Massachusetts Institute of Technology
Engineering Systems Division

SAND2015-2159PE

Beyond a Series of Security Nets:

Applying STAMP & STPA to Port Security

Adam D. Williams*

March 2015

4th STAMP Workshop
Massachusetts Institute of Technology||Cambridge, MA

*SAND2015-XXXX

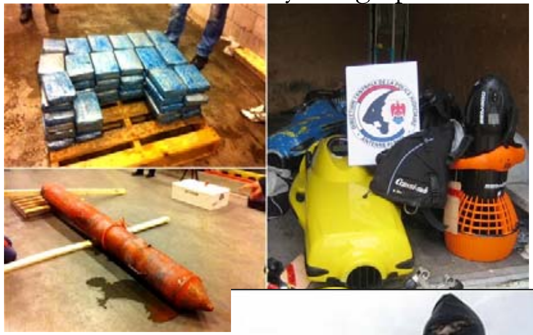
Unlimited Release. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Motivation

Range of threats

- WMD smuggling
- Weaponized LNG ships
- Cyber attacks

Courtesy: telegraph.co.uk



Philosophical Transition:

- From anti-smuggling to anti-terrorism post 9/11

Courtesy: safety4sea.com

Courtesy: nit.org

Copyright: A. Williams

Need new approach to meet US port security needs

- 100% scanning mandate expensive/ineffective
- Coordinate multi-entity intel gathering

Outline

Motivation

Current Approaches

A New Approach

Applied to Port Security

Conclusions

Summary

The **views expressed herein are those of the author** and do **NOT** reflect the official policy, position or recommendation of Sandia National Laboratories, the National Nuclear Security Administration, the Lockheed Martin Corporation, the U.S. Department of Energy or the U.S. Government.

History of Port Security Legislation

9/11

Emphasis = ‘anti-smuggling’

- Port & Waterways Safety Act of 1972

Emphasis = ‘anti-terrorism’

- Maritime Transportation Security Act (MTSA) of 2002
- Coast Guard and Maritime Act of 2004
- Intelligence Reform and Terrorism Prevention Act of 2004
- National Strategy for Maritime Security (2005, 2013?)

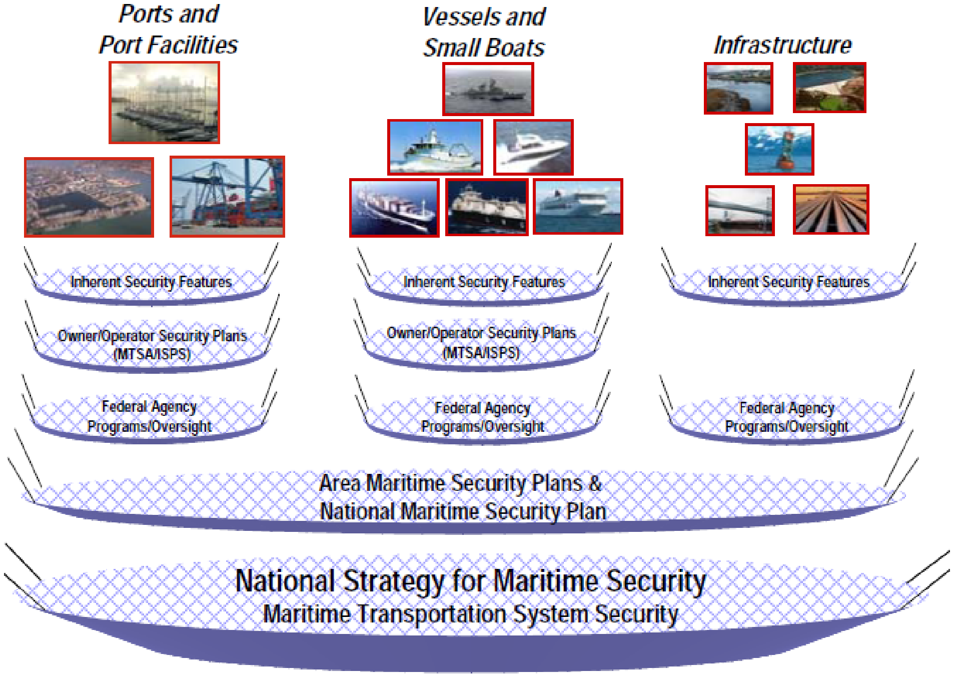
USG Port Security Programs

Program	Sponsoring Stakeholder	Port-Security Goal
International Ship and Port Facility Security (ISPS) Code	International Maritime Organizations (IMO)	Informs security measures through standardized assessments of vulnerabilities, risks, threats & consequences (Helmick, 2008; International Maritime Organization, 2012).
Customs-Trade Partnership Against Terrorism (C-TPAT)	Customs and Border Patrol (CBP)	Incentivize enhanced supply chain security with expedited cargo processing through U.S. ports (Frittelli, 2005; O'Connell, 2009)
Container Security Initiative (CSI)	Customs and Border Patrol (CBP)	Pre-screen 'high-risk' U.S.-bound containers (U.S. Customs & Border Protection, 2011)
Secure Freight Initiative	Department of Homeland Security (DHS) & Department of Energy (DOE)	Scan U.S.-inbound containers for radiation & information risk factors at foreign ports (U.S. Department of Homeland Security, 2012)
Operation Safe Commerce	Transportation Security Administration (TSA)	Pilot project to verify the contents & physical integrity of a container from origin to destination (Frittelli, 2005)
Megaports Initiative	National Nuclear Security Administration (NNSA)	Provides a multilayered network to detect nuclear or radiological materials at key international ports (U.S. National Nuclear Security Administration, 2010)
Maritime Domain Awareness (MDA)	Multi-stakeholder	Provides multi-source information flows that analyze behavioral patterns to more quickly identify potential threats (Frittelli, 2005)

Current Approaches

'series of security nets that provide layers of protection necessary to effectively manage security risks' [U.S. DHS, 2005a., p.3]

- Implementation ranges from **voluntary programs** to **bilateral government** agreements (previous table)
- Similarly varying analytical approaches
  - Risk management to **minimize R = P x C** [Akhtar, Bjørnskau, & Veisten, 2010; Ghafoori & Altiok, 2012]
  - **Game theoretic optimization** of purchasing equipment to meet 100% cargo scanning mandate [Gkonis & Psaraftis, 2010]
  - **Monte Carlo simulations** to estimate risk reductions [Akhtar, Bjørnskau, & Veisten, 2010]
  - **Econometric model optimization** for sensor placement around a port [Burns 2013]



Ports and Port Facilities

Vessels and Small Boats

Infrastructure

Inherent Security Features

Owner/Operator Security Plans (MTSA/ISPS)

Federal Agency Programs/Oversight

Inherent Security Features

Owner/Operator Security Plans (MTSA/ISPS)

Federal Agency Programs/Oversight

Inherent Security Features

Federal Agency Programs/Oversight

Area Maritime Security Plans & National Maritime Security Plan

National Strategy for Maritime Security
Maritime Transportation System Security

[U.S. DHS, 2005a., p.3]

Current Approaches

‘series of security nets that provide layers of protection necessary to effectively manage security risks’ [U.S. DHS, 2005a., p.3]

What’s Missing?

- Considering a **port as a complex, socio-technical system**
  - Need to better mitigate vulnerability of cargo containers as means of terrorism [Fritelli, 2005]
  - Vulnerabilities created by design & processes inherent to port itself [Gould, Macharis, & Haasis, 2010]

- **Security** of system ≠ **reliability** of components in series
  - Defense-in-depth philosophy [U.S. DHS 2005a, 2005b]
  - Untenable assumptions
    - ‘Swiss Cheese’ model [Reason, 1997]
    - Path of least resistance [Ghafoori & Altiok, 2012]

- **Dynamic** & **interactive** complexity
  - The reality of the ‘insider threat’ & flawed security design [O’Connel, 2009]
  - Vulnerabilities from redundancy, complacency & threat escalation [Sagan 2004]

- **Inclusion** of **organizational**/ **social** aspects
  - Congressional mandates & economic pressures [Chatterjee 2003]
  - Inconsistent security metrics & resulting confusion [Fritelli, 2005]
  - Tension from unanswered question of ‘who’s responsible?’ [Fritelli, 2005]

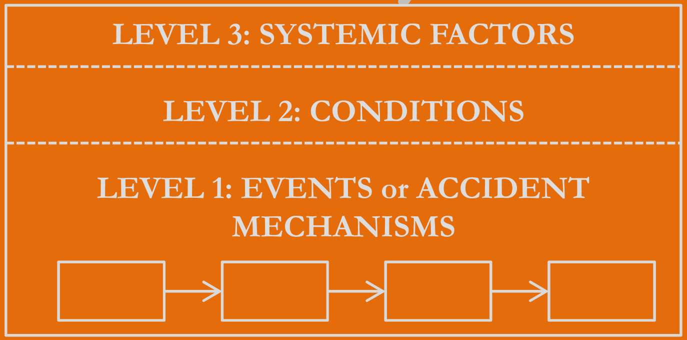
Current Approaches

'series of security nets that provide layers of protection necessary to effectively manage security risks'

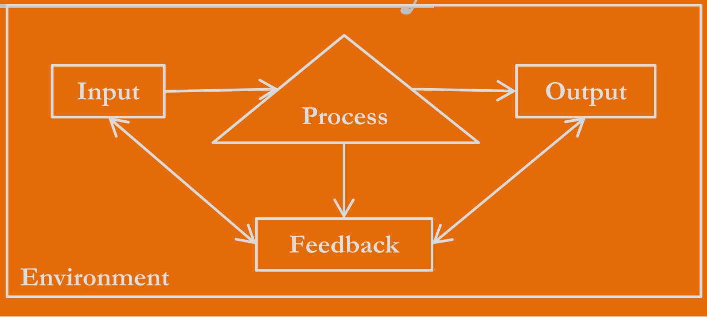
[U.S. DHS, 2005a., p.3]

What's Needed?

