Proceedings of the 19th International Symposium on the
Packaging and Transportation of Radioactive Materials
PATRAM 2019
August 4-9, 2019, New Orleans, LA, USA

MULTI-MODAL CHALLENGES IN THE INTERNATIONAL TRANSPORT OF NUCLEAR AND RADIOACTIVE MATERIALS (THE ONLY INTERESTING PARTS OF A SYSTEM ARE THE INTERFACES.)

Paul Singley[1,2]
Oak Ridge National Laboratory

Marc Fialkoff
Oak Ridge National Laboratory

ABSTRACT

There is an old systems engineering aphorism: the only interesting parts of a system are the interfaces. In the System of Systems that comprise international shipments of nuclear or radioactive material, the intermodal transfer points contain some of the most security critical interfaces.

Transportation of nuclear and radioactive material exposes these materials to the most risk for malicious acts. Unlike physical facilities, securing radioactive and nuclear materials during transport requires that many different organizations including operators, regulatory agencies, and security agencies work together to ensure the security of the cargo. A major security challenge for international movement of nuclear and radioactive material is the need to use multiple transport modes. Ensuring security of these cargos as they move through intermodal facilities, some of which may take multiple hours, or days, depending on operational constraints at the yards, ports, or other facilities, is a major operational and regulatory challenge. Especially in the international context, ensuring the security of material in transport through in-transit countries and coordinating transport activities across jurisdictions can lead to challenges as to whose security plan controls, whose transport regulations are to be followed, and how might plans need to be adjusted to adapt to in-transit conditions and ultimately how to ensure cargo security. This paper introduces and highlights selected challenges in the multi-modal movement of nuclear and radioactive material in transport. While the paper will address selected challenges in coordination of stakeholders and resources, activities at intermodal facilities, and other selected issues, this does not address all the challenges, rather it brings issues forward and suggests solutions and strategies for enhancing the security of nuclear and radioactive material transported internationally.

INTRODUCTION

Transport is the most vulnerable part of the life cycle for nuclear and radioactive materials, it is also the most complex. Regardless of the material being transported, the need for multiple

---

[2] The authors would like to acknowledge the support of the Department of Energy, Office of Radiological Security (ORS) for funding support of this paper.

modes of transport to complete the trip increases the complexity, both logistically and ensuring the material stays secure from possible theft or malicious acts. Multimodal transport operations require interface between the transport companies handing off the freight to its subsequent mode. In doing so, this hand-off may change the regulatory environment (what law the shipment is operating under), may change the carrier (the stakeholder(s) involved in the transport), and/or may change the handling requirements (how to move the material from a truck to a rail car or from a truck or rail car to a hold in a vessel). When adding the security challenges associated with nuclear and other radioactive materials, the concerns for theft, sabotage, or diversion of material during transport increase. When moving material internationally, ensuring continuity of security through intermodal transfers can highlight weaknesses at the interfaces.

When describing interfaces in multimodal transport, we refer to the intermodal terminals, including airports, seaports, and surface intermodal terminals between truck and railway. At these intermodal points, there is a convergence of people, processes, technologies, and security that if not focused on, can lead to breaks in the security chain. With this increased complexity, how do security managers, transport planners, security professionals, carriers, and shippers develop and think about security across a multimodal transport system for nuclear and radioactive materials?

This paper builds upon previous work developed by [1] applying the System of Systems (SoS) framework to transport security of nuclear and other radioactive materials. While [1] focused primarily on the supply chain of radioactive materials broadly, this paper focuses on the interfaces, namely the challenges and threats for transport security at intermodal locations. Building off previous SoS research for maritime transport [2][3], this paper investigates the interfaces for multimodal transport of radioactive and nuclear material. While using a seaport as an example, the paper also addresses other intermodal points like the transfer between truck and rail systems. The paper will discuss transport as an SoS but focus on the interaction at the intermodal terminals and provide examples of security interfaces between multiple transport systems. The discussion will subsequently shift towards identifying threats at intermodal facilities and provide mitigation strategies where appropriate. Ultimately the goal of this paper is two-fold: First, to further develop the System of Systems framework to radioactive material security and second, to identify potential weaknesses with the intermodal element of transport and highlight how applying a SoS approach can provide opportunities to strengthen the interfaces for multimodal transport.

