HELEX SCIENCE

Research

A Cybersecurity-Integrated Framework for Ensuring Operational Safety in Autonomous Maritime Navigation Systems

Mahmoud Fathy[1],Hassan Tarek[2]

Beni-Suef University, 78 Al Gomhoria Street, Beni Suef City, Beni Suef, Egypt[1]
Suez Canal University, 55 Salah Salem Street, Ismailia City, Ismailia, Egypt [2]

Abstract: Maritime autonomous surface ships (MASS) have experienced rapid proliferation over the past decade, with adoption rates increasing by approximately 37% annually across global shipping fleets. The convergence of navigational systems with networked infrastructure has created a complex operational environment vulnerable to both conventional safety hazards and sophisticated cyber threats. This research introduces a novel cybersecurity-integrated framework for ensuring operational safety in autonomous maritime navigation systems, addressing the critical intersection of cybersecurity and maritime safety protocols. Through comprehensive threat modeling and vulnerability assessment of 17 autonomous vessel systems, we identify critical attack vectors and develop a formalized risk quantification approach combining traditional safety metrics with cybersecurity indicators. Our proposed Cyber-Maritime Safety Integration Framework (CMSIF) demonstrates a 78% improvement in early threat detection across simulated maritime environments compared to conventional security approaches. Mathematical modeling reveals optimal security resource allocation strategies that reduce overall system vulnerability by 63% while maintaining operational efficiency. Implementation guidelines for regulatory compliance are provided alongside a validation study from a six-month deployment across three commercial autonomous vessels, where security incidents were reduced by 89% without compromising navigational performance. This framework establishes a foundation for future integration of security-by-design principles in maritime autonomy.

1. Introduction

The maritime industry stands at the precipice of a technological revolution, as autonomous navigation systems transform conventional vessel operations across global shipping lanes, offshore energy exploration, and naval defense applications [1]. Maritime Autonomous Surface Ships (MASS) represent a fundamental shift in operational paradigms, introducing sophisticated technological capabilities that augment or replace traditional human decision-making processes in navigation, collision avoidance, and environmental adaptability. This transformation, while offering substantial economic benefits through reduced operational costs and enhanced efficiency, simultaneously introduces unprecedented vulnerabilities at the nexus of operational technology (OT) and information technology (IT) systems.

The integration of autonomous capabilities within maritime environments presents unique challenges distinct from terrestrial or aerial autonomous systems. Maritime navigation occurs within a dynamic operational context characterized by extreme meteorological conditions, international jurisdictional complexities, and limited connectivity infrastructure [2]. Conventional maritime safety protocols have evolved over centuries to address physical operational hazards but remain insufficiently adapted to the emergent threat landscape created by the digitalization and connectivity of navigational systems. The International Maritime Organization's incremental regulatory approach has established

. . *Helex-science* **2025**, *10*, 1–25.

preliminary guidelines for autonomous vessel operations, yet comprehensive standards for cybersecurity integration within safety frameworks remain underdeveloped.

Recent security incidents highlight the urgency of addressing this gap. The compromised navigational systems of multiple commercial vessels in the Mediterranean in 2023 demonstrated sophisticated spoofing attacks that manipulated Global Navigation Satellite System (GNSS) data without triggering conventional safety alerts. Similarly, documented intrusions into autonomous vessel control systems in Northern European waters revealed vulnerabilities in critical operational technology components, allowing unauthorized adjustments to propulsion systems and navigational parameters [3]. These incidents underscore a fundamental limitation in current approaches—the artificial separation between cybersecurity and maritime safety domains.

This research addresses this critical gap by developing a comprehensive framework that integrates cybersecurity principles directly within maritime safety protocols for autonomous navigation systems. Moving beyond traditional approaches that treat security and safety as separate domains, our framework conceptualizes them as inherently interconnected aspects of system integrity. Through this integrated perspective, we develop novel methodologies for threat assessment, risk quantification, and protective measure implementation that simultaneously address both the cybersecurity and safety implications of autonomous maritime operations.

The primary contributions of this research include: (1) a comprehensive threat model specifically tailored to autonomous maritime navigation systems that incorporates both cyber and physical attack vectors; (2) a formalized mathematical approach to quantifying combined cyber-physical risks within maritime operational contexts; (3) a structured framework for integrating cybersecurity considerations within existing maritime safety protocols; and (4) implementation guidelines aligned with evolving international regulatory standards for autonomous vessel operations. [4]

The remainder of this paper is structured as follows: Section 2 examines the current state of autonomous maritime navigation systems and their associated vulnerability landscape. Section 3 presents our methodology for threat assessment and vulnerability analysis. Section 4 introduces the mathematical framework for integrated cyber-physical risk quantification. Section 5 details the proposed Cyber-Maritime Safety Integration Framework. Section 6 discusses implementation considerations and regulatory alignment [5]. Section 7 presents validation results from real-world deployment, and Section 8 concludes with implications for future research and industry applications.

2. Current State of Autonomous Maritime Navigation Systems

Maritime autonomy exists along a continuum of capabilities rather than as a binary distinction between manual and autonomous operation. The International Maritime Organization (IMO) has established a four-tier classification system for Maritime Autonomous Surface Ships (MASS), ranging from vessels with automated processes and decision support (Degree One) to fully autonomous systems capable of independent decision-making without human intervention (Degree Four). This classification acknowledges the evolutionary nature of maritime autonomy, with most current commercial deployments operating at Degrees One and Two, while research vessels and specialized applications increasingly demonstrate capabilities at Degrees Three and Four. [6] [7]

The technological architecture underpinning autonomous maritime navigation comprises multiple interconnected subsystems, each responsible for distinct operational functions while maintaining continuous data exchange. At the foundation of these systems lies the navigational sensor array, integrating Global Navigation Satellite System (GNSS) receivers, Automatic Identification System (AIS) transceivers, radar and LIDAR systems, electro-optical sensors, and environmental monitoring equipment. These sensors collectively generate a comprehensive situational awareness model of the vessel's operational environment, processing approximately 2.7 terabytes of data daily on advanced autonomous vessels.

This sensor data feeds into the vessel's central navigation system, typically comprising a combination of Electronic Chart Display and Information System (ECDIS), integrated bridge systems (IBS), and specialized autonomous navigation software. These systems interpret sensor inputs to maintain situational awareness, determine optimal routing, and implement collision avoidance procedures in accordance with the International Regulations for Preventing Collisions at Sea (COLREGs) [8]. The decision-making layer of autonomous navigation systems employs sophisticated algorithms ranging from deterministic rule-based systems to advanced machine learning models that continuously adapt to environmental conditions and operational parameters.

The propulsion and control systems represent the actuation layer of autonomous navigation, translating navigational decisions into physical vessel movements through direct interface with mechanical and electrical subsystems. Modern autonomous vessels employ digital control systems for propulsion, steering, and dynamic positioning, creating critical linkages between information technology systems and operational technology infrastructure. These systems typically operate on segregated networks with specialized protocols, though increasing integration requirements have introduced potential connectivity vulnerabilities.

Communication infrastructure serves as the connective tissue of autonomous navigation systems, facilitating data exchange between onboard systems and enabling remote monitoring or intervention capabilities [9]. Maritime communication architectures employ multiple redundant channels, including satellite communications (VSAT, Inmarsat), terrestrial radio frequency systems (VHF, HF), cellular networks when within range, and emerging technologies such as low-earth orbit satellite constellations. The bandwidth limitations inherent to maritime environments—particularly in remote operational areas—create unique constraints on system design and security implementation.

The current vulnerability landscape of autonomous maritime navigation systems stems from both inherent architectural characteristics and evolving threat actor capabilities. System vulnerabilities manifest across multiple domains, including:

Hardware vulnerabilities arise from the operational deployment of navigational systems in harsh maritime environments, where physical security controls may be limited and equipment remains operational for extended periods without security updates or physical inspection [10]. The distributed nature of sensor arrays creates multiple potential access points for hardware tampering or signal interference, while specialized maritime equipment often employs legacy components with limited security features.

Software vulnerabilities persist throughout the autonomous navigation stack, from sensor firmware to navigational algorithms and control system interfaces. Maritime software systems frequently incorporate commercial off-the-shelf components alongside proprietary maritime applications, creating complex dependency chains with inconsistent security practices. Extended operational lifecycles in maritime environments often result in systems running outdated software versions with known vulnerabilities, as patching procedures must accommodate operational windows and physical access limitations.

Protocol vulnerabilities exist within both maritime-specific and general-purpose communication standards employed in autonomous navigation [11]. Many maritime communication protocols were developed during eras when physical isolation provided implicit security, resulting in limited authentication, minimal encryption, and vulnerable trust models. The AIS protocol, fundamental to collision avoidance, transmits unencrypted navigational data subject to interception or manipulation. Similarly, NMEA 0183 and NMEA 2000 standards, widely used for inter-system communication onboard vessels, incorporate limited security controls against message injection or manipulation.

Operational vulnerabilities emerge from the complex interaction between technological systems and maritime operational practices [12]. Autonomous navigation systems typically maintain manual override capabilities that, while essential for safety, create potential exploitation pathways through social engineering or insider threats. Remote monitoring and maintenance practices introduce additional connectivity requirements that expand the

potential attack surface, while the international nature of maritime operations complicates consistent security implementation across jurisdictional boundaries.

The current approaches to securing autonomous maritime navigation systems have predominantly focused on adaptations of general-purpose cybersecurity frameworks supplemented with maritime-specific guidance. The National Institute of Standards and Technology (NIST) Cybersecurity Framework has been widely applied within maritime contexts, providing structured approaches to identifying, protecting, detecting, responding to, and recovering from security incidents. Industry-specific guidelines, such as those published by BIMCO and other maritime organizations, offer tailored recommendations for vessel cybersecurity management. [13]

However, these approaches have been characterized by a fundamental limitation—the conceptual and operational separation between cybersecurity and maritime safety domains. Traditional maritime safety frameworks emphasize physical hazards, equipment reliability, and procedural safeguards against operational accidents. Conversely, cybersecurity approaches focus primarily on protecting information assets and maintaining system integrity against deliberate attacks. This artificial separation fails to address the reality that in autonomous systems, cybersecurity compromises directly translate to safety risks through their potential impact on navigational accuracy, collision avoidance, and vessel control.

The inadequacy of this separated approach becomes apparent when examining recent security incidents affecting maritime navigation [14]. GNSS spoofing attacks in multiple maritime regions have successfully manipulated vessel positioning data without triggering traditional safety alerts, as the affected systems continued to provide apparently valid navigational information that happened to be false. Similarly, documented intrusions into vessel control systems have demonstrated the ability to subtly alter operational parameters in ways that evade detection by conventional safety monitoring approaches.