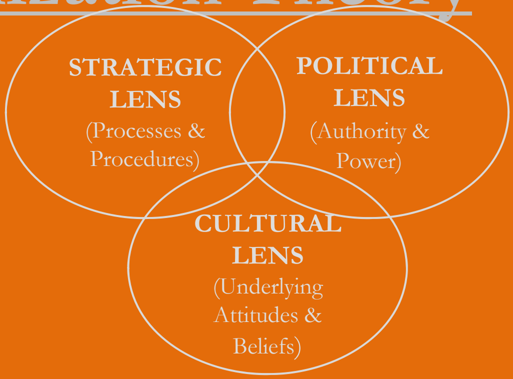
Systems Theory


LEVEL 3: SYSTEMIC FACTORS
LEVEL 2: CONDITIONS
LEVEL 1: EVENTS or ACCIDENT MECHANISMS

Control Theory



Organization Theory


STRATEGIC LENS (Processes & Procedures)
POLITICAL LENS (Authority & Power)
CULTURAL LENS (Underlying Attitudes & Beliefs)

MIT/Sloan Approach [Carroll 2006]

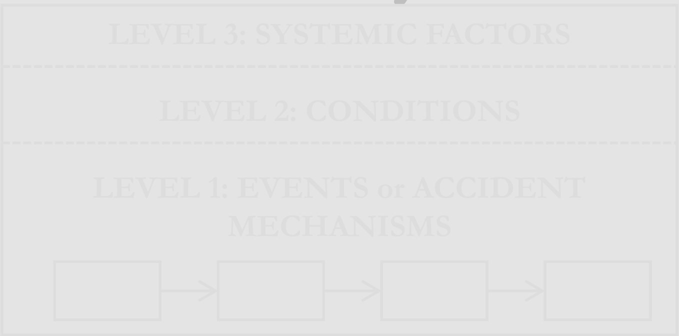
A New Approach

System Theoretic Accident Model & Process (STAMP)

[Leveson, 2012]

What's Needed?

Systems Theory

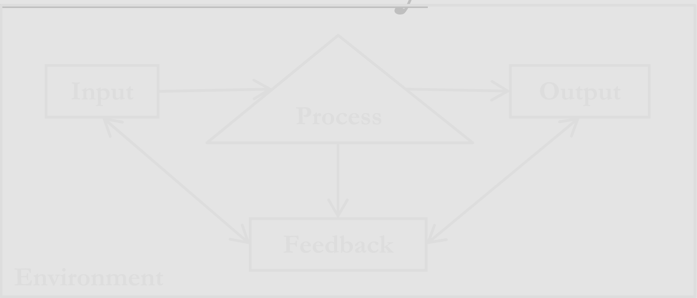

LEVEL 3: SYSTEMIC FACTORS

LEVEL 2: CONDITIONS

LEVEL 1: EVENTS or ACCIDENT MECHANISMS

- Systems & control theory-based causality model for complex, socio-technical systems [Leveson 2012]
- 'top-down' model for hazards & losses used across complex technical domains [Leveson 2012; Stringfellow, et. al. 2010; Alemzadeh, et. al. 2013]

Control Theory


Input

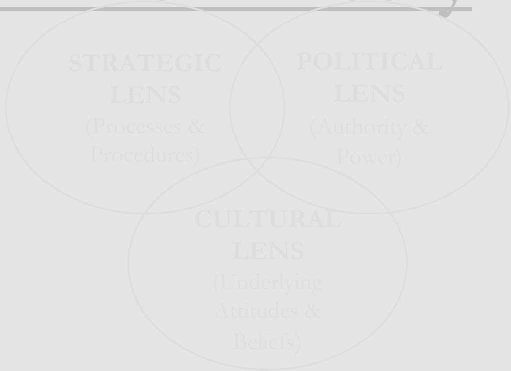
Process

Output

Feedback

Environment

Organization Theory


STRATEGIC LENS (Processes & Procedures)

POLITICAL LENS (Authority & Power)

CULTURAL LENS (Underlying Attitudes & Beliefs)

MIT/Sloan Approach [Carroll 2006]

System Theoretic Accident Model & Process (STAMP)

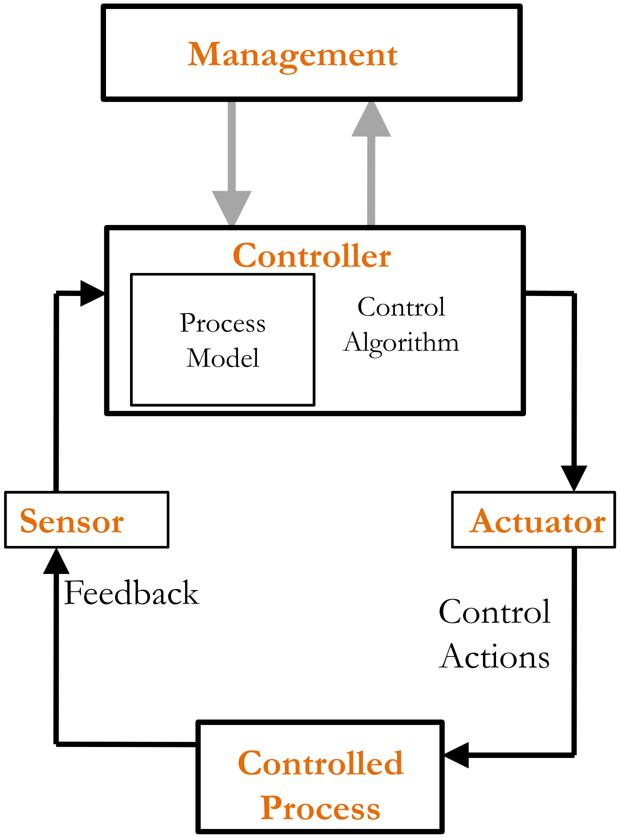
[Leveson, 2012]

- '**top-down**' causality model for vulnerabilities
- Based on **systems** (emergence & hierarchy) and **control** (communications & constraints) theory
- Identify vulnerabilities to **eliminate/minimize vulnerable system states** (e.g., redesign)
- Safety (and thus security) is considered an **emergent system property**

System Theoretic Process Analysis (STPA)

- Identify **high level vulnerabilities**
- Identify **vulnerable control actions** and **security constraints**
- Identify **scenarios that lead** to **violation** of security constraints
- **Redesign** system to **eliminate** or **minimize** such violations

STPA-SEC is an extension of STPA being developed for **cyber** and **physical** complex systems [Young 2015 (forthcoming diss.); Williams 2013]



STPA Basic Control Structure

[Leveson, 2012; Thomas 2012]

Applied to Port Security

System Theoretic Accident Model & Process (STAMP)

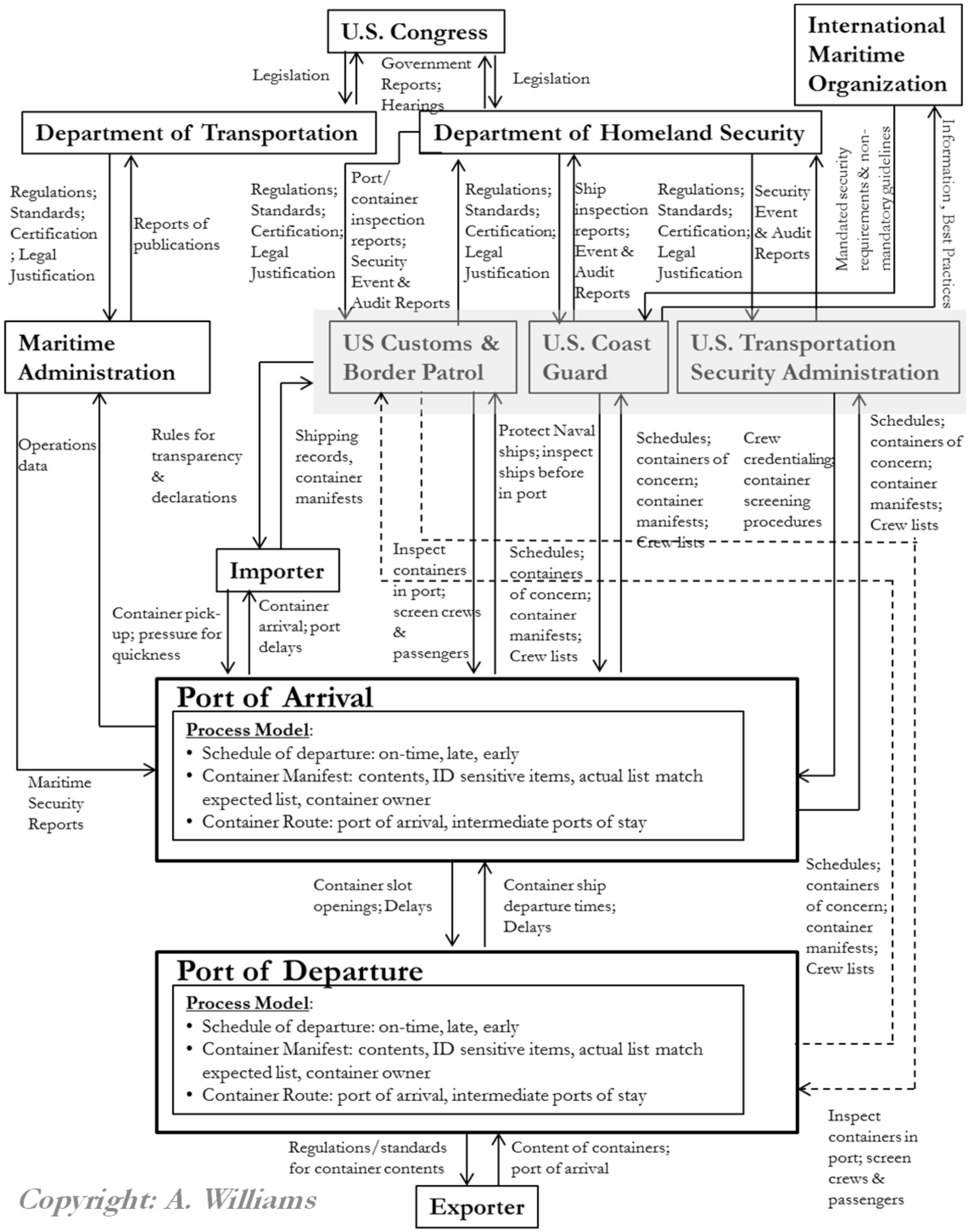
[Leveson, 2012]

