A Pattern for Controlled Access to a Cargo Port Terminal Physical Structure

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

Cyber-physical systems (CPSs) are systems that integrate physical processes, computational resources, and communication capabilities with the monitoring and/or control of entities in the physical world. An important type of CPS is a maritime container terminal. Maritime container terminals are facilities where cargo containers are transported between ships and land vehicles, for example trains or trucks, for onward transportation, and vice versa. Every maritime terminal performs four basic functions: receiving, storing, staging and loading for both, import and export containers. 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. The need to protect assets in buildings and to control access to restricted areas in a container terminal is a strong requirement in the cargo port design and container handling protection. A cargo port requires a specific set of functional roles that need specific controlled physical access so they can perform their functions. This pattern illustrates the core functional units of a cargo port terminal, the organization of its physical locations, and the assignment of permissions to roles to access such locations.

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: architecture patterns, cargo port terminal, container terminal, cyber-physical systems, physical access control

ACM Reference Format: V. M. Romero**,** and E. B. Fernandez, "A Pattern for Controlled Access to a Cargo Port Terminal Physical Structure", 2018. Procs. Sugarloaf PLoP'18, November 20-23, Valparaiso, Chile. 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. These systems are highly heterogenous and complex. Their inherent cross-domain architecture (physical and computational) blurs the boundaries of infrastructure ownership and operability and makes their design difficult to implement. An important example of a CPS is a cargo port. A cargo port requires a set of functional roles that need to be mapped to specific physical units with controlled access. The fact that some areas of the port may contain dangerous or valuable containers makes access control a necessity.

Since its introduction in the early 1960's, containerized transportation has rapidly taken the market for intercontinental transport. According to UNCTAD (United Nations Conference on Trade and Development) world container port throughput volumes in 2016 totaled 699.7 million TEUs (UNCTAD 2016). A TEU is the twenty foot equivalent of cargo capacity often used to describe the capacity of container ships and container terminals. This growth has put a strong pressure on ports and terminal operations to increase productivity so these containers can be handled in an efficient way. In response to the growing demand for transportation and the presence of strong competition, new investments have been made on terminal design and container handling technology as a solution for more efficient container terminals. The selection of a design for container terminals and their technology for handling containers is an important issue. A great variety of container terminals exist mainly depending on what

---

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

type of handling equipment is used in their operation, although all of the decisions on which equipment to use depend on several factors such as space restrictions, economic reasons, or even historical reasons (Andritsos 2013).

Container terminals provide many services, i.e., container loading/unloading to/from vessel and feeder ships for import or export purposes, internal container movement from ships to stacking areas and vice versa, stacking containers in dedicated areas distributed in the terminal area, container inspection for customs requirements, refrigerated containers handling and storage, etc. All the above processes need several shared and reusable resources and equipment to fulfill the tasks involved in handling and transporting containers: quay cranes, yard cranes, transport vehicles, e.g. multi-trailers or automatically guided vehicles, straddle carriers, yard stacking deposits, automatic stacking cranes or automatic storage/retrieval systems, railway tracks, human operators. All processes and operations are usually planned, scheduled, monitored, and controlled by a central supervisor and make use of information technologies, to allow fast ship operations, optimization of the usage of facilities, and to reduce lag times.

A typical modern container terminal installation includes a section for Port Security and Access Control, this incorporates the physical entrance to the terminal, video surveillance (CCTV), gates, and the infrastructure necessary to check the credentials of the maritime transportation workers that require unescorted access to the secure areas of the port. A container terminal installation also includes a Terminal Operating Center that incorporates the financial, communications, customs, security and other back office functions, an automated Cargo Container Tracking System, and an area for intermodal transportation of the containers using commercial long-haul trucks or a railway interface. The container terminal also includes cargo handling equipment at the port side and the ship side, vehicles and similar conveyances (York Wallischeck 2013). Container terminals work day and night and their amount of work depends on the quantity of containers in transit. Containers arrive at the terminal by trains, ships or trucks and are stored in the terminal yard. Then, they leave the terminal by the same means to reach their final destination. Remote crane operations are becoming more popular in yard operations and in ship-to-shore cranes. A detailed description of the operations in a container terminal can be found in (Rida 2014).

