Cyber Defence Trainer for Marine Integrated Platform Management Systems

Joey Lord[1], Scott Knight[2] and Brian Lachine[2]
[1]Royal Canadian Navy, Maritime Forces Atlantic Formation Technical Authority, Halifax, Canada
[2]Royal Military College of Canada, Kingston, Canada

joey.lord@forces.gc.ca
knight-s@rmc.ca
brian.lachine@rmc.ca

Abstract: Modern civilian and military marine vessels employ integrated platform management systems to monitor and control various different operational ship systems such has engine control, navigation and potentially weapon systems. These platform management systems consist of information and operational technology (IT/OT) environments that integrate commercial operating systems, TCP/IP based protocols and supervisory control and data acquisition (SCADA) systems in order to monitor and control marine cyber physical systems. This integration of technologies introduces threat vectors as well as unique operational, safety and potentially environmental impacts for marine vessels. Ships' crews do not always have security monitoring capabilities and trained security staff who understand the various onboard systems to the extent they could detect a cyber attack. Furthermore, there is a lack of training environments that could be used to educate marine cyber operators. The aim of this research is to build an environment based on effective cyber training techniques to enable the education of marine cyber operators in defensive cyber operations. The environment in this context is a defensive cyber security trainer that enables students to analyse network traffic in order to detect attacks against any ship systems, including cyber physical systems. Effective training techniques refers to the pedagogical recommendations for successful cyber education and effective gamified design. Educating marine cyber operators how to detect attacks on marine IT/OT environments within an integrated platform management system will enable better protection from cyber attack against marine vessels. To accomplish this aim, defensive cyber trainer was developed that consisted of three key components. The first was a Capture the Flag (CTF) framework. The second was a server that included the emulation and simulation of key ship integrated platform management system components within a virtualized environment. Third, were open source and customized plugins used to analyse traffic in our virtualized ship and the inclusion of three different kill chains based on real attacker tactics, techniques and procedures (TTPs). This defensive cyber trainer was validated against research methodologies for effective gamified environment design.

Keywords: Cyber education, OT cybersecurity, Defensive cyber operations

1. Introduction

Modern civilian and military maritime vessels rely on often interconnected information and operational technology (IT and OT) systems to successfully operate at sea and exposes these maritime platforms to cybersecurity threats (Karaś, 2023; Afenyo and Caesar, 2023; Harish et al, 2025). To defend against cyber threats, it has been proposed that marine cyber operators (MCOs) supporting modern maritime vessels require cyber defence training (United States Senate Committee on Armed Services, 2018; Soner and Kandemir, 2024). MCOs must be able to defend IT/OT systems that enable the control and monitoring of numerous ship-borne systems such as fire suppression, propulsion management and flooding management. In the marine sector, these types of integrated IT/OT systems are referred to as Integrated Platform Management Systems (IPMS) (Norris, 2025; RH Marine, 2025). Across other sectors, such systems may also be referred to as Cyber Physical Systems (CPS), Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition Systems (SCADA).

Various countries have, or are in the process of, creating new trades and careers for cyber security specialists (Australian Navy 2025; Canadian Armed Forces 2025; Royal Navy 2025). Similarly, in the private sector, one can find frequent postings for cybersecurity specialist jobs at various cruising and shipping companies. The need for IT/OT cyber specialists is not unique to the marine sector, such skilled staff are also needed in other business sectors such as energy, mining and manufacturing. However, the IT/OT systems in ships not only enable the core function of the ship whether it be warfighting, security/law enforcement and human or cargo transportation, they also support daily living and safety functions of a ship's crew. An IPMS is an example of such a system that supports such cross functional domains. An IPMS may also have some level of connectivity to other ship networks such as weapon and navigation system, further highlighting the need for its cyber defence. There is a need to educate and train MCOs for the unique cyber security challenges in a marine operational environment and specifically an IPMS.

While there exist examples of cybersecurity training specific to OT systems, the majority of available cybersecurity training is traditionally based on enterprise IT systems. Within naval and marine environments there are limited examples of training specific to IPMS type systems. Further, IPMS is a generic term and each IPMS may consist of different sub-system types, proprietary protocols and be employed within a sector that has different operational priorities. There lacks a methodology to develop an environment that enables the effective training of MCOs to monitor and defend an IPMS.

