# Asset Matrix Case Study: Smart Ports

Liam Brew

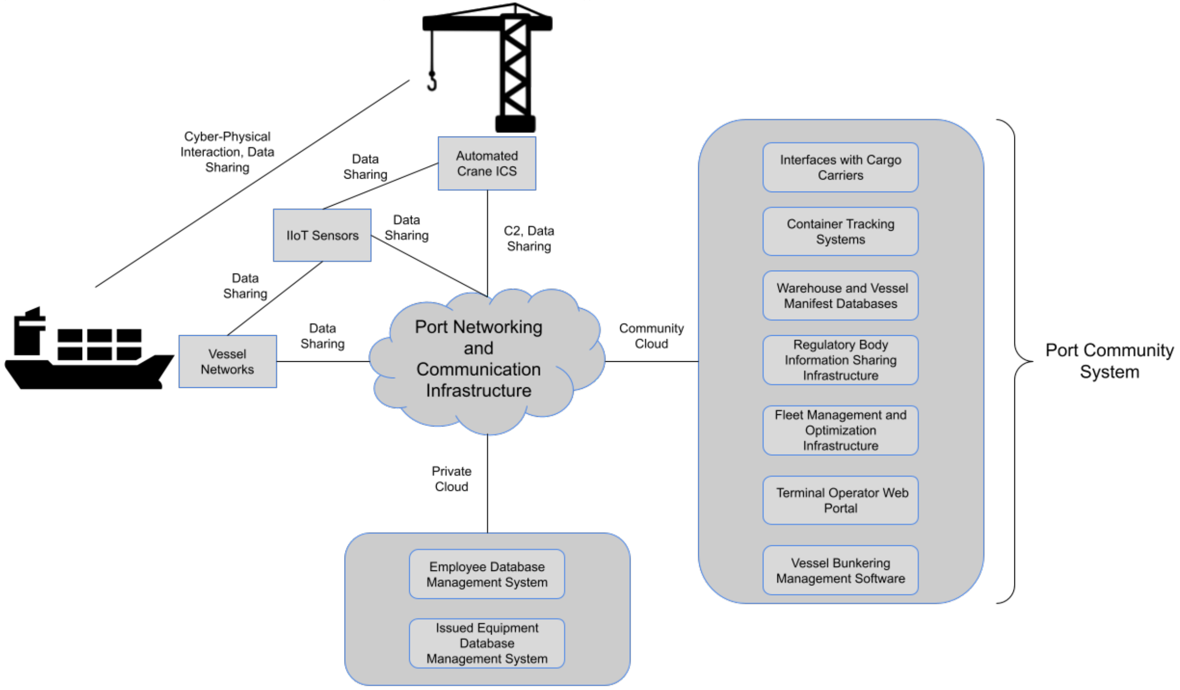
March 19, 2022

## 1 Introduction

The maritime transportation system (MTS) represents a key piece of critical infrastructure that plays a crucial role in both the national and global economies. While the MTS encompasses a wide range of industries ranging from shipyards to ferries to oil rigs, none are more vital than that of ports. Bridging the gap between land and sea, ports form the basis on which all other sectors of the MTS are able to function. As a result of this importance, significant investment into new technological infrastructure has taken place to promote maximum efficiency, with advanced assets such as sensory networks, artificial intelligence (AI), and automated control systems being leveraged to achieve a high operational tempo. However, the deployment of these new technologies *en masse* may yield significant risks that, if not identified and mitigated, may threaten both ports as well as the entire MTS as a whole.

## 2 Asset Descriptions

Smart ports make use of various information technology systems in their day-to-day operations. These may range from cutting-edge cyber-physical systems such as autonomous cranes to the more conventional but still important employee database management software. Due to the integrated nature of the MTS and the concentrated importance of ports to the many subsectors of this industry, these assets maintain a high degree of connectivity with each other. The following descriptions define the prominent assets most vital to a port's standard operation.


Cyber-Physical Interaction, Data Sharing
Data Sharing
Automated Crane ICS
IIoT Sensors
Data Sharing
C2, Data Sharing
Data Sharing
Vessel Networks
Data Sharing
Port Networking and Communication Infrastructure
Community Cloud
Private Cloud
Employee Database Management System
Issued Equipment Database Management System
Interfaces with Cargo Carriers
Container Tracking Systems
Warehouse and Vessel Manifest Databases
Regulatory Body Information Sharing Infrastructure
Fleet Management and Optimization Infrastructure
Terminal Operator Web Portal
Vessel Bunkering Management Software
Port Community System

Potential system architecture of a hypothetical smart port using the assets described here. Note that due to the high level of integration of assets, only the major interfaces between components are shown for clarity's sake.