The system design of a physical access control system for a container terminal is different from a traditional access control in many ways. Such access control system must be able to manage access and area control, entrance permits and ID cards, employees of the port, terminal staff, access to customs and the actual terminals, trailers, trains, trucks, ship crews, maintenance crews, emergency vehicles and personnel (just to name a few). Furthermore, at any given moment during the day or night, there are tens of millions of dollars of cargo equipment on the premises and there can be competing terminals with highly sensitive business information located next to each other (York Wallischeck 2013). Each port also has a variety of specific needs depending on the International Ship and Port Facility Security (ISPS) code (International Maritime Organization 2017). However, the authorization rules are similar to IT systems (Fernandez et al. 2007).

We present a pattern to represent a controlled access framework for a cargo port terminal, the organization of its physical locations and the assignment of permission to individuals or roles to access such locations. This is a composite pattern that combines an instance of the Assignment pattern (Fernandez et al. 2005) and an instance of the Physical Access Control pattern (Fernandez et. al. 2007). Our audience includes container terminal systems designers and developers as well as designers of applications that need to run in these systems. We use the template of (Buschmann et al. 1996) to present our pattern.

This pattern is part of our work on building a Reference Architecture for cargo ports. Figure 1 shows how our previously published patterns, represented by colored dashed lines, are used to model a cargo port. The red dashed lines represent the pattern for the loading and unloading of containers to/from a ship at a cargo port facility, “Secure and Safe Port Loading Facility” (Fernandez et. al. 2014). The purple dashed lines represent the pattern for the secure delivery of containers at a cargo port, “Secure Cargo Port Drayage” (Romero and Fernandez 2018). The blue dashed lines represent the pattern for ship arrivals and departures. This new pattern, “A Pattern for Controlled Access to a Cargo Port Terminal Physical Structure” presented in the following chapters, will be using some of the classes presented in this partial reference architecture, specifically: Port, Quay, Crane and Storage. Patterns can have overlapping classes.

