Article

Not peer-reviewed version

Regulating Cyberworthiness: Governance Frameworks for Safety-Critical Cyber-Physical Systems

Mark Van Zomeren , Felicity Deane , Keith Francis Joiner * , Li Qiao , Rachel Horne , Emiliya Suprun

Posted Date: 5 August 2025

doi: 10.20944/preprints202508.0294.v1

Keywords: cyber; safety; cybersecurity; cyberworthiness; cyber-physical; complex; governance; regulation; cybernetics; resilience

 doi:10.20944/preprints202508.0294.v1

Article

Regulating Cyberworthiness: Governance Frameworks for Safety-Critical Cyber-Physical Systems

Mark van Zomeren [1], Felicity Deane [2], Keith Joiner [3,*], Li Qiao [4], Rachel Horne [2] and Emiliya Suprun [1]

[1] School of Systems and Computing, University of New South Wales, Northcott Drive, CAMPBELL, ACT 2612, Australia

[2] Queensland University of Technology, 2 George Street, Brisbane, QLD, 4000, Australia

[3] Capability Systems Centre, University of New South Wales, Northcott Drive, CAMPBELL, ACT, 2612, Australia

[4] School of Engineering and Technology, University of New South Wales, Northcott Drive, CAMPBELL, ACT 2612, Australia

* Correspondence: k.joiner@unsw.edu.au

Abstract

The objective of this paper is to frame research improving the governance of modern cyber-physical systems (CPS) and Complex Systems of CPS through better regulation and compliance. CPS are increasingly being used to undertake high-hazard activities that have the potential to cause significant impact on people and the environment. The analysis detailed in this paper provides insights into how maritime, aviation, and nuclear regulators from the United States of America, the European Union, and Australia, in particular, facilitate the global trend of integrating cyber components into the high-hazard physical systems they regulate. This insight is gained by undertaking a systematic document review and word search analysis of the regulations, codes, standards and guidance documents published or referred to by these regulators, relevant to the operation of the high-hazard CPS they regulate. These documents were selected to assess the importance that these regulators place on cybersecurity, cyber safety, and cyberworthiness. This analysis confirmed that current regulations primarily treat cyber and physical safety in isolation and generally perceive the application of cybersecurity as adequate for achieving safety for the cyber aspects of a CPS. This demonstrates the need for the application of more contemporary concepts, such as cyberworthiness, to the regulation of high-hazard CPS, as well as methods to pathologically assess and incrementally improve governance of such systems through approaches like Complex Systems Governance.

Keywords: cyber; safety; cybersecurity; cyberworthiness; cyber-physical; complex; governance; regulation; cybernetics; resilience

1. Introduction

Given the rapid pace of technological change for high-hazard cyber-physical systems (CPS), there are numerous potential avenues for research on how to govern their development, operation, sustainment, and eventual disposal. The primary research question being addressed in this paper is as follows:

How can Complex Systems Governance (CSG) principles inform cyber-resilience for use in cyber-physical applications undergoing constant technological change, that ensures:

1. Continuous validation of the status of cyber-physical safety?
2. Lifecycle traceability of cyber-resilience claims?

 doi:10.20944/preprints202508.0294.v1

3. Interoperability across multi-jurisdictional Complex Systems of Cyber-Physical Systems (CSoCPS)?

Note that both cyber-resilience and cyberworthiness are terms used somewhat interchangeably between Western nations as a measure of a capability's suitability to operate in its intended environment, where that intended environment includes a contested cyber domain [136]. The results obtained in addressing this research question will then be used to inform future research on how to best assess and measure the cyberworthiness of CSoCPS, which regulators may then utilize to evaluate compliance against their regulations. It is anticipated that the results of any additional research will be reported in future publications.

The paper first introduces the concept of modern CPS and the more complex CSoCPS, and their increasing use in high-hazard activities that have the potential to cause a significant impact on people and the environment. This paper then demonstrates the need for the application of more contemporary concepts, such as cyberworthiness, to the regulation of high-hazard CPS. That demonstration is achieved through the analysis of current regulatory practices for CPS through the lens of instructive contemporary case studies, as well as a content analysis of the regulations and guidance material of a representative group of domestic regulators of high-hazard CPS that have global reach.

In Section 2, we explain in more depth the concept of cyberworthiness and the research questions to be addressed by the analysis associated with this paper, including a regulator-focused definition of cyberworthiness. We further examine the role of CPS in modern society, highlighting the need in most instances for more regulation to ensure their safe operation. We also discuss the significance of applying cyberworthiness principles to their ongoing safety.

In Section 3, we examine the various ways CPS are currently being regulated. Using contemporary case studies, we demonstrate a current regulatory gap that exists due to the narrow application of cybersecurity practices in addressing CPS safety.

In Section 4, through the analysis of international organizations and their domestic counterparts that regulate high-hazard CPS, we demonstrate the limited focus on the cyber aspects of CPS when regulating high-hazard systems for safety. This section provides evidence of cyber-physical safety governance gaps in three international physical domains.

In Section 5 we look at potential principles-based cyberworthiness regulations that can be used by regulators to bridge the regulatory gaps highlighted in Sections 3 and 4. This section explains Complex Systems Governance approaches and an aligned cyberworthiness governance framework prototype that regulators of high-hazard CPS can utilize.

In Sections 6 and 7 the limitations of this paper are then discussed, along with useful future research and investigations that could be conducted to inform the future development of a cyberworthiness governance framework, and final conclusions are presented.

2. The Cyber-Physical Safety Challenge

As cyber components are increasingly integrated into existing physical systems for critical and non-critical system functions, the number of CPS is growing correspondingly. The Cisco Annual Internet Report (2018-2023) Public White Paper [1], indicates increased machine-to-machine (M2M) connections from 2018 to 2023. The number of M2M connections is used as a proxy for internet-connected CPS, indicating increasing growth in the number of CPS rather than actual CPS numbers. This report also shows that the proportion of M2M connections increased from 33% to 50% of all internet-connected devices over the same period, thus indicating a more rapid increase in CPS than traditional IT systems and devices. These numbers do not include M2M operating across networks that are not connected to the internet, so the total number of M2Ms is likely to be larger.

The rise of cyberspace as a more recent technological advance and its ongoing integration with the Physical domain manifests broadly into the Internet of Things (IoT). Hogan and Newton (2015) identify Advanced Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition (SCADA), and distributed control systems (DCS) components [2] as the primary interface

 doi:10.20944/preprints202508.0294.v1

between cyberspace and physical domains. This technology is broadly referred to as Operational Technology [3], distinct from traditional Information and Communication Technology (ICT) systems that are primarily focused on the storage, retrieval, computation, and transmission of data and information.

This Operational Technology interface gives rise to the broad concept of Industrial Control Systems (ICS) [4], CPS [5,6] and the interconnection of many CPS into a CSoCPS [7].

2.1. Cyber-Physical Systems

The cyber domain is increasingly merging with the physical domain through the rapid growth and widespread adoption of the IoT and more substantial CPS, which are critical to a safe and functional modern society. **Figure 1** provides a high-level depiction of ICT and operational technology components that can be found in a common modern CPS. For this article, the definition of a CPS is drawn from the US National Science Foundation, Ross, R. and V. Pillitteri, and Networking and Information Technology Research and Development, as follows:

> ***CPS*** *– are engineered systems that are built from and depend upon the seamless integration of computation and physical components [8]. They are systems that are interacting digital, analog, physical, and human components engineered for function through integrated physics and logic [5]. They can be smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications. In CPS systems, the joint behavior of the "cyber" and "physical" elements of the system is critical - computing, control, sensing and networking can be deeply integrated into every component, and the actions of components and systems must be safe and interoperable [9].*

While the cyber domain brings significant benefits to physical systems, such as enhanced coordination, efficiency, and autonomous capabilities, these benefits can also give rise to substantial hazards to the physical domain. CPS exhibit fragmented accountability due to multi-vendor supply chains (no unified safety case), lifecycle mismatches (i.e., 20-year physical assets compared to 3-year cyber refresh cycles). In part, this occurs because of the insidious evolution of malicious exploitation by cyber threat actors and the difficulty with which 'patching' and protective mitigations can be put in place by CPS operators and practitioners to mitigate these threats after CPS are already in operation, and after they become aware of 'new' or 'exploited' vulnerabilities.

 doi:10.20944/preprints202508.0294.v1

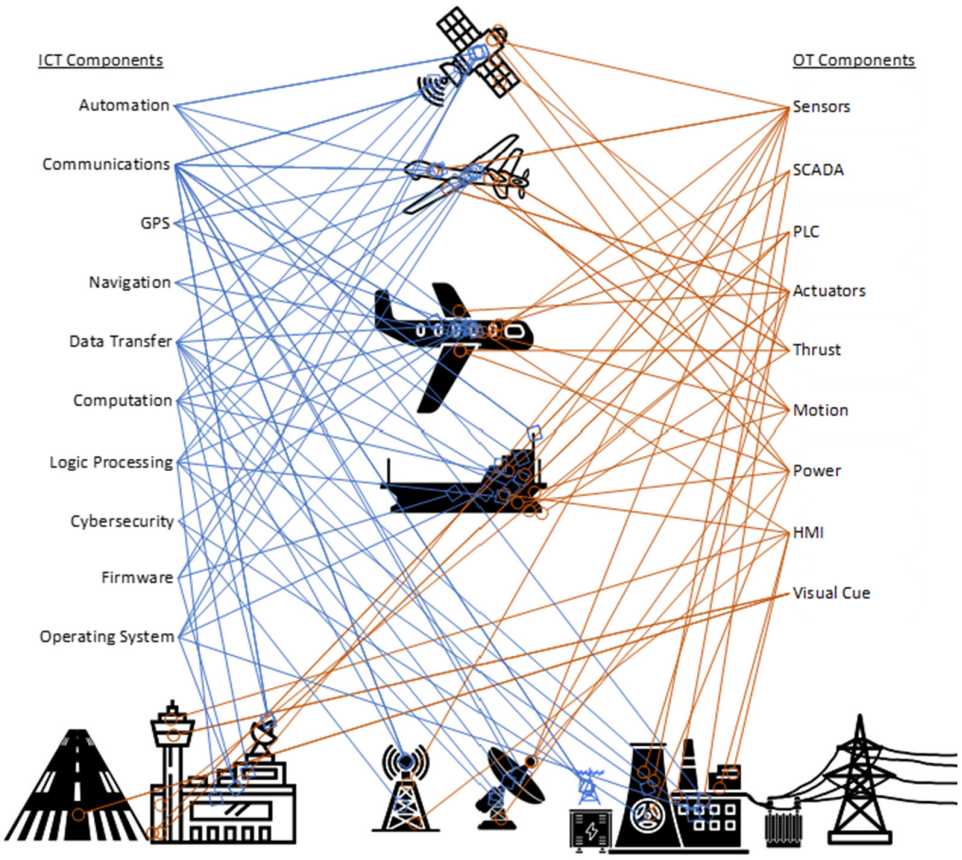

Figure 1. Example Cyber-Physical Systems and their high-level ICT and operational technology components labelled.

2.2. Complex Systems of Cyber-Physical Systems

Engell)[7] defines a CSoCPS as:

> ***Complex Systems of CPS*** *– complex systems of connected, or interacting, CPS that can exist across vast distances, and are engineered systems that are built from and depend upon the seamless integration of computation and physical components [7].*

The need to ensure the safety of CPSs is commensurate with the amount of harm that can be done to people and the environment if the system behaves in an unintended and detrimental manner. Individual instances of CPS include modern cars, aircraft, trains, and ships, while examples of CSoCPS include road systems, airports, rail systems, ports, hospitals, nuclear reactors, and the electricity grid supplying power to infrastructure CPS. **Figure 2** provides an example of how CPS form CSoCPS in modern society.

 doi:10.20944/preprints202508.0294.v1

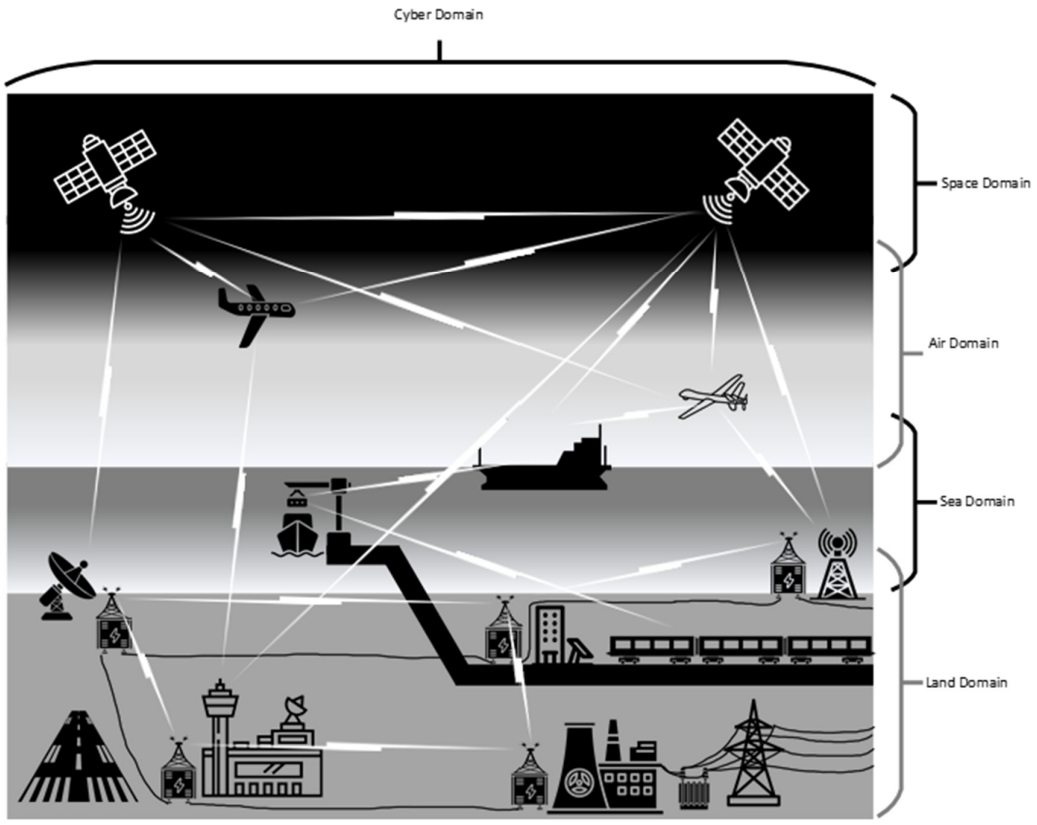

Figure 2. Interconnected CPS Creating CSoCPS showing the cyber domain spanning all macro physical domains. (Adapted from RMIT - https://sites.rmit.edu.au/cyber-physical-systems).