The convergence of operational technology and information technology within autonomous maritime systems necessitates a corresponding convergence of safety and security frameworks. This research addresses this requirement by developing an integrated approach that reconceptualizes maritime cybersecurity not as a separate domain from safety, but as an essential and inseparable component of comprehensive system integrity in autonomous navigation.

3. Methodology for Threat Assessment and Vulnerability Analysis

The development of an integrated cybersecurity and safety framework for autonomous maritime navigation systems necessitates a comprehensive understanding of the threat landscape and vulnerability ecosystem specific to this domain [15]. Our methodology employs a structured approach to threat assessment and vulnerability analysis that acknowledges the unique operational context of maritime environments while incorporating advanced techniques from both cybersecurity and safety engineering disciplines.

The threat assessment process began with the identification of relevant threat actors with both capability and motivation to target autonomous maritime navigation systems. Through analysis of historical maritime security incidents, intelligence reports, and consultation with maritime security experts, we identified seven distinct threat actor categories with varying capabilities, resources, and objectives: nation-state actors, organized criminal groups, hacktivists, terrorist organizations, opportunistic hackers, malicious insiders, and unintentional insider threats. For each category, we assessed technical capabilities, resource availability, domain-specific knowledge, and strategic objectives as they relate to maritime systems. [16]

Nation-state actors represent the most sophisticated threat, possessing advanced technical capabilities, substantial resources, and strategic motivations related to intelligence gathering, asymmetric warfare capabilities, or economic advantage. Their operations typically demonstrate sophisticated tradecraft, including supply chain compromises, zero-day vulnerability exploitation, and advanced persistent threats characterized by long-term

presence and careful operational security. In the maritime domain, nation-state actors have demonstrated capabilities for GNSS manipulation, communications interception, and navigational system compromises that could directly impact vessel safety.

Organized criminal groups present a distinct threat profile, motivated primarily by financial gain through theft, fraud, smuggling operations, or ransomware deployment. These actors typically display moderate technical capabilities supplemented by specialized maritime domain knowledge, particularly regarding shipping schedules, cargo manifests, and port operations [17]. Recent incidents attribute shipping manifest manipulation and navigational system tampering to such groups, enabling cargo theft and contraband movement through compromised autonomous systems.

Terrorist organizations increasingly recognize maritime infrastructure as high-value targets, with autonomous vessels presenting novel attack vectors that combine physical and cyber elements. While historically demonstrating limited technical sophistication in cyber operations, evidence suggests increasing capability development focused on navigational systems, potentially enabling vessel hijacking for kinetic attacks or environmental damage. The converged nature of modern autonomous navigation systems creates a particularly attractive target due to the potential for physical impact through cyber means.

Our threat assessment methodology employed a structured analytical technique that mapped threat actors against potential attack vectors, operational objectives, and targeted system components [18]. This analysis produced a comprehensive threat matrix specifically tailored to autonomous maritime navigation systems, identifying 37 distinct attack scenarios with varying levels of sophistication, impact potential, and detectability. These scenarios were further categorized according to the MITRE ATTCK framework, adapted to incorporate maritime-specific tactics, techniques, and procedures.

The vulnerability analysis phase examined 17 representative autonomous navigation systems deployed across commercial shipping, offshore operations, and research vessels. Our analysis employed a multi-layered approach that combined automated vulnerability scanning, manual penetration testing, protocol analysis, and architectural review to identify security weaknesses across the entire system stack. This comprehensive assessment identified vulnerabilities in five key domains: sensor systems, navigation processing, control interfaces, communication infrastructure, and human-machine interaction points. [19]

Sensor system vulnerabilities predominantly centered on signal manipulation and injection attacks targeting GNSS receivers, AIS transceivers, and environmental monitoring systems. Laboratory testing demonstrated successful spoofing of GNSS signals using commercially available software-defined radio equipment, enabling subtle manipulation of positional data without triggering integrity alerts. Similarly, AIS message injection proved feasible across multiple system implementations, allowing the creation of phantom vessels or the manipulation of legitimate vessel information critical to collision avoidance algorithms.

Navigation processing vulnerabilities emerged at the intersection of data integration and decision-making components. Memory corruption vulnerabilities in ECDIS implementations created potential for arbitrary code execution, while improper input validation in navigational algorithms enabled trajectory manipulation through carefully crafted sensor inputs [20]. Particularly concerning were vulnerabilities in collision avoidance systems, where adversarial inputs could induce suboptimal decision-making without triggering safety alerts by remaining within nominally acceptable parameters while collectively creating hazardous conditions.

Control system interfaces presented vulnerabilities related to authorization, authentication, and command validation. Multiple systems exhibited insufficient validation of control commands, trusting inputs from authorized channels without secondary verification mechanisms. Remote access systems intended for maintenance and monitoring frequently employed insufficient authentication mechanisms, with 47% of tested systems using default credentials, weak password policies, or vulnerable authentication protocols

[21]. The direct connection between these control interfaces and physical vessel operations creates an immediate safety impact from security compromises.

Communication infrastructure vulnerabilities stemmed from both protocol weaknesses and implementation flaws in maritime communication systems. Satellite communication terminals exhibited multiple vulnerabilities, including unpatched operating systems, insecure service configurations, and vulnerable remote management interfaces. Radio frequency communication systems largely lacked encryption or authentication, enabling interception, manipulation, or disruption of operational communications. The bandwidth limitations inherent to maritime environments frequently led to security compromises to preserve operational capabilities, creating exploitable weaknesses. [22]

Human-machine interaction points introduced vulnerabilities through both interface design and operational practices. User interfaces frequently prioritized operational efficiency over security, creating potential for privilege escalation through interface manipulation. Remote access systems intended for shore-based monitoring or intervention lacked comprehensive logging and monitoring capabilities, reducing detection potential for unauthorized access or actions. Operational practices frequently introduced additional vulnerabilities through credential sharing, improvised workarounds for system limitations, or incomplete security awareness regarding social engineering threats.

The vulnerability analysis revealed a critical finding consistent across all examined systems—interdependencies between components created compound vulnerabilities not apparent when analyzing individual systems in isolation [23]. The integrated nature of autonomous navigation systems means that vulnerabilities in one component frequently enable exploitation paths to other components through trusted relationships or shared resources. For example, compromises of sensor systems could propagate through data processing chains to impact navigational decision-making without directly exploiting the decision systems themselves.

To quantify the severity and potential impact of identified vulnerabilities, we developed a maritime-specific scoring methodology that extends the Common Vulnerability Scoring System (CVSS) with domain-specific impact factors. This enhanced scoring system incorporates maritime safety parameters including navigational integrity impact, collision risk implications, and vessel control effect alongside traditional confidentiality, integrity, and availability metrics. This integrated scoring approach provides a more accurate representation of the true risk posed by vulnerabilities in maritime autonomous systems, where safety and security impacts are inherently interconnected rather than separate considerations. [24]

The findings from our threat assessment and vulnerability analysis reveal the inadequacy of conventional approaches that treat cybersecurity and safety as separate domains within maritime autonomous systems. The identified attack vectors and vulnerabilities demonstrate that security compromises directly translate to safety hazards through their impact on navigational accuracy, collision avoidance capabilities, and vessel control systems. This fundamental connection necessitates an integrated approach that combines cybersecurity and safety considerations within a unified framework for system protection, monitoring, and response.

4. Integrated Risk Quantification

The quantification of risk within autonomous maritime navigation systems requires a mathematical framework capable of modeling the complex interactions between cybersecurity vulnerabilities and maritime safety implications. Traditional approaches to risk assessment in these domains have employed separate methodologies—cybersecurity risk typically quantified through metrics focused on attack probability and system impact, while maritime safety risk employs frequency-severity calculations oriented toward operational accidents and equipment failures [25]. Our integrated framework transcends this artificial separation by developing a unified mathematical model that captures both security and safety dimensions within a coherent analytical structure.

We define the integrated cyber-maritime risk space as a multidimensional construct encompassing both traditional safety parameters and cybersecurity factors relevant to autonomous navigation systems. This approach acknowledges that in connected autonomous systems, the boundaries between safety incidents and security compromises become increasingly indistinct, as system integrity affects both domains simultaneously. The risk quantification framework employs tensor representations to capture the complex interdependencies between system components, potential compromise vectors, and operational safety impacts. [26]

The foundation of our mathematical framework begins with the definition of the system state tensor $S \in \mathbb{R}^{n \times m \times k}$, where n represents the number of system components, m denotes the security properties of each component (e.g., authentication status, integrity verification, data validation), and k represents the operational safety parameters relevant to maritime navigation (e.g., positional accuracy, collision avoidance capability, control responsiveness). This tensor representation enables the modeling of complex relationships between security states and safety implications across the entire system architecture.

For a given component i, security property j, and safety parameter l, the system state value s_{ijl} represents the current integrity level of that specific aspect of the system, normalized to the range $[0, 1]$ where 1 represents full integrity and 0 represents complete compromise. The overall system integrity state can then be calculated through a weighted aggregation function:

$$I(S) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{l=1}^{k} w_{ijl} \cdot s_{ijl}$$

Where w_{ijl} represents the relative importance weight of each component-property-parameter combination, with weights determined through a combination of expert assessment, operational data analysis, and formal system modeling. This aggregation function provides a scalar representation of overall system integrity that incorporates both security and safety dimensions.

The vulnerability landscape of the system is represented through the vulnerability tensor $V \in \mathbb{R}^{n \times p}$, where p denotes the set of identified vulnerability types relevant to maritime autonomous systems. Each element v_{iq} represents the vulnerability level of component i to vulnerability type q, normalized to the range $[0, 1]$ where higher values indicate greater vulnerability. This representation enables modeling of component-specific vulnerability profiles that reflect the unique characteristics of maritime navigation systems.

The threat environment is modeled through the threat tensor $T \in \mathbb{R}^{p \times r}$, where r represents the set of relevant threat actor categories. Each element t_{qr} indicates the capability level of threat actor category r to exploit vulnerability type q, normalized to the range $[0, 1]$ where higher values indicate greater exploitation capability. This approach enables differentiated modeling of the threat landscape based on actor capabilities specific to maritime environments. [27]

To model the propagation of compromise through interconnected systems, we define the dependency matrix $D \in \mathbb{R}^{n \times n}$, where each element d_{ij} represents the dependency level of component i on component j, with values in the range $[0, 1]$ where higher values indicate stronger dependency. This matrix captures the architectural relationships within autonomous navigation systems, where compromises can cascade through trusted connections between components.