TRANSPORT AS A SYSTEM OF SYSTEMS

Transport, in general, is complex. Transport can involve multiple modes of conveyance, requires multiple stakeholder interactions (shippers, carriers, receivers, competent authorities), and may involve multiple legal regimes (transboundary and international legal regimes). Previously, [1] applied a System of Systems framework to the whole supply chain for radiological material transport, as represented in Figure 1.

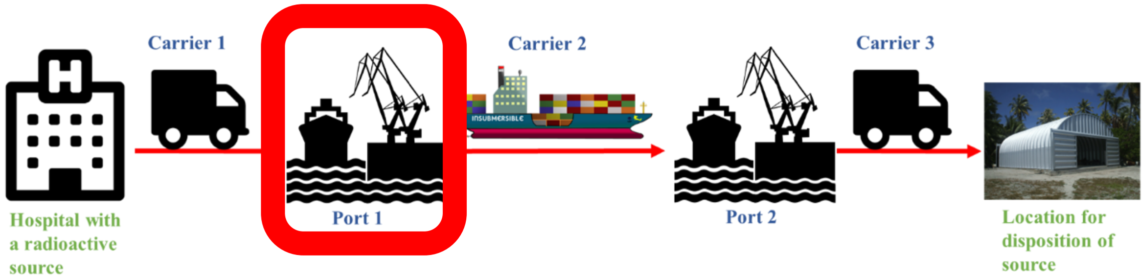

Figure 1. Movement of radioactive material from shipper to receiver using multiple modes of transportation. Source: [1].

Focusing on Port 1 in Figure 1, the Port alone is a system, with various functional areas, including the infrastructure, the people, processes, licensing, safety and security. Similarly, the same attributes can be applied to Carrier 1 (the truck entering the port) and Carrier 2 (the vessel transiting between Port 1 and Port 2). As each of these are a system unto themselves, the question becomes, how do multiple systems interact to ensure continuity of operations, and of importance for this paper, continuity of security operations for radioactive and nuclear material?