Port Security-Related Stakeholder	Port Security-Related Responsibilities
International Maritime Organization	Maintains the International Ship and Port Facility Security (ISPS) Code (United Nations stakeholder)
U.S. Congress	Sets port security related policy & legislation for the U.S.
U.S. Department of Transportation	Lobbies, funds & sets regulations for the Maritime Administration
U.S. Department of Homeland Security	Lobbies, funds & sets regulations/operations for the U.S. Customs & Border Patrol, Coast Guard and Transportation Security Administration
U.S. Customs & Border Patrol	Inspects containers & ships while in port; checks crew and ship passenger lists
U.S. Coast Guard	Inspects ships before they arrive in port (e.g., in U.S. territorial waters); protects Naval ships while in port
U.S. Transportation Security Administration	Provides crew credentialing, background investigations & advanced container/ship screening procedures
Maritime Administration	Provides security planning guides & 'Maritime Security Reports' (civilian stakeholder)
Importer	Declares goods/containers received and maintains transparent shipping records
Port of arrival	Reports any ship/container of concern and provides resources (e.g., time) for above agencies to perform any necessary inspections
Port of departure	Reports any ship/container of concern and provides resources (e.g., time) for above agencies to perform any necessary inspections

Applied to Port Security

Slide 12 of 25

Hierarchical Control Structure


U.S. Congress

International Maritime Organization

Legislation

Government Reports; Hearings

Legislation

Department of Transportation

Department of Homeland Security

Mandated security requirements & non-mandatory guidelines

Information, Best Practices

Regulations; Standards; Certification; Legal Justification

Reports of publications

Regulations; Standards; Certification; Legal Justification

Port/container inspection reports; Security Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Ship inspection reports; Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Security Event & Audit Reports

Maritime Administration

US Customs & Border Patrol

U.S. Coast Guard

U.S. Transportation Security Administration

Operations data

Rules for transparency & declarations

Shipping records, container manifests

Protect Naval ships; inspect ships before in port

Schedules; containers of concern; container manifests; Crew lists

Crew credentialing; container screening procedures

Schedules; containers of concern; container manifests; Crew lists

Importer

Container pick-up; pressure for quickness

Container arrival; port delays

Inspect containers in port; screen crews & passengers

Schedules; containers of concern; container manifests; Crew lists

Port of Arrival

Process Model:

- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Maritime Security Reports

Container slot openings; Delays

Container ship departure times; Delays

Schedules; containers of concern; container manifests; Crew lists

Port of Departure

Process Model:

- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Inspect containers in port; screen crews & passengers

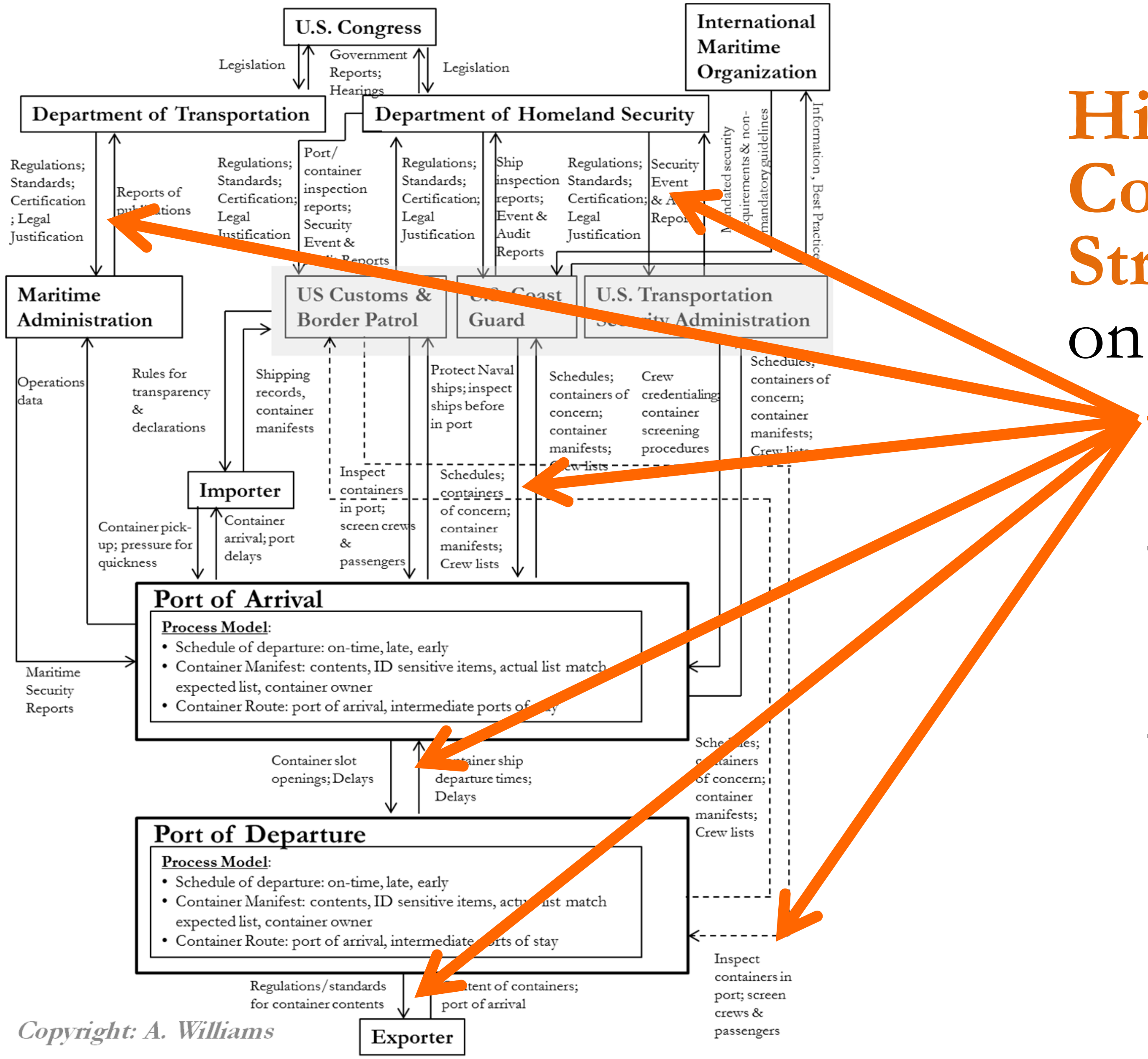
Regulations/standards for container contents

Content of containers; port of arrival

Exporter

Copyright: A. Williams

Applied to Port Security



U.S. Congress

Legislation

Government Reports; Hearings

Legislation

International Maritime Organization

Department of Transportation

Department of Homeland Security

Regulations; Standards; Certification ; Legal Justification

Reports of publications

Regulations; Standards; Certification; Legal Justification

Port/ container inspection reports; Security Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Ship inspection reports; Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Security Event & Audit Reports

Mandated security requirements & non-mandatory guidelines

Information, Best Practices

Maritime Administration

US Customs & Border Patrol

U.S. Coast Guard

U.S. Transportation Security Administration

Operations data

Rules for transparency & declarations

Shipping records, container manifests

Protect Naval ships; inspect ships before in port

Schedules; containers of concern; container manifests; Crew lists

Crew credentialing; container screening procedures

Schedules; containers of concern; container manifests; Crew lists

Importer

Inspect containers in port; screen crews & passengers

Schedules; containers of concern; container manifests; Crew lists

Container pick-up; pressure for quickness

Container arrival; port delays

Port of Arrival

Process Model:

- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Maritime Security Reports

Container slot openings; Delays

Container ship departure times; Delays

Schedules; containers of concern; container manifests; Crew lists

Port of Departure

Process Model:

- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Inspect containers in port; screen crews & passengers