The convergence of the cyber and physical domains into highly complex CPSs provides unprecedented capability, with the associated benefit of increased productivity and enhanced ability for a broad range of human endeavors. However, these benefits do not come without significant potential hazards to the CPS, the environment, and the people who may encounter CPS. When considering the rapid increase in the number and variety of CPS, the potential for unintended harm takes on significant additional abstraction, complexity and uncertainty. The root causes of unintended harmful behavior in CPS may be traced back to obsolete interfacing systems or factors in the system's cyber-physical operating environment that were not considered during the system's development. Many of these hazards are novel and require careful management and mitigation to prevent catastrophic incidents from occurring.

2.3. Complex Systems Governance

Complex Systems Governance – can be applied to the operation and management of any complex system or complex system of systems, which CPS and CSoCPS inherently are. Complex Systems Governance foundations are in the theory of cybernetics developed in the 1950s by Ashby and considered to be an evolution of systems engineering [35]. Keating and Katina detail how the application of Complex Systems Governance provides a methodology to provide control, communication, coordination, and integration of a complex system using nine metasystem functions. The analysis in Section 4 of this paper utilizes three of the nine metasystem functions, namely, strategic monitoring, environmental monitoring, and operational performance, in the assessment of a representative set of regulations for high-hazard CPS.

 doi:10.20944/preprints202508.0294.v1

2.4. Cyberworthiness

CPS can range from a surgically implanted pacemaker to an electronic door lock, and from commercial airliners to spacecraft and nuclear power stations. Due to the high-hazard nature of many types of CPS, there is an increasing need to assure the public of their safe ongoing operation. Considering the importance of the safe operation of high-hazard CPS, safety regulators should actively keep up with technology trends and become informed about more contemporary concepts, such as the cyberworthiness of CPS. While cyberworthiness is not yet a widely used concept, Fowler and Sitnikova describe cyberworthiness in terms of the cyber resilience of critical cyber systems and the ability of an entity, regardless of its size and complexity, to manage its cyber resources effectively through adversity, including deliberate attacks. Building on Fowler and Sitnikova's concept of cyberworthiness and applying it to CPS in the context of the analysis undertaken for this article, the term ***Cyberworthiness*** shall be defined as a:

> *the overall state of operation and resilience of a cyber-physical system, or a complex system of cyber-physical systems, with specific regard to the ongoing and effective operation of all critical cyber components of the CPS, operating within a potentially contested and hostile cyberspace, to assure (to a tolerable level) the continuing and safe provision of the physical outputs of the cyber-physical system.*

Given the pace with which technology changes, it is challenging to regulate technology directly. Regulations may prohibit the introduction of new technologies or focus on the activities and behaviors of the people who effectively control the CPS over its complete lifecycle, with a focus on the people responsible for the development, maintenance, operation, and disposal of CPS. It follows that to regulate the cyberworthiness of CPS, it is critical to be able to measure the level of cyberworthiness of high-hazard CPS throughout the complete lifecycle of the CPS. Currently, this research considers and contributes to the argument that there are no specific high-hazard CPS regulations that comprehensively cover the intersection of cybersecurity and physical safety, fully accounting for the cyberworthiness of a high-hazard CPS. The definition provided above gives regulators an operational focus on the ongoing provision of safe physical outputs of CPS. This definition of cyberworthiness is tied to the demonstrable capability of a CPS and CSoCPS to:

1. Maintain safety-critical functions under cyber-induced disruptions
2. Distinguish security-safety dependencies and conflicts
3. Sustain evidence-based assurance across lifecycle phases

2.5. Proliferation of CPS in High-Hazard Applications

The critical infrastructure that supplies these high-hazard CPS with their physical outputs, in the form of services and utilities necessary for their safe and ongoing operation, is itself a high-hazard CPS. These cyber and physical interactions between high-hazard CPS also create high-hazard CSoCPS. If large enough numbers of normally innocuous CPS are connected into a CSoCPS, their numbers alone may give rise to emergent hazards that have not been contemplated and for which no mitigation has been developed or applied. Lithium batteries are a good example of this, as they are an actual CPS that would be practically useless without the associated control electronics. One lithium battery may not be considered hazardous. Still, a high concentration of many lithium batteries could constitute a significant hazard. If large numbers of lithium batteries were simultaneously compromised across a dispersed area through a coordinated cyberattack, the consequences could be catastrophic, quickly overwhelming any standard emergency response.

2.6. The Drawbacks of CPS

Combining the cyber domain with physical systems can have potentially catastrophic drawbacks. Allowing systems to rapidly update remotely on mass with insufficient testing and security may cause otherwise appropriately controlled physical systems, such as electric vehicles, to become unacceptably hazardous. Providing remote operation and unsupervised autonomy to

 doi:10.20944/preprints202508.0294.v1

existing hazardous systems, such as nuclear reactors, may allow for nuclear safety and security incidents that are catastrophic to major human populations worldwide. For these reasons, it is paramount that the worthiness of physical systems to utilize the cyber domain is meticulously tested and evaluated before initial operation and equally meticulously assured through regular operational tests and evaluations. Such test and evaluation regimes would assure operators, users, and regulators of high-hazard CPS of their cyberworthiness.

2.7. Inherent CPS Vulnerabilities

Inherent vulnerabilities in CPSs often relate to the relatively static nature of their ICT and Operational Technology systems once in operation and the difficulties associated with patching, upgrading, and testing legacy CPSs that interact with new CPSs brought into service [11]. Considering the benefits of networking many CPSs of varying types with one another and additional ICT systems to form CSoCPS, an operator of CPS may have large numbers of purposely networked CPSs, with the possibility of many more externally controlled ICT systems and other CPSs that have the potential to network with them. This means that the overall attack surface of the CCoCPS that the CPS belongs to is far larger than the attack surface of any individual CPS, causing them all to be vulnerable to a cyber-attack.

An additional vulnerability inherent to CPS is the potential for misalignment of the cybersecurity workforce and the (physical) technical workforce working on a CPS [12]. Very few individuals possess deep cybersecurity knowledge and a deep understanding of the critical failure modes of a given CPS, much less across sectors that utilize CPS. This problem is an inherent workforce and skills problem that is a key vulnerability in the ongoing cyberworthiness of CPS.

The prospect of cyber-attacks presents a unique inherent vulnerability of CPS, and this poses a specific, newer threat to operators, users, and people near high-hazard CPSs, as they have the potential to realize the hazards associated with the systems. Many types of actors might perform cyberattacks, and they may do so for various reasons and from a great distance from the CPS. Regardless of intent and motivation, unauthorized personnel or organizations in the ICT systems associated with the operation of high-hazard CPSs are highly undesirable and potentially catastrophic.

2.8. Ensuring the Cyberworthiness of CPS and CSoCPS

As cyberworthiness focuses on the assurance of the physical outputs of CPS, it is insufficient to determine the state of cybersecurity of the CPS' ICT systems and extrapolate the cyberworthiness of the CPS to be the same or similar. This inappropriateness is because cybersecurity focuses predominately on the confidentiality, integrity, and availability of an ICT system, known as the cybersecurity "triad". The assurance of this triad is insufficient to ensure the safety of the physical outputs of CPS. Conversely, indications that one of the cybersecurity triads (e.g., confidentiality of the data) of a CPS is compromised do not necessarily mean that the cyberworthiness of the CPS is compromised, since the confidentiality of the data associated with the ICT of the CPS may not be critical to its operations. So, while cybersecurity remains an important component of the cyberworthiness of a CPS, it is only one of many factors that may determine the cyberworthiness of a CPS. Other factors that need to be considered include the age and obsolescence of the ICT in the CPS, how ICT system updates are applied to the CPS, the operator's ability to understand and test the interactions between the CPS and other CPS, and the CPS's dependencies on other CPS.

2.9. Current Regulatory Landscape for CPS

The operators of high-hazard CPS typically have significant incentives to maintain their CPS as safe and operational as possible. These incentives range from profit-making to providing life-supporting services to supporting national security. In the case of high-hazard CPS, the system is typically required to provide a higher net benefit to compensate for the inherent system hazards that

 doi:10.20944/preprints202508.0294.v1

workers or the community must tolerate. It may, therefore, be expected that the operators of high-hazard CPS are more likely to have good internal organizational governance structures and are therefore more likely to demonstrate effective internal self-regulation for the safe operation of their CPS [13]. However, the safety of CPSs is not guaranteed through internal regulation alone, as shown later in this section (i.e., The Changing Environment and Disruptors). A regulator must consider many other factors and influences before it can be satisfied that overall CPS safety is assured, leaving operators and users vulnerable to weaknesses in these internal governance measures. These weaknesses may be driven by incentives for individuals and organizations not to operate their high-hazard CPS in a manner expected. For example, such practices could include reducing operating costs by failing to conduct proper maintenance practices or by not engaging the most appropriate cybersecurity specialists.

Furthermore, operators of high-hazard CPS may choose to continue operating system components beyond their point of obsolescence when they are no longer supported by the original equipment manufacturer and security patches are no longer available [14]. From the humble Radio Frequency Identification Device (RFID) to more complex CPS and CSoCPS, the safety implications of physical and cyber obsolescence must be adequately understood, considered, and planned for [15,16].

In Australia, the Security of Critical Infrastructure (SOCI) Rules 2025 [17] require critical infrastructure operators to establish and maintain a critical infrastructure risk management program, as well as enforce additional cybersecurity obligations on them. Current practices focus on preventing the occurrence and minimizing the impact of cybersecurity incidents. However, encouraging operators of CPS to become more mature, cybersecurity-minded organizations is not enough. Operators of CPS, and organizations that rely on CPS operated by others, need to develop a proper understanding of their role within the broader complex system of CPS, identify cyberworthiness issues that may affect their critical physical outputs, and actively implement measures that can meaningfully mitigate them.

3. Relevant Regulatory Practices

The regulators selected as part of the assessment in Section 4 have a broad range of regulatory tools at their disposal to regulate the CPS within their remit. In practice, these regulators will use a mix of these regulatory tools to achieve the best safety outcome given the type and magnitude of hazard they are seeking to have appropriately managed by the communities they regulate. In this section, we consider these tools in a broad sense, along with contemporary case studies, to demonstrate the difficulties in applying particular tools to specific CPS situations and to identify the most appropriate regulatory tools when seeking to apply regulations specific to cyberworthiness outcomes.

3.1. Regulatory Approaches to Assure the Safety of High-Hazard CPS for Safety

Regulation comes in many forms and is a category far broader than legislation. Indeed, regulation encapsulates "any rule endorsed by government where there is an expectation of compliance."[18] Often, regulators rely on a mix of self-regulation and external regulation to achieve the safety outcomes they seek to assure. Baldwin, Scott and Hood contend that Regulation is broadly:

> *'…the promulgation of rules accompanied by mechanisms for monitoring and enforcement.'[19] The phrase regulation can include a combination of laws, regulations, technical standards, policies and processes, that apply to a specific thing.*

Given the breadth of this definition, there are different forms of regulation, including those considered 'voluntary' or 'self-regulatory'. On the other end are 'coercive', 'deterrence-based' or 'command and control' measures. Both voluntary and command-and-control approaches could be considered prescriptive or otherwise. Two broad categories of regulation may impact the safety of a CPS. That is, regulation that is internal to the entity responsible for a CPS's safe development, operation, and disposal, and regulation imposed externally on the responsible entity.

 doi:10.20944/preprints202508.0294.v1

An external regulator may have legislative powers provided to it by a government, such as the US Coast Guard for ships operating in US coastal waters or registered in the US [20]. A second example is an international body such as the International Atomic Energy Agency for the safeguarding of nuclear material [21] who may regulate certain activities with the agreement of participating countries through treaties and other international agreements.

Peak industry bodies may behave as a regulator, empowered by the consensus of the broad industry participants that operate similar high-hazard CPS that deal with similar hazards, such as the colleges of surgeons or the oil and gas industry [22]. In these instances, there may be a driving incentive within the regulated community to ensure strong internal regulation at the industry level to safeguard against more stringent and potentially prohibitive legislative regulations being imposed externally. This self-regulation may occur due to community pressure following a significant incident involving a particular type of CPS [23].

For both internal and external regulation, there are two primary ways that the regulations can be applied; either voluntarily through the regulated community's strict adherence to published regulations or codes of practice, or through permissive regulation, where the applicable regulator permits the regulated community to undertake hazardous activities in a way that is bespoke to their specific hazards and circumstances. Many high-hazard CPS can operate across international borders or cause a significant impact across multiple jurisdictions. Hence, they must comply with local regulations in whichever jurisdiction they operate and concurrently adhere to international conventions when operating in international areas, such as trains, commercial aircraft, and maritime vessels.

As Mathews notes, it is generally accepted in regulatory literature that the type and extent of direct government regulation should be commensurate with the complexity of the risk and the magnitude of harm that could be caused by, or hazards associated with, the activity being regulated [24]. The operation of CPS may be considered high-risk in certain circumstances, which may warrant the application of regulation to the CPS and its operators. For example, the harm that could be caused if the CPS ceases to operate such that its physical outputs are not available for use, and the loss of these physical outputs creates a hazard. Accordingly, it is the operators of higher-hazard CPSs that need to demonstrate their cyberworthiness to a regulator, and this is likely best achieved through externally applied principles-based regulation that focuses on self-governance [25] settings. Such regulation ought to require regulated entities to demonstrate that these CPS are adequate for addressing the magnitude of the hazards being managed by these entities. These regulatory philosophies are considered in more detail through this Section.

