Cyber-attacks against the Cyber-enabled ship

Critical Infrastructure Security and Resilience Group
Dep. of Information Security and Communication technology

COINS Winter School, Finse, 2019

Ph.D student: Georgios Kavallieratos, georgios.kavallieratos@ntnu.no

Supervisor: Sokratis K. Katsikas

Agenda

- Cyber-enabled ship: aim of the project
- Cyber-enabled ship systems
- Digging deeper to the architecture…
- Security analysis of OT systems
- Maritime Architecture Framework – MAF
- Towards a Cyber-physical Range – C-ES testbed
- Ongoing and future work

Aim of the project

Security of the Cyber-enabled ship, 3 years Project

Goals of the project:

G1: Define a reference architecture for the C-ES:

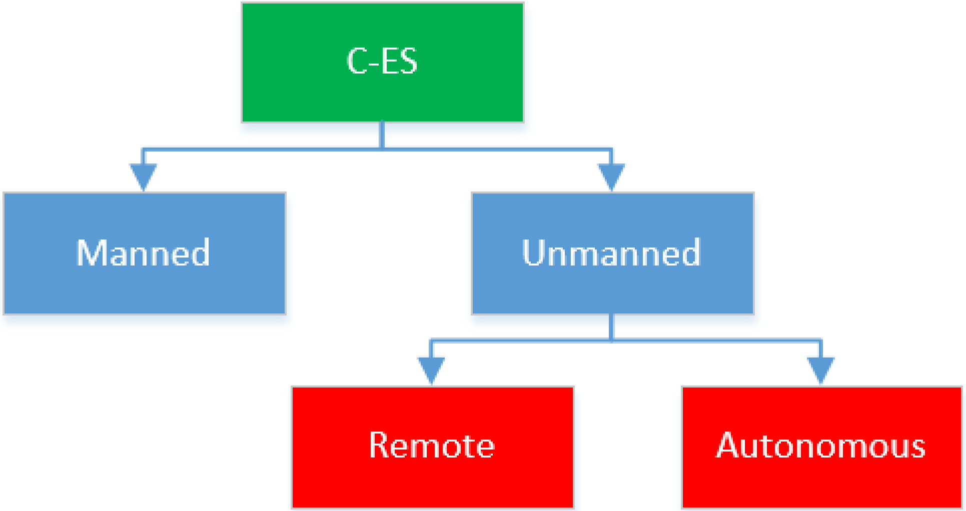
- Identify C-ES's cyber-physical systems
- Clarify systems interconnections and interdependencies

G2: Identify potential security and safety risks.

G3: Propose an appropriate security architecture for the C-ES.

Cyber-enabled ship: what it is..