## 2.1 Port Networking and Communication Infrastructure

The communication infrastructure of a port facilitates the use of numerous digital systems and is therefore vital to maintaining efficient operations. In this sense, infrastructure encompasses such systems that enable connectivity for core port services, with major examples being application servers, storage/database servers, switches, controllers/decoders, network video recorders, and other related information technology (IT) systems [1]. In addition to these more conventional systems, the rapid digitalization of formerly non-computer systems has created a proliferation of sensors, Internet of Things (IoT) equipment, and other 'micro' devices. These new tools oftentimes rely on more advanced communications technologies such as 5G, thus substantially increasing the network spread and connectivity of port environments [2].

## 2.2 Port Community Systems

Port Community Systems (PCSs) represent the electronic interfaces between the disparate systems and organizations that are representative of a typical port environment. While the specifics of PCs tend to vary based on their implementation, according to the International Port Community Systems Association the following key capabilities are typically offered [3]:

- electronic handling of information
- processing of maritime and other statistics
- status information and control

In the general sense, PCSs exist to provide a standardized information sharing medium for use by the various parties associated with a particular port. It is up to the individual parties to implement this information within their own internal processes. Therefore, PCSs may best be thought of as communication platforms whose responsibility it is to share information, not act on it. They are, however, an important asset of ports and go a long way in helping to manage the vast amount of data at play.

## 2.3 IIoT Sensors

Industrial Internet of Things (IIoT) technologies facilitate the collection of vast quantities of operational data from cyber-physical systems. This data, once analyzed and modeled,plays a large role in process optimization and driving efficiency improvement. According to telecommunications giant Inmarsat, in the maritime port environment IIoT sees significant adoption for use cases such as equipment and energy usage monitoring, employee tracking, and the implementation of area-based controls [4]. The data collected by IIoT devices is oftentimes fed into specialized analytical software to provide crucial domain-specific context, some of which represent critical port IT assets in their own right.

## 2.4 Automated Crane ICS

Automated cargo cranes for use in loading/unloading vessels require a significant amount of supporting information technology and industrial control systems (ICS) infrastructure. This may range from the LiDAR sensors that facilitate crane steering [5] to the safety mechanisms that monitor nearby vehicles and personnel [6]. In addition to their primary task of physically moving containers, these cranes must also constantly relay information about *what* they are moving to ensure that the proper databases and status trackers are continuously kept up-to-date.

## 2.5 Vessel Networks

In addition to the aforementioned port communication infrastructure, each individual vessel also has its own networking capabilities. These facilitate the day-to-day operations of the ship, and include long-range ship-to-shore very small aperture terminal (VSAT) satellite networks [7] as well as on-board networks to control intra-vessel sensors [8]. Additionally, the proliferation of IoT and other smart devices for use on ships has spurred on-board 5G technology in a manner similar to ports [9]. When docked, vessels interface directly with the port's networking infrastructure and PCS for official purposes such as using automated cargo cranes and uploading manifests. Additionally, they often utilize shore-based infrastructure to provide connectivity to the crew in order to save on VSAT charges.

## 2.6 Interfaces with Cargo Carriers

Trucks, trains, and planes all facilitate the movement of cargo to and from ports. Therefore, the operational status of these key assets is vital to the efficiency of the port itself. The requirements of each of these inter-modal transport methods vary. For example, rail and air transport require significantly larger life-cycle infrastructure investment then that required by trucks, but make up for this by enabling increased efficiency and economy-of-scale. Nevertheless, a tremendous amount of data sharing and synchronization is required regardless of the specific mode in question. Countless timetables, manifests, and resource allocation must be perfectly balanced to ensure that assets are in-place where they are needed when they are needed and not a second longer. Joint research conducted by Crux Systems and Kühne Logistics University stresses the importance that data availability plays in securing this harmonization of moving parts [10]. Technologies such as edge computing and predictive modeling are used here to ensure continual optimization based on real-time data [11].

## 2.7 Container Tracking Systems

Container tracking systems encompass several hardware and software solutions. Modules such as standalone GPS locators and Bluetooth-based tracking devices provide real-time location data on a container's whereabouts, with the latter having the important characteristic of interfacing directly with a port's communication infrastructure [12]. On the opposite end of the spectrum, software solutions such as IBM's TradeLens blockchain work to serve this information to relevant parties [13] anywhere in the world.

## 2.8 Warehouse and Vessel Manifest Databases

The scale of vessel throughput at major ports necessitates a significant amount of storage infrastructure. This storage may be semi-temporary, such as that used during the loading/unloading of a vessel, or more permanent, such as the dedicated warehouses and staging locations used by large cargo carriers. Regardless of their specific type, the status and contents of all these storage locations must be constantly known by port administrators both for the purposes of efficient operation (e.g., directing cargo-handling assets to where they are needed) as well as regulatory compliance (e.g., informing CBP of who-has-what and where they have it). Solutions such as Nicom IT's TRACS automated manifest system play a large role in facilitating the smooth flow of this type of information within a port environment [14].

