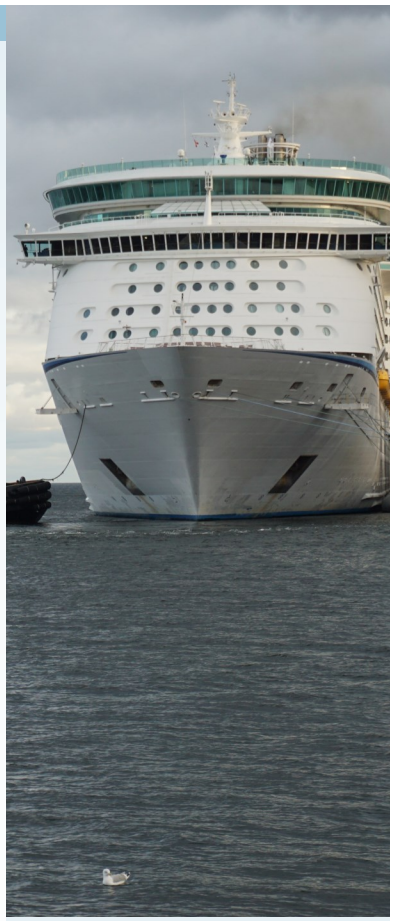
International Association of Maritime Security Professionals

30 August 2023
Volume 1, Issue 1



# Wavefront

## Professional Certificate in Maritime Security

Wolfeville, NS

The *Professional Certificate in Maritime Security (PCMS)*, a joint offering with Acadia University, is underway with its first group of students having completed the first course and well into the second. This marks a unique milestone in Canada's maritime security education and training that officially moves the certificate program out of the design and implementation phase and into the operations and management phase.

The certificate is now expanding courses to broaden the number of elective courses on the Acadia University side. This will allow candidates greater variety in their courses. At this time, however, a registering candidate can proceed through the full suite of courses without concern that they will have to wait for any further course development.

The IAMSP (International Association of Maritime Security Professionals) has made certain adjustments to its delivery model to assist students. This primarily focuses on returning to a more one-to-one approach that allows individual candidates greater flexibility as they balance their professional development, work, and home lives. (Visit https://maritimesecurity.acadiau.ca for details).

## IACS Incoming Requirements

The International Association of Classification Societies is pushing forward with Unified Requirements intending to improve the cyber resilience of vessels. In addition to the two new requirements (IACS UR E26 Cyber Resilience of Ships and IACS UR E27 Cyber Resilience of Equipment Carried on Board Ships) that are intended to come into force for ships contracted after 01 January 2024, there are also significant efforts being made to update the currently in-force IACS UR E22 that has underpinned many cyber security considerations and their linkages to safety critical systems.

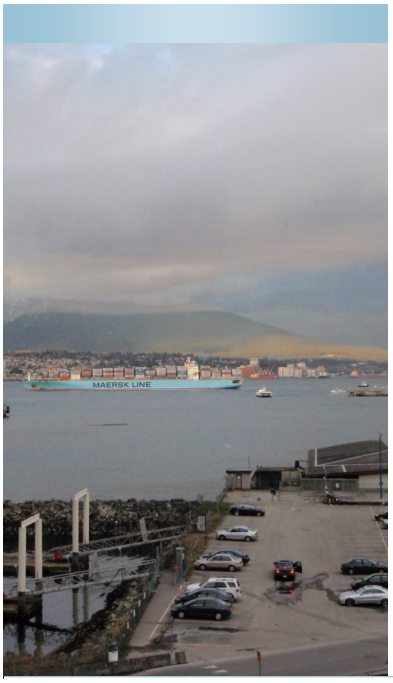
Those working in these domains will face some significant challenge. One of these will be how to conduct the verification and validation that these requirements have actually been integrated into the various designs. It will also challenge those involved in field inspections.

### Inside this issue



### Special points of interest

- Our first group of candidates in the PCMS is nearing the half-way mark of Association hybrid (online an direct support) courses
- Severe weather events are forcing a rethinking of supply chain and infrastructure management.