Regulations/standards for container contents

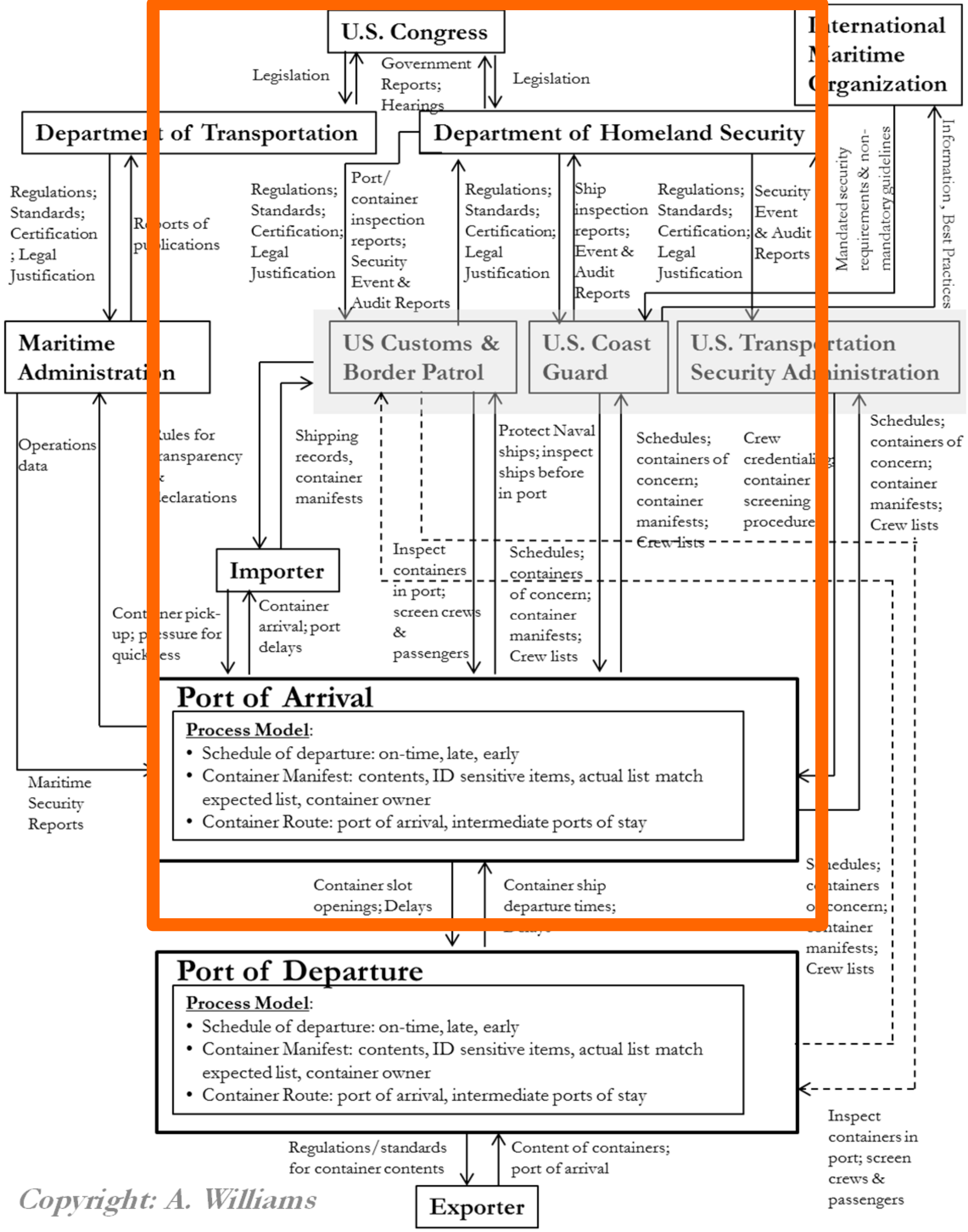
Content of containers; port of arrival

Exporter

Hierarchical Control Structure based on:

- **Security constraints**
- Hierarchical levels of control
- Process models

Applied to Port Security



U.S. Congress

Legislation

Government Reports; Hearings

Legislation

International Maritime Organization

Department of Transportation

Department of Homeland Security

Regulations; Standards; Certification ; Legal Justification

Reports of publications

Regulations; Standards; Certification; Legal Justification

Port/ container inspection reports; Security Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Ship inspection reports; Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Security Event & Audit Reports

Mandated security requirements & non-mandatory guidelines

Information, Best Practices

Maritime Administration

US Customs & Border Patrol

U.S. Coast Guard

U.S. Transportation Security Administration

Operations data

Rules for transparency & declarations

Shipping records, container manifests

Protect Naval ships; inspect ships before in port

Schedules; containers of concern; container manifests; Crew lists

Crew credentialing; container screening procedures

Schedules; containers of concern; container manifests; Crew lists

Importer

Inspect containers in port; screen crews & passengers

Schedules; containers of concern; container manifests; Crew lists

Container pick-up; pressure for quickness

Container arrival; port delays

Port of Arrival

<u>Process Model</u>:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Maritime Security Reports

Container slot openings; Delays

Container ship departure times; Delays

Schedules; containers of concern; container manifests; Crew lists

Port of Departure

<u>Process Model</u>:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Inspect containers in port; screen crews & passengers

Regulations/standards for container contents

Content of containers; port of arrival

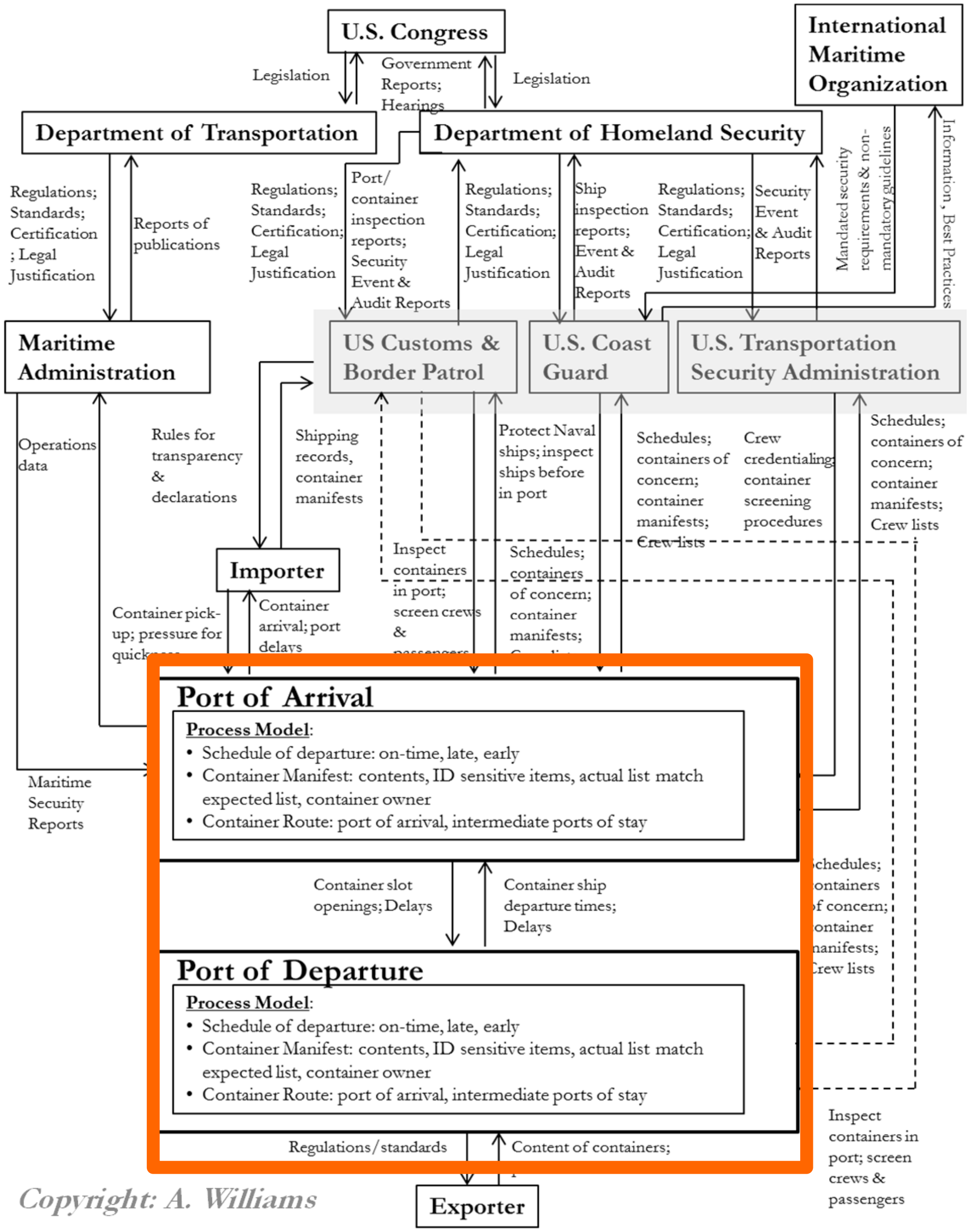
Exporter

Copyright: A. Williams

Hierarchical Control Structure based on:

- Security constraints
- **Hierarchical levels of control**
- Process models

Applied to Port Security



U.S. Congress

Legislation

Government Reports; Hearings

Legislation

International Maritime Organization

Department of Transportation

Department of Homeland Security

Regulations; Standards; Certification ; Legal Justification

Reports of publications

Regulations; Standards; Certification; Legal Justification

Port/ container inspection reports; Security Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Ship inspection reports; Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Security Event & Audit Reports