## 2.9 Regulatory Body Information Sharing Infrastructure

Numerous government agencies play a role in the day-to-day operations of ports. A list of organisations that includes Customs and Border Protection (CBP), Homeland Security Investigations, the U.S. Coast Guard, the Department of Commerce, and state and local police departments is responsible for everything from searching for counterfeit goods to performing perimeter security. Of these, CBP plays arguably the most important role when it comes to facilitating the flow of cargo into and out of the port. The agency maintains an extensive information system, termed its Automated Manifest System (AMS), for the purpose of filing shipping documentation before cargo even arrives in the U.S. [15]. In addition to enabling an efficient flow of goods, this system assists CBP personnel in performing their tasks by maintaining highly-detailed cargo information in an available manner. To further promote efficiency and enforce regulatory compliance, CBP maintains a list of requirements that details how the container tracking and warehouse/vessel manifest systems used by the industry must interface with

AMS [16]. This inter-connectivity goes a long way in smoothing operations and reducing hassle, and is therefore a major selling point of products such as the aforementioned TRACS [14].

## 2.10 Fleet Management and Optimization Systems

The enormous amount and distributed nature of an international shipping firm's assets under management means that any efficiency or savings, no matter how small, quickly pays dividends. Enter fleet management and optimization systems, which leverage emerging technologies such as AI and IoT to develop, monitor, and (if necessary) modify highly efficient vessel and trade routes [17]. These systems utilize data such as vessel fuel consumption, historical and active weather conditions, and port congestion to build AI models that yield the most optimal voyage routes in terms of maximum profits and minimized downtime.

## 2.11 Terminal Operator Web Portal

Several major ports provide web portals through which terminal operators may view announcements, request and modify vessel schedules, configure operations, and perform other tasks and functions. While the specifics tend to vary based on their implementation, the general purpose of these tools is to provide the companies that lease and operate terminals with an easy-to-use and accessible platform in which to efficiently conduct certain types of administrative business. Some ports, such as the Port of Oakland, maintain their own portals [18], while others contract with specialized companies such as Ports of America to provide functionality in a software-as-a-service manner [19].

## 2.12 Vessel Bunkering Management Software

Vessel bunkering and provisioning can at times be a complex process due to the quantities and characteristics of the resources involved. To ease this burden, several companies offer specialized software to assist in this process and better coordinate with the bunkering services offered at ports of call. Some, such as the bunkering dashboard offered by Norcomms, are web-based solutions that help to organize and manage fuel purchases and deliveries [20]. Others are sophisticated tools that embed themselves within an organization's cloud environment, with vendor ClearLynx's Bunker Platform software offering advanced capabilities such as optimization planning, supplier profiles, and audit compliance [21].

## 2.13 Employee Database Management System

Ports employ a vast amount of workers, with career fields ranging from longshoremen to office clerks to security guards. Like other enterprises of similar scale, databases are used in human resources departments to provide record keeping for employee information. These databases are often times interfaced with additional enterprise resource planning tools to provide further functionality such as timekeeping and payroll. In addition to the employees of the port itself, these databases may also contain information about others, such as corporate partners and regulatory liaisons, for use in identity and access management purposes.

## 2.14 Issued Equipment Database Management System

The unique operating environments of ports necessitates the issuance of large varieties and quantities of issued equipment. Everything from individual radios to personal protective equipment must be stored, issued, and tracked. Some equipment, such as the HCV trucks used to scan containers for radioactive material, require significant maintenance routines at regularly scheduled intervals. Others, such as seized narcotics awaiting destruction, entail detailed chain-of-custody records. Databases facilitate this by storing records in highly available formats accessible by other tools and platforms while also being (theoretically) secure behind access control systems.