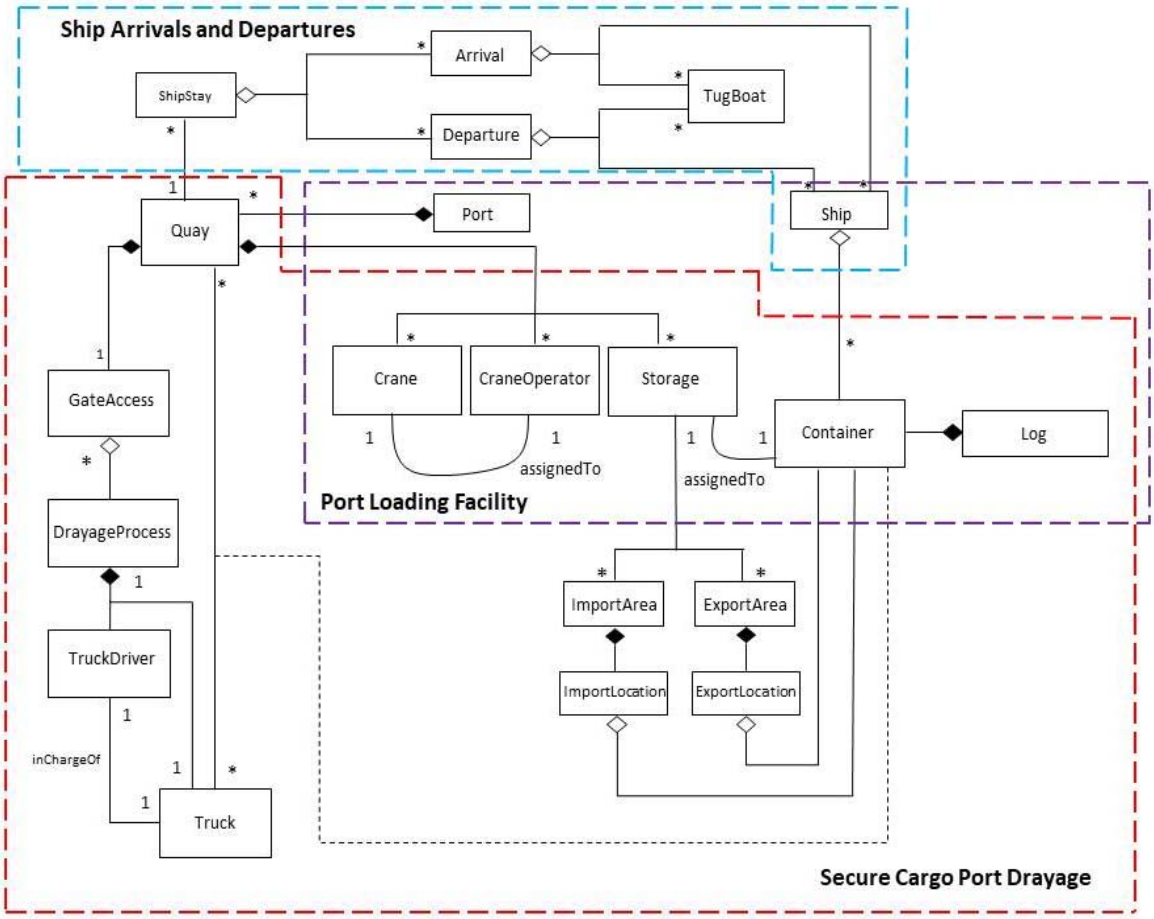

Figure 1. Partial Reference Architecture for a Cargo Port

2. CONTROLLED ACCESS TO A CARGO PORT TERMINAL PHYSICAL STRUCTURE

2.1 Intent

Describe the mapping of a cargo port's functional units to its physical locations and define the allocation of the rights of the individuals or roles associated with these units to access such locations.

2.2 Context

Physical locations are defined by zones. A zone is a physical unit that can be identified, and to which access can be controlled. A zone may contain other zones. An example of one of the zones in the cargo port terminal is the remote crane operations station. The cranes are being fitted with advanced automation and remote control. Although crane operations in the future may have no "physical distance", i.e., they can be located in any part of the world, nowadays most control rooms are located within the cargo port terminal premises. Figure 2. shows an example of a physical location zone A, this zone is an area composed of smaller zones zone 1 and zone 2, which may be restricted in access. Zones W, X, Y and Z are the workstations for the crane operators who remotely carry out the loading and unloading operations in the container stack and may also be restricted in access by operator. These are all located in Zone 1 with the same access for all the operators of W, X, Y and Z. Zone 2 in this example only has one workstation V. The areas shaded in blue depict entrance to the specified zones. The access control system should

be able to deal with nested restricted rooms and workstations (for this example). In other zones of the cargo port, it may be storage areas.

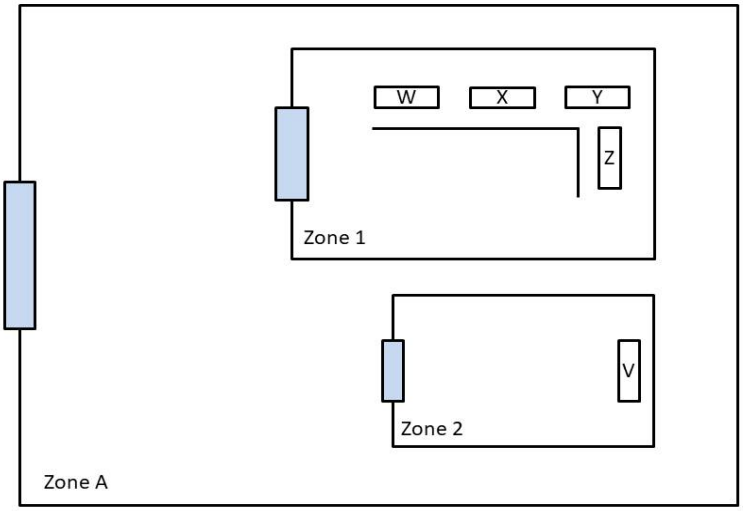

Figure 2. Physical Location in Remote Crane Operations Station

2.3 Problem

Some zones may contain dangerous or very valuable materials; others may contain critical functions. Access to these zones must be restricted to specific roles or individuals, otherwise we can have thefts and potential disruption.