Mandated security requirements & non-mandatory guidelines

Information, Best Practices

Maritime Administration

US Customs & Border Patrol

U.S. Coast Guard

U.S. Transportation Security Administration

Operations data

Rules for transparency & declarations

Shipping records, container manifests

Protect Naval ships; inspect ships before in port

Schedules; containers of concern; container manifests; Crew lists

Crew credentialing; container screening procedures

Schedules; containers of concern; container manifests; Crew lists

Importer

Inspect containers in port; screen crews & passengers

Schedules; containers of concern; container manifests;

Container pick-up; pressure for quick

Container arrival; port delays

Maritime Security Reports

Port of Arrival

<u>Process Model</u>:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Container slot openings; Delays

Container ship departure times; Delays

chedules; ontainers f concern; ontainer anifests; rew lists

Port of Departure

<u>Process Model</u>:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Regulations/standards

Content of containers;

Inspect containers in port; screen crews & passengers

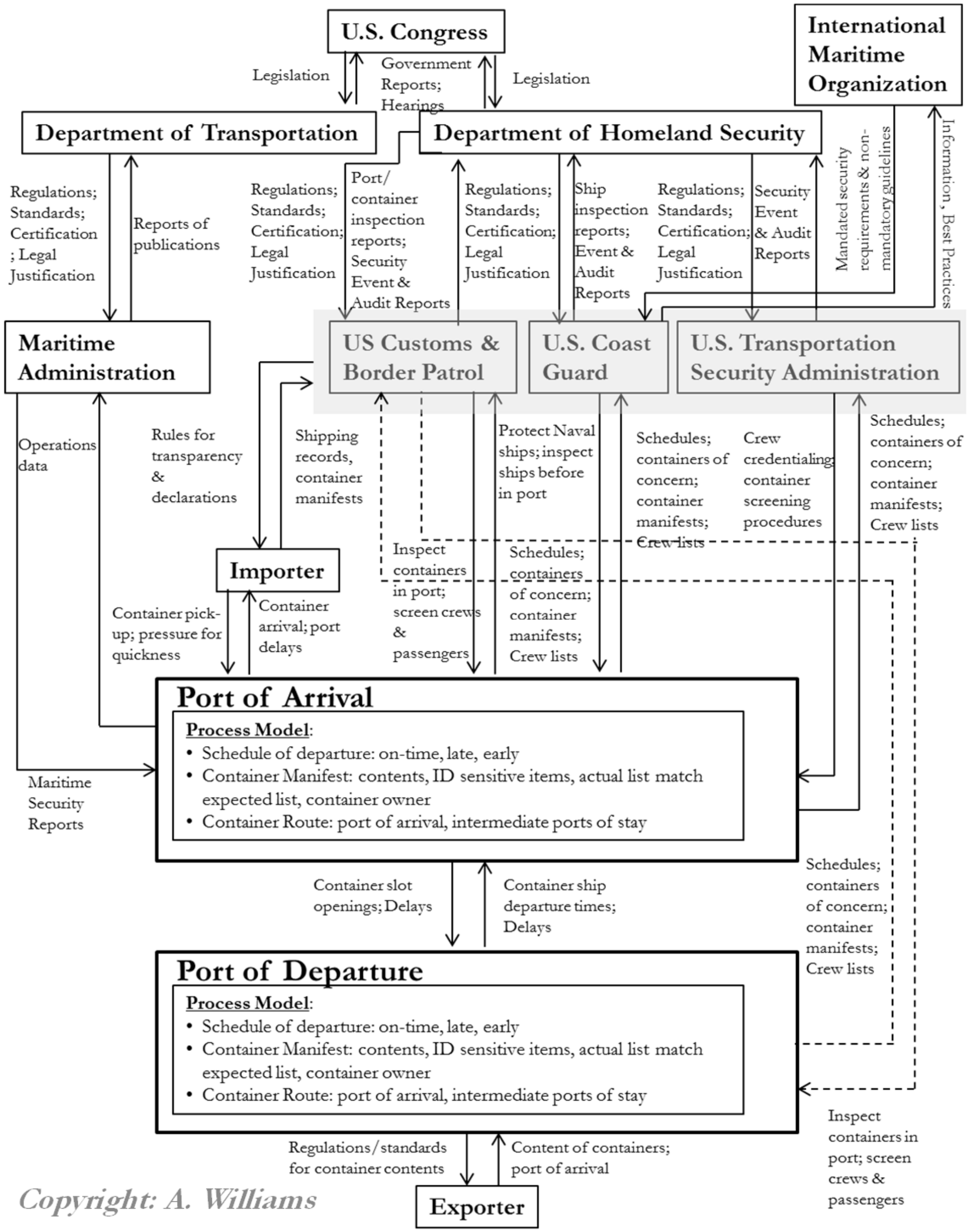
Exporter

Copyright: A. Williams

Hierarchical Control Structure based on:

- Security constraints
- Hierarchical levels of control
- Process models

Applied to Port Security



U.S. Congress

Legislation

Government Reports; Hearings

Legislation

International Maritime Organization

Department of Transportation

Department of Homeland Security

Regulations; Standards; Certification; Legal Justification

Reports of publications

Regulations; Standards; Certification; Legal Justification

Port/ container inspection reports; Security Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Ship inspection reports; Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Security Event & Audit Reports

Mandated security requirements & non-mandatory guidelines

Information, Best Practices

Maritime Administration

US Customs & Border Patrol

U.S. Coast Guard

U.S. Transportation Security Administration

Operations data

Rules for transparency & declarations

Shipping records, container manifests

Protect Naval ships; inspect ships before in port

Schedules; containers of concern; container manifests; Crew lists

Crew credentialing; container screening procedures

Schedules; containers of concern; container manifests; Crew lists

Importer

Inspect containers in port; screen crews & passengers

Schedules; containers of concern; container manifests; Crew lists

Container pick-up; pressure for quickness

Container arrival; port delays

Port of Arrival

Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Maritime Security Reports

Container slot openings; Delays

Container ship departure times; Delays

Schedules; containers of concern; container manifests; Crew lists

Port of Departure

Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Inspect containers in port; screen crews & passengers

Regulations/standards for container contents

Content of containers; port of arrival

Exporter

Copyright: A. Williams

Define Mission

↓

Identify Losses

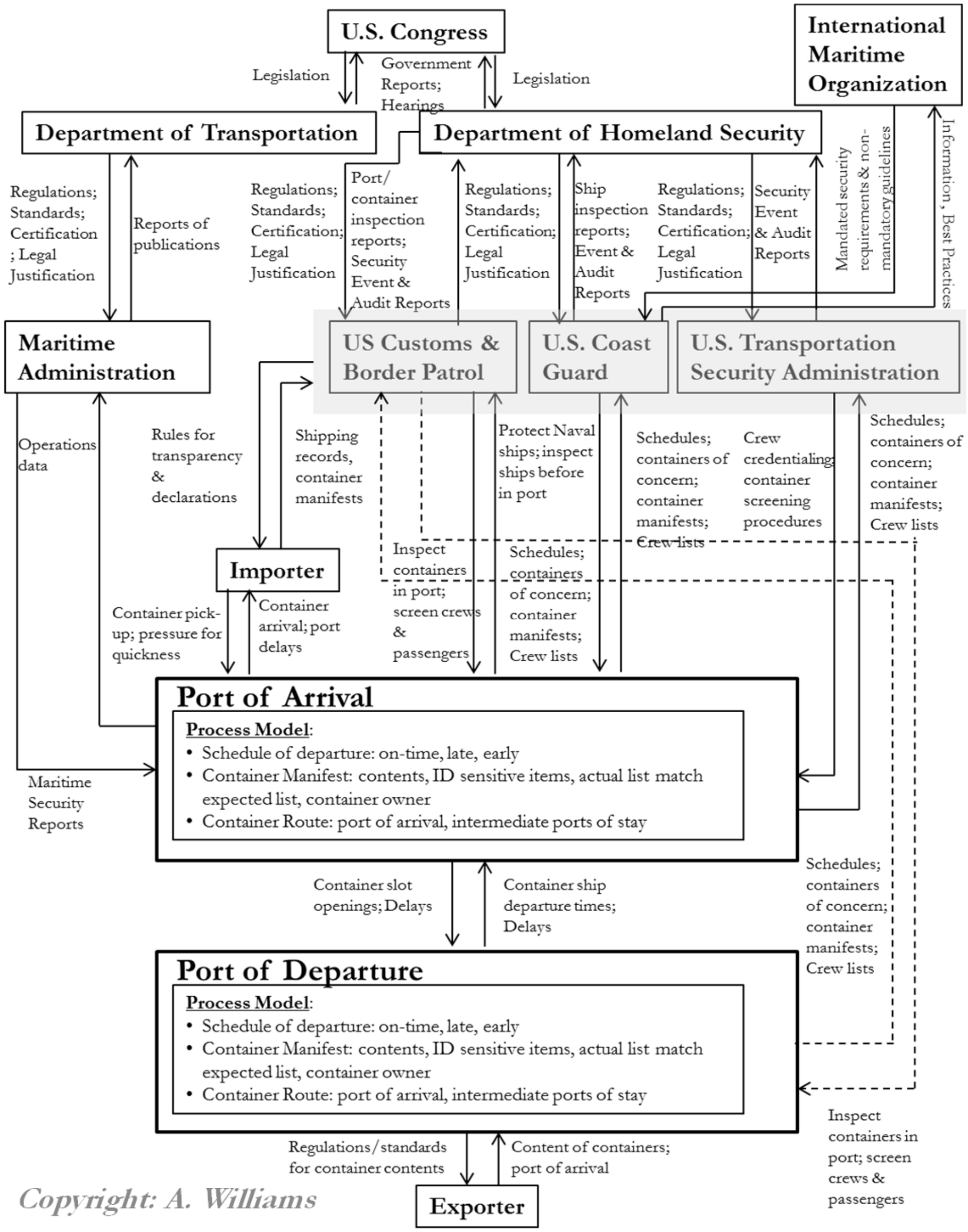
↓

Identify Vulnerable States

Losses	Descriptions
L1	Human serious injury or loss of life
L2	Significant damage to the port system infrastructure
L3	Significant loss of revenue