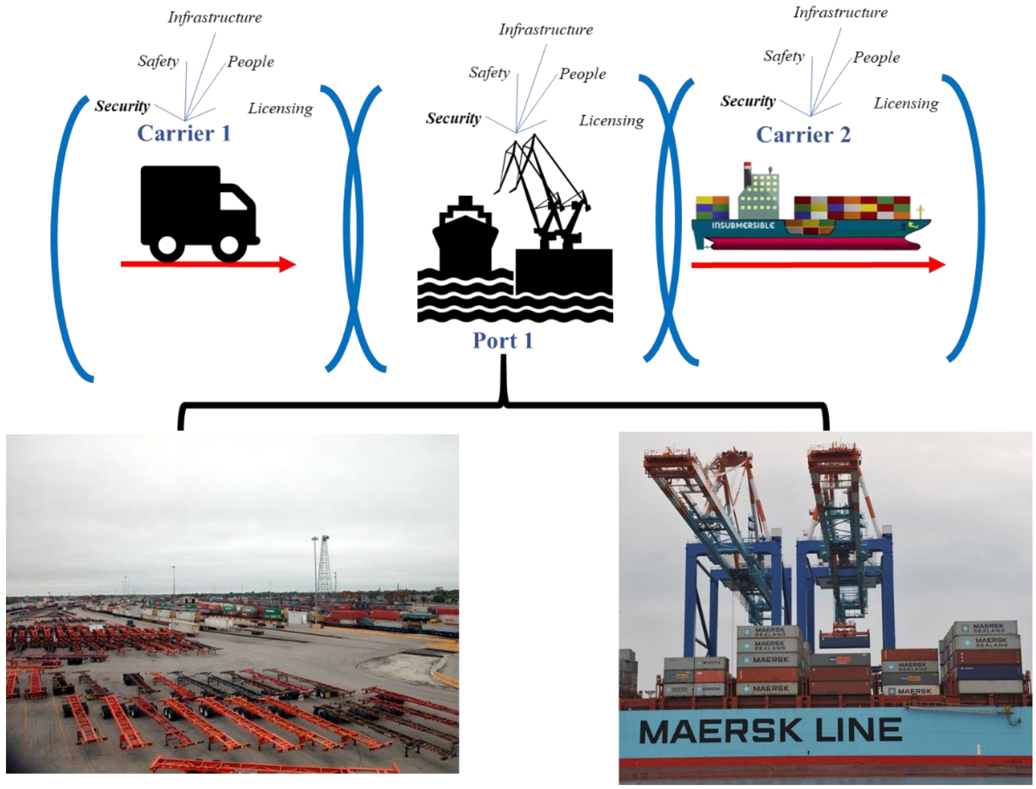

Figure 2: Interfaces for Multimodal Transport System of Systems. Source: Authors.

As Figure 2 illustrates, Port 1 is interacting with Carrier 1 and Carrier 2 by receiving material from Carrier 1 and subsequently transferring the material to Carrier 2 for ocean-going transport. The blue brackets overlapping at each boundary represent interfaces between the Systems. Those interfaces include, but are not limited to:

- ***Regulatory*****:** within the context of transport, when an intermodal movement occurs, different legal systems may apply. For example, when transferring cargo, including Class 7 material from truck to a maritime vessel, different regulatory regimes may apply. In the context of the United States Code of Federal Regulation, these different regulations under Title 49 include Part 172 (carriage by highway requirements) and Part 176 (carriage by vessel requirements) [4][5]. Internationally, there are multiple transport conventions, including the Convention for the Physical Protection of Nuclear Material [6], the Safety of Life at Sea (SOLAS) Convention [7], and the International Maritime Dangerous Goods (IMDG) Code [8].

- ***Security:*** at each stage of transport, depending on the categorization of materials, security may accompany the material. When material enters an intermodal facility, there may be pauses when security "starts" and when it may subsequently "end". Especially when multiple security forces (public or private are involved), there is an increased risk of a security gap that can be exploited. This highlights the need for communication and coordination amongst all security personnel is essential to avoid miscommunications or misunderstandings during intermodal transfers.
- ***Physical Cargo handling:*** with intermodal transfers, as illustrated in Figure 2, extra pieces of equipment are used to transfer containers, casks, or other packages from one mode of transport to another. These pieces of equipment are usually operated by a driver, such as Rubber Tire Gantries, Overhead Cranes, or Drayage Vehicles. In these instances, and many others, the potentiality for theft or diversion could increase due to more individuals "touching" and moving the package from one mode to another which increases the opportunity for an insider to access the shipment.
- ***Roles and Responsibilities:*** Within multimodal transportation, especially at intermodal transfer locations, there is potential for overlap in responsibilities. For example, maritime security officers may be present at facilities and on vessels in accordance with international law. At the same time, trucks and other vehicles may have transport security personnel accompanying a shipment into a port or other intermodal facility. At that point, it is imperative that all individuals know where their responsibilities start and end. Outside the security context, many individuals are involved in shipping materials (freight forwarders, shippers, carriers, third party logisticians). Understanding their security roles and responsibilities will help to avoid overlap or miscommunications, especially during a movement. Answering who is in charge at any given moment illustrates the complexity of transporting radioactive material securely.

THREATS TO INTERMODAL TRANSPORT

At the interfaces of intermodal transport is the place where the most activity occurs. Airports, seaports, and rail terminals are a hive of activity. With multiple modes of transport loading and unloading cargo and the movement of various people within facilities, the potentiality of a theft, sabotage, or loss of cargo increase dramatically. This section will briefly discuss three possible threats to intermodal transport.

