}$) energy storage. The original secondary level controller ($K = 1$) also remains available as part of the semantic database in case *DoS* events affect part of the energy storage. In addition, the monitoring system is enhanced with the addition of an agent monitoring the health of the sensors included with the additional battery stack. The complete knowledge graph accounting for both system and automation components is shown in Figure 7.7b.

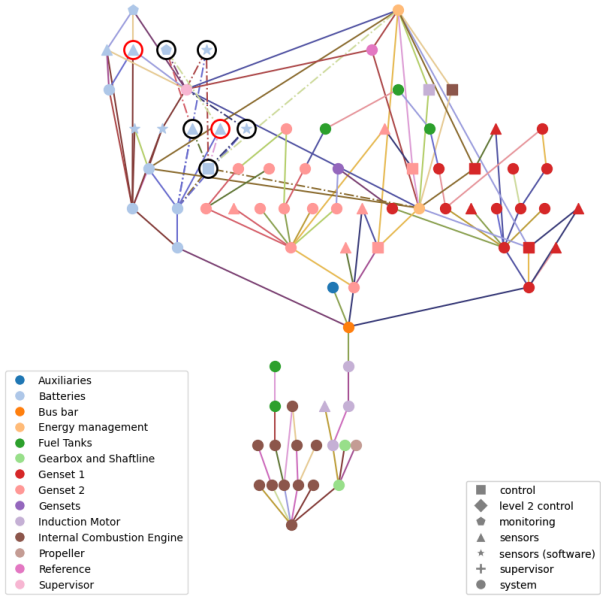


Figure 7.8: Simulation scenario representation with indicated vulnerabilities affecting the PPP *using the knowledge graph in Figure 7.7b. The hardware sensor vertices affected by faults are highlighted with a red encompassing circle and the vertices under Denial-of-Service are highlighted with a black encompassing circle and dash-dotted connection edges.*

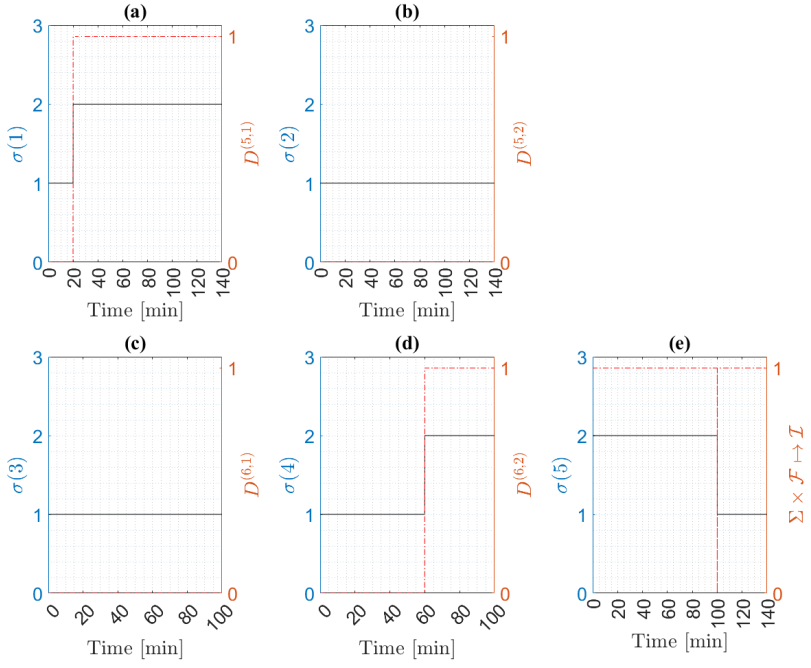


Figure 7.9: Switching vector σ components for power profile 2 under the specified anomaly scenario. The decisions of the monitoring agents regarding sensor faults shown as a red dash-dotted line in subfigures (a)-(d) activates the switching from hardware sensors with index 1 to virtual sensors with index 2 as can be seen with the black continuous lines on the same subfigures. Due to the DoS *event of the added energy storage, the supervisor switches the secondary level controller to utilise only the available energy storage as can be seen by the switching component $\sigma^{(5)}$ in Figure (e)*

For the simulation scenario in Mission 2 we consider that the *PPP* is affected by two sensor faults, occurring at $T_{f1}^{(5)} = 20\ min$ and $T_{f2}^{(6)} = 60\ min$ in the current sensor $\mathcal{S}^{(5)}\{1\}$ of the first battery and the voltage sensor $\mathcal{S}^{(6)}\{2\}$ of the second battery with magnitudes of $f_1^{(5)} = -60\ A$ and $f_2^{(5)} = 40\ V$ accordingly. Moreover, at $T_{DoS}^{(6)} = 100\ min$ battery 2 can no longer be reached due to a *DoS*. The illustration of the simulation scenario with reference to the knowledge graph is shown in Figure 7.8. In order to simulate the behavior of the marine *PPP* under the aforementioned conditions, the models described in Chapter 3 are used. The simulation results for the specified scenario are shown in Figures 7.9-7.10.

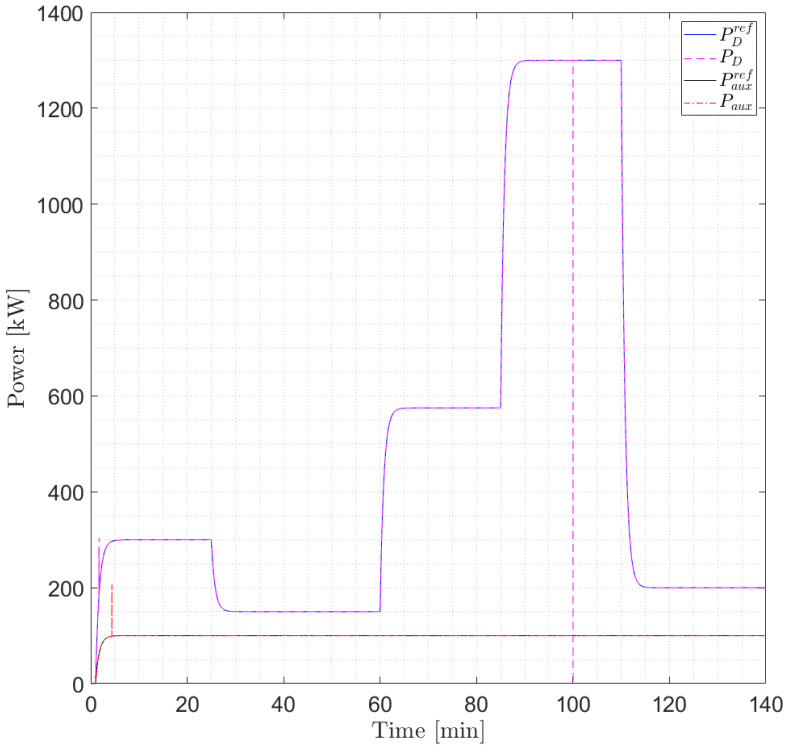
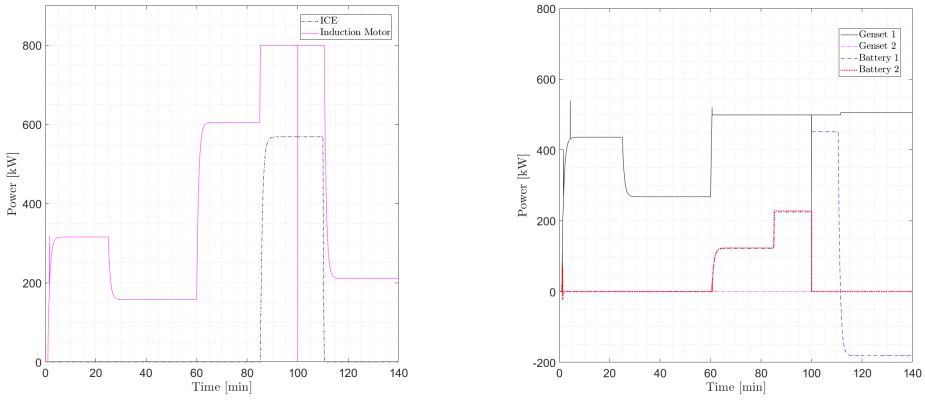


Figure 7.10: Reference and achieved power profile using the base PPP *layout and* ECMS *for K=2 batteries. The reference signals for the secondary level, regarding the required propulsion P_D and auxiliary P_{aux} power are shown with continuous lines. Dashed lines showcase the performance of the multi-level control system to track power profile 2.*

The switching vector σ, derived using the switching logic of the intelligent automation supervisor (Algorithm 7.2), can be seen in Figure 7.9. Since only sensor faults in the onboard batteries are considered and the number of batteries is $K = 2$, the switching vector σ is composed of 5 $(2K + 1)$ elements. The decision on which battery current sensor to use (hardware or virtual) is contained in $\sigma(1)$ for Battery 1 and $\sigma(3)$ for Battery 2. In a similar manner, $\sigma(2)$ and $\sigma(4)$ store the decision on which battery voltage sensor to use for Battery 1 and Battery 2, respectively. Finally, $\sigma(5)$ stores the decision regarding the secondary level controller to use.

As seen from Figures 7.9(a), (d) the two simulated faults are almost instantly diagnosed after their occurrence using the designed monitoring agents. The reader is encouraged to find more details and performance analysis characteristics for this



(a) *(b)*

Figure 7.11: (a) Split of the required propulsion power into equivalent loadings of the ICE *(black dashed line) and the* IM *(magenta continuous line), (b) Split of the required power on equivalent loadings of generator sets (black continuous and magenta dash-dotted lines) and the onboard battery stack (blue dashed and red dotted lines).*

design in Chapter 4. At the same time, the respective element, $\sigma(1)$ or $\sigma(4)$, of the switching vector changes from '1' to '2' indicating the switching between the "hardware" and "virtual" sensors. Since no sensor faults are detected in sensors $\mathcal{S}^{(5)}\{2\}$ and $\mathcal{S}^{(6)}\{1\}$, the vector elements $\sigma(2)$ and $\sigma(3)$ remain the same and equal to '1' indicating the use of hardware sensors, as shown in Figures 7.9(b), (c). Finally, aside from the monitoring agents, the feasibility of the mapping operation $\Sigma \times \mathcal{F} \mapsto \mathcal{I}$ can alter the switching vector by switching between energy management controllers and rerouting the power split. This can be seen in Figure 7.9(e) where, for the sake of notation, the feasibility of the mapping takes the value '1' when applicable and '0' otherwise. At $t = 100$ *min*, the *DoS* takes place and element $\sigma(5)$ changes from $K = 2$ to $K = 1$ so that only one battery can still be used.

Figure 7.10 shows the tracking performance of the power profile using the proposed multi-level control scheme and the switching logic of the intelligent automation supervisor. Aside from the transient behavior encountered for $t \leq 10$ *min* and the rerouting of power at $t = 100$ *min* due to the *DoS*, the *PPP* manages to follow very closely the power profile. In particular, the normalised root mean square error (RMSE) between the power profile and the power output is used as the main *Key Performance Indicator* (*KPI*). For propulsion, an RMSE of 2% is attained while the RMSE for the auxiliary power corresponds to 1.82%. Finally, Figures 7.11a,7.11b show the power split found as the solution of the *ECMS* formulated problem previ-

ously explained in Section 7.4. It can be seen from Figure 7.11a that throughout the mission, mostly the *IM* is used while the *ICE* is activated only during the peak of the power profile (90 $min \leq t \leq 110$ *min*), thus promoting sustainability. The switching of the secondary level controller affects the split to the *IM* since this is connected to the available energy storage. The power split between the generator sets and the batteries is then shown in Figure 7.11b. The first generator set supplies most of the power throughout the vessel mission (black continuous line in Figure 7.11b) with the two batteries activated at higher power loads occurring from $t \geq 60$ *min* in the power profile for mission 2 shown in Figure 7.6. The *DoS* affecting battery 2 from $t \geq 100$ *min* leads to controller switching and battery 2 not being in use after that moment (red dash-dotted line in Figure 7.11b. Subsequently, battery one assumes a higher load (blue dashed line in Figure 7.11b) until the power demand decreases at $t \geq 110$ *min* and battery charging is preferred, as indicated by the negative sign of the battery power. Generator 2 in this case ($\alpha = 0.5$) indeed remains inactive during the whole mission, further advocating for increased sustainability in the *PPP* operation under the implemented topology and control adaptations.

7.6 Conclusions

In this chapter, an intelligent framework for human decision support in mission adaptable marine *PPP*s' design was proposed. In doing so, the following research question was addressed (**Q6:**) *"How to design a resilient control scheme to facilitate the adaptation of the power and propulsion systems to changes in operational requirements?"*.

The connection between adaptations in topology and control was rendered possible through the use of a qualitative knowledge-representation technique based on semantics. Then, two intelligent modules were designed to assist both the vessel designers and the operators. First, an intelligent decision support module was designed to select the optimal *PPP* layout adaptations when the power requirements for the mission change. Second, an intelligent supervisor was developed to execute the following tasks; decide whether the power profile can be executed with the available equipment or not, and to switch between (a) hardware and virtual sensors or (b) between secondary level controllers, in case a combination of multiple sensor faults and *DoS* events is detected. The results from the tugboat case study demonstrate that the intelligent framework successfully manages to promote safety and robustness in the marine *PPP*, by tracking the power profile with minimal errors.

The next chapter summarizes the results of Chapters 2-7 in order to answer the research questions formulated in Chapter 1. Future potential research directions are also proposed.

Chapter 8

Conclusions and Future Research

In this thesis we investigated safe and resilient control strategies for marine *Power and Propulsion Plant*s (*PPP*s). This last chapter concludes the thesis by addressing the overall research question (**Q:**) *"How to design safe and resilient autonomous control systems to handle the uncertain future adaptations in vessel automation and to compensate for malfunction effects without human intervention?"*. This Chapter is structured as follows. Section 8.1 collects the answers to the research subquestions defined in Chapter 1, and provides the answer to the main research question. Potential directions for future research are then discussed in Section 8.2

8.1 Conclusions

This section summarizes the main research findings and concludes this thesis. To this end, the six sub-research questions identified in Chapter 1 are answered below.

Q1: *What are the state of the art, state of practice and research gaps regarding the monitoring and resilient control of marine power and propulsion plants?*

Regarding the monitoring of marine *PPP*s, it was found in Chapter 2 that mostly centralised monitoring approaches have been discussed so far in marine literature, while the performance analysis of the proposed monitoring schemes have been omitted. Moreover, the thresholds used as part of the monitoring process are usually fixed and arbitrarily set, thus not guaranteeing minimal false alarms and missed detections. From the different types of vulnerabilities, sensor faults and cyberattack scenarios have been overlooked. The state of practice considers multiple sensors for monitoring and control purposes relying though on hardware redundancy.

Resilient control of marine *PPP*s is also a rising topic in literature. The majority of relevant papers in the literature considers a single level of control (either primary or secondary), despite multiple levels being involved in the control of marine *PPP*s. In the primary level, either a decentralised or centralised control agent architecture is followed, using a model-free agent design. In the secondary level case, a centralised control agent is designed with an objective to either minimize the fuel consumption or maximize the energy performance. However, in most cases, the secondary level control agent design is based on a fixed *PPP* topology. Considering resilient control, mostly malfunctions (e.g., faults, attacks) and mission changes are discussed as an adaptation driver, potentially due to the short and medium time horizon they take place in respectively (see Figure 2.3). Nonetheless, control adaptations due to more than one adaptation drivers concerning a multi-level control scheme have been so far mostly overlooked. Finally, both accommodation and reconfiguration strategies are discussed, though commonly based on hardware redundancy.

