# A Pattern for Secure Cargo Port Drayage

VIRGINIA M. ROMERO, Florida Atlantic University
EDUARDO B. FERNANDEZ, Florida Atlantic University

A cyber-physical system (CPS) integrates computing and communication capabilities with the monitoring and control of entities in the physical world. An important type of CPS is a maritime cargo port. Port drayage, in intermodal freight transport, is defined as the transport of containerized cargo by specialized trucking companies between a maritime port terminal and an inland distribution point or a rail terminal. A typical drayage assignment involves either delivering an export container to a marine terminal or picking up an import container. Drayage of marine containers to and from port terminals is a complex process involving interactions between customers (importers, exporters, third-party logistics firms), ocean carriers, terminal operators and trucking firms. We present a pattern for the secure drayage of containers at a maritime cargo port. This pattern describes the basic operations of the system and the relationship of the components involved. It uses a systematic approach to identify threats from internal or external sources, and applies security patterns to handle these threats.

Categories and Subject Descriptors: D.2.11 **[Software Engineering]** Software Architectures–Patterns; D.5.1 D.4.6 **[Security and Protection]** Authentication, Authorization, Logging
General Terms: Design
Additional Key Words and Phrases: Drayage, cargo port, security patterns, cyberphysical systems

**ACM Reference Format**: V. M.Romero**,** and E.B.Fernandez, 2018. Procs. 7th Asian Conference on Pattern Languages of Programs, Asian PLoP'18, March 1-2, Tokyo, Japan. 9 pages.

## 1. Introduction

Cyber Physical Systems (CPS) are systems that integrate physical processes, computational resources, and communication capabilities with the monitoring and/or control of entities in the physical world. The components of a CPS can be centralized or distributed and usually include embedded devices, sensors, actuators and wireless links. Many system components are remotely deployed, have unique constraints and may be physically inaccessible for maintenance but not for attacks. Examples include transportation systems, smart power grids, patient monitoring, smart buildings, flexible manufacturing systems, and many others. Mobile devices have sensors and they can participate in CPS, clouds are also being used. Their main objective is to perform safely, securely, reliably, efficiently and in real time.

In our approach we consider all architectural levels and lifecycle stages of software development when building secure systems (Fernandez 2013). If, when we build CPS applications, we also consider the effect of the physical entities, middleware, operating systems, and networks as a whole, we can build systems that exhibit a unified architecture where we can identify attacks and then apply global solutions. All safety and security constraints should be defined at the application level, where their semantics are understood and propagated to the lower levels (Fernandez 1999). The lower levels must provide the assurance that the constraints are being followed, i.e., they implement these constraints and enforce that there are no ways to bypass them. The description of architectures and mechanisms using patterns makes them easier to understand, provides guidelines for design and analysis, and can define a way to make their structure more secure. Their abstraction properties make them ideal for dealing with highly heterogeneous systems such as CPSs.

Securing CPSs requires a relatively complete catalog of patterns, covering all architectural levels, as well as Computation, Communications, and Control aspects. To select which security patterns or create new ones, we need to enumerate the threats to the system and we proposed a method that analyzes the activities in a Use Case to see

---

Authors' addresses: Virginia M. Romero (corresponding author), Dept. of Computer and Electrical Eng. and Computer Science,Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, USA; email: vromero@fau.edu Eduardo B. Fernandez Dept. of Computer and Electrical Eng. and Computer Science,Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, email: ed@cse.fau.edu;

how they can be subverted by an attacker (F. Braz et al. 2008). We applied these ideas to CPSs, including physical access control (Fernandez et al. 2007), and SCADA systems (Fernandez et al. 2010). We also investigated the natures of CPS threats (Fernandez 2016).

We intend now to build a reference architecture for CPSs. Because there is a large variety of CPSs, with very different structures, we started analyzing cargo ports. Today U.S. port facilities and around the world rely much more upon computer and control systems than they do upon dock workers to ensure the flow of maritime commerce. Using this methodology we wrote a pattern for the loading and unloading of containers to/from a ship at a cargo port facility (Fernandez et. al. 2014). We present here a pattern for the secure delivery and pick up of a container at a cargo port.