2.4 Forces

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

- *Flexibility*—The description of the physical structure should be flexible and scalable. The physical units may change their functions, within restrictions, and we may need more physical units of some type.
- *Security* – Access to the physical units, including subunits, needs to be controlled dynamically (i.e. provide or deny access at any given time), and with additional restrictions (time, date, id…) when needed.
- *Logging and Auditing* – We need to keep track of who entered each area and when. Logs should be audited at regular intervals to detect suspicious activity.
- *Alarm and Alarm Monitoring* – Any attempt to access a building, container handling equipment or a zone in the terminal without proper permission must produce an alarm and should be logged. Any attempt to use an invalid credential to access a zone in the terminal must also produce an alarm and should be logged and reported to interested parties.
- *Boundaries* – The boundaries of the zones must be clearly defined and access to them enforced.

2.5 Solution

Map operational functions to available zones. Clearly define the boundaries of the zones in a container terminal and only provide access to them depending on roles and operational needs, including content-dependent access. Allow dynamic definition or redefinition of access control policies.

If access to a zone is given, access to its component zones is inherited. On the other hand, access to some specific zones can be given only to specific roles, overriding inherited accesses.

An example of a zone in a cargo port terminal may be the Storage Area zone where the containers are parked, some restrictions may include access to only shuttle trucks and assigned drayage drivers and their trucks, and only at specific dates and times. Some containers may be further restricted.

2.5.1 Structure

The class diagram of Figure 3, shows the classes in our cargo port terminal model functional units. The classes in blue, Port, Quay, Crane, Storage, ImportStorage and ExportStorage represent the functional aspects of the port structure; the classes in yellow, Zone, Building, ContainerZone and CraneZone represent the zone aspects. The class Port represents the cargo port. It aggregates multiple objects of class Quay, each representing a berth. Crane represents all the types of cranes in the terminal. Storage represents the different areas to park the containers. Class Zone represents the abstract common characteristics of all the zones; e.g., the CraneZone represents the area where the cranes are operating, ContainerZone is the area for storing the containers. Every access to a zone is recorded by the Security Logger/Auditor and authenticated by the Authenticator. The Reference Monitor enforces the authorization rules for each zone. An Alarm is associated with each zone. Roles CraneOperator, CraneScheduler, StorageManager, QuayEmployee are associated with their corresponding functional units Crane, Storage and Quay respectively. Similarly, for the other roles. Note that these are a subset of all the possible roles in a cargo port. Each Role is given a set of Rights that describe their access to physical units. These rights may have additional constraints defined by content-dependent access control rules.

