Arab Academy
for Science Technology & Maritime Transport

The International Maritime
Transport and Logistics Conference
"Marlog 11"

1972 - 2022
Years Of Excellence

"Cyber-Physical Security for Ports Infrastructure"

11 2022 Marlog

Towards a SUSTAINABLE BLUE ECONOMY

20 - 22 March, 2022
Hilton Green Plaza Hotel

Prof. Nikitas Nikitakos
Iosif Progoulakis (PhDc)
Prof. Dimitrios Dalaklis
CAPT. Razali Yaacob

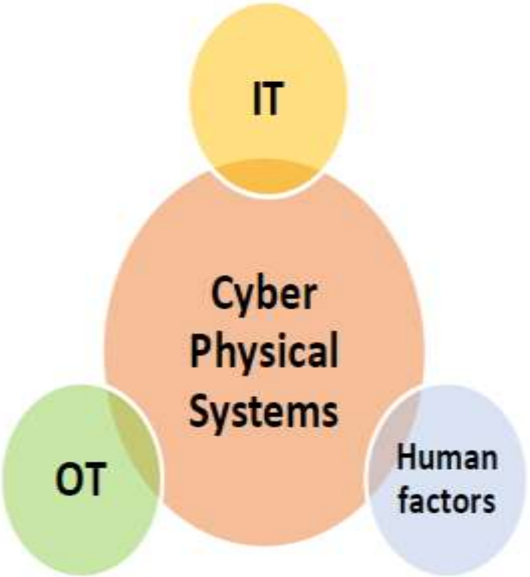
UNIVERSITY OF THE AEGEAN
WMU WORLD MARITIME UNIVERSITY
NMUC

CYBER-PHYSICAL SECURITY FOR PORTS INFRASTRUCTURE: INTRODUCTION

Aims:

- Major attributes of cyber-physical security in ports will be presented.
- Security threats and vulnerabilities faced by ports' infrastructure will be discussed.
- An overview of the major initiatives by the industry and governmental entities will be presented.
- An overview of some security assessment methodologies for the evaluation of cyber-physical security threats and vulnerabilities will be provided.
- Conclusions derived will be discussed.

DEFINITIONS



"Cyber-physical systems pertain to the integration of IT and OT systems along with human factors"

→ ***IT systems***: *"..used to manage complex data and information flow." :*

- Transaction Processing Systems.
- Office Automation Systems.
- Knowledge Management Systems.
- Management Information Systems.
- Decision Support Systems.
- Executive Support System.

→ ***OT systems***: *"… control the physical world."*

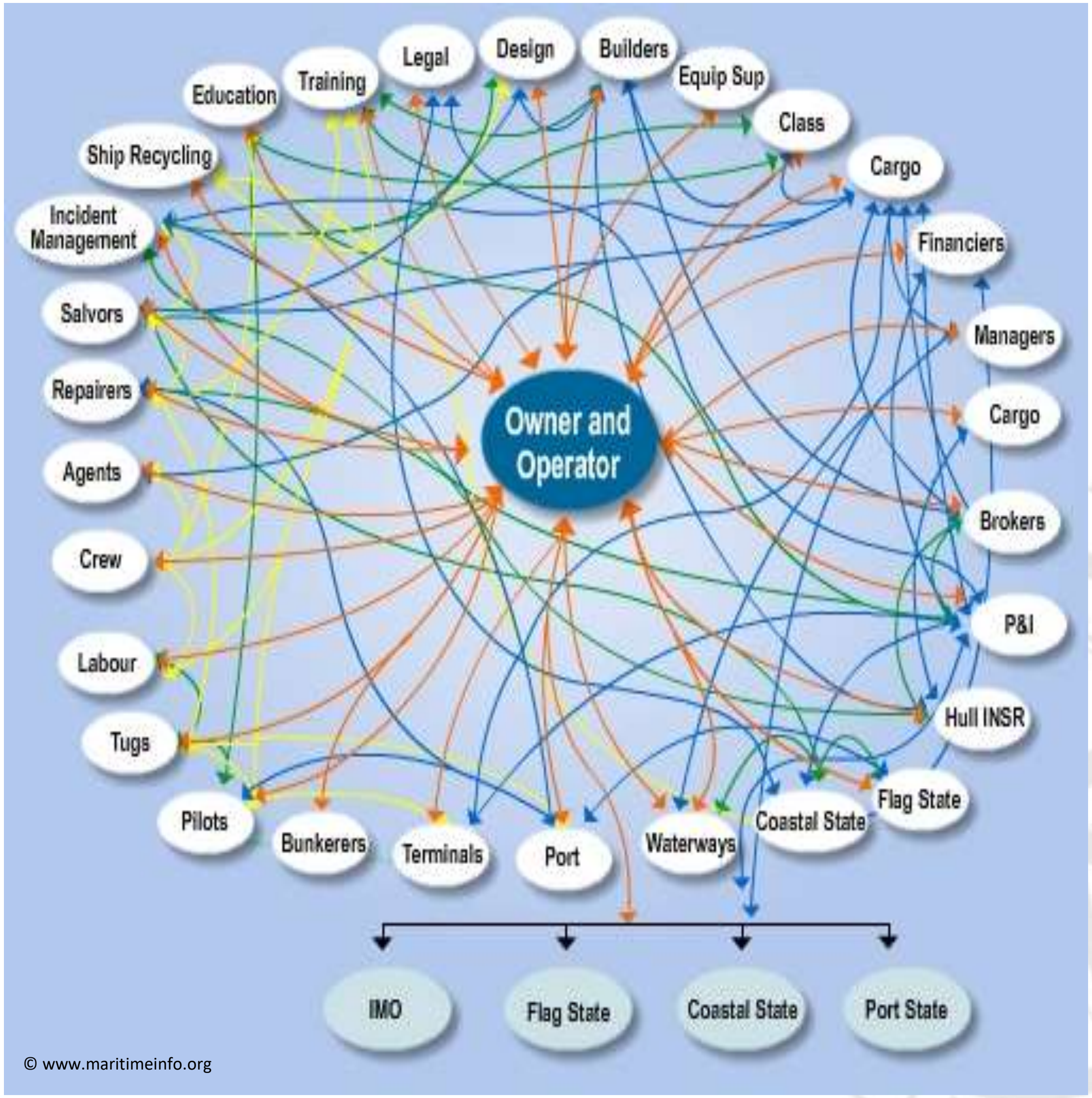
- Programmable Logic Controllers (PLCs)
- Supervisory Control And Data Acquisition Systems (SCADA)
- Distributed Control Systems (DCS)
- Industrial Control Systems (ICS)