We use the template of (Buschmann 1996) to present our pattern. Our audience includes CPSs designers as well as designers of applications that need to run in CPSs. For conciseness, we only show in detail one of its use cases.

## 2. A Security Pattern for Cargo Port Drayage

### 2.1 Intent

Provide all the typical functions and security mechanisms for the secure delivery and pick up of containers at a maritime cargo port.

### 2.2 Context

For millennia, mankind has shipped goods across the oceans, from one land to another. The loading and unloading of a ship has always been very labor intensive. A ship could spend easily more time in port than at sea while dock workers handled cargo into and out of tight spaces below decks. The introduction of containerization has greatly simplified this process and nowadays goods can be moved seamlessly between ships, trucks and trains. Port automation has been playing an increasing role with the introduction of robots, artificial intelligence and other digital tools that keep the goods flowing into and out of major ports. This technology is widely seen as the most efficient way for seaports to cope with rising global shipping traffic and massive new ships that haul more and more containers. By digitizing and automating activities once handled by human crane operators and cargo haulers, seaports can reduce the amount of time ships sit in port and otherwise boost port productivity by up to 30% by some estimates. Due to its global reach and freight volume, the maritime sector plays a central role in the economic security and stability of a nation. Any disruption to the maritime transportation system, whether through natural disasters, accidents, failures of infrastructure, or acts of terrorism or cybercrime, can have an immediate and cascading effect throughout the entire supply chain (York 2013).

Port drayage refers to the movement of containers between a port terminal and an inland distribution point or rail terminal. A typical drayage assignment involves either delivering an export container to a marine terminal or picking up an import container that has arrived in a ship (NCFRP 2011).

### 2.3 Problem

Security attacks in port drayage can severely disrupt the flow of operations that are crucial to the functioning of a maritime cargo port. This disruption may lead to a halt or serious disruption in the entire supply chain affecting the economic security and stability of a nation. For example, a degradation in the availability of any of the components in the gate operations system may result in trucks idling inside or outside the terminal causing air pollution, a serious health concern, and congestion on the roads that lead to the terminal and the communities adjacent to the seaports. A more severe attack may cause human and economic loss as the potential consequences of even a minimal disruption of the flow of goods would result in grocery store shelves and gas tanks at service stations to run empty. In certain ports, a disruption affecting energy supplies would likely send not just a ripple but a shockwave through a country and maybe the global economy. Security attacks can also affect the safety of the people involved in the handling of containers. How can we assure the smooth operation of these activities in the presence of possible attacks?

## 2.4 Forces

The solution to this problem is guided by the following forces:

- Flexibility—several internal and external roles may be involved, i.e. truck operators, storage area workers and supervisors, crane operators, etc. Resources and devices used as well as its corresponding operations must be flexible to accommodate this variety of roles.

- Usability—the software used to identify and authenticate the individuals entering the port, their trucks and their container contents should be easy to use by roles who do not have technical backgrounds.

- Alerting—any attempt to deviate from the normal operations of the terminal must produce an alert and should be logged.

- Logging – any activity should be recorded and logged for future auditing. In general, every visit should be logged to keep track of any access to the facility. All containers must be registered and logged.

- Physical Damage Avoidance—containers are heavy and may have fragile contents. A dropped container may kill people and produce costly damage. A cyberthreat can make containers be dropped or misplaced.

- Location Tracking—we need to be able to find every container. A container in the wrong place can delay operations.

## 2.5 Solution

Every maritime port container terminal (Quay) should include Port Security and Access Control functions. Drivers arriving at a maritime terminal entrance gate intend to either drop off a loaded export container, or an empty container; and/or to pick up a loaded import container, or an empty container. The variety of external users and the fact that the contents of the containers are usually not in plain sight bring many threats. Continuous checks are required, not only to the individuals entering the terminal but also to the contents of their trucks. We must authenticate drivers and their loads before they enter the terminal. We must log every container move. All activities need to be recorded for future auditing in case of a security violation. All truck and container moves need to be recorded using videos to improve security and operations at the port. The containers need to be tagged, tracked and their location recorded for identification and to prevent illegal entry of weapons and chemical or biological agents as well as human trafficking. Attackers may replace container tags while in the storage yard posing serious consequences. In general, every visit should be logged. There are other transactions that may be possible (such as moving trucks without containers or chassis) but these movements of empty containers or bare chassis are a result of loaded movements.