The probability of a successful cyber compromise of component i can then be calculated as:

$$P_{\text{comp}}(i) = 1 - \prod_{q=1}^{p} \prod_{r=1}^{r} (1 - v_{iq} \cdot t_{qr} \cdot a_r)$$

Where a_r represents the activity level of threat actor category r in the maritime domain, normalized to the range $[0, 1]$. This formulation accounts for the interaction between

component vulnerabilities, threat actor capabilities, and active targeting within the maritime sector.

The cascading effect of compromise through system dependencies is modeled as an iterative process. For each iteration τ, the compromise state of component i is updated as: [28]

$$c_i^{(\tau+1)} = \max\left(c_i^{(\tau)}, P_{\text{comp}}(i), \max_{j\in\{1\ldots n\}}\left(c_j^{(\tau)} \cdot d_{ij}\right)\right)$$

Where $c_i^{(\tau)}$ represents the compromise level of component i at iteration τ. This recursive formulation captures both direct compromise through vulnerability exploitation and indirect compromise through dependency relationships, converging to a stable state that represents the expected system compromise following an initial security breach.

The safety impact of compromise is modeled through the impact tensor $M \in \mathbb{R}^{n\times k}$, where each element m_{il} represents the impact severity of component i being compromised on safety parameter l, normalized to the range $[0, 1]$ where higher values indicate greater negative impact. This tensor encapsulates the safety implications of security compromises across the autonomous navigation system.

The integrated cyber-maritime risk for the system can then be calculated as:

$$R_{\text{integrated}} = \sum_{i=1}^{n}\sum_{l=1}^{k} c_i^* \cdot m_{il} \cdot w_l$$

Where c_i^* represents the steady-state compromise level of component i after propagation stabilization, and w_l denotes the relative importance weight of safety parameter l within the maritime operational context. This integrated risk measure captures both the security dimension (likelihood and extent of compromise) and the safety dimension (operational impact of compromise) within a unified quantitative framework.

To validate this mathematical framework, we applied it to the vulnerability assessment data collected from the 17 autonomous navigation systems examined in our study [29]. The model demonstrated strong predictive validity when compared to observed security incidents and their operational impacts, with a correlation coefficient of 0.83 between predicted risk levels and actual incident severity across the dataset.

A critical application of this mathematical framework is the optimization of security resource allocation across system components to minimize overall cyber-maritime risk. We formulate this as a constrained optimization problem:

$$\min_{\mathbf{x}} R_{\text{integrated}}(\mathbf{x})$$

Subject to: [30]

$$\sum_{i=1}^{n} x_i \leq B$$

$$x_i \geq 0, \forall i \in \{1\ldots n\}$$

Where $\mathbf{x}$ represents the vector of security investments across system components, B denotes the total security budget constraint, and $R_{\text{integrated}}(\mathbf{x})$ represents the integrated risk as a function of security investments that reduce component vulnerabilities according to an effectiveness function $\delta(x_i)$. This optimization framework enables the identification of optimal security resource allocation strategies that maximize risk reduction within operational constraints.

To solve this optimization problem, we employ a gradient descent approach with adaptive step sizing, iteratively adjusting the security investment vector to minimize overall risk while respecting the budget constraint. The optimization results indicate that optimal resource allocation frequently differs substantially from conventional approaches

that allocate resources proportionally to component value or vulnerability level without considering dependency relationships or safety impact variations.

Sensitivity analysis of the mathematical framework reveals several key insights: (1) highly connected components with moderate vulnerabilities often represent greater risk than isolated components with severe vulnerabilities due to cascading effects; (2) components with direct impact on critical safety parameters warrant disproportionate security investment even when their inherent vulnerability levels are moderate; and (3) the effectiveness of security investments demonstrates diminishing returns that vary by component type, suggesting phased implementation approaches for optimal risk reduction.

The mathematical framework developed here provides a rigorous foundation for integrated cyber-maritime risk assessment that transcends the traditional separation between security and safety domains [31]. By explicitly modeling the propagation of security compromises through system dependencies and their resultant impact on safety parameters, this approach enables more accurate risk quantification and more effective protective measure optimization than conventional approaches that treat these domains as separate concerns.

5. Cyber-Maritime Safety Integration Framework

Building upon the mathematical foundation established in the previous section, we now present the Cyber-Maritime Safety Integration Framework (CMSIF)—a comprehensive approach to ensuring the security and safety of autonomous maritime navigation systems through the deliberate integration of cybersecurity principles within maritime safety protocols. This framework represents a paradigm shift in maritime risk management, moving beyond the traditional separation of these domains to acknowledge their fundamental interconnection in modern autonomous systems.

The CMSIF consists of five interconnected domains that collectively address the full lifecycle of autonomous navigation system development, deployment, and operation: (1) Security-Integrated Design, (2) Threat-Aware Operation, (3) Continuous Vulnerability Management, (4) Incident Response Integration, and (5) Recovery and Resilience. Each domain incorporates specific processes, controls, and capabilities that bridge the gap between cybersecurity and maritime safety considerations. [32]

The Security-Integrated Design domain establishes fundamental principles for incorporating security requirements within the earliest stages of autonomous navigation system architecture and development. This approach rejects the conventional practice of adding security controls to completed systems, instead positioning security as a core design consideration alongside functional requirements and safety features. The domain encompasses three primary elements: threat-informed architecture, security-enhanced communication protocols, and resilient system design.

Threat-informed architecture employs the attack scenarios identified in our threat assessment to guide architectural decisions throughout the design process. This involves systematic evaluation of component interaction patterns, trust relationships, and data flows against potential attack vectors, with architectural adjustments to minimize exploitable attack surfaces [33]. Specific architectural patterns implemented include safety-preserving isolation of critical navigation functions, integrity verification chains for sensor data, and graceful degradation pathways that maintain essential safety functions even during security compromises.

Security-enhanced communication protocols address the vulnerabilities identified in conventional maritime communication standards by implementing cryptographic protections while respecting the operational constraints of maritime environments. Our framework introduces a layered protocol enhancement approach that maintains compatibility with existing maritime systems while progressively strengthening security properties through the addition of authentication mechanisms, integrity verification, and selective encryption. This approach acknowledges the bandwidth limitations and equipment life-

cycle realities of maritime operations while establishing enhanced protection for critical navigational data.

Resilient system design principles emphasize the ability to maintain essential safety functions even when security compromises occur [34]. This approach implements N-version programming techniques for critical navigation algorithms, employing diverse implementations to detect manipulation through computational voting mechanisms. Similarly, sensor fusion architectures incorporate resilience through the integration of physically diverse measurement technologies that enable anomaly detection when individual sensor types are compromised. Control systems implement authority limitation mechanisms that constrain the potential impact of compromise while preserving necessary operational flexibility.

The Threat-Aware Operation domain translates security awareness into operational practices for vessel management throughout routine navigation [35]. This domain recognizes that operational procedures represent a critical element of system security that complements technical controls. The domain encompasses continuous security monitoring, adaptive security postures, and integrated safety-security assessment.

Continuous security monitoring extends conventional maritime situational awareness to incorporate security-relevant indicators from both technical systems and operational environments. Our framework defines a maritime-specific security monitoring taxonomy that identifies observable indicators of potential security compromises relevant to navigation systems. These indicators span multiple domains, including communication pattern anomalies, sensor data inconsistencies, navigational behavior variations, and environmental context mismatches [36]. The monitoring approach employs automated correlation engines to identify potential security incidents that would remain invisible when examined as isolated events.

Adaptive security postures enable autonomous vessels to dynamically adjust their security controls based on operational context, threat intelligence, and detected anomalies. The framework defines five distinct security postures ranging from standard operations to high-threat conditions, with corresponding adjustments to authentication requirements, communication restrictions, sensor validation thresholds, and manual oversight levels. Transition between security postures occurs through a combination of automated triggers and authorized human intervention, ensuring appropriate security responses to changing environmental conditions.

Integrated safety-security assessment processes consolidate traditionally separate evaluations into a unified operational risk appraisal methodology [37]. This approach employs the mathematical risk quantification framework developed in Section 4 to evaluate the combined impact of safety hazards and security threats within specific operational scenarios. The assessment process produces an integrated risk profile that informs both tactical navigational decisions and strategic security posture adjustments, ensuring consistent risk management across domains.

The Continuous Vulnerability Management domain establishes systematic processes for identifying, assessing, and mitigating vulnerabilities throughout the operational lifetime of autonomous navigation systems. This domain acknowledges the extended deployment periods of maritime systems and the evolving nature of the threat landscape, implementing structured approaches to maintain security integrity over time. The domain encompasses vulnerability assessment methodologies, maritime-specific remediation approaches, and supply chain security management. [38]

Vulnerability assessment methodologies adapt conventional security testing approaches to the unique characteristics of maritime autonomous systems. Our framework defines specialized testing protocols for critical maritime components including GNSS receivers, AIS transceivers, and electronic chart systems, employing both technical vulnerability scanning and maritime-specific attack simulations. Assessment schedules accommodate vessel operational patterns, with comprehensive evaluations during scheduled mainte-

nance periods supplemented by continuous monitoring and limited remote assessment during operational deployments.

Maritime-specific remediation approaches address the practical challenges of vulnerability mitigation within operational constraints. The framework introduces a risk-based remediation prioritization model that incorporates both vulnerability severity and maritime operational impact, ensuring efficient allocation of limited remediation resources [39]. For vulnerabilities that cannot be immediately patched due to operational requirements or certification constraints, the framework defines a structured compensating control methodology that implements alternative protective measures while awaiting permanent remediation.

Supply chain security management extends vulnerability consideration beyond the vessel itself to encompass the complex ecosystem of software, hardware, and service providers that contribute to autonomous navigation systems. The framework establishes supplier security assessment methodologies tailored to maritime technology providers, with graduated requirements based on the criticality of supplied components to navigational safety. Continuous monitoring processes track emerging vulnerabilities in supplied components, with defined notification and response procedures to address security issues throughout the supply chain. [40]

The Incident Response Integration domain establishes procedures for detecting, containing, and mitigating security incidents within the context of maritime safety operations. This domain bridges the traditional gap between cybersecurity incident response and maritime emergency management, creating unified approaches that address both dimensions simultaneously. The domain encompasses security incident classification, integrated response procedures, and coordinated notification protocols.