→ ***Human factors***: *"… operate the IT/OT systems."*

- Operators
- Maritime operations stakeholders
- Service providers
- Maintenance providers

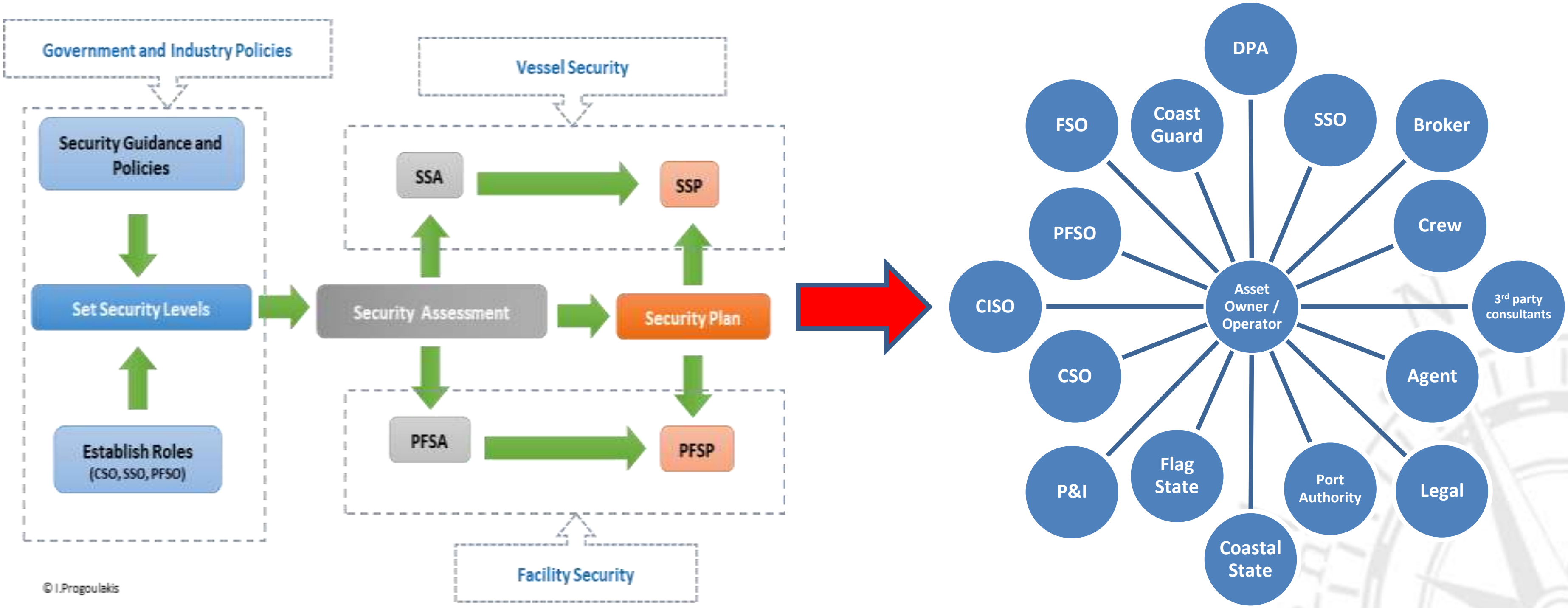
STAKEHOLDERS IN THE MARITIME INDUSTRY - OPERATIONS

- Multiple stakeholders
- Multiple interconnections
- Worldwide connections
- Interdisciplinary connections (legal, financial, engineering, services, operational, 3rd party consultancy, insurance, governmental, etc)



© www.maritimeinfo.org

STAKEHOLDERS IN MARITIME (AND CYBER) SECURITY: ISPS APPLICATION



© I.Progoulakis

CYBER-PHYSICAL ASPECTS IN PORT INFRASTRUCTURE AND OPERATIONS

Examples of maritime IT/OT systems and networks

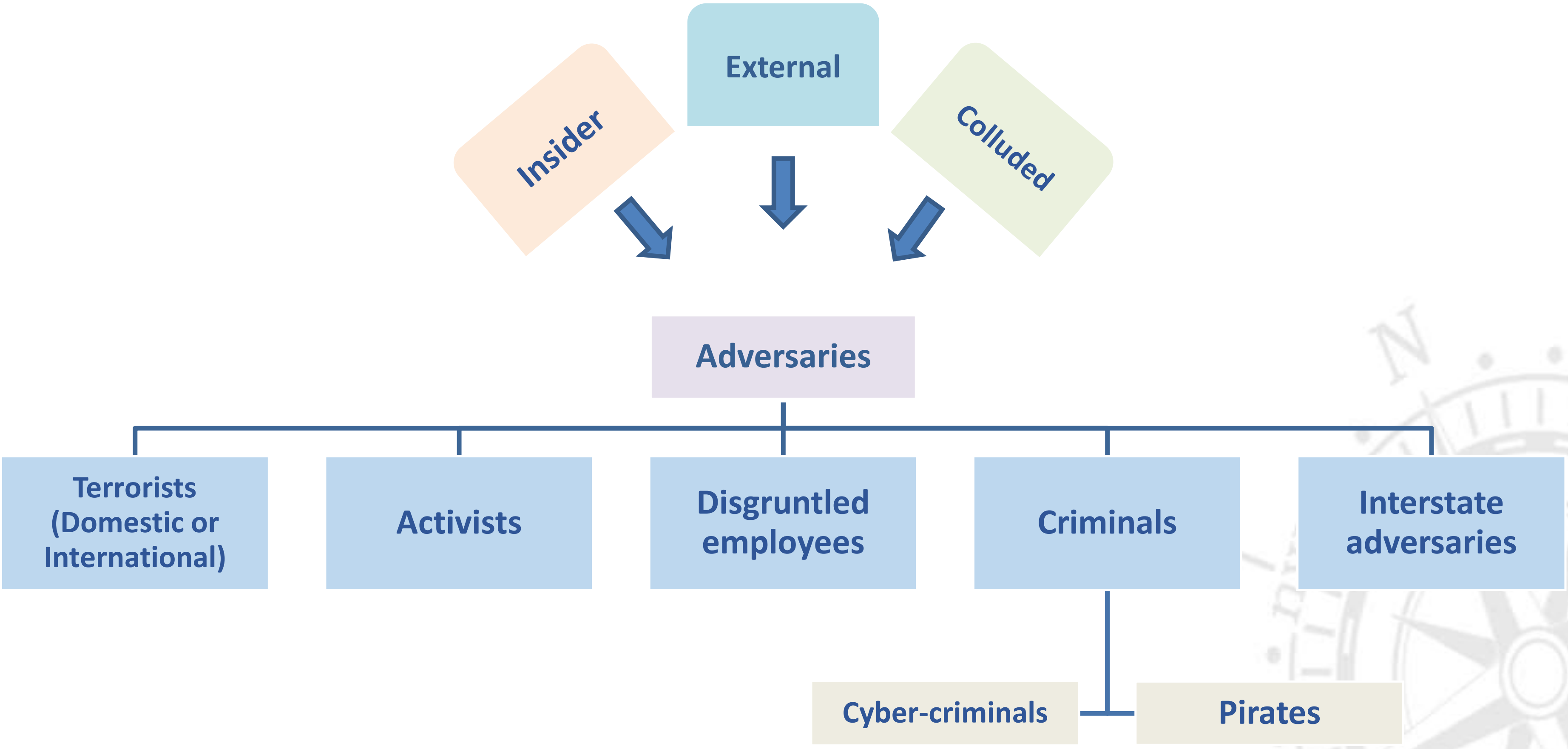
Shore facilities:

- Transfer and load out racks
- Terminal automation systems
- Crane control systems
- IP cameras
- VOIP/ROIP communications
- Physical security access controls
- Life safety systems
- Environmental control systems
- Warehouse management
- Tank management systems
- Utilities

Vessel:

- Tension monitoring
- Ship-to-shore comms/ESD
- Vessel propulsion
- Navigation
- AIS, GPS
- Ballast control systems
- Dynamic Positioning Systems (DSP)
- Engine monitoring
- IoT
- Custody transfer systems

SECURITY ADVERSARIES AGAINST PORT INFRASTRUCTURE



CYBER PHYSICAL THREATS AND VULNERABILITIES IN IT/OT SYSTEMS

Threats

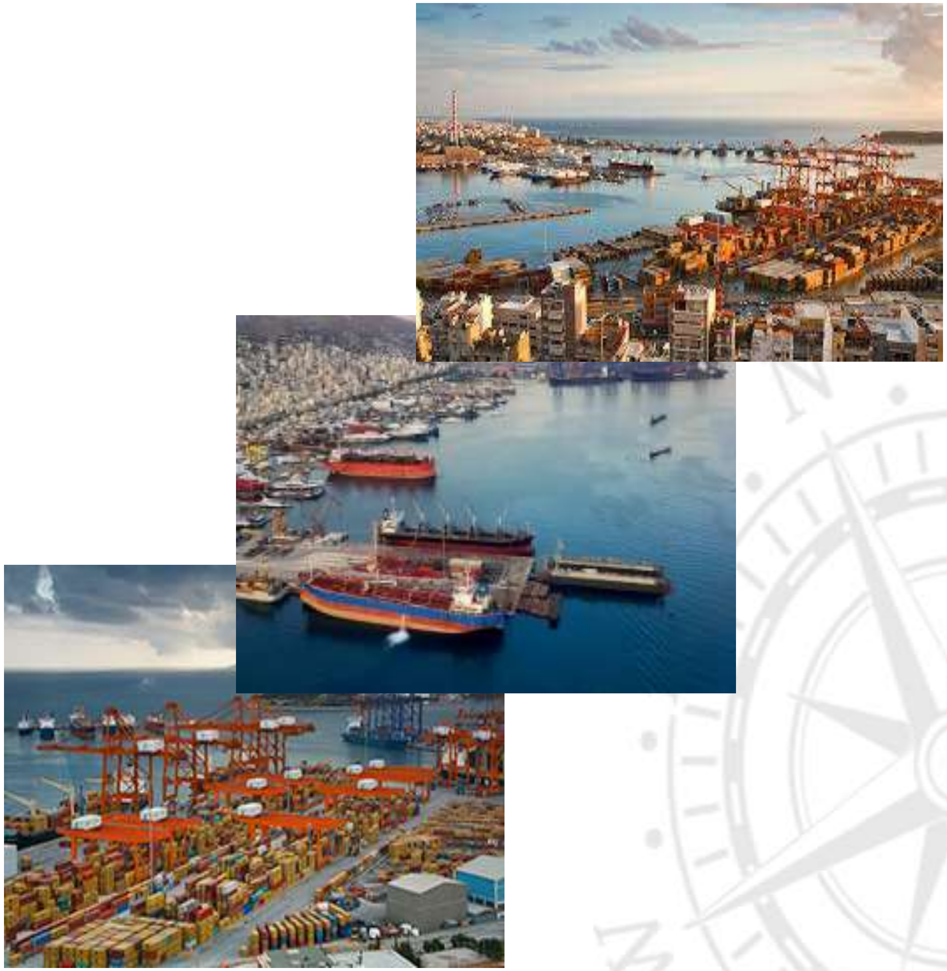
- Lack of network segmentation
- DDoS attacks
- Web apps attacks
- Malware
- Manipulation of systems commands and parameters and procedures