### 2.5.1 Structure

Figure 1 presents the class diagram of a cargo port drayage operation and the relationship of its components. Class *Quay* represents the platform for loading and unloading ships. *GateAccess* represents the entrance to the terminal. Each Quay aggregates only one GateAccess since each port terminal has only one gate for entrance. GateAccess aggregates multiple instances of *DrayageProcess*, where each instance represents a single drayage transaction; where a transaction implies the delivery or pickup of a Container to the Quay. DrayageProcess consists of entities *Truck, TruckDriver* and *Container*. For each drayage transaction there is one truck driver in charge of one truck and one to two containers depending on the size of the containers, and on whether they drop off and pick up a different one.. GateAccess must verify that the drayage operation is a legitimate one. *ImportArea* and *ExportArea* represent the

surfaces on the terminal assigned to stack the containers. Each container has a unique location in the storage yard which is represented by *ImportLocation* or *ExportLocation*. These unique locations are kept and updated in the *Log*.

### 2.5.2 Dynamics

We describe the dynamic aspects of the Secure Cargo Port Drayage pattern using an activity diagram for the following use case.

***Use Case: Drop off Export Container***

Summary: TruckDriver requests entrance to the maritime cargo port. GateAccess verifies the identity of the driver, the truck and its load. GateAccess also verifies that the driver's transaction is a legitimate one. Driver obtains the location and proceeds to drop the container off in the storage yard.

Actors: TruckDriver, GateAccess.

Precondition: The drayage operation information has been previously entered in the system.

Description:

1 TruckDriver arrives to the terminal entrance.

2 GateAccess authenticates the driver.

3 GateAccess authenticates the truck.

4 GateAccess authenticates the container load.

5 TruckDriver obtains the location for the drop and proceeds to the storage yard.

6 TruckDriver drops the container in the appropriate location in the storage yard and exits the terminal or picks up another container. The Log is written indicating the container id and its location.

Postcondition: A container has been deposited in the port and the transaction is recorded.

Other typical use cases include: Pick up import container, Assign locations to the containers, Assign drivers to the trucks. Typical roles include: gate attendant, storage yard supervisor, storage yard worker, truck driver, gate access worker.