# 3 Risk Discussion

The varied natures and implementations of assets necessitates the examination of risk on a case-by-case basis. The following matrix details the risks associated with confidentiality, integrity, availability, and theft-related attacks on each asset, with the following discussion going into more detail regarding the justification for such scores.

| **Threat/Asset** | **Confidentiality** | **Integrity** | **Availability** | **Theft** |
|---|---|---|---|---|
| **Port Networking and Communication Infrastructure** | P = 2, C = 3<br>R = 6 | P = 2, C =3<br>R = 6 | P = 3, C = 3<br>R = 9 | P = 2, C = 2<br>R = 4 |
| **Port Community Systems** | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 | P = 2, C = 3<br>R = 6 | P = 1, C = 1<br>R = 1 |
| **IIoT Sensors** | P = 2, C = 1<br>R = 2 | P = 3, C = 2<br>R = 6 | P = 3, C = 3<br>R = 9 | P = 1, C = 1<br>R = 1 |
| **Automated Crane ICS** | P = 1, C = 1<br>R = 1 | P = 2, C = 3<br>R = 6 | P = 3, C = 3<br>R = 9 | P = 1, C = 1<br>R = 1 |
| **Vessel Networks** | P = 2, C = 2<br>R = 4 | P = 2, C = 3<br>R = 6 | P = 2, C = 3<br>R = 6 | P = 1, C = 1<br>R = 1 |
| **Interfaces with Cargo Carriers** | P = 2, C = 2<br>R = 4 | P = 2, C = 3<br>R = 6 | P = 2, C = 3<br>R = 6 | P = 2, C = 2<br>R = 4 |
| **Container Tracking Systems** | P = 2, C = 1<br>R = 2 | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 |
| **Warehouse and Vessel Manifest Databases** | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 | P = 2, C = 3<br>R = 6 | P = 2, C = 3<br>R = 6 |
| **Regulatory Body Information Sharing Infrastructure** | P = 1, C = 1<br>R = 1 | P = 1, C = 2<br>R = 2 | P = 1, C = 2<br>R = 2 | P = 1, C = 1<br>R = 1 |
| **Fleet Management and Optimization Systems** | P = 2, C = 2<br>R = 4 | P = 1, C = 2<br>R = 2 | P = 3, C = 3<br>R = 9 | P = 1, C = 2<br>R = 2 |
| **Terminal Operator Web Portal** | P = 3, C = 2<br>R = 6 | P = 3, C =2<br>R = 6 | P = 3, C = 3<br>R = 9 | P = 3, C = 2<br>R = 6 |
| **Vessel Bunkering Management Software** | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 | P = 2, C = 3<br>R = 6 | P = 2, C = 2<br>R = 4 |
| **Employee Database Management System** | P = 3, C = 3<br>R = 9 | P = 2, C = 3<br>R = 6 | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 |
| **Issued Equipment Database Management System** | P = 2, C = 1<br>R = 2 | P = 2, C = 2<br>R = 4 | P = 2, C = 2<br>R = 4 | P = 3, C = 2<br>R = 6 |

Table 1: Threat-Asset matrix detailing the risks of confidentiality, integrity, availability, and theft-related attacks on assets. Based on the governing equation of *Risk = Probability x Consequence*, wherein probability and consequence values are rated on a scale of 1 (not significant) to 3 (extremely significant).

## 3.1 Port Networking and Communication Infrastructure

### 3.1.1 Confidentiality Risk

The many systems that comprise a port's networking and communication infrastructure increase the odds of some form of data leakage occurring. The high value of data transmitted over this system, which provides insight into sensitive port operations across numerous tools and services, necessitates a high consequence score.

### 3.1.2 Integrity Risk

The large amount of tools and equipment used here, as well as its dispersed nature, increases the chance of integrity threats (both 'benign' as in defects and malicious as in attacks) of 'slipping through the cracks', with the potential of going unnoticed until the damage has been done. Modified communications data holds dire consequences when the potential use cases are considered, such as a hypothetical radiation alarm being redirected to the wrong location.

### 3.1.3 Availability Risk

So much relies on this infrastructure that a port cannot be expected to reasonably function without it. As seen in MTS-related cyber attacks such as the 2017 Maersk incident, attackers know this and act accordingly [22].

### 3.1.4 Theft Risk

The distribution of networking and other equipment over a relatively large geographic space means that it is unlikely for every asset to be directly monitored twenty-four hours a day. Due to the value of this equipment, it may pose a tempting target for theft, especially by insiders. Depending on the asset itself, any data that is exposed as a result of theft and subsequent sale and/or usage may prove harmful to operations.

## 3.2 Port Community Systems

### 3.2.1 Confidentiality Risk

As a community cloud environment, nothing shared on port community systems should be overly confidential or damaging. However, if leaked, data may prove to be damaging to the participants by being helpful to their competitors. The broad membership of PCSs and the many interfaces this necessitates increases the exposure factor of the data contained within, thereby also increasing the probability of such a leak occurring.

### 3.2.2 Integrity Risk

The data exchanged through PCSs is used by several participants to both plan their own operations as well as coordinate joint actions and ventures with other parties. Therefore, it is important that these entities are able to make their informed decisions based on reliable data. While it is possible for an adversary to modify data in this environment, such a modification would have to go unnoticed by the involved parties.