## Accommodations for Seafarers?

The mental health of seafarers has a maritime security impact that very closely mirrors, if not overlaps, the safety aspects. From the safety perspective, human error tends to increase where people are under mental strain (or even duress) or become unduly fatigued.

What does this means from the security side of the equation? Part of this solution may involve adopting zones within international seaports where seafarers can leave the ship and receive shore based services. The idea here is that by creating a controlled environment that can be accessible during these kinds of environments, we reduce the risks of crew members reaching that threshold.

These would likely need to be hotel-style accommodations. Calculating the size of this facility is fairly straight forward: simply look at the vessel schedules and crew sizes and there should be more than enough data to make reasonable estimates.

The hotel-style structure also allows for a degree of centralization of certain services. These could range from the various services offered by CBSA and other federal entities.

The key to this would be to have this area being designated within the Customs area of the port in such a way that those leaving the ship have not technically entered Canada. This model already exists in several ports around the world.

*Innovation within the maritime space needs to build security into its thinking, not as an "add on" but as an emergent property resulting from good engineering.*

### Systems Engineering

The Department of National Defense (DND) has made two major announcements that will impact the maritime security domain, particularly in shipyards and in DND's supply chain.

The first of these involves the announcement that Canada will be working with the USA on the Cybersecurity Maturity Model Certification (CMMC) .

The second of these involves the adoption of the Systems Engineering approach within its procurement processes (DAOD 3033-0). While this pertains more to Canadian firms, the requirement does mark a shift within the NATO community to require more rigor in procurement processes.

## Security within Innovation

There are billions of dollars currently being expended on innovation to help us understand the world's oceans and how they affect climate. This space has become highly competitive and nearly its own market. Some thoughts with respect to "design philosophy" may be in order.

There are two main questions that any product needs to answer. First, is it doing what it's supposed to be doing? Second, is it doing so in a way that avoids being a detriment to the other elements or services around it? Recent conferences have shown that the traditional approaches of simply applying a framework at the end of the process continue to permeate this space.

Innovation is often a complex enough challenge so the approach may benefit from taking a balanced approach. Those involved in the innovative space may want to answer the following questions:

- Am I aware of the range of environments in which the product may be required to work?
- Can it deliver its core services under that full range of conditions?

The interaction in the security context is through the infrastructure assurance lens. While many traditional security programs focus on data loss (or information security breaches), this lens focuses on the *availability* and *integrity* security attributes.

The next step would be to communicate the requirements stemming from those needs and expectations to the engineers working on the issue so that those requirements can be incorporated into the list of requirements to be met before acceptance.

Taking this approach not only helps build better products, but those that approach security as a core requirement of the system may find that the overall cost of security is more rational that simply following compliance and "bolt on" approaches.

*Continued on Page 6...*

## Climate Change Impacts and Supply Chain

A recent significant rainstorm in the Halifax, Nova Scotia area provides a quick illustration of how significant weather events can impact port operations and security in short order. July 22nd saw significant rainfalls (in some areas three months of rain fell in less than a day) cause widespread flooding. In addition to tragic loss of life and the difficult circumstances families found themselves experiencing, a key rail line was significantly undermined. This rail line was the primary support for the Port of Halifax for container and other rail-borne shipping.

The lesson here can be summarized in three major parts:

1. Understand your supply chain and that local events may cause system-wide impacts. What may look like a very efficient system may also be one that presents to many opportunities for this kind of disruption.
2. Get used to operating less from an infrastructure protection / asset protection perspective and start making sure that there's resilience in the system. While the protective aspects are important, we need to start layering our thinking to look at resilient systems that offer us the means or opportunities to adapt to those impacts.
3. Build up a capability to respond effectively and test it. There are currently a range of discussions about how this response went. This is not to cast aspersion towards the first responders (who were traditionally going well above and beyond), but it is to say that there are clear indications of certain areas that could stand improvement.

This, however, is normal. What is important is to focus less on "fixing the blame" and to get on with "fixing the problem." This means reducing the instances and temptation to look for "who's at fault" and to focus on what can each party do better.