3.2. Prescriptive Versus Principle-Based Regulation

The two fundamental ways in which regulators can direct their regulated communities to assure safety are via prescriptive regulations or through principles-based regulation [26]. Prescriptive regulations detail the approved methods for achieving compliance, and these methods must be followed precisely to achieve the desired safety outcome. Prescriptive regulations are typically most appropriate for circumstances where the systems being regulated for safety are relatively mature and have specific, limited ways in which safety is achieved. These methods for achieving safety are then distilled into standards set by the industry and endorsed by regulatory authorities as authorized methods for ensuring safety while undertaking hazardous activities. Operators and practitioners then learn through training and experience to gain qualifications that the regulatory authorities recognize as evidence that individual practitioners and operators can apply the standards or codes competently in every relevant circumstance [27,28]. An example of prescriptive regulation is how electricians in many jurisdictions are regulated with very prescriptive rules, based on industry-developed standards or codes, e.g., Part 1 of the AS/NZS 3000 - Wiring Rules for Australian and New Zealand electrical installations [135]. Typically, local and state authorities require that licensed electricians follow standardized industry-set standards or codes when working on residential or commercial electrical installations [29,135] , which are comprehensively covered by the rules-based

 doi:10.20944/preprints202508.0294.v1

standard or code [30]. Once an installation is complete, the electrician will test the installation in a prescribed manner and then self-certify that the installation was completed via the methods specified in the Wiring Rules. The electrical installation may then be subject to inspection by the local electrical regulator. As the Wiring Rules do not prescribe cybersecurity requirements, there is no regulation of the electrician's cybersecurity practices. These agreed industry standards are also key to ensuring compatibility of systems and components across broad geographical areas, reducing the risk of unexpected emergent hazards as interconnected systems (such as the electricity grid) grow larger, more diverse, and complex.

In contrast, Part 2 of the wiring rules [135] provides regulation through the application of first principles by an appropriately qualified Electrical Engineer to address electrical installations not covered by Part 1 of the Wiring rules. An electrician would then use the bespoke design from the Electrical Engineer to carry out the installation, and the Electrical Engineer would verify compliance against their design. If the Electrical Engineer considers the need to include cybersecurity requirements within the design, they may do so. Regulating safety via principles requires the regulator to articulate high-level principles critical to the safety of the systems of interest [27,28]. Regulating via principles allows the operators of the systems of interest to demonstrate to the external regulator that their organizational systems, processes, governance, and internal regulation are adequate to address all associated hazards and manage their systems' safety appropriately [31]. Principles-based regulations can be helpful when regulating an industry or sector that regularly experiences change in the technology that underpins safety, where the sector is diverse and it would be hard to make a 'one size fits all' prescriptive requirement, or where the regulated community's approach to undertaking hazardous activities is in flux [31]. An example of principles-based regulation is Australia's National Offshore Petroleum Safety and Environmental Management Authority's safety case regulatory approach [32] to offshore petroleum activities through the Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009 [33]. These regulations allow the regulated community to manage safety and environmental hazards using the risk-based '*As Low As Reasonably Practicable (ALARP)*' principle, providing flexibility in how hazards associated with offshore drilling are managed and regulated.

Given the rapid pace with which the cyber domain is developing, including the emergence of novel threats and the rapid rate with which cyber components are being incorporated into physical systems to create CPS, it is challenging to apply prescriptive regulations to the development and operation of CPS. To add to this, CPS are becoming increasingly reliant on their cyber components for safe operation, and this adds significant complexity to the CPS, which again makes it challenging to apply prescriptive regulations to them. Therefore, due to their rapidly evolving nature, the most appropriate way to regulate the cyberworthiness of CPS would be by applying principles-based regulations. Regulators must, however, acknowledge that the more principles-based their regulations are, the more 'in-house expertise' they need to understand the methodologies that the practitioners they regulate may utilize. Unfortunately, though, there is a significant workforce shortage to overcome to achieve appropriate regulation of high-hazard CPS through prescriptive regulation because skilled workers who are proficient in both cybersecurity and the (physical) technical aspects of CPS are generally in short supply, and there is a requirement for the regulatory workforce to be at least as equally skilled.

3.3. The Impact of Changing Technology and Disruptors on the Effectiveness of Regulation

All industries that utilize CPS are susceptible to the emergence of disruptors who, often through the application of advances in technology unproven for that industry, aim to reduce the cost and overhead of providing the same physical outputs that incumbent industry participants offer. These disruptors can destabilize industry safety conventions and norms by introducing new technology, and as new industry participants, they are less likely to understand the safety risk profile that the incumbent participants have developed over decades or more.

 doi:10.20944/preprints202508.0294.v1

Regulatory conventions and norms may have been established over decades or more, and due to the mature safety focus of the incumbent industry players, much of this conservatism may not have been codified in industry standards and regulations. This situation means that not only do the new players present a higher risk to the safety of the physical outputs of the industry they are entering, but if they demonstrate initial early success, then incumbent participants may opt to ignore their traditional conservative approach to safety. Thus, incumbents adjust to survive in the industry because of the impact of the disruptor.

The introduction of Artificial Intelligence (AI) and quantum computing into broad networks of connected systems is poised to drastically change the cyberspace environment of CPS and CSoCPS. While these AI and quantum computing technologies have great potential to improve the operation, efficiency, and safety of CPS and CSoCPS, there is a commensurate risk of embedding significant novel hazards into CPS. Methods to assure AI-enabled systems in safety-critical circumstances beyond simple transparency and documentation include explainable AI [137], uncertainty analysis [138], and alternative AI monitoring of critical AI [139,140]; however, these are at best nascent. Moreover, in the current decentralized commercial environments for society's critical infrastructure and IoT, rapid commercial development of AI-enabled systems outpaces and dwarfs the development of such assurance techniques. One promising possibility for improving safety of CPS and CSoCPS is through advanced AI-monitoring through intrusion detection systems, such as those developed for common use communication devices [141], although these intrusion detection systems do not easily extend to the physical safety and the uniqueness of CSoCPS.

Even in industries utilizing high-hazard CPS that an external regulator already regulates due to their safety impacts, there may be industry incumbents with a long track record (brand) associated with quality and safety that undergo an internal upheaval that negatively impacts their long-standing systems and processes of quality and safety assurance. One notable recent high-profile failure in the regulation of CPS is the Boeing 737 Max aircraft Maneuvering Characteristics Augmentation System (MCAS) system, which included the development of a cyber-physical system. The subject CPS suffered a sensing and subsequent (cyber)automation failure of a physical system that was in no way related to a cybersecurity or cyber-maturity issue [34]. According to [142], '*The House Committee's report revealed that there were several factors such as information concealment, lack of attention to issues raised by lower-ranked employees, communicated production pressure, ineffective ARs* [Authorized Representatives], *and relaxed safety standards behaviour taking place in a linear and tightly connected system*.' This example illustrates the failure of internal and external regulation that significantly impacted the airworthiness of an aircraft type upgrade.

If regulations are not in place within high-hazard industry sectors to effectively counter these adverse effects of disruptors and internal upheaval as technology advances rapidly, then this may lead to an unconscious race to diminishing safety with potential tragedy in the short-term pursuit of profit and market dominance. To assure that operators of high-hazard CPS operate their CPS in a manner that supports the safety of the operator and members of the public, it may be necessary for CPS operators to be explicitly regulated for cyberworthiness by an external regulator.

3.4. Internal Self-Regulation Vs External Regulation

There are two ways to regulate the safety of CPS. That is, the responsible entity introduces self-regulation and external regulation imposed on the responsible entity. Often, components of both self-regulation and external regulation are applied in unison. For example, where an external regulator primarily relies on the ability of a regulated entity to self-regulate particular hazardous activities, but they issue a certification or licence to the entity or its personnel before the entity conducts those activities. An external regulator may have legislative powers provided to it by a government [21], or they may have the consensus of the broader industry participants that operate similar CPS that deal with similar hazards [27]. In the latter case, there may be a driving incentive to ensure strong internal regulation at the industry level to safeguard against more stringent and potentially prohibitive legislative regulations being imposed [23,35].

 doi:10.20944/preprints202508.0294.v1

Externally imposed regulation may occur due to community pressure following a significant incident, or a string of incidents, involving a particular type of hazardous activity, which may include CPS. An example of forced change from internal self-regulation to external authorizing regulation occurred in the UK medical profession following a series of scandals in the 1990s [23]. A second example is the development of boiler codes in the US in the early 1900s, following high annual death and injury rates due to boiler explosions, later adopted as mandatory prescriptive rules and standards by the government.

One of the driving factors that may determine the application of internally applied self-regulation rather than externally imposed authorizing regulation is whether an external authorizing regulator possesses knowledge about the hazardous activity that is the same or better than that of the regulated entity or community [36]. As Shavell (1983) postulates, *"If the private parties possess information about these elements that is superior to the regulatory authority's, then, other things equal, it would be desirable for it to be the parties who perform the calculations to decide how to control risks."*. Should an external regulator impose strict regulations under these conditions, it can readily lead to under-regulation or over-regulation due to the regulatory authority not understanding the risks and hazards involved in the activity. It is noted here that a lack of expertise within a regulator alone would not justify exclusive self-regulation of private entities, particularly when dealing with high-hazard activities, as this is very unlikely to meet community expectations of their elected representatives. Shavell does, however, highlight the importance of ensuring that regulators possess the appropriate expertise so that, at a minimum, they can effectively verify calculations and risk control measures even if there is considerable confidence in the ability of private entities to self-regulate hazardous activities. Moreover, there will always be a spectrum of abilities in private entities and the regulation must cater for the lower end of the spectrum.

3.5. The Relevance of Cyberworthiness to CPS and CSoCPS

For high-hazard and high-reliability CPS, there is a need to consider its cyberworthiness. When considering networked or integrated complex systems of CPS, the overall cyberworthiness of the CSoCPS as a complete operating entity must be considered. How they interact with their cyber and physical environments must be fully understood, and any associated hazards must be accounted for and mitigated. The claimed cyberworthiness of a CPS or CSoCPS must be measurable against defined cyber threats and physical hazards to assure the desired operation of the CPS and ensure safe and hazard-free physical outputs of the CPS. The many pathways through the cyber and physical domains, often back and forth, have to be mapped and regularly revisit for current malicious threats [10,136].Ways to assess and address cyberworthiness must be determined so that the cyberworthiness of CPS can be appropriately factored into existing regulatory frameworks. For those responsible for the safety of a CPS and for the regulators that regulate those responsible, there is a need to efficiently and effectively measure the cyberworthiness of a given CPS or a complex system of CPS.

Traditionally, cyber system owners and operators have focused on the cybersecurity (confidentiality, integrity, and availability) of the data associated with their systems [2] to ensure that the system is performing its objectives properly. When integrating cyber and physical systems with potentially hazardous physical outputs, the application of cybersecurity alone does not adequately account for the magnitude and type of physical dangers that the resultant CPS may impose on people and the environment [10,136]. **Figure 3** below provides a valuable depiction of the difference between cyberworthiness, cybersecurity, and system safety for a given CPS. **Section 5** outlines potential principles-based cyberworthiness regulations that regulators of high-hazard CPS may utilize to assure that the physical harms associated with CPS are being adequately considered by the communities they regulate.

 doi:10.20944/preprints202508.0294.v1

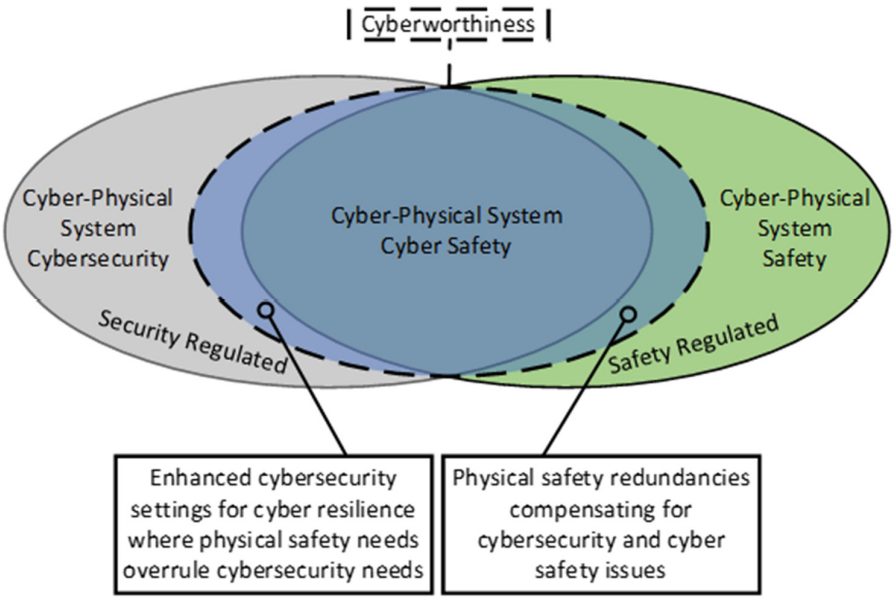

Figure 3. Venn Diagram of Regulatory Interest of Cyber-Physical Systems. (Adapted from Aerospace Industries Association's view of the role of Aviation Regulators in the regulation of Cyber-physical safety in the aviation industry, Feb 2020).

3.6. Illustrative Case Studies of Cyberworthiness Issues of Cyber-Physical Systems

The oft-cited Stuxnet incident of 2010, involving a highly complex and coordinated cyber-attack on nuclear enrichment facilities, was a watershed international event concerning the security vulnerabilities inherent to ICS. This cyber-attack highlights the significance of the impact that the cyber aspects of CPS can have on their physical outputs, and how vulnerable the physical outputs of a CPS are to a cyber-attack [37]. The more recent 2024 CrowdStrike cybersecurity software update failure that disrupted a broad range of transport and infrastructure systems, including public safety systems, highlighted that vulnerabilities with the cyber components of the CPS do not need to be related to security or malicious intent. Often categorized as supply chain issues, these non-security-related and non-malicious issues can manifest in major disruptions to transportation worldwide due to a failed software update of cybersecurity software utilized globally. Hence, the more recent focus on the broader cyber-resilience rather than just cybersecurity, noting that cyberworthiness is a subset of cyber-resilience focused on safety. Although this second incident did not directly involve CPS, it more broadly captured CSoCPS as the impacted computer systems were a point of failure in the interface between the travelling public and the transport CPS, which they could no longer access due to the incident [38].