Vulnerabilities

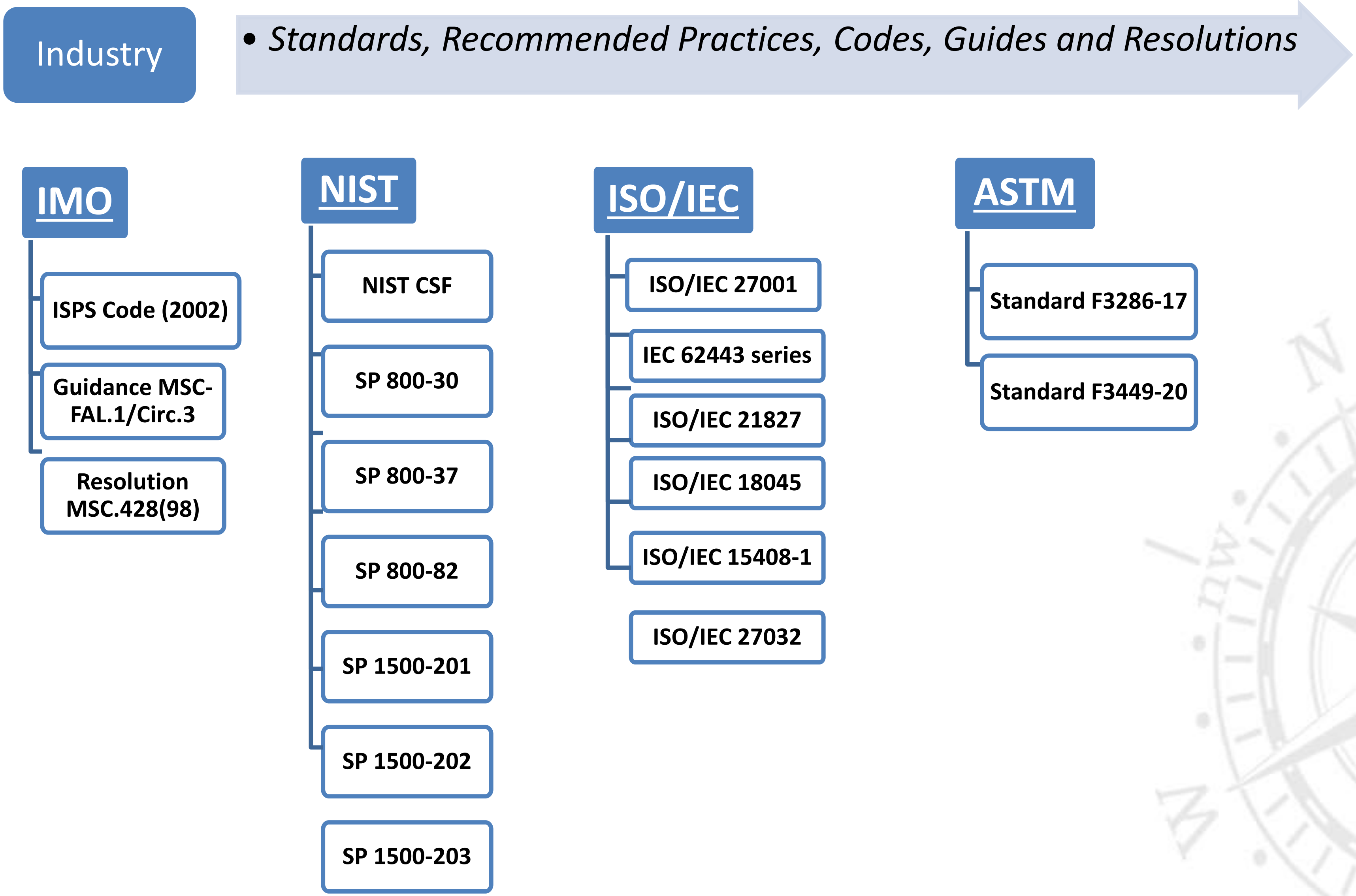
- Legacy software
- Default configuration
- Lack of encryption
- Remote access policies
- Policies and procedures
- Cybersecurity knowledge in the workforce

EXAMPLES OF MARITIME CYBERSECURITY INCIDENTS

- Multiple ports South Africa (2021)
- Port of Houston, USA (2021)
- Shahid Rajaee Port, Iran (2020)
- Toll Group, Australia (2020)
- Mediterranean Shipping Company (2020)
- Deep draft vessel, NYC USA (2018)
- Port of San Diego, USA (2018)
- Port of Barcelona, USA (2018)
- COSCO Shipping, USA (2018)
- MAERSK, global (2017)



CURRENT STATUS - INDUSTRY



Industry

- *Standards, Recommended Practices, Codes, Guides and Resolutions*

IMO

- ISPS Code (2002)
- Guidance MSC-FAL.1/Circ.3
- Resolution MSC.428(98)