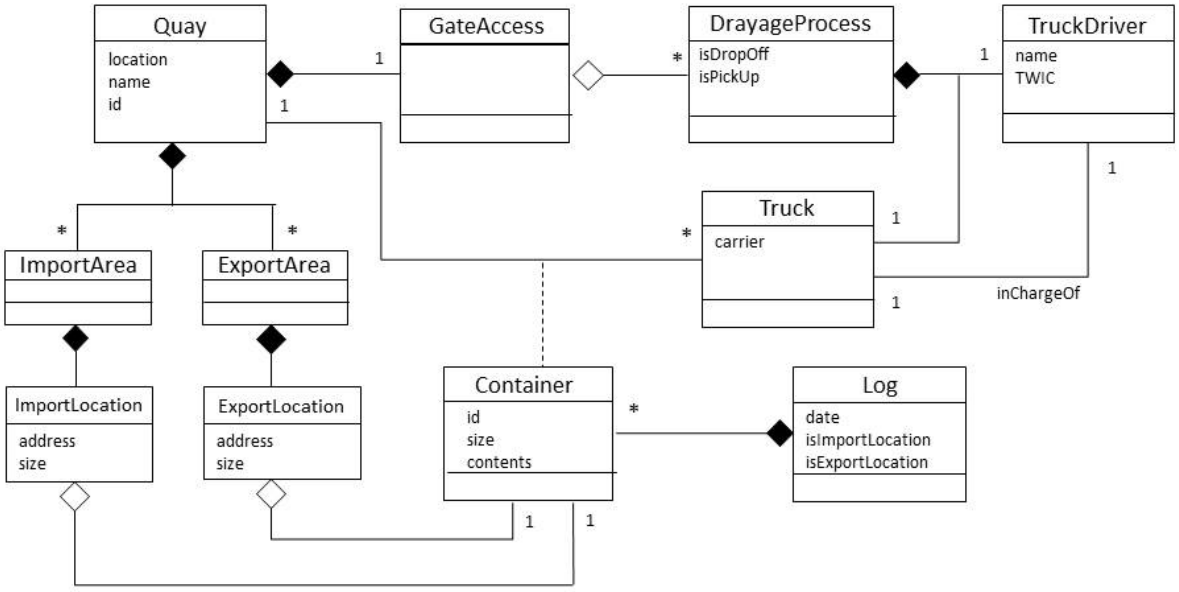


**Figure 1 Class Diagram of Cargo Port Drayage**

2.5.3 Enumerating Threats

Figure 2 shows the activity diagram for the use case Drop off export container at a maritime container port. For each activity we can analyze its possible threats. We do not try to be exhaustive, only to show the procedure to enumerate threats; i.e. we are not showing in detail the threats that can happen during the other use cases. The activities in this Use Case present the following threats:

- **a1 Authenticate Driver:** Stolen credentials or a fake Transportation Worker Identification Credential (TWIC ID) may allow an impostor to enter the terminal. Unauthorized individuals may possess high powered weapons, contraband or illegal drugs. Possession of counterfeit TWICs purchased illegally may facilitate unescorted entry into secure areas of regulated facilities in the port.

- **a2 Authenticate Truck:** Incorrect truck RFID tag, tampered or stolen may allow unregistered trucks to enter the terminal causing a broad range of consequences. These include: Mild impact consequences such as a delay or congestion at the gate, or more severe consequences such as loss of human life as these vehicles can be used as weapons in a hostile vehicle attack.

- **a3 Authenticate Load:** Container information deleted, modified or not accessible may allow for weapons, deadly chemicals, explosives and perhaps human trafficking to enter the terminal.

- **a4 Obtain Location:** Receiving the incorrect location for drop off of the container can cause long queue times, processing delays, miss a shipment.

- **a5 Drop Container:** Container can be placed in the wrong location disrupting the future placement of other containers or making it hard to find.

- **a6 Update Log:** Wrong entry in the log would create later disruption. Deleting an entry or deleting the log may cause never finding the container and complete chaos as the flow of goods would be disrupted.

- **a7 Exit Gate:** Not verifying the correct paperwork for exiting the terminal may cause weapons of mass destruction to enter the country, human trafficking or smuggling of goods.