### 3.2.3 Availability Risk

PCSs are responsible for much of the inter-corporate activity that takes place in ports. Therefore, any prolonged disruption in services would have a severe impact on the involved parties. While adversaries may definitely exploit this, they tend to target the underlying networking and communication infrastructure more often.

### 3.2.4 Theft Risk

Aside from the previously mentioned benefit to competitors should data be leaked, there is not much in the way of threat risk that PCSs are exposed to.

## 3.3 IIoT Sensors

### 3.3.1 Confidentiality Risk

The raw data provided by IIoT sensors provides microscopic insight into a very specific port operation, and is therefore likely not to be of much use to the vast majority of adversaries.

### 3.3.2 Integrity Risk

The data collected by these devices is typically used in monitoring and analytical systems, therefore making its integrity and accuracy important to the efficiency of port operations. It is common knowledge that the majority of IoT/IIoT devices lack sufficient security hardening, meaning that it is reasonable to expect a competent adversary to successfully execute attacks against them.

### 3.3.3 Availability Risk

As mentioned, the lack of security for many of these devices significantly increases the likelihood for successful attacks to be performed against them. Due to the importance of the services that utilize data from these devices (such as fleet management and optimization systems), the consequence of large suites of these sensors being taken offline for prolonged periods of time is significant.

### 3.3.4 Theft Risk

The low relative cost of these devices means that for the majority of attackers, the reward to be gained by stealing them is not worth the accompanying risk to do so. Even so, the theft of lone sensors here-and-there is unlikely to be much more than a nuisance to a port.

## 3.4 Automated Crane ICS

### 3.4.1 Confidentiality Risk

The data that cranes process is available in several more exposed locations, and is not necessarily valuable to begin with. Therefore, the confidentiality risk here is low.

### 3.4.2 Integrity Risk

The potential malfunction (whether accidental or through nefarious actions) of these massive machines pose significant threats to personnel safety as well as the safety of involved vessels, cargo, and the cranes themselves.

### 3.4.3 Availability Risk

In an extremely simplified manner, the basic purpose that ports serve is to load/unload cargo on to/off from vessels. If a crane is taken offline for whatever reason, the ability to fulfill this mission has been drastically reduced. Such a pronounced bottleneck may prove to be a tempting target for attackers.

### 3.4.4 Theft Risk

The scale of these assets and the requirements to operate them generally preclude them from the majority of theft-oriented risks.

## 3.5 Vessel Networks

### 3.5.1 Confidentiality Risk

These networks oftentimes transmit data that may be sensitive to an individual ship's operation, such as its cargo or destination. Depending on the technical implementation of the network used, it is oftentimes possible for competent adversaries to sniff traffic. This is especially so in the crowded confines of most ports, wherein there is greater access to a vessel's nearby geographic proximity.

### 3.5.2 Integrity Risk

The integrity of a vessel's network is important due to the role it plays in facilitating smooth operations. Examples of tasks a network may be responsible for range from communicating the status of bilge pumps to transmitting a cargo manifest to shore-based authorities. Due to this criticality, there is little tolerance for the dissemination of faulty information.

### 3.5.3 Availability Risk

As mentioned, several of a vessel's key systems rely on its network for operation. Therefore, if said network is unavailable, then it may reasonably be assumed that the ship is operating at a high degree of inefficiency, if it is not for all intents and purposes 'dead in the water'. A disabled ship has severe consequences on the tight schedules and just-in-time resource allocations that several major ports utilize.

### 3.5.4 Theft Risk

Aside from the previously mentioned data leakage aspect, the exposure to ship networks to theft is fairly limited.

## 3.6 Interfaces with Cargo Carriers

### 3.6.1 Confidentiality Risk

Should certain cargo be sensitive in nature, then a potential data breach may result in notable damages. As this system services to bridge the operations of the port with those of the cargo carrier, it has a significantly larger attack surface than operations bounded within the confines of the port alone.

### 3.6.2 Integrity Risk

The integrity of this system is vital in ensuring cargo gets to its correct destinations on-time. As a result, adversaries may seek to modify locations and/or schedules to wreak havoc. Depending on the capabilities of the specific system, more enterprising adversaries may even redirect shipments to new destinations that are favorable to them.

### 3.6.3 Availability Risk

If these systems are to be taken offline, the resulting congestion and disorganization of cargo services would be enough to cripple a port if not halt operations entirely. The exposed nature of these systems make this a very real threat.

### 3.6.4 Theft Risk

These systems often control, or at least record, what is going where. Therefore, they may prove to be tempting targets for those with thievery in mind. The large attack surface exposes this system to threats from many angles, with insiders on both the port and cargo carrier side having equality of access.