- **Cargo Theft**

According to the Federal Bureau of Investigation, cargo theft is defined as:

> The criminal taking of any cargo including, but not limited to, goods, chattels, money, or baggage that constitutes, in whole or in part, a commercial shipment of freight moving in commerce, from any pipeline system, railroad car, motor truck, or other vehicle, or from any tank or storage facility, station house, platform, or depot, or from any vessel or wharf, or from any aircraft, air terminal, airport, aircraft terminal or air navigation facility, or from any intermodal container, intermodal chassis, trailer, container freight station, warehouse, freight distribution facility, or freight consolidation facility [9].

Cargo theft is a global issue, with [10] recently publishing a report of cargo thefts globally. According to Figure 3, the most vulnerable mode of transport is truck, followed by facility theft, rail, van, and other modes of transport.

Truck	76
Facility	19
Rail	3
Van	1
Other	1

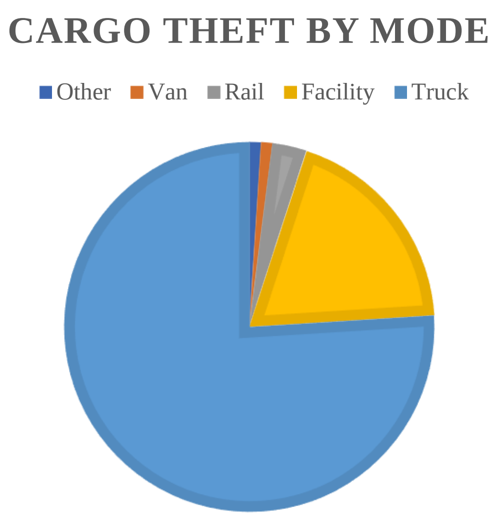

Figure 3: Cargo Theft by Mode. Source: [10].

In contrast to mode, Figure 4 compares the percentage of cargo theft by location, with in transit shipment theft occurring 38% of the time and theft at warehouse around 19% [10].

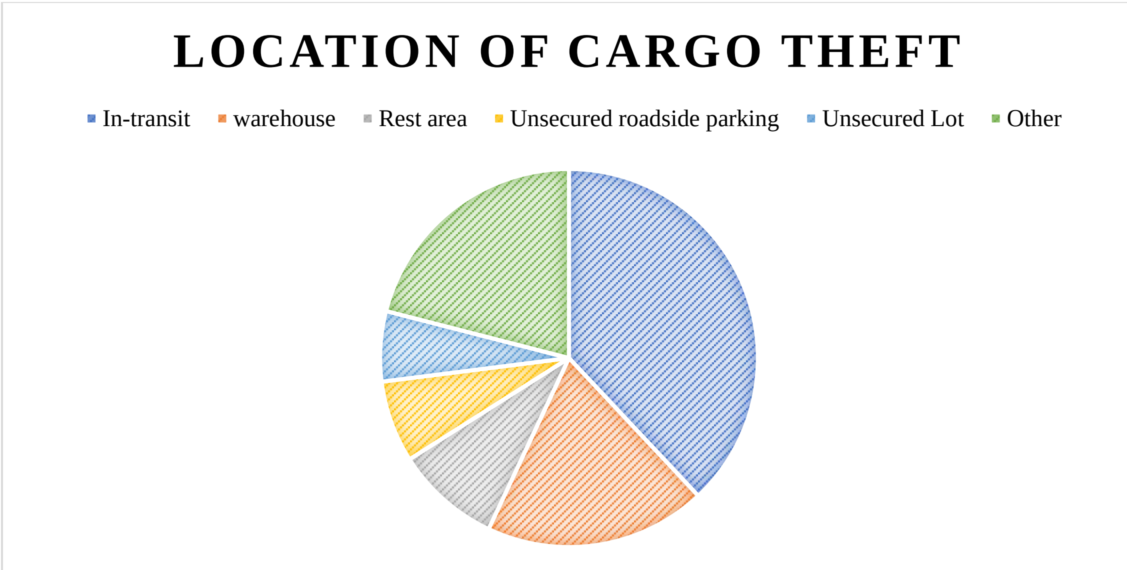

Figure 4: Cargo Theft by Location. Source: [10].