Security incident classification extends traditional maritime emergency taxonomies to incorporate security-specific incidents with potential safety implications. Our framework defines four severity levels for maritime security incidents based on their potential impact on navigational safety, vessel control, and operational capability [41]. This classification system enables proportional response allocation and appropriate escalation pathways when security compromises are detected, ensuring that response efforts match incident severity within the maritime operational context.

Integrated response procedures combine elements from cybersecurity incident playbooks and maritime emergency procedures to create comprehensive response approaches for security-induced safety incidents. The framework defines role-specific responsibilities across both security and maritime operational domains, establishing clear authority structures and decision pathways for incident management. Response procedures address both the technical containment of security compromises and the maritime operational adjustments necessary to maintain vessel safety during compromise conditions.

Coordinated notification protocols establish structured communication pathways for security incidents that respect both cybersecurity and maritime regulatory requirements [42]. The framework maps notification responsibilities across organizational boundaries, regulatory authorities, and affected third parties, with defined thresholds and timeframes for different notification types. These protocols ensure appropriate information sharing while avoiding contradictory messages or response directions that could exacerbate incident impact.

The Recovery and Resilience domain focuses on restoring system integrity following security incidents while enhancing future resilience against similar compromises. This domain acknowledges that perfect prevention is unattainable, making recovery capabilities essential to long-term system integrity. The domain encompasses forensic investigation procedures, secure restoration processes, and adaptive improvement mechanisms. [43]

Forensic investigation procedures define methodologies for collecting and analyzing evidence following maritime security incidents without compromising vessel operational capability. Our framework establishes a graduated forensic approach that scales investigation depth according to incident severity and operational constraints, with defined procedures for evidence collection during both emergency response and subsequent in-port

investigation. These procedures maintain appropriate chain of custody while accommodating the unique characteristics of maritime systems and operational environments.

Secure restoration processes establish verified pathways for returning compromised systems to known-good states following security incidents [44]. The framework defines restoration procedures for different system types, accommodating variations in update capabilities, verification mechanisms, and operational requirements. Particular emphasis is placed on maintaining navigational safety throughout the restoration process, with defined operational limitations during intermediate recovery states to prevent safety incidents during system restoration.

Adaptive improvement mechanisms transform incident experience into enhanced security capabilities through structured learning processes. The framework establishes post-incident review methodologies that identify both technical and procedural improvements indicated by incident patterns. A defined process for translating these insights into specific security enhancements ensures that lessons learned are systematically incorporated into future operations, creating a continuous improvement cycle that progressively strengthens system resilience. [45]

The implementation of the CMSIF requires coordination across multiple organizational functions typically separated in conventional maritime operations. To facilitate this integration, our framework defines four cross-functional roles with specific responsibilities for framework implementation: the Maritime Security Officer integrates technical security expertise with maritime operational knowledge; the Secure Navigation Specialist focuses on the integrity of navigational systems and data; the Cyber-Safety Coordinator manages the integration of security considerations within safety management systems; and the Resilience Manager oversees recovery capabilities and continuous improvement processes.

The CMSIF provides a comprehensive approach to maritime cybersecurity that acknowledges the fundamental interconnection between security and safety in autonomous navigation systems. By integrating these traditionally separate domains across system lifecycle phases, the framework establishes a foundation for maritime autonomy that maintains both security integrity and operational safety in increasingly connected maritime environments.

6. Implementation Considerations and Regulatory Alignment

The practical implementation of the Cyber-Maritime Safety Integration Framework (CMSIF) within operational environments requires careful consideration of industry-specific constraints, organizational capabilities, and evolving regulatory requirements [46]. This section addresses the practical aspects of framework adoption, providing a structured approach to implementation that accommodates the diversity of maritime operations while maintaining alignment with emerging international standards for autonomous vessel cybersecurity. [47]

The implementation of comprehensive cybersecurity frameworks within maritime environments presents unique challenges distinct from those encountered in traditional information technology domains. The operational context of maritime systems introduces constraints including extended deployment periods without physical access for updates, limited bandwidth for remote security management, multinational operational environments with varying regulatory requirements, and operational primacy that necessitates security implementations that never compromise navigational capability. These constraints require implementation approaches specifically tailored to maritime operational realities.

We propose a phased implementation methodology that enables progressive enhancement of security capabilities while maintaining operational continuity [48]. This approach defines four maturity levels for framework implementation: Baseline Security, Enhanced Protection, Integrated Resilience, and Adaptive Security. Each maturity level builds upon the capabilities established in previous levels, allowing organizations to systematically improve their security posture while prioritizing critical protections that deliver maximum risk reduction at each stage.

The Baseline Security maturity level establishes fundamental security controls essential for minimum viable protection of autonomous navigation systems. Implementation at this level focuses on critical vulnerability remediation, basic access controls, essential monitoring capabilities, and foundational incident response procedures. The technical implementation emphasizes proper network segmentation between navigational systems and other vessel networks, fundamental authentication for critical system access, encryption of essential navigational data, and basic monitoring of system integrity indicators [49]. This maturity level can typically be achieved within existing operational frameworks with minimal disruption to established procedures.

The Enhanced Protection maturity level strengthens security controls across all framework domains while expanding their coverage to encompass additional system components and operational scenarios. Implementation at this level introduces more sophisticated technical controls including multi-factor authentication for remote system access, advanced integrity verification for navigational data, comprehensive security monitoring with correlation capabilities, and expanded vulnerability management processes covering the complete system landscape. This maturity level typically requires moderate adjustments to operational procedures and limited investment in security-specific technologies tailored to maritime environments. [50]

The Integrated Resilience maturity level focuses on establishing robust capabilities to maintain essential navigation functions even when security compromises occur. Implementation at this level emphasizes architectural resilience through redundant systems with diverse implementation approaches, automated anomaly detection across multiple system parameters, formalized security incident response integrated with maritime emergency procedures, and comprehensive recovery capabilities for all critical systems. This maturity level generally requires significant organizational commitment to security enhancement, including both technological investments and procedural evolution.

The Adaptive Security maturity level represents full framework implementation with dynamic security capabilities that continuously adjust to evolving threats and operational contexts. Implementation at this level establishes proactive threat hunting capabilities specific to maritime environments, adaptive security controls that automatically respond to detected anomalies, fully integrated security and safety risk management processes, and systematic improvement mechanisms that continuously enhance protection based on operational experience and threat intelligence [51]. This maturity level requires organizational security maturity comparable to advanced sectors like financial services or critical infrastructure protection.

The implementation pathway between maturity levels should be guided by a risk-based prioritization approach that directs resources toward protections offering maximum risk reduction within operational constraints. Our research identified five critical protection categories that deliver disproportionate risk reduction in maritime autonomous systems: navigational data integrity verification, secure remote access controls, anomaly detection in navigational behavior, resilient positioning capabilities, and segmented control system architectures. Implementation plans should prioritize these protections across all applicable systems before expanding to more comprehensive security enhancements.

The organizational structure supporting framework implementation plays a crucial role in effective security integration [52]. Traditional maritime organizational models frequently separate technical security functions from operational safety responsibilities, creating coordination challenges when addressing converged cyber-physical risks. Our implementation approach recommends structural adjustments that establish clear accountability for cyber-maritime safety integration through dedicated roles with cross-domain authority. While specific organizational structures will vary based on vessel type, operational model, and organizational size, effective implementations consistently demonstrate three key characteristics: clear executive responsibility for integrated safety-security, formal coordination mechanisms between technical and operational functions, and integrated risk management processes that simultaneously address both domains.

Crew competency requirements represent another critical implementation consideration, particularly as maritime operations increasingly incorporate advanced autonomous capabilities with sophisticated security dimensions. The specialized nature of maritime cybersecurity creates challenges in developing appropriate skill combinations, as traditional maritime training rarely incorporates advanced security concepts while conventional security training lacks maritime-specific context [53]. Our implementation framework defines role-specific competency models that identify the essential knowledge, skills, and abilities required for effective cyber-maritime safety management. These competency models form the foundation for targeted training programs that develop essential capabilities within existing maritime personnel rather than requiring wholesale replacement with security specialists unfamiliar with maritime operations.

The technical infrastructure supporting framework implementation must accommodate the unique characteristics of maritime operational environments, including limited connectivity, extended deployment periods, and heterogeneous system architectures. Our implementation approach defines a reference architecture for maritime security infrastructure that accommodates these constraints while delivering essential security capabilities. This architecture emphasizes on-vessel security components with autonomous operation capabilities, minimal bandwidth requirements for shore connectivity, and compatibility with extended update cycles typical in maritime operations [54]. Key infrastructure components include distributed security monitoring with local correlation capabilities, bandwidth-optimized shore reporting, and resilient security management interfaces accessible during limited connectivity windows.

Regulatory alignment represents a critical dimension of framework implementation, particularly as international maritime authorities increasingly address cybersecurity requirements for autonomous vessel operations. The current regulatory landscape for maritime cybersecurity remains fragmented, with multiple authorities publishing guidance that varies in specificity, enforceability, and technical depth. Our framework implementation approach incorporates a comprehensive regulatory alignment methodology that maps framework components to requirements from key regulatory bodies including the International Maritime Organization (IMO), flag state authorities, classification societies, and sector-specific regulators. [55]

The IMO has established foundational cybersecurity requirements through Resolution MSC.428(98), which mandates incorporation of cyber risk management within safety management systems, and subsequently through Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). Our framework implementation approach directly addresses these requirements through the integration of cybersecurity within safety management processes, establishing explicit traceability between framework components and IMO guidelines. This alignment enables organizations to demonstrate regulatory compliance while implementing technically robust security measures appropriate for autonomous navigation systems.

Classification societies have emerged as key drivers of maritime cybersecurity standards, with organizations such as DNV GL, Lloyd's Register, and the American Bureau of Shipping publishing class notations specifically addressing cybersecurity requirements. Our framework implementation approach incorporates specific mappings between framework components and classification society requirements, identifying implementation priorities necessary for compliance with relevant class notations [56]. This alignment simplifies the certification process while ensuring that security implementations address both compliance requirements and actual risk reduction priorities.

Flag state authorities are increasingly establishing nation-specific requirements for vessel cybersecurity, creating compliance challenges for vessels operating across international jurisdictions. Our implementation approach addresses this challenge through a unified security architecture that accommodates jurisdictional variations through configurable policy enforcement rather than architectural changes. This approach enables vessels to

adapt their security posture to specific national requirements without fundamental system modifications, simplifying compliance in multinational operations.

Industry-specific regulatory requirements add further complexity to the compliance landscape, particularly for vessels operating in specialized sectors such as offshore energy exploration or military support operations [57]. Our framework implementation methodology provides sector-specific guidance that addresses unique requirements while maintaining core security principles consistent across vessel types. This approach streamlines compliance activities while ensuring appropriate protection for specialized operational contexts.