Q2: *How to derive models of marine power and propulsion systems for monitoring and resilient control purposes?*

An abundance of quantitative models for the most common vessel power and propulsion systems is available in literature (e.g., Hansen et al. (2013)). In most cases these models follow a *DAE* representation, and are thus associated with high non-linearity and complexity (e.g., interconnections, heterogeneous systems). In order to handle this complexity, Chapter 3 discussed complementary qualitative models based on semantics. The use of both qualitative and quantitative models was proven capable of enabling the development of monitoring and resilient control approaches in Chapters 4-7.

Q3: *How to design and verify the performance of a sensor fault diagnosis architecture for marine propulsion systems?*

Considering the *DAE* representation commonly used for marine *PPP*s and their complexity, Chapter 4 presented a distributed *Sensor Fault Diagnosis* (*SFDI*) architecture for marine *Internal Combustion Engine*s (*ICE*s). The architecture was designed having two levels; the local and global level. At the local level, multiple monitoring agents were designed to monitor the health of different subsets of sensors, each composed by one or more monitoring modules. The monitoring modules followed a model-based design with multiple residuals being formed and compared against certain thresholds. In an effort to reduce the conservativeness in decision making while excluding false alarms, adaptive thresholds were developed based on

the system dynamical model. The binary decisions of the monitoring modules regarding the occurrence of sensor faults were collected in a vector for each agent and compared to the columns of predefined binary *FSM*s, to determine the local diagnosis sets. At the global level, a global agent was designed to collect the additional decisions of the local monitoring agents regarding the propagation of sensor faults, thus accounting for possible propagation of fault effects through the agent interconnections in the distributed architecture. This decision vector was then compared to the columns of a global *FSM*, to determine the global diagnosis set. The different diagnosis sets were then combined to indicate the diagnosed fault cases. Moreover, the performance of the proposed diagnosis architecture was verified through the new formulation and use of novel *Key Performance Indicator*s (*KPI*s), related to sensor fault detectability and isolability.

It was found that the application of the proposed methodology results in minimal fault detection delays (in most cases < 1 *min*) for marine *ICE*s due to the decreased conservativeness in threshold design (minimum detectable fault magnitudes comparable to the considered noise level). Moreover, more than half of the considered sensors were guaranteed to be healthy from the isolation process, while considering a more accurate *ICE* model with a great number of interconnections and associated nonlinearity.

Q4: *How to switch between hardware and virtual sensors during operation for enhanced fault resilience in marine propulsion plants?*

In order to enable switching between hardware and virtual sensors, in case of sensor faults, a fault-resilient multi-agent control scheme was proposed in Chapter 5. Following the diagnosis of sensor faults, the monitoring agent design was enhanced through the development of two resilience mechanisms; the generation of virtual sensors and a multi-sensory switching logic. The design of the virtual sensors was based on the *DAE* representation of the propulsion plant model and validated through the use of an estimation error-based *KPI*. Sensor switching was activated based on multiple defined criteria related to control performance, manufacturer-specified operational constraints of the *ICE* and control stability. The provision of control stability guarantees was facilitated by employing a model-based design for the primary level control agents and using Lyapunov stability analysis. The proposed scheme can provide resilience against the effects of sensor faults during the plant operation while maintaining both system and control stability.

More specifically, the application of the multi-sensory switching scheme resulted in mean absolute percentage errors less than the considered noise level for simulation purposes (3 %) with a relatively small control effort by the designed controllers.

Q5: *How to optimise the fault diagnosis capabilities and the required hardware redundancy for safe operation of marine* PPP*s?*

Based on the isolability-related *KPI*s in Chapter 4, it was found that isolability could still be improved. One of the main aspects in the fault diagnosis process that can influence multiple sensor fault isolability is the sensor set decomposition problem. The sensor set decomposition problem aims to determine the optimal number and composition of sensor subsets, stemming from the starting sensor set, in order to enhance the isolation of multiple sensor faults (Reppa et al., 2016). To handle this problem, in Chapter 6 an *SFDI* designer module was proposed, using a greedy stochastic optimiser approach. In contrast to the common approaches found in literature, the analytical redundancy available to the system in the form of virtual sensors was considered, instead of hardware redundancy. Meanwhile, the modelling complexity associated with marine *PPP*s was managed, using qualitative/semantic information.

The implementation of the *SFDI* designer module resulted in local and global *FSM*s with an enhanced number of isolable columns. It was also found that increasing the number of monitoring agents results in a significant increase in the number of isolable columns (up to 33 % between the 2 and 5 agent configuration), though at the expense of greater communication requirements.

Q6: *How to design a resilient control scheme to facilitate the adaptation of the power and propulsion systems to changes in operational requirements?*

In order to better capture the uncertainty in design adaptations, in Chapter 7, an integrated framework bridging the topology and control design perspectives of marine *PPP*s was proposed. Using this framework, the topology design decisions can be transformed - using semantics- into useful information for the control system, providing cognitive knowledge on the *PPP* components and their interconnections. In turn, this information can be employed to enable online switching between the automation components through the use of an intelligent supervisor under the effects of unforeseen events such as faults and attacks. By exploring another adaptation driver, that is the change in mission characteristics, the intelligent supervisor is able to instigate design adaptations from the topology perspective when the feasibility of the mission with the current components is questionable. To summarize, the proposed resilient control scheme manages to facilitate *PPP* adaptations to updated requirements (e.g., due to mission changes, faults), by connecting the topology and control design perspectives and providing better quality of information to both vessel designers and operators (i.e., feasibility of operation, fault-free sensor feedback,

updated power requirements for topology adaptations).

The implementation of the developed resilient control scheme rendered satisfactory tracking results both considering the power profile and the rest of the local control objectives (reference tracking errors less than 3 %).

Based on the above answers, the answer to the overall research question of this thesis is provided next.

Q:*How to design safe and resilient autonomous control systems to handle the uncertain future adaptations in vessel automation and to compensate for malfunction effects without human intervention?*

Safety and resilience are two fundamental properties for dealing with dangerous (e.g., loss of propulsion power) and uncertain (e.g., mission changes) scenarios for marine vessels. The *PPP* is regarded as the heart of the vessel operation and is the focus of the majority of design adaptations in recent years (i.e., due to changes in emission regulations). The types of adaptations, their drivers and the state of the art concerning the safe and resilient control of marine *PPP*s were reviewed in Chapter 2. A key element in the design of safe and resilient control systems of *PPP*s is their modelling, which in this thesis is twofold: quantitative using first principles and qualitative using semantics, both described in Chapter 3. The utilization of both quantitative and qualitative models contributes to handling the high complexity of marine *PPP*s.

For safe control, proper monitoring methods that are able to detect and isolate different kinds of vulnerabilities were investigated. In particular, this thesis considered the case of multiple sensor faults consecutively affecting a marine *ICE* and proposed the use of a distributed monitoring architecture, considering the large scale and complexity of the system. For fault detection, model-based residuals, based on the *Differential-Algebraic Equation*s (*DAE*s) model of the *ICE*, were used alongside designed adaptive thresholds. This design choice of the thresholds allowed for reducing conservativeness in decision making of the monitoring agents while excluding false alarms. Isolation was then carried out in two levels; the local and the global level. At the local level, the decision vectors of each monitoring agent were used to generate the local diagnosis sets (i.e., sets containing potential fault scenarios). At the global level, the propagation of fault effects between the local agents was considered to exonerate some of the fault scenarios. The proposed monitoring architecture was presented and validated using multiple defined *Key Performance Indicator*s (*KPI*s) targeted at both sensor fault detectability and isolability, in Chapter 4. Based on the obtained results, the use of a more optimal sensor set decomposition than the physical one was then investigated in Chapter 6, as a means

to enhance sensor fault isolability.

In the case of resilient control, as identified in Chapter 2, two factors were considered; the available type of redundancy and the resilience mechanism. In contrast to the majority of maritime literature, this thesis employed the analytical redundancy of marine *PPP*s, expressed through the collected models in Chapter 3, and proposed the design of virtual (software-based) sensors in Chapter 5. The resilience mechanisms were then based on reconfiguration strategies, with a multi-sensory switching logic between hardware and virtual sensors proposed to handle the effects of sensor faults in Chapter 5 and a control supervisor proposed to handle uncertain design adaptations in the marine *PPP* due to changes in the mission characteristics described in Chapter 7.

The **safe and resilient control** methods discussed in Chapters 4-7 extend beyond marine *PPP*s and also hold potential for various marine systems and other application domains. For systems described mathematically by the *Differential-Algebraic Equations* (*DAE*) formulation in (3.1) and (3.2) , such as in chemical engineering (Vemuri et al., 2001), the sensor fault diagnosis methodology from Chapter 4 can be applied. The specifics of system modeling primarily affect the generation of adaptive thresholds, as explained in Section 4.2.2, with only minor modifications needed when adapting to alternative subsystem dynamics. Similarly, virtual sensors based on *DAE* modeling, as outlined in Chapter 5, can be implemented, with the specifics of the model-based control scheme adjusting to the application. The use of semantics as a qualitative modeling technique to describe systems with complex dynamics further expands the applicability of the safe and resilient control strategies presented in Chapters 6 and 7 across a wide range of research fields. For centralized (1-agent) and distributed (multi-agent) monitoring architectures, the methodology in Chapter 6 enhances sensor fault isolability. Lastly, the technical aspects of resilient control approaches found in the literature, along with the relationship between the system topology and control design perspectives, can be addressed with using the approaches in Chapter 7, also for different application domains.

8.2 Future research

Even though READINESS (READINESS, 2020) is quite a broad project considering flexible automation systems, novel energy carriers and the optimal routing of cables and pipes in the machinery space, irrespective of the type of fuel, it served as a common ground for many other projects that were formulated after it. Project MENENS started in 2021 with the main goal to enable the use of methanol as a maritime fuel, due to its low cost and low emissions (MENENS, 2022). Similar approaches considering hydrogen as a potential maritime fuel are currently investigated in project S$\mathbf{H}_2$IPDRIVE (SH2IPDRIVE, 2022), while ammonia is considered

in project AmmoniaDrive (AmmoniaDrive, 2022). Finally, project SEAMLESS was initiated in 2022 to develop the missing technology building blocks that are required to ensure safe, resilient, efficient, and environmentally friendly vessel operation for Short Sea Shipping and Inland Waterways Transport (SEAMLESS, 2022).

As the interest in the safe and resilient control of marine *PPP*s is ongoing and increasing along with the number of relevant projects, the following directions for future research are proposed, and classified in terms of safety and resilience in Figure 8.1.

1. **Certification of safe and resilient control solutions**

   In this thesis, the proposed safe and resilient control methods for marine *PPP*s were evaluated using certain formulated *KPI*s. These metrics are particularly useful for certification purposes of the developed methods. Nonetheless, product development still requires further theoretical and experimental analysis to increase the *Technology Readiness Level* (*TRL*) (RVO, 2022). Moreover, this development should also be accompanied by the creation of further guidelines concerning not only the physical but also the cyber infrastructure of the vessel, from the part of classification societies.

2. **Addressing Cybersecurity challenges**

   Similar to other *Cyber-Physical System*s (*CPS*s), as the reliance to cyber infrastructure intensifies in pursuit of higher degrees of autonomy the need to also consider cyber vulnerabilities in the *PPP*, such as cyberattacks, increases. Cyberattacks have been introduced relatively recently in the maritime literature (see Chapter 2). Moreover, the available Cybersecurity methods mostly concern a broader range of applications (e.g., microgrids). However, future approaches should also take into account the intricate nature of marine *PPP*s, like the limited space for on-board hardware redundancy, the centralised architecture of onboard monitoring and control and the difficulties associated with the communication between components sourced by different manufacturers (i.e., due to different communication protocols).

3. **Consideration of regulations as an adaptation driver**

   The uncertainty regarding the regulatory framework is rarely considered in research works as an adaptation driver. Despite taking place in a longer time horizon than mission changes and the occurrence of malfunctions, changes in regulations often lead to more wide-scale design adaptations which in turn incurs bigger costs for the vessel owner. Moreover, it would be interesting to consider combinations of adaptation drivers including regulations, as was done with mission changes and malfunctions in Chapter 7 of this thesis. Finally, the consideration of regulations could provide better insights for the

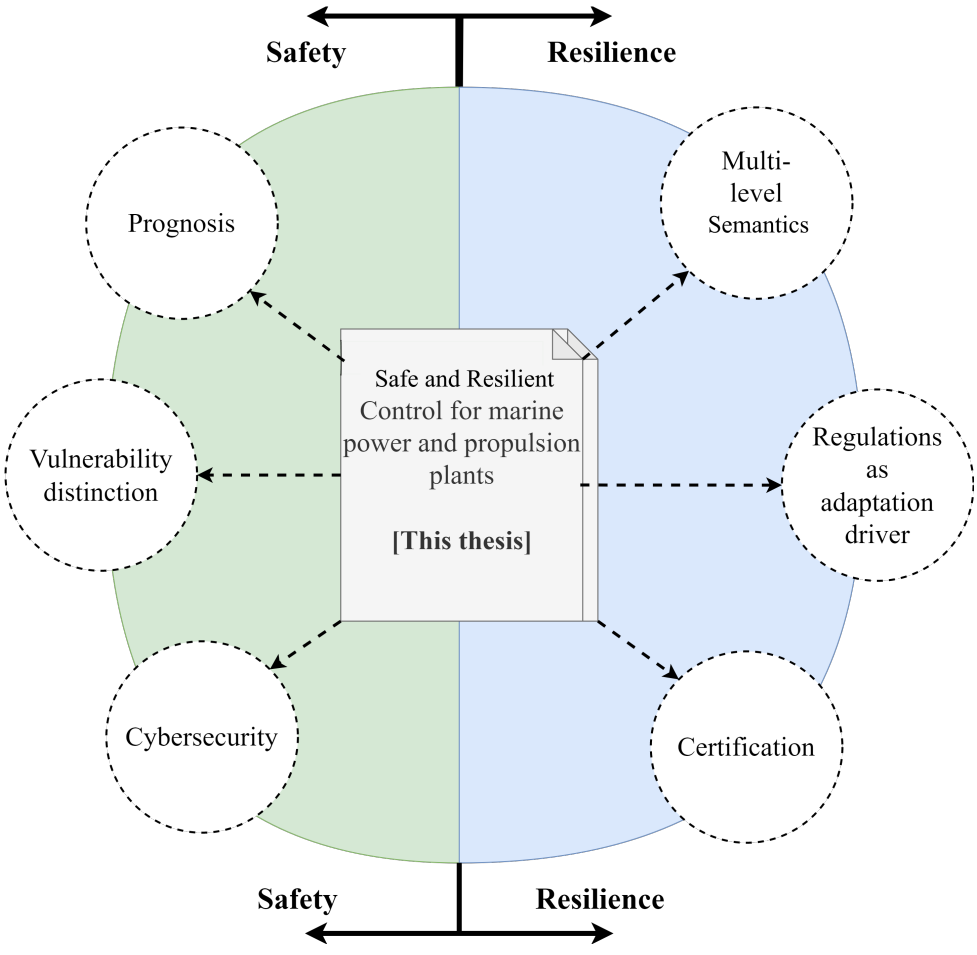


Figure 8.1: Proposed future research directions. The directions are classified in terms of their added value in either safety or resilience oriented directions.

achieved resilience and act as feedback to the decisions made by both vessel operators and the *International Maritime Organisation* (*IMO*).