Complex system of CPS behavior was also witnessed in the 2023 outage of the Optus telecommunications network in Australia due to scheduled patch updates of their parent company, Singtel, that carried through to Optus' local information handling exchanges, causing them to fail nationwide [39]. This incident led to customers' inability to utilize their telecommunications network for some time, subsequently denying some customers the ability to access potentially lifesaving emergency services. While this casts a wide net over the concept of CSoCPS, it highlights the harmful consequences of losing physical outputs (emergency services) due to an upstream IT failure initiated by routine and reasonable remote actions on IT equipment. While traditional cybersecurity practitioners may be inclined to categorize issues like CrowdStrike and the Optus outage as supply chain issues, it is not adequate to group other non-security-related cyber-issues into this limited cybersecurity category.

 doi:10.20944/preprints202508.0294.v1

3.7. International Cooperation on External Regulations for the Safety of CPS

Many high-hazard CPS can operate across international borders or cause a significant impact across multiple jurisdictions. Hence, they must comply with local regulations in whichever jurisdiction they may be operating and adhere to international conventions when operating in international areas to satisfy the requirements of their 'home' regulator with which they are registered or affiliated. Examples of CPS crossing jurisdictions are trains, commercial aircraft, and maritime vessels, while examples of high-hazard CPS that are immobile but can have a significant impact across international borders include nuclear power plants and critical energy distribution infrastructure. A high degree of international cooperation and coordination is required to ensure consistent regulations applicable to any mobile high-hazard CPS across jurisdictions. To support this international cooperation and coordination, many international agencies have been established to, among other functions and responsibilities, promote the safety of high-hazard CPS through treaties and conventions that require member states to enact domestic regulations; for instance:

IAEA – International Atomic Energy Agency

OECD – Organisation for Economic Co-operation and Development

ICAO – International Civil Aviation Organization

UNOSA – United Nations Office for Outer Space Affairs

Additional internationally recognized cyber standard-setting organizations that these international agencies rely on to ensure international consistency and interoperability include:

ENISA – European Union Agency for Cybersecurity

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

ISO – International Standards Organization

NIST – National Institute of Standards and Technology (noting that NIST is a US organization that publishes inter alia cybersecurity standards, guidance, and frameworks that are key references worldwide.)

There is a considerable degree of cooperation and coordination between domestic regulators of high-hazard CPS, their domestic cybersecurity lead agency, and international organizations that coordinate international consistency of CPS that impose hazards across international borders. As an example, the United States (US) has a domestic aviation regulator, the Federal Aviation Authority (FAA), that regulates civil aviation in the US in cooperation with ICAO. The US also has the domestic Nuclear Regulatory Commission (NRC) that cooperates with the IAEA. From a cybersecurity perspective, federal US government organizations are required to adhere to NIST standards and guidance. Similarly, the European Union requires member states to utilize ENISA-driven regulations for cybersecurity. Australia's approach to regulating critical infrastructure requires applying the Security of Critical Infrastructure Act 2024 (SOCI)[40] which industry advisors note still has significant deficiencies in its legislative coverage, such as water, sewerage, Defence Industry, and ports not being required to register, and banking and ports not requiring risk management programs [143]. Australian Commonwealth departments and agencies must implement the Protective Security Principles Framework (PSPF)[41] to ensure the cybersecurity of government assets and information.

3.8. Regulatory Gaps in Regulating the Cyberworthiness of High-Hazard Cyber-Physical Systems

There are no specific high-hazard CPS regulations that comprehensively cover the intersection of cybersecurity and physical safety to fully account for the cyberworthiness of a high-hazard CPS. The initial and continuing airworthiness [42,43] requirements of various domestic civil aviation regulators (e.g., FAA and EASA) concerned with the application of modern avionics to modern aircraft are arguably the closest to covering this intersection from an individual aircraft's perspective [44,140,142]. Avionics are a specialized subset of industrial control systems that control the aircraft during aircraft operations and are a key component of aircraft CPS. However, there remain gaps in airworthiness regulations when considering modern aircraft as an individual CPS within a CSoCPS. Many regulatory frameworks consider only each instance of a CPS in isolation [42] and do not

 doi:10.20944/preprints202508.0294.v1

provide clear requirements or guidance on how to account for their interactions with a wide range of other CPS during their operation, thereby creating a CSoCPS. No united and consistent guidance exists on how to regulate or manage a broader grouping of CPS that form CSoCPS. **Table 1** provided a useful summary of the key regulatory gaps identified through the case studies considered in Section 3.

Table 1. Summary of the Regulatory/Governance Gaps identified in Section 3.

Incident	Cyber-Physical Failure	Regulatory/Governance Gap
Boeing 737-Max	MCAS	Lack of regulatory rigour in establishing the existence of mission creep in a new automated system, leading to it becoming an unnoticed critical safety operational technology subsystem of a CSoCPS. Lack of regulatory rigour in scanning environmental drivers in the civil aviation industry, prioritizing minimal pilot re-training on re-engineered aircraft. Failure of the regulator to identify a systematic breakdown of internal safety governance within a major regulated industry participant.
Optus / Singtel	Forced Patch Error	Lack of regulatory rigour in strategic monitoring of the potential for telecommunications providers to cause a failure of broader systems (within the CSoCPS construct), reliant on the telecommunications system, to supply critical physical outputs (e.g., emergency services).
Stuxnet	Operational Technology Cyber-attack	A lack of application of basic cybersecurity to operational technology systems. A lack of operator governance on the use of operational technology to perform operations and report back on them without the use of alternative means of verification.

Cybersecurity-focused organizations such as NIST and ENISA provide frameworks that provide some depth into the cybersecurity of operational technology. Still, the focus remains on cybersecurity as the foundation for safety, rather than the overall and ongoing performance of the CPS in ensuring safety through all modes of operation across CSoCPS.

The regulated CPS community entities must be responsible for the CPS they control and operate, including all interactions with external cyber systems and CPS external to their CPS. To do this effectively, they, too, require the ability to properly internally regulate the safety of their CPS. To enable effective external regulation, regulators must acknowledge that the more principles-based their regulations, the more in-house expertise they need to understand the methodologies that the practitioners they regulate use.

The rapid pace of development of CPS requires principles-based regulation; however, there remains a need for practitioners and regulators to be able to measure the cyberworthiness of CPS and its complex systems to allow for effective internal and external regulation. To this end, the application of theories and practices in the governance of complex systems is critical.

4. Analysis of International Cybersecurity Regulation of High–Hazard CPS

As previously discussed in this paper, numerous types of high-hazard CPS exist that, if not properly managed, can harm people and the environment, spanning international borders and vast geographical distances. Accordingly, it is appropriate to consider how a representative subset of domestic regulators addresses the safety of high-hazard CPS within their jurisdiction, and how they collaborate through international organisations to coordinate and standardise regulatory oversight of these high-hazard CPS.

 doi:10.20944/preprints202508.0294.v1

4.1. Regulatory Analysis of International Organisations and Domestic Regulators of Their Member States

Historically, the existence of high-hazard (physical) systems that have impacts across international borders has resulted in the creation of international conventions and treaties for consistent regulation of the operation of these systems; this study includes the following international organizations and representative state members:

- International Maritime Organization (IMO) for civilian maritime vessels and port facilities
  - USA – United States Coast Guard (USCG)
  - EU – European Maritime Safety Agency (EMSA)
  - Australia – Australian Maritime Safety Authority (AMSA)
- International Civil Aviation Organization (ICAO) for civilian aircraft and aerodromes
  - US – Federal Aviation Authority (FAA)
  - EU – European Aviation Safety Agency (EASA)
  - Australia –Civil Aviation Safety Authority (CASA)
- International Atomic Energy Agency (IAEA) for the civilian use of nuclear material
  - US – Nuclear Regulatory Commission (NRC)
  - EU – European Nuclear Safety Regulators Group (ENSREG)
  - Australia – Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)

Using publicly available documents on websites associated with the international organizations and domestic regulators, first, the study assessed the Operational Technology Cybersecurity Maturity requirements within each of the international organizations' guidance material and the regulations and guidance materials of the counterpart domestic regulators of a representative group of member states identified in the list above. The study then considered the conformance of the regulations and guidance material to the contemporary Complex Systems Governance attributes of strategic monitoring, environmental monitoring, and operational performance, as outlined by Keating and Katina [45].

4.2. Purpose of Analysis

The hazards to the safety of life and ongoing operation of CPS arising from the powerful natural forces of the marine and aviation environments, as well as the unrelenting nature of the radiation hazard associated with human nuclear endeavors, readily cross international borders. As such, it is in the interest of all member states of the respective international safety organizations to ensure that all other member states apply appropriate regulatory controls to these systems, ensuring their safe operation regardless of their physical location. To support less advanced member nations, the more advanced member nations lead the development of codes and standards that can be incorporated into the domestic legislation of all member states, as depicted in **Figure 4**.

The more recent development of the cyber domain and its integration into high-hazard physical systems has ushered in the era of high-hazard CPS. As the cyber domain continues to develop and advance rapidly, there is a corresponding need for robust and practical guidance on regulating high-hazard cyber-physical systems.

This analysis examines indicative regulations, codes, and standards developed by advanced member states in the international bodies listed above, as well as cybersecurity-themed guidance for CPS provided by these international bodies, to determine whether the international guidance and corresponding domestic regulations are adequate for effectively regulating high-hazard CPS that are developing at an increasingly rapid pace.

The United States of America is a member state of the IMO, ICAO, and the IAEA. The US has established its respective domestic agencies, including the USCG, FAA, and the NRC, to assure the appropriate conduct of regulated domestic entities in these critical hazardous endeavors and to fulfill its international obligations as a member state. When considering the cybersecurity posture of these US agencies, it is essential to include the aforementioned National Institute of Standards and

 doi:10.20944/preprints202508.0294.v1

Technology (NIST), as the premier agency for setting cybersecurity standards and guidance in the US.

The European Union is a conglomerate of 27 European countries, many of which are also members of the IMO, ICAO, and the IAEA. The EU has a common parliament and Commission [47] that produce regulations, regulatory guidance, and standards for member states. The EU has been included in this analysis for simplicity, rather than assessing individual European member states, many of which do not use English as their primary written language. The EU, as a collective, has corresponding agencies, including the European Maritime Safety Agency (EMSA), the European Aviation Safety Agency (EASA), and the European Network and Information Security Agency (ENISA), which have standard regulations and guidance written in English, among other European languages. Similar to the NIST for the US, the EU is supported by the European Union Agency for Cybersecurity (ENISA), which provides cybersecurity standards and guidance to EU member states and is empowered by the EU Cybersecurity Act 2019 [47]. While each EU member state maintains its regulators and regulations, the EU groupings provide for a collective and standard view.

Australia is a member state of the IMO, ICAO, and the IAEA. Australia has established its respective domestic agencies, including AMSA, CASA, and ARPANSA, to ensure the operation of high-hazard CPSs that they regulate. However, it is noted that Australia has far smaller industries in all three sectors, and it does not produce large numbers of ships, aircraft, or nuclear-enriched material. While Australia does not have an equivalent of NIST or ENISA, combining the Australian Cyber Security Centre (ACSC) and the Department of Home Affairs' (HA) SOCI Act provides partial equivalence.

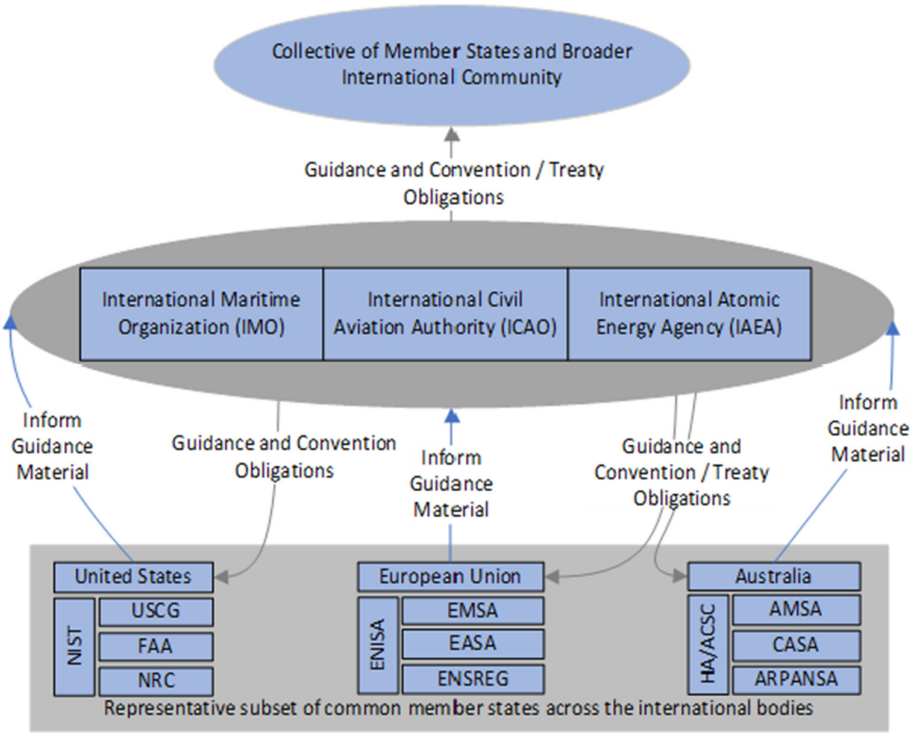

Figure 4. Select Domestic Regulator Member Contributions to Respective International Entities.

4.3. Method of Analysis

Through this analysis, the regulations of several international regulators of high-hazard cyber-physical systems were assessed for their level of cybersecurity maturity, specifically concerning Operational Technology, and for their degree of conformance to contemporary Complex Systems Governance theory and practices. Through this analysis, these regulations and guides are

 doi:10.20944/preprints202508.0294.v1

qualitatively assessed to develop an understanding of potential gaps in the overall regulation of high-hazard CPS, which could lead to adverse safety outcomes or a loss of critical physical outputs of CPS essential to the operation of modern society. High-profile contemporary case studies are also incorporated later in the paper to highlight how these gaps may manifest as harmful incidents initiated through the cyber-domain portion of high-hazard CPS.