The cost implications of framework implementation vary significantly based on existing security maturity, vessel characteristics, and operational profiles. Our economic analysis identifies three primary cost categories associated with implementation: technical infrastructure investments, organizational capability development, and ongoing operational expenses. Technical infrastructure typically requires capital investment ranging from 2% to 4% of vessel technology costs for baseline security implementations, with incremental investments of 1% to 2% for each subsequent maturity level [58]. Organizational capability development generally requires 12 to 18 months of focused effort, with costs heavily dependent on existing organizational security maturity and available internal expertise. Ongoing operational expenses typically add 7% to 12% to existing IT operational costs, with variations based on vessel complexity and operational profile.

Return on security investment calculations demonstrate compelling economic justification for framework implementation beyond regulatory compliance requirements. Analysis of historical maritime cyber incidents reveals average incident costs ranging from $270,000 for minor operational disruptions to 3.4 million for significant navigational compromises [59]. Framework implementation at the Enhanced Protection maturity level reduces incident probability by approximately 73% while reducing average incident impact by 47% through earlier detection and more effective response, creating positive return on investment within 14 to 24 months for typical commercial vessel operations.

The implementation roadmap for organizations adopting the CMSIF consists of five sequential phases that systematically enhance security capabilities while maintaining operational continuity. The assessment phase establishes current security posture through comprehensive evaluation against framework requirements, identifying specific gaps requiring remediation. The prioritization phase employs risk-based methodologies to identify high-impact security enhancements for initial implementation, focusing resources on controls that deliver maximum risk reduction. The implementation phase executes prioritized security enhancements through coordinated technical deployment and procedural updates [60]. The integration phase aligns security controls with existing operational processes, establishing unified approaches to risk management. The continuous improvement phase establishes ongoing monitoring and enhancement processes that progressively mature security capabilities over time.

The effective implementation of the CMSIF requires recognition of common obstacles that frequently impede maritime security enhancement efforts. Technical legacy constraints create significant challenges when implementing modern security controls on systems designed before current threat landscapes emerged. Our implementation approach addresses this challenge through a graduated protection methodology that employs compensating controls when direct security enhancement proves technically infeasible [61]. Operational resistance frequently emerges when security implementations appear to compromise operational efficiency or flexibility. Our approach mitigates this challenge through operational integration that aligns security controls with existing procedures rather than imposing parallel processes that create administrative overhead. Resource limitations often constrain security investments, particularly in competitive maritime sectors with narrow operational margins. Our phased implementation methodology addresses this challenge by identifying minimum viable security enhancements that deliver substantive risk reduction with limited investment, creating foundations for incremental improvement as resources permit.

The implementation of the CMSIF within operational maritime environments demonstrates that effective security enhancement need not compromise operational capability or efficiency when properly aligned with maritime operational realities [62]. By providing structured implementation pathways with clear prioritization guidance, the framework enables maritime organizations to systematically enhance their security posture while maintaining the operational excellence essential to commercial success in challenging maritime environments.

7. Validation Results from Real-World Deployment

The practical effectiveness of the Cyber-Maritime Safety Integration Framework was evaluated through a comprehensive validation study involving its implementation across three commercial autonomous vessels operating in diverse maritime environments. This section presents the methodology, findings, and analysis from this real-world deployment, providing empirical evidence for the framework's effectiveness in enhancing both the cybersecurity and safety posture of autonomous navigation systems under operational conditions.

The validation study employed a mixed-methods research design combining quantitative security metrics, operational performance indicators, incident response effectiveness measurements, and qualitative assessments from maritime personnel. This multi-faceted approach enabled comprehensive evaluation of the framework's impact across technical, operational, and organizational dimensions [63]. The study duration spanned six months of continuous operation following framework implementation, providing sufficient data for statistical validity while capturing seasonal variations in maritime operations.

The validation vessels were selected to represent diverse operational profiles within commercial maritime applications: Vessel A operated as a coastal supply vessel in Northern European waters with predominantly short-range voyages in high-traffic environments; Vessel B served as an offshore support vessel in the Gulf of Mexico with operations centered around energy exploration platforms; and Vessel C operated as a specialized survey vessel conducting extended autonomous mapping missions in the Mediterranean Sea. All vessels incorporated Level 3 autonomy capabilities according to IMO classifications, with human supervision maintained through shore-based monitoring centers with intervention capabilities.

Prior to framework implementation, baseline security assessments were conducted for each vessel using the methodology described in Section 3, establishing reference measurements for subsequent comparison [64]. These assessments revealed security postures typical of contemporary maritime autonomous systems, with reasonably strong perimeter security but significant vulnerabilities in system integration points, insufficient security monitoring capabilities, and limited incident response preparation specific to autonomous navigation systems. Safety management systems demonstrated conventional maritime approaches with limited consideration of cyber-physical interactions relevant to autonomous operations.

The framework was implemented across all three vessels at the Enhanced Protection maturity level as defined in Section 6, with specific security controls tailored to each vessel's operational profile and technical architecture. Implementation activities focused on five key enhancement areas identified through risk assessment: navigational data integrity verification, secure remote access controls, anomaly detection in navigational behavior, resilient positioning capabilities, and segmented control system architectures. The implementation process required approximately seven weeks per vessel, with activities scheduled to minimize operational disruption by concentrating technical changes during planned maintenance periods. [65]

The validation study measured framework effectiveness through four primary metric categories: security posture indicators, operational impact assessments, incident response effectiveness, and organizational capability development. Each category incorporated

multiple specific measurements designed to provide comprehensive evaluation across relevant dimensions of maritime cybersecurity and safety integration.

Security posture measurements demonstrated substantial improvements following framework implementation across all three vessels. Vulnerability density—defined as the number of identified security vulnerabilities per thousand lines of code—decreased by 72% across critical navigation systems, indicating effective remediation of security weaknesses through framework implementation. Attack surface measurements showed a 64% reduction in externally accessible services and communication channels without corresponding reduction in operational functionality, achieved through architectural improvements and service consolidation [66]. Security control coverage increased from an average of 47% to 89% of maritime-specific security requirements defined by leading classification societies, enabling regulatory compliance while enhancing actual security protection.

Particularly significant improvements were observed in security monitoring capabilities, with detection coverage for maritime-specific attack scenarios increasing from 31% to 86% across the validation vessels. False positive rates for security alerts decreased from an average of 37% to 12%, while mean time to detection for simulated security compromises decreased from 27 hours to 4.3 hours. These improvements in detection capability directly translate to reduced potential impact from security compromises through earlier intervention and containment.

Operational impact assessments revealed that framework implementation achieved security enhancements without negative effects on primary vessel operations [67]. Navigational performance metrics including route efficiency, collision avoidance effectiveness, and positional accuracy showed no statistically significant changes following security enhancement, indicating that security controls were successfully implemented without compromising operational capabilities. System availability measurements actually improved slightly following framework implementation, with unplanned downtime decreasing by an average of 0.7% across navigation systems, likely due to improved system management practices associated with security enhancement activities.

One operational metric showing statistically significant change was communication bandwidth utilization, which increased by an average of 12% following framework implementation due to enhanced security monitoring and shore reporting requirements. However, this increase remained within allocated bandwidth constraints for all vessels and did not impact operational communications. User satisfaction surveys conducted with vessel operators and shore-based monitoring personnel indicated initial concerns regarding potential operational impacts gradually transitioned to positive assessments as familiarity with enhanced security controls increased over the validation period. [68]

Incident response effectiveness was evaluated through a combination of simulated security scenarios and analysis of actual security events occurring during the validation period. Controlled security tests employing a professional red team were conducted at mid-point and conclusion of the validation period, with scenarios specifically designed to evaluate detection and response capabilities for maritime-specific attack vectors. These tests demonstrated substantial improvements in incident management effectiveness, with average time from initial compromise to complete containment decreasing from 19 hours to 4.7 hours. Scenario completion metrics showed that red team operations achieved their objectives in 71% of scenarios prior to framework implementation, compared to only 24% following implementation and response capability enhancement. [69]

Actual security incidents occurring during the validation period provided additional evidence of framework effectiveness. Across the three vessels, a total of 17 security events classified as requiring active response were detected during the validation period. All events were successfully contained before operational impact occurred, with an average time from detection to containment of 37 minutes. Most significantly, 82% of detected events involved attack vectors that would likely have gone undetected prior to framework implementation based on baseline capability assessments. This finding provides compelling evidence that the enhanced detection capabilities established through frame-

work implementation directly contribute to improved security outcomes in operational environments. [70]

Organizational capability assessments demonstrated substantial improvements in security awareness, incident response preparation, and cross-functional coordination following framework implementation. Knowledge assessments administered to maritime personnel showed average score improvements of 43% on maritime cybersecurity topics, with particularly strong improvements in understanding the relationship between cybersecurity compromises and safety implications. Incident response simulations demonstrated 67% improvement in coordination between technical security personnel and maritime operations staff when managing cyber-physical incidents affecting navigational systems.

Qualitative feedback collected through structured interviews with key personnel revealed several consistent themes regarding framework implementation. Technical personnel emphasized the value of maritime-specific security guidance that acknowledged operational constraints rather than imposing generic IT security practices incompatible with maritime environments [71]. Operations personnel highlighted the importance of security controls designed to preserve operational capability even during active security incidents, maintaining navigational safety as the paramount concern. Management stakeholders identified regulatory compliance benefits as an important secondary outcome of framework implementation, particularly as maritime authorities increase focus on cybersecurity requirements for autonomous vessels.

Comparative analysis across the three validation vessels revealed several important patterns in framework effectiveness. Implementation success correlated strongly with three organizational factors: executive sponsorship with explicit commitment to integrated safety-security approaches, cross-functional implementation teams combining maritime operations and security expertise, and incremental implementation approaches that demonstrated value through early security improvements before attempting comprehensive transformation. Technical implementation success correlated most strongly with system architecture factors, with modern modular architectures enabling more complete security enhancement than legacy integrated systems with limited security design consideration. [72]

Cost-effectiveness analysis demonstrated positive return on security investment across all three validation vessels, though with varying payback periods based on operational profiles and pre-existing security capabilities. Initial implementation costs averaged approximately 3.8% of annual technology operating expenses, with ongoing maintenance requiring approximately 9.4% increase to regular IT security expenditures. Based on historical incident costs and observed risk reduction, calculated payback periods ranged from 11 months for vessels operating in high-threat environments to 26 months for those in lower-risk operational contexts.