4. **Properly distinguishing between vulnerabilities**

   While papers in marine literature as well as this thesis propose approaches to handle the effects of vulnerabilities such as sensor and process faults, distinguishing between these two cases is still an open problem. This distinction is especially important, considering that the course of actions required to be assumed after the diagnosis of a vulnerability is different in the case of a process and in that of a sensor fault. Cyberattacks are also becoming more and more prominent for marine vessels and should also be able to get isolated from the other cases of faults.

5. **Expansion of semantic description to incorporate other control levels**

   In this thesis we proposed the use of qualitative information, in the form of semantics, as a complementary modelling method to handle the complexity of marine *PPP*s. However, there is still the possibility for an expansion of the semantic database to also include relevant information encountered in other control levels. For instance, similar to robotics applications (Dharmadhikari &Alexis, 2023), the navigation of the vessel in an inland waterway could be described with semantics as well. Taking this step can help us leverage the benefits of Computational Intelligence tools for a broader pool of control applications in the maritime domain, while handling the involved modelling complexity.

6. **Expansion to prognosis for improved maintenance scheduling**

   Following the development of novel monitoring approaches for the diagnosis of system and sensor health problems in marine *PPP*s, prognosis methods can be leveraged. Prognosis is usually concerned with estimating the *Remaining useful life* (*RUL*) of the various components through estimation of the progression of fault effects based on available models or data (Kim et al., 2017). In the context of marine *PPP*s, prognosis could potentially improve maintenance scheduling by considering the natural degradation of systems and sensors, aside from the effects of vulnerabilities. As a result, the overall maintenance costs can be reduced while increasing the operational time of the vessel.

Bibliography

Adamczyk, M., T. Orlowska-Kowalska (2019) Virtual current sensor in the fault-tolerant field-oriented control structure of an induction motor drive, *MDPI Sensors*, 19(22), pp. 1–15.

Aimiyekagbon, O. K., L. Muth, M. Wohlleben, A. Bender, W. Sextro (2021) Rule-based diagnostics of a production line, in: *PHM Society European Conference*, vol. 6, pp. 10–10.

Amin, S., A. A. Cárdenas, S. S. Sastry (2009) Safe and secure networked control systems under denial-of-service attacks, in: *Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control, San Francisco, CA*, pp. 31–45.

AmmoniaDrive (2022) Ammonia Powered Ships - NWO Project AmmoniaDrive, URL https://ammoniadrive.tudelft.nl/.

Bassam, A. M., A. B. Phillips, S. R. Turnock, P. A. Wilson (2017) Development of a multi-scheme energy management strategy for a hybrid fuel cell driven passenger ship, *International Journal of Hydrogen Energy*, 42(1), pp. 623–635.

Bendtsen, J., K. Trangbaek, J. Stoustrup (2013) Plug-and-play control-Modifying control systems online, *IEEE Transactions on Control Systems Technology*, 21(1), pp. 79–93.

Bendtsen, J. D., K. Trangbaek, J. Stoustrup (2008) Plug-and-play process control: Improving control performance through sensor addition and pre-filtering, *IFAC Proceedings Volumes (IFAC-PapersOnline)*, 17(1), pp. 336–341.

Bertaska, I. R., K. D. von Ellenrieder (2018) Experimental evaluation of supervisory switching control for unmanned surface vehicles, *IEEE Journal of Oceanic Engineering*, 44(1), pp. 7–28.

Bidram, A., A. Davoudi, F. L. Lewis (2013) Distributed control for AC shipboard power systems, *2013 IEEE Electric Ship Technologies Symposium, ESTS 2013*, pp. 282–286.

Blanke, M., M. Kinnaert, J. Lunze, M. Staroswiecki (2016) *Diagnosis and Fault-Tolerant Control Third Edition*, Springer, 695 pp.

Bo, T. I., T. A. Johansen (2013) Scenario-based fault-tolerant model predictive control for diesel-electric marine power plant, in: *Proceedings of the OCEANS 2013 MTS/IEEE: The Challenges of the Northern Dimension, Bergen, the Netherlands*, pp. 1–5.

Bolbot, V., O. Methlouthi, O. V. Banda, L. Xiang, Y. Ding, P. Brunou (2022) *Trends in Maritime Technology and Engineering*, chap. Identification of cyber-attack scenarios in a marine Dual-Fuel engine, CRC Press, pp. 503–510.

Bolbot, V., N. L. Trivyza, G. Theotokatos, E. Boulougouris, A. Rentizelas, D. Vassalos (2020) Cruise ships power plant optimisation and comparative analysis, *Energy*, 196(117061), pp. 1–22.

Boveri, A., F. Silvestro, M. Molinas, E. Skjong (2018) Optimal sizing of energy storage systems for shipboard applications, *IEEE Transactions on Energy Conversion*, 34(2), pp. 801–811.

Cai, B., X. Sun, J. Wang, C. Yang, Z. Wang, X. Kong, Z. Liu, Y. Liu (2020) Fault detection and diagnostic method of diesel engine by combining rule-based algorithm and bns/bpnns, *Journal of Manufacturing Systems*, 57, pp. 148–157.

Cai, C., X. Weng, C. Zhang (2017) A novel approach for marine diesel engine fault diagnosis, *Cluster Computing*, 20(2), pp. 1691–1702.

Campa, G., M. Thiagarajan, M. Krishnamurty, M. R. Napolitano, M. Gautam (2008) A neural network based sensor validation scheme for heavy-duty diesel engines, *Journal of Dynamic Systems, Measurement and Control, Transactions of the ASME*, 130(2), pp. 0210081–02100810.

Caprolu, M., R. D. Pietro, S. Raponi, S. Sciancalepore, P. Tedeschi (2020) Vessels Cybersecurity: Issues, Challenges, and the Road Ahead, *IEEE Communications Magazine*, 58(6), pp. 90–96.

Çetin, O., M. Z. Sogut (2021) A new strategic approach of energy management onboard ships supported by exergy and economic criteria: A case study of a cargo ship, *Ocean Engineering*, 219(108137), pp. 1–10.

Chen, F., H. Deng, Z. Shao (2020) Decentralised control method of battery energy storage systems for soc balancing and reactive power sharing, *IET Generation, Transmission & Distribution*, 14(18), pp. 3702–3709.

Cheong, K. L., P. Y. Li, J. Xia (2010) Control oriented modeling and system identification of a diesel generator set (genset), in: *Proceedings of the 2010 American Control Conference*, IEEE, pp. 950–955.

Choi, M. (2018) *Modular Adaptable Ship Design for Handling Uncertainty in the Future Operating Context*, Ph.D. thesis, Norwegian University of Science and Technology.

Cómbita, L. F., J. Giraldo, A. A. Cárdenas, N. Quijano (2015) Response and reconfiguration of cyber-physical control systems: A survey, in: *Proceedings of the 2015 IEEE 2nd Colombian Conference on Automatic Control, Manizales, Colombia*, IEEE, pp. 1–6.

Cui, M., J. Wang, B. Chen (2020) Flexible Machine Learning-Based Cyberattack Detection Using Spatiotemporal Patterns for Distribution Systems, *IEEE Transactions on Smart Grid*, 11(2), pp. 1805–1808.

Darvishi, H., D. Ciuonzo, E. R. Eide, P. S. Rossi (2021) Sensor-Fault Detection, Isolation and Accommodation for Digital Twins via Modular Data-Driven Architecture, *IEEE Sensors Journal*, 21(4), pp. 4827–4838.

de Vos, J., R. G. Hekkenberg, O. A. Valdez Banda (2021) The Impact of Autonomous Ships on Safety at Sea – A Statistical Analysis, *Reliability Engineering and System Safety*, 210(June 2020), p. 107558.

Delft High Performance Computing Centre (DHPC) (2024) DelftBlue Supercomputer (Phase 2), https://www.tudelft.nl/dhpc/ark:/44463/DelftBluePhase2.

Deng, C., C. Wen, J. Huang, X.-M. Zhang, Y. Zou (2021) Distributed observer-based cooperative control approach for uncertain nonlinear mass under event-triggered communication, *IEEE Transactions on Automatic Control*, 67(5), pp. 2669–2676.

Dharmadhikari, M., K. Alexis (2023) Semantics-aware exploration and inspection path planning, in: *Proceedings of the 2023 IEEE International Conference on Robotics and Automation, London, UK*, IEEE, pp. 3360–3367.

Ding, S. X. (2013) *Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms and Tools*, second edition ed., Springer London Heidelberg New York Dordrecht, Duisburg, Germany, 505 pp.

Djagarov, N., Z. Grozdev, G. Enchev, J. Djagarova (2019) Ship's induction motors fault diagnosis, in: *Proceedings of the 2019 16th Conference on Electrical Machines, Drives and Power Systems, Varna, Bulgaria*, IEEE, pp. 6–8.

DNV (2012) Dynamic Positioning Vessel: Design Philosophy Guidelines, Tech. rep.

European Maritime Safety Agency (2023) Annual Overview of Marine Casualties and Incidents 2023, Tech. rep., European Maritime Safety Agency.

Farrell, J. A., M. M. Polycarpou (2006) *Adaptive Approximation Based Control*.

Felski, A., K. Zwolak (2020) The ocean-going autonomous ship - Challenges and threats, *Journal of Marine Science and Engineering*, 8(1), pp. 1–16.

Ferrari, R. M., A. M. Teixeira (2021) *Safety, security and privacy for cyber-physical systems*, Springer.

Fu, M., J. Ning, Y. Wei (2011) Fault-tolerant control of dynamic positioning vessel by means of a virtual thruster, in: *Proceeding of the 2011 IEEE International Conference on Mechatronics and Automation, Beijing, China*, pp. 1706–1710.

Gallo, A. J., M. S. Turan, P. Nahata, F. Boem, T. Parisini, G. Ferrari-Trecate (2018) Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids, in: *Proceedings of the 2018 European Control Conference, Limassol, Cyprus*, European Control Association (EUCA), pp. 344–349.

García, E., E. Quiles, A. Correcher, F. Morant (2019) Marine NMEA 2000 smart sensors for ship batteries supervision and predictive fault diagnosis, *Sensors (Switzerland)*, 19(20).

Gasparjan, A., A. Terebkov, A. Zhiravetska (2015) Monitoring of electro-mechanical system "diesel-synchronous generator", in: *Proceedings of the 2015 IEEE 5th International Conference on Power Engineering, Energy and Electrical Drives, Riga, Latvia*, pp. 103–108.

Geertsma, R. D. (2019) *Autonomous Control for Adaptive Ships with Hybrid Propulsion and Power Generation*, Ph.D. thesis, TU Delft.

Geertsma, R. D., R. R. Negenborn, K. Visser, J. J. Hopman (2017a) Design and control of hybrid power and propulsion systems for smart ships: A review of developments, *Applied Energy*, 194, pp. 30–54.

Geertsma, R. D., R. R. Negenborn, K. Visser, J. J. Hopman (2017b) Parallel Control for Hybrid Propulsion of Multifunction Ships, *IFAC-PapersOnLine*, 50(1), pp. 2296–2303.

Geertsma, R. D., R. R. Negenborn, K. Visser, M. A. Loonstijn, J. J. Hopman (2017c) Pitch control for ships with diesel mechanical and hybrid propulsion: Modelling, validation and performance quantification, *Applied Energy*, 206(April), pp. 1609–1631.

Geertsma, R. D., K. Visser, R. R. Negenborn (2018) Adaptive pitch control for ships with diesel mechanical and hybrid propulsion, *Applied Energy*, 228, pp. 2490–2509.

Group, M. E. (2024) Marine Engine / Marine Propulsion System /Business & Products —, URL https://www.mes.co.jp/english/business/engine/diesel.html.

GSA (2016) STRIKE3 - Monitor, Detect, Characterise, Standardize, Mitigate and Protect, URL https://aric-aachen.de/strike3/S3-work/.

Hansen, J. F. (2000) Modelling and Control of Marine Power System, *PhD Thesis NTNU*, p. 111.

Hansen, J. M., M. Blanke, H. H. Niemann, M. Vejlgaard-Laursen (2013) Exhaust gas recirculation control for large diesel engines - Achievable performance with SISO design, *IFAC Proceedings Volumes*, 9, pp. 346–351.

Haseltalab, A. (2019) *Control for Autonomous All-electric Ships Integrating Maneuvering, Energy Management, and Power Generation Control*, Ph.D. thesis, TU Delft.

Haseltalab, A., M. A. Botto, R. R. Negenborn (2018) On-Board Voltage Regulation For All-Electric DC Ships, *IFAC-PapersOnLine*, 51(29), pp. 341–347.

Haseltalab, A., R. R. Negenborn (2019) Model predictive maneuvering control and energy management for all-electric autonomous ships, *Applied Energy*, 251, pp. 1–27.

Haseltalab, A., R. R. Negenborn, G. Lodewijks (2016) Multi-Level Predictive Control for Energy Management of Hybrid Ships in the Presence of Uncertainty and Environmental Disturbances, *IFAC-PapersOnLine*, 49(3), pp. 90–95.

Haseltalab, A., L. van Biert, H. Sapra, B. Mestemaker, R. R. Negenborn (2021) Component sizing and energy management for sofc-based ship power systems, *Energy Conversion and Management*, 245, pp. 1–16.

Hou, J., Z. Song, H. Park, H. Hofmann, J. Sun (2018) Implementation and evaluation of real-time model predictive control for load fluctuations mitigation in all-electric ship propulsion systems, *Applied Energy*, 230(February), pp. 62–77.

Hu, H., W. Shi (2021) Modeling and simulation of all-electric propulsion system with three-closed loop control, *Journal of Computational Methods in Sciences and Engineering*, 21(1), pp. 109–123.

Hu, J., J. Wang, J. Zeng, X. Zhong (2018) Model-based temperature sensor fault detection and fault-tolerant control of urea-selective catalyst reduction control systems, *Energies*, 11(7), pp. 1–17.

IHC, R. (2020) IHC Drives & Automation Integrated Vessel Automation, Tech. rep., Royal IHC.

IMO (1974) *International Convention for the Safety of Life at Sea*, International Maritime Organization, London, UK, latest edition ed.

IMO (2018) Initial IMO Strategy on reduction of GHG emission from ships. Resolution MEPC.304(72) (adopted on 13 April 2018), Tech. rep., International Maritime Organisation (IMO).

ING (2020) ZES: a zero-emission service cleans up inland shipping, URL https://shorturl.at/mwFX5.

Isermann, R. (2006) Fault-tolerant components and control, in: *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*, chap. 19, Springer Science & Business Media, Berlin Heidelberg, pp. 355–365.

Jaulin, L., M. Kieffer, O. Didrit, E. Walter, L. Jaulin, M. Kieffer, O. Didrit, É. Walter (2001) *Interval Analysis*, Springer, London, UK.

Jiang, Y., Y. Yang (2024) A distributed proportional-integral observer-based hierarchical control for ac microgrids under fdi attacks, *IEEE Transactions on Industrial Electronics*, pp. 1–13.

Jilg, M., O. Stursberg (2013) Hierarchical distributed control for interconnected systems, in: *IFAC Proceedings Volumes (IFAC-PapersOnline)*, vol. 13, IFAC, pp. 419–425.

Jones, N. B., Y. H. Li (2000) A review of condition monitoring and fault diagnosis for diesel engines, *Tribo Test*, 6(3), pp. 267–291.