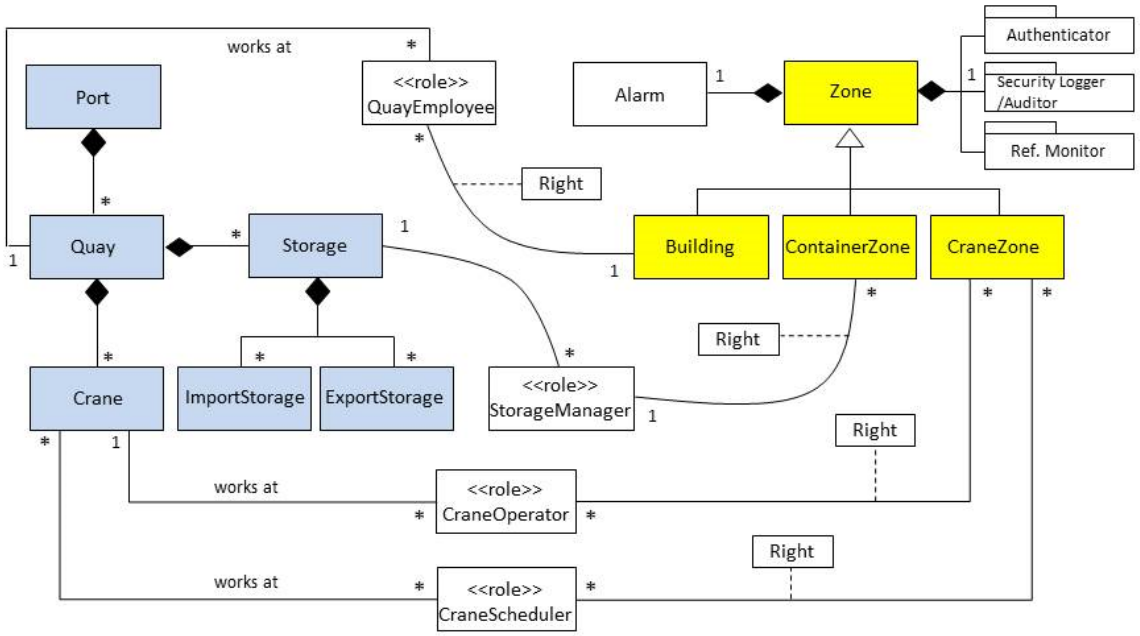

Figure 3. Class Diagram of Cargo Port Terminal Structure

2.5.2 Dynamics

We describe the dynamic aspects of the use case Request Access from a Role to a Zone (Figure 4).

Other use cases include: Assign Controlled Access from a Role to a Zone, Remove Controlled Access from a Role to a Zone, and Exit a Zone.

Use Case: Request Access from a Role to a Zone.

Summary: A Person from a role requests access to a zone.

Actors: Person

Precondition: The Reference Monitor has rules defining physical access for roles and each Zone stores authentication information.

Description:
1. A Person requests access for a zone by indicating her id.
2. The Zone authenticates the Person
3. If successful, the Zone checks the Authorization of the Person to access this Zone.
4. It also checks for any constraints.
5. The Zone opens its door to allow the Person to enter.
6. The Person is notified that it can enter, including specific constraints (time limit, forbidden actions, etc).
7. The Zone writes the Log (part of the Security Logger/Auditor) indicating the Person has entered.

Postcondition: A Person of a given role is allowed to access a physical location at the cargo port terminal physical structure.