## 3.7 Container Tracking Systems

### 3.7.1 Confidentiality Risk

The underlying technologies of most container tracking systems, GPS and Bluetooth, are not particularly secure. This is especially so when adversaries are in close physical proximity to the targeted container. However, by that point there is little information to be gained by infiltrating the system.

### 3.7.2 Integrity Risk

In addition to providing location data, several of these systems are also used to monitor access to the container in question. This may be accomplished by means such as access logs to a low-tech seal on the door. No matter the specific implementation, however, there is little in the way of ensuring integrity. Location data may be spoofed, access logs may be overwritten, and broken seals may be replaced. Smugglers in particular have ample motivation for these integrity-centric attacks.

### 3.7.3 Availability Risk

Due to the lack of sufficient security hardening as described above, these systems are relatively easy to attack and therefore bring offline. Several groups may have a vested interest in doing so. Smugglers, for example, would be served by temporarily disrupting the location services of a container while loading it with contraband. Once finished, the container would be re-sealed and brought back online, with nothing in particular pointing to foul play. Additionally, a lack in availability of these systems even from non-malicious incidents may also result in damages, such as disruption of package tracking and estimated arrival calculations.

### 3.7.4 Theft Risk

The smuggler adversarial scenarios described in the integrity and availability sections also lend themselves well to thieves.

## 3.8 Warehouse and Vessel Manifest Databases

### 3.8.1 Confidentiality Risk

If leaked, the data stored in these systems may provide valuable insight into adversaries. This may be in the form of a list of valuable items a port may currently have, or in the broader sense, information as to how a port sorts and organizes goods. The nature of these systems generally require that they are accessible to other tools and services such as those used by regulatory agencies. Therefore, they posses a non-insignificant attack surface.

### 3.8.2 Integrity Risk

It is important that these systems provide accurate data. Rectified mislabeled and/or improperly stored cargo can cause inefficiencies in port operations and may result in damages. Additionally, it would not be in the port's best interest if adversaries were able to quietly remove certain items from manifests for later retrieval or destruction.

### 3.8.3 Availability Risk

These systems play a large role in a port's data sharing environment. As mentioned, they are utilized by other systems and services to get cargo where it needs to be. Therefore, constant up-time and availability is required to ensure a smooth flow of operations.

### 3.8.4 Theft Risk

As touched on, integrity threats may also result in potential theft. Due to its nature, this system may in essence serve as a catalog, with thieves using it the information contained within to plan attacks and prioritize targets.

## 3.9 Regulatory Body Information Sharing Infrastructure

### 3.9.1 Confidentiality Risk

Due to the public nature of most regulatory standards, there is little to be concerned with the confidentiality aspect of this system.

### 3.9.2 Integrity Risk

The information on this platform may be modified by attackers to trigger false-positives in regulatory compliance software, which would flag the port as non-compliant for some such standard when it truly is. However, due to these tools connecting only the port and government authorities, there is little access to them from the outside, thereby reducing the potential attack surface. Additionally, there is also little gain in doing so, as any misunderstandings may be easily rectified once the valid data is shown to authorities.

### 3.9.3 Availability Risk

Bringing these systems offline may likewise cause issues as a result of a port missing reporting deadlines. However, this action would be relatively obvious, and in a similar manner as above there is little gain in doing so.

### 3.9.4 Theft Risk

This asset does not have any significant vectors through which theft may either utilize or harm it.

## 3.10 Fleet Management and Optimization Systems

### 3.10.1 Confidentiality Risk

The models used by these systems reflect overarching corporate strategy, containing detailed information about the assets and capabilities of a company. As a result, competitors would benefit from these models being leaked, whether it be through adopting them for their own usage or even being able to interpret what the opposition is doing.

### 3.10.2 Integrity Risk

The feeding of forged data to these models may reduce the accuracy of the generated plans, thereby potentially disrupting operations and promoting inefficiency. However, this requires control over a sufficient amount of data streams for a sufficient duration in order to make a noticeable impact. Additionally, this would result in little gain to adversaries when compared to confidentiality and availability attacks, so the probability of this risk manifesting itself may be considered minor.

### 3.10.3 Availability Risk

As companies heavily rely on these systems to both perform day-to-day operations as well as develop and maintain strategies, a prolonged loss of usage would be devastating. Therefore, it would be in the interests of adversaries to pursue this route if they wish to cause damage to a firm. This would be more straightforward to accomplish than integrity-based attacks, as only a few servers would need to be taken offline as opposed to numerous data streams being controlled.

### 3.10.4 Theft Risk

While these systems may include data such as asset locations, its macro scale doesn't lend itself well to planning individual instances of theft. From the point of view of adversaries there are better targets for this, such as the aforementioned manifest databases.