This isn't just limited to government or first responders either. People also need to understand that they have a role to play in these events, even if it means just having basic preparedness in place and having a working understanding of what they would do under certain circumstances.

### Climate and Weather

Confusion still seems to exist when discussing climate change and extreme weather events. These two things, while linked, are not the same.

Climate change is must be looked at as in two contexts. First, it is systemic in nature. It is not just about sea temperatures, air temperatures, changes in humidity, or the distribution of moisture. It is about all of those things together.

It must also be looked at in terms of a longer-term shift. This is not a "one-and-done" kind of issue but is one that requires longer term solutions. Those longer term solutions are going to impact how we would like to organize ourselves and how we want to live—like it or not.

Extreme weather, on the other hand, is what hits you when you step on deck or walk out the front door. Severe storms, rainfall events, heat, winds, and other immediate conditions fall into this category.

Extreme weather may or may not be caused only by climate change. These are not simple systems, they are complex, adaptive systems that are rebalancing into a "new normal." What can be certain, however, is that the changes to climate are certainly one factor (and likely a very significant one) that is helping form these events.

## Being Left Behind?

While industry continues to push on with the research and development of various forms of automation in shipping, we continue to see an emerging gap with respect to how the various underpinning aspects of that automation can be handled.

Consider, for example, the difference between the European Union and North America with respect to the development of Artificial Intelligence.

As we look at the European Union's AI Act, there is a clear declaration that AI systems which "are safety components of products" will be considered "high risk" and come with a number of requirements in their development.

This needs to be superimposed on the requirements that we are likely to see under IACS Unified Requirement E22 that will come into force on 01 July 2024. These two sets of requirements set out a series of requirements for design artefacts, plans, tests, and other forms of checks and balances.

In this respect, Canada is clearly lagging on this issue. The current guidance from Transport Canada points towards the use of a voluntary standard derived in the United Kingdom but has some puzzling statements like having an authorized representative that may not know the course or speed of the MASS.

The risk here is that Canadian industries may be forced to adopt European requirements in order to keep pace with the market, leaving Canadian interests by the wayside.

# A Subtle but Profound Shift

While ships have often been considered relatively isolated as a result of their difficulties connecting at sea, this is changing. New services entering the market can now connect ships with better-than-high speed internet that covers the world.

As a result, there needs to be an understanding of two attack vectors. These attack vectors are not new to those working in the port operations, but may require some validation of requirements for those heading out to sea.

Directly connecting to the internet comes with its own host of challenges . Maintaining the infrastructure necessary to protect the ship from those issues will also take up its own resources. These need to be understood very early in the planning and design phases.

The second element involves memory devices such as personal devices. This has two aspects. The first involves the ability to carry malware onto the ship. The second involves the presence of applications or other forms of activity that may interfere with systems.

There will be a temptation to carry these two systems on the same infrastructure. At this point, network segregation needs to be complete between those systems identified as being safety sensitive (in the context of IACS UR E22, E26, and E27) and the relatively uncontrolled connections to the internet.

# Approaching Cyber Security

Cyber Security needs to be looked at differently as we look at different phases of the lifecycle, both within ports and for ships. Consider the life cycle that involves planning, analysis, design, implementation, ,management, and removal from service. Each of these phases need to approach the issue from different perspectives.

For those involved in innovation, the analysis of requirements underpinning new technology, or design activities, cyber security is much more than simply adopting the latest and greatest in terms of standards or best practices. Cyber security in this aspect needs to be related (strongly) to the business it intends to serve and the organizations that it affects. Those involved in this phase of activities may wish to consult the doctrines put forward by the International Council on Systems Engineering (InCoSE) or the National Institute for Standards and Technology (NIST) doctrine on either Engineering Trustworthy Secure Systems (NIST SP 800-160 vol 1 rev 1) and Developing Cyber Resilient Systems (NIST SP 800-160 vol 2 rev 1). Those that are remaining current in this area will not that these approaches support the stated goals associated with the incoming IACS Unified Requirements E26 and E27 that will come into force for ships contracted to be built after 01 January 2024. In this context, the structured and analytic approach to cyber security (not simply the adoption of measures communicated in a standard) needs to be undertaken.

As we more through the design phases and into more of the implementation (building) phases, guidance with respect to cyber security will largely depend on what kind of infrastructure is being built. In Canada, however, one should be ready to look towards not only C-26 (currently passed second reading) and similar legislation. For those involved in defense contracting, however, the incoming CMMC (Cybersecurity Maturity Model Certification) is coming into force soon.

The concept of cyber hygiene and best practices on board vessels may be enough for those operating existing infrastructure in the near term, but this will change and may change rapidly. Organizations, and particularly those responsible for their cyber security function (either in-house or third parties) may wish to get ahead of the curve and broaden their understanding.

## Situational Awareness

The recent NHL Stenden's University of Applied Sciences MCAD Maritime Cyber Attack Database (MCAD) has become publicly available and one of several organizations that is providing a view of cybersecurity threats to the maritime domain.

Understanding the threat picture is a key aspect to building effective cyber security controls. If we take the mantra that threats exploit vulnerabilities to attack assets and thereby put organizations (or operations) at risk, the reason for this is self-evident.

The database itself is a significant and positive step but it is still nascent. Not only will it require broad net to capture data, it will also need to recognize that if the public is providing that data, then the reports and returns should be equally available to the public.

The database, at first look, needs to be considered as part of a constellation of sources. This is largely to (1) establish a more complete view of the issue and (2) establish the reliability and credibility of the database in relation to other sources.

The first very positive steps have been taken. The launching of this database, however, will require "care and feeding" into the long term, something that can be challenging for organizations.


*A recent study conducted by the Cyber Risk Management Project indicated an attack where 92% of the total economic costs were uninsured.*

## An Operational Gap?

While we have concentrated much of our understanding of cyber security on ports or on ships, the approaches to cyber security continue to demonstrate an approach that fails to recognize the maritime industry's role within supply chains.

The role of any transportation network is the movement of persons and goods so that they arrive at their expected destination on time, in acceptable condition, and for reasonable cost. Achieving this goal is a combination of the outputs of various systems coming together, each of which relies upon the contributions of persons, tools, spaces, information, and supporting services to be successful.

In looking at this issue, the question of how cyber security risks flows between the ship and the port during interfaces in an area that warrants attention.

This was identified in a report published by the Cyber Risk Management (CyRIM) project referred to as the Shen Report. This report took a hypothetical transit and looked at the potential impacts associated with the movement of malware or otherwise disruptive code from the ship to the ports along the transit. The link here will take you to the Lloyd's page where the report can be read in its entirety.

The operational gap being referred to here involves the ability of those operating in ports and for ship operators to be able to make reasonable comparisons between the increasingly divergent systems used to assess the cyber security on board vessels and those in ports.

Cyber security on board vessels is largely being dictated through IMO guidance, industry best practices (tied more to cyber hygiene or cyber security at the operations and management phase of the life cycle), and the evolving requirements from IACS At ports, cyber security faces a different weave of requirements, ranging from critical infrastructure protection, national legislation and guidance and supply chain security.

Mariner Innovations, a Halifax-based company, is currently soliciting participation from Canadian ports and shipping companies on the development and implantation of tools of this type.

## A Knowledge Gap

As we look towards new and improved ways of ensuring that security is built into the various systems, we need to review and update our education, training, and mentoring regimes to ensure that we maintain that critical mass of practitioners within the space.

While IT security practitioners are plentiful, what is lacking is a combination of IT security practitioners that have a good understanding of the maritime space, how it operates, and the various safety considerations that need to be considered.

At the same time, we need to be careful that the market is not simply dominated by structures that are more akin to guilds or licensing regimes. These tend to serve those organizations more than the industry itself.

One alternative to this may be to provide free familiarization training through the IMO eLearning platform. Courses on pollution control and similar challenges already exist in that space, they can be distributed fairly to any individual that has the capability to receive them, and can be separated from commercial interests.

This may also help communities that currently face economic challenges in accessing training. Care will need to be taken, however, in ensuring that access to the technology does not become the limiting factor. While there is only so far an organization can go to ensure fair and equitable distribution across all environments, we should not let perfect get in the way of good. An attempt should be made to keep things well balanced.

# Security Within Innovation

*Continued from Page 2*

To be clear, using the Assurance lens does not mean reducing the need for good security within the system or service being offered. Quite the opposite. If we accept the National Institute of Standards and Technology (NIST) definition of system assurance, we find that we are focusing on the "justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its life cycle." (NIST Computer Research Center definition)

The first aspect of this is the need for this activity to span the full life cycle of the project. These different phases are often expressed in different ways but generally resolve to conceptualization, design, production, operations and management, and removal from service. Some regimes include the acquisition of raw materials and transportation / shipping as distinct phases and these should be considered when they fit the context. For example, we may be more worried about shipping when we are delivering a software product as opposed to a centralized software service.

Those involved in the innovation process need to map these kinds of activities and how they are going to be represented early in the process. Failing to do so may not impact the product immediately, but it will serve to confuse processes, lead to challenges in inconsistent documentation, and may force rework behind the project—all undesirable.

*Initially a chain link fence, this fence required modification to prevent persons from simply cutting the fabric. Both an example of good risk management and infrastructure management, but also an example of issues that can led to rework*

The second aspect that needs to be emphasized with the evolution of security doctrine applies to innovations that may affect what are considered safety-critical systems. The key definition for safety-critical systems in the maritime space can be found in IACS Unified Requirement E22 Section 3. While the ISM Code for ships speaks to the identification of equipment (etc.) supporting safety functions, the IACS definition refines this into a reasonably structured approach. What should be of concern to innovators is if their innovation pertains to equipment that could fall into either Category 2 (failure could eventually lead to dangerous situations) or Category 3 (failure could immediately lead to dangerous or catastrophic situations) equipment, noting that these apply in the contexts of "human safety, safety of the vessel and / or threat to the environment." (IACS UR E22 Section 3.1).

If your innovation falls into either of these categories, then you need to be aware of the Quality Management System guidance provided (currently proposed) in IACS UR E22 Revision 3. You may be well-served by also looking to the various levels of progressive testing and evaluation that will need to be demonstrated as part of the documentation necessary to have the systems certified.

The IACS UR E22 Revision 3 is intended to come into force on 01 July 2024. This means that there is still a little bit of time to make controlled adjustments to various project plans and even adjust engineering-led processes to ensure that any requirements that would apply to the innovation are actually thought through (as opposed to being pushed through).

Of course, while this article is intended to be informative, it should not be your sole basis for action. It is intended to make you aware of another potential source of requirements and those involved in the innovative process should conduct their own evaluation of the incoming UR's impact on their efforts.

# Climate Change and Supply Chain

*...Continued from Page 3*

If we look at the severe weather events and conditions that are being exacerbated by climate change, we can see that we have a challenge ahead of us from an infrastructure perspective. That being said, we can reduce the challenges to some basic principles.

The first principle involves the ability to maintain a capacity to deliver critical services when faced by (1) an increase in demand and (2) the loss of part of that capacity due to impacts. Consider the road networks behind ports. Is there enough capacity to move trucks through the road networks and out of harms way if those roads are suddenly needed for evacuations? Is there a way to preserve some of that capacity for the movement of persons and goods without endangering public safety or putting evacuating populations at increased risk?

Answering this challenge comes in two parts. First, is there enough useful infrastructure? This refers to infrastructure that can be counted on to provide that capacity both normally and during the event. If your infrastructure is being threatened by a forest fire, for example, this may not be the time to route shipments of dangerous cargo over wooden bridges.

*Port Operations need to be understood in terms of their being both a Critical Infrastructure entity but also a key transition point in supply chains.*

The second part of this question looks at the mitigation strategy. What is the preferred option to reduce the potential risks associated with the port's operations? Given the circumstances, is it better to leave certain things in place or should they be moved? For example, if the threat involves fire, is it safer to protect containers in place or is it more prudent to locate them outside of the impact area? That is a question that a good risk assessment should be able to answer but also needs to be looked at in terms of immediate circumstances and contexts.

When we look at recent severe weather events, there are some warnings we may want to pay attention to. The first involves the state of the infrastructure and its ability to withstand the severe weather events. The image on page 3 of the rail line that was undermined is a clear example of this as are the various other images you can find of bridges and roads that were severely impacted. Fortunately, we appear to be moving past the age of "replacement only" to an age where organizations (including governments) understand that "building back better" is the way to go.

Our second challenge falls into the domains of preparation and response. If we look at the resources that have had to be committed in fire response, it does not take long for a reasonable person to conclude that it would be beneficial to have a greater capacity to deal with those events. There is also a bit of stratification happening between administrations that are making investments to improve this kind of capacity and those that believe they can simply rely on the good will of their neighbours. While there is always a need for a level of fiscal prudence, there may well be some benefit to maintaining at least a modest internal capability (at a baseline) knowing that when things become difficult, you're part of a community of contributors and not just a consumer of other entities' resources.

Finally, there is the need to build resilience into the systems and not just robustness. Recent events have shown how the transportation systems behind and around communities have been challenged through single routes in and out. Fires in Halifax, NS, for example, faced challenges in evacuation due to the fire crossing that road. Other communities, such as Yellowknife NWT have faced significant challenges requiring pre-emptive evacuations due to there being a single highway needed for a significant number of evacuees.

We have also seen, largely in the tragedy of Lahaina, Hawaii and in Kelowna, BC, we see events that pushed through communities right down to the waterfront. For those involved in port operations (and specifically where items held at the port may involve dangerous goods or cargos, there may be a need to take steps that are more in the mitigation phase of the Emergency Management cycle than preparedness and response. These considerations may include making arrangements for advanced warning of events, assistance in the movement of dangerous goods, or even arrangements to have equipment available that can be used to protect such items from events.

*Emergency Management often looks to tragic circumstances as a way of preventing or reducing the impacts of future events. We would encourage readers wanting to help to seek out credible and capable organizations, such as the International Red Cross or similar organizations to assist those caught in tragic circumstances*

## International Association of Maritime Security Professionals

The International Association of Maritime Security Professionals ' goal is to build capacity within the maritime security space through a combination of efforts supporting education, training, and research. Made up of a combination of academics and practitioners from across multiple domains, the Association seeks to build a trusted community, not to dominate a market but to support those within the maritime security sector.

# Publication Schedule

This newsletter will be sent out every two months (February, April, June, August, October, and December) around the last business day of the month. The focus of the newsletter are those activities within the International Association of Maritime Security Professionals (IAMSP) that seek to build capacity as well as other developments outside of the Association that may serve those seeking to improve their maritime security posture, education, skills, or experience.

The publication falls under the oversight of the Chief Learning Officer for the Association.


## International Association of Maritime Security Professionals

International Association of
Maritime Security Professionals, Ltd.
Registered Office
Office 4 - 219 Kensington High Street
London W8 68D
United Kingdom

Email: clo at iamsponline.org
https:.//www.iamsponline.org


For those seeking to support those facing catastrophic circumstances such as those in Lahaina, Hawaii or similar events, please visit the relevant links below. Our hope and thoughts are with those caught in those very difficult times. These addresses should be used in search criteria to take you to the appropriate websites:

- American Red Cross: https://www.redcross.org or call 1-800-733-2767 (RED CROSS)
- The Hawaii Community Foundation: https://www.hawaiicommunityfoundation.org/maui-strong
- Hawaii Animal Rescue Foundation: https://www.nfggive.org/donation/45-2081227

For events in Canada, the Canadian Red Cross donation page can be found at https://www.redcross.ca/donate/appeal/donate-to-the-canadian-red-cross-fund#a0650cb6-ce29-4c40-b663-e749a0a9163f

*It is regretful that certain people or organizations choose to take advantage of these kinds of events for their own gain or profit by scamming individuals seeking to support those in need. Be aware that these scams are occurring and that care should be taken to make sure that the organization you are supporting is actually providing that support "on the ground."*