Jung, D., Y. Dong, E. Frisk, M. Krysander, G. Biswas (2020) Sensor selection for fault diagnosis in uncertain systems, *International journal of control*, 93(3), pp. 629–639.

Kalikatzarakis, M., R. D. Geertsma, E. J. Boonen, K. Visser, R. R. Negenborn (2018) Ship energy management for hybrid propulsion and power supply with shore charging, *Control Engineering Practice*, 76, pp. 133–154.

Kerrigan, E. C., J. M. Maciejowski (1999) Fault-tolerant control of a ship propulsion system using model predictive control, in: *Proceedings of the 1999 European Control Conference, Karlsruhe, Germany*, IEEE, pp. 4602–4607.

Khalil, H. K. (2002) *Control of nonlinear systems*, Prentice Hall, New York, NY.

Kherif, O., Y. Benmahamed, M. Teguar, A. Boubakeur, S. S. M. Ghoneim (2021) Accuracy improvement of power transformer faults diagnostic using knn classifier with decision tree principle, *IEEE Access*, 9, pp. 81693–81701.

Kim, N.-H., D. An, J.-H. Choi (2017) *Prognostics and Health Management of Engineering Systems*, Springer International Publishing, Switzerland.

Knežević, V., J. Orović, L. Stazić, J. Čulin (2020) Fault tree analysis and failure diagnosis of marine diesel engine turbocharger system, *Journal of Marine Science and Engineering*, 8(12).

Kodakkadan, A. R., V. Reppa, S. Olaru (2016) Switching-stable control mechanism in the presence of guaranteed detectable sensor faults, in: *Proceedings of the 2016 Conference on Control and Fault-Tolerant Systems, Barcelona, Spain*, pp. 93–98.

Konda, R., D. Grimsman, J. R. Marden (2022) Execution Order Matters in Greedy Algorithms with Limited Information, in: *Proceedings of the 2022 American Control Conference, Atlanta, Georgia, USA*, American Automatic Control Council, pp. 1305–1310.

Kougiatsos, N., R. Negenborn, V. Reppa (2022a) Distributed model-based sensor fault diagnosis of marine fuel engines, *IFAC-PapersOnLine*, 55(6), pp. 347–353.

Kougiatsos, N., R. Negenborn, V. Reppa (2022b) A multi-sensory switching-stable architecture for distributed fault tolerant propulsion control of marine vessels, in: *Proceedings of the 2022 International Ship Control Systems Symposium, Delft, the Netherlands*, vol. 16, Institute of Marine Engineering Science and Technology, pp. 1–13.

Kougiatsos, N., V. Reppa (2022) A distributed virtual sensor scheme for marine fuel engines, *IFAC-PapersOnLine*, 55(31), pp. 333–338.

Kougiatsos, N., V. Reppa (2024a) A Distributed cyber-physical framework for sensor fault diagnosis of marine fuel engines, *IEEE Transactions on Control Systems Technology*, pp. 1–12.

Kougiatsos, N., V. Reppa (2024b) Sensor set decomposition for enhanced distributed sensor fault isolability of marine propulsion systems, in: *Proceedings of 2024 IFAC SAFEPROCESS, Ferrara, Italy*, pp. 55–60.

Kougiatsos, N., E. L. Scheffers, M. C. van Benten, D. L. Schott, P. de Vos, R. R. Negenborn, V. Reppa (2024a) An intelligent topology and control design framework for mission-adaptive marine power and propulsion plants, *submitted to a journal*, pp. 1–21.

Kougiatsos, N., M. Vagia, R. R. Negenborn, V. Reppa (2024b) Fault-resilient multi-agent control for marine hybrid propulsion plants, *submitted to a journal*, pp. 1–15.

Kougiatsos, N., J. Zwaginga, J. Pruyn, V. Reppa (2023) Semantically enhanced system and automation design of complex marine vessels, in: *Proceedings of the 2023 IEEE Symposium Series on Computational Intelligence, Mexico City, Mexico*, IEEE, pp. 512–518.

Kularatna, N., K. Gunawardane (2021) 3 - rechargeable battery technologies: An electronic circuit designer's viewpoint, in: Kularatna, N., K. Gunawardane, eds., *Energy Storage Devices for Renewable Energy-Based Systems (Second Edition)*, second edition ed., Academic Press, Boston, pp. 65–98.

Kurt, M. N., Y. Yilmaz, X. Wang (2018) Distributed quickest detection of cyber-attacks in smart grid, *IEEE Transactions on Information Forensics and Security*, 13(8), pp. 2015–2030.

Letafat, A., M. Rafiei, M. Sheikh, M. Afshari-Igder, M. Banaei, J. Boudjadar, M. H. Khooban (2020) Simultaneous energy management and optimal components sizing of a zero-emission ferry boat, *Journal of Energy Storage*, 28, p. 101215.

Li, B., R. Wang, M. Chen, L. Zhang (2016) Fault diagnosis for the ship electric propulsion system, in: *Proceedings of the 2016 International Conference on Natural Computation, Fuzzy Systems and Knowledge discovery, Changsha, China*, IEEE, pp. 714–718.

Li, H., H. Xie, Y. Xie (2018) Research on PMSM model predictive control for ship electric propulsion, *Proceedings of the 30th Chinese Control and Decision Conference, CCDC 2018*, pp. 1392–1398.

Li, N., J. R. Marden (2010) Designing games to handle coupled constraints, in: *Proceedings of the 2010 IEEE Conference on Decision and Control, Atlanta, Georgia, USA*, pp. 250–255.

Li, T., M. Hua, Q. Yin (2019) The temperature forecast of ship propulsion devices from sensor data, *Information*, 10(10), pp. 1–17.

Li, Z., M. Shahidehpour, F. Aminifar (2017) Cybersecurity in Distributed Power Systems, *Proceedings of the IEEE*, 105(7), pp. 1367–1388.

Li, Z., X. Yan, Z. Guo, P. Liu, C. Yuan, Z. Peng (2012a) A new intelligent fusion method of multi-dimensional sensors and its application to tribo-system fault diagnosis of marine diesel engines, *Tribology Letters*, 47(1), pp. 1–15.

Li, Z., X. Yan, C. Yuan, Z. Peng (2012b) Intelligent fault diagnosis method for marine diesel engines using instantaneous angular speed, *Journal of Mechanical Science and Technology*, 26(8), pp. 2413–2423.

Liang, X., P. Wang, X. Zhang, B. Wen, X. Li, X. Tian (2022) Multi-objective robust energy management for environment powered unmanned surface vehicles, *Ocean Engineering*, 247(110624), pp. 1–10.

Lin, X., K. Liang, C. Ding (2017) Sensors fault detection for dynamic positioning systems based on first order perturbation theory, in: *Proceedings of the 2017 International Conference on Computer Technology, Electronics and Communication, Dalian, China*, pp. 1136–1141.

Lin, Y., J. Du (2016) Fault-tolerant control for dynamic positioning of ships based on an iterative learning observer, in: *Proccedings of the 2016 35th Chinese Control Conference, Chengdu, China*, IEEE, pp. 1116–1122.

Listou Ellefsen, A., P. Han, X. Cheng, F. T. Holmeset, V. Aesoy, H. Zhang (2020) Online Fault Detection in Autonomous Ferries: Using Fault-Type Independent Spectral Anomaly Detection, *IEEE Transactions on Instrumentation and Measurement*, 69(10), pp. 8216–8225.

Liu, J., D. Shi, G. Li, Y. Xie, K. Li, B. Liu, Z. Ru (2020) Data-driven and association rule mining-based fault diagnosis and action mechanism analysis for building chillers, *Energy and Buildings*, 216, pp. 1–16.

Liu, S., Y. Sun, L. Zhang, P. Su (2021) Fault diagnosis of shipboard medium-voltage DC power system based on machine learning, *International Journal of Electrical Power and Energy Systems*, 124(July 2020), pp. 1–10.

Luo, H., H. Zhao, S. X. Ding, S. Yin, H. Gao, X. Yang (2017) Scalability of feedback control systems for plug-and-play control, *IFAC-PapersOnLine*, 50(1), pp. 7529–7534.

MACSEA (2012) Sensors – the Eyes and Ears of Ship Automation, Tech. rep.

Magdy, Samy (2023) Oil tanker breaks down in Egypt's Suez Canal, briefly disrupting traffic in the global waterway, URL https://apnews.com/article/suez-canal-oil-tanker-egypt-waterway-malta-07e8264c8b44e7107ffaf92249b13091.

MENENS (2022) Methanol Powered Shipping - RvO Project Menens, URL https://menens.nl/.

Meredith, Sam (2024) Baltimore bridge collapse: What we know about the container ship, URL https://www.cnbc.com/2024/03/27/baltimore-bridge-collapse-what-we-know-about-the-container-ship.html.

Mesbahi, E. (2001) An intelligent sensor validation and fault diagnostic technique for diesel engines, *Journal of Dynamic Systems, Measurement and Control, Transactions of the ASME*, 123(1), pp. 141–144.

Milis, G. M. (2018) *SEMIoTICS : Semantically-enhanced IoT-enabled Intelligent Control Systems*, Ph.D. thesis, University of Cyprus.

Milis, G. M., C. G. Panayiotou, M. M. Polycarpou (2017) Semiotics: Semantically enhanced iot-enabled intelligent control systems, *IEEE Internet of Things Journal*, 6(1), pp. 1257–1266.

Milis, G. M., C. G. Panayiotou, M. M. Polycarpou (2018) Semantically Enhanced Online Configuration of Feedback Control Schemes, *IEEE Transactions on Cybernetics*, 48(3), pp. 1081–1094.

Nayyar, A., A. Mahajan, D. Teneketzis (2013) Decentralized stochastic control with partial history sharing: A common information approach, *IEEE Transactions on Automatic Control*, 58(7), pp. 1644–1658.

Negenborn, R. R., F. Goerlandt, T. A. Johansen, P. Slaets, O. A. Valdez Banda, T. Vanelslander, N. P. Ventikos (2023) Autonomous ships are on the horizon: here's what we need to know, *Nature*, 615(7950), pp. 30–33.

Ni, K., W. Li, L. Xie, D. T. Lagos, M. Alkahtani, Y. Hu (2019) Control of Doubly-Fed Induction Motor Based Shipboard Propulsion System for More-Electric Ships, in: *Proceeding of the 2019 Industrial Electronics Conference, Lisbon, Portugal*, vol. 2019-Octob, IEEE, pp. 3187–3192.

Nielsen, K. V., M. Blanke, L. Eriksson, M. Vejlgaard-Laursen (2017) Adaptive feedforward control of exhaust recirculation in large diesel engines, *Control Engineering Practice*, 65(August), pp. 26–35.

Nielsen, K. V., M. Blanke, L. Eriksson, M. Vejlgaard-Laursen (2018) Marine diesel engine control to meet emission requirements and maintain maneuverability, *Control Engineering Practice*, 76(March), pp. 12–21.

NTNU (2018) ORCAS– Online risk management and risk control for autonomous ships, URL https://www.ntnu.edu/imt/orcas.

NWO (2019) Topsector Water & Maritime: the Blue route, URL https://www.nwo.nl/en/researchprogrammes/topsector-water-maritime-blue-route.

Ostojic, P., C. Stinson (2013) Integrated synchronous motor protection and control, in: *Proceedings of the 2013 66th Annual Conference for Protective Relay Engineers, College Station, Texas, USA*, IEEE, pp. 234–249.

Panagi, P., M. M. Polycarpou (2013) A coordinated communication scheme for distributed fault tolerant control, *IEEE Transactions on Industrial Informatics*, 9(1), pp. 386–393.

Papadopoulos, P. M. (2020) *Distributed Monitoring and Control for Smart Buildings: A Model-based Fault Diagnosis and Accomodation Framework*, Ph.D. thesis, University of Cyprus.

Papanikolaou, A. (2018) *A Holistic Approach to Ship Design: Optimisation of ship design and operation for life cycle*, vol. 1, Springer, 1–490 pp.

Perera, L. P. (2016) Marine engine centered localized models for sensor fault detection under ship performance monitoring, *IFAC-PapersOnLine*, 49(28), pp. 91–96, 3rd IFAC Workshop on Advanced Maintenance Engineering, Services and Technology AMEST 2016.

Pierer von Esch, M., D. Landgraf, M. Steffel, A. Völz, K. Graichen (2024) Distributed stochastic optimal control of nonlinear systems based on admm, *IEEE Control Systems Letters*, 8, pp. 424–429.

Planakis, N., G. Papalambrou, N. Kyrtatos (2021) Integrated Load-Split Scheme for Hybrid Ship Propulsion Considering Transient Propeller Load and Environmental Disturbance, *Journal of Dynamic Systems, Measurement and Control, Transactions of the ASME*, 143(3).

Pop, M.-D., O. Proștean, G. Proștean (2020) Fault detection based on parity equations in multiple lane road car-following models using bayesian lane change estimation, *Journal of Sensor and Actuator Networks*, 9(4), p. 52.

Puig, V., F. Schmid, J. Quevedo, B. Pulido (2005) A new fault diagnosis algorithm that improves the integration of fault detection and isolation, in: *Proceedings of the 44th IEEE Conference on Decision and Control, Seville, Spain*, IEEE, pp. 3809–3814.

Pullaguram, D., S. Mishra, N. Senroy (2018) Event-triggered communication based distributed control scheme for dc microgrid, *IEEE Transactions on Power Systems*, 33(5), pp. 5583–5593.

Qi, Z., Y. Qi, G. Hu (2020) A Practical Approach to Detect Faults of Marine Diesel Engine, *Journal of Computer and Communications*, 08(08), pp. 12–21.

Qin, Z., Y. Luo, W. Zhuang, Z. Pan, K. Li, H. Peng (2018) Simultaneous optimization of topology, control and size for multi-mode hybrid tracked vehicles, *Applied Energy*, 212, pp. 1–15.

Rajkumar, R. R., I. Lee, L. Sha, J. Stankovic (2010) Cyber-physical systems: the next computing revolution, in: *Proceedings of the 47th Design Automation Conference*, DAC '10, Association for Computing Machinery, New York, NY, p. 731–736.

Raju, D., G. Bakirtzis, U. Topcu (2022) Sensor placement for online fault diagnosis, *arXiv preprint arXiv:2211.11741*, pp. 1–12.

Raptodimos, Y., I. Lazakis, G. Theotokatos, T. Varelas, L. Drikos (2016) Ship sensors data collection & analysis for condition monitoring of ship structures & machinery systems, *RINA, Royal Institution of Naval Architects - Smart Ship Technology 2016, Papers*, pp. 77–86.

READINESS (2020) NWO READINESS, URL https://www.ship-readiness.nl/.

Reppa, V., P. Papadopoulos, M. M. Polycarpou, C. G. Panayiotou (2014) A distributed virtual sensor scheme for smart buildings based on adaptive approximation, in: *Proceedings of the 2014 International Joint Conference on Neural Networks, Beijing, China*, IEEE, pp. 99–106.

Reppa, V., M. M. Polycarpou, C. G. Panayiotou (2015) Distributed sensor fault diagnosis for a network of interconnected cyberphysical systems, *IEEE Transactions on Control of Network Systems*, 2(1), pp. 11–23.

Reppa, V., M. M. Polycarpou, C. G. Panayiotou (2016) Sensor fault diagnosis, *Foundations and Trends in Systems and Control*, 3(1-2), pp. 1–248.