Autonomous ship security, COINS Winter School, Finse, 2019



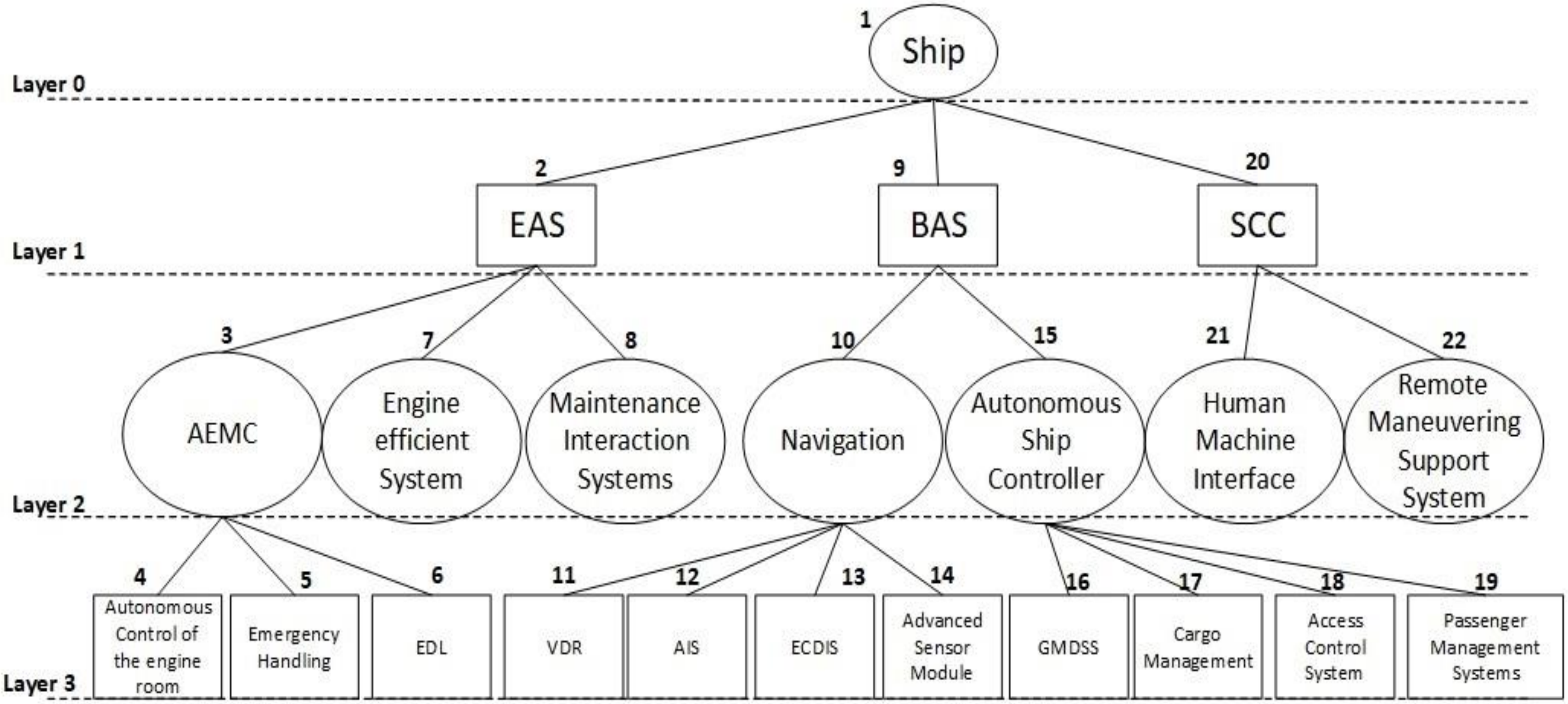
The tasks of operating the ship are performed via a remote control mechanism

Advanced decision support systems on board are responsible for the ship’s operation

Agenda

- Cyber-enabled ship: aim of the project
- **Cyber-enabled ship systems**
- Digging deeper to the architecture…
- Security analysis of OT systems
- Maritime Architecture Framework – MAF
- Towards a Cyber-physical Range – C-ES testbed
- Ongoing and future work

Cyber-Enabled ship systems



System architecture

Digging deeper to the architecture

Engine Automation Systems

- Autonomous Engine Monitoring and Control-AEMC
- Autonomous Control of the Engine Room
- Emergency Handling-EmH
- Engine Data Logger-EDL
- Engine Eciency System-EES
- Maintenance Interaction System-MIS

Shore Control Center

- Human Machine Interface-HMI
- Remote Maneuvering Support System-RMSS

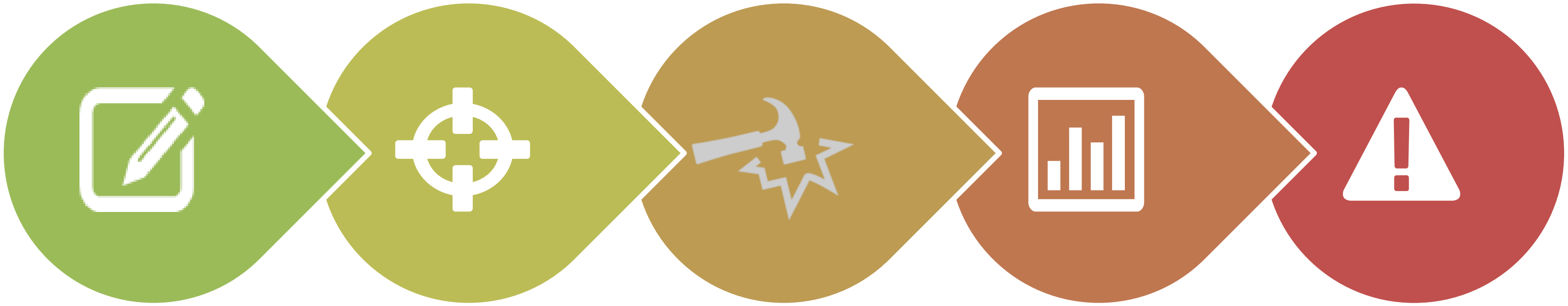
Bridge Automation Systems

- Navigation System
- Voyage Data Recorder-VDR
- Automatic identication system-AIS
- Electronic Chart Display and Information System-ECDIS
- Advanced Sensor Systems-ASS
- Autonomous Ship Controller
- Global Maritime Distress and Safety System-GMDSS
- Cargo Management / Cargo Control Room-CCR
- Access Control system
- Passenger service system