The aim of this research is to build an environment based on effective cyber training techniques to enable the education of marine cyber operators in defensive cyber operations. To achieve this aim, a proof-of-concept defensive cyber trainer is developed to train MCOs in defending an IPMS. Effective cyber training techniques in this context refer to a combination of gamification and pedagogical frameworks. The educational requirements are guided by selected knowledge, skills and tasks required by MCOs to defend marine vessels.

Section 2 provides background information important to the experimentation fundamental to achieving the aim. Section 3 outlines the methodology and design of the experimentation, followed by Section 4 that highlights the results that demonstrate achievement of the aim. Lastly, Section 5 concludes this research.

2. Background

This section provides core information regarding key components related to the experimentation conducted. First is an overview of an Integrated Platform Management System (IPMS) that outlines the typical scope of an IPMS, the types of systems involved and security concerns. Following is an outline of the National Initiative for Cybersecurity Education (NICE) Framework released by the National Institute of Standards and Technology (NIST) (NIST 2020) from which desired knowledge, skills and tasks for MCOs to defend an IPMS are selected. Lastly, gamification frameworks are explored.

2.1 Integrated Platform Management System

An IPMS provides the capability for crew to remotely monitor and control numerous systems onboard a ship and enable the live and move functions. IPMS systems generally fall into different categories such as propulsion and steering, power generation and distribution, auxiliary systems and damage control as illustrated below in Figure 1.

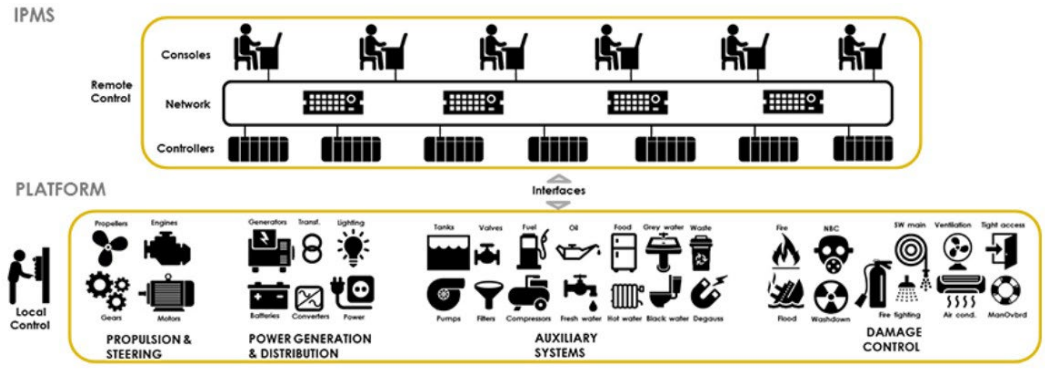

Figure 1: IPMS Conceptual Components (Defence Connect, 2021)

An IPMS is a distributed system that incorporates human machine interface (HMI) consoles, network switches and servers akin to an enterprise network, and also includes controllers: Remote Terminal Units (RTUs), programmable logic controllers (PLCs) that interact with the physical systems associated with the ship platform. The IPMS is a Supervisory Control and Data Acquisition (SCADA) System.

2.1.1 IPMS Lab

The IPMS lab installed at the Royal Military College uses a combination of virtualization, emulation, and simulation as illustrated below in Figure 2. This lab offers a realistic environment that closely mimics what is currently installed onboard modern vessels.