- **False shipping papers**

Another possible threat to intermodal transport is the forging of shipping papers, also known as fraudulent Bills of Lading. In those instances, the reason for forging Bills of Lading is to steal the cargo. In the maritime sector, a possible scenario for a forged Bill of Lading is as follows, as reported by [11]. In the scenario, an individual creates a fake set of Bills of Lading that look genuine in an attempt to take delivery of the cargo in advance of the genuine receiver. In the scenario presented by [11], the use of insider assistance to provide key information, including the real Bill of Lading, highlights the need for human reliability and trustworthiness programs across the supply chain. In these scenarios, the lessons learned include ensuring clear chain of custody for both the cargo and Bill of Lading. Additionally, making sure shippers, carriers, and receivers remain in constant communication to ensure cargo is transferred and verified at each step of the process, including intermodal transfer points.

- **Rogue crane**

One final threat is a threat at facilities, specifically the misuse of equipment to transfer cargo outside of its stream of commerce. In this "rogue crane" scenario, a piece of equipment like a rubber tire gantry (as shown in Figure 5a and 5b) could be used to pick up a package and place the package on a drayage vehicle or vehicle that is meant to steal the cargo.

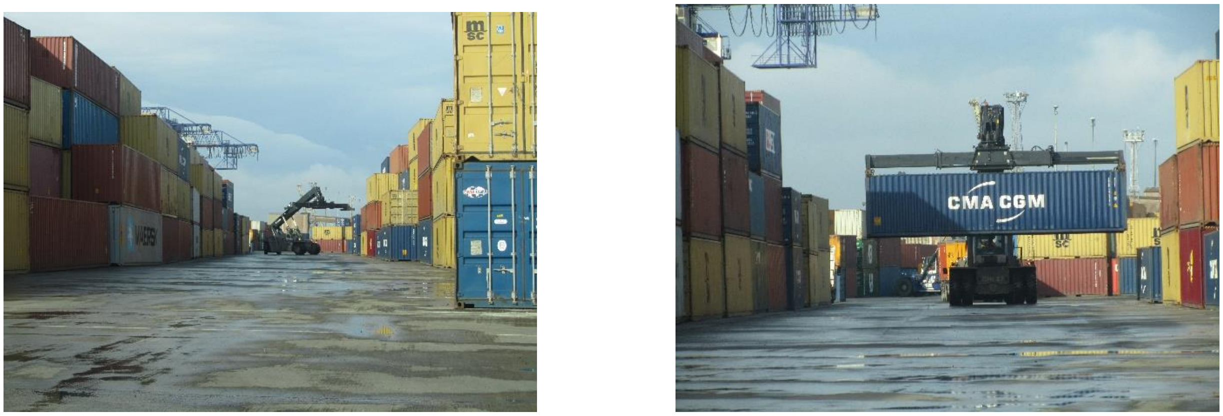

Figure 5 a & b: Rubber Tire Gantry at a Port. Source: Author

The challenge with these pieces of equipment are they can be moved through a facility with relative ease. As discussed previous, the use of an insider to take control of the crane and know which container or package to pick up can lead to cargo diversion or theft. In contrast, other cranes that are fixed guide-way cranes as illustrated in Figure 6 have the potential for cargo diversion if the crane is operated by an insider and lowers the container onto a chassis operated by an accomplice. In that case, the diversion may be more noticeable by port personnel as the fixed guideway crane is more prominent than a rubber tire gantry.