## 3.11 Terminal Operator Web Portal

### 3.11.1 Confidentiality Risk

As this system represents an interface between two entities in the form of a public-facing website, it has a significant attack surface when compared to more 'private' assets such as internal networks. The administrative data processed by this system, such as non-public announcements and detailed operation schedules, may result in damages if leaked.

### 3.11.2 Integrity Risk

Likewise, due to the importance of this data on managing operations, there exists the potential for integrity attacks to cause significant disruptions. Examples of this include modifying schedules, placing fraudulent orders, and reserving resources to handle non-existent deliveries.

### 3.11.3 Availability Risk

As terminal operators rely on these systems to conduct day-to-day business, downtime has the potential to cause significant losses as a result of an inability to work. Ports too stand to suffer from this, as a backlog at any one terminal may quickly affect others, to say nothing of a port-wide denial of terminal service.

### 3.11.4 Theft Risk

The financial information stored within these systems may prove to be a tempting target for thieves. Other data, such as asset locations and expectant arrival times of goods, may be considered further motivation.

## 3.12 Vessel Bunkering Management Software

### 3.12.1 Confidentiality Risk

The implementation of some of these systems as websites or online portals increases the number of attack vectors that they must contend with. The data found within them, such as a company's order history and their most frequented ports, may be of some value to competitors.

### 3.12.2 Integrity Risk

The modification of data within these systems, such as the placement of fraudulent orders, may result in disruptions to business flow and possible deterioration in relations with partners.

### 3.12.3 Availability Risk

Bringing these systems offline would result in firms having to resort to conventional means of arranging vessel replenishment, such as manual communication with ports and bunkering service providers. This would result in major delays and marked decrease in operational efficiency.

### 3.12.4 Theft Risk

The payment processing information used to facilitate the remote purchase of supplies may prove a tempting target for thieving adversaries.

## 3.13 Employee Database Management System

### 3.13.1 Confidentiality Risk

These systems contain very large amounts of employee personally identifiable information such as names, addresses, social security numbers, and potentially health information as well. Additionally, the frequent connection of these systems with other forms of enterprise resource planning software may expose even more data to the risk of loss. Therefore, breaches may yield catastrophic damages to a port, which is a fact that attackers are well aware of.

### 3.13.2 Integrity Risk

If the database is used for such purposes as regulating identity and access management, such as through the storing of user roles under a roles-based access control scheme, then modification of data by insiders proves to be a significant security risk.

### 3.13.3 Availability Risk

Compared to other critical port assets, denial of service attacks on this system would yield a lesser immediate impact on day-to-day operations. However, the implications of prolonged outages, such as the inability to pay wages or track leave time, may prove to be just as damaging.

#### 3.13.4 Theft Risk

The previously mentioned employee data represents an ideal target for adversaries interested in committing identify theft and other types of fraud.

### 3.14 Issued Equipment Database Management System

#### 3.14.1 Confidentiality Risk

The distribution of assets within a port, at least in the general sense, may be learned from observation in a relatively straightforward manner. Nevertheless, the exact details of equipment distribution is not something that a port would want to publicly share for no reason. Due to the amount and range of employees that utilize this system everyday, it may have a significant exposure factor to insider threats.

#### 3.14.2 Integrity Risk

Certain nefarious modifications of data that this system may track, such as revoking asset usage and issuance rights to qualified users, may promote inefficiencies and result in a slow-down of operational tempo.

#### 3.14.3 Availability Risk

As with the aforementioned employee database, denial of usage of this system will not result in immediate catastrophe. However, damages will definitely increase the longer the system remains down, so it would be in the port's best interest to maintain the availability of this system.

#### 3.14.4 Theft Risk

Certain information that this system may track, such as detailed distributions of expensive equipment and chain-of-custody records, may prove useful to theft-motivated adversaries who likely recognize the importance of such a target.

## 4 Conclusion

The results of this risk assessment indicate that the more exposed an asset is, the larger its attack surface and therefore the greater its associated risk. This is seen in assets such as the web portal for terminal operators, port networking infrastructure, highly-available databases, and third party interfaces having the highest risk scores. Not only are these systems exposed outsiders beyond a port's direct control, they also have value in the forms of one or more of sensitive data, expensive goods, or the ability to wreak havoc on operational efficiency. Therefore, it is no surprise that adversaries may be drawn to attack them, and that sufficient security should be dedicated to prevent such an occurrence.

| **Asset** | **Total Risk** |
|---|---|
| Terminal Operator Web Portal | 27 |
| Port Networking and Communication Infrastructure | 25 |
| Employee Database Management System | 23 |
| Interfaces with Cargo Carriers | 20 |
| Warehouse and Vessel Manifest Databases | 20 |
| IIoT Sensors | 18 |
| Vessel Bunkering Management Software | 18 |
| Automated Crane ICS | 17 |
| Vessel Networks | 17 |
| Fleet Management and Optimization Systems | 17 |
| Issued Equipment Database Management System | 16 |
| Port Community Systems | 15 |
| Container Tracking Systems | 14 |
| Regulatory Body Information Sharing Infrastructure | 6 |

Table 2: Assets ranked in order of maximum total risk.