This analysis began with the examination of the public websites of each international organization and national regulator for the documentation reviewed during the study. Relevant safety and security/cybersecurity guidance documentation from each of the international organizations related to the specific CPS they are concerned with (e.g., marine vessels and ports for the IMO, aircraft and aerodromes for the ICAO, and nuclear reactors and supporting infrastructure for the IAEA) was downloaded and compiled for further analysis. Likewise, the regulations and associated guides from a select group of advanced member states were downloaded from their public websites and compiled for further analysis. On rare occasions, when a few relevant documents were unavailable due to restrictions placed on them, these documents were not directly included in the analysis.

A qualitative assessment of two criteria was conducted to evaluate the relevant international organizations' and national regulators' regulations and guidance materials. A short description of how the qualitative evaluation was applied to the regulations and guidance material is as follows:

Operational Technology Cybersecurity Maturity – The regulations and guidance materials of each international organization and domestic regulator were qualitatively assessed by searching for the term 'cyber' or 'computer' within each safety-related regulation or guide. The passages of text that included the terms 'cyber', 'computer', 'Operational Technology', or 'OT' were then read. Consideration was given to the degree to which the information provided regulation or guidance specific to the safety impacts of operational technology associated with the types of CPS that are the subject of regulation. This technique was used to determine the extent to which each entity prioritized the importance of cybersecurity for operational technology in maintaining the safety outcomes of high-hazard CPS. The rating categories are as follows, noting that lower-level guidance materials could still be used to bridge information gaps:

- No Importance – Where the words 'cyber' or 'computer' were not included in a document (reiterating, lower-level guidance materials could still be used to bridge information gaps)
- Low Importance - Only mentions the term 'cybersecurity' or 'computer security' as areas to be considered.
- Moderate Importance - Identifies a requirement to conduct cybersecurity risk assessments, report cyber incidents, and apply fundamental cybersecurity to the CPS.
- High Importance - Identifies a requirement to conduct cybersecurity risk assessments, report cyber incidents, and apply advanced cybersecurity to the CPS, with consideration for operational technology and specialist associated technical practitioners.

The aggregate of regulatory and guidance material was then considered for each international organization or domestic regulator, including instances where supporting cyber-fused national bodies were referenced in the documents (e.g., NIST), and an overall descriptive qualitative result was assigned. These qualitative descriptions are provided in the Analysis – Findings section.

Conformance to contemporary Complex Systems Governance theory and practices – Key Complex System Governance metasystem function attributes, as outlined by Keating and Katina [45], were also considered as part of the assessment. The key Complex Systems Governance metasystem attributes considered in the analysis included:

- ***Strategic monitoring*** of the cybersecurity of the operational technology components of the regulated CPS,
- ***Environmental scanning*** of the cybersecurity of the operational technology components of the regulated CPS, and

 doi:10.20944/preprints202508.0294.v1

- ***Operational performance*** of the CPS relating to maintaining system safety while assuring the ongoing delivery of the physical outputs of the regulated CPS.

During the qualitative assessment of document conformance to Complex Systems Governance practices, consideration was given to whether there was evidence that the Complex Systems Governance metasystem attributes were being considered, regardless of any specific intent by international organizations or domestic regulators to apply contemporary Complex Systems Governance practices explicitly to their guidance and regulation. The conformance ratings used to assess the publicly available documents from each of the international organizations and regulators are as follows:

- ***No conformance*** – no indication of the contemporary Complex Systems Governance theories and practices listed above being incorporated in the aggregate documentation and established practices of the organization under assessment.
- ***Low conformance*** – indications that one of the types of contemporary Complex Systems Governance theories and practices listed above has been incorporated in the aggregate documentation and established practices in a high-level, cursory way.
- ***Moderate conformance*** – indicates two of the types of contemporary Complex Systems Governance theories and practices listed above have been incorporated in the aggregate documentation and established practices with some guidance and structure.
- ***High conformance*** – indicates that all three types of contemporary Complex Systems Governance theories and practices listed above have been incorporated in the aggregate documentation and established practices with strong guidance and structure.

The documents of each international organization and their domestic counterparts were assessed for Complex Systems Governance conformance in parallel with the assessment of operational technology cybersecurity maturity. **Tables 2–5** provide a summary of the types of organizations assessed as part of the analysis, as well as the number of documents assessed from each. The Analysis- Findings section provides the aggregate descriptive qualitative position of each international organization or domestic regulator.

Table 2. Number of relevant documents from the international organizations.

	IMO	**ICAO**	**IAEA**
Agreement	Convention based	Convention based	Treaty and Convention based
Members	176	193	180
Relevant Docs	9	37+	27

+ A highly relevant but restricted document not available to the public was identified but not included in the assessment.

Table 3. Number of relevant documents from select US domestic Regulators.

	USCG	**FAA**	**NRC**
Authorized by	Legislation	Legislation	Legislation
Relevant docs	16	18	84

Table 4. Numbers of relevant documents from select EU Regulators.

	EMSA	**EASA**	**ENSREG**
Authorized by	Legislation*	Legislation*	Agreement
Relevant docs	24	32	2

*English-language only; the EU provides a unique context of 27 mainly non-English-speaking countries, with the collective EU Parliament and Commission providing regulations and guidance written in English.

 doi:10.20944/preprints202508.0294.v1

Table 5. Number of relevant documents from select Australian domestic Regulators.

	AMSA	CASA	ARPANSA
Authorized by	Legislation	Legislation	Legislation
Relevant docs	7	16	2

Note that the standards-setting organizations listed below are occasionally mentioned throughout the documents produced by the agencies identified in Tables 2–5. However, their documents were not included in the analysis, as they are not regulatory organizations, and the regulatory bodies do not identify their documents for mandatory application under their regulations.

- International Electrotechnical Commission (IEC)
- International Standards Organization (ISO)
- Institute of Electrical and Electronics Engineers (IEEE)
- MITRE Corporation

4.4. Findings of Analysis

Tables 6–9 below summarizes the findings of the analysis performed on the three international organizations and representative domestic regulators.

Table 6. Results from the Analysis of International Organizations.

International Organization	Operational Technology Cybersecurity Maturity	Complex Systems Governance Conformance
IMO	High Importance	Moderate Conformance
ICAO	Moderate to High Importance	Low Conformance
IAEA	Low to Moderate Importance	Low Conformance

Table 7. Results from Analysis of US Regulators.

US Regulator	Operational Technology Cybersecurity Maturity	Complex Systems Governance Conformance
USCG	High Importance	Moderate Conformance
FAA	High Importance	Low Conformance
NRC	High Importance	Moderate to High Conformance

Table 8. Results from the Analysis of EU Regulators.

EU Regulator	Operational Technology Cybersecurity Maturity	Complex Systems Governance Conformance
EMSA	High Importance	Low Conformance
EUASA	High Importance	Low Conformance
ENSREG	No Importance	No Conformance

 doi:10.20944/preprints202508.0294.v1

Table 9. Results from the Analysis of Australian Regulators.

Australian Regulator	Operational Technology Cybersecurity Maturity	Complex Systems Governance Conformance
AMSA	High Importance	Moderate Conformance
CASA	Moderate to High Importance	Low Conformance
ARPANSA	Low to Moderate Importance	Low Conformance

A more detailed account of the analysis for each entity is provided in the sections below.

4.4.1. Results of Analysis for International Organizations

International Maritime Organization – One of the primary regulatory documents from the IMO is the International Convention for the Safety of Life at Sea (SOLAS) [48]. While this document makes minor references to computer systems, including software responsible for controlling ship stability and record-keeping systems, it does not contain any mention of cybersecurity requirements. In 2017, the IMO passed Resolution MSC.428(98) [49], which requires approved Safety Management Systems (SMSs) to consider conformance to the International Safety Management (ISM) Code, which identifies cybersecurity considerations for managing cyber risks associated with safety systems. Additionally, IMO links to *The Guidelines on Cyber Security Onboard Ships* [50]. This document identifies the differences between IT and operational technology systems, highlighting the need for operational technology specialists.

Using the qualitative criterion for the Analysis – Methodology, overall, the IMO is assessed as assigning a **High Importance** to the application of cybersecurity to high-hazard maritime CPS. Furthermore, the Guidelines on Cyber Security Onboard Ships guide contains guidance on the NIST Cybersecurity Framework [51], which includes the Identify, Protect, Detect, Respond, and Recover methodology, which has parallels to the key Complex Systems Governance metasystems identified in the Analysis – Methodology. Accordingly, the IMO demonstrates **Moderate conformance** to contemporary CGS theory and practice.

International Civil Aviation Organisation – Documents related to the initial and ongoing airworthiness and certification of aircraft represent the primary regulatory guidance of ICAO. Airworthiness is primarily concerned with ensuring the safe operation of aircraft [52,53]. Equally critical to the safe operation of aircraft is the guidance material that ICAO produces on the initial and ongoing certification of aerodromes [54].

In terms of the safe and ongoing operation of aircraft, the concept of avionics is tantamount to the idea of operational technology in aircraft. In this regard, ICAO place high importance on the critical role of aircraft avionics in achieving and maintaining airworthiness [52]. However, through their regulatory guidance documents, ICAO does not explicitly provide a strong link between cybersecurity and avionics. ICAO places high importance on the need to address emerging cyber threats through its security regulatory guidance [55,56]. However, this guidance has a stronger focus on information security and information associated with aerodromes, and the responsibility for implementing it is passed to member states. It is noted that ICAO produces a restricted Aviation Security Manual [57], which was not included in this analysis.

Considering the qualitative criterion from the Analysis – Methodology, with ICAO's explicit identification of hazards associated with cyber threats, but no significant emphasis on operational technology for aerodromes, overall, ICAO is assessed as assigning a **Moderate to High importance** to the application of cybersecurity to high-hazard CPS. Through its regulatory guidance and supporting documents, ICAO acknowledges that cyber threats are an emerging issue; however, ICAO has minimal documentation and established practices, which demonstrate a **Low Conformance** to contemporary CGS theory and practice.

 doi:10.20944/preprints202508.0294.v1

International Atomic Energy Agency – The IAEA provides guidance on regulatory design and regulations for nuclear safety [58,59], which is of key consideration for this analysis. The IAEA also provides similar guidance on nuclear security, safeguards, and non-proliferation, which are not the primary focus of this analysis, as they are not strictly safety-focused [60]. However, when considering cybersecurity in the context of nuclear safety, cybersecurity is often more accurately captured in the security aspects of the guidance, and in this respect, there is a strong link between nuclear safety and security [61,62].

While the IAEA has extensive documentation on nuclear safety, as well as equally extensive documentation on nuclear security, it has limited guidance on applying cybersecurity to nuclear safety. The IAEA's nuclear safety documentation includes the need to develop justification for the use of nuclear material in specific facilities and approved activities, with a requirement to categorize systems that are important to safety appropriately. This generally includes any operational technology components in CPS critical to safety. In these instances, the IAEA documents emphasize the need to consider safety aspects related to the operation of computer systems [63–65]; however, the documentation generally lacks emphasis on the importance of cybersecurity for operational technology.

When considering the qualitative criterion from the Analysis – Methodology, with the IAEA having no clear identification of nuclear safety hazards associated with cyber threats and no significant emphasis on operational technology, the IAEA is overall assessed as assigning a **Low to Moderate importance** to the application of cybersecurity to high-hazard CPS. Through an assessment of its regulatory guidance and supporting documents, the IAEA was found to have minimal documentation and established practices demonstrating **Low conformance** to contemporary CGS theory and practice.

4.4.2. Results of Analysis for Regulators from the United States of America

United States Coast Guard (USCG) – The USCG has specific regulatory requirements for individuals responsible for operational technology [66–70]. The USCG links to the IMO and generally aligns with the regulations and guidance of the IMO [71,72]. As such, it is assessed that the USCG assigns **High Importance** to cybersecurity for high-hazard CPS. Similarly, the USCG demonstrates **Moderate conformance** to contemporary CGS theory and practice.

Federal Aviation Administration (FAA) – The FAA is closely aligned with ICAO regulations regarding aircraft airworthiness [73] and the development, operation, and maintenance of aerodromes [74]. As a US government body, the FAA adheres to NIST guidelines and is subject to federal government directives and presidential orders on improving systems and infrastructure against cyber threats, which includes cybersecurity for operational technology [75–78]. These cybersecurity requirements are passed on to airport operators receiving federal infrastructure funding [79]. The FAA was assessed as assigning **High Importance** to cybersecurity for aircraft and aerodrome operational technology. The FAA also supports the ongoing operation of the Aerospace Industries Association Cyber Safety Commercial Aviation Team, which has extensive links to national and international aviation and other organizations that operate and regulate high-hazard CPS [80]. It is assessed that the FAA demonstrates **Low conformance** to contemporary Complex Systems Governance theory and practice in strategic monitoring and environmental scanning.

Nuclear Regulatory Commission (NRC) – The NRC regulations [81] and IAEA guidance are very similar in content and scope, and the NRC provides regulatory guidance on complying with cybersecurity requirements associated with national security regulations [82]. The NRC also offers substantial guidance on introducing new technologies into nuclear reactor activities [83]. The NRC provides specific training on the significance of digital systems and high-level guidance on how to incorporate them into nuclear reactor settings. It is assessed that the NRC assigns **High importance** to cybersecurity for high-hazard nuclear ICS/operational technology critical to safety.

The NRC provision of extensive guidance on applying new and emerging technologies to nuclear reactors, as well as training and guidance on incorporating digital systems within a nuclear

 doi:10.20944/preprints202508.0294.v1

reactor, coupled with the inclusion of diversity and defense in depth strategies, which resemble strategic monitoring and operational performance Complex Systems Governance metasystems theory, the NRC was assessed as demonstrating a **Moderate to High conformance** to contemporary Complex Systems Governance theory and practice.