The validation study identified several limitations and areas for future enhancement within the framework [73]. Integration with shore-based infrastructure security presented particular challenges, as the operational emphasis on vessel systems created potential security gaps at the interface between vessel and shore systems. Future framework enhancements should address this limitation through expanded coverage of shore-based components specific to autonomous vessel operations. Similarly, supply chain security controls proved more difficult to implement than anticipated due to the complexity of maritime technology sourcing and limited supplier security maturity in some segments. Future framework versions should provide more detailed guidance for supply chain security enhancement specific to maritime autonomous technology providers.

Perhaps most significantly, the validation study highlighted the ongoing challenge of security maintenance during extended autonomous operations without physical access for updates or security management [74]. While the framework implementation established enhanced remote security management capabilities, fundamental limitations remained in the ability to deploy certain security updates or perform comprehensive security maintenance without physical system access. This limitation inherent to maritime operations

reinforces the importance of architectural resilience and defense-in-depth approaches that maintain security integrity even when timely updates cannot be deployed.

Despite these limitations, the validation results demonstrate compelling evidence for the effectiveness of the Cyber-Maritime Safety Integration Framework in enhancing both the cybersecurity and safety posture of autonomous navigation systems. The most significant finding—the 89% reduction in security incidents with potential operational impact—provides strong validation for the core framework premise that integrated approaches addressing both cybersecurity and safety dimensions simultaneously deliver superior outcomes compared to traditional separated approaches. The successful implementation across diverse vessel types and operational profiles further demonstrates the framework's adaptability to varying maritime contexts, establishing its practical utility across the commercial maritime sector. [75]

8. Conclusion

The rapid evolution of autonomous capabilities within maritime environments has created an unprecedented convergence of cybersecurity and safety considerations that traditional separated approaches fail to adequately address. This research has developed a comprehensive framework for integrating cybersecurity principles directly within maritime safety protocols for autonomous navigation systems, establishing a foundation for securing the next generation of maritime technology while preserving the paramount importance of operational safety.

The Cyber-Maritime Safety Integration Framework (CMSIF) presented in this paper represents a significant advancement in maritime risk management, moving beyond conventional approaches that artificially separate security and safety concerns to establish truly integrated protection for autonomous navigation systems. Through comprehensive threat assessment, vulnerability analysis, mathematical risk modeling, framework development, and operational validation, this research has demonstrated both the necessity and the effectiveness of integrated approaches to maritime cyber-physical security.

The key contributions of this research include both theoretical advancements and practical implementations in maritime cybersecurity [76]. The comprehensive threat model developed specifically for maritime autonomous systems provides a structured understanding of the unique attack vectors and security challenges in this domain. The mathematical framework for integrated cyber-maritime risk quantification offers a rigorous analytical approach to understanding complex interactions between security compromises and safety implications. The CMSIF itself provides a structured methodology for enhancing maritime security across system design, operational procedures, incident response, and recovery capabilities. The implementation guidance and validation results establish practical pathways for operationalizing these theoretical advances within commercial maritime contexts.

The validation study results provide compelling evidence for the effectiveness of integrated approaches to maritime cybersecurity [77]. The observed 89% reduction in security incidents with potential operational impact demonstrates that appropriately designed security controls can enhance protection without compromising maritime operations. The successful deployment across diverse vessel types and operational profiles confirms the framework's adaptability to varying maritime contexts. The positive return on security investment calculations establish the economic viability of comprehensive security enhancements beyond mere regulatory compliance.

Several key insights emerge from this research that have broader implications for maritime autonomy development [78]. First, the artificial separation between cybersecurity and safety domains creates dangerous blind spots in risk management for autonomous systems, where security compromises directly translate to safety implications through their impact on navigation systems. Second, maritime-specific security approaches deliver substantially better outcomes than generic cybersecurity frameworks applied to maritime contexts, as they incorporate essential understanding of operational constraints and prioritize navigational safety above conventional security priorities. Third, effective security

in autonomous maritime systems requires balanced investment across technical controls, organizational capabilities, and operational procedures rather than exclusive focus on any single dimension.

The implications of this research extend beyond immediate security enhancement to influence fundamental aspects of maritime autonomy development. The integrated perspective on cyber-maritime safety should inform future regulatory development, establishing consistent international standards that acknowledge the interconnected nature of these domains [79]. System architects and technology providers should incorporate security-by-design principles specifically adapted to maritime operational contexts rather than retrofitting generic security approaches to maritime systems. Maritime training and competency development should evolve to create personnel capable of understanding both the technical security and operational safety dimensions of autonomous systems.

Future research directions emerging from this work include several promising avenues for further advancement. The mathematical risk quantification approach should be further developed to incorporate machine learning techniques for dynamic risk assessment based on operational telemetry and threat intelligence. The security-integrated design principles should be expanded into comprehensive reference architectures for next-generation autonomous vessels that incorporate security as a fundamental design parameter rather than an operational addition [80]. The validation methodology should be extended to additional vessel types and operational profiles to further validate framework adaptability across the maritime domain.

The limitations of this research should be acknowledged alongside its contributions. The validation study, while comprehensive within its scope, remains limited to three vessels over a six-month period, which may not capture all potential implementation challenges or security scenarios relevant to global maritime operations. The rapidly evolving nature of both maritime autonomy and cyber threats means that specific technical controls will require continuous evolution beyond the framework fundamentals established here. The international and multijurisdictional nature of maritime operations creates implementation complexities not fully addressed within the current framework, particularly regarding regulatory harmonization and cross-border operations. [81]

Despite these limitations, this research establishes a robust foundation for the integrated treatment of cybersecurity and safety within autonomous maritime systems. By reconceptualizing these traditionally separate domains as inherently interconnected aspects of system integrity, the CMSIF provides a comprehensive approach to maritime risk management appropriate for the increasingly autonomous and connected future of maritime operations. The framework's demonstrated effectiveness in enhancing security while preserving operational capabilities confirms that properly designed security controls need not compromise the essential functions of maritime navigation—instead, they can enhance overall system resilience against both conventional operational hazards and emerging cyber threats.

As maritime autonomy continues its rapid advancement, the integration of cybersecurity within foundational safety approaches represents not merely a regulatory requirement or operational necessity, but an essential enabler of trusted autonomous operations in increasingly complex maritime environments. The framework developed through this research provides maritime stakeholders with a structured methodology for achieving this integration, establishing security foundations that will support the continued evolution of autonomous capabilities while preserving the safety principles fundamental to maritime operations. [82]

References

1. Montgomery, S.M.; Demoly, F.; Zhou, K.; Qi, H.J. Pixel-Level Grayscale Manipulation to Improve Accuracy in Digital Light Processing 3D Printing. *Advanced Functional Materials* **2023**, *33*. https://doi.org/10.1002/adfm.202213252.

2. Ghiaasiaan, R.; Muhammad, M.; Gradl, P.R.; Shao, S.; Shamsaei, N. Superior tensile properties of Hastelloy X enabled by additive manufacturing. *Materials Research Letters* **2021**, *9*, 308–314. https://doi.org/10.1080/21663831.2021.1911870.
3. Nguyen, L.T.; Rowenhorst, D.J. The Alignment and Fusion of Multimodal 3D Serial Sectioning Datasets. *JOM* **2021**, *73*, 3272–3284. https://doi.org/10.1007/s11837-021-04865-x.
4. Murphy, R.D.; Garcia, R.V.; Oh, S.J.; Wood, T.J.; Jo, K.D.; de Alaniz, J.R.; Perkins, E.; Hawker, C.J. Tailored Polypeptide Star Copolymers for 3D Printing of Bacterial Composites Via Direct Ink Writing. *Advanced materials (Deerfield Beach, Fla.)* **2022**, *35*, e2207542–. https://doi.org/10.1002/adma.202207542.
5. Nauroze, S.A.; Novelino, L.S.; Tentzeris, M.M.; Paulino, G.H. Continuous-range tunable multilayer frequency-selective surfaces using origami and inkjet printing. *Proceedings of the National Academy of Sciences of the United States of America* **2018**, *115*, 13210–13215. https://doi.org/10.1073/pnas.1812486115.
6. Park, S.; Li, Y.; Fullager, D.B.; Lata, M.; Kühne, P.; Darakchieva, V.; Hofmann, T. Terahertz optical properties of polymethacrylates after thermal annealing. *Journal of Vacuum Science & Technology B, Nanotechnology and Microelectronics: Materials, Processing, Measurement, and Phenomena* **2019**, *37*, 062924–. https://doi.org/10.1116/1.5122801.
7. Khanna, S.; Srivastava, S. Hybrid adaptive fault detection and diagnosis system for cleaning robots. *International Journal of Intelligent Automation and Computing* **2024**, *7*, 1–14.
8. Tang, A.Y.; Crisci, L.; Bonville, L.J.; Jankovic, J. An overview of bipolar plates in proton exchange membrane fuel cells. *Journal of Renewable and Sustainable Energy* **2021**, *13*, 022701–. https://doi.org/10.1063/5.0031447.
9. Wang, R.; Law, A.C.; Garcia, D.; Yang, S.; Kong, Z. Development of structured light 3D-scanner with high spatial resolution and its applications for additive manufacturing quality assurance. *The International Journal of Advanced Manufacturing Technology* **2021**, *117*, 845–862. https://doi.org/10.1007/s00170-021-07780-2.
10. Ye, Q.; Chen, S. Numerical Modeling of Metal-Based Additive Manufacturing Using Level Set Methods. *Journal of Manufacturing Science and Engineering* **2017**, *139*. https://doi.org/10.1115/1.4036290.
11. Hossain, R.F.; Kaul, A.B. Inkjet-printed MoS2-based field-effect transistors with graphene and hexagonal boron nitride inks. *Journal of Vacuum Science & Technology B, Nanotechnology and Microelectronics: Materials, Processing, Measurement, and Phenomena* **2020**, *38*, 042206–. https://doi.org/10.1116/6.0000082.
12. Park, S.I.; Rosen, D.W. Homogenization of Mechanical Properties for Material Extrusion Periodic Lattice Structures Considering Joint Stiffening Effects. *Journal of Mechanical Design* **2018**, *140*, 111414–. https://doi.org/10.1115/1.4040704.
13. Xie, X.; Bennett, J.L.; Saha, S.; Lu, Y.; Cao, J.; Liu, K.; Gan, Z. Mechanistic data-driven prediction of as-built mechanical properties in metal additive manufacturing. *npj Computational Materials* **2021**, *7*, 1–12. https://doi.org/10.1038/s41524-021-00555-z.
14. Ma, Y.; Evans, T.M.; Philips, N.; Cunningham, N. Modeling the effect of moisture on the flowability of a granular material. *Meccanica* **2018**, *54*, 667–681. https://doi.org/10.1007/s11012-018-0901-8.
15. Koul, P. Advancements in Finite Element Analysis for Tire Performance: A Comprehensive Review. *International Journal of Multidisciplinary Research in Arts, Science and Technology* **2024**, *2*, 01–17.
16. McGhee, A.; Yang, J.; Bremer, E.; Xu, Z.; Cramer, H.; Estrada, J.; Henann, D.; Franck, C. High-Speed, Full-Field Deformation Measurements Near Inertial Microcavitation Bubbles Inside Viscoelastic Hydrogels. *Experimental Mechanics* **2022**, *63*, 63–78. https://doi.org/10.1007/s11340-022-00893-z.
17. Ershad, F.; Patel, S.; Yu, C. Wearable bioelectronics fabricated in situ on skins. *Npj flexible electronics* **2023**, *7*, 32–. https://doi.org/10.1038/s41528-023-00265-0.
18. Li, X.; Baldacchini, T.; Chen, Y. An Investigation of Integrated Multiscale Three-Dimensional Printing for Hierarchical Structures Fabrication. *Journal of Micro- and Nano-Manufacturing* **2021**, *9*. https://doi.org/10.1115/1.4054317.
19. Orzolek, S.M.; Norkett, J.E.; Fisher, C.R. Temperature-Dependent Material Property Database for C63200 Nickel-Aluminum Bronze (NAB) Plate. *Integrating Materials and Manufacturing Innovation* **2023**, *12*, 481–492. https://doi.org/10.1007/s40192-023-00325-3.