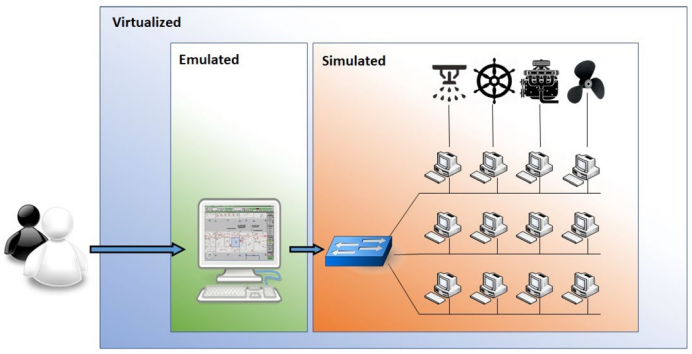

Figure 2: IPMS Lab Functional Diagram

The IPMS HMI is emulated by using the same OS, software and interface that operators use to control an actual Canadian shipborne IPMS network. The system and sub-system states are simulated with software that provides responses to inputs modelled on real machinery though no moving parts or hardware are involved. The entire IPMS lab environment is virtualized using VMWare. Three attack kill chains were developed to be used against an IPMS, targeting its confidentiality, integrity and availability, respectively (Timmins et al, 2021). The IPMS used in this lab also contains a proprietary protocol coupled at the transport layer, referred to as the IPMS protocol. The IPMS protocol enables all HMIs to communicate in a broadcast fashion so that each HMI maintains the same current state of all subsystems.

2.1.2 IPMS Security Concerns

The traditional CIA triad is used to identify defence priorities related the confidentiality, integrity and availability of the IPMS and its component systems (Ackerman, 2017). Confidentiality is the safeguarding of the information contained within the system. Integrity is the ability to ensure the information transmitted and stored is not altered and assures the trustworthiness of the system. Availability is the ability to ensure the network is redundant, suffers minimal downtime and is operational when needed. In OT systems, the priority is often considered to be availability, integrity and confidentiality and all three are a concern with an IPMS and ship operation.

2.2 NICE Framework

The NICE Framework (NIST 2020), enumerates tasks to be performed and the knowledge and skills needed to enable the completion of tasks. It can be challenging for organizations to understand how to describe the knowledge and skills needed for its cyber specialists, and the tasks such specialists must perform. To meet this challenge, the NICE framework defines a series of tasks, knowledge and skill statements associated with common cyber security roles and functions. A task statement outlines an activity performed to achieve an objective. Knowledge refers to a known set of concepts that an individual holds. Skill is the capacity that one has, to apply the knowledge in order to complete a given task. The NICE Framework details task, knowledge and skills (TKS) across 7 role categories and 52 specific cyber security roles.

2.3 Gamification Frameworks

Gamification has been the focus of much research resulting in well over 100 theories, many of which have overlapping concepts (Krath et al, 2021). From the numerous options, four relevant approaches to serious game design are presented.

2.3.1 R-EACTOR framework

R-EACTOR is a design framework for military cyber exercises, grounded on the core principle that an exercise must feel realistic (Dobson et al, 2017). In order to achieve this realism, a cyber exercise must reasonably achieve the following aspects of the exercise experience: Environment, Adversary, Communication, Tactics and Roles with components of each outlined in Figure 3.

R-EACTR FRAMEWORK		
REALISTIC	Environment	Physical
		Virtual
		Psychological
	Adversary	Threat
		Resources
	Communication	Internal
		External
	Tactics	Individual
		Collective
	Roles	Red
		White
		Blue

Figure 3: R-EACTOR Framework (Dobson et al, 2017)

2.3.2 Nested elements of educational game design

An educational game has the goal of teaching knowledge to the players, while being engaging to keep players motivated and committed to the game. Annetta (2010) researched and developed six nested educational game elements that should be incorporated in the design of the game in order to maximize the players level of engagement towards the educational game: Identity, Immersion, Interactivity, Increasing Complexity, Informed Teaching, and Instructional, illustrated below in Figure 4.

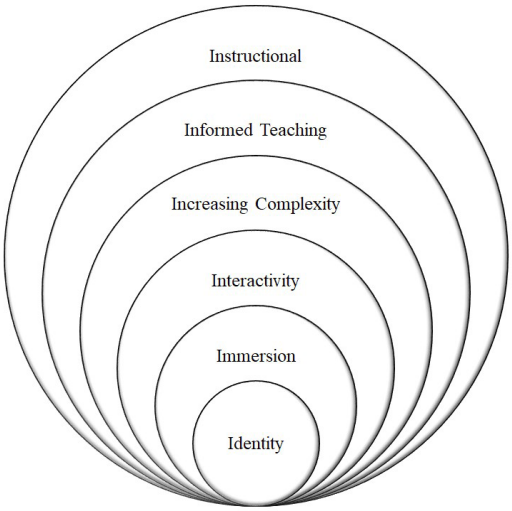

Figure 4: Nested Elements of Educational Game Design (recreated from Annetta, 2010)