NIST

- NIST CSF
- SP 800-30
- SP 800-37
- SP 800-82
- SP 1500-201
- SP 1500-202
- SP 1500-203

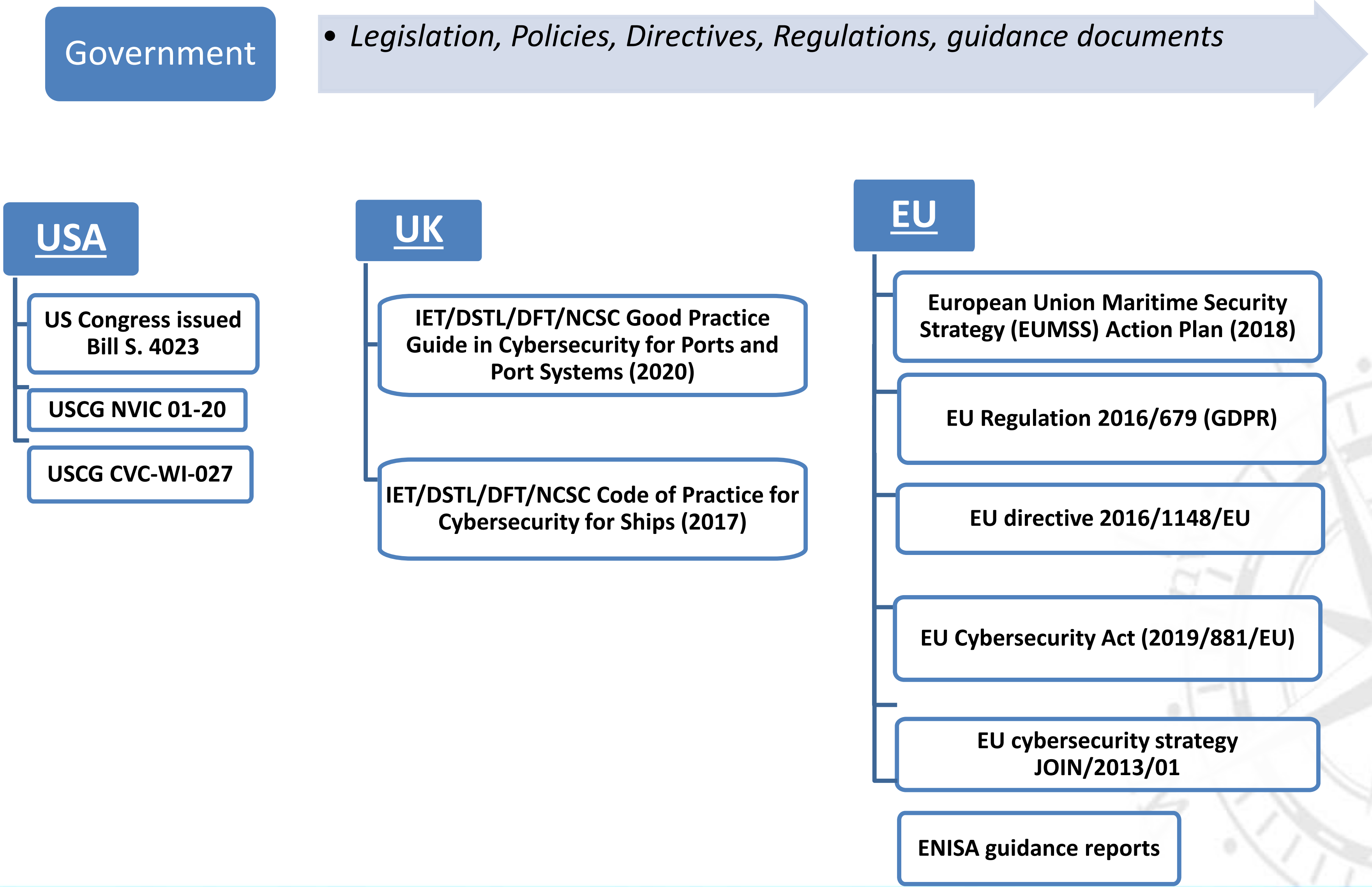
ISO/IEC

- ISO/IEC 27001
- IEC 62443 series
- ISO/IEC 21827
- ISO/IEC 18045
- ISO/IEC 15408-1
- ISO/IEC 27032

ASTM

- Standard F3286-17
- Standard F3449-20

CURRENT STATUS - GOVERNMENT



Government

- *Legislation, Policies, Directives, Regulations, guidance documents*

USA

- US Congress issued Bill S. 4023
- USCG NVIC 01-20
- USCG CVC-WI-027

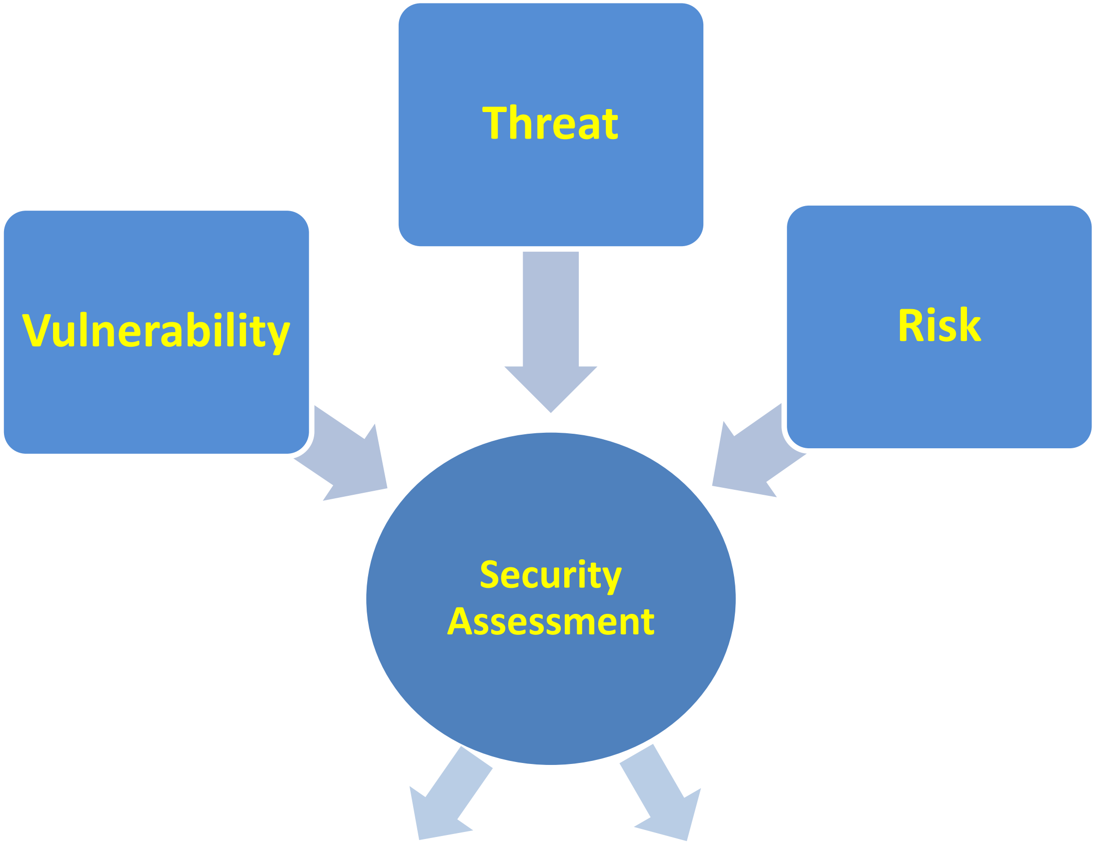
UK

- IET/DSTL/DFT/NCSC Good Practice Guide in Cybersecurity for Ports and Port Systems (2020)
- IET/DSTL/DFT/NCSC Code of Practice for Cybersecurity for Ships (2017)

EU

- European Union Maritime Security Strategy (EUMSS) Action Plan (2018)
- EU Regulation 2016/679 (GDPR)
- EU directive 2016/1148/EU
- EU Cybersecurity Act (2019/881/EU)
- EU cybersecurity strategy JOIN/2013/01
- ENISA guidance reports

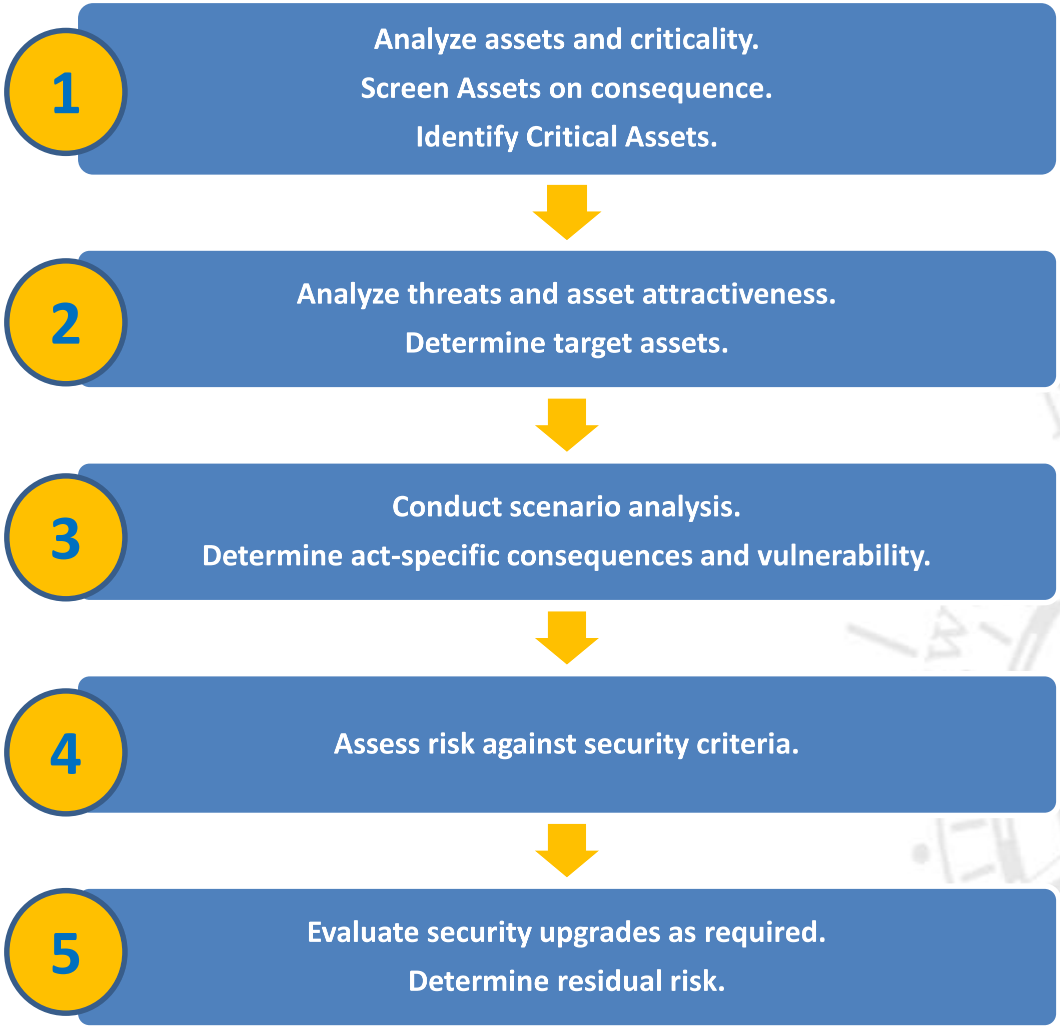
SECURITY ASSESSMENT AND CYBER PHYSICAL SECURITY