,

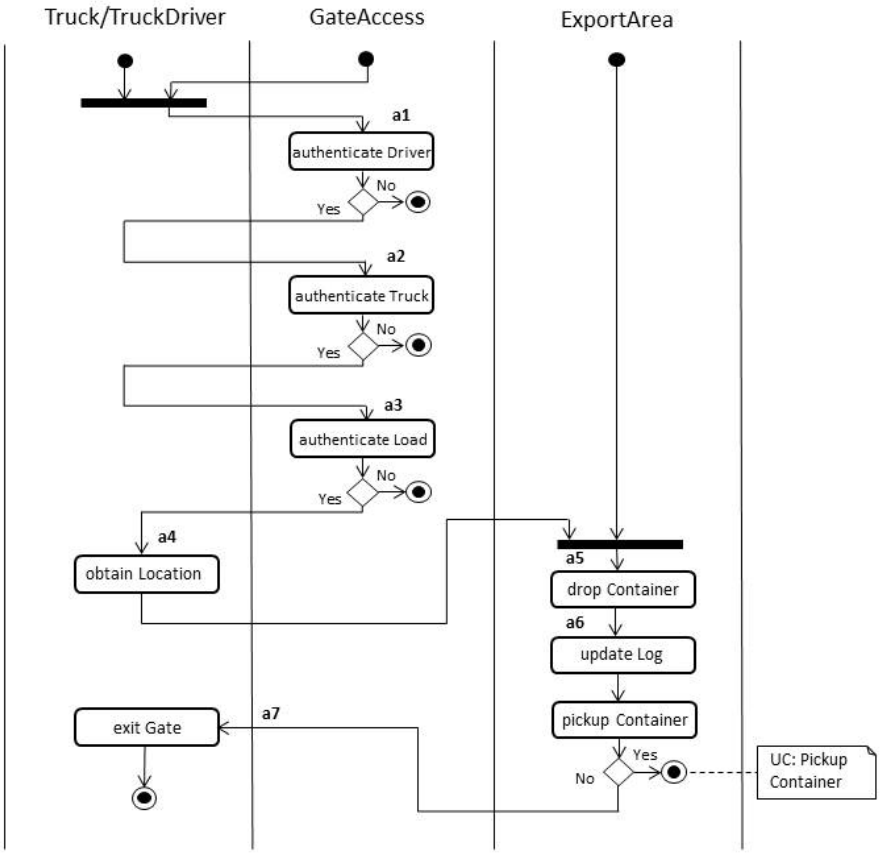


**Figure 2 Activity Diagram for Use Case Drop Off Export Container**

2.5.4 Countermeasures

Threats can be enumerated systematically. We may not be able to prevent all attacks but a good number of them would be minimized and controlled when we match them to their defenses. Using the semantics of the application we can also classify them and estimate their impact.

The identified threats in the activities of Figure 2 (a1, a2, a3, a4, a5, a6, a7) can be stopped by using authentication, authorization and logging patterns. For authorization we use a Role-Based Access Control (RBAC) model which assigns rights to roles to perform some actions in a resource. Individual users may be assigned one or more roles.

We can use security patterns and OCL assertions for defining security policies to stop the identified threats and safety assertions to avoid unsafe conditions. These assertions realize pre-specified policies based on regulations and equipment constraints. Possible assertions include:

- For every access to the terminal port, all conditions must be valid (authenticate driver, authenticate truck and authenticate container load).

- For every container placed in the storage yard, an entry in the log must be entered.

### 2.5.5 Implementation

This pattern can be implemented at all gate entrance operations for all ports. Roles and access rights need to be standard across port terminal locations.

When implementing authentication, we can embed anti-forgery devices in the ID cards used for identification, i.e. biometric information. An additional security measure that is part of the authentication process implements a security code for each port drayage operation. This security code is to be shared between the authenticating system and the individual trying to gain access to the port. Techniques like Multi-factor authentication may be used to strengthen the authentication process.

To prevent the forgery and image manipulation of documents, we can use image processing applications that detect irregularities in font and design of inserted words, spaces between letters, discrepancies in size, crowding and non-uniformities in the background (Saini 2016).

Access to the storage yard should be limited only to the area indicated by the authenticating system. The different areas may have physical separations and gates. Any deviation should be alerted, reported and logged as it may present a security attack.

### 2.5.6 Consequences

The advantages of this pattern include:

- Flexibility—Role Based Access Control (RBAC) allows us to accommodate several roles that participate in the system, it allows for all type of users. People performing the same tasks are given the same rights.

- Usability—easy to use by individuals that do not have technical background.

- Alerting—we can use the Alarm Monitoring and Security Logger and Auditor patterns to record all activities that are security relevant. Any deviation from normal activities will be logged and if necessary, an alert will be displayed.

- Logging—the places where the containers have been placed are registered. All transactions are logged and later audited to assure compliance with security regulations.

- Physical Damage Avoidance—loss or misplacement of containers and their contents are minimized. With accurate information on where to locate a container and where to place it, damage to the container or its contents can be averted.

- Location Tracking – logging will keep track of locating the containers.

The pattern has some liabilities:

All the mechanisms needed for security have some overhead, require maintenance and have an extra cost associated to them. Containers may have dangerous loads and physical measures are needed to detect them, such as x-rays and radiation portal monitors that may be costly.

### 2.5.7 Related Patterns

- Authenticator (Fernandez 2013). When a user or system (subject) identifies itself to the system, the Authenticator pattern allows verification that the subject intending to access the system is who or what it claims to be. As discussed in that reference, there is a variety of authentication protocols, including passwords, credentials, biometrics, and card-based authentication.

- Authorization (Fernandez 2013). Describes who is authorized to access specific resources in a system and how, in an environment in which we have resources whose access needs to be controlled.