The identity element represents the ability for the participant to assume a unique identity within the game to facilitate the immersion and increase user commitment. When users are immersed in the gaming environment, they can achieve a heightened sense of concentration, intrinsically motivating them to complete the challenges. Interactivity refers to keeping participants psychologically invested in the game. Another way to keep participants psychologically invested is through increasing complexity, by progressively challenging them through levels. Informed teaching refers to the importance of students having feedback, and the value of embedded assessments to measure participant performance throughout the game. Instructional is the final component, where the goal of serious games is learning, accomplished through challenge-based learning.

2.3.3 Learning and gaming mechanics mapping

There are many definitions of game mechanics (Lo et al, 2021), the most relevant definition for this work is that game mechanics are “the various actions, behaviours and control mechanisms afforded to the player within a game context. Together with the game’s content (levels, assets and so on) the mechanics support overall gameplay dynamics” (Hunicke et all, 2004). Arnab et al (2015) created a classification table that maps

game mechanics to learning mechanics from Low Order Thinking Skills (LOTS) to High Order Thinking Skills (HOTS): Creating, Evaluating, Analysing, Applying, Understanding and Retention outlined in Figure 5.

Game Mechanics	THINKING SKILL	Learning Mechanics
○ Design/Editing ○ Infinite Game play ○ Ownership ○ Protégé Effect ○ Status ○ Strategy/Planning ○ Tiles/Grids	CREATING	○ Accountability ○ Ownership ○ Planning ○ Responsibility
○ Action Points ○ Assessment ○ Collaboration ○ Communal Discovery ○ Game Turns ○ Pareto Optimal ○ Resource Management ○ Rewards/Penalties ○ Urgent Optimism	EVALUATING	○ Assessment ○ Collaboration ○ Hypothesis ○ Incentive ○ Motivation ○ Reflect/Discuss
○ Feedback ○ Meta-game ○ Realism	ANALYSING	○ Analyse ○ Experimentation ○ Feedback ○ Identify ○ Observation ○ Shadowing
○ Capture/Elimination ○ Competition ○ Cooperation ○ Movement ○ Progression ○ Selecting/Collecting ○ Simulate/Response ○ Time Pressure	APPLYING	○ Action/Task ○ Competition ○ Cooperation ○ Demonstration ○ Imitation ○ Simulation
○ Appointment ○ Cascading Information ○ Questions And Answers ○ Role-play ○ Tutorial	UNDERSTANDING	○ Objectify ○ Participation ○ Question And Answers ○ Tutorial
○ Behavioural Momentum ○ Cut scenes/Story ○ Goods/Information ○ Pavlovian Interactions ○ Tokens ○ Virality	RETENTION	○ Discover ○ Explore ○ Generalisation ○ Guidance ○ Instruction ○ Repetition

LOTS to HOTS

Figure 5: Learning and Game Mechanics Mapping (recreated from Arnab et al, 2015)

This approach focuses on task-centred learning to provide a continuous assessment as the participant progresses through challenge levels.

2.3.4 Capture-the-Flag (CTF)

Capture-the-flag competitions are events which attract skilled analysts to test their prowess against other skilled analysts. These competitions have different variants; two of the most popular ones are the Jeopardy style and Attack & Defend style (Zafar et al, 2023). In jeopardy style, teams or individuals select challenges across various categories such as networking, cryptography and reverse engineering. Attack and defend style often involves live red on blue activity with a refereeing white team. Variations exist that can be synchronous, or asynchronous.

This section provided an overview the fundamentals important to understanding the experimentation, first outlining the general concept of an IPMS, introducing the NICE framework and the concepts of roles and associated tasks, knowledge and skills. The section closed with an overview of a pedagogical approach to gamification and serious game design.

3. Methodology and Design

This section outlines the research methodology and design used to develop an IPMS defensive cyber trainer incorporating the pedagogical game design components that can successfully be used in training MCOs. The methodology involved five key phases. The first phase is determining key MCO tasks required to defend an IPMS from a network attack. The second phase is the development of a training plan to ensure an MCO first understands how the IPMS operates under normal conditions. Third is to develop an evaluation plan, to validate that the MCO can perform the selected tasks from phase one. The fourth phase involves the design of training environment. Phase five is the design of the gamification environment, followed by phase six which implements the defensive cyber trainer through integration of the training and gamification environment.

3.1 Determine MCO Tasks

Prior to the development of any training environment and gamification design, the first step was to determine the key tasks that MCOs must be able to perform in order to defend an IPMS. The tasks identified as the learning objectives of the cyber defence trainer were selected from the *Defensive Cybersecurity* work role detailed in the NICE Framework Components (NIST, 2024). The selected tasks listed in Table 1, collectively represent the core knowledge and skills to be learned.

Table 1: Defensive Cybersecurity Tasks

Task ID	Task Description
T0299	Identify network mapping and operating system (OS) fingerprinting activities
T1084	Identify anomalous network activity
T1085	Identify potential threats to network resources
T1347	Detect cybersecurity attacks and intrusions
T1348	Distinguish between benign and potentially malicious cybersecurity attacks and intrusions
T1350	Perform continuous monitoring of system activity
T1385	Identify network traffic anomalies
T1386	Analyse network traffic anomalies

Understanding the cyber defence tasks required, one can then proceed with a plan on how to develop the associated knowledge and skills in the MCOs. For this research, it was assumed that MCOs had prior training that included a basic introduction to TCP/IP networking, packet analysis and attacker TTPs.

3.2 Training Plan

A training plan was developed to capture the requirements for knowledge and skillsets. MCOs in the defensive cybersecurity role will need to detect attacks targeting the confidentiality, integrity and availability of the IPMS at various different stages of each respective kill chain. Before TTPs can be derived from the tasks listed in Table 1, an MCO first needs to understand normal IPMS operation. This will follow a progressive approach, first with a refresher on basic networking concepts and packet analysis tool usage. Next, MCOs will need to understand how the combination of proprietary and TCP/IP protocols function under normal IPMS operation. To gain this understanding they will require a custom toolset in order to conduct analysis of normal IPMS traffic patterns. After gaining the knowledge and skills to analyse IPMS network traffic and understand normal operations, the MCO, or trainee, can then be evaluated to verify their ability to conduct these defensive cyber security tasks.

3.3 Evaluation Plan

An evaluation plan was developed to capture evaluation strategies and procedures. Each trainee is evaluated to determine whether they have learned the necessary knowledge and skills in the training phase, and is able to conduct the selected defensive cybersecurity tasks in Table 1. The evaluation must include realistic attack scenarios that target the Confidentiality, Integrity, and Availability of the network, as these attack categories encompass most known attacker objectives. In addition, these scenarios should mimic known attacker TTPs to add realism and to enhance the training value. During their evaluation, trainees will also need to have their progress monitored as they work through different scenarios. The trainees are to be provided feedback on their incremental successes or failures. This will help guide trainee actions in detecting threats at various stages of the kill chain and provide useful positive feedback on the effectiveness of their actions.

3.4 Training Environment Design

The training environment was designed to leverage the IPMS implementation outlined in section 2.1.1 and be to support the skillset requirements identified by the training and evaluation plans described above. The flexibility offered by the virtualization and emulation of the IPMS implementation enables the development of a configuration that resembles the number of HMIs and simulated systems on an actual ship. In addition, common open-source packet tools will need to be extended to enable analysis of both the proprietary and open-source protocols used in the training and evaluation phases.

3.5 Gamification of the Training Environment

As identified by Arnab et all (2015) and Annetta (2010), an engaging, realistic and immersive training environment keeps participants stimulated and focused on the learning objectives. The goal of this phase is to design a cyber trainer environment that supports the requirements for training and evaluation within the context of gamification strategies, toolsets and game platforms. The guidance from the studies described in sections 2.3.1, 2.3.2, and 2.3.3 are used to make effective use of the available tools and to design engaging training scenarios

3.5.1 CTF platform design

The CTF must enable the inclusion of the gamification techniques outline in section 2.3 to enable the development of a defensive cyber trainer that maximizes learning. At a high level, this design includes seven core gamification techniques outlined in Table 2.

Table 2: Core Gamification Techniques

Technique	Brief Technique Description
Identity	Trainees register and choose an avatar to identify themselves in the environment.
Increased Complexity	Challenges increase in difficulty, each unlocking individual or groups of increasingly difficult challenges as the game progresses.
Feedback	Feedback is provided throughout the various challenges.
Reward/Penalties	Trainees are awarded points based on the complexity of challenge solved. Should trainees require hints to solve any challenge, penalties can be used that subtract points based on how helpful the hint may be to solving the given challenge.
Assessment	Trainees are assessed on each answer provided whether correct or incorrect.
Competition	Scores from teams or individuals can be viewed by all.
Storyline	The CTF includes a realistic narrative to provide context to the trainee, supporting overall role-play and immersion of the trainee.
Realism	Applicable components of the R-EACTOR framework.

Depending on the format of the training event, other aspects to gamification such as collaboration and communal discovery may also be implemented external to the CTF environment. R-EACTOR framework components related to Internal/External Communications are not applicable to this training environment.

3.6 Training and Gaming Environment Integration

Putting it all together, this last phase integrates the CTF-based training and evaluation packages with the high-realism of the shipborne IPMS emulation/simulation. This involved the development of a training package regarding basic network and tool usage. Next, network traffic from benign IPMS operation was captured, the output being a series of progressively complex challenges that enable the MCO to learn and understand normal IPMS operation. A similar process of network traffic capture and challenge development was conducted for the three attack kill chains. Each progressively complex challenge enables the MCO to learn and understand how to detect and track the attacker within the IPMS system.

4. Results

A proof-of-concept cyber trainer for a marine IPMS, following the methodology and design outlined in section 3, was developed. This proof-of-concept cyber trainer was evaluated on its ability to train MCOs and its application of relevant gamification pedagogical components.

4.1 Experimental Design

The proof-of-concept trainer used the lab environment outlined in 2.1.1 to create a virtual marine vessel running an IPMS that included 39 HMIs, 11 virtual RTUs, 1 rogue HMI and an Ubuntu server operating system that hosted the gaming environment. The virtualized environment was hosted on VMware ESXi and shell scripts using the VMX toolkit were used to create the environment in a known clean state. Networked into the virtualized environment through an external switched connection was a single attacker VM running Kali linux. The HackTheBox CTF solution was used to provided the gamification component of the proof-of-concept trainer.

4.1.1 Toolset development

Integral to this cyber trainer was extending existing tools that allowed for the parsing of packet capture (pcap) files, specifically to parse the IPMS proprietary protocol. The two tools selected for this effort were Wireshark and Zeek. Wireshark is an open-source network protocol parser with an API for custom dissector development. The IPMS protocol parser for wireshark was implemented in a Lua script. Likewise, zeek is an open-source packet analyser that outputs log files categorized by high level connection details and protocol specific files. BinPAC, a zeek-related tool that provides a high-level language to describe protocols, was used to develop the IPMS protocol package for zeek.

4.2 Training Scenario Development

To realize the training plan, the known clean state implemented in section 4.1 was used and benign traffic was captured using tshark. The pcaps were analysed from which a series of progressively challenging questions were created. The questions focused on basic network traffic understanding to specific details regarding the IPMS protocol, time series analysis and unique functions with IPMS. The unique functions were implemented by interacting with various different sub-systems during the packet capture. The scenarios involve the implementation of a rogue device on the IPMS that has a wireless connection to the attacker when at port, the installation of which was considered outside the scope of this research.

4.3 Evaluation Scenario Development

The evaluation scenarios were based on the three developed attacks against IPMS, each focused on compromising IPMS confidentiality, availability and integrity, respectively. Each scenario increases in complexity from a detection perspective, and as the trainee progresses, fewer hints are provided.

Evaluation 1 – Confidentiality Scenario. The confidentiality scenario involved the attacker wirelessly connecting to the rogue device that is masquerading as a legitimate IPMS device. The rogue HMI impersonates a legitimate HMI by mimicking IPMS broadcast communications that inform other network hosts of its address. The rogue device can also receive broadcast IPMS messages. The objective is for the trainee to detect this new rogue device through understanding of the standard IPMS configuration, including expected HMIs.

Evaluation 2 – Availability Scenario. In this scenario, the attacker performs a scan for a vulnerability on the HMIs, selects one HMI to target, and exploits the vulnerability. This attack adversely impacts the availability of the targeted HMI. The objective is for the trainee to identify which subsystem has been compromised.

Evaluation 3 – Integrity Scenario. In this scenario, the attacker turns off the target being exploited in the Evaluation 2 scenario, targets/compromises another device, then uses that device to indicate evidence of a fire in multiple locations on the ship. This attack adversely impacts the fire suppression sub-system of the IPMS. The objective is for the trainee to identify that one device was turned off, what new device was compromised and which sub-system was responsible for falsely indicating the presence of fires.

Successful completion of the evaluation scenarios demonstrates achievement of the desired tasks listed in Table 1.

4.4 Gamified Environment

The gamified environment provided three different training components using the RootTheBox (RTB) environment (DeMesy, 2024): a playbook, training scenarios and evaluation scenarios. The playbook provides background information about the operation and protocols of the IPMS. The playbook along with the previously described scenarios were implemented in the RTB framework.

4.5 Evaluating Cyber Trainer to Pedagogical Components

This section describes how the implemented cyber training achieved the pedagogical components described by the R-EACTOR Framework, Game Mechanics to Learning Mechanics and a Framework for Serious Educational Game Design that were outlined in section 2. The core components of each framework are listed below with a brief explanation regarding their implementation.

4.5.1 R-EACTOR

Environment. The pcaps from the simulated environment have a similar configuration and activities as do a real IPMS installation.

Adversary. The attack scenarios are modelled against real TTPs and objectives from known attacker groups.

Tactics. The defensive TTPs and the extended tools are applicable to investigations on real ships.

Roles. The MCO's role in the framework is the same as their real word role and responsibilities.

4.5.2 Game mechanics to learning mechanics – thinking skills

Creating. MCO's are responsible and accountable to devise a strategy to resolve each challenge.

Evaluating. Each challenge is worth a certain number of points and during evaluation, points are deducted for incorrect answers to dissuade guessing. Instructors can also monitor progress in real time.

Analysing. Immediate feedback is provided to the trainee when entering a solution. The packet captures from the IPMS system in the CTF framework were captured from a simulated distributed system with emulated HMI and RTU that closely mimics the configuration seen onboard a ship.

Applying. With progressively more challenging questions, MCOs must apply what they have learned to apply what they have learned.

Understanding. The Playbook is offered to the trainees as a reference to help them understand concepts they need to succeed at the challenges. The knowledge and skills needed to progress through the evaluation scenarios confirms their understanding.

Retention. The realism of the environment and storyline, along with the feedback and continual assessment aid in retaining the knowledge and skills gained.

4.5.3 Framework for serious educational game design

Identity. When registering to the CTF platform, trainees choose their individual name and an avatar to represent themselves in the platform in the MCO role.

Immersion. The trainee is uniquely tasked to investigate an event on a very realistic implementation of IPMS from a known threat actor. This allows the trainee to become more immersed in the scenario and gaming environment.

Interactivity. The trainees interact with the framework by progressing through the playbook and scenarios with immediate feedback and scoring when submitting answers to each challenge.

Increased Complexity. As trainees progress through the CTF, challenges become increasingly more complex.

Informed Teaching. Instructors can virtually observe trainees' progress and routinely conduct analysis on various statistics and patterns across each.

Instructional. Challenges are designed in such a way that it requires creative and critical thinking to solve via experimentation and analysis.

This section provided an overview of the results that highlighted the experimental design, scenario development and the gamified environment based on the RootTheBox framework. It concluded by validating the pedagogical components that it implemented.

5. Conclusion

An IPMS is integral to modern marine vessels that consist of enterprise and operational technologies that monitor and control various different cyber physical systems. This research provided a methodology for creating a gamified learning environment for MCOs that also resulted in a proof-of-concept defensive cyber trainer for an IPMS. The trainer implements pedagogical learning components and extended open-source packet analysis toolsets, and provides a structured, progressively challenging approach.

References

Ackerman, P. (2017) "Industrial Cybersecurity", Packt Publishing, Birmingham, United Kingdom.

Afenyo, M. and Caesar, L.D. (2023) "Maritime cybersecurity threats: Gaps and directions for future research", Ocean & Coastal Management, 236, 106493.

Annetta, L.A. (2010) "The "I's" Have It: A Framework for Serious Educational Game Design", Review of General Psychology, 14(2), 105–113.

Arnab, S., Lim, T., Carvalho, M.B., Bellotti, F., de Freitas, S., Louchart, S., Suttie, N., Berta, R., De Gloria, A. (2015) "Mapping learning and game mechanics for serious games analysis", British Journal of Educational Technology, 46(2), 391–411.

Australian Navy (2025) "Cyber Operator", [Online], https://www.adfcareers.gov.au/jobs/navy/cyber-operator.

Canadian Armed Forces (2025) "Cyber Operators", [Online], https://forces.ca/en/career/cyber-operator/.

Defence Connect (2021) "Integrated Platform Management System – a key system for Australia's warships", Article.

DeMesy, J. (2024) "RootTheBox", [Online], https://github.com/moloch--/RootTheBox.

Dobson, G.B., Podnar, T.G., Cerini, A.D. and Osterritter, L.J. (2017) "R-EACTR: A Framework for Designing Realistic Cyber Warfare Exercises", Carnegie-Mellon University Technical Report, CMU/SEI-2017-TR-005.

Harish, A.V., Tam, K. and Jones, K. (2025) "Literature review of maritime cyber security: The first decade", Maritime Technology and Research, 7(2), 273805–273805.

Hunicke, R., leBlanc, M., Zubek, R. (2004) "MDA: A Formal Approach to Game Design and Game Research", Proceedings of the Association for the Advancement of Artificial Intelligence.

Karaś, A. (2023) "Maritime industry cybersecurity: a review of contemporary threats", European Research Studies Journal, Vol XXVI, Issue 4.

Krath, J., Schürmann, L., von Korflesch H.F.O, (2021) "Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning", Journal of Computers in Human Behaviour, Vol 124.

Lo, P., Thue, D. and Carstensdottir, E. (2021) "What Is a Game Mechanic?", 20th International Conference Entertainment Computing, 336–347, [Online], https://doi.org/10.1007/978-3-030-89394-1_25.

NIST (2020) "Workforce Framework for Cybersecurity (NICE Framework)", NIST Special Publication 800-181 Revision 1, [Online], https://doi.org/10.6028/NIST.SP.800-181r1.

NIST (2024) "NICE Framework Components v1.0.0", [Online], https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions.

Norris (2025) "Integrated Platform Management Systems", [Online], https://www.noris-group.com/products-and-systems/maritime-system-solutions/integrated-platform-management.

RH Marine (2025) "Integrated Platform Management Systems", [Online], https://rhmarine.com/en/ipms.

Royal Navy (2025) "Cyber Operative", [Online], https://www.royalnavy.mod.uk/careers/roles/cyber-operative.

Soner, O. and Kandemir, C. (2024) "Proposing the future skill requirements for maritime cyber security", Cognition, Technology & Work, 26(2), 361–374.

Timmins, J., Knight, S., Lachine, B. (2021) "Offensive Cyber Security Trainer for Platform Management Systems", IEEE International Systems Conference (SysCon), 1-8.

United States Senate Committee on Armed Services (2018) "Cyber Posture of the Services", 115th Congress (Testimony of Vice Admiral Michael M. Gilday, USN), March.

Zafar, A., Yamin, M. M., Kattt, B., Torseth, E. (2024) "All flags are not created equal: A deep look into CTF Scoring Algorithms", Expert Systems with Applications, Volume 254.