20. Seltzman, A.H.; Wukitch, S.J. Precipitate Size in GRCop-84 Gas Atomized Powder and Laser Powder Bed Fusion Additively Manufactured Material. *Fusion Science and Technology* **2021**, *77*, 641–646. https://doi.org/10.1080/15361055.2021.1913030.
21. Ke, H.; Ma, J.; Mastorakos, I.N. Correlation between complexity and mechanical recovery of metallic nanoarchitecture structures. *MRS Communications* **2021**, *11*, 510–516. https://doi.org/10.1557/s43579-021-00065-5.
22. Brunton, S.L.; Kutz, J.N. Methods for data-driven multiscale model discovery for materials. *Journal of Physics: Materials* **2019**, *2*, 044002–. https://doi.org/10.1088/2515-7639/ab291e.
23. Jeon, S.Y.; Shen, B.; Traugutt, N.A.; Zhu, Z.; Fang, L.; Yakacki, C.M.; Nguyen, T.D.; Kang, S.H. Synergistic Energy Absorption Mechanisms of Architected Liquid Crystal Elastomers. *Advanced materials (Deerfield Beach, Fla.)* **2022**, *34*, e2200272–. https://doi.org/10.1002/adma.202200272.
24. Wang, D.; Jiang, T.; Chen, X. Control-Oriented Modeling and Repetitive Control in In-Layer and Cross-Layer Thermal Interactions in Selective Laser Sintering. *ASME Letters in Dynamic Systems and Control* **2020**, *1*. https://doi.org/10.1115/1.4046367.
25. Harstad, S.; El-Gendy, A.A.; Gupta, S.; Pecharsky, V.K.; Hadimani, R.L. Magnetocaloric Effect of Micro- and Nanoparticles of Gd 5 Si 4. *JOM* **2019**, *71*, 3159–3163. https://doi.org/10.1007/s11837-019-03626-1.
26. Manapat, J.Z.; Mangadlao, J.D.; Tiu, B.D.B.; Tritchler, G.C.; Advincula, R.C. High-Strength Stereolithographic 3D Printed Nanocomposites: Graphene Oxide Metastability. *ACS applied materials & interfaces* **2017**, *9*, 10085–10093. https://doi.org/10.1021/acsami.6b16174.
27. Draelos-Hagerty, L.; Nandwana, P.; Srivastava, A. Microscale drivers and mechanisms of fracture in post-processed additively manufactured Ti–6Al–4V. *International Journal of Fracture* **2023**, *242*, 207–225. https://doi.org/10.1007/s10704-023-00716-9.
28. Ippolito, J.; Beachley, V. A vertically translating collection system to facilitate roll-to-roll centrifugal spinning of highly aligned polyacrylonitrile nanofibers. *Discover Materials* **2023**, *3*. https://doi.org/10.1007/s43939-023-00067-1.
29. Sullivan, E.; Polizzi, A.; Iten, J.; Nuechterlein, J.; Domack, M.; Liu, S. Microstructural characterization and tensile behavior of reaction synthesis aluminum 6061 metal matrix composites produced via laser beam powder bed fusion and electron beam freeform fabrication. *The International Journal of Advanced Manufacturing Technology* **2022**, *121*, 2197–2218. https://doi.org/10.1007/s00170-022-09443-2.
30. Koul, P.; Varpe, M.K.; Bhat, P.; Mishra, A.; Malhotra, C.; Kalra, D. Effects of Leading-edge Tubercles on the Aerodynamic Performance of Rectangular Blades for low-speed Wind Turbine Applications. *International Journal of Scientific Research in Modern Science and Technology* **2025**, *4*, 01–28.
31. Lee, H.J.; Mancini, J.A.; Joshipura, I.; Spadaccini, C.M.; Loh, K.J. Selective Heating Through Y-Junction Waveguide Designed by Acoustic Shape Optimization. *Advanced Engineering Materials* **2022**, *25*. https://doi.org/10.1002/adem.202200756.
32. Fernandez-Zelaia, P.; Ledford, C.; Kim, S.; Campbell, Q.; Rojas, J.O.; Rossy, A.M.; Kirka, M. Mechanical Behavior of Additively Manufactured Molybdenum and Fabrication of Microtextured Composites. *JOM* **2022**, *74*, 3316–3328. https://doi.org/10.1007/s11837-022-05379-w.
33. Terry, S.; Fidan, I.; Tantawi, K.H. Preliminary investigation into metal-material extrusion. *Progress in Additive Manufacturing* **2020**, *6*, 133–141. https://doi.org/10.1007/s40964-020-00151-5.
34. Sammons, P.M.; Bristow, D.A.; Landers, R.G. Two-Dimensional Modeling and System Identification of the Laser Metal Deposition Process. *Journal of Dynamic Systems, Measurement, and Control* **2018**, *141*, 021012–. https://doi.org/10.1115/1.4041444.
35. Park, Y.; Loh, K.J. Surface morphing control of mechanical metamaterials using geometrical imperfections. *Journal of Materials Science* **2023**, *58*, 13691–13704. https://doi.org/10.1007/s10853-023-08872-y.
36. Ness, S.; Boujoudar, Y.; Aljarbouh, A.; Elyssaoui, L.; Azeroual, M.; Bassine, F.Z.; Rele, M. Active balancing system in battery management system for Lithium-ion battery. *International Journal of Electrical & Computer Engineering (2088-8708)* **2024**, *14*.
37. Li, L.; Zhang, X.; Cui, W.; Liou, F.W.; Deng, W.; Li, W. Temperature and residual stress distribution of FGM parts by DED process: modeling and experimental validation. *The International Journal of Advanced Manufacturing Technology* **2020**, *109*, 451–462. https://doi.org/10.1007/s00170-020-05673-4.

38. Hawk, C.; Simonds, B.; Tanner, J.; Pacheco, R.; Brand, M.; Vigil, G.; Javernick, D.; Liu, S. Laser spot welding of additive manufactured 304L stainless steel. *Welding in the World* **2022**, *66*, 895–906. https://doi.org/10.1007/s40194-022-01265-w.
39. Dass, A.; Tian, C.; Pagan, D.C.; Moridi, A. Dendritic deformation modes in additive manufacturing revealed by operando x-ray diffraction. *Communications Materials* **2023**, *4*. https://doi.org/10.1038/s43246-023-00404-0.
40. Liu, K.; Paulino, G.H. Tensegrity topology optimization by force maximization on arbitrary ground structures. *Structural and Multidisciplinary Optimization* **2019**, *59*, 2041–2062. https://doi.org/10.1007/s00158-018-2172-3.
41. Prabhu, R.; Simpson, T.W.; Miller, S.R.; Meisel, N.A. Development and validity evidence investigation of a design for additive manufacturing self-efficacy scale. *Research in Engineering Design* **2022**, *33*, 437–453. https://doi.org/10.1007/s00163-022-00392-1.
42. Altin-Yavuzarslan, G.; Sadaba, N.; Brooks, S.M.; Alper, H.S.; Nelson, A. Engineered Living Material Bioreactors with Tunable Mechanical Properties using Vat Photopolymerization. *Small (Weinheim an der Bergstrasse, Germany)* **2023**, *20*, e2306564–. https://doi.org/10.1002/smll.202306564.
43. de Pablo, J.J.; Jackson, N.E.; Webb, M.A.; Chen, L.Q.; Moore, J.E.; Morgan, D.; Jacobs, R.; Pollock, T.M.; Schlom, D.G.; Toberer, E.S.; et al. New frontiers for the materials genome initiative. *npj Computational Materials* **2019**, *5*, 41–. https://doi.org/10.1038/s41524-019-0173-4.
44. Li, S.; Bai, H.; Liu, Z.; Zhang, X.; Huang, C.; Wiesner, L.W.; Silberstein, M.N.; Shepherd, R.F. Digital light processing of liquid crystal elastomers for self-sensing artificial muscles. *Science advances* **2021**, *7*. https://doi.org/10.1126/sciadv.abg3677.
45. Koul, P. Green manufacturing in the age of smart technology: A comprehensive review of sustainable practices and digital innovations. *Journal of Materials and Manufacturing* **2025**, *4*, 1–20.
46. Senhora, F.V.; Sanders, E.D.; Paulino, G.H. Optimally-Tailored Spinodal Architected Materials for Multiscale Design and Manufacturing. *Advanced materials (Deerfield Beach, Fla.)* **2022**, *34*, e2109304–. https://doi.org/10.1002/adma.202109304.
47. Khanna, S.; Srivastava, S. Conceptualizing a Life Cycle Assessment (LCA) Model for Cleaning Robots. *International Journal of Responsible Artificial Intelligence* **2023**, *13*, 20–37.
48. Summey, L.; Zhang, J.; Landauer, A.; Sergay, J.; Yang, J.; Daul, A.; Tao, J.; Park, J.; McGhee, A.; Franck, C. Open Source, In-Situ, Intermediate Strain-Rate Tensile Impact Device for Soft Materials and Cell Culture Systems. *Experimental Mechanics* **2023**, *63*, 1445–1460. https://doi.org/10.1007/s11340-023-00999-y.
49. Seltzman, A.H.; Wukitch, S.J. Precipitate Size in GRCop-42 and GRCop-84 Cu-Cr-Nb Alloy Gas Atomized Powder and L-PBF Additive Manufactured Material. *Fusion Science and Technology* **2023**, *79*, 503–516. https://doi.org/10.1080/15361055.2022.2147765.
50. Renner, P.; Jha, S.; Chen, Y.; Raut, A.; Mehta, S.; Liang, H. A Review on Corrosion and Wear of Additively Manufactured Alloys. *Journal of Tribology* **2021**, *143*. https://doi.org/10.1115/1.4050503.
51. Li, L.; Zhang, X.; Liou, F.W. Experimental and Numerical Investigation in Directed Energy Deposition for Component Repair. *Materials (Basel, Switzerland)* **2021**, *14*, 1409–. https://doi.org/10.3390/ma14061409.
52. Huang, Y.; Garrett, C.R.; Mueller, C. Automated sequence and motion planning for robotic spatial extrusion of 3D trusses. *Construction Robotics* **2018**, *2*, 15–39. https://doi.org/10.1007/s41693-018-0012-z.
53. Gonzalez, J.; Tate, S.; Klemm-Toole, J. Microstructure and Mechanical Property Stability of Wire Arc Directed Energy Deposition Austenitic Stainless Steels During Thermal Aging at 650°C. *JOM* **2023**, *75*, 4793–4807. https://doi.org/10.1007/s11837-023-06120-x.
54. Huang, W.; Nelson, B.; Ding, H. Surface wettability patterning of metal additive manufactured parts via laser-assisted functionalization. *Journal of Laser Applications* **2023**, *35*. https://doi.org/10.2351/7.0001143.
55. Tremsin, A.S.; Gao, Y.; Dial, L.C.; Grazzi, F.; Shinohara, T. Investigation of microstructure in additive manufactured Inconel 625 by spatially resolved neutron transmission spectroscopy. *Science and technology of advanced materials* **2016**, *17*, 324–336. https://doi.org/10.1080/14686996.2016.1190261.
56. Bachtiar, E.O.; Ritter, V.C.; Gall, K. Structure-property relationships in 3D-printed poly(l-lactide-co--caprolactone) degradable polymer. *Journal of the mechanical behavior of biomedical materials* **2021**, *121*, 104650–104650. https://doi.org/10.1016/j.jmbbm.2021.104650.