Vulnerable States	Related Losses
(V1) Unauthorized individuals accessing port system infrastructure	L1, L2, L3
(V3) Uncoordinated implementation of inspection procedures	L1, L2, L3

Applied to Port Security



U.S. Congress

International Maritime Organization

Legislation

Government Reports; Hearings

Legislation

Department of Transportation

Department of Homeland Security

Regulations; Standards; Certification ; Legal Justification

Reports of publications

Regulations; Standards; Certification; Legal Justification

Port/ container inspection reports; Security Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Ship inspection reports; Event & Audit Reports

Regulations; Standards; Certification; Legal Justification

Security Event & Audit Reports

Mandated security requirements & non-mandatory guidelines

Information, Best Practices

Maritime Administration

US Customs & Border Patrol

U.S. Coast Guard

U.S. Transportation Security Administration

Operations data

Rules for transparency & declarations

Shipping records, container manifests

Protect Naval ships; inspect ships before in port

Schedules; containers of concern; container manifests; Crew lists

Crew credentialing; container screening procedures

Schedules; containers of concern; container manifests; Crew lists

Importer

Inspect containers in port; screen crews & passengers

Schedules; containers of concern; container manifests; Crew lists

Container pick-up; pressure for quickness

Container arrival; port delays

Port of Arrival

Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Maritime Security Reports

Container slot openings; Delays

Container ship departure times; Delays

Schedules; containers of concern; container manifests; Crew lists

Port of Departure

Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Inspect containers in port; screen crews & passengers

Regulations/standards for container contents

Content of containers; port of arrival

Exporter

Copyright: A. Williams

Identify Vulnerable States

↓

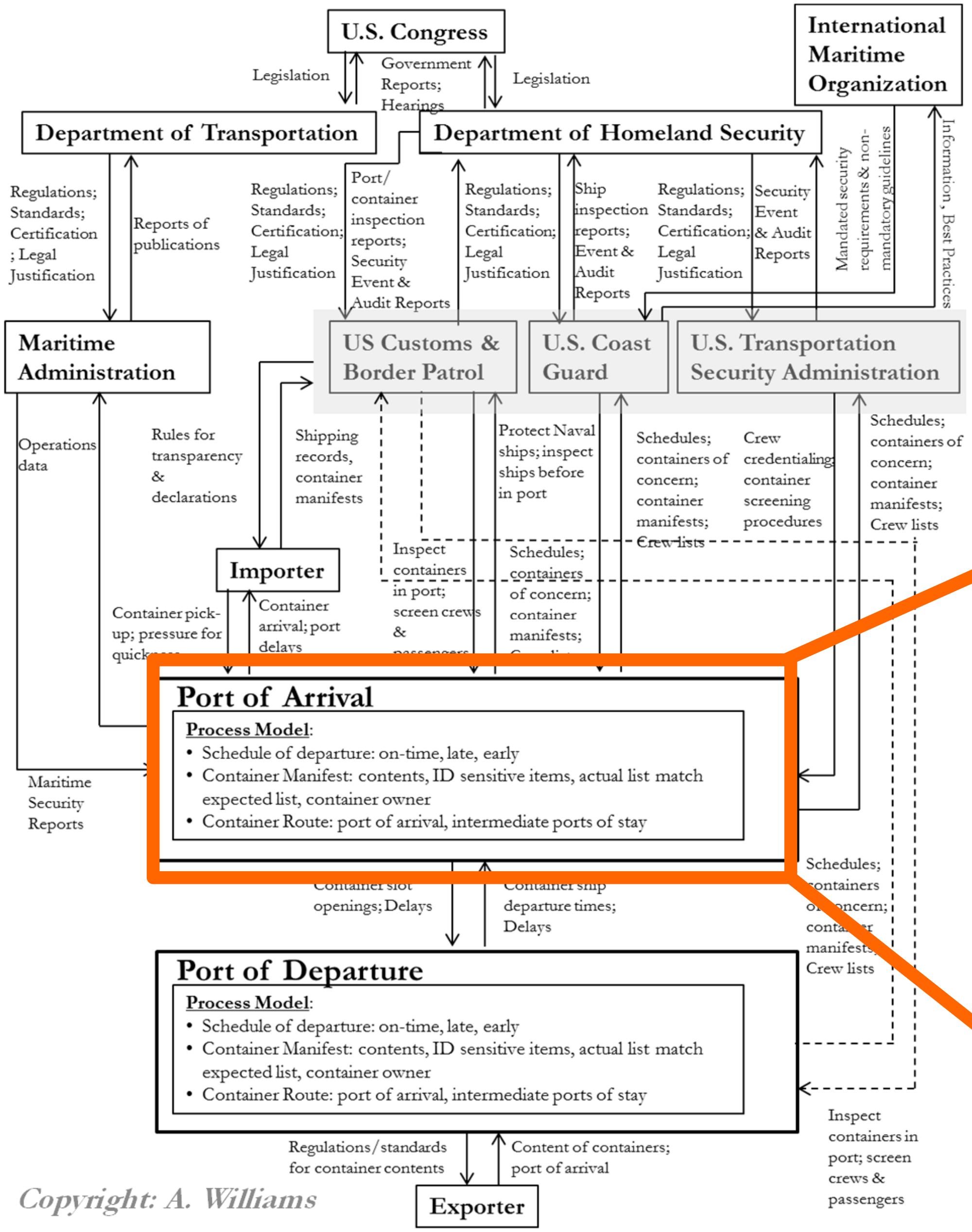
Derive Security Requirements

↓

Define Security Control Actions

Vulnerable States	Security Requirement (System Constraint)	Example Security Control Action
(V1) Unauthorized individuals accessing to port system infrastructure	Unauthorized individuals must not access the port system infrastructure	Check the access credential of any individual entering the container security area
(V3) Uncoordinated implementation of inspection procedures	All inspection procedures must be coordinated between implementers	Coast Guard communicates completion of a successful inspection to Customs & Border Patrol

Applied to Port Security


U.S. Congress
International Maritime Organization
Legislation
Government Reports; Hearings
Legislation
Department of Transportation
Department of Homeland Security
Regulations; Standards; Certification ; Legal Justification
Reports of publications
Regulations; Standards; Certification; Legal Justification
Port/ container inspection reports; Security Event & Audit Reports
Regulations; Standards; Certification; Legal Justification
Ship inspection reports; Event & Audit Reports
Regulations; Standards; Certification; Legal Justification
Security Event & Audit Reports
Mandated security requirements & non-mandatory guidelines
Information, Best Practices
Maritime Administration
US Customs & Border Patrol
U.S. Coast Guard
U.S. Transportation Security Administration
Operations data
Rules for transparency & declarations
Shipping records, container manifests
Protect Naval ships; inspect ships before in port
Schedules; containers of concern; container manifests; Crew lists
Crew credentialing; container screening procedures
Schedules; containers of concern; container manifests; Crew lists
Importer
Inspect containers in port; screen crews & passengers
Schedules; containers of concern; container manifests;
Container pick-up; pressure for quick
Container arrival; port delays
Maritime Security Reports
Port of Arrival
Container slot openings; Delays
Container ship departure times; Delays
Schedules; containers of concern; container manifests; Crew lists
Port of Departure
Inspect containers in port; screen crews & passengers
Regulations/standards for container contents
Content of containers; port of arrival
Exporter

Port of Arrival

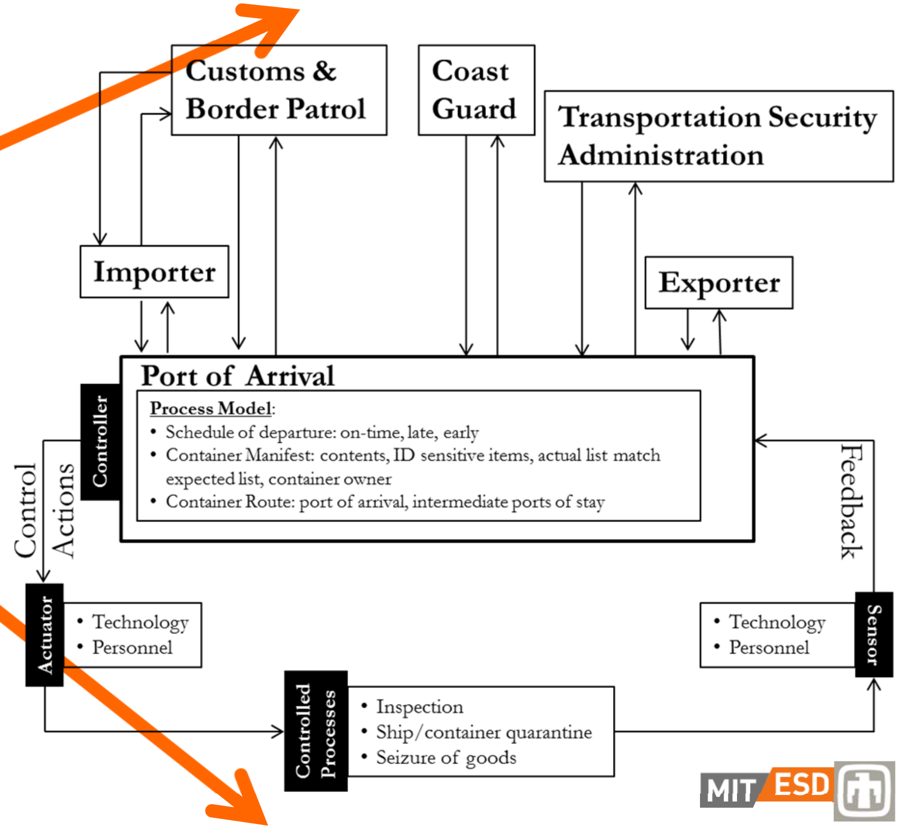
Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Port of Departure

Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Copyright: A. Williams

Simplified Security Control Loop



Port of Arrival

Process Model:
- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

Actuator:
- Technology
- Personnel

Sensor:
- Technology
- Personnel

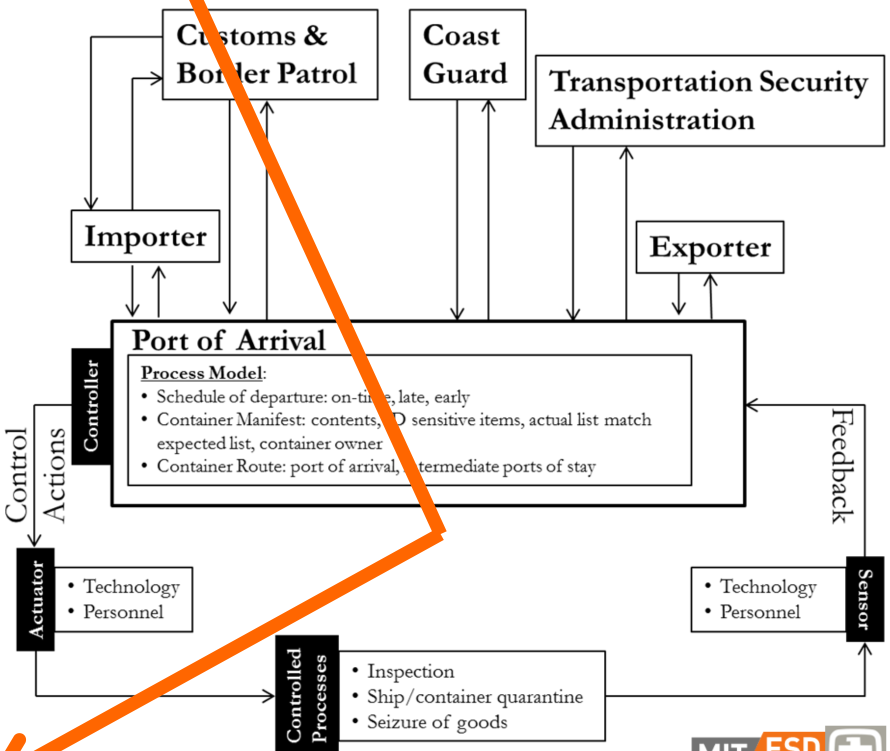
Controlled Processes:
- Inspection
- Ship/container quarantine
- Seizure of goods

Applied to Port Security

Example Security Control Actions	Command Needed & Not Provided	Command Not Needed & Provided	Command Given Too Early/Late or in Wrong Order	Command Stopped Too Soon/ Engaged Too Long
Check the access credential of any individual entering the container security area	*Unauthorized individual accesses container storage area [V1, V3]	*Already credentialed person is re-checked (e.g., different agency or badge) [V3]	*Check credential after individual in container storage area (e.g., too late/wrong order) [V1, V3]	*Not Applicable (a binary command)
Coast Guard communicates completion of a successful inspection to Customs & Border Patrol	*Coast Guard does not communicate their inspection, therefore both stakeholders inspect the container or ship [V3, L3]	* Coast Guard does communicate their inspection, Border Patrol allows other/similar container or ship needing inspection to continue without it [V2, V3]	*If Coast Guard communicated their inspection too late, both stakeholders inspect ship or container [V2, V3]	*Not Applicable (a binary command)

STPA Step 1:

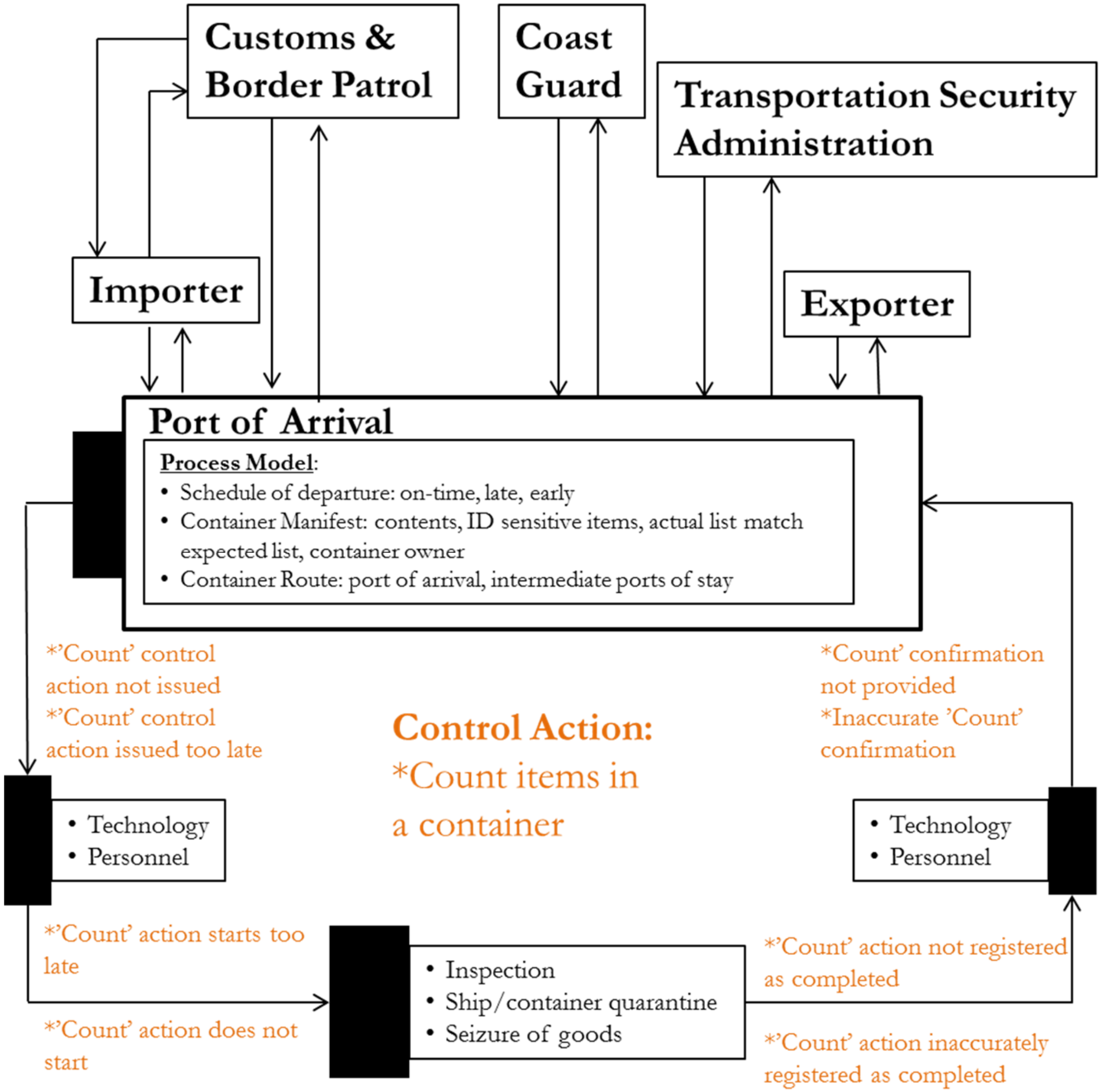
Derive Security Control Action Violations



Applied to Port Security

STPA Step 1:

Derive Security Control Action Violations



Customs & Border Patrol

Coast Guard

Transportation Security Administration

Importer

Exporter

Port of Arrival

Process Model:

- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

*'Count' control action not issued
*'Count' control action issued too late

*'Count' confirmation not provided
*Inaccurate 'Count' confirmation

Control Action:
*Count items in a container

- Technology
- Personnel

- Technology
- Personnel

*'Count' action starts too late

*'Count' action does not start

- Inspection
- Ship/container quarantine
- Seizure of goods

*'Count' action not registered as completed

*'Count' action inaccurately registered as completed

Applied to Port Security

Security Control Action Violations	Adversary Action: Stealth	Adversary Action: Deceit	Adversary Action: Force
***Unauthorized individual accesses container storage area [V1, V3]**	*Cutting hole in a fence without triggering any related alarm to access the container storage area	*Using a forged badge to access the container storage area	*Use vehicle to drive through/ over barriers to the container storage area
***Both Coast Guard and Customs & Border Patrol inspect the container or ship [V3, L3]**	* Jam the communications channels between Coast Guard and Customs & Border Patrol causing both to inspect the container assuming the other has/will not	*Spoof the comms channels between Coast Guard and Customs & Border Patrol indicating the other has/will not inspect the cargo or ship	*This strategy is not likely to be employed for this security control action violation

STPA Step 2:

Generate Causal Scenarios – Adversary Actions

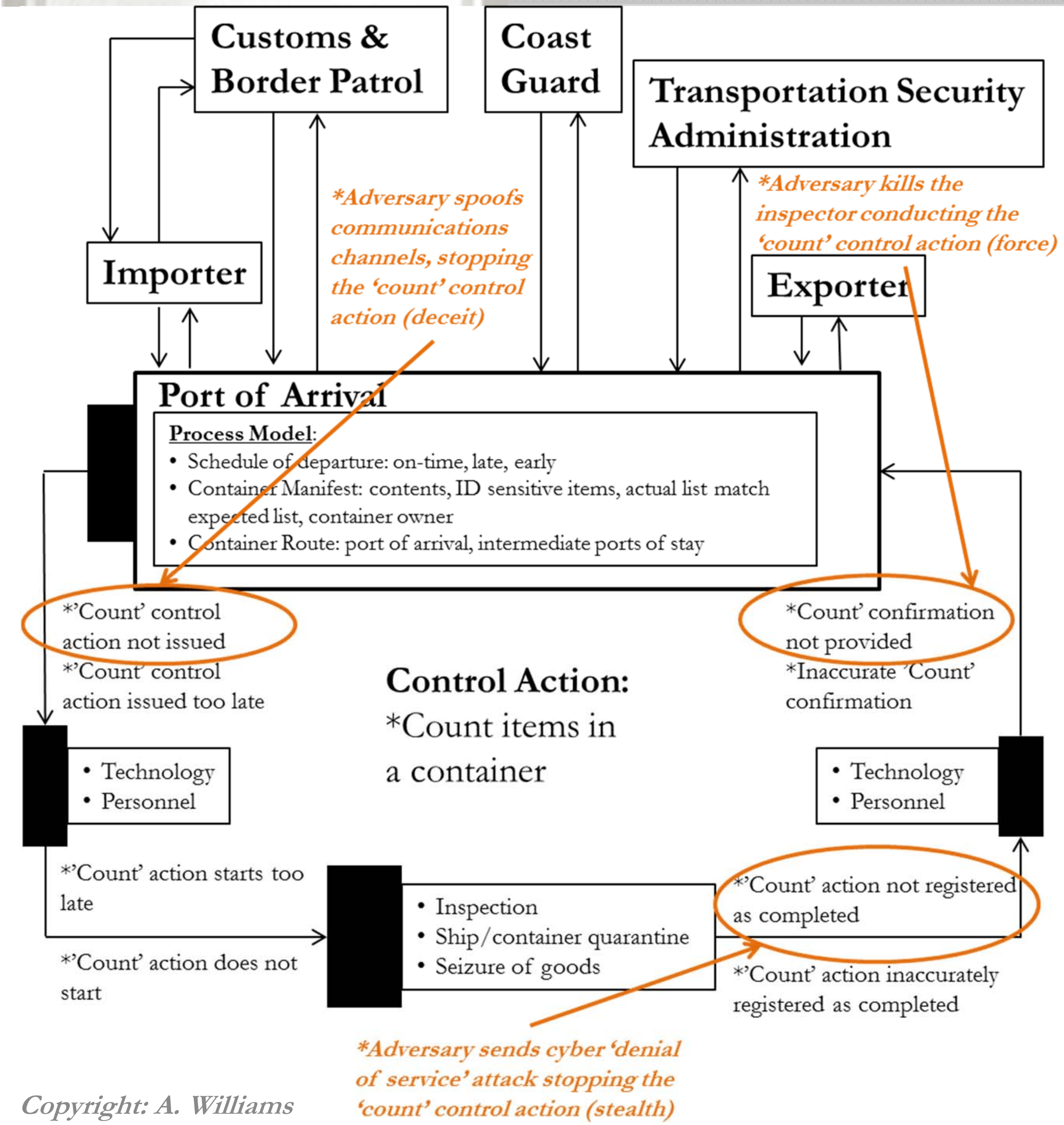
- What causes security control action violations?
  - –Environmental events
  - –Non-random adversary actions
- Generic adversary categories

[Garcia 2007]

Applied to Port Security

STPA Step 2:

Generate Causal Scenarios – Adversary Actions



Adversary spoofs communications channels, stopping the 'count' control action (deceit)

Adversary kills the inspector conducting the 'count' control action (force)

Process Model:

- Schedule of departure: on-time, late, early
- Container Manifest: contents, ID sensitive items, actual list match expected list, container owner
- Container Route: port of arrival, intermediate ports of stay

*'Count' control action not issued

*'Count' control action issued too late

*'Count' confirmation not provided

*Inaccurate 'Count' confirmation

Control Action:
*Count items in a container

*'Count' action starts too late

*'Count' action does not start

*'Count' action not registered as completed

*'Count' action inaccurately registered as completed

Adversary sends cyber 'denial of service' attack stopping the 'count' control action (stealth)

Conclusions

- Port security enhanced by orienting toward identifying **component, systemic & interactive** security **control action violations**

Recommendations

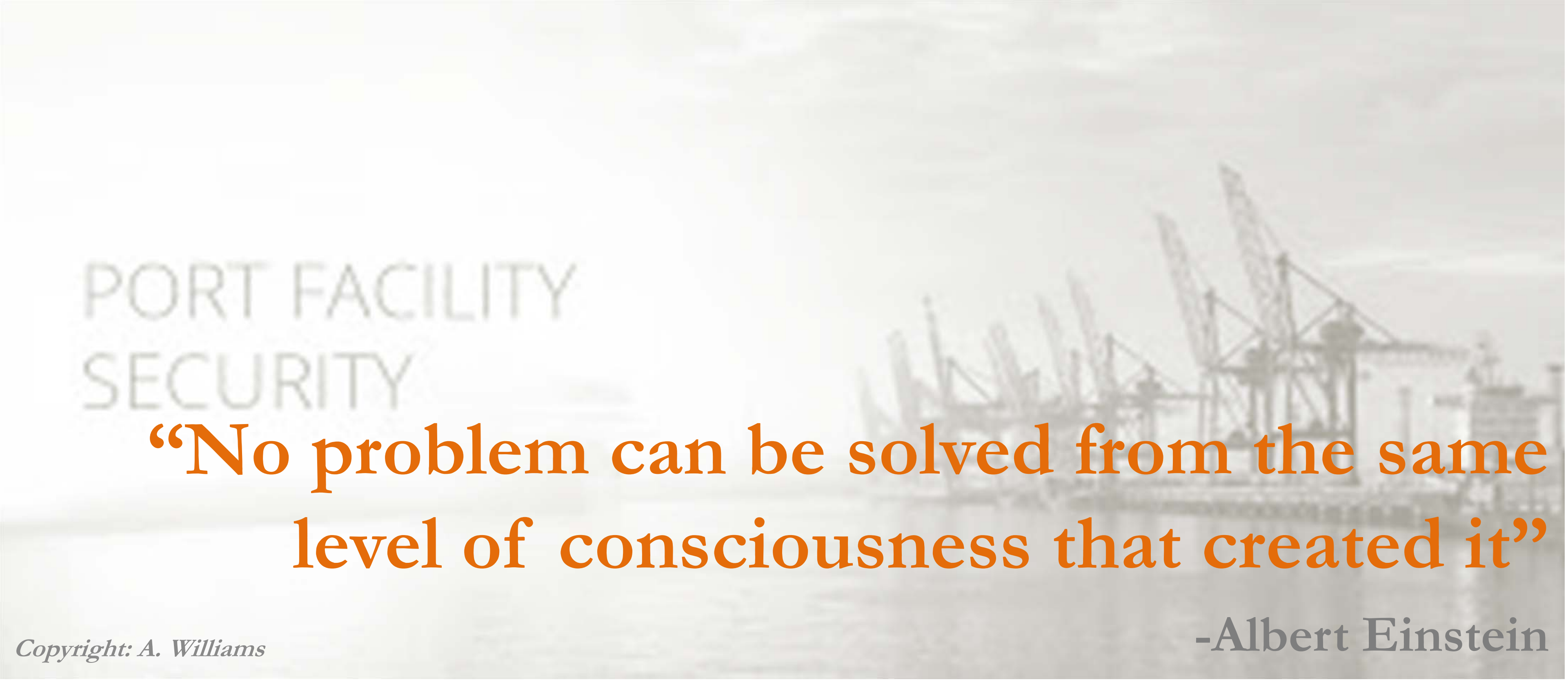
- From concentric layers to eliminate port security control action violations
- Port security 'embedded' in everyday business practices
- Port security more than trading expedited service for increased transparency
- Functional control structures help overcome lack of coordinated port security regulatory body
- Consider economic pressures on port security implementation as fundamental design variable

Summary

System Attribute	Current Approaches	STAMP Approach
Definition of Security	Protection of ports against most probable adversary actions	Maintaining a system state that can protect ports from unacceptable loss
Basis for Analytical Framework	Reliability engineering, probability theory	Systems theory, control theory (organization theory)
Treatment of Organizational Factors	As one-time (and unchangeable) probability(ies) of human action	As ongoing (designable) influences on ability to enforce security control actions
Type of Complexity	Combinatorial	Dynamic, Interactive
Security improvements are	Considered 'add-ons' to an already operating system	Traceable back to (and having influence on) overall system objectives

- Potential for **port security** paradigm shift away from **preventing failures** & toward **enforcing control actions**
- **STAMP** & **STPA** provide foundation for more effective comprehensive port security strategies

Questions???



"No problem can be solved from the same level of consciousness that created it"

-Albert Einstein