# References

[1] “Smart Port & Maritime Solution,” 2017. [Online]. Available: https://www.hikvision.com/content/dam/hikvision/eu/support/brochures/vertical-solution-brochure/Smart%20Port%20&%20Maritime%20Solution.pdf

[2] R. Cardone, “The 5G Port of the Future,” November 27 2017. [Online]. Available: https://www.ericsson.com/en/blog/2020/7/the-5g-port-of-the-future

[3] “Port Community Systems - General.” [Online]. Available: https://ipcsa.international/pcs/pcs-general/

[4] “Industrial IOT on land and at sea: Maritime.” [Online]. Available: https://www.inmarsat.com/content/dam/inmarsat/corporate/documents/maritime/insights/Inmarsat_IIoT_on_land_and_at_sea_Maritime.PDF

[5] “The Importance of LiDAR Technology in Port and Crane Automation.” [Online]. Available: https://hokuyo-usa.com/resources/blog/importance-lidar-technology-in-port-and-crane-automation

[6] “Three Liebherr automated RMGs start operations at CSX Intermodal in North Carolina.” [Online]. Available: https://container-news.com/three-liebherr-automated-rmgs-start-operations-at-csx-intermodal-in-north-carolina/

[7] “VSAT and Connectivity on Ship.” [Online]. Available: https://maritronics.com/vsat-connectivity-ship/

[8] “Sensors and IoT in the shipping industry.” [Online]. Available: https://marine-digital.com/article_sensors

[9] S. E. . J. S. . J. Leigh, “The Role for 5G in Transportation and Logistics,” May 2021. [Online]. Available: https://www.t-mobile.com/content/dam/tfb/pdf/Role-of-5G-in-Transportation-and-Logistics.pdf

[10] M. Leonard, “Why carrier data is key to solving intermodal’s visibility issues,” October 23, 2020. [Online]. Available: https://www.supplychaindive.com/news/intermodal-visibility-eta-train-data-predictability/587594/

[11] K. Delaney, “The smart, sustainable port: where sea, rail, and road meet seamlessly,” November 22, 2021. [Online]. Available: https://newsroom.cisco.com/feature-content?articleId=2209602

[12] “Container Tracking Systems: Everything You Need To Know,” April 26, 2018. [Online]. Available: https://www.link-labs.com/blog/container-tracking

[13] “TradeLens container logistics solution.” [Online]. Available: https://www.ibm.com/blockchain/container-logistics

[14] “TRACS Automated Manifest System for Ports & Shipping.” [Online]. Available: https://www.nicommaritime.com/products/seaport-logistics-software/automated-manifest-system/

[15] “What is the CBP Automated Manifest System (AMS)?” [Online]. Available: https://customscity.com/what-is-the-cbp-automated-manifest-system-ams/#:~:text=What%20is%20AMS%3F%20The%20Automated%20Manifest%20System%20%28AMS%29,system%20and%20an%20imported%20goods%20inventory%20regulation%20system.

[16] “CBP and Trade Automated Interface Requirements,” November 2021. [Online]. Available: https://www.cbp.gov/sites/default/files/assets/documents/2021-Nov/trade-draft-ace-cargo-releawse-implementation-guide-V32-November%2017%202021.pdf

[17] “Artificial Intelligence to Improve the Shipping Industry’s Efficiency,” February 10, 2021. [Online]. Available: https://maritime-executive.com/article/artificial-intelligence-to-improve-the-shipping-industry-s-efficiency

[18] “Port of Oakland Launches Maritime Operations Web Portal,” February 11, 2015. [Online]. Available: https://www.portofoakland.com/press-releases/press-release-379/

[19] “iDockworks for Ports America.” [Online]. Available: https://dockworks.portsamerica.com/Default.aspx

[20] “Bunkering Software for Optimising Bunker Purchases.” [Online]. Available: https://www.norcomms.com/bunkeringsoftware.php

[21] “ClearLynx Bunker Platform.” [Online]. Available: https://www.clearlynx.com/bunker-fuel-platform

[22] J. Gronholt-Pederson, “Maersk says global IT breakdown caused by cyber attack,” June 27, 2017. [Online]. Available: https://www.clearlynx.com/bunker-fuel-platform