National Institute of Standards and Technology (NIST) – While NIST is not a regulatory body for cybersecurity, US government agencies must follow NIST guidance on cybersecurity, and NIST is recognized globally as one of the leading cybersecurity standard-setting bodies [84]. NIST has developed frameworks on cybersecurity [51] and provides advanced guidance on cybersecurity for CPS/operational technology [85]. While NIST does not demonstrate any purposeful application of Complex Systems Governance within its guidance documents, the NIST Cybersecurity Framework [51] includes the Identify, Protect, Detect, Respond, and Recover methodology, which parallels the key Complex Systems Governance metasystems identified in the Analysis – Methodology. Accordingly, NIST demonstrates **Moderate conformance** to contemporary Complex Systems Governance theory and practice.

4.4.3. Results of Analysis for Regulators from the European Union

European Maritime Safety Agency (EMSA) – The EMSA closely aligns with the IMO, providing the EU legislation on maritime safety through the European Parliament [86], including guidance on cybersecurity for operational technology related to safety [87,88]. Accordingly, EMSA is assessed as assigning **High Importance** to the application of cybersecurity to high-hazard CPS. EMSA has established a European Coast Guard Functions Forum Cybersecurity Working Group [89], which is assessed as **Low Conformance** to Complex Systems Governance's strategic monitoring and environmental scanning.

European Union Aviation Safety Agency (EUASA) – The EUASA closely follows ICAO's regulatory guidance, as established by the European Parliament, for EU member states [90–93]. This linkage includes developing guidance on aviation cybersecurity and cyber-resilience that incorporates information and guidance on aviation operational technology [43,94–96]. Accordingly, EUASA is assessed as assigning **High Importance** to the application of cybersecurity to high-hazard CPS.

EUASA established the European Centre for Cybersecurity in Aviation (ECCSA) [97], and the European Strategic Coordination Platform (ESCP) for Cybersecurity in Aviation [98], which jointly bring together European aviation community organizations to cooperate and better understand emerging cybersecurity risks in aviation. This is assessed as **Low Conformance to** the strategic monitoring and environmental scanning aspect of Complex Systems Governance.

European Nuclear Safety Regulators Group (ENSREG) – The authority of ENSREG is not established through the European Parliament and European Commission in the same manner as EMSA and EUASA, and its members participate optionally and cooperatively [99,100]. As ENSREG is considered an independent and authoritative expert body, it advises the European Commission on its rules related to nuclear safety. As ENSREG is not a regulatory body, there were no legislative instruments or associated documentation to assess in the study. An assessment of the material available on ENSREG's website, conducted using the regular assessment methodology, indicated that ENSREG attributes **No importance** to the application of cybersecurity to high-hazard CPS. Furthermore, ENSRED documentation indicates **No conformance** to Complex Systems Governance theory and practice.

ENISA – While ENISA is not a regulatory body for cybersecurity, it is recognised globally as one of the leading cybersecurity standard-setting bodies, and it has powers established through the European Parliament and European Commission via the EU Cybersecurity Act [101]. ENISA has developed extensive documentation on cybersecurity for operational technology and CPS [102–109]. When considering this documentation through the lens of Complex Systems Governance, ENISA does not demonstrate any specific application of Complex Systems Governance within its guidance documents.

 doi:10.20944/preprints202508.0294.v1

4.4.4. Results of Analysis for Regulators from Australia

Australian Maritime Safety Authority (AMSA) – The Australian Maritime Safety Authority Act 1990 [110] establishes AMSA. AMSA's marine orders 01 – 98 [111] apply international convention requirements to vessels subject to the Navigation Act 2012. As they match the requirements and guidance of the IMO, it is assessed that AMSA places **High Importance** on cybersecurity for high-hazard maritime CPS. Similarly, AMSA is assessed as demonstrating **Moderate Conformance** to contemporary Complex Systems Governance theory and practice.

Civil Aviation Safety Authority (CASA) – The Civil Aviation Act [112] establishes CASA. Along with the various subordinate legislative instruments [113–120] and strategic documentation [121] CASA documentation closely aligns with the regulatory guidance provided by ICAO. Similarly to ICAO, CASA is assessed as assigning **Moderate to High Importance** to cybersecurity for high-hazard CPS and **Low Conformance** to contemporary Complex Systems Governance theory and practice.

Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) – Although the Australian Radiation Protection and Nuclear Safety Act 1998 [122] and accompanying regulations [123] are specific to the Australian nuclear landscape, ARPANSA regularly cites IAEA guidance on nuclear safety as international best practice and closely aligns its regulations with the regulatory guidance provided by the IAEA. This link to the IAEA flows through to ARPANSA's application of cybersecurity to operational technology and CPS. Accordingly, this analysis has identified that ARPANSA assigns a **Low to Moderate Importance** to cybersecurity for high-hazard CPS. Similarly, ARPANSA is assessed as demonstrating **Low conformance** to contemporary Complex Systems Governance theory and practice.

Australian Security of Critical Infrastructure – The SOCI Act 2024 is designed to ensure that infrastructure critical to the functioning of modern society is appropriately protected from external threats [40]. As such, it requires the owners and operators of critical infrastructure to report cyber incidents and breaches, undertake cybersecurity risk assessments on their critical infrastructure, and adopt minimum cybersecurity techniques to protect their infrastructure. It is assessed that the SOCI Act assigns a Medium to **High Importance** to cybersecurity for high-hazard CPS, but with minimal reference in supporting documents to operational technology and no detail on establishing cybersecurity frameworks, such as the Australian Government PSPF[41], the Cyber Security Act 2024 [124] and the associated Cyber Security Rules 2025 [125]. The SOCI Act is assessed as demonstrating **Low conformance** to contemporary CGS theory and practice.

5. The Need for Cyberworthiness Governance and Regulation

Despite the incentives for operators of high-hazard CPS to apply stringent internal regulation of cyberworthiness to ensure that their CPS remain safe and operational, this paper has identified that this is not enough to ensure that operators continue to operate their high-hazard CPS safely. The cyberworthiness of the CPS and CSoCPS must be considered to address these uncertainties.

As previously identified, achieving, determining, and maintaining the cyberworthiness of CPS is a complex and multidisciplinary undertaking. Further, any regulation of the cyberworthiness of CPS must begin within the governance and assurance functions of the organization operating the CPS [45]. In addition to internal cybersecurity and physical system safety governance determined by the operator of a high-hazard CPS, the state of cyberworthiness of the CPS or a CSoCPS also needs to be regulated. As shown in this paper, there exist many ways to regulate physical systems to ensure system safety. However, cyber-resilience and cyberworthiness are not a traditional part of CPS regulation.

To support the introduction of regulations governing the cyberworthiness of CPS, operators of CPS and their regulators alike would greatly benefit from the application of complex systems governance. Complex Systems Governance could be applied to a CPS from the earliest manifestations of the concept of a CPS, to the latest stages of their operational life, and in some cases, could be applied well into obsolescence and disposal. Additionally, aligning Complex Systems Governance to the

 doi:10.20944/preprints202508.0294.v1

verification, test, validation and evaluation activities of the development, operation, and disposal of a CPS is an important consideration. In this way, the assurance activities of individual CPS can be amalgamated and aligned across CSoCPS.

Regulations should specifically require the operators of high-hazard CPS to develop a cyberworthiness system to ensure that the desired physical outputs of the CPS and SCoCPS are safe and available [136]. When considering cyberworthiness as a component of existing safety regulation regimes, some key components should be considered for inclusion, as shown in the list in Section 5 (Essential Elements of Cyberworthiness Regulations).

5.1. Potential Benefits of Regulating Cyberworthiness

As identified through the analysis in Section 4, a notable cyberworthiness capability gap currently exists in the way in which organizations that operate high-hazard infrastructure-based CPS are regulated, and this gap is likely more pronounced in organizations that operate complex systems of CPS incorporating infrastructure CPS throughout the operational phase as part of a larger system of CPS. While organizations that operate high-hazard CPS may be narrowing this gap with increased rigour in establishing cybersecurity maturity within their organizations, few appear to be actively focusing on the safety implications of a significant upward trend in incorporating operational technology into their systems (aka, IoT). This suggests that the existing internal governance mechanisms responsible for regulating their systems are not adequately equipped to handle this rapidly changing environment.

Likewise, external regulators of high-hazard CPS do not yet appear to adequately recognize the significance of the rapid adoption of operational technology in high-hazard CPS. Their overarching regulatory frameworks and specific regulations, whether prescriptive or principles-based, do not yet appropriately account for the complexities of high-hazard interdomain systems that increasingly rely on the cyber domain to assure the outputs in the physical domain.

Given these significant deficits, the issues related to a lack of demonstrable cyberworthiness in high-hazard CPS are going to take time to address. These issues involve considerable complexity, require highly skilled personnel to work collaboratively across technical domains, are costly to implement, and require significant effort to reach consensus and achieve international harmonization across cooperative international jurisdictions. Nevertheless, the implementation of cyberworthiness regulations, both internal and external, for the operators of high-hazard CPS will provide numerous benefits, in addition to providing assurances of the safe operation of the CPS of interest. Additional benefits include improved availability and uptime of the CPS, enhanced reliability of the CPS, improved organizational resilience, a more positive organizational mindset towards the application of new technologies in operations, and a safety-focused organizational culture.

5.2. Essential Elements of Cyberworthiness Governance

CPS operators need to demonstrate through their internal self-governance [24] that their CPS are worthy of operating, with full consideration of the cyber aspects of their CPS, and any CSoCPS that they interact with, or are a part of. Operators need to demonstrate that they have a credible process for replacing obsolete cyber componentry and organizational practices that are no longer able to credibly assure the safe physical outputs of their CPS, with a firm understanding of the potential harms associated with their CPS providing no physical outputs.

Using the insights gained from the case studies detailed in Section 3 and the content analysis detailed in Section 4, the research questions presented in Section 1 are primarily addressed by the development of the following principles-based requirements. These requirements need to apply to designers, operators, maintainers, and owners of all high-hazard CPS to demonstrate an appropriate level of cyberworthiness, and they include the core metafunctions for enduring complex systems governance of the cyberworthiness of CPS and CSoCPS:

- Establish a Cyberworthiness governance regime for their high-hazard CPS.
  - Apply contemporary cybersecurity principles [51,104,126–129]:

 doi:10.20944/preprints202508.0294.v1

- Apply relevant cybersecurity practices to the cyber-systems within CPS.
- Ensure cybersecurity certification of cyber-systems within the CPS.
- Ensure cybersecurity accreditation of practitioners working with the CPS.
- Ensure appropriate patch management of cyber-systems within CPS.
- Ensure that the obsolescence of cyber-systems is planned for and managed.

- Design for the cyber-resilience of the physical system and physical outputs [130,131]:
  - Incorporate diversity of cyber-technology into the CPS.
  - Design into the CPS the upgradability of components.
  - Provide diversity in the operation of critical functions of the CPS with gradual and degraded modes of failure.
- Foster a Skilled and Cooperative Workforce[11,12]:
  - Develop and maintain a workforce proficient in both the cyber and physical aspects of the CPS and CSoCPS.
  - Provide for the organisation's ICT and CPS engineering personnel to consult, cooperate, and coordinate to ensure that they are collectively addressing the cyberworthiness of their CPS and CSoCPS in a collaborative manner.
- Ensure comprehensive through-life verification, test, validation and evaluation [132,133]:
  - Establish a through-life test and evaluation plan that includes testing of new systems with legacy systems.
  - Regularly test the effects of the interactions via the cyber-domain for new CPS and ICT systems that have been determined to, will, or may interact with the cyber-domain.
- Undertake regular environmental scanning [45] to:
  - Ensure all knowable cyber and physical hazards are known.
  - Ensure trends in cyber technology are understood.
  - Identify changes in cybersecurity, cyber standards, cyber trends, and emerging cyber hazards (not only cybersecurity threats) that have the potential to affect the safe and ongoing operation of the CPS.
  - Rapidly assess changes and apply as contemporary, where appropriate.
  - Identify new CPS and ICT systems that do, will, or may interact with the CPS via the cyber-domain.
  - Maintain a thorough understanding of all cyber systems and CPS that their CPS connects to or interfaces with.
- Communicate risks and hazards associated with the CPS effectively [133,134]:
  - Develop and enforce a standard risk management framework.
  - Use contemporary risk management tools like model-based systems engineering to assess risks rapidly and communicate risk effectively.

The above listing has deliberately been kept to an elegant existential set and so through such parsimony may be considered incomplete.

Regulators of high-hazard CPS may include the above principles-based cyberworthiness requirements as part of their regulations within their existing regulatory frameworks. In a complementary way, the operators of high-hazard CPS may incorporate them into their internal governance structures. Via collaboration across the regulated community, and with the support of key regulators, these cyberworthiness governance requirements could be used as the basis for a cyberworthiness certification system for safety-regulated high-hazard CPS. These principles-based cyberworthiness requirements would also provide a basis for auditability to regulators and traceability to relevant cybersecurity standards, changing technologies, and contemporary methods for achieving compliance with dynamic standards.

The application of these principles-based cyberworthiness requirements would help to ensure that practitioners have the competence and capacity to operate their CPS, including ensuring continued cyberworthiness. Regulators and supporting agencies may also use them to maintain the appropriate competencies to understand the cyberworthiness status of the CPS they regulate more

 doi:10.20944/preprints202508.0294.v1

fully. Coupled with analysis and digital twinning techniques like those at [136], all involved parties should become proficient in cybernetics and the application of Complex Systems Governance to enable effective through-life environmental scanning, which can detect changes in both the cyber and physical domains.

High-hazard CPS and CSoCPS exhibit critical dependencies on cyber components for safety-critical functions. As these systems grow in scale and complexity, ensuring cyberworthiness — the demonstrable resilience of cyber-physical integrations against disruptions — becomes imperative for preventing physical harm. This paper establishes three core contributions towards achieving this highly desirable outcome:

1. Regulatory Gap Analysis. Current standards (e.g., NIST SP 800-82r3, IEC 62443) and agency guidelines (FAA, IMO, NRC) prioritise cybersecurity but lack binding mechanisms to enforce safety-security co-assurance. Our document analysis reveals <15% of regulatory texts address cyber-physical interaction hazards (e.g., sensor spoofing causing control instability), leaving systemic cyberworthiness unregulated.
2. Cyberworthiness as a Governance Mandate. Self-regulation based on fragmented cybersecurity principles is insufficient. Cyberworthiness requires lifecycle validation of safety invariants under cyber disruptions, emergent risk monitoring in CSoCPS and evidence-backed assurance cases traceable to operators.
3. Principles-Based Cyberworthiness Requirements : Legislation cannot keep pace with technological change. We propose adopting Complex Systems Governance principles to enable adaptive compliance, environmental scanning, and metasystem tracking.