- Role-Based Access Control (Fernandez 2013). Describes how to assign rights based on the functions or tasks of people in an environment in which control of access to computing resources is required and where there is a large number of users, information types, or a large variety of resources.

- Security Logger/Auditor (Fernandez 2013). How can we keep track of user's actions in order to determine who did what and when. Log all security-sensitive actions performed by users and provide controlled access to records for audit purposes.

- Security Patterns for Physical Access Control Systems (Fernandez et. al. 2007). Alarm Monitoring, defines a way to raise events in the system that might require special attention. Access Control to Physical Structures applies authentication and authorization to the control of access to physical units.

- Secure and Safe Port Loading Facility (Fernandez et. al. 2014). Provides the typical functions of a port loading facility (loading and unloading of containers to/from a ship) including security and safety mechanisms that can defend against all identified threats.

### 2.5.8 Known Uses

The Port of Los Angeles (The Port of Los Angeles Port Drayage) and the Port of Long Beach in Southern California, USA, are applying defenses of the type used here for their port drayage operations. We used their port drayage process as the basis for this pattern.

The Port of Miami and Port Everglades in Fort Lauderdale also apply similar defenses for their port drayage operations.

## 3. Conclusions

This type of model could be part of a Reference Architecture (RA) for cargo ports. An RA is an abstract architecture about a specific domain without implementation details. A port RA would also have ship handling (arrival and departure operations), ship manifest handling, dangerous material handling, and similar. One of these has been described, port loading facility, for the loading and unloading of containers to/from a ship. As indicated, our long-term objective is a complete reference architecture for cargo ports.

## Acknowledgements

We thank our shepherd Foutse Khomh for his useful comments.

## References


F. Braz, E.B.Fernandez, and M. VanHilst, "Eliciting security requirements through misuse activities" Procs. of the 2nd Int. Workshop on Secure Systems Methodologies using Patterns (SPattern'08). In conjunction with the 4th International Conference onTrust, Privacy & Security in Digital Business (TrustBus'08), Turin, Italy, September 1-5, 2008. 328-333.

F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal. Pattern-Oriented Software Architecture: A System of Patterns, Volume 1, Wiley, 1996.

E. B. Fernandez, "Coordination of security levels for Internet architectures," Proceedings of the 10th Intl. Workshop on Database and Expert Systems Applications, 1999, 837-841 http://www.cse.fau.edu/~ed/Coordinationsecurity4.pdf

E. B. Fernandez, J. Ballesteros, A.C. Desouza-Doucet and M.M. Larrondo-Petrie, "Security Patterns for Physical Access Control Systems", In: Barker S., Ahn GJ. (eds) Data and Applications Security XXI. DBSec 2007. Lecture Notes in Computer Science, vol 4602. Springer, Berlin, Heidelberg

E. B .Fernandez, "Security patterns in practice: Building secure architectures using software patterns", Wiley Series on Software Design Patterns, 2013.

E. B. Fernandez, Raul Monge, and Rene Carvajal, "A pattern for a secure and safe port loading facility", 10th Latin American Conference on Pattern Languages of Programs - SugarLoafPLoP 2014.

E. B. Fernandez, "Threat modeling in cyber-physical systems", IEEE Dependable Autonomic and Secure Computing, Aug. 8-12, 2016, Auckland, New Zealand

NCFRP Report 11, "Truck Drayage Productivity Guide", National Cooperative Freight Research Program, Grant No. DTOS59-06-00039, March 2011

K. Saini and S. Kaur, "Forensic Examination of Computer-Manipulated Documents using Image Processing Techniques", Egyptian Journal of Forensic Sciences, Volume 6, Issue 3, September 2016, Pages 317-322. https://doi.org/10.1016/j.ejfs.2015.03.001

The Port of Los Angeles Port Drayage, retrieved from https://www.portoflosangeles.org/, The Port of Long Beach Port Drayage, retrieved from http://www.polb.com/ Gate to Gate: What Happens When a Truck Picks up a Container?, retrieved from https://www.youtube.com/watch?v=P9IJN1yIIJ4

E. York Wallischeck, "ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure", June 2013, DOT-VNTSC-MARAD-13-01.