Agenda

- Cyber-enabled ship: aim of the project
- Cyber-enabled ship systems
- Digging deeper to the architecture…
- **Security analysis of OT systems**
- Maritime Architecture Framework – MAF
- Towards a Cyber-physical Range – C-ES testbed
- Ongoing and future work

Security analysis of OT systems



System Identification

- Identify System Architecture
- Analyze Interconnections

Attack Development

- Develop STRIDE attack scenarios

Impact Deternination

- According to specific Criteria

Likelihood Determination

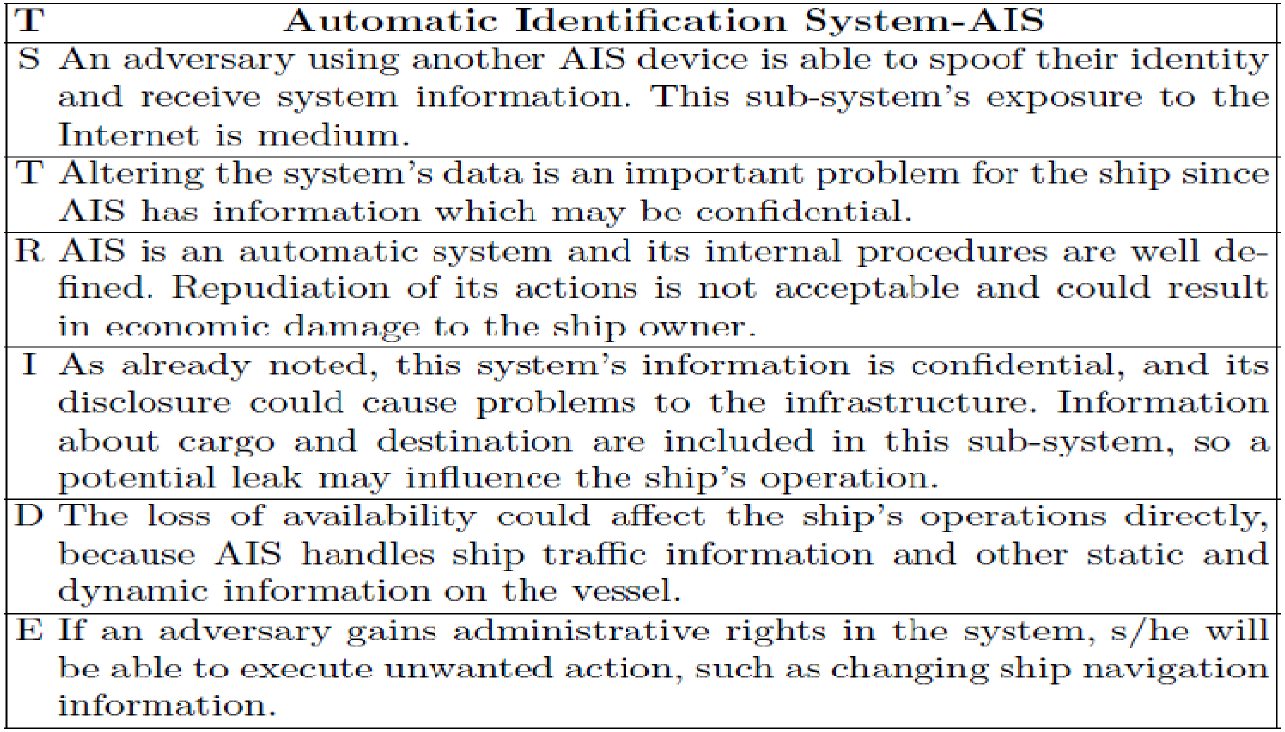
- According to specific Criteria

Risk Analysis

- Risk Matrix

STRIDE-Attack scenarios -AIS

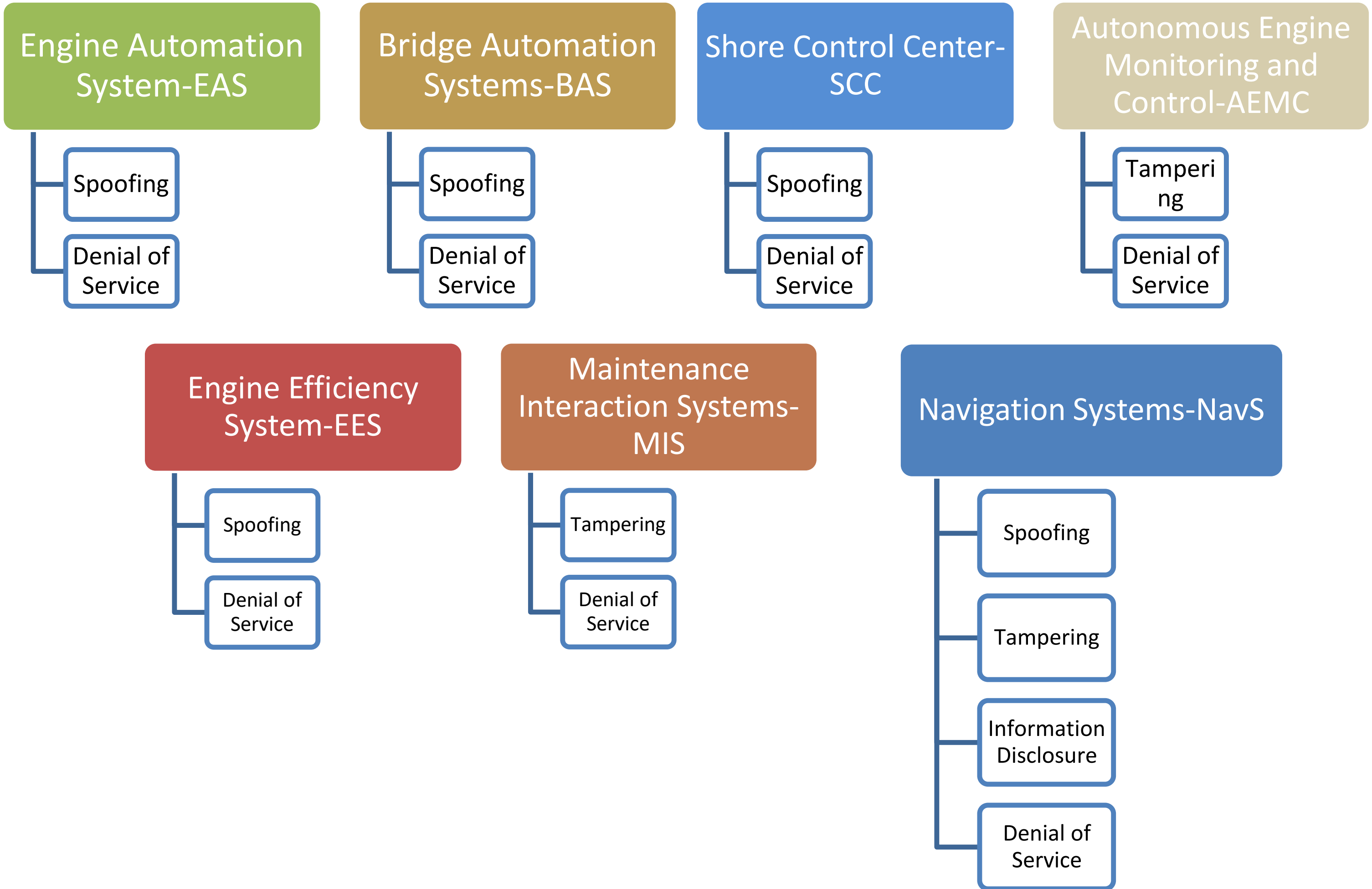
- **STRIDE** — **Security Properties**
  - **S**poofing → Authentication
  - **T**ampering → Integrity
  - **R**epudiation → Non-repudiation
  - **I**nformation disclosure → Confidentiality
  - **D**enial of service → Availability
  - **E**levation of privileges → Authorization



T	Automatic Identification System-AIS
S	An adversary using another AIS device is able to spoof their identity and receive system information. This sub-system's exposure to the Internet is medium.
T	Altering the system's data is an important problem for the ship since AIS has information which may be confidential.
R	AIS is an automatic system and its internal procedures are well defined. Repudiation of its actions is not acceptable and could result in economic damage to the ship owner.
I	As already noted, this system's information is confidential, and its disclosure could cause problems to the infrastructure. Information about cargo and destination are included in this sub-system, so a potential leak may influence the ship's operation.
D	The loss of availability could affect the ship's operations directly, because AIS handles ship traffic information and other static and dynamic information on the vessel.
E	If an adversary gains administrative rights in the system, s/he will be able to