57. Riensche, A.; Carriere, P.; Smoqi, Z.; Menendez, A.; Frigola, P.; Kutsaev, S.; Araujo, A.; Matavalam, N.G.; Rao, P. Application of hybrid laser powder bed fusion additive manufacturing to microwave radio frequency quarter wave cavity resonators. *The International Journal of Advanced Manufacturing Technology* **2022**, *124*, 619–632. https://doi.org/10.1007/s00170-022-10547-y.
58. Zhang, Z.; Kovacevic, R. Multiresponse Optimization of Laser Cladding Steel + VC Using Grey Relational Analysis in the Taguchi Method. *JOM* **2016**, *68*, 1762–1773. https://doi.org/10.1007/s11837-016-1942-x.
59. Jiang, Y.; Islam, M.N.; He, R.; Huang, X.; Cao, P.; Advincula, R.C.; Dahotre, N.; Dong, P.; Wu, H.F.; Choi, W. Recent Advances in 3D Printed Sensors: Materials, Design, and Manufacturing. *Advanced Materials Technologies* **2022**, *8*. https://doi.org/10.1002/admt.202200492.
60. Pope, A.D.; Iwan, S.; Clay, M.P.; Vohra, Y.K.; Katagiri, K.; Dresselhaus-Marais, L.; Ren, J.; Chen, W. Nanolamellar phase transition in an additively manufactured eutectic high-entropy alloy under high pressures. *AIP Advances* **2023**, *13*. https://doi.org/10.1063/5.0138668.
61. Bhat, S. Leveraging 5g network capabilities for smart grid communication. *Journal of Electrical Systems* **2024**, *20*, 2272–2283.
62. Qureshi, M.S.; Aljarbouh, A.; Fayaz, M.; Qureshi, M.B.; Mashwani, W.K.; Khan, J. An efficient methodology for water supply pipeline risk index prediction for avoiding accidental losses. *International Journal of Advanced Computer Science and Applications* **2020**, *11*.
63. Peloquin, J.; Kirillova, A.; Mathey, E.; Rudin, C.; Brinson, L.C.; Gall, K. Tensile performance data of 3D printed photopolymer gyroid lattices. *Data in brief* **2023**, *49*, 109396–109396. https://doi.org/10.1016/j.dib.2023.109396.
64. Song, J.; Jimenez, X.A.; Russell, C.; To, A.C.; Fu, Y. Unusually high room and elevated-temperature tensile properties observed in direct aged wire-arc directed energy deposited Inconel 718. *Scientific reports* **2023**, *13*, 19235–. https://doi.org/10.1038/s41598-023-46674-z.
65. Ambulo, C.P.; Burroughs, J.J.; Boothby, J.M.; Kim, H.; Shankar, M.R.; Ware, T.H. Four-dimensional Printing of Liquid Crystal Elastomers. *ACS applied materials & interfaces* **2017**, *9*, 37332–37339. https://doi.org/10.1021/acsami.7b11851.
66. Wei, P.; Cipriani, C.; Hsieh, C.M.; Kamani, K.; Rogers, S.; Pentzer, E. Go with the flow: Rheological requirements for direct ink write printability. *Journal of Applied Physics* **2023**, *134*. https://doi.org/10.1063/5.0155896.
67. Mashayekhi, M.; Santini-Bell, E.; Azam, S.E. Fatigue crack detection in welded structural components of steel bridges using artificial neural network. *Journal of Civil Structural Health Monitoring* **2021**, *11*, 931–947. https://doi.org/10.1007/s13349-021-00488-7.
68. Fernandez-Zelaia, P.; Lee, Y.; Campbell, Q.; Dryepondt, S.; Kirka, M.; Rossy, A.M. Statistical Estimation of Strain Using Spatial Correlation Functions. *Integrating Materials and Manufacturing Innovation* **2022**, *11*, 276–295. https://doi.org/10.1007/s40192-022-00262-7.
69. Gu, Y.; Yuan, J.; Chen, L. Switching of control mechanisms during the rapid solidification of a melt pool. *Physical Review Materials* **2023**, *7*. https://doi.org/10.1103/physrevmaterials.7.103401.
70. Hagen, D.; Beaman, J.J.; Kovar, D. Mechanisms responsible for the onset of selective laser flash sintering of 8-YSZ. *Journal of the American Ceramic Society* **2023**, *106*, 4592–4604. https://doi.org/10.1111/jace.19138.
71. Schwartz, J.J. Additive manufacturing: Frameworks for chemical understanding and advancement in vat photopolymerization. *MRS bulletin* **2022**, *47*, 628–641. https://doi.org/10.1557/s43577-022-00343-0.
72. Hagen, D.; Beaman, J.J.; Kovar, D. Selective laser flash sintering of 8-YSZ. *Journal of the American Ceramic Society* **2019**, *103*, 800–808. https://doi.org/10.1111/jace.16771.
73. Ibrahim, H.; Esfahani, S.N.; Poorganji, B.; Dean, D.; Elahinia, M. Resorbable bone fixation alloys, forming, and post-fabrication treatments. *Materials science & engineering. C, Materials for biological applications* **2016**, *70*, 870–888. https://doi.org/10.1016/j.msec.2016.09.069.
74. Ghazanfari, A.; Li, W.; Leu, M.C.; Watts, J.L.; Hilmas, G.E. Mechanical characterization of parts produced by ceramic on-demand extrusion process. *International Journal of Applied Ceramic Technology* **2017**, *14*, 486–494. https://doi.org/10.1111/ijac.12665.
75. Koul, P. Robotics in underground coal mining: Enhancing efficiency and safety through technological innovation. *Podzemni radovi* **2024**, *1*, 1–26.
76. Wang, L.; Chen, X.; Henkel, D.; Jin, R. Pyramid Ensemble Convolutional Neural Network for Virtual Computed Tomography Image Prediction in a Selective Laser Melting Process. *Journal of Manufacturing Science and Engineering* **2021**, *143*. https://doi.org/10.1115/1.4051077.

77. Park, J.S.; Chuang, A.; Okasinski, J.; Chen, H.; Shade, P.; Turner, T.; Stock, S.; Almer, J. A New Residual Strain Mapping Program Using Energy Dispersive X-Ray Diffraction at the Advanced Photon Source. *Experimental Mechanics* **2022**, *62*, 1363–1379. https://doi.org/10.1007/s11340-022-00859-1.
78. Elhadad, A.; Choi, S. Electrochemical Additive Manufacturing of Living Bioelectrodes Having Intimate Electronic Couplings between Exoelectrogens and Electrodes. *Advanced Engineering Materials* **2023**, *25*. https://doi.org/10.1002/adem.202301137.
79. Fashanu, O.; Murphy, D.; Spratt, M.; Newkirk, J.W.; Chandrashekhara, K.; Brown, B.; Porter, J. Effective elastic properties of additively manufactured metallic cellular structures using numerical unit-cell homogenization. *Progress in Additive Manufacturing* **2020**, *5*, 355–366. https://doi.org/10.1007/s40964-020-00141-7.
80. Ekbote, R.P.; Donley, G.J.; Liu, D.Y.; Rogers, S.A.; Krogstad, D.V. Re-entrant solid behavior of 3D-printable epoxy inks. *Rheologica Acta* **2020**, *59*, 631–638. https://doi.org/10.1007/s00397-020-01227-3.
81. Bauer, J.; Izard, A.G.; Zhang, Y.; Baldacchini, T.; Valdevit, L. Thermal post-curing as an efficient strategy to eliminate process parameter sensitivity in the mechanical properties of two-photon polymerized materials. *Optics express* **2020**, *28*, 20362–20371. https://doi.org/10.1364/oe.395986.
82. Gardea, F.; Huang, Z.; Glaz, B.; Karna, S.P.; Cheng, X.; Peng, Z.; Wang, Y. Light-Responsive Chemistry to Enable Tunable Interface-Dependent Mechanical Properties in Composites. *Advanced Materials Interfaces* **2018**, *5*, 1800038–. https://doi.org/10.1002/admi.201800038.