Drawing from the study's findings, we propose several potential regulatory pathways for the implementation of cyberworthiness governance requirements.

1. Short-term. Regulators should pilot cyberworthiness clauses referencing established cyber standards for operational technology, such as NIST SP 800-82r3 ISO 21448 (SOTIF) for high-hazard CPS.
2. Mid-term. Develop quantifiable cyberworthiness indices based on operational performance parameters from Complex Systems Governance metasystem (e.g., mean-time-to-safe-recovery under cyber-attack) for compliance monitoring and auditing.
3. Long-term. Establish international CSoCPS safety committees to harmonise governance of cross-border CPS hazards.

6. Limitations and Future Research

The documents included in the analysis in Section 4 are limited to publicly accessible documents from international organisations and national regulators. As indicated in Table 1, ICAO is one example where the international body maintains a document that is highly likely relevant to the analysis, but is restricted and not readily available to the public. Similarly, the study did not consider any military documentation, and it is further noted that international bodies do not cater to military applications of the CPS they relate to.

The analysis detailed in Section 4 also utilised very limited documentation from the owners and operators of the Civil Maritime, Civil Aviation, and Civil Nuclear CPS and CSoCPS, who are subject to safety regulations. While a minor amount of owner and operator documentation was incidentally considered in the analysis, the potential significance of this limitation relates to regulators that regulate through principle-based regulation. In these cases, members of the regulated community are expected to develop prescriptive processes and procedures to ensure the safe operation of their CPS and CSoCPS.

As noted in the analysis methodology in Section 4, the analysis was limited to assessing the international organisation and corresponding regulator documents against three of the nine Complex Systems Governance Metasystems. The three Complex Systems Governance metasystems chosen — strategic monitoring, environmental scanning, and operational performance — were judged to be the

 doi:10.20944/preprints202508.0294.v1

most likely of the nine to be incorporated into regulatory requirements without an explicit intention to do so. While assessing against the other six Complex Systems Governance metasystems has the potential to provide additional insights, it is anticipated that without a specific and concerted effort to regulate the owners and operators of CPS and CSoCPS, specifically to include the application of Complex Systems Governance in their methodologies, it is unlikely that these metasystems will be evident in the documentation.

Future research of this kind would benefit from liaising directly with the international organisations and domestic regulators to request that they inform members of their regulated community who they perceive as being advanced in the application of cybersecurity for the CPS and CSoCPS about the opportunity to participate in the research. Additionally, more international organisations and their domestic counterparts, as well as high-hazard CPS and CSoCPS (e.g., space, train), and members of their regulated communities, could be brought into the research.

In addition to including documentation from more regulators of relevant regulated sectors and members of all the respective regulated communities, future research would also benefit from the inclusion of industry and sector standards, codes, and guidelines. This additional documentation could be assessed using an enhanced grounded theory analysis, incorporating questionnaires with appropriately experienced personnel from regulators and industry to determine their understanding and practical application of cyberworthiness. The survey-based research would be further enhanced by undertaking a more thorough frequency analysis of the survey data and additional documents using advanced qualitative data analysis software, and by assessing the documents and survey data for evidence of the application of elements of all nine Complex Systems Governance metasystems. These research methodologies would then be complemented well by conducting additional case studies looking at how CPS have operated successfully, or otherwise, in domestic and international settings. These future case studies would benefit from a focus on investigating the regulatory approaches used, what worked and what didn't, and what can be learned from them and applied to future regulatory development.

7. Conclusions

High-hazard CPS are becoming increasingly reliant on their cyber components for basic and critical safety-related functions, growing in complexity, and combining with an ever-growing number of other CPS to create complex systems of CPS. Given this increase in complexity and reliance on cyber components, the cyberworthiness of high-hazard CPS and complex systems of CPS must be appropriately considered to ensure that their physical output remains safe and available when needed.

Several international standards and various guides and frameworks have been developed by national governments for developers, operators, maintainers, owners, and regulators of high-hazard CPS. These standards and frameworks enable self-regulation of activities that contribute to achieving a rudimentary level of cyberworthiness in CPS, based on cybersecurity principles. As shown in this article through the analysis of several international bodies concerned with the safety of different types of high-hazard CPS and their respective domestic regulators, there are numerous ways in which CPS can be regulated. Applying their guides, standards, and regulations alone does not yet achieve cyberworthiness for high-hazard CPS, nor does it amount to systematic regulation of the safety of the physical outputs of high-hazard CPS and CSoCPS.

Moreover, as CPS become more prevalent and are used to undertake more hazardous tasks, the need to regulate them for safety becomes greater, and potential regulators are not currently fully equipped to do so. Given the rapid pace of technological change, legislation and regulators empowered by legislation have trouble keeping up. For existing regulators to effectively regulate the cyberworthiness of CPS and ensure desired safety outcomes, applying contemporary complex systems governance theory and techniques in a principles-based approach is advisable. Through a principles-based approach to the regulation of cyberworthiness, and the application of the essential elements of cyberworthiness regulation outlined in Section 5 of this paper, the entities responsible for

 doi:10.20944/preprints202508.0294.v1

the safe operation of high-hazard CPS and CSoCPS could apply their deep knowledge and understanding of their CPS to better assure the safety and ongoing availability of the physical outputs of their CPS.

This paper establishes three core contributions that will benefit regulators of high-hazard CPS and the regulated communities alike, as follows: (1) the undertaking of a Regulatory Gap Analysis; (2) establishing cyberworthiness as a governance mandate for CPS; and (3) development of a principles-based complex systems governance framework for cyberworthiness. Drawing from the study's findings, we propose several potential short-term, mid-term, and long-term strategies that can serve as regulatory pathways for implementing cyberworthiness governance requirements.

Without these steps, high-hazard CPS will remain vulnerable to asymmetric threats where minor cyber faults or minor cybersecurity deficiencies may trigger physical catastrophes. Regulators must transition from cybersecurity checklist approaches to CPS safety compliance to a physical consequence-focused cyberworthiness governance model —a paradigm shift this paper seeks to catalyze.

Author Contributions: Conceptualization, M.V., K.J., and L.Q.; methodology, M.V., F.D., K.J., and L.Q.; software, M.V. and K.J.; validation and formal analysis, M.V., F.D., and R.H.; investigation, M.V. and F.D.; resources, M.V., F.D., K.J., and L.Q.; data curation, M.V.; writing—original draft preparation, M.V.; writing—review and editing, M.V., F.D., K.J., L.Q., R.H. and E.S.; visualization, M.V.; supervision, M.V., K.J., L.Q., and E.S.; project administration, M.V., K.J., and L.Q.; funding acquisition, M.V. and K.J.. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The only data used in this research were drawn from public sites as listed, and the results are presented in tables herein.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CSG	Complex Systems Governance
OT	Operational Technology
ICT	Information and Communication Technology
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
ICS	Industrial Control System
IoT	Internet of Things
CPS	Cyber-Physical System
CSoCPS	Complex System of Cyber-Physical Systems
FAA	Federal Aviation Authority
IAEA	International Atomic Energy Agency
OECD	Organisation for Economic Co-operation and Development
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ISO	International Standards Organization
ENISA	European Union Agency for Cybersecurity
NIST	National Institute of Standards and Technology
USCG	United States Coast Guard
EMSA	European Maritime Safety Agency
AMSA	Australian Maritime Safety Authority
EASA	European Aviation Safety Agency

 doi:10.20944/preprints202508.0294.v1

CASA	Australia –Civil Aviation Safety Authority
NRC	Nuclear Regulatory Commission
ENSREG	European Nuclear Safety Regulators Group
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
IMO	International Maritime Organization
ICAO	International Civil Aviation Organization
HA	(Australian Department of) Home Affairs
ACSC	Australian Cyber Security Centre

References

1. CISCO, Cisco Annual Internet Report (2018-2023) Public White Paper, 2020.
2. Hogan, M. and E. Newton (2015). Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity NIST. NISTIR 8074 Volume 2
3. Stouffer, K., et al. (2023). Guide to Operational Technology (OT) Security. U. S. D. o. Commerce. Washington, U.S. Department of Commerce
4. Mattioli, R. and K. Moulinos (2015). Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors. Heraklion, Greece, European Union Agency For Network And Information Security.
5. Ross, R. and V. Pillitteri (2024). Protecting Controlled Unclassified Information in Non federal Systems and Organizations.
6. Ross, R., et al. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Washington, U.S. Department of Commerce.
7. S. Engell. et al., 2015, Cyber Physical Systems Design, Modelling, and Evaluation - Core Research and Innovation Areas in Cyber-Physical Systems of Systems Initial Findings of the CPSoS Project, Springer
8. NSF (2024). Cyber-Physical Systems - National Science Foundation 24-581. Alexandria, VA, National Science Foundation.
9. NITRD (2015). Cyber Physical Systems (CPS) Vision Statement, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT.
10. Fowler, S. and E. Sitnikova (2019). "Toward a Framework for Assessing the Cyber-worthiness of Complex Mission Critical Systems." Military Communications and Information Systems Conference.
11. Liveri, D., et al. (2020). RAILWAY CYBERSECURITY - Security measures in the Railway Transport Sector. Attiki, Greece, European Union Agency for Cybersecurity.
12. Pauna, A. (2014). Certification of Cyber Security skills of ICS/SCADA professionals
13. Smith, D. and Tombs, S. (1995). Beyond Self-Regulation: Towards a Critique of Self-Regulation as a Control Strategy for Hazardous Activities. Journal of Management Studies 32:5 September 1995
14. Devereaux. J.E., 2010, Obsolescence: A Systems Engineering and Management Approach for Complex Systems, Massachusetts Institute of Technology (February 2010).
15. Turki Alelyani et al. 2019.Procedia Computer Science 153 (2019) 135–145, A literature review on obsolescence management in COTS-centric cyber physical systems, 17th Annual Conference on Systems Engineering Research (CSER),
16. A. Barichella et al. (eds.), The Threat of Technological Obsolescence for Cybersecurity in the Energy Sector, The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions, Palgrave Studies in Energy Transitions, https://doi.org/10.1007/978-3-031-04196-9_6-1
17. Commonwealth of Australia, 2025, Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025
18. The Office of Best Practice Regulation, Department of the Prime Minister and Cabinet, Australian Government Guide to Regulatory Impact Analysis (Guide, 30 March 2020) ('Australian Government Guide to Regulatory Impact Analysis').
19. R Baldwin, C Scott and C Hood, A Reader on Regulation (Oxford, 1998); R Baldwin and M Cave, Understanding Regulation (Oxford, 1999) in Julia Black, 'Decentring Regulation: Understanding the Role

 doi:10.20944/preprints202508.0294.v1

of Regulation and Self-regulation in a 'Post-regulatory' World' [2001] Vol 54 (Issue 1) Current Legal Problems 1403-146.

20. United States Code, 2019, Title 14 Coast Guard – Part 101 to 106, ESTABLISHMENT AND DUTIES, Office of the Law Revision Counsel
21. International Atomic Energy Agency, 2023, Safeguards Statement for 2023
22. Handl. G and Svendsen. K, 2019, Managing the Risk of Offshore Oil and Gas Accidents – The International Legal Dimension, Edward Elgar Publishing
23. Dixon-Woodsa. M et al., 2011, Why is UK medicine no longer a self-regulating profession? The role of scandals involving "bad apple" doctors, Social Science & Medicine.
24. Ben Mathews, 'Optimising Implementation of Reforms to Better Prevent and Respond to Child Sexual Abuse in Institutions: Insights from Public Health, Regulatory Theory, and Australia's Royal Commission' (2017) 74(Dec 2017) Child abuse & neglect 86.
25. Maurer. M, and von Engelhardt, 2013, Industry self-governance: A new way to manage dangerous technologies, Bulletin of the Atomic Scientists, Sage.
26. Coglianese. C, et.al., 2003, Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection, 55 Admin. L. Rev 705
27. Wilpert.B, 2007, Regulatory styles and their consequences for safety, Safety Science 46 (Elsevier)
28. Leveson.N, 2011, The Use of Safety Cases in Certification and Regulation, ESD-WP-2011-13, Massachusetts Institute of Technology Engineering Systems Division
29. National Fire Protection Association, 2023, National Electrical Code- NFPA 70 (web page), accessed 06 Jun 2025 via: https://www.nfpa.org/codes-and-standards/nfpa-70-standard-development/70
30. National Fire Protection Association, 2023, National Electrical Code- NFPA 70, US
31. Carter R.B and Marchant G.E, 2011, The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight – The Pacing Problem. Chapter 10 – Principles-Based Regulation and Emerging Technology, The International Library of Ethics , Law and Technology, Volume 7, Springer, London
32. National Offshore Petroleum Safety and Environmental Management Authority, 2020, Guidance Note, The safety case in context: An overview of the safety case regime, Document No: N-04300-GN0060 A86480
33. Commonwealth of Australia, 2009, Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009
34. House-Committee, T. I. (2020). 737 MAX Report for Public Release. U. S. H. o. Representatives. Washington, DC, House Committee on Transportation and Infrastructure.
35. Lindøe, P. H., Baram, M., & Renn, O. (Eds.). (2013). Risk governance of offshore oil and gas operations. Cambridge University Press.
36. Shavell. S, 1983, Liability for Harm Versus Regulation of Safety, Working Paper No. 1218, National Bureau of Economic Research, Cambridge, Massachusetts.
37. Farwell, J. P. and R. Rohozinski (2011). "Stuxnet and the Future of Cyber War." Survival 53(1): 23-40.
38. Pechtol, C. (2024). CrowdStrike IT Outage: Impacts to Public Safety Systems and Considerations for Congress
39. N.PAG (2023). "What CIOs Can Learn from the Massive Optus Outage."
40. Commonwealth of Australia, 2024, Security of Critical Infrastructure Act 2018, Australia
41. Department of Home Affairs, 2024, Australian Government Protective Security Policy Framework, Canberra, Australia
42. Code of Federal Regulations, 2024, Title 14 Aeronautics and Space – Parts 1 to 59, Office of the Federal Register, National Archives and Records Administration
43. European Union Aviation Safety Agency, 2024, Easy Access Rules for Initial Airworthiness and Environmental Protection
44. US Government Accountability Office, 2020, Aviation Cybersecurity – FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks, GAO-21-86, Report to Congressional Requesters
45. Keating. C, Katina. P, 2019, Complex system governance: Concept, utility, and Challenges, Systems Research and Behavioral Science