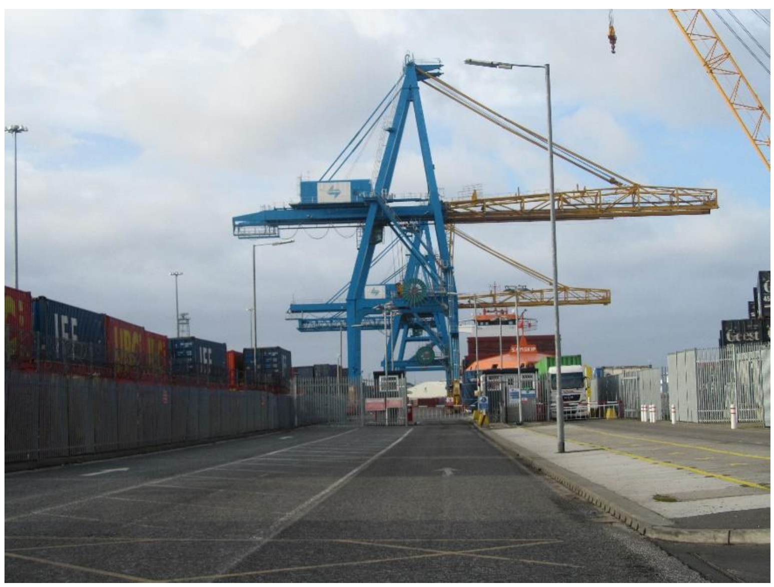

Figure 6: Fixed Guideway Crane. Source: Author.

MITIGATION METHODS AND NEXT STEPS

As with most security enhancement the human element is both the most vulnerable and most useful part of the system. As this paper discusses, humans are a part of every diversion scenario. Of course, humans are the critical part of all security systems. Training and vetting of the personnel responsible for transport security form the foundation of any robust transport security environment.

In many, if not all, of the examples discussed in the previous sections, the use of an insider, either passive, unwittingly, or with intent, highlights the need for human reliability and trustworthiness programs to ensure seaport and airport personnel have been properly vetted.

In the intermodal context, processes and procedures for ensuring the security of cargos should be developed and coordinated among all of the systems. Such coordinated process and procedures form a strong basis to ensure continuous robust security as cargo transit the regulatory, commercial, and physical interfaces present at an intermodal transfer. This coordination requires strong communication between the transport systems and communication amongst government stakeholders; one primary tool for this is a robust Transport Security Plan.

In addition to the human element there are technological elements that can be deployed to assist the security system to detect and react to cargo diversion. The primary technology to consider are cargo location tracking systems particularly those systems that allow geo-fences to be set. These systems can provide a notification if a cargo is moved away from an authorize location, like a port. The notification allows the transport monitoring center to assess if the movement is part of the authorized transport or if an attempt at cargo diversion is in progress.

REFERENCES

[1] SINGLEY, P.T.; FIALKOFF, M.R.; TOTH, W.J.; ANDERSON, K.K., Developing a Secure Logistics System for Radiological Material Transport. Presented at the IAEA Radiological Security Conference, December 2018, Vienna.

[2] HARRALD, J. R., STEPHENS, H. W., & VAN DORP, J. R, A framework for sustainable port security. *Journal of Homeland Security and Emergency Management*, *1*(2), 1-13, 2004.

[3] MANSOURI, M., GOROD, A., WAKEMAN, T. H., & SAUSER, B., Maritime transportation system of systems management framework: A system of systems engineering approach. *International Journal of Ocean Systems Management*, *1*(2), 200-226, 2009.

[4] 49 CFR § 174, 2019.

[5] 49 CFR § 176, 2019.

[6] CONVENTION FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL, International Atomic Energy Agency, 1987.

[7] SAFETY OF LIFE AT SEA CONVENTION, International Maritime Organization, 1974.

[8] INTERNATIONAL MARITIME DANGEROUS GOODS CODE, International Maritime Organization, 2018

[9] CARGO THEFT, Federal Bureau of Investigation, Crime in the United States, 2015. https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/additional-reports/cargo-theft/cargotheft-report_-2015-_final

[10] BSI & TT Club, Cargo Theft Report, 2018, https://www.ttclub.com/fileadmin/uploads/tt-club/Documents/BSI_TT_ClubCargoTheftReportH1_2018_FinalRev.pdf

[11] MAREX, 4 Cargo Frauds to Watch Out For, The Maritime Executive, 2014, https://www.maritime-executive.com/article/4-Cargo-Frauds-to-Watch-Out-For-2014-01-30