"Macro"-Scale "Micro"-Scale

API SECURITY RISK ASSESSMENT (SRA) – API STD 780

"Security risks should be managed in a risk-based, performance-oriented management process to ensure the security of assets and the protection of the public, the environment, workers, and the continuity of the business."



1 Analyze assets and criticality.
Screen Assets on consequence.
Identify Critical Assets.

2 Analyze threats and asset attractiveness.
Determine target assets.

3 Conduct scenario analysis.
Determine act-specific consequences and vulnerability.

4 Assess risk against security criteria.

5 Evaluate security upgrades as required.
Determine residual risk.

CYBER SECURITY ASSESSMENT AND PSM (PROCESS SAFETY MANAGEMENT)

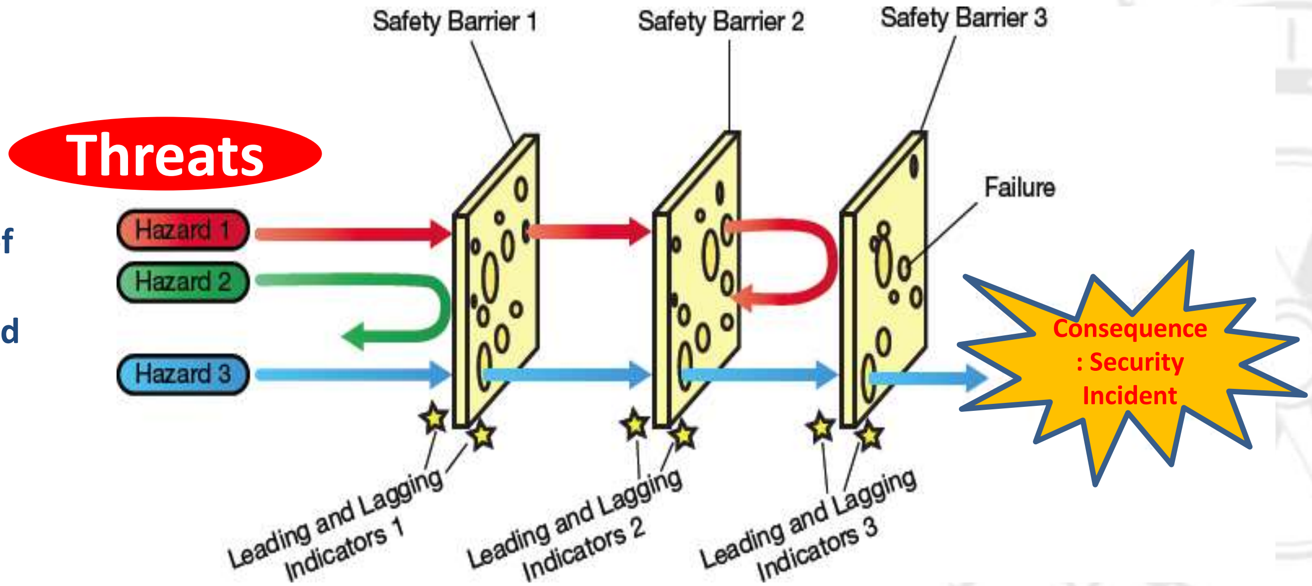
Qualitative

- Check Lists
- PHA (Process Hazards Analysis)
- What-If Reviews
- HAZOP (Hazard and Operability) Review
- Bow-Tie Analysis (Barrier Analysis)

Quantitative

- ETA (Event Tree Analysis)
- FTA (Fault Tree Analysis)
- FMEA (Failure Modes and Effects Analysis)

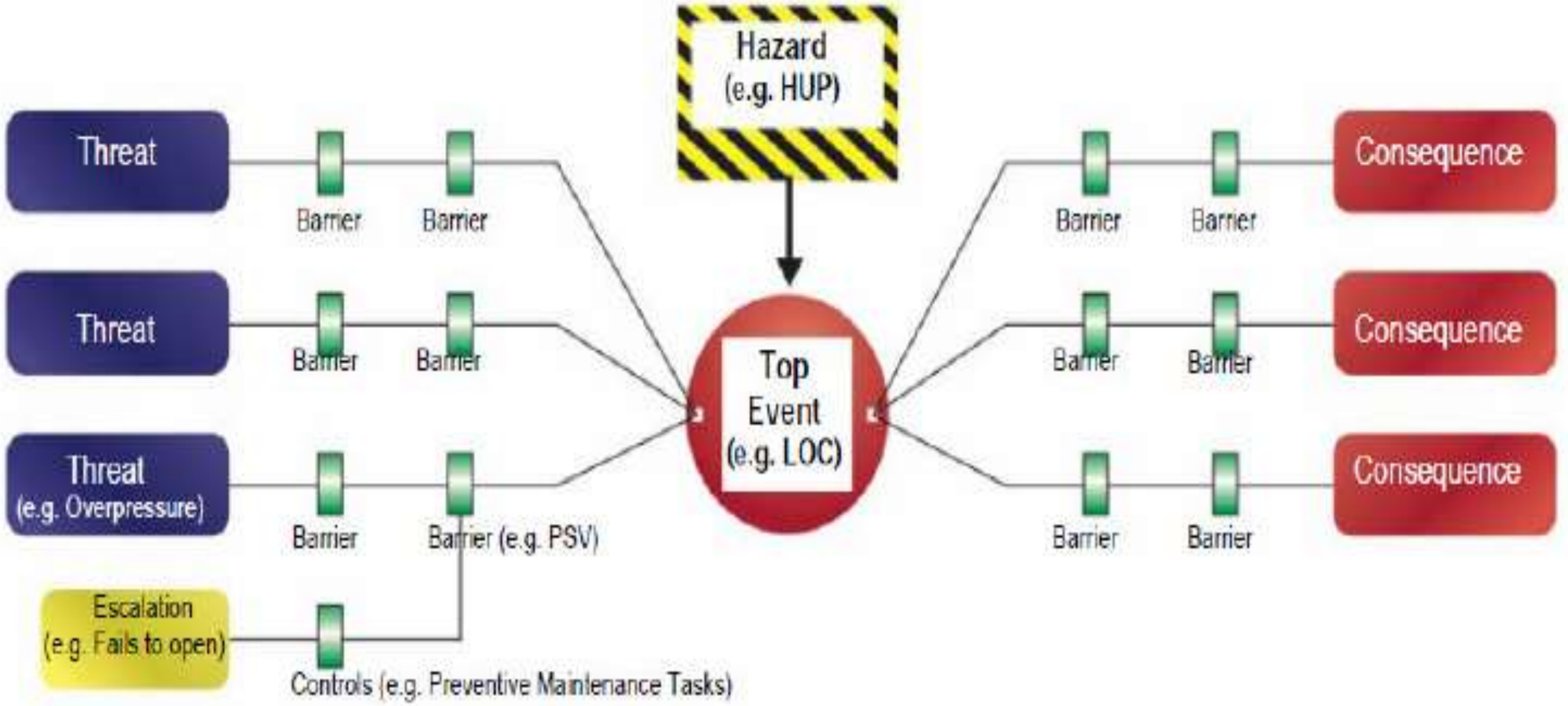
Quantitative and Qualitative process safety review can define risks, hazards and consequences of security incidents in maritime systems, equipment, processes and operations.


Threats
Safety Barrier 1
Safety Barrier 2
Safety Barrier 3
Failure
Hazard 1
Hazard 2
Hazard 3
Consequence : Security Incident
Leading and Lagging Indicators 1
Leading and Lagging Indicators 2
Leading and Lagging Indicators 3

Source: ABS with information elaborated by authors.

BOW TIE ANALYSIS (BTA)

Utilize bow-tie analysis for the identification of security barriers and measures for assets in the micro- and macro- scales .



PREVENTION

MITIGATION

WHY USING BOW-TIE ANALYSIS?

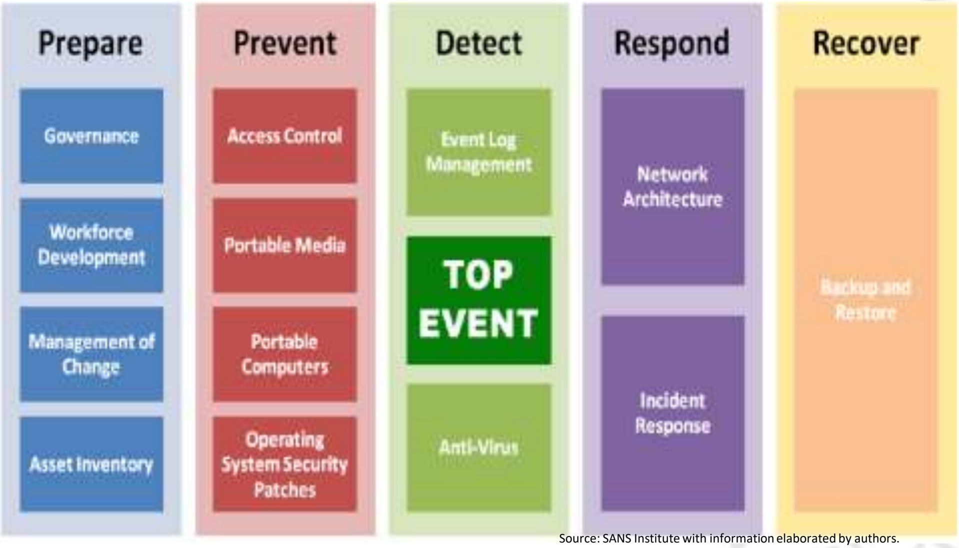
“By linking ‘Hazards’ & ‘Consequences’ to an ‘Event’ it is possible to develop the relationship to include the causes, or ‘Threats’, and the ‘Prevention’ & ‘Recovery Measures’” (ABS)

→ Simple & pragmatic approach
→ Emphasis on effectiveness of risk reduction measures
→ Effective visualization
→ Allows better communication of hazards
→ Can be applied for all types of hazards
→ Increasingly becoming the preferred techniques by regulatory bodies & leading companies
→ Efficiently aided by user-friendly software

WHY USING BOW-TIE ANALYSIS?

"By linking 'Hazards' & 'Consequences' to an 'Event' it is possible to develop the relationship to include the causes, or 'Threats', and the 'Prevention' & 'Recovery Measures'" (ABS)

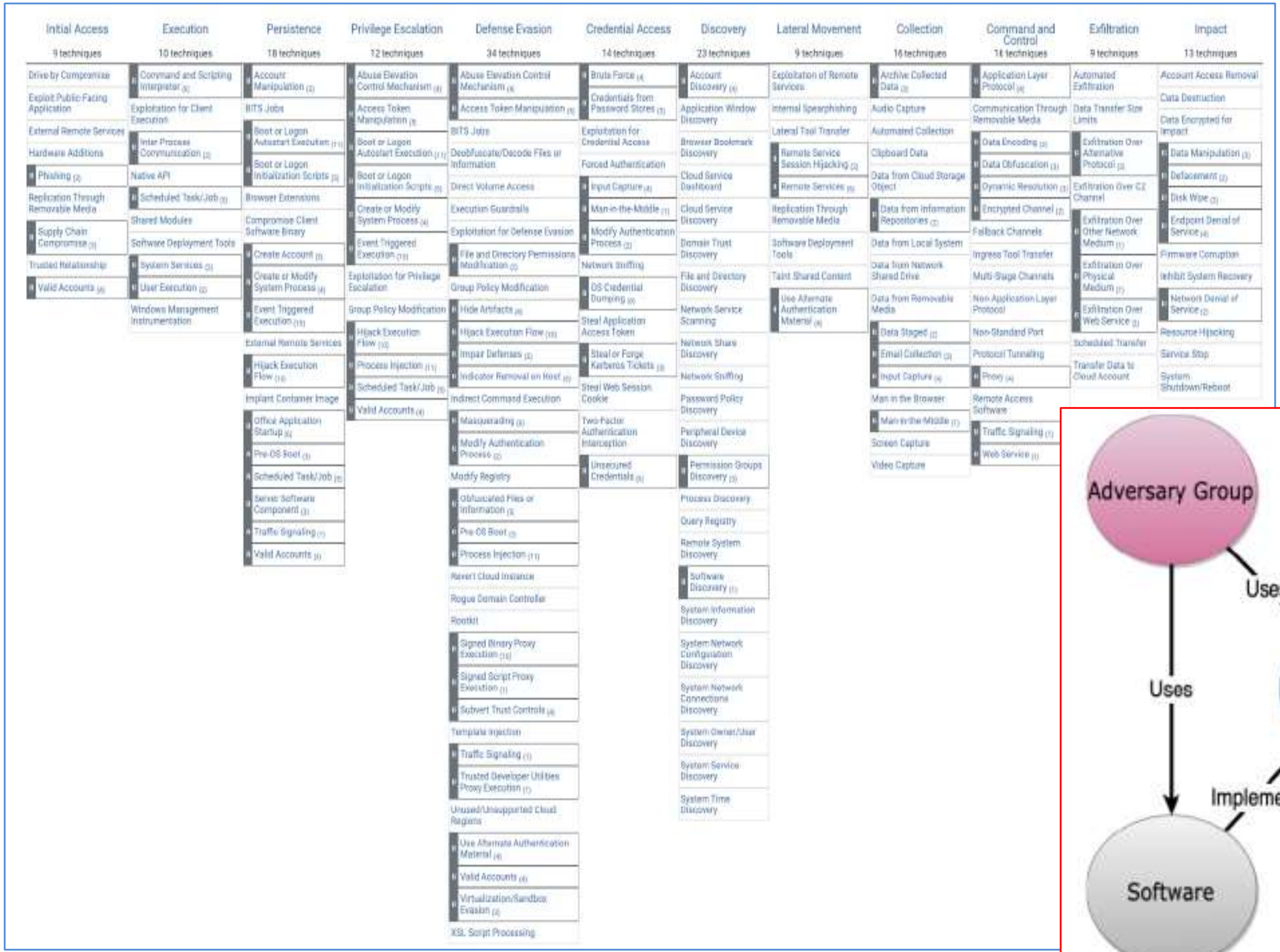
→ Simple & pragmatic approach
→ Emphasis on effectiveness of risk reduction measures
→ Effective visualization
→ Allows better communication of hazards
→ Can be applied for all types of hazards
→ Increasingly becoming the preferred techniques by regulatory bodies & leading companies
→ Efficiently aided by user-friendly software



Source: SANS Institute with information elaborated by authors.

Port ICS Security Bow Tie Analysis

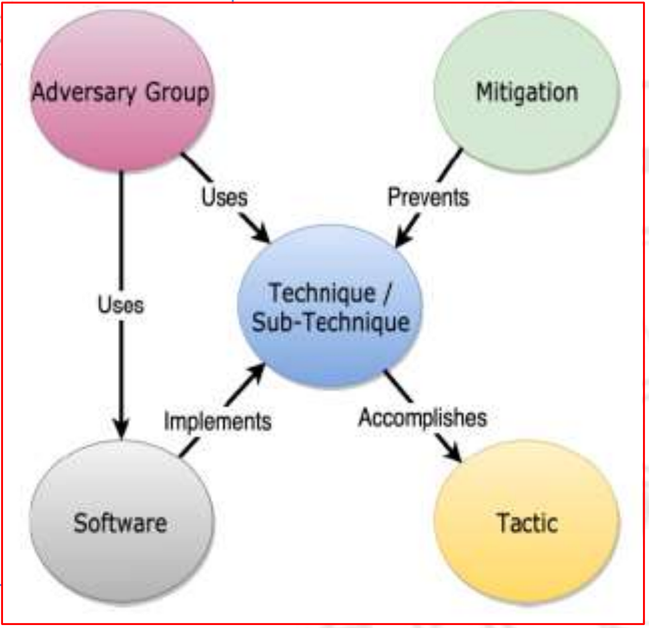
MITRE ATT&CK THREAT MODEL



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques
Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication
Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails	Man-in-the-Middle (1)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (7)	Steal Application Access Token
		Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)
		Scheduled Task/Job (6)		Masquerading (6)	
		Server Software Component (3)		Modify Authentication Process (3)	
		Traffic Signaling (1)		Modify Registry	
		Valid Accounts (4)		Obfuscated Files or Information (5)	
				Pre-OS Boot (3)	
				Process Injection (11)	
				Revert Cloud Instance	
				Rogue Domain Controller	
				Rootkit	
				Signed Binary Proxy Execution (11)	
				Signed Script Proxy Execution (1)	
				Subvert Trust Controls (4)	
				Template Injection	
				Traffic Signaling (1)	
				Trusted Developer Utilities Proxy Execution (1)	
				Unused/Unsupported Cloud Regions	
				Use Alternate Authentication Material (4)	
				Valid Accounts (4)	
				Virtualization/Sandbox Evasion (3)	
				XSL Script Processing	

Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
23 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
Query Registry		Screen Capture	Traffic Signaling (1)		
Remote System Discovery		Video Capture	Web Service (3)		
Software Discovery (1)					
System Information Discovery					
System Network Configuration Discovery					
System Network Connections Discovery					
System Owner/User Discovery					
System Service Discovery					
System Time Discovery					

The Enterprise ATT&CK Matrix



ATT&CK Object Model Relationships

CONCLUSIONS

(1) More industry and government directives and standards need to be developed specifically for ports infrastructure and the maritime transport sector.

(2) The physical protection of assets, processes and IT and OT components in ports infrastructure needs to be enhanced.

(3) The assessment of IT/OT vulnerabilities in ports needs to be improved.

(4) The port industry needs to adopt security assessment methods from other industry sectors.

(5) Cybersecurity training of port infrastructure stakeholders needs to be widely pursued.

(6) The convergence of cyber and physical security for the ports infrastructure and vessels should be pursued.

Thank you
شكرا لك

Prof. Nikitas Nikitakos - nnik@aegean.gr
(University of the Aegean, Chios, Hellas – Greece)

Iosif Progoulakis (PhDc) - iprogoulakis@aegean.gr
(University of the Aegean, Chios, Hellas – Greece)

Prof. Dimitrios Dalaklis
(WMU, Sweden)

CAPT. Razali Yaacob
(Netherland Maritime Institute of Technology, Malaysia)