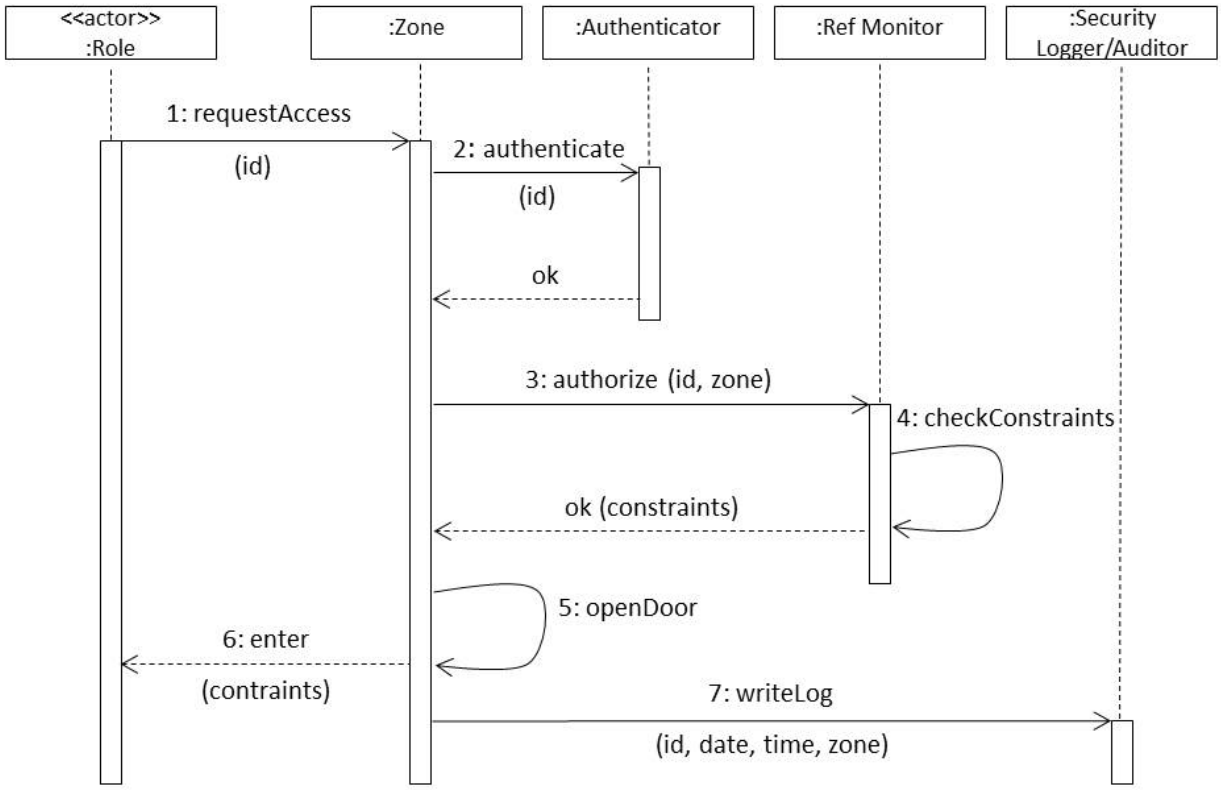

Figure 4. Sequence diagram for use case Request Access from a Role to a Zone

2.5.3 Implementation

This pattern can be implemented for all existing and new container terminals. It presents all the necessary elements regardless of cost and size.

There is variety of possible implementations to take advantage of technological advances. Roles must be defined using role engineering (Verde et al. 2012).

Remote crane operations are becoming more popular in yard operations and in ship-to-shore cranes. The cranes are being fitted with advanced automation and remote control.

2.5.4 Known Uses

Ports in Damman Saudi Arabia, Sohar Oman, Amsterdam and Rotterdamn in The Netherlands and Basra Irak have deployed remotely controlled gantry cranes with access control at their terminals (HutchisonPorts 2018).

The Port of Los Angeles (The Port of Los Angeles Port Drayage 2018) and the Port of Long Beach (The Port of Long Beach Port Drayage 2018) in Southern California, USA, have been used as models for our design of a container terminal.

The ports of Miami (Port of Miami 2018), Port Everglades (Port Everglades Security 2018), and West Palm Beach (Port of Palm Beach 2018) in Florida, USA, implement controlled access to their terminals.

The port of Hong Kong has recently installed remote controlled gantry cranes at its Kwai Tsing container terminal 9 North.

(Marti-Soberon et al. 2014) describe automation facilities in the Port of Valencia, Spain.

2.5.5 Consequences

The advantages of this pattern include:

- Flexibility – Adding access rights to a new role only requires to add another object of an existing class. Each right may have content-dependent constraints. Zones can be reconfigured.
- Security – The boundaries of each zone are clearly defined and access can be controlled based on individuals or roles to access those locations. Each zone may have subdivisions for finer control. We usually apply a closed system policy where everything is closed unless explicitly permitted, so we only need positive access rules, although negative rules can be useful to define exceptions.
- Logging and Auditing – We can have a Security Logger/Auditor pattern to record every access with later auditing.
- Alarm and Alarm Monitoring – An alarm will be raised for any attempt to enter an area or zone without proper permission or invalid credentials. Alarms will be logged. Interested parties will be informed when alarms are raised.
- Boundaries – The boundaries of the areas of access are defined by zone containment.

The disadvantages of this pattern include:

- Complexity and Cost – All the mechanisms needed for the monitoring and control of access to all the different areas, such as cameras and sensors, have an extra cost and add complexity.
- Performance overhead – Logging each device and its activity in real time may cause network overload and delays in accessing the zones.

2.5.6 Related Patterns

- 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 identified threats.

- Secure Cargo Port Drayage (Romero and Fernandez March 2018). Provides the typical functions and security mechanism for the secure delivery and pick up of containers at a maritime cargo port.

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

- Constrained Resource Assignment Description (Fernandez et al. 2005). Describes how to perform assignments of resources to subjects such as roles or individuals.