Reppa, V., S. Timotheou, M. M. Polycarpou, C. Panayiotou (2018) Performance index for optimizing sensor fault detection of a class of nonlinear systems, *IFAC-PapersOnLine*, 51(24), pp. 1387–1394.

Rieger, C. G., D. I. Gertman, M. A. McQueen (2009) Resilient control systems: Next generation design research, in: *Proceedings of the 2nd Conference on Human System Interactions, Catania, Italy*, IEEE, pp. 632–636.

Riverso, S., F. Boem, G. Ferrari-Trecate, T. Parisini (2016) Plug-and-Play Fault Detection and Control-Reconfiguration for a Class of Nonlinear Large-Scale Constrained Systems, *IEEE Transactions on Automatic Control*, 61(12), pp. 3963–3978.

Riverso, S., M. Farina, G. Ferrari-Trecate (2013) Plug-and-play decentralized model predictive control for linear systems, *IEEE Transactions on Automatic Control*, 58(10), pp. 2608–2614.

Rojas, H. D., H. E. Rojas, J. Cortés-Romero (2022) Fault diagnosis based on algebraic identification assisted by extended state observers, *Nonlinear Dynamics*, 107(1), pp. 871–888.

Rosich, A., R. Sarrate, V. Puig, T. Escobet (2007) Efficient optimal sensor placement for model-based FDI using an incremental algorithm, in: *Proceedings of the 2007 IEEE Conference on Decision and Control, New Orleans, Louisiana*, pp. 2590–2595.

RVO (2022) Technology Readiness Levels (TRL), URL https://www.rvo.nl/onderwerpen/trl.

Sadjina, S., L. T. Kyllingstad, M. Rindarøy, S. Skjong, V. Esøy, E. Pedersen (2019) Distributed co-simulation of maritime systems and operations, *Journal of Offshore Mechanics and Arctic Engineering*, 141(1).

Sattarzadeh, S., T. Roy, S. Dey (2021) Clustering-based Sensor Placement for Thermal Fault Diagnostics in Large-Format Batteries, *IFAC-PapersOnLine*, 54(20), pp. 381–386.

Sciberras, E., R. Norman (2012) Multi-objective design of a hybrid propulsion system for marine vessels, *IET Electrical Systems in Transportation*, 2(3), pp. 148–157.

SE, M. D. (2008) Project guide for marine plants diesel engine 28/33d, Tech. rep., MAN Diesel SE, Augsburg, Germany.

SEAMLESS (2022) EU Project Seamless, URL https://www.seamless-project.eu/.

Seron, M. M., X. W. Zhuo, J. A. De Doná, J. J. Martínez (2008) Multisensor switching control strategy with fault tolerance guarantees, *Automatica*, 44(1), pp. 88–97.

SH2IPDRIVE (2022) Hydrogen for Maritime - RvO Project SH2IPDRIVE, URL https://sh2ipdrive.com/.

Skjong, E., T. A. Johansen, M. Molinas, A. J. Sørensen (2017) Approaches to economic energy management in diesel–electric marine vessels, *IEEE Transactions on Transportation Electrification*, 3(1), pp. 22–35.

Sonandkar, S., R. Selvaraj, T. R. Chelliah (2020) Fault tolerant capability of battery assisted quasi-Z-source inverter fed five phase PMSM drive for marine propulsion

applications, in: *Proceedings of the 9th IEEE International Conference on Power Electronics, Drives and Energy Systems, Jaipur, India*, pp. 1–6.

Sørensen, A. J. (2011) A survey of dynamic positioning control systems, *Annual Reviews in Control*, 35(1), pp. 123–136.

Stoican, F., S. Olaru, M. M. Seron, J. A. De Doná (2014) A fault tolerant control scheme based on sensor-actuation channel switching and dwell time, *International Journal of Robust and Nonlinear Control*, 24(4), pp. 775–792.

Stoumpos, S., G. Theotokatos (2022) A novel methodology for marine dual fuel engines sensors diagnostics and health management, *International Journal of Engine Research*, 23(6), pp. 974–994.

Stoustrup, J. (2009) Plug & play control: Control technology towards new challenges, *European Journal of Control*, 15(3-4), pp. 311–330.

Tan, X., Z. Zhang (2023) Research on ddos attack detection method based on dynamic threshold, in: *Proceedings of the 3rd International Conference on Machine Learning and Computer Application, Shenyang, China*, vol. 12636, SPIE, pp. 503–508.

Tsaganos, G., D. Papachristos, N. Nikitakos, D. Dimitrios, A. Ölçer (2018) Fault detection and diagnosis of two-stroke low-speed marine engine with machine learning algorithms, in: *Proceedings of the 3rd international symposium on naval architecture and maritime, Instanbul, Turkey*, pp. 1–14.

Vafamand, N., M. H. Khooban, T. Dragicevic, J. Boudjadar, M. H. Asemani (2019) Time-Delayed Stabilizing Secondary Load Frequency Control of Shipboard Microgrids, *IEEE Systems Journal*, 13(3), pp. 3233–3241.

van Benten, M. (2022) *Mission-oriented Modular Control of Retrofittable Marine Power Plants*, Master's thesis, Delft University of Technology.

van Benten, M., N. Kougiatsos, V. Reppa (2022) Mission-oriented modular control of retrofittable marine power plants, in: *Proceedings of the International Ship Control Systems Symposium*, vol. 16, Institute of Marine Engineering Science and Technology, pp. 1–15.

Velarde, P., J. M. Maestre, H. Ishii, R. R. Negenborn (2018) Vulnerabilities in Lagrange-based distributed model predictive control, *Optimal Control Applications and Methods*, 39(2), pp. 601–621.

Vemuri, A. T., M. M. Polycarpou, A. R. Ciric (2001) Fault diagnosis of differential-algebraic systems - Systems, Man and Cyb ernetics, Part A, IEEE Transactions on, 31(2), pp. 143–152.

Vrijdag, A., D. Stapersma, T. van Terwisga (2007) Tradeoffs in ship propulsion control: engine overloading and cavitation inception in operational conditions, in: *Proceedings of the 9th International Naval Conference and Exhibition, Hamburg, Germany, INEC'08*, 1550, pp. 82–93.

Vu, T. L., A. A. Ayu, J. S. Dhupia, L. Kennedy, A. K. Adnanes (2015) Power Management for Electric Tugboats Through Operating Load Estimation, *IEEE Transactions on Control Systems Technology*, 23(6), pp. 2375–2382.

Vu, T. V., B. Papari, D. Perkins, K. Schoder, D. Gonsoulin, M. Stanovich, C. S. Edrington, M. Steurer (2018) Large-scale distributed control for MVDC ship power systems, in: *Proceedings of the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA*, IEEE, pp. 3431–3436.

Wang, S., J. Wang, R. Wang (2020) A novel scheme for intelligent fault diagnosis of marine diesel engine using the multi-information fusion technology, *IOP Conference Series: Materials Science and Engineering*, 782(3).

Wang, Y., F. Zhang, T. Cui (2017) Fault diagnosis and fault-tolerant control for Manifold Absolute Pressure Sensor (MAP) of diesel engine based on Elman network observer, *Control Engineering and Applied Informatics*, 19(2), pp. 90–100.

Wärtsilä (2024a) Exhaust gas recirculation (EGR), URL https://www.wartsila.com/encyclopedia/term/exhaust-gas-recirculation-(egr).

Wärtsilä (2024b) Scrubber, URL https://www.wartsila.com/encyclopedia/term/scrubber.

Wärtsilä (2024c) Selective Catalytic Reduction (SCR), URL https://www.wartsila.com/encyclopedia/term/selective-catalytic-reduction-(scr).

Wildi, T. (2002) *Electrical Machines, Drives, and Power Systems*, New Jersey: Upper Saddle River.

Wohlthan, M., D. Schadler, G. Pirker, A. Wimmer (2021) A multi-stage geometric approach for sensor fault isolation on engine test beds, *Measurement: Journal of the International Measurement Confederation*, 168(May 2020), p. 108313.

Woods, D. D., E. Hollnagel (2017) *Resilience engineering: Concepts and Precepts*, Crc Press, Boca Raton, Florida.

Wu, N. E., S. Thavamani, Y. M. Zhang, M. Blanke (2006) Sensor fault masking of a ship propulsion system, *Control Engineering Practice*, 14(11), pp. 1337–1345.

Xinsheng, W., Z. Mingli, C. Guorui (2018) Distributed power system control of new energy ship, in: *Proceedings of the 30th Chinese Control and Decision Conference, Shenyang, China*, IEEE, pp. 2159–2164.

Yang, M., W. Shi (2018) Research on Fault Diagnosis of Ship Power System Based on Improved Particle Swarm Optimization Neural Network Algorithm, in: *Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference, Chongqing, China*, IEEE, pp. 108–113.

Yuan, L. C. W., T. Tjahjowidodo, G. S. G. Lee, R. Chan, A. K. Ådnanes (2016) Equivalent consumption minimization strategy for hybrid all-electric tugboats to optimize fuel savings, in: *2016 American control conference (ACC)*, IEEE, pp. 6803–6808.

Zhang, G., M. Yao, J. Xu, W. Zhang (2020a) Robust neural event-triggered control for dynamic positioning ships with actuator faults, *Ocean Engineering*, 207, pp. 1–12.

Zhang, M., Y. Zi, L. Niu, S. Xi, Y. Li (2019) Intelligent Diagnosis of V-Type Marine Diesel Engines Based on Multifeatures Extracted from Instantaneous Crankshaft Speed, *IEEE Transactions on Instrumentation and Measurement*, 68(3), pp. 722–740.

Zhang, P., Z. Gao, L. Cao, F. Dong, Y. Zou, K. Wang, Y. Zhang, P. Sun (2022) Marine Systems and Equipment Prognostics and Health Management: A Systematic Review from Health Condition Monitoring to Maintenance Strategy, *Machines*, 10(2).

Zhang, Y., F. Ji, Q. Hu, L. Fu, X. Gao (2020b) Decentralised control strategy for hybrid battery energy storage system with considering dynamical state-of-charge regulation, *IET Smart Grid*, 3(6), pp. 890–897.

Zhang, Y., L. Sun, T. Fan, F. Ma, Y. Xiong (2023) Speed and energy optimization method for the inland all-electric ship in battery-swapping mode, *Ocean Engineering*, 284, pp. 1–12.

Zhang, Y., N. E. Wu, B. Jiang (2008) Fault detection and isolation applied to a ship propulsion benchmark, *IFAC Proceedings Volumes (IFAC-PapersOnline)*, 17(1), pp. 1908–1913.

Zhang, Z., C. Guan, Z. Liu (2020c) Real-Time Optimization Energy Management Strategy for Fuel Cell Hybrid Ships Considering Power Sources Degradation, *IEEE Access*, 8, pp. 87046–87059.

Zhou, J., Y. Yang, S. X. Ding, Y. Zi, M. Wei (2018) A Fault Detection and Health Monitoring Scheme for Ship Propulsion Systems Using SVM Technique, *IEEE Access*, 6, pp. 16207–16215.

Zhou, L., T. Lin, X. Zhou, S. Gao, Z. Wu, C. Zhang (2020) Detection of winding faults using image features and binary tree support vector machine for autotransformer, *IEEE Transactions on Transportation Electrification*, 6(2), pp. 625–634.

Zohrabi, N., S. Abdelwahed (2017) On the application of distributed control structure for medium-voltage DC shipboard power system, in: *Proceedings of the 1st Annual IEEE Conference on Control Technology and Applications, Hawaii, USA*, pp. 1201–1206.

Zwaginga, J. J., J. F. J. Pruyn (2022) An Evaluation of Suitable Methods to Deal with Deep Uncertainty Caused by the Energy Transition in Ship Design, in: *Proceedings of the 2022 SNAME International Marine Design Conference, Vancouver, Canada*, vol. Day 2 Mon, June 27, 2022, pp. 1–16.

Glossary

Conventions

The following conventions are used in this thesis for notation and symbols:

- A superscript in parentheses e.g.,$x^{(k)}$ indicates the allocation of the variable x to the cyber-physical system k.
- A double superscript in parentheses e.g.,$x^{(k,l)}$ indicates the allocation of the variable x to the l-th module of cyber-physical system k.
- A superscript $\top$ e.g.,$x^{\top}$ signifies that a transpose operation is taking place.
- Subscript *nom* of a variable e.g., x_{nom} represents the value of x under nominal conditions.
- Subscript ref of a variable e.g., x_{ref} indicates a reference signal.
- The notations $\bar{x}$, $\underline{x}$, $[x]$ represent the upper bound, lower bound and interval of this variable x.
- $ad_f g(x)$ denotes the Lie bracket of function $g(x)$ with respect to function $f(x)$, $L_f g(x)$ the Lie derivative and $span\{g(x)\}$ the span of function $g(x)$
- $\rho(A)$ signifies the rank of matrix A

List of symbols and notations

Below follows a list of the most frequently used symbols and notations in this thesis. Symbols particular to power network applications are explained only in the relevant chapters.

Differential-Algebraic modelling

$\bar{\epsilon}_{y_x}^{(I,q)}$ Adaptive threshold of the state variable-based residual vector $\epsilon_{y_x}^{(I,q)}$

$\bar{\epsilon}_{y_z}^{(I,q)}$	Adaptive threshold (upper bound) of the algebraic variable-based residual vector $\epsilon_{y_z}^{(I,q)}$
$\bar{d}^{(I)}$	Uniform bound of the noise vector $d^{(I)}$
$\epsilon_{y_x}^{(I,q)}$	State variable residual vector associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\epsilon_{y_z}^{(I,q)}$	Algebraic variable residual vector associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\Gamma^{(I,q)}$	Learning rate of the adaptive law in (5.15d)
$\hat{f}_x^{(I,q)}$	Fault estimation of $f_x^{(I)}$ by the monitoring module $\mathcal{M}^{(I,q)}$
$\hat{f}_z^{(I,q)}$	Fault estimation of $f_z^{(I)}$ by the monitoring module $\mathcal{M}^{(I,q)}$
$\hat{z}^{I,q)}$	Estimation of the algebraic state $z^{(I))}$ involved with the module $\mathcal{M}(I,q)$
$\mathcal{D}[\epsilon_{y_x}^{(I,q)}]$	Dead-zone operator, used to activate sensor fault identification
$\mathcal{G}$	Global monitoring agent
$\Omega^{(I,q)}$	Filtering term to ensure the stability of the state-equation adaptive scheme in (5.15b)
$\sigma^{(2)}$	Sensor switching law for the *ICE* controller feedback
$\sigma^{(5)}$	Sensor switching law for the *IM* controller feedback
$\underline{\epsilon}_{y_z}^{(I,q)}$	Adaptive threshold (lower bound) of the algebraic variable-based residual vector $\epsilon_{y_z}^{(I,q)}$
N_{max}	Maximum number of monitoring agents
$y_{\chi H}^{(I,q)}$	Fault-free output of the virtual sensors for the interconnection variables, through sensor fault identification in $\mathcal{M}^{(I,q)}$
$y_{xH}^{(I,q)}$	Fault-free output of the differential virtual sensors, through sensor fault identification in $\mathcal{M}^{(I,q)}$
$y_{zH}^{(I,q)}$	Fault-free output of the algebraic virtual sensors, through sensor fault identification in $\mathcal{M}^{(I,q)}$
$\chi^{(I)}$	Interconnection variables of subsystem $\Sigma^{(I)}$ from the neighbouring subsystems $\Sigma^{(J)}$, $J \neq I$

$\epsilon_x^{(I,q)}$	State estimation error associated with the module $\mathcal{M}^{(I,q)}$
$\epsilon_y^{(I,q)}$	Residual vector of the module $\mathcal{M}^{(I,q)}$
$\hat{\phi}_j^{(I)}(t)$	Sensor fault magnitude of sensor j, belonging to the sensor set $\mathcal{S}^{(I)}$
$\hat{x}^{(I,q)}$	Estimation of the differential state $x^{(I)}$ involved with the module $\mathcal{M}^{(I,q)}$
λ_{γ_I}	Lipschitz constant associated with the vector field $\gamma^{(I)}$
λ_{h_I}	Lipschitz constant associated with the vector field $h^{(I)}$
$\mathbb{U}^{(I,q)}$	Control variables interval associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\mathbb{X}^{(I,q)}$	State variables interval associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\mathbb{Y}^{(I,q)}$	Inversion set associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\mathbb{Z}^{(I,q)}$	Algebraic variables' interval associated with the monitoring module $\mathcal{M}^{(I,q)}$ and estimated using *SIVIA*
$\mathbb{Z}_0^{(I,q)}$	Algebraic variables' interval initial estimation associated with the monitoring module $\mathcal{M}^{(I,q)}$ and estimated using *SIVIA*
$\mathcal{D}_s^{\mathcal{G}}$	Global *SFDI* diagnosis set
$\mathcal{D}_s^{(I)}$	Local *SFDI* diagnosis set of agent $\mathcal{M}^{(I)}$
$\mathcal{D}_s^{\chi}$	Diagnosis set of propagated sensor faults
$\mathcal{E}^{(I,q)}$	*Analytical Redundancy Relation*s (*ARR*s) associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\mathcal{I}_{\mathcal{D}}^{(I)}$	Consistency index set between $D^{(I)}$ and $F^{(I)}$
$\mathcal{J}^{(I,q)}$	Index set associated with $\mathcal{M}^{(I,q)}$
$\mathcal{M}^{(I)}$	Monitoring agent of subsystem $\Sigma^{(I)}$
$\mathcal{M}^{(I,q)}$	Monitoring modules comprising the monitoring agent $\mathcal{M}^{(I)}$, $q = 1, \cdots, q_I$
$\mathcal{S}^{\mathcal{F}}$	Isolated faulty sensors set
$\mathcal{S}^{H}$	Exonerated healthy sensors set

$\mathcal{S}^{(I)}$	Hardware sensors of subsystem $\Sigma^{(I)}$
$\mathcal{S}^{(I,q)}$	Sensor subset assigned to be monitored by $\mathcal{M}^{(I,q)}$
$\mathcal{X}^{(I,q)}$	Interconnection variables interval associated with the monitoring module $\mathcal{M}^{(I,q)}$
$\rho^{(I,q)}$	Positive constant associated with the adaptive threshold computation in the module $\mathcal{M}^{(I,q)}$
$\rho_d^{(I,q)}$	Positive constant associated with the adaptive threshold computation in the module $\mathcal{M}^{(I,q)}$
$\Sigma^{(I)}$	Subsystem I, $I = 1, \cdots, N$
$\Xi^{(I,q)}$	Interval image associated with the interval estimation process in the monitoring module $\mathcal{M}^{(I,q)}$
$\xi^{(I,q)}$	Positive constant associated with the adaptive threshold computation in the module $\mathcal{M}^{(I,q)}$
$\xi_d^{(I,q)}$	Positive constant associated with the adaptive threshold computation in the module $\mathcal{M}^{(I,q)}$
$A^{(I)}$	Linear system dynamics of subsystem $\Sigma^{(I)}$
$C^{(I)}$	Observability matrix of subsystem $\Sigma^{(I)}$
$C^{(I,q)}$	Observability matrix associated with the module $\mathcal{M}^{(I,q)}$
$D^{(I)}$	Local binary decision vector of agent $\mathcal{M}^{(I)}$
$d^{(I)}$	Measurement noise vector of subsystem $\Sigma^{(I)}$
$D^{(I,q)}$	Output decision (0 or 1) of $\mathcal{M}^{(I,q)}$ regarding fault detection
$D_\chi^{(I)}$	Binary decision on the propagation of sensor faults of agent $\mathcal{M}^{(I)}$
$d_x^{(I,q)}(t)$	Noise vector of the state variable measurements assigned to $\mathcal{M}^{(I,q)}$
$d_z^{(I,q)}(t)$	Noise vector of the algebraic variable measurements assigned to $\mathcal{M}^{(I,q)}$
$DL^{(I,q)}$	Detection delay for each of monitoring modules $\mathcal{M}^{(I,q)}$
$E_{\mathcal{G}}$	Exoneration efficiency of the global diagnosis set
$F^{(I)}$	Local binary *Fault Signature Matrix* (*FSM*) of agent $\mathcal{M}^{(I)}$

$f^{(I)}$	Sensor fault vector of subsystem $\Sigma^{(I)}$
F^{χ}	Global binary *Fault Signature Matrix* (*FSM*) of agent $\mathcal{M}^{(I)}$
$f_{\chi}^{(I)}$	Sensor faults propagated to the agent $\mathcal{M}^{(I)}$ from the neighbouring agents
$f_{p}^{(I)}$	Sensor faults that are propagated from the agent $\mathcal{M}^{(I)}$ to its neighbouring agents
k_I	Number of interconnection variables of subsystem $\Sigma^{(I)}$
$L^{(I,q)}$	Luenberger estimator gain associated with the module $\mathcal{M}^{(I,q)}$
l_I	Number of control variables of subsystem $\Sigma^{(I)}$
$m^{(I,q)}$	Cardinality of the sensor subset $\mathcal{S}^{(I,q)}$
m_I	Number of hardware sensor outputs of subsystem $\Sigma^{(I)}$
$MDF_{j}^{(I)}$	Minimum detectable sensor fault magnitude for each of the local monitoring modules $\mathcal{M}^{(I,q)}$
MDR	Missed detection rate (MDR) concerning the propagation of sensor faults
$MDR^{(I,q)}$	Missed detection rate (MDR) for each of the local monitoring modules $\mathcal{M}^{(I,q)}$
N	Number of subsystems
N_I	Number of rows of $F^{(I)}$
n_I	Number of both state and algebraic variables of subsystem $\Sigma^{(I)}$
$P^{E_{\mathcal{G}}}$	Exoneration performance of the *SFDI* process
$P^{U_{\mathcal{G}}}$	Isolation performance of the *SFDI* process
r_I	Number of algebraic variables of subsystem $\Sigma^{(I)}$
T	Running time of the system
T_{D0}	Time the first sensor fault gets detected
$T_{D}^{(I,q)}$	Time instant of fault detection by the local SFDI module $\mathcal{M}^{(I,q)}$

$T_{f_j}^{(I)}$ Time instant of occurrence of the fault affecting the j-th sensor of the sensor set $\mathcal{S}^{(I)}$

$u^{(I)}$ Control input vector of subsystem $\Sigma^{(I)}$

$U_{\mathcal{G}}$ Uncertainty of the global diagnosis set

$x^{(I)}$ State variable vector of subsystem $\Sigma^{(I)}$

$y^{(I)}$ Hardware sensor measurements of subsystem $\Sigma^{(I)}$

$y_x^{(I,q)}(t)$ Hardware sensor measurements of state variables assigned to $\mathcal{M}^{(I,q)}$

$y_z^{(I,q)}(t)$ Hardware sensor measurements of algebraic variables assigned to $\mathcal{M}^{(I,q)}$

$z^{(I)}$ Algebraic variable vector of subsystem $\Sigma^{(I)}$

Quantitative Functions

h Change of variables function satisfying (5.6a)-(5.6c)

$\gamma^{(I)}$ Known nonlinear system dynamics of subsystem $\Sigma^{(I)}$

$\xi^{(I)}$ Algebraic system dynamics of subsystem $\Sigma^{(I)}$

$h^{(I)}$ Known interconnection dynamics of subsystem $\Sigma^{(I)}$ with the neighbouring subsystems $\Sigma^{(J)}$, $J \neq I$

Constants

$\eta_{b,k}$ Efficiency [%] of battery k, $k = 1, 2$

η_{FC} Equivalent consumption conversion factor between mechanical and electrical power sources

$a_i^{g,j}$ Polynomial fitting factors to account for the fuel consumption rate of each generator set j, $i = 1, \cdots, 3$, $j = 1, 2$

a_i^{ICE} Polynomial fitting factors to account for the fuel consumption rate of marine *ICE*, $i = 1, \cdots, 6$

i_{ICE} *ICE* gearbox ratio

i_{IM} *IM* gearbox ratio

K Number of batteries

k_1	*ICE* controller gain (see (5.11))
k_2	*ICE* controller gain (see (5.11))
k_3	*IM* controller gain (see (5.13))
$p_{g,j}$	Number of poles of each generator set j, $j = 1, 2$
$\bar{P}_i$	Maximum rated power of the internal combustion engine in $[W]$
$\bar{P}_m$	Maximum rated power of the *IM* in $[W]$
Δt	Timestep in $[sec]$
ϵ_{inl}	Parasitic effectiveness of the heat exchange between inlet duct and the air
η	Thermal efficiency incorporating both the combustion and heat release processes in $[\%]$
η_T	Efficiency of the transmission system
η_{com}	Mechanical efficiency of the compressor
κ_a	Specific heat ratio of the air
κ_g	Specific heat ratio of the exhaust gas
τ_X	Fuel injection time delay in $[sec]$
τ_{p_d}	Time delay for filling the exhaust receiver in $[sec]$
τ_{TC}	Compressor time delay in $[sec]$
a_Z	Zinner turbine area decrease factor
a_η	Polynomial coefficient of the turbocharger for estimating its efficiency
$a_{B,0}$	Battery *SOC* to voltage linear correlation coefficient in $[V]$
$a_{B,1}$	Battery *SOC* to voltage linear correlation coefficient in $[V]$
A_{eff}	Turbine's effective area in $[m^2]$
$a_{G,i}$	Generator set constant, $i = 0, 1$
a_{tur}	Polynomial coefficient of the isentropic turbine efficiency

b_η	Polynomial coefficient of the turbocharger for estimating its efficiency
b_{tur}	Polynomial coefficient of the isentropic turbine efficiency
c	Propeller constant in $[N \cdot m \cdot sec^2]$
C_0	Battery capacity in $[A \cdot h]$
c_η	Polynomial coefficient of the turbocharger for estimating its efficiency
$c_{p,a}$	Specific heat at constant pressure for the scavenge air in $[J/kgK]$
c_{pg}	Specific heat at constant pressure for the exhaust gas in $[J/kgK]$
c_{tur}	Polynomial coefficient of the isentropic turbine efficiency
$c_{v,a}$	Specific heat at constant volume for the scavenge air in [J/kgK]
h_L	Lower heating value of fuel at ISO conditions in $[J/kg]$
H_r	Induction motor rotor reluctance in $[H]$
H_s	Induction motor stator reluctance in $[H]$
i_e	Number of *ICE* cylinders
I_X	Excitation current of the generator set in $[A]$
i_{gb}	Gearbox ratio
J_{GS}	Inertia of the generator set in $[kg \cdot m^2]$
J_{tot}	Total inertia of the engines, shaft, gearbox and propeller
k_e	Number of crank revolutions per *ICE* cycle
k_{GS}	Torque constant of the generator set
L	Inductance of the generator set in $[H]$
n_{bld}	Polytropic expansion coefficient of the blowdown process
n_{exp}	Polytropic exponent for expansion
n_{fe}^{nom}	Nominal rotational engine speed in $[rps]$
p	Number of poles of the induction motor

p_{amb}	Ambient air pressure in $[Pa]$
p_{ex}	Pressure after the turbocharger in $[Pa]$
P_{fe}^{nom}	nominal power output of the engine in $[W]$
Q_{loss}^{grad}	Gradient of mechanical losses of the engine in [Nm]
Q_{loss}^{nom}	Nominal mechanical losses of the engine in [Nm]
R_a	Gas constant of air in $[J/kgK]$
R_B	Battery resistance in $[\Omega]$
r_c	Effective compression ratio determined by the inlet valve timing
R_g	Gas constant of the exhaust gas in $[J/kgK]$
R_r	Induction motor rotor resistance in $[\Omega]$
R_s	Induction motor stator resistance in $[\Omega]$
r_{eo}	Ratio of the volume at Seiliger point 6
$R_{GS,int}$	Internal resistance of the generator set in $[\Omega]$
s	Induction motor slip
SFC^{nom}	Nominal fuel consumption of the ICE in $[kg/W \cdot h]$
T_c	Charge air temperature after the intercooler in $[K]$
T_{amb}	Ambient air temperature in $[Pa]$
T_{inl}	Temperature of the inlet duct that heats the inducted air in $[K]$
T_{sl}	Temperature of the air slip during scavenging in $[K]$
v_1	Cylinder volume at start of compression in $[m^3]$
$V_{GS,ref}$	Reference voltage of the generator set in $[V]$
$x_{nom}^{(1)}$	Amount of fuel injected per cylinder per engine cycle in $[kg]$ under nominal engine conditions
X_{ct}^{nom}	Nominal constant temperature portion of Seilinger thermodynamic cycle
X_{cv}^{grad}	Gradient constant volume portion of Seilinger thermodynamic cycle

X_{cv}^{nom} Nominal constant volume portion of Seilinger thermodynamic cycle

Variables

α Generator sets utilisation factor $[\%]$

ΔE Energy deficit in $[J]$

ΔP_{aux} Variation of the required auxiliary power during the vessel's mission in $[W]$

$\epsilon_{\tilde{x}}^{(2)}$ *ICE* state reference tracking error vector

$\epsilon_{z}^{(5)}$ *IM* state reference tracking error

σ Switching vector

f_{grid} Required grid frequency in $[Hz]$

$m_{T,K}$ Fuel consumption of the *PPP* in $[kgfuel]$

$P_{aux,c}$ Mean required auxiliary power during the vessel's mission in $[W]$

P_{aux} Power requirements dictated by the power profile for auxiliary functions in $[W]$

$P_{b,k}$ Power split of the requested power profile that's assigned to batteries in $[W]$, $k = 1,2$

P_D Power requirements dictated by the power profile for propulsion in $[W]$

$P_{g,j}$ Power split of the requested power profile that's assigned to the generator sets in $[W]$, $j = 1,2$

P_{ICE} Power split of the requested power profile that's assigned to the *ICE* in $[W]$

$P_{IM,mec}$ Power split of the requested power profile that's assigned to the *IM* in $[W]$

P_{tot} Power requirements dictated by the power profile for propulsion and auxiliary functions in $[W]$

$ref^{(2)}$ *ICE* torque reference

$ref^{(5)}$ *IM* shaft speed reference

$ref_j^{(7)}$	Voltage and shaft speed reference for each generator set j, $j = 1,2$
$ref_k^{(8)}$	Reference power for each battery k, $k = 1, \cdots, K$
V_{grid}	Required grid voltage in $[V]$
$m_{f,GS}$	Fuel index of the generator set in $[kg\ fuel]$
P_{GS}	Assigned power to the generator set (secondary level controller) in $[W]$
s_{sl}	Total slip ratio of the *ICE*
$u^{(1)}$	Fuel injection setting in $[\%]$
$u^{(5)}$	Input voltage of the induction motor in $[V]$
$u^{(8)}$	Requested power from the battery in $[W]$
$x^{(1)}$	Amount of fuel injected per cylinder per engine cycle in $[kg]$
$x^{(2)}$	Same as $x^{(6)}$. **Change of notation only for Chapter 5.**
$x^{(3)}$	Exhaust receiver pressure in $[Pa]$
$x^{(4)}$	Charge air pressure after the compressor in $[Pa]$
$x^{(6)}$	Propeller shaft rotational speed
$x^{(7)}$	State vector expressing the torque of the internal combustion engine driving the generator set in $[Nm]$ and the rotational speed of the generator's shaft in $[rps]$
$x^{(8)}$	Battery *SOC* in $[\%]$
X_{ct}	Constant temperature portion of Seilinger thermodynamic cycle
X_{cv}	Constant volume portion of Seilinger thermodynamic cycle
$y^{(1)}$	Fuel injection sensor output in $[kg]$
$y^{(2)}$	Cylinder pressure, temperature and *ICE* torque sensor outputs in $[Pa]$, $[K]$, $[N \cdot m]$, respectively
$y^{(3)}$	Exhaust manifold pressure and temperature before and after the turbine sensor outputs in $[Pa]$ and $[K]$, respectively
$y^{(4)}$	Pressure after the compressor and temperature before and after the intercooler sensor outputs in $[Pa]$ and $[K]$, respectively

$y^{(5)}$ Sensor torque output of the induction motor in $[N \cdot m]$

$y^{(6)}$ Shaft speed sensor output in $[rps]$

$y^{(7)}$ Output of the hardware engine torque, generator torque, shaft speed and current sensors assigned to each generator sets in $[Nm]$, $[Nm]$, $[rps]$ and $[A]$ respectively.

$z^{(5)}$ Output torque of the induction motor in $[N \cdot m]$

$z^{(7)}$ Algebraic vector expressing the torque of the generator part in the generator set in Nm and the the generator output current in $[A]$

$z_1^{(2)}$ Pressure inside the *ICE*'s cylinders in $[Pa]$

$z_1^{(3)}$ Temperature before the turbine in $[K]$

$z_1^{(4)}$ Air temperature before the intercooler in $[K]$

$z_1^{(8)}$ Battery current in $[A]$

$z_2^{(2)}$ Temperature inside the *ICE*'s cylinders in $[K]$

$z_2^{(3)}$ Temperature after the turbine in $[K]$

$z_2^{(4)}$ Air temperature after the intercooler in $[K]$

$z_2^{(8)}$ Battery output voltage in $[V]$

$z_3^{(2)}$ Output torque of the *ICE* in $[N \cdot m]$

Qualitative sets and databases

$\mathcal{L}$ Features of interest for the vessel mission

$\mathcal{P}$ Capabilities of the vessel

$\mathcal{U}$ Input vector for the definition of a vessel mission

$\mathcal{Z}$ Mission parameters

Σ Vector space of σ

O_m Available vessel operational modes during the mission

$\mathcal{F}$ Semantic database of *PPP* components

$\mathcal{F}_p^{(s)}$ Semantic database of the selected system topology

$\mathcal{F}_A$	Semantic database of automation *PPP* components (control)
$\mathcal{F}_a$	Semantic database of actuator components
$\mathcal{F}_c$	Semantic database of controller components
$\mathcal{F}_e$	Semantic database of state-estimator components
$\mathcal{F}_m$	Semantic database of monitoring agent components
$\mathcal{F}_s$	Semantic database of sensor components
$\mathcal{F}_u$	Semantic database of post-control function components
$\mathcal{F}_v$	Semantic database of virtual sensor components
$\mathcal{F}_y$	Semantic database of pre-control function components
$\mathcal{F}_{p,i}$	Semantic database of system *PPP* components for the topology iteration i, $i = 1, \cdots, N_t$
$\mathcal{S}_F^{(I)}$	Faulty sensor set, result of the diagnosis process
$R^{(I)}$	Set of residuals

Semantic representation

η_D	Propulsive efficiency
$\mathcal{I}$	Active *PPP* configuration
$\mathcal{S}_R$	Sensor requirements for satisfying the inputs of virtual sensors
∇	Displacement of the vessel
ρ	Water density
a	Power relation between the vessel speed and required power
c_s	Current characteristics
D	Propeller diameter
f_h	Hull fouling factor
F_{tow}	Towing force
h	Water depth
K_Q	Propeller torque coefficient

K_T	Propeller thrust coefficient
O_e	Parameters of the operational environment
S_m	Travel route of the vessel
s_s	Wave characteristics
t_0	Starting time of a vessel mission
T_a	Ambient temperature
t_{end}	Ending time of a vessel mission
V_{O_m}	Speed of the vessel during each operational mode O_m
w_s	Wind characteristics
w_w	Waterway width
X	Transport object (e.g., cargo, passengers) by a vessel during its mission
X_v	Type of the vessel
$\hat{g}_p$	Estimation of possible unknown system dynamics
$\hat{x}$	Estimated system state
Υ	Mediums of knowledge graph G
ζ_c	Parameters used by the controller implementation (e.g. controller gains)
$\zeta_s^{(I)}$	Design parameters of the virtual sensor
E	Edges of knowledge graph G
f_c	Algorithm for deciding on which action to take next
G	Knowledge graph of *PPP* components
$G_{p,i}$	Knowledge graph of the topology iteration i, $i = 1, \cdots, N_t$
l	Control level
N_t	Number of candidate *PPP* topologies
ref	Reference trajectory of the system state

u	Control decision signal
V	Vertices of knowledge graph G
y	Plant feedback

List of abbreviations

A-ECMS	*Adaptive Equivalent fuel Consumption Minimisation Strategy*
AC	*Alternating current*
ADMM	*Alterating Direction Method of Multipliers*
ARR	*Analytical Redundancy Relation*
CI	*Computational Intelligence*
CPP	*Controllable Pitch Propeller*
CPS	*Cyber-Physical System*
DAE	*Differential-Algebraic Equations*
DC	*Direct Current*
DIVA	*Drive & automation Integrated Vessel Automation*
DoS	*Denial-of-Service*
DX	*Artificial Intelligence Diagnostic*
ECMS	*Equivalent fuel Consumption Minimisation Strategy*
EGR	*Exhaust Gas recirculation*
FDI	*Fault Detection and Isolation*
FSM	*Fault Signature Matrix*
GHG	*Green House Gas*
GNSS	*Global navigation satellite system*
ICE	*Internal Combustion Engine*
IM	*Induction Motor*
IMO	*International Maritime Organisation*
KPI	*Key Performance Indicator*
MPC	*Model-Predictive Control*
MVFP	*Mean Value First Principle*
NWO	*Dutch Research Council*
ODE	*Ordinary Differential Equations*
PID	*Proportional–integral–derivative*
PPP	*Power and Propulsion Plant*
QoS	*Quality of Service*
RUL	*Remaining useful life*
SCR	*Selective Catalytic Reduction*
SFDI	*Sensor Fault Diagnosis*
SIVIA	*Set Inversion via Interval Analysis*
SM	*Signature Matrices*
SOC	*State of Charge*
SOLAS	*International Convention for the Safety of Life at Sea*
SVM	*Support Vector Machine*
TRL	*Technology Readiness Level*

Summary

This thesis proposes a set of safe and resilient control methods for marine *Power and Propulsion Plant*s (*PPP*s) to facilitate the ongoing energy transition, increase autonomy and enhance the operational safety of vessels.

In recent years, the *International Maritime Organisation* (*IMO*) issued regulations pushing for a reduction in CO_2-emissions of 40% by 2030 and a simultaneous reduction of 70% carbon emissions and of 50% Green House Gas emissions, by 2050. In order to adapt to the updated requirements, the interest of the maritime industry is shifting to alternative fuels as well as novel power and propulsion system technologies (e.g., dual-fuel engines). However, what technologies will prevail for each type and size of vessel is still greatly uncertain and the industry is in paralysis.

Meanwhile, the degree of autonomy onboard marine vessels is expected to increase in the following years. To this end, the control infrastructure of *PPP*s will be enhanced by multiple cyberdevices, communication and computation mechanisms, allowing for automated decisions. These decisions can be analyzed in three categories based on their time scale; **(i)** long-term decisions (years to decades) due to changes in regulations and available technologies, **(ii)** medium-term decisions (days to years) regarding changes in the vessel's missions, and **(iii)** short-term decisions (minutes to days) considering the occurrence of malfunctions affecting the cyber-physical *PPP*s infrastructure, such as faults and cyberattacks. Thus, the research question addressed in this thesis is: *"How to design safe and resilient autonomous control systems to handle the uncertain future adaptations in vessel automation and to compensate for malfunction effects without human intervention?"*

Through the analysis of the monitoring and control schemes typically involved in marine *PPP*s, non-centralised control and monitoring approaches are mostly discussed in this thesis. This design choice is made considering the large-scale of the systems involved, their multiple interconnections, and safety considerations. The considered dynamic models follow a *Differential-Algebraic Equations* (*DAE*) representation, and are thus associated with high non-linearity and complexity. Under certain application scenarios and in order to handle this complexity, a complementary qualitative system representation is used, based on semantics.

In this thesis, the proposed methods are organised in different chapters and

address either safety or resilience.

Safe control of marine *PPP*s

Considering the safety of the *PPP* operation, a distributed model-based *Sensor Fault Diagnosis* (*SFDI*) methodology for the diagnosis of faults affecting multiple sensors used for condition monitoring and control of marine *Internal Combustion Engine*s (*ICE*s). For every *ICE* subsystem, the detection of sensor faults relies on the design of cyber agents, where every agent monitors one subsystem. To handle the heterogeneous dynamics of each subsystem in the fault detection decision-making process, each agent uses differential and algebraic residuals alongside adaptive bounds. For isolation purposes, a combinatorial decision logic is employed, realized in two cyber levels: the local and the global decision logic. The first aims at the recognition of all sensor fault patterns that might have affected the engine based on the local agent fault signatures and certain binary decision matrices. The latter is used to capture the propagation of sensor faults between the different monitoring agents. The design of the monitoring agents is assessed, using performance analysis tools, in terms of the detectability and isolability of multiple sensor faults.

In order to further enhance the optimality of the diagnosis approach, this thesis proposes a greedy stochastic optimization algorithm for the sensor set decomposition used in the sensor fault monitoring of marine propulsion systems, based on fault isolability criteria. These criteria are expressed mathematically in terms of the number of unique columns in the theoretical *Fault Signature Matrices* (*FSM*s) used during the sensor fault isolation process. The *FSM*s of both isolation levels are, thus, formulated as an integrated optimization problem. Each solution regarding the sensor set decomposition is used to generate the respective distributed monitoring architecture, using semantic knowledge for the propulsion plant. Moreover, based on the design of the distributed monitoring architecture, the respective theoretical *FSM*s (quantitative) are automatically generated and used for the evaluation of the objective function.

Resilient control of marine *PPP*s

Regarding short-term decisions due to the effects of sensor faults, this thesis proposes a multi-agent fault-resilient control architecture for use in marine propulsion plants. The architecture is composed of the control scheme itself and the multi-sensory switching logic. From the control perspective, a multi-agent control scheme is employed consisting of two levels; the primary and secondary levels. A rule-based design is employed in the secondary control level to perform the power split between the *ICE* and the *Induction Motor* (*IM*). The primary level

consists of two novel, model-based and distributed control agents, designed using feedback linearization. Then, the design of the multi-sensory switching logic is aimed at providing both system and control stability guarantees. The multi-sensory scheme, considered in this research work, integrates both hardware and virtual sensors. Moreover, analytical conditions are derived for control stability, based on well-established Lyapunov stability criteria and used alongside other conditions for safe and efficient system operation.

For responding to mission changes, this thesis presents the design of an intelligent decision-support framework to assist marine engineers and vessel operators in updating the topology and control systems' design of marine power and propulsion plants. The connection between the topology and control design perspectives is enabled using semantics. From the control aspect, an intelligent automation supervisor is designed to make both offline and online decisions regarding the energy deficit to execute a new mission and the active automation configuration during operation. For offline decisions, topology modifications are requested by the vessel designers to cover the calculated energy deficit. During operation, switching between hardware and virtual sensors as well as switching between energy management controllers is implemented to handle the effects of sensor faults or *Denial-of-Service* (*DoS*) conditions on the onboard energy storage.

Overall, the proposed safe and resilient control architectures in the context of this thesis enable the seamless adaptation of marine *PPP*s to updated power requirements, system changes and unexpected events. Under the occurrence of multiple sensor faults, the designed *SFDI* methodology manages to diagnose the simulated faults with minimal detection delays and adequate isolation performance. In addition, using the analytical redundancy of the system and the multi-sensory switching logic, the fault effects are properly compensated while maintaining system and control stability. Finally, under changes in the mission characteristics, the intelligent automation supervisor is able to provide both offline and online decisions, concerning topology adaptations and malfunctions, respectively. Therefore, this research improves the safety and resilience of marine *PPP*s and is a significant step towards the concept of "smart shipping".

Samenvatting

Dit proefschrift stelt een reeks veilige en veerkrachtige controlemethoden voor maritieme *Power and Propulsion Plant*s (*PPP*s) om de huidige energietransitie te faciliteren, de autonomie te vergroten en de operationele veiligheid van schepen te verbeteren.

In de afgelopen jaren heeft de *International Maritime Organisation* (*IMO*) regelgeving uitgevaardigd die streeft naar een vermindering van CO_2-emissies met 40% in 2030 en een gelijktijdige vermindering van 70% koolstofemissies en 50% broeikasgasemissies tegen 2050. Om zich aan de bijgewerkte eisen aan te passen, verschuift de interesse van de maritieme industrie naar alternatieve brandstoffen en nieuwe aandrijfsystemen (bijvoorbeeld dual-fuel motoren). Het is echter nog steeds zeer onzeker welke technologieën voor elk type en formaat schip de voorkeur zullen krijgen, en de industrie is in afwachting.

Ondertussen verwacht men dat de mate van autonomie aan boord van maritieme schepen in de komende jaren zal toenemen. Daartoe zal de controle-infrastructuur van *PPP*s worden verbeterd door meerdere cyberapparaten en communicatie- en rekenmechanismen, waardoor geautomatiseerde beslissingen mogelijk worden. Deze beslissingen kunnen in drie categorieën worden geanalyseerd op basis van hun tijdschaal: **(i)** lange termijn beslissingen (jaren tot decennia) als gevolg van veranderingen in regelgeving en beschikbare technologieën, **(ii)** middellange termijn beslissingen (dagen tot jaren) met betrekking tot veranderingen in de missies van het schip, en **(iii)** korte termijn beslissingen (minuten tot dagen) rekening houdend met het optreden van storingen die de cyberfysieke *PPP*s infrastructuur beïnvloeden, zoals storingen en cyberaanvallen. De onderzoeksvraag die in dit proefschrift wordt behandeld, is: *"Hoe kunnen veilige en veerkrachtige autonome controlesystemen worden ontworpen om de onzekere toekomstige aanpassingen in scheepsautomatisering aan te kunnen en om storingen zonder menselijke tussenkomst te compenseren?"*

Door de analyse van de monitorings- en controleschema's die typisch betrokken zijn bij maritieme *PPP*s, worden in dit proefschrift voornamelijk gedecentraliseerde controle- en monitoringsbenaderingen besproken. Deze ontwerpkeuze is gemaakt met inachtneming van de grootschaligheid van de betrokken systemen, hun meerdere verbindingen en veiligheidsconsideraties. De bestuurkade dynamische model-

len volgen een *Differential-Algebraic Equations* (*DAE*) representatie en zijn dus geassocieerd met hoge niet-lineariteit en complexiteit. Om met deze complexiteit om te gaan, wordt onder bepaalde toepassingsscenario's een complementaire kwalitatieve systeemrepresentatie gebruikt op basis van semantiek. De combinatie van de twee modelleringsbenaderingen maakt de ontwinkkeling van veilige en veerkrachtige controlebenaderingen mogelijk.

In dit proefschrift zijn de voorgestelde methoden onderverdeeld in verschillende hoofdstukken en richten zich op ofwel veiligheid ofwel veerkracht.

Veilige controle van maritieme *PPP*s

Met het oog op de veiligheid van de *PPP* operatie, wordt een gedistribueerde modelgebaseerde *Sensor Fault Diagnosis* (*SFDI*) methodologie voorgesteld voor de diagnose van storingen die meerdere sensoren beïnvloeden die worden gebruikt voor conditiebewaking en controle van maritieme *Internal Combustion Engine*s (*ICE*s). Voor elk *ICE* subsysteem berust de detectie van sensorfouten op het ontwerp van cyberagenten, waarbij elke agent één subsysteem bewaakt. Om de heterogene dynamiek van elk subsysteem in het sensorfoutdetectie-besluitvormingsproces aan te pakken, gebruikt elke agent differentiële en algebraïsche residuen naast adaptieve grenzen. Voor isolatiedoeleinden wordt een combinatorische besluitlogica gebruikt, gerealiseerd in twee cyberniveaus: de lokale en de globale besluitlogica. De eerste is gericht op de herkenning van alle sensorfoutpatronen die de motor kunnen hebben beïnvloed op basis van de lokale agent foutsignaturen en bepaalde binaire beslissingsmatrices. De laatste wordt gebruikt om de voortplanting van sensorfouten tussen de verschillende bewakingsagenten vast te leggen. Het ontwerp van de bewakingsagenten wordt beoordeeld met behulp van prestatie-analysetools, in termen van de detecteerbaarheid en isoleerbaarheid van meerdere sensorfouten.

Om de diagnosebenadering verder te optimaliseren, presenteert dit proefschrift een gretig stochastisch optimalisatiealgoritme voor voor de sensor set decompositie die wordt gebruikt bij de sensorfout monitoring van maritieme voortstuwingssystemen, op basis van criteria voor foutisolatie. Deze criteria worden wiskundig uitgedrukt in termen van het aantal unieke kolommen in de theoretische *Fault Signature Matrices* (*FSM*s) die tijdens het sensorfout isolatieproces worden gebruikt. De *FSM*s van beide isolatieniveaus worden dus geformuleerd als een geïntegreerd optimalisatieprobleem. Elke oplossing met betrekking tot de sensordecompositie wordt gebruikt om de respectieve gedistribueerde monitoringarchitectuur te genereren, waarbij semantische (kwalitatieve) kennis van de voortstuwingssystemen wordt gebruikt. Bovendien worden, op basis van het ontwerp van de gedistribueerde monitoringarchitectuur, de respectieve theoretische *FSM*s (kwantitatief) automatisch gegenereerd en gebruikt voor de evaluatie van de doelfunctie.

Veerkrachtige controle van maritieme *PPP*s

Met betrekking tot kortetermijnbeslissingen vanwege de effecten van sensorfouten, stelt dit proefschrift een multi-agent storingsveerkrachtige controlearchitectuur voor, te gebruiken in maritieme voortstuwingsinstallaties. De architectuur is samengesteld uit het controleschema zelf en de multisensor schakelingslogica. Vanuit controleperspectief wordt een multi-agent controleschema gebruikt dat bestaat uit twee niveaus; het primaire en het secundaire niveau. Een op regelsgebaseerd ontwerp wordt gebruikt in het secundaire controleniveau om de vermogensverdeling tussen de *ICE* en de *Induction Motor* (*IM*) uit te voeren. Het primaire niveau bestaat uit twee nieuwe, modelgebaseerde en gedistribueerde controleagents, ontworpen met behulp van feedback linearisatie. Vervolgens is het ontwerp van de multisensor schakelingslogica gericht op het bieden van zowel systeem- als controlestabiliteitsgaranties. Het multisensor schema dat in dit onderzoek wordt overwogen, integreert zowel hardware- als virtuele sensoren. Bovendien worden analytische voorwaarden afgeleid voor controlestabiliteit, gebaseerd op algemeen aanvaarde Lyapunov stabiliteitscriteria en gebruikt naast andere voorwaarden voor veilige en efficiënte systeembediening.

Om te reageren op missie veranderingen, presenteert dit proefschrift het ontwerp van een intelligent beslissingsondersteunend raamwerk om maritieme ingenieurs en scheepsexploitanten te helpen bij het bijwerken van de topologie en het ontwerp van controlesystemen van maritieme kracht- en voortstuwingsinstallaties. De verbinding tussen de topologie en het controleontwerp wordt mogelijk gemaakt met behulp van semantiek. Vanuit controleperspectief wordt een intelligente automatiseringssupervisor ontworpen om zowel offline als online beslissingen te nemen over het energietekort om een nieuwe missie uit te voeren en de actieve automatiseringsconfiguratie tijdens de operatie. Voor offline beslissingen worden topologiemodificaties aangevraagd door de scheepsontwerpers om het berekende energietekort te dekken. Tijdens de operatie wordt schakelen tussen hardware- en virtuele sensoren evenals schakelen tussen energiebeheercontrollers geïmplementeerd om de effecten van sensorfouten of *Denial-of-Service* (*DoS*) condities op de energieopslag aan boord te behandelen.

Over het algemeen stellen de voorgestelde veilige en veerkrachtige controlearchitecturen in de context van dit proefschrift de naadloze aanpassing van maritieme *PPP*s aan bijgewerkte energie-eisen, systeemveranderingen en onverwachte gebeurtenissen mogelijk. Bij het optreden van meerdere sensorfouten slaagt de ontworpen *SFDI* methodologie erin om de gesimuleerde storingen te diagnosticeren met minimale detectievertragingen en adequate isolatieprestaties. Bovendien worden door

gebruik te maken van de analytische redundantie van het systeem en de multisensor schakelingslogica, de effecten van storingen op de juiste manier gecompenseerd terwijl systeem- en controlestabiliteit wordt behouden. Ten slotte, onder veranderingen in de missiekenmerken, is de intelligente automatiseringssupervisor in staat om zowel offline als online beslissingen te nemen met betrekking tot topologieaanpassingen en storingen. Daarom verbetert dit onderzoek de veiligheid en veerkracht van maritieme *PPP*s en is het een belangrijke stap richting het concept van "smart shipping".

Curriculum vitae

Nikos Kougiatsos received his integrated B.Sc. and M.Sc. degree in Naval Architecture and Marine Engineering from the National Technical University of Athens, Greece, in 2020. Since October 2020, he has been a Ph.D. Candidate in the Department of Maritime and Transport Technology at Delft University of Technology, The Netherlands. He is actively involved in the research project titled "**R**obust, **E**ffective, and **A**daptable ship **D**es**I**gns for u**N**c**E**rtain tran**S**ition path**S**" (READINESS). His current research interests focus on distributed fault diagnosis of cyber-physical systems, fault-tolerant control, non-centralized and modular control architectures, particularly applied to waterborne transport systems.

Mr. Nikos Kougiatsos is an Associate member of the Society of Naval Architects and Marine Engineers (SNAME). During his Master studies, he was awarded two scholarships from the American Bureau of Shipping (ABS) and the Ch. Papakyriakopoulou scholarship in recognition of his academic performance.

Publications

Journal papers

1. **N. Kougiatsos**, and V. Reppa, "A Distributed Cyber-Physical Framework for Sensor Fault Diagnosis of Marine Internal Combustion Engines," IEEE Trans. Control Syst. Technol. SI Resilient Control Cyber Phys. Power Energy Syst., pp. 1–12, 2024.

2. **N. Kougiatsos**, M. Vagia, R.R. Negenborn, and V. Reppa, "Sensor fault-resilient multi-agent control for marine hybrid propulsion plants," submitted to a journal, 15 pp., 2024.

3. **N. Kougiatsos**, E.L Scheffers, M.C. van Benten, D.L. Schott, P. de Vos, R.R. Negenborn, and V. Reppa, "An intelligent agent-based resilient framework for marine vessel mission adaptations," submitted to a journal, 21 pp., 2024.

Conference papers

1. **N. Kougiatsos**, R.R. Negenborn, and V. Reppa,"Distributed model-based sensor fault diagnosis of marine fuel engines," IFAC-PapersOnLine, 55(6), 347-353, 2022.

2. **N. Kougiatsos** and V. Reppa, "A distributed virtual sensor scheme for marine fuel engines," IFAC-PapersOnLine, vol. 55, no. 31, pp. 333–338, 2022

3. **N. Kougiatsos**, R. R. Negenborn, and V. Reppa. "A Multi-Sensory Switching-stable Architecture for Distributed Fault Tolerant Propulsion Control of Marine Vessels." Proceedings of the 2022 International Ship Control Systems Symposium, Delft, the Netherlands. Vol. 16. 2022.

4. M. C. van Benten, **N. Kougiatsos**, and V. Reppa. "Mission-oriented Modular Control of Retrofittable Marine Power Plants." in: Proceedings of the 2022 International Ship Control Systems Symposium, Delft, the Netherlands. Vol. 16. 2022.

5. **N. Kougiatsos**, J. Zwaginga, J. Pruyn, and V. Reppa, "Semantically enhanced system and automation design of complex marine vessels," in: Proceedings of the 2023 IEEE Symposium Series on Computational Intelligence, Mexico City, Mexico, pp. 512-518, 2023.

6. **N. Kougiatsos** and V. Reppa, "Sensor Set Decomposition for Enhanced Distributed Sensor Fault Isolability of Marine Propulsion Systems," in: Proceedings of the 2024 IFAC SAFEPROCESS, Ferrara, Italy, pp. 55–60, 2024.

TRAIL Thesis Series

The following list contains the most recent dissertations in the TRAIL Thesis Series. For a complete overview of more than 400 titles, see the TRAIL website: www.rsTRAIL.nl.

The TRAIL Thesis Series is a series of the Netherlands TRAIL Research School on transport, infrastructure and logistics.

Kougiatsos, N., *Safe and Resilient Control for Marine Power and Propulsion Plants*, T2024/12, November 2024, TRAIL Thesis Series, the Netherlands

Uijtdewilligen, T., *Road Safey of Cyclists in Dutch Cities*, T2024/11, November 2024, TRAIL Thesis Series, the Netherlands

Liu, X., *Distributed and Learning-based Model Predictive Control for Urban Rail Transit Networks*, T2024/10, October 2024, TRAIL Thesis Series, the Netherlands

Clercq, G. K. de, *On the Mobility Effects of Future Transport Modes*, T2024/9, October 2024, TRAIL Thesis Series, the Netherlands

Dreischerf, A.J., *From Caveats to Catalyst: Accelerating urban freight transport sustainability through public initiatives*, T2024/8, September 2024, TRAIL Thesis Series, the Netherlands

Zohoori, B., *Model-based Risk Analysis of Supply Chains for Supporting Resilience*, T2024/7, October 2024, TRAIL Thesis Series, the Netherlands

Poelman, M.C., *Predictive Traffic Signal Control under Uncertainty: Analyzing and Reducing the Impact of Prediction Errors*, T2024/6, October 2024, TRAIL Thesis Series, the Netherlands

Berge, S.H., *Cycling in the age of automation :Enhancing cyclist interaction with automated vehicles through human-machine interfaces*, T2024/5, September 2024, TRAIL Thesis Series, the Netherlands

Wu, K., *Decision-Making and Coordination in Green Supply Chains with Asymmet-*

ric Information, T2024/4, July 2024, TRAIL Thesis Series, the Netherlands

Wijnen, W., *Road Safety and Welfare*, T2024/3, May 2024, TRAIL Thesis Series, the Netherlands

Caiati, V., *Understanding and Modelling Individual Preferences for Mobility as a Service*, T2024/2, March 2024, TRAIL Thesis Series, the Netherlands

Vos, J., *Drivers' Behaviour on Freeway Curve Approach*, T2024/1, February 2024, TRAIL Thesis Series, the Netherlands

Geržinič, N., *The Impact of Public Transport Disruptors on Travel Behaviour*, T2023/20, December 2023, TRAIL Thesis Series, the Netherlands

Dubey, S., *A Flexible Behavioral Framework to Model Mobilityon-Demand Service Choice Preference*, T2023/19, November 2023, TRAIL Thesis Series, the Netherlands

Sharma, S., *On-trip Behavior of Truck Drivers on Freeways: New mathematical models and control methods*, T2023/18, October 2023, TRAIL Thesis Series, the Netherlands

Ashkrof, P., *Supply-side Behavioural Dynamics and Operations of Ride-sourcing Platforms*, T2023/17, October 2023, TRAIL Thesis Series, the Netherlands

Sun, D., *Multi-level and Learning-based Model Predictive Control for Traffic Management*, T2023/16, October 2023, TRAIL Thesis Series, the Netherlands

Brederode, L.J.N., *Incorporating Congestion Phenomena into Large Scale Strategic Transport Model Systems*, T2023/15, October 2023, TRAIL Thesis Series, the Netherlands

Hernandez, J.I., *Data-driven Methods to study Individual Choice Behaviour: with applications to discrete choice experiments and Participatory Value Evaluation experiments*, T2023/14, October 2023, TRAIL Thesis Series, the Netherlands

Aoun, J., *Impact Assessment of Train-Centric Rail Signaling Technologies*, T2023/13, October 2023, TRAIL Thesis Series, the Netherlands

Pot, F.J., *The Extra Mile: Perceived accessibility in rural areas*, T2023/12, September 2023, TRAIL Thesis Series, the Netherlands

Nikghadam, S., *Cooperation between Vessel Service Providers for Port Call Performance Improvement*, T2023/11, July 2023, TRAIL Thesis Series, the Netherlands

Li, M., *Towards Closed-loop Maintenance Logistics for Offshore Wind Farms: Approaches for strategic and tactical decision-making*, T2023/10, July 2023, TRAIL

Thesis Series, the Netherlands

Berg, T. van den, *Moral Values, Behaviour, and the Self: An empirical and conceptual analysis*, T2023/9, May 2023, TRAIL Thesis Series, the Netherlands

Shelat, S., *Route Choice Behaviour under Uncertainty in Public Transport Networks: Stated and revealed preference analyses*, T2023/8, June 2023, TRAIL Thesis Series, the Netherlands

Zhang, Y., *Flexible, Dynamic, and Collaborative Synchromodal Transport Planning Considering Preferences*, T2023/7, June 2023, TRAIL Thesis Series, the Netherlands

Kapetanović, M., *Improving Environmental Sustainability of Regional Railway Services*, T2023/6, June 2023, TRAIL Thesis Series, the Netherlands

Li, G., *Uncertainty Quantification and Predictability Analysis for Traffic Forecasting at Multiple Scales*, T2023/5, April 2023, TRAIL Thesis Series, the Netherlands

Harter, C., *Vulnerability through Vertical Collaboration in Transportation: A complex networks approach*, T2023/4, March 2023, TRAIL Thesis Series, the Netherlands