 doi:10.20944/preprints202508.0294.v1

46. European Union, 2007, Official Journal of the European Union, Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007.
47. European Union, 2019, Regulation (Eu) 2019/881 of The European Parliament and of The Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the European Union,
48. International Maritime Organization, 2018, SOLAS 2018 Consolidated Edition.
49. International Maritime Organization, 2017, Annex10 - Resolution MSC.428(98) Maritime Cyber Risk Management In Safety Management Systems.
50. BIMCO et al., 2020, The Guidelines on Cyber Security Onboard Ships, Version 4
51. NIST, 2024, The NIST Cybersecurity Framework (SCF) 2.0,
52. ICAO, 2018, Annex 8 to the Convention on International Civil Aviation – Airworthiness of Aircraft
53. ICAO, 2014, Airworthiness Manual, Third Edition
54. ICAO, 2018, Annex 14 to the Convention on International Civil Aviation – Aerodromes – Volume 1: Aerodrome Design and Operations.
55. ICAO, 2017, Annex 17 to the Convention on International Civil Aviation – Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference, Tenth Edition.
56. ICAO, 2022, Cybersecurity Policy Guidance
57. ICAO, 2022, Aviation Security Manual (Doc 8973 – Restricted), Third Edition.
58. IAEA, 2025, Long Term Structure of The IAEA Safety Standards and Current Status.
59. IAEA, 2024, IAEA Safety Standards – protecting people and the environment.
60. IAEA, 2023, IAEA Nuclear Security Series.
61. IAEA, 2024, Regulatory Oversight of the Interfaces between Nuclear Safety and Nuclear Security in Nuclear Power Plants, Technical Report Series No.1003
62. IAEA, 2023, A Systems View of Nuclear Security and Nuclear Safety: Identifying Interfaces and Building Strategies, AdSec/INSAG Report No. 1
63. IAEA, 2020, Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, IAEA Nuclear Energy Series No. NR-T-3.30
64. IAEA, 2021, Computer Security for Nuclear Security, Implementing Guide, IAEA Nuclear Security Series No. 42-G
65. IAEA, 2021, Computer Security Techniques for Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 17-T(Rev.1)
66. USCG, 2025, Fact Sheet: U.S. Coast Guard Issues Final Rule & Request for Comments on New Cybersecurity Regulations for the Marine Transportation System.
67. U.S Department of Homeland Security Coast Guard, 2025, Cybersecurity in the Marine Transportation System, Federal Register Vol. 90, No. 112025 Rules and Regulations
68. U.S Department of Homeland Security Coast Guard, 2020, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, Navigation And Vessel Inspection Circular NO. 01-20.
69. U.S Department of Homeland Security Coast Guard, 2025, Small Entity Compliance Guide for MTSA-regulated Facilities and OCS Facilities, The U.S. Coast Guard Cybersecurity Regulations for the Marine Transportation System.
70. U.S Department of Homeland Security Coast Guard, 2025, Small Entity Compliance Guide for MTSA-regulated U.S.-Flagged Vessels, The U.S. Coast Guard Cybersecurity Regulations for the Marine Transportation System.
71. IMO, 2017, Maritime Cyber Risk Management in Safety Management Systems, Annex 10 Resolution MSC.428(98).
72. IMO, 2022, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.2.
73. US Code of Federal Regulations, 2024, Part 21 – Certification Procedures for Products and Articles, Title 14 – Aeronautics and Space.

 doi:10.20944/preprints202508.0294.v1

74. US Code of Federal Regulations, 2025, Part 139 – Certification of Airports, Title 14 – Aeronautics and Space.
75. US Government, 2016, FAA Extension, Safety and Security Act of 2016. Public Law 114–190, As Amended Through P.L. 118–63, Enacted May 16, 2024
76. United States, 2017, Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Federal Register Vol. 82, No. 93, Presidential Documents
77. United States, 2021, Executive Order 14028 of May 17, 2021, Improving the Nation's Cybersecurity, Federal Register Vol. 86, No. 93, Presidential Documents
78. US Department of Transport, 2011, DOT Order 1351.37 Departmental Cybersecurity Policy.
79. Federal Aviation Administration, 2025, Memorandum (dated 12 May 2025) - Reauthorization Program Guidance Letter (R-PGL) 25-06: Planning and Project Eligibility
80. Aerospace Industries Association (Isidore Venetos), 2020, Overview of Cyber Safety – Cyber Safety Commercial Aviation Team.
81. US Nuclear Regulatory Commission, 2010, Regulations: Title 10, Code of Federal Regulations
82. US Nuclear Regulatory Commission, 2010, Cyber Security Programs for Nuclear Facilities, Regulatory Guide Office of Nuclear Regulatory Research.
83. US Nuclear Regulatory Commission, 2025, Digital Instrumentation and Controls Research; accessed 15 March 2025 via: https://www.nrc.gov/about-nrc/regulatory/research/digital.html#7
84. Stabelin H., 2025, What is NIST and Why Is It Critical to Cybersecurity?; accessed 29 April 2025 via: https://segura.security/post/what-is-nist.
85. Stouffer K., et al., 2023, Guide to Operational Technology (OT) Security, NIST Special Publication - NIST SP 800-82r3
86. European Union, 2002, establishing a European Maritime Safety Agency, Regulation (EC) No 1406/2002 of the European Parliament and of the Council.
87. European Union, 2024, EU Maritime Security Strategy.
88. European Commission and EMSA, 2023, Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections.
89. European Border and Coast Guard Agency (Frontex), 2022, Working together at sea: European cooperation on coast guard functions.
90. European Union, 2018, Regulation (EU) 2019/881 of The European Parliament and of The Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency.
91. European Union, 2018, Regulation (EU) 2019/881 of The European Parliament and of The Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency
92. European Union, 2012, Commission Regulation (EU) No 784/2012 - laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations
93. European Union, 2012, Commission Implementing Regulation (EU) No 2023/1769 - laying down technical requirements and administrative procedures for the approval of organisations involved in the design or production of air traffic management/air navigation services systems and constituents
94. European Union Aviation Safety Agency, 2025, Easy Access Rules for Air Operations.
95. European Union Aviation Safety Agency, 2024, Easy Access Rules for Aerodromes.
96. European Union Aviation Safety Agency, 2024, Easy Access Rules for Continuing Airworthiness
97. ECCSA, 2025, European Centre for Cybersecurity in Aviation (ECCSA), accessed via: https://www.easa.europa.eu/en/eccsa, accessed 05 April 2025.
98. European Strategic Coordination Platform, 2019, Strategy for Cybersecurity in Aviation,
99. European Nuclear Safety Regulators Group, 2011, European High Level Group on Nuclear Safety and Waste Management Revised Rules Of Procedure.
100. European Nuclear Safety Regulators Group, 2012, ENSREG WG Rules of Procedure.
101. European Union, 2019, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.
102. ENISA, 2019, INDUSTRY 4.0 Cybersecurity: Challenges & Recommendations.

 doi:10.20944/preprints202508.0294.v1

103. ENISA, 2018, IoT Security Standards Gap Analysis Mapping of existing standards against requirements on security and privacy in the area of IoT .
104. ENISA, 2017, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.
105. ENISA, 2018, Good Practices for Security of Internet of Things in the context of Smart Manufacturing.
106. ENISA, 2016, Securing Smart Airports.
107. ENISA, 2019, Good Practices for Security of IOT Secure Software Development Lifecycle
108. ENISA, 2016, Communication network dependencies for ICS/SCADA Systems.
109. ENISA, 2010, Flying 2.0 Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology
110. Commonwealth of Australia, 2014, Australian Maritime Safety Authority Act 1990, Australia
111. Australian Maritime Safety Authority, Marine Order:
112. 12 (Construction - subdivision and stability, Machinery and electrical installations) 2023, Australia
113. 15 (Construction — fire protection, fire detection and fire extinction) 2014, Australia
114. 21 (Safety and emergency arrangements) 2016, Australia
115. 27 (Safety of navigation and radio equipment) 2023, Australia
116. 58 (Safe management of vessels) 2020, Australia
117. 72 (Engineer officers) 2014, Australia
118. Index of marine orders | Australian Maritime Safety Authority - https://www.amsa.gov.au/about/regulations-and-standards/index-marine-orders
119. Commonwealth of Australia, 2024, Civil Aviation Act 1988, Australia
120. Commonwealth of Australia, 2024, Civil Aviation Regulations 1988 - Volume 1, Australia
121. Commonwealth of Australia, 2024, Civil Aviation Regulations 1988 - Volume 2, Australia
122. Civil Aviation Safety Authority, 2025, Part 91 (General Operating Flight Rules) Manual of Standards 2020, Australia
123. Civil Aviation Safety Authority, 2024, Part 121 (Australian Air Transport Operations – Larger Aeroplanes) Manual of Standards 2020, Australia
124. Civil Aviation Safety Authority, 2024, Part 138 (Aerial Work Operations) Manual of Standards 2020, Australia
125. Civil Aviation Safety Authority, 2024, Part 139 (Aerodromes) Manual of Standards 2019, Australia
126. Civil Aviation Safety Authority, 2016, Manual of Standards Part 171 Aeronautical Telecommunication and Radio Navigation Services, Australia
127. Civil Aviation Safety Authority, 2023, Manual of Standards Part 172 Air Traffic Services Version 2.2, Australia
128. Civil Aviation Safety Authority, 2024, Roadmap – RPAS and AAM Strategic Regulatory Roadmap, Australia
129. Commonwealth of Australia, 2024, Australian Radiation Protection and Nuclear Safety Act 1998, Australia
130. Commonwealth of Australia, 2024, Australian Radiation Protection and Nuclear Safety Regulations 1998, Australia
131. Commonwealth of Australia, 2024, Cyber Security Act 2024, Australia.
132. Commonwealth of Australia, 2025, Cyber Security (Security Standards for Smart Devices) Rules 2025, Australia.
133. Mark Bristow and Irving Lachow, 2025, Past is Prologue: Creating a Civil Defense Mindset to Address Modern Cyber Threats, The Mitre Corporation
134. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
135. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
136. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls International Organization for Standardization (ISO), 27001 Cybersecurity Framework.

 doi:10.20944/preprints202508.0294.v1

137. Alessandro Fantechi and Pateizio Pelliccione (Eds.), 2015, Software Engineering for Resilient Systems, 7th International Workshop, SERENE 2015, Paris, France
138. Jiaxin Wu. Pingfeng Wang, 2019, A Comparison of Control Strategies for Disruption Management in Engineering Design for Resilience, ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, ASME Part B: Mechanical Engineering
139. Leandros Maglaras, Helge Janicke and Mohamed Amine Ferrag, 2022, Cyber Security and Critical Infrastructures, Printed Edition of the Topics Published in Applied Sciences, Electronics, Future Internet, Sensors and Smart Cities
140. Ikjae Kim. et al., 2024, A Study on the Multi-Cyber Range Application of Mission-Based Cybersecurity Testing and Evaluation in Association with the Risk Management Framework, MDPI, Journal of Information
141. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risk
142. AS/NZS 3000:2018 - Electrical installations (known as the Australian/New Zealand Wiring Rules)
143. Fowler S., Joiner K.F. and Ma S., 2025: accepted, 'Assessing Cyberworthiness of Complex System Capabilities using the Cyber Evaluation and Management Toolkit (CEMT)', Computers and Security.
144. Nanyonga A; Wasswa H; Joiner K; Turhan U; Wild G, 2025, 'Explainable Supervised Learning Models for Aviation Predictions in Australia', Aerospace, 12, http://dx.doi.org/10.3390/aerospace12030223
145. Klein N.K., Geyer M.A., Hinds M.A. and Koerner S.C., 2025: accepted, 'Beyond Accuracy: Evaluating Bayesian Neural Networks in a Real-World Application', ITEA Journal of Testing, International Test and Evaluation Association, 46(3)
146. Rausch, A., Sedeh, A. M., & Zhang, M. (2021). Autoencoder-Based Semantic Novelty Detection: Towards Dependable AI-Based Systems. Applied Sciences, 11(21), Article 9881. https://doi.org/10.3390/app11219881
147. Christoph Torens, Franz Juenger, Sebastian Schirmer, Simon Schopferer, Dmytro Zhukov and Johann C. Dauer. "Ensuring Safety of Machine Learning Components Using Operational Design Domain," AIAA 2023-1124. AIAA SCITECH 2023 Forum. January 2023
148. Mutambik, I. 2025, 'A Hybrid CNN–BiLSTM Framework Optimized with Bayesian Search for Robust Android Malware Detection', Systems 2025, 13(7), 612; https://doi.org/10.3390/systems13070612
149. Eshun, E. A., Waters, S., & Amoako, R. O. (2024). Implicating Communication: An Analysis of the US House Committee on Transportation and Infrastructure's Investigative Report of the Boeing 737 MAX Crises. Journal of Contingencies and Crisis Management, 32(4), Article e70006. https://doi.org/10.1111/1468-5973.70006
150. Whittfield C., Jones P., Kelly H. and Lim, L. (2025), 'Demystifying Australia's Security of Critical Infrastructure Regime', Herbert Smith Freehills Kramer LLP 2025, 28 April, accessed on 1 August 2025 at https://www.hsfkramer.com/insights/2023-03/demystifying-australias-recent-security-of-critical-infrastructure-act-reforms