- Reference Monitor (Fernandez 2013). This pattern describes how to force authorizations when a subject requests a protection object and provide the subject with a decision.

- Security Logger/Auditor (Fernandez 2013). This pattern describes how to keep track of users' actions in order to determine who did what and when. It logs all security-sensitive actions performed by users and provides controlled access to records for audit purposes.

3. CONCLUSIONS

We have presented a pattern for defining controlled access to the zones of a port based on role functions. This pattern can be used to manage access to such locations by selecting security policies for the system as well as expand a role base access control model to include physical objects as protection objects.

We will continue to expand our Reference Architecture (RA) by considering new Use Cases for our Cargo Ports. We will also analyze and identify threats in its Use Cases and create Security and Misuse Patterns to stop and describe these threats. We will apply these security patterns to our RA and build a Security Reference Architecture (SRA) for Cargo Ports. We intend to validate our models by inspection of several ports.

ACKNOWLEDGEMENTS

We thank our shepherd Eduardo Fernandez-Medina Paton for his valuable comments.

We also thank the participants of Group A of the SugarLoaf PLoP of 2018 who provided further useful comments

REFERENCES

F. Andritsos, "Port Security & Access Control A systemic approach", European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen. Conference Paper · July 2013 DOI: 10.1109/IISA.2013.6623728

A. Boulmakoul, M. Rida, "Discrete event simulation component specification for container terminals operational management", In: Proceedings of the 2nd IEEE ISSPIT (International Symposium on Signal Processing and Information Technology), Marrakesh, Morocco, December, 18-21, 2002, pp. 266-271.

E.B.Fernandez, Tami Sorgente, and M. VanHilst, "Constrained Resource Assignment Description Pattern". Proceedings of the Nordic Conference on Pattern Languages of Programs, Viking PLoP 2005, Otaniemi, Finland, 23-25 September 2005.

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", Procs. of the 10th Latin American Conference on Pattern Languages of Programs - SugarLoafPLoP 2014.

HutchisonPorts, https://hutchisonports.com/en/media/stories/implementation-of-remote-control-operations-in-full-swing-at-hutchison-ports/ (last retrieved Sept. 30, 2018)

International Maritime Organization 2017, http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx

A.M. Martín-Soberón, ArturoMonfort, Rafael Sapina, NoemíMonterde, DavidCalduch, "Automation in port container terminals", Procedia, vol. 160 (2014), 195-204, https://www.sciencedirect.com/science/article/pii/S1877042814062326 (last retrieved Sept. 30, 2018)

Port Everglades Security, http://www.porteverglades.net/about-us/security/ (last retrieved Sept. 30, 2018)

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 (last retrieved Sept. 30, 2018)

Port of Los Angeles Port Drayage, retrieved from https://www.portoflosangeles.org/ (last retrieved Sept. 30, 2018)

Port of Miami, http://www.miamidade.gov/portmiami/cargo-security.asp (last retrieved Sept. 30, 2018)

Port of Palm Beach, https://www.portofpalmbeach.com/141/Security (last retrieved Sept. 30, 2018)

M. Rida, "Modeling and Optimization of Decision-Making Process During Loading and Unloading Operations at Container Port", Arab J Sci Eng (November 2014) 39: 8395. https://doi.org/10.1007/s13369-014-1328-8

V. M. Romero and E. B. Fernandez, "A Pattern for Secure Cargo Port Drayage", Procs. of the 7th Asian Conference on Pattern Languages of Programs, Asian PLoP'18, March 1-2, Tokyo, Japan.

V. M. Romero and E. B. Fernandez, "Building a Reference Architecture for Cargo Ports using Patterns", Proceedings of the 16th Latin American and Caribbean Conference for Engineering and Technology, July 18-20, 2018, Lima, Peru.

UNCTAD Review of Maritime Transport 2016, https://unctad.org/en/PublicationChapters/rmt2016ch4_en.pdf

N.V. Verde, J. Vaidya, V. Atluri, A. Colantonio,"Role engineering: From theory to practice", Procs. CODASPY'12, 2nd. ACM Conf. on Data and Applic. Security and Privacy, 181-192, ACM 2012.

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.