Port Operations Cyber Risk Assessment

An Operations-Based Approach to Port Cyber Risk
A Port Houston Proof of Concept

WRITTEN BY
John A. Wilson, Ph.D.

2026

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY

Port Operations Cyber Risk Assessment
An Operations-Based Approach to Port Cyber Risk
A Port Houston Proof of Concept

Technical Paper Prepared for the
Sam Houston State University Institute for Homeland Security
Enhancing Infrastructure Security and Efficiency through IT/OT/ICS Integration

John A. Wilson, Ph.D.
Entellect LLC
JohnWilson@EntellectLLC.com
July 2026

Abstract

Port operations depend on interconnected digital, operational technology, and industrial control systems that span many organizations and exchange information under time pressure. When those dependencies are not well understood, a cyber event in one system can cascade across stakeholders and disrupt the movement of ships and cargo. Traditional cybersecurity work is necessary, but it often focuses on individual systems, compliance requirements, or control checklists. Port leaders also need a complementary operations-based answer: which systems, data exchanges, stakeholders, and workarounds matter most to keeping port operations moving?

This paper presents an operations-based approach to port cyber risk, demonstrated through a proof of concept for the Port Houston public terminal complex. The approach adapts Mission-Based Cyber Risk Assessment (MBCRA) logic to civilian port operations by starting with the work of the port, not with a technology inventory [1], [2]. It uses a Port Operations Framework to define the operational scope; Operations Threads and Operations Engineering Threads to show how selected operations unfold; a Systems Repository to connect activities to systems, data, actors, and dependencies; and an Operational Impact Assessment to identify where confidentiality, integrity, or availability failures may have the greatest operational consequence.

The proof of concept focuses on container handling throughput, but its larger purpose is to give stakeholders a concrete starting point for a common cyber-risk process. The framework, threads, repository, and preliminary ranking are straw-man artifacts, not a final stakeholder-approved risk register. Used through a Port Cyber Table Top (CTT) Exercise, they can be validated, corrected, prioritized, and converted into action by the organizations that own, operate, secure, regulate, or depend on the selected operation [1]. The Port CTT Exercise is intended to provide the recurring forum for surfacing stakeholder concerns, building shared understanding, maintaining a backlog of operations to assess, and focusing cybersecurity work on resilience and continuity.

Over time, validated Port CTT Exercise results could be maintained in a practical Enterprise Architecture repository: a living, searchable map of how port operations, systems, data exchanges, vendors, stakeholders, and manual workarounds connect. This systems-of-systems view can help port leaders see operational cyber exposure across organizational boundaries and use it to guide cybersecurity investment, continuity planning, incident response, vendor and remote-access governance, and U.S. Coast Guard cybersecurity assessment and planning requirements [3].

Contents

1. Introduction and Overview 1
1.1 Purpose and Audience 1
1.2 The Institute for Homeland Security 1
1.3 What This Paper Provides 1
1.4 Scope of the Proof of Concept 2

2. Gap Assessment and Problem Statement 2
2.1 The Core Problem 2
2.2 Why Current Approaches Fall Short 3
2.3 The Regulatory Clock 3

3. Topic Discussion 4
3.1 Mission-Based Cyber Risk Assessment as the Foundation 4
3.2 Method Overview: Four Phases 4
3.3 Phase 1 — The Port Operations Framework 4
3.4 Selecting an Operation for the Proof of Concept 8
3.5 Phase 2 — Operations Threads and Operations Engineering Threads 9
3.6 Phase 3 — The Port Operations Systems Repository 10
3.7 Phase 4 — The Operational Impact Assessment 13

4. Way Forward 16
4.1 Use the Proof-of-Concept Artifacts as Straw Men 16
4.2 Convene the Port CTT Exercise 17
4.3 Convert Findings into Prioritized Cybersecurity Requirements 18
4.4 Maintain a Living Enterprise Architecture Repository 19
4.5 Repeat the Process Through a Prioritized Backlog 20

Appendix A. How the Framework Was Developed 21

Appendix B. Port Operations Framework — Level 3 Detail 22

Appendix C. Extended OET Detail — Integrity Decision Points 28

Appendix D. Prioritization Method Provenance — Lean Portfolio Principles 29

Appendix E. Port CTT Exercise Roles 31

Appendix F. References 32

Author Biography 34

1. Introduction and Overview

1.1 Purpose and Audience

This technical paper is written for port executives, terminal operators, facility security officers, cybersecurity and incident-response teams, and the information-technology (IT) and operational-technology (OT) professionals who support them. It gives these leaders a repeatable way to bring multiple organizations into a common cyber-risk process focused on one practical question: which systems, data exchanges, stakeholders, and workarounds matter most to keeping port operations moving?

1.2 The Institute for Homeland Security

The Sam Houston State University Institute for Homeland Security (IHS) provides applied research and practical guidance for organizations that protect critical infrastructure, spanning transportation, energy, healthcare, water and wastewater, chemical facilities, cybersecurity, supply chain, artificial intelligence, crisis management, and workforce development. In that context, this paper is presented as an extension of that portfolio into applied port operations cyber risk assessment, with Port Houston as the initial application domain.

1.3 What This Paper Provides

The paper describes a four-phase method for translating port operations into cybersecurity priorities. It adapts Mission-Based Cyber Risk Assessment, a Department of Defense approach, to the civilian port environment and keeps the analysis anchored in operations rather than in technical control checklists [1], [2]. The artifacts are intended to support stakeholder discussion and action, not to serve as a final answer by themselves. The method describes systems by the function they provide (the system capability categories in Section 3.6), not by specific products or configurations. This is called the capability level. Detailed analysis of specific systems stays with each system's owner, as described in Section 4.2.

The method is designed to be portable and repeatable. The framework, selection matrix, Operations Thread, Operations Engineering Thread, Systems Repository, and impact assessment are intended to give the Houston port community a structured starting point for Port CTT Exercise review. In that exercise, the organizations that operate, secure, regulate, or depend on a

port operation validate the thread, supply local system and data information, and agree on cybersecurity requirements. The worked example, container handling throughput, has received an initial subject-matter sanity check and is offered for broader stakeholder validation, refinement, and use.

1.4 Scope of the Proof of Concept

- The scope includes the Port Houston public terminal complex, including the Barbours Cut and Bayport container terminals and the general cargo terminals at Turning Basin, Care, Jacintoport, and Woodhouse.
    - Framework intent. Port Houston is the proof-of-concept site. The method is designed so comparable U.S. deep-water ports can adapt it to their own operations and systems.
    - Vessels. Container ships calling at Barbours Cut and Bayport are the vessel class in scope. Harbor craft such as pilot boats, tugs, and line-handling launches appear only where they interface with the container ship arrival, berthing, and departure sequence, including pilot boarding, tug assist, and mooring. They are not standalone assessment targets.
    - Interfacing systems. A small number of private terminal and third-party systems appear in the framework because they directly enable public terminal workflows. For example, Lynx driver registration (2b.5.1) provisions the driver and carrier credentials that public terminal gate and appointment operations depend on, and private liquid bulk transfer (2a.5.2) is included only as a reference boundary because it shares the same channel, security district, and vessel scheduling context. These interfacing systems are in scope only where they bridge into or support the public terminal complex, not as standalone assessment targets. Their assessment is the responsibility of their owners, and the method requires no access to any organization's internal systems. The operational purpose of driver registration is throughput: pre-validating driver and carrier identity before arrival shortens the gate transaction and reduces the time trucks spend queued at the terminal boundary.

2. Gap Assessment and Problem Statement

2.1 The Core Problem

Port operations can be understood as systems of systems involving many organizations, but cyber-risk assessments are often stovepiped within both systems and stakeholders.

A modern port is a dense mesh of digital, operational technology, and industrial control systems operated by terminal operators, the port authority, carriers, customs and regulators, vendors, and service providers. Each organization sees part of the picture. No single stakeholder is likely to have a complete view of how a cyber event in one system could cascade into delays, safety concerns, cargo-release problems, or recovery decisions for others.

The deeper problem is organizational as well as technical: stakeholders need a shared way to see dependencies, agree on priorities, assign ownership, and sustain action over time.

2.2 Why Current Approaches Fall Short

- Frameworks describe cyber practices, not port consequences. The NIST Cybersecurity Framework (CSF) 2.0 and MITRE ATT&CK are valuable tools [4], [5]. By themselves, they may not show which local port operations would be most affected if a system, data exchange, or manual workaround failed.
- Vulnerability findings outpace the ability to prioritize. Scanning and penetration testing can identify many weaknesses. An operations-based view helps decide which findings matter most and can make future testing more focused on the systems and data exchanges that support critical port operations.
- Cross-stakeholder dependencies are difficult to see in full. Because port operations cross both systems and organizations, the dependencies that most drive risk may sit at the boundaries between stakeholders rather than within one stakeholder's field of view.
- No shared mechanism turns findings into funded work. Even good analysis can stall unless stakeholders validate it, agree on ownership, and convert it into prioritized cybersecurity requirements, investment decisions, and follow-up actions.

The method in Section 3 addresses these gaps by building the operation-to-system map before an incident occurs, so impact can be traced in both directions: from a compromised system forward to the operations it supports, and from a degraded operation back to its candidate systems and owners.

2.3 The Regulatory Clock

The gap is time-bound. The U.S. Coast Guard's Cybersecurity in the Marine Transportation System final rule was published in the Federal Register on January 17, 2025, and became effective on July 16, 2025 [3]. The rule sits within the broader Maritime Transportation Security Act (MTSA) regulatory structure in 33 C.F.R. Parts 101-106 and establishes cybersecurity requirements for regulated entities in the marine transportation system [3], [6].

Compliance is required, but compliance alone does not tell port leaders where to invest first or how to coordinate action across stakeholders. This paper addresses that coordination and prioritization problem: how can a port identify the systems, data exchanges, stakeholders, and workarounds that matter most to operations, then use that knowledge to support capital decisions, cybersecurity requirements, continuity planning, and required Coast Guard documentation?

3. Topic Discussion

3.1 Mission-Based Cyber Risk Assessment as the Foundation

Mission-Based Cyber Risk Assessment (MBCRA) is a Department of Defense (DoD) approach for assessing cyber risk to mission-critical systems, as reflected in the DoD Cyber Table Top Guide and the Cyber Developmental Test and Evaluation Guidebook [1], [2]. Its logic is simple: start with the mission, identify the systems and data the mission depends on, ask what happens if they are compromised, and rank the results by mission impact [1], [2].

The same logic can be adapted to civilian critical infrastructure. In this paper, the word operation replaces mission. The method asks how port operations such as container ship movement, container discharge, gate processing, and emergency response depend on systems and data, and what would happen if confidentiality, integrity, or availability were lost. In the terms of the project proposal, the Operations Engineering Thread developed in this paper is the mission thread artifact, and the Systems Repository with its dependency matrix is the system dependency map.

3.2 Method Overview: Four Phases

The assessment works through four sequential phases. The framework bounds the analysis. The threads sequence and choreograph it. The repository operationalizes it. The impact assessment prioritizes it.

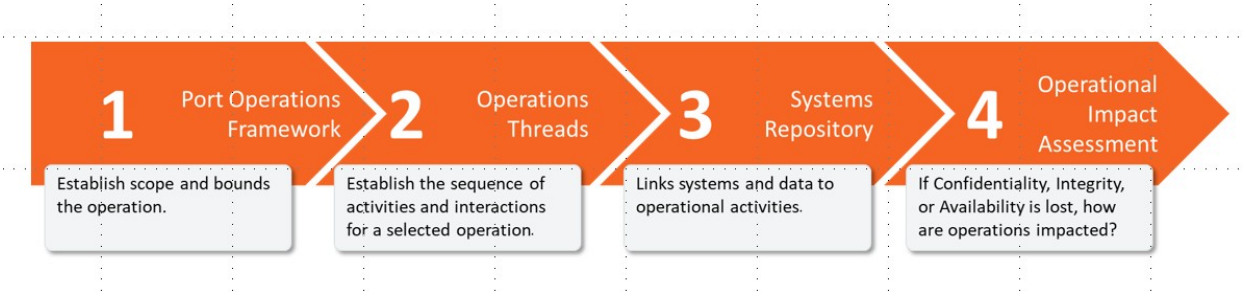

Figure 1. The four-phase method of the port operations cyber risk assessment.

3.3 Phase 1 — The Port Operations Framework

The Port Operations Framework is a plain-language breakdown of port operations. It uses American Productivity & Quality Center (APQC) Process Classification Framework conventions and is aligned with the MTSA-regulated environment [7]. It decomposes port activity across four levels: Domain, Process Group, Process, and Activity.

A. The Three Domains

Three Level 1 domains cover the operational surface of the port. Services to Ships and Services to Cargo are the two primary flows, while Integration, Safety, and Security is the connective domain that coordinates and secures both. The framework describes the full port operational surface. The proof-of-concept analysis in Sections 3.4 through 3.7 applies only to the container ship scope defined in Section 1.4.

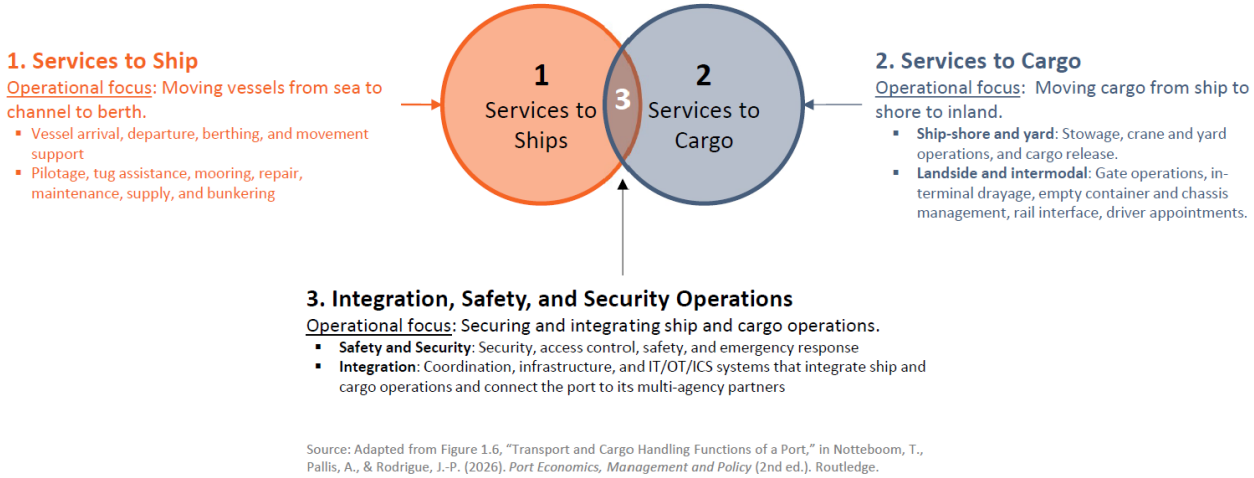

Figure 2. The three domains of the Port Operations Framework, adapted from Notteboom, Pallis, and Rodrigue [8].

1. Services to Ships. Moving vessels from sea to channel to berth, including pre-arrival notification and clearance, pilot boarding and channel transit, tug and line-handler coordination, berthing and mooring, at-berth services, departure, and vessel traffic management.
2. Services to Cargo. Moving cargo from ship to shore to inland, including ship-to-shore and yard operations and landside/intermodal activities such as gate operations, drayage, rail interface, empty-container management, and driver access and appointments.
3. Integration, Safety, and Security. Securing and integrating ship and cargo operations, including port-wide coordination, safety, environmental and emergency response, security and access control, and infrastructure, utility, and information and communications technology (ICT) operations.

At Level 2, each domain decomposes into the process groups shown below. This is the framework map; the full Level 3 process detail for all three domains is provided in Appendix B.

Figure 3. Domain 1 — Services to Ships (Level 2 process groups).

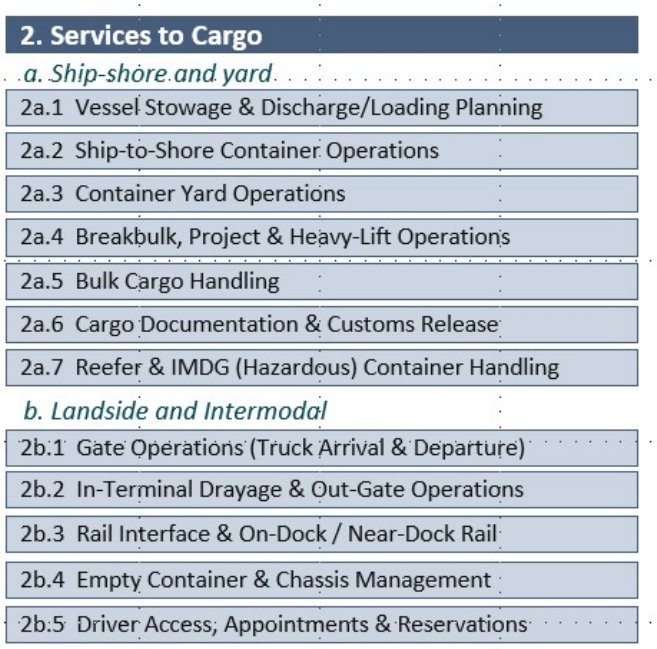

Figure 4. Domain 2 — Services to Cargo (Level 2 process groups).

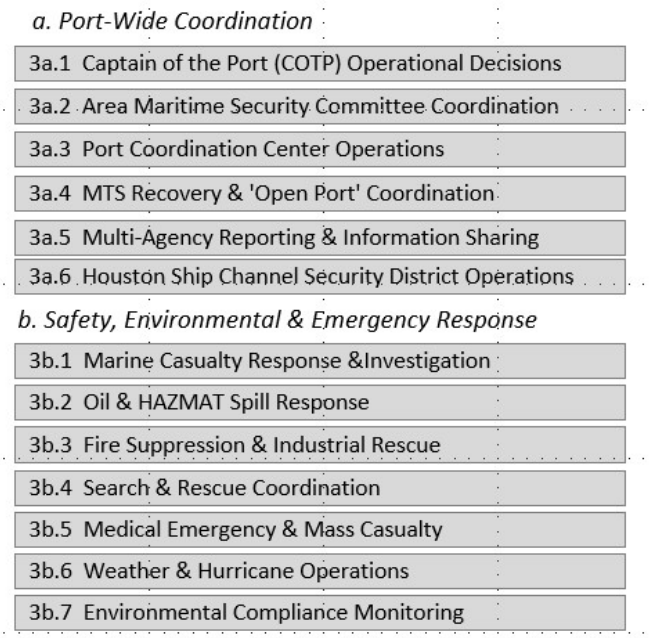

Figure 5. Domain 3 — Integration, Safety, and Security: Port-Wide Coordination and Emergency Response (Level 2 process groups).

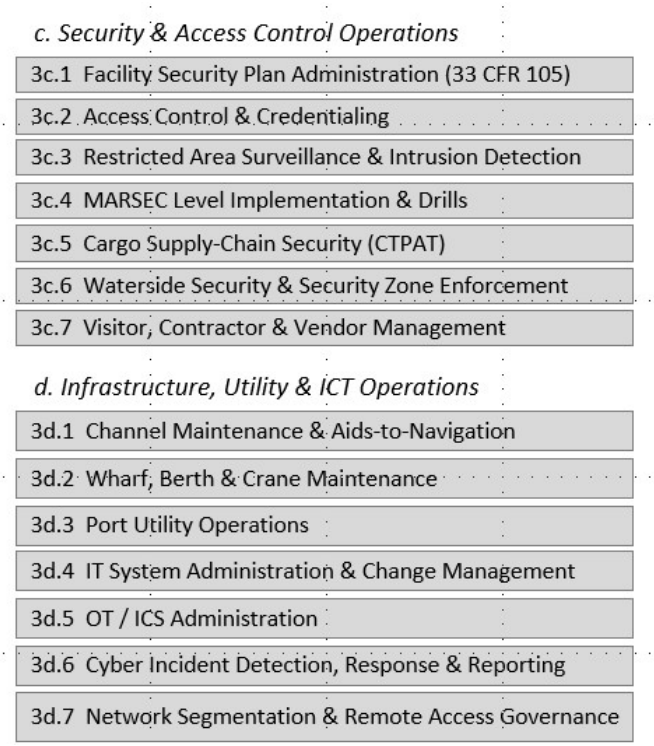

Figure 6. Domain 3 — Integration, Safety, and Security: Security & Access Control and Infrastructure, Utility & Information and Communications Technology (ICT) (Level 2 process groups).

The framework serves two purposes. It bounds the analysis, and it provides a common vocabulary that operators, security staff, and IT and OT staff can all recognize.

3.4 Selecting an Operation for the Proof of Concept

The framework covers the full port operating environment, but a proof of concept must start with one operation. The selection matrix is a first-stage screen for choosing that operation, not a final cyber-risk score. A later Port CTT Exercise would develop specific disruption scenarios for the selected operation and consider operational impact, local likelihood, known weaknesses, cyber exposure, and the limits of manual workarounds. The screen deliberately uses only the two criteria that can be judged from structural information before stakeholder engagement. The remaining factors enter at the Port CTT Exercise because that is where their evidence exists.

- **Operational criticality.** The consequence if the operation is degraded or lost, including whether manual workarounds can keep the work moving**.**
- **Stakeholder and system complexity.** The number of organizations, systems, data exchanges, and handoffs involved. An operation that crosses many boundaries is a better test of the method.

An operation that scores high on both operational criticality and stakeholder/system complexity is a strong proof-of-concept candidate because it is important to the port community and complex enough to reveal cross-stakeholder cyber dependencies. Container throughput was selected as that candidate.

Candidate operation (Services to Cargo)	Operational criticality	Stakeholder/system complexity
Container throughput — selected	High	High
Gate operations (truck arrival & departure, TWIC, OCR)	High	Medium
Cargo documentation & customs release (ACE, holds, pin issuance)	High	Medium
Vessel stowage & discharge/load planning (BAPLIE / EDI)	Medium	Medium
Reefer & IMDG (hazardous) container handling	High	Low
Rail interface & on-dock / near-dock rail	Medium	Medium
Empty container & chassis management	Low	Medium

Why container throughput was selected. Container throughput scores high on both criteria in the screening table. It spans the ship-to-gate chain: discharge from the container ship, yard placement, documentation and customs release, driver access, gate processing, and out-gate release. It also involves multiple systems and stakeholders, including the Terminal Operating System (TOS), optical character recognition (OCR), customs-release interfaces, Transportation Worker Identification Credential (TWIC) verification, appointment systems, terminal operators, U.S. Customs and Border Protection, drayage drivers, and Port Houston. At vessel arrival, the thread also touches the port-wide shared information layer: the common vessel-traffic picture maintained through the Coast Guard Vessel Traffic Service and the Marine Exchange of Texas, which feeds vessel movement, pilot, and scheduling information to many operations at once. Because that layer serves the whole channel, its disruption would cascade beyond any one terminal, and it is flagged as a candidate shared dependency for Port CTT Exercise validation. Manual fallbacks may be limited during peak periods, which can quickly create queuing, demurrage, and supply-chain backup; this is an operational judgment offered for confirmation through Port CTT Exercise review.

3.5 Phase 2 — Operations Threads and Operations Engineering Threads

With the scope bounded and an operation selected, the method decomposes that operation in two layers.

- **Operations Thread.** A sequence of activities, drawn from the framework, that together accomplish a defined operational outcome.
- **Operations Engineering Thread (OET).** A deeper decomposition of an Operations Thread, modeled at the activity level using business-process notation to show tasks, decisions, swim lanes, and data exchanges.

Together the two layers answer a single question: what does this operation look like in practice, step by step, and where does it interact with systems and data? The Operations Thread names the sequence; the OET shows the choreography.

Worked example. This paper presents a six-activity OET for container-handling throughput, covering ship-to-shore discharge, yard placement, documentation, driver and appointment

management, gate processing, and out-gate release. It should be read as the paper's worked example rather than as a fully validated enterprise representation.

The thread's success conditions are explicit. The operation succeeds when the vessel is worked within its scheduled window, containers are discharged and loaded accurately, cargo is released only with proper clearance, gate flow keeps pace with yard operations, and no safety events occur. The decision points in the OET, detailed in Appendix C, mark where these conditions come under threat and who acts to protect them.

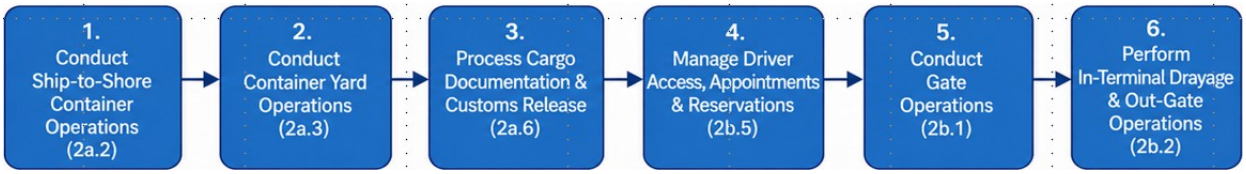

Figure 7. Container handling throughput Operations Engineering Thread (OET). Additional framework details are included in Appendix B, and extended thread details are in Appendix C.

3.6 Phase 3 — The Port Operations Systems Repository

The Systems Repository links each activity in the Operations Thread and OET to the systems and data that make the activity work. In the public report, the repository uses system capability categories rather than sensitive product-level detail. Each category describes a function the operation needs, such as recording a movement, tracking a location, verifying an identity, exchanging regulatory data, scheduling a truck, or processing a gate transaction.

The repository is the bridge between the operational view and the cyber-risk view. It shows how a cyber event could affect an activity, a decision, a handoff, or a stakeholder. It also aligns conceptually with the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Buy-Ship-Pay reference model, which describes common trade, transport, and regulatory information exchanges in international supply chains [9].

Worked example. For the container handling throughput OET, this paper identifies seven initial system capability categories. They are listed below as straw-man categories for stakeholder review.

B. Container movement & inventory record-keeping

- **Includes:** recording each container movement and maintaining the authoritative inventory of what is where.
- **Systems:** Terminal Operating System (TOS); TOS yard module; TOS dispatch.

C. Equipment & asset position tracking

- **Includes:** sensing and tracking the position of handling equipment and containers in the yard.
- **Systems:** yard equipment positioning; container location tracking.

D. Automated identification & capture

- **Includes:** reading container, chassis, and equipment identifiers automatically at operational boundaries.
- **Systems:** crane optical character recognition (OCR); gate OCR / license-plate recognition (LPR) capture.

E. Regulatory & customs data exchange

- **Includes:** exchanging manifest, hold, and release data with customs and regulatory authorities.
- **Systems:** U.S. Customs and Border Protection (CBP) Automated Commercial Environment (ACE); release / documentation interface.

F. Identity & access verification

- **Includes:** confirming that people and carriers presenting at the boundary are authorized.
- **Systems:** Transportation Worker Identification Credential (TWIC) readers; access control system.

G. Appointment & scheduling coordination

- **Includes:** sequencing truck arrivals and reservations against terminal capacity.
- **Systems:** appointment system; driver / Standard Carrier Alpha Code (SCAC) registration portal.

H. Gate & transaction processing

- **Includes:** executing the gate transaction and completing out-gate release.
- **Systems:** gate operating system; out-gate transaction system.

Matrix. Rows are the seven system capability categories (A through G); columns are the six OET activities from Figure 3-7 (1 through 6, shown here in shortened form). A check mark indicates that a system category supports that OET activity.

System category	1. Conduct Ship-to-Shore	2. Conduct Yard Ops	3. Process Documentation	4. Manage Driver Access	5. Conduct Gate Ops	6. Perform In-Terminal Drayage & Out-Gate Operations
A. Container movement & inventory record-keeping	✓	✓				✓
B. Equipment & asset position tracking	✓	✓				
C. Automated identification & capture	✓				✓	
D. Regulatory & customs data exchange			✓			
E. Identity & access verification				✓	✓	
F. Appointment & scheduling coordination				✓		
G. Gate & transaction processing					✓	✓

The matrix shows where cyber dependency concentrates. Container movement and inventory record-keeping support discharge, yard, and out-gate activities, so it rises in priority. Other categories may touch fewer activities but still control critical decisions, such as legal cargo release or physical gate access. The Navis N4 example used to illustrate the terminal-operating-system category in Appendix B (3d.4.2) is supported by CISA's 2025 industrial control systems advisory on the Kaleris Navis N4 Terminal Operating System [10]. The gate, OCR, and access-control detail in this repository draws on documentation rather than direct confirmation. Where entries reference CBP's ACE processes or Port Houston gate systems, the relevant system owners should confirm those details before the repository is used operationally.

3.7 Phase 4 — The Operational Impact Assessment

The final component applies a confidentiality, integrity, and availability lens to every system capability category in the repository and asks what the loss of each property would do to operations.

Loss type	What it means and an illustrative consequence
Confidentiality	**An adversary reads data they should not see.** Impact ranges from negligible to enabling a targeted physical or cyber-physical attack. Example: leaked container ship transit timing and berth assignments enabling adversary positioning.
Integrity	**An adversary alters or fabricates data**. Often the most severe, because operations proceed on falsified information with safety, regulatory, and commercial consequences. Example: falsified manifest data leading to a misrouted hazardous container.
Availability	**Data or systems are denied for a period**. Impact depends on duration, alternatives, and operational tempo. Example: loss of container movement record-keeping during peak gate operations causing truck queuing, demurrage, and supply-chain backup.

Each lens is applied to every system capability category by asking a concrete operational question: if this capability were compromised, what would happen to the operation that depends on it? The output is a preliminary ranking of system capability categories by operational impact, to be refined through Port CTT Exercise review using local knowledge and stakeholder judgment.

At that review, each loss type is evaluated against four explicit consequence dimensions rather than left implied: safety impact, regulatory impact, recoverability, and detectability. These dimensions matter especially for operational technology and industrial control systems, where the consequence of a loss is measured in physical and regulatory terms as much as in data terms.

Worked example. The table below applies the lens to four system capability categories from Section 3.6. It is illustrative, not exhaustive. It shows which type of loss is most important for each category.

Categories B, F, and G require local operational evidence that only stakeholder review can supply and will be completed during the stakeholder Port CTT Exercise. Until then, the table is a worked demonstration, not a complete ranking.

System capability category	Confidentiality loss	Integrity loss	Availability loss
A. Container movement & inventory record-keeping	Low. Exposed stow and yard data is commercially sensitive but not operationally disabling.	High. Falsified movement or location records send yard decisions down a degraded branch on bad data.	High. An outage at peak tempo stops discharge and yard work, cascading into vessel and gate delays.
C. Automated identification & capture	Low. Identifier reads are not sensitive in isolation.	High. A wrong or spoofed read misidentifies a container, corrupting the movement record at its source.	Medium. Loss falls back to manual keying, slower and error-prone but not a full stop.
D. Regulatory & customs data exchange	Medium. Manifest and release data has security value if disclosed.	High. A falsified release status lets held cargo move or wrongly stops released cargo.	Medium. Short outages can be buffered; sustained loss halts customs release.
E. Identity & access verification	Low. Credential data is protected but disclosure is not the primary concern.	High. A spoofed or altered credential admits an unauthorized person or vehicle.	Medium. Loss forces manual escort and identity checks, slowing but not stopping the gate.

In this illustrative assessment, integrity appears to be the dominant concern for several categories because container throughput proceeds on recorded movements, locations, and release decisions. On that logic, falsified data may be more consequential than either disclosure or a bounded outage in some categories. Availability remains a close second where a capability has no rapid manual fallback at peak tempo.

I. Preliminary Identification of Critical Capability Categories

The preliminary ranking rests on two questions: how many activities depend on the same capability (dependency centrality), and how much damage the operation suffers when that capability is lost (operational consequence). It is a starting point for Port CTT Exercise review, not a final risk score.

Priority	System capability category	Why it ranks here
1	A. Container movement & inventory record-keeping	Highest centrality (three activities) and High on both integrity and availability. The operation's authoritative record; a compromise degrades every downstream decision.
2	D. Regulatory & customs data exchange	Gates legal release. High integrity consequence: a falsified release status has safety, regulatory, and commercial effects even though it touches one activity.
3	E. Identity & access verification	Gates physical entry across two activities. High integrity consequence: a bad credential admits an unauthorized person or vehicle.
4	C. Automated identification & capture	Feeds the movement record at its source across two activities. High integrity consequence, with a manual fallback that limits availability impact.

This preliminary ranking can help stakeholders focus early review, but it should be refined by mapping actual local systems, testing assumptions in a Port CTT Exercise, and converting the results into prioritized cybersecurity requirements.

4. Way Forward

This proof of concept should be treated as a starting point for sustained stakeholder action. It gives the Port CTT Exercise a concrete set of straw-man artifacts to review instead of forcing stakeholders to start from a blank page.

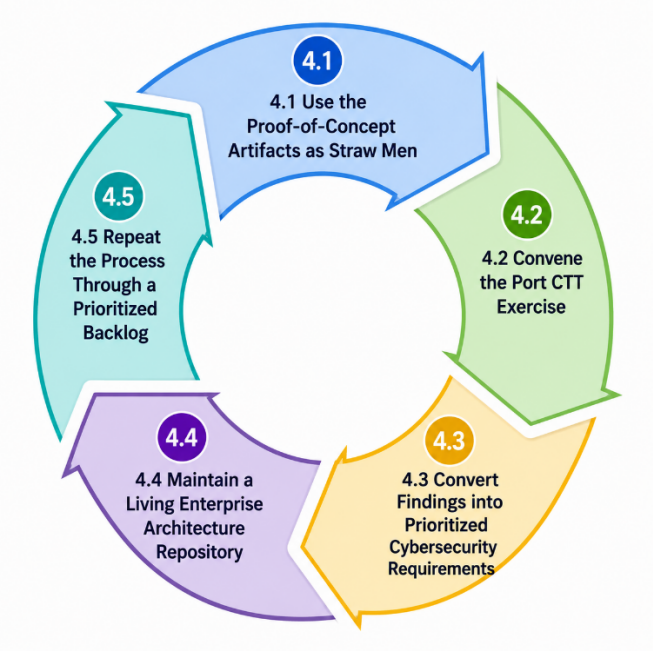

Figure 8. How to Implement Report Artifacts.

4.1 Use the Proof-of-Concept Artifacts as Straw Men

The report provides four starting artifacts: the Port Operations Framework, the container handling throughput Operations Engineering Thread, the Systems Repository, and a preliminary impact ranking. These artifacts should be validated, corrected, and adopted by the organizations that own, operate, secure, regulate, or depend on the selected operation.

The immediate value is speed. A straw-man framework lets stakeholders react to something concrete, identify missing handoffs, correct assumptions, and agree on what should be analyzed next.

4.2 Convene the Port CTT Exercise

The Port CTT Exercise is the recurring forum for turning analysis into agreement and action. It combines three functions in a single recurring event: a validation workshop that confirms the artifacts, a tabletop scenario exercise that walks through the disruption, and a decision forum that converts findings into owned, tracked actions. It should have a clear sponsor, a neutral facilitator, a decision process, and an action-tracking process so findings can be resourced and implemented. Appendix E summarizes the exercise roles, who fills them, and what each can access. The facilitator runs the exercise itself: keeps the walk-through moving, holds the discussion at the capability level, and stays neutral among the organizations in the room. The facilitator also serves as the sponsor's point of contact for exercise operations, and should be a third party or staff without a direct stake in the operation under review. Participants should include the relevant operations, security, IT, OT, terminal, regulatory, vendor, and external partner representatives for the operation being examined.

Depending on the operation, external partners may include the Coast Guard / Captain of the Port, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), U.S. Customs and Border Protection, the Texas Cyber Command, state and local emergency-management or law-enforcement partners, the Houston Pilots, the Marine Exchange, carriers, and critical vendors.

For each selected operation, participants first confirm or revise the Operations Thread, the Operations Engineering Thread, and the Systems Repository. They then walk through a realistic disruption and answer practical questions: What system or data is affected? What happens if it is wrong, unavailable, or exposed? What workaround exists? How long can the workaround hold? Who notices first? What is the safety consequence? What regulatory obligation is triggered? How long would recovery take? Who decides whether to continue, slow, stop, or escalate?

The proof of concept identifies likely operational consequences. The Port CTT Exercise adds local evidence: known weaknesses, prior incidents, vendor dependencies, remote-access paths, and the time available before manual workarounds fail. That local judgment turns the straw-man ranking into a stakeholder-owned risk picture.

The Port CTT Exercise deliberately stops at the capability level. Its job is to establish which system capabilities each operation depends on, what losing them costs, and where the weak

points sit, including at the interfaces between organizations. Finding the detailed attack paths behind those weak points is a different job with a different owner. Each organization conducts that analysis on its own systems, inside its own boundary, using its own architecture documentation. No participant requires, or is granted, access to another organization's systems at any point in the method. For MTSA-regulated facilities, this is not new work. The Coast Guard rule already requires each facility to complete its own Cybersecurity Assessment [3]. The Port CTT Exercise makes that mandated assessment better targeted, because each facility leaves the exercise knowing which of its capabilities matter most to the operations it serves, and can focus its detailed analysis there first.

In practice, many organizations do not have current architecture documentation at the depth this analysis requires. Where that is true, the first task is to build it. Because the analysis looks for weaknesses in systems the organization depends on, it calls for an objective set of eyes: an analyst with the engineering skill to do the work, no stake in the systems under review or in the findings, and confidentiality obligations that run to the owning organization. Review by the vendors or integrators who built or maintain a system is not a substitute for independent analysis. Each organization selects and engages this support under its own agreement and control.

Two kinds of findings then follow two different paths. Weaknesses inside one organization go into that organization's own assessment and remediation planning, and only sanitized status returns to the group: the capability is confirmed at risk, remediation is funded, the fix is in place. Weaknesses at the interfaces between organizations, such as the shared vessel-traffic picture maintained through the Coast Guard Vessel Traffic Service and the Marine Exchange, or a data exchange that no single facility's assessment covers, remain with the Port CTT Exercise as shared findings, worked jointly by the parties on each side. In both cases, product-level detail stays where it lives. The shared record advances at the level of capabilities and interfaces.

4.3 Convert Findings into Prioritized Cybersecurity Requirements

Port CTT Exercise findings should be converted into a prioritized backlog of cybersecurity requirements. Each requirement should identify the affected operation, the system or data dependency, the stakeholder owner, the recommended action, the urgency, and the expected operational benefit.

Each requirement should also travel with the operational context that produced it: the thread, the scenario, and the consequence. The participant from the owning organization serves as the point of contact, so the people implementing the fix can trace its intent and ask questions (Appendix E). Whether a fix closes the finding is verified at a later Port CTT Exercise, by walking the scenario again against the fix.

Requirements should be sequenced economically rather than by severity score alone: each requirement is ranked by the cost of delaying it relative to the effort to implement it, with cost of delay scored from the operational impact findings of the assessment, the regulatory deadline, and the requirement's effect on cascade interruption and recovery. Appendix D describes the provenance and mechanics of this method. Regulatory-mandated requirements should be funded within a protected allocation so that inexpensive discretionary work never displaces mandated or foundational work merely because it is cheaper.

That backlog can support capital planning, Coast Guard cybersecurity assessment and planning documentation, incident-response playbooks, continuity planning, vendor and remote-access governance, and focused penetration testing. It can also guide coordination with CISA, the FBI, U.S. Customs and Border Protection, the Texas Cyber Command, state and local emergency-management or law-enforcement partners, the Houston Pilots, the Marine Exchange, carriers, and critical vendors when those stakeholders are relevant to the operation.

4.4 Maintain a Living Enterprise Architecture Repository

A one-time assessment ages quickly. Validated Port CTT Exercise results should be maintained in a practical Enterprise Architecture repository: a living, searchable map of how port operations, systems, data exchanges, vendors, stakeholders, and manual workarounds connect. This repository is not a collection of static diagrams. It is the shared record that lets the port community see the systems-of-systems view across organizational boundaries. It is an architecture of the shared operation, not of any participant's enterprise. Each organization's detailed system documentation stays inside its own boundary; the repository holds the capability-level view and the interfaces between organizations. The repository is the responsibility of a repository steward named by the Port CTT Exercise sponsor. Keeping it current is skilled work: the record must stay structured and searchable so it can answer the questions above, and the sponsor may engage a qualified architect to maintain it (Appendix E). The maintainer works only

with what participants report and needs no access to any organization's systems. Updates follow the exercise cadence, and each participating organization's representation is refreshed only through the sanitized status it reports. No organization maintains another's content.

Maintained over time, the repository helps leaders answer practical questions: Which operations depend on a given system or vendor? What is affected if a data exchange fails? Where are manual workarounds thin? Which cybersecurity requirements are already funded, assigned, or still open? This approach is consistent with NIST guidance on organization-wide risk management and enterprise-oriented cybersecurity governance [4], [11].

4.5 Repeat the Process Through a Prioritized Backlog

Container handling throughput is only one of many potential port operations. The Port CTT Exercise should maintain a stakeholder-approved backlog of operations to assess next, using factors such as operational criticality, stakeholder concern, regulatory urgency, known incidents, and system/data dependency. Each new exercise updates the Enterprise Architecture repository and produces new cybersecurity requirements. Re-scoring the backlog on the port's natural rhythm, after each Port CTT Exercise and at each budget cycle, keeps it a decision tool rather than a document.

Over time, the port community builds a durable capability: a shared way to understand cyber risk in operational terms, choose what to fix first, track action to completion, and keep port operations resilient beyond the compliance horizon established by the Coast Guard rule [3].

Appendix A. How the Framework Was Developed

The Port Operations Framework uses APQC Process Classification Framework structural conventions [7], populated from authoritative port operations sources. The APQC PCF is a widely used cross-industry standard for decomposing operations into a hierarchical taxonomy. The framework was populated from an evolving catalog of documents ingested across six source categories.

- **Port Houston operational documents.** Port authority tariffs, terminal security and access procedures, crane and trucker references, pilotage rules and guidance, Houston Ship Channel Security District materials, and Greater Houston Port Bureau resources.
- **Federal regulation and guidance.** Relevant subparts of 33 CFR governing maritime security and vessel traffic management; USCG cybersecurity rules and navigation and vessel inspection circulars; CTPAT and TWIC documentation; CISA, NIST, and GAO resources on maritime and operational-technology security; and DoD mission engineering guidance.
- **International standards.** Maritime security and maritime cyber-risk sources, including IMO maritime cyber risk guidance [13] and IAPH port cybersecurity guidelines [14].
- **Industry doctrine and academic texts.** AAPA professional-manager curriculum, ASCE port planning proceedings, academic container-terminal operations literature [12], and standard port management textbooks [8].
- **Comparable U.S. ports.** Operational and security references from peer ports including Virginia, Los Angeles/Long Beach, and New York/New Jersey.
- **Project-internal references.** The originating project proposal establishing the Operations Thread and Operations Engineering Thread vocabulary, and a recent study on cascading failures in critical-infrastructure networks informing the resilience framing.

Appendix B. Port Operations Framework — Level 3 Detail

The following pages present the Level 3 process detail for all three domains. Level 1 and Level 2 elements are shown as headers; the bulleted entries beneath each Level 2 process are its Level 3 processes.

J. B.1 Domain 1 — Services to Ships

Domain 1 entries describe port-wide vessel services. Only those supporting container ship calls are within the proof-of-concept scope defined in Section 1.4.

1.1 Pre-Arrival Notification & Clearance
- 1.1.1 Notice of Arrival / Departure (NOAD) Submission
- 1.1.2 USCG Boarding Risk Assessment
- 1.1.3 CBP Vessel Entry Processing
- 1.1.4 Agent-Port Authority ETA Coordination

1.2 Pilot Boarding & Channel Transit
- 1.2.1 Pilot Dispatch & Boarding at Galveston Bar
- 1.2.2 Bridge Resource Management During Transit
- 1.2.3 VHF Communications with Sector & VTS
- 1.2.4 Restricted Visibility & Weather Transit Protocols

1.3 Tug & Line-Handler Coordination
- 1.3.1 Tug Order & Assignment
- 1.3.2 Line Handler Scheduling
- 1.3.3 Tug-Pilot Maneuvering Coordination

1.4 Berthing & Mooring
- 1.4.1 Berth Allocation & Window Confirmation
- 1.4.2 Mooring Operations & Equipment Inspection
- 1.4.3 Declaration of Security (DoS) Execution
- 1.4.4 First Lines Ashore / All Fast Reporting

1.5 At-Berth Vessel Services
- 1.5.1 Bunkering Coordination
- 1.5.2 Garbage & Slops Reception
- 1.5.3 Ship Chandlering & Stores Loading
- 1.5.4 Crew Shore-Leave Access

1.6 Departure & Outbound Transit

- 1.6.1 Sailing Approval & Stores/Crew Clearance
- 1.6.2 Outbound Channel Transit
- 1.6.3 Pilot Disembark at Sea Buoy

1.7 Vessel Traffic Management & Channel Conditions

- 1.7.1 VTS Traffic Coordination & Advisories
- 1.7.2 AIS-Based Position Monitoring
- 1.7.3 Movement Restriction Decisions
- 1.7.4 Channel Closure & Reopening

K. B.2 Domain 2 — Services to Cargo (Ship-Shore and Yard)

2a.1 Vessel Stowage & Discharge/Loading Planning

- 2a.1.1 BAPLIE / EDI Stowage Plan Exchange
- 2a.1.2 Discharge & Load Sequencing
- 2a.1.3 Stevedore Crew & Shift Assignment

2a.2 Ship-to-Shore Container Operations

- 2a.2.1 STS Crane Discharge Operations
- 2a.2.2 STS Crane Loading Operations
- 2a.2.3 Twin-Lift / Tandem-Lift Operations
- 2a.2.4 Crane OCR Container ID & Damage Capture

2a.3 Container Yard Operations

- 2a.3.1 RTG / Yard Crane Stacking Operations
- 2a.3.2 Yard Tractor / UTR Horizontal Transport
- 2a.3.3 Yard Block Allocation & Stack Planning
- 2a.3.4 Container Position Inventory & Audit

2a.4 Breakbulk, Project & Heavy-Lift Operations

- 2a.4.1 Breakbulk Discharge & Marshalling at Turning Basin
- 2a.4.2 Project Cargo Rigging & Heavy-Lift
- 2a.4.3 RORO Cargo Operations

2a.5 Bulk Cargo Handling

- 2a.5.1 Dry Bulk Conveyor & Hopper Operations
- 2a.5.2 Liquid Bulk Transfer (Private Terminals — Reference)
- 2a.5.3 Bulk Sampling & Survey

2a.6 Cargo Documentation & Customs Release

- 2a.6.1 ACE Vessel Manifest Submission
- 2a.6.2 Hold / Exam Coordination
- 2a.6.3 Release Verification & Pin Issuance

2a.7 Reefer & International Maritime Dangerous Goods (IMDG) Container Handling

- 2a.7.1 Reefer Plug-In, Monitoring & Alarm Response
- 2a.7.2 International Maritime Dangerous Goods (IMDG) Stowage & Segregation
- 2a.7.3 HazMat Notification & COTP Approvals

L. B.3 Domain 2 — Services to Cargo (Landside and Intermodal)

2b.1 Gate Operations (Truck Arrival & Departure)

- 2b.1.1 Pre-Gate Appointment Validation
- 2b.1.2 TWIC & Driver Identity Verification
- 2b.1.3 Container & Chassis OCR Capture
- 2b.1.4 Truck Routing to Yard Block

2b.2 In-Terminal Drayage & Out-Gate Operations

- 2b.2.1 Live Load / Drop & Hook Coordination
- 2b.2.2 Out-Gate Inspection & Release

2b.3 Rail Interface & On-Dock / Near-Dock Rail

- 2b.3.1 Rail Car Inventory & Position Mgmt
- 2b.3.2 Intermodal Rail Loading/Unloading

2b.4 Empty Container & Chassis Management

- 2b.4.1 Empty Container Returns & Stack Management
- 2b.4.2 Chassis Pool Operations & M&R Status

2b.5 Driver Access, Appointments & Reservations

- 2b.5.1 Lynx Driver Registration & SCAC Validation
- 2b.5.2 Appointment Slot Allocation

M. B.4 Domain 3 — Integration, Safety, and Security (Port-Wide Coordination)

3a.1 Captain of the Port (COTP) Operational Decisions

- 3a.1.1 Port Condition / MARSEC Authority Decisions
- 3a.1.2 Movement Authorizations & Restrictions
- 3a.1.3 DoD / Naval Vessel Coordination

3a.2 Area Maritime Security Committee Coordination

- 3a.2.1 AMSC Meetings & Subcommittee Work
- 3a.2.2 Area Maritime Security Plan (AMSP) Updates
- 3a.2.3 Maritime Security Information Sharing

3a.3 Port Coordination Center Operations

- 3a.3.1 PCC Watch-Stander Operations

- 3a.3.2 Common Operating Picture Maintenance

3a.4 MTS Recovery & 'Open Port' Coordination
- 3a.4.1 Incident Action Plan Development (NIMS/ICS)
- 3a.4.2 MTS Recovery Unit Activation
- 3a.4.3 Salvage & Wreck Removal Coordination

3a.5 Multi-Agency Reporting & Information Sharing
- 3a.5.1 Cyber Incident Reporting (FBI / CISA / COTP)
- 3a.5.2 Suspicious Activity & BOS Reporting
- 3a.5.3 Texas Cyber Command Coordination
- 3a.5.4 USCG Sector Watch Updates

3a.6 Houston Ship Channel Security District Operations
- 3a.6.1 HSCSD Funded Security Initiatives
- 3a.6.2 Joint Patrols & Threat Detection

N. B.5 Domain 3 — Integration, Safety, and Security (Safety, Environmental & Emergency Response)

3b.1 Marine Casualty Response & Investigation
- 3b.1.1 Allision / Collision Initial Response
- 3b.1.2 Vessel Grounding Response
- 3b.1.3 Marine Casualty Investigation

3b.2 Oil & HAZMAT Spill Response
- 3b.2.1 NRC Notification & FOSC Activation
- 3b.2.2 Area Contingency Plan Activation
- 3b.2.3 OSRO Mobilization & Boom Deployment
- 3b.2.4 Damage Assessment & Trustee Coordination

3b.3 Fire Suppression & Industrial Rescue
- 3b.3.1 Shipboard Fire Response
- 3b.3.2 Wharf / Cargo Fire Response
- 3b.3.3 Industrial / Confined-Space Rescue

3b.4 Search & Rescue Coordination
- 3b.4.1 Person-in-Water Response
- 3b.4.2 Vessel Distress Response

3b.5 Medical Emergency & Mass Casualty
- 3b.5.1 EMS Dispatch to Vessel / Terminal
- 3b.5.2 Mass Casualty Coordination

3b.6 Weather & Hurricane Operations
- 3b.6.1 Port Condition Setting (Whiskey/X-Ray/Yankee/Zulu)

- 3b.6.2 Pre-Storm Vessel Sortie
- 3b.6.3 Terminal Equipment Securing
- 3b.6.4 Post-Storm Channel Survey & Reopening

3b.7 Environmental Compliance Monitoring
- 3b.7.1 Air Emissions Monitoring
- 3b.7.2 Ballast Water Management Verification
- 3b.7.3 Stormwater & Wastewater Discharge

O. B.6 Domain 3 — Integration, Safety, and Security (Security & Access Control Operations)

3c.1 Facility Security Plan Administration (33 CFR 105)
- 3c.1.1 FSP Development, Approval, & 5-Year Renewal
- 3c.1.2 Facility Security Assessment (FSA) Updates
- 3c.1.3 PFSO Recordkeeping & Compliance Audits

3c.2 Access Control & Credentialing
- 3c.2.1 TWIC Reader Operations at Facility Boundary
- 3c.2.2 Escort Procedures for Non-TWIC Holders
- 3c.2.3 Personnel Credential Database Management

3c.3 Restricted Area Surveillance & Intrusion Detection
- 3c.3.1 CCTV / VMS Monitoring
- 3c.3.2 Perimeter Intrusion Detection
- 3c.3.3 Waterside Sensor & Patrol Coverage

3c.4 MARSEC Level Implementation & Drills
- 3c.4.1 MARSEC Level Change Implementation
- 3c.4.2 Quarterly Security Drills
- 3c.4.3 Annual Multi-Agency Security Exercises

3c.5 Cargo Supply-Chain Security (CTPAT)
- 3c.5.1 CTPAT Member Verification & Best Practices
- 3c.5.2 Container Seal Verification (ISO 17712)
- 3c.5.3 High-Risk Cargo Examination Coordination

3c.6 Waterside Security & Security Zone Enforcement
- 3c.6.1 Security Zone Enforcement (33 CFR 165.814)
- 3c.6.2 Vessel Escort / Sensitive Cargo Movements
- 3c.6.3 Naval Vessel Protection Zone Enforcement

3c.7 Visitor, Contractor & Vendor Management
- 3c.7.1 Visitor Pre-Registration & Badging
- 3c.7.2 Contractor Security Briefing

- 3c.7.3 Vehicle / Material Inspection

P. B.7 Domain 3 — Integration, Safety, and Security (Infrastructure, Utility & Information and Communications Technology Operations)

3d.1 Channel Maintenance & Aids-to-Navigation
- 3d.1.1 USACE Channel Survey & Dredging
- 3d.1.2 ATON Service & Maintenance
- 3d.1.3 Project 11 Expansion Operations

3d.2 Wharf, Berth & Crane Maintenance
- 3d.2.1 Crane Preventive Maintenance & Inspection
- 3d.2.2 Wharf Structural Inspection
- 3d.2.3 Fender & Bollard Maintenance

3d.3 Port Utility Operations
- 3d.3.1 Electrical Substation & Crane Power
- 3d.3.2 Water, Fire Loop & Wastewater
- 3d.3.3 Voice & Data Communications Infrastructure

3d.4 IT System Administration & Change Management
- 3d.4.1 Business System Administration
- 3d.4.2 TOS (Navis N4) Administration [10]
- 3d.4.3 IT Change Management Board

3d.5 OT / ICS Administration
- 3d.5.1 STS / Yard Crane Control Systems
- 3d.5.2 Gate, OCR & Access Control Systems
- 3d.5.3 Reefer Monitoring & Refrigeration ICS

3d.6 Cyber Incident Detection, Response & Reporting
- 3d.6.1 SOC / Detection Alert Triage
- 3d.6.2 Incident Response Playbook Execution
- 3d.6.3 Cyber Incident Reporting Under Cyber Rule
- 3d.6.4 USCG Cybersecurity Plan Compliance Documentation

3d.7 Network Segmentation & Remote Access Governance
- 3d.7.1 IT/OT Segmentation Verification
- 3d.7.2 Remote Vendor Access Governance (Cranes, TOS)
- 3d.7.3 Cloud Shared-Responsibility Operations

Appendix C. Extended OET Detail — Integrity Decision Points

Section 3.5 presents the container handling throughput Operations Engineering Thread (OET) as a six-activity sequence, Section 3.6 links each activity to its system categories, and Section 3.7 illustrates the confidentiality, integrity, and availability assessment. This appendix carries the worked example one level deeper, into the activity-level decision points the OET exposes. The framework structure and this thread have received an initial subject-matter sanity check and are offered for broader stakeholder validation, refinement, and use.

At the activity level, the OET exposes integrity-dependent decision points in the operation. As a container moves through discharge, yard placement, and release, the operation passes through three sequential validation questions. At each, an integrity failure, bad or falsified data, may send the operation down a degraded branch rather than stopping it outright, which is what makes integrity loss potentially consequential: operations may continue on false information.

Validation point	Question asked	Consequence of an integrity failure
Movement record	Was the movement recorded correctly?	A wrong discharge or load record means downstream decisions start from bad data.
Location record	Do we know where the box is?	A bad location record means the box cannot be found, causing yard congestion and retrieval delays.
Release status	Is the box legally released?	A bad release status means held cargo may move, or released cargo may be improperly stopped.

These three validation points map directly to system capability categories in the repository shown in Section 3.6: container movement and inventory record-keeping, equipment and asset position tracking, and regulatory and customs data exchange. They help explain why the illustrative integrity assessment in Section 3.7 ranks highly for those categories. Decomposing the operation to this level of detail lets the Operational Impact Assessment rank system capability categories by the operational consequence of an integrity loss, rather than treating them as undifferentiated entries in a control catalog.

Appendix D. Prioritization Method Provenance — Lean Portfolio Principles

The prioritization approach in Section 4.3 adapts three principles from Lean portfolio management, most visibly codified in the Scaled Agile Framework (SAFe) [15]. The port community does not need to adopt SAFe to use them. The principles predate the framework, and they are designed to work within the governance structures the port complex already has.

That last point matters, because a port complex is not a single enterprise. The Houston Ship Channel brings together a port authority, terminal operators, carriers, federal and state agencies, and private facilities, each with its own budget, its own decision process, and its own regulatory obligations. No organization directs another's cybersecurity spending, and this approach does not ask any of them to. The Port CTT Exercise produces validated priorities; each participating organization carries the requirements it owns into its own planning and budget cycle. Participation does not require any organization to expose internal system detail. The Systems Repository operates at the level of capability categories, so stakeholders can discuss shared dependencies at the interfaces between them without disclosing sensitive product-level detail. Detailed vulnerability analysis of the systems behind those capabilities remains inside each organization, as described in Section 4.2.

The Houston port community also has a long record of defending the Channel itself collectively. Channel Industries Mutual Aid has combined the firefighting, rescue, and emergency response capabilities of competing refining and petrochemical companies along the Channel since 1955 [16]. The Houston Ship Channel Security District funds shared security measures across public and private facilities [17], and the Area Maritime Security Committee provides the standing forum for port-wide security planning [6]. Organizations that compete commercially have cooperated for seven decades when the threat is to the Channel that every one of them depends on. A cyber event that interrupts a shared operation has the same character. This approach asks for nothing more than that same established habit, extended to the cyber dependencies of shared operations. No new authority is required.

In a complex where no one is in charge of everyone, change travels through advocates. The organizations that adopt validated priorities will do so because someone inside them, an operations leader, a security officer, an IT or OT manager who took part in the Port CTT

Exercise, makes the case to their own leadership in their own budget process. The purpose of the prioritization method is to arm those advocates. It replaces “we should do this because it scored high” with a case any executive can weigh: what this failure would do to operations, what waiting costs, and what acting buys. Three principles shape that case:

1. Sequence by economics. Each cybersecurity requirement is ranked by a simple question: what does it cost to wait, compared with what it takes to do? (SAFe formalizes this ratio as Weighted Shortest Job First.) The cost of waiting is not guesswork. It comes directly from the assessment: the operational consequences identified in Section 3.7, the July 2027 Coast Guard deadline and known adversary activity, and how much the requirement limits cascading disruption and speeds recovery. Scoring is comparative rather than absolute, so operational staff answer questions they can actually judge, such as “is losing gate operations worse than losing vessel scheduling?”

2. Protect the budget for work that must be done. Leadership sets aside fixed shares of the cybersecurity budget for regulatory-mandated requirements, risk-driven hardening, and resilience and recovery measures. Inexpensive discretionary work can never crowd out mandated or foundational work simply because it is easier to do.

3. Leadership sets the rules; staff sequence the work. Leadership decides the budget shares and the priorities that matter most. Security and operations staff order the work within those boundaries, re-scoring on the organization’s normal budget and assessment cycle as threats and findings change.

The SAFe citation serves the same purpose as the DoD citation in Section 3.1: it shows where the reasoning comes from. The reasoning transfers; the organizational machinery does not need to.

Appendix E. Port CTT Exercise Roles

The table below summarizes the roles that make the Port CTT Exercise work, who fills each role, and what each role can access. The access boundary column records the rule that protects every participant: no role reaches into any organization's systems.

Role	Responsibility	Filled by	Access boundary
Sponsor	Charters the exercise, names the facilitator and repository steward, secures participation, and owns decisions and resourcing.	A senior stakeholder-side leader, such as a port authority or Area Maritime Security Committee figure.	Shared artifacts only.
Facilitator	Runs the exercise and keeps it at the capability level; administers the decision process and action tracking; captures findings and actions; point of contact for the sponsor.	A third party or staff without a direct stake in the operation under review, with scribe support as needed.	Shared artifacts only.
Repository steward	Accountable for keeping the Systems Repository current and correct; performs or directs the work of maintaining a structured, searchable record of capabilities, dependencies, and interfaces.	Named by the sponsor; the maintenance work may be done by a qualified architect engaged by the sponsor.	Works only with what participants report; no access to any organization's systems.
Participants	Validate the artifacts, walk the scenarios, and contribute local evidence; each carries the requirements its organization owns back into that organization's planning and serves as the point of contact for implementers.	Operations, security, IT, OT, terminal, regulatory, vendor, and partner representatives.	Own systems only.
SMEs	Provide specialized operational, technical, or analytical information to the exercise as needed; where an organization needs detailed architecture or attack-path analysis, it engages that support directly.	Consulted as needed; analysis support is selected and engaged by each owning organization under its own agreement.	Own or engaging organization's systems only, under confidentiality to that organization; shared artifacts otherwise.

Appendix F. References

[1] U.S. Department of Defense, The Department of Defense Cyber Table Top Guide, Version 3.0. Office of the Under Secretary of Defense for Research and Engineering, Oct. 14, 2025. [Online]. Available: https://www.cto.mil/wp-content/uploads/2025/12/DoD_Cyber_Table_Top_Guide_V3-10142025.pdf.

[2] U.S. Department of Defense, Cyber Developmental Test and Evaluation Guidebook, Version 3.0. Office of the Under Secretary of Defense for Research and Engineering, June 27, 2025. [Online]. Available: https://www.cto.mil/dtea/cyber/.

[3] U.S. Coast Guard, "Cybersecurity in the Marine Transportation System," Federal Register, vol. 90, no. 11, pp. 6298-6453, Jan. 17, 2025. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2025-01-17/pdf/2025-00708.pdf

[4] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 / NIST SP 1299. U.S. Department of Commerce, Feb. 26, 2024. doi: 10.6028/NIST.CSWP.29

[5] MITRE Corporation, "Enterprise matrix," MITRE ATT&CK. Accessed: July 8, 2026. [Online]. Available: https://attack.mitre.org/matrices/enterprise/

[6] Maritime Transportation Security Act facilities, 33 C.F.R. pts. 101-106 (2025). [Online]. Available: https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H

[7] American Productivity & Quality Center, "Process classification framework (PCF): Cross-industry." Accessed: July 8, 2026. [Online]. Available: https://www.apqc.org/process-frameworks

[8] T. Notteboom, A. Pallis, and J.-P. Rodrigue, Port Economics, Management and Policy, 2nd ed. New York: Routledge, 2026. doi: 10.4324/9781003585367.

[9] United Nations Centre for Trade Facilitation and Electronic Business, "UN/CEFACT reference data models (semantic models): Introduction," Dec. 2017. [Online]. Available: https://uncefact.unece.org/download/attachments/17830155/UNCEFACT%20Reference%20Data%20Models%20intro%20DEC17.pdf?api=v2.

[10] Cybersecurity and Infrastructure Security Agency, "Kaleris Navis N4 Terminal Operating System (ICS Advisory ICSA-25-175-01)," June 24, 2025. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-01

[11] National Institute of Standards and Technology, Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39. U.S. Department of Commerce, Mar. 2011. doi: 10.6028/NIST.SP.800-39

[12] D. Steenken, S. Voss, and R. Stahlbock, "Container terminal operation and operations research-A classification and literature review," OR Spectrum, vol. 26, no. 1, pp. 3-49, 2004, doi: 10.1007/s00291-003-0157-z.

[13] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3/Rev.1, June 14, 2021. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf

[14] International Association of Ports and Harbors, IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0, July 2, 2021. [Online]. Available:

https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
[15] Scaled Agile, Inc., “SAFe 6.0 knowledge base,” Scaled Agile Framework. Accessed: July 24, 2026. [Online]. Available: https://framework.scaledagile.com/
[16] Channel Industries Mutual Aid, “Channel Industries Mutual Aid (CIMA).” Accessed: July 26, 2026. [Online]. Available: https://www.cimatexas.org/
[17] Houston Ship Channel Security District, “Securing the Houston Ship Channel and its partners.” Accessed: July 26, 2026. [Online]. Available: https://hscsd.org/

Author Biography

John A. Wilson, Ph.D. is a public sector strategist at Entellect LLC with over 25 years of experience advising senior U.S. Department of Defense and Federal leaders on strategy, organizational transformation, and enterprise architecture. He holds a Ph.D. in Economics from Oklahoma State University, completed a post-doctoral fellowship at the UC Berkeley School of Public Health, and earned a B.S. in Economics from the University of Tulsa. He has also provided professional training in Scaled Agile and Lean Six Sigma to public sector managers.

His career spans the Center for Naval Analyses, the Logistics Management Institute, and the MITRE Corporation, where he applied mission engineering to military logistics, conducted cybersecurity vulnerability assessments for space and satellite tracking systems, and established Lean-Agile Centers of Excellence across DoD and Federal organizations. He is currently a Professor of Economics at San Jacinto College and leads the Entellect LLC Strategy and Transformation Division. Under contract to the SHSU Institute for Homeland Security, he is the researcher and author of the Technical Paper *Enhancing Infrastructure Security and Efficiency through IT/OT/ICS Integration*.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water/Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security

Sam Houston State University

Wilson, J. (2026). Port Operations Cyber Risk Assessment An Operations-Based Approach to Port Cyber Risk A Port Houston Proof of Concept. (Report No. 2026-1052). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/RGF89

INSTITUTE FOR HOMELAND SECURITY
SAM HOUSTON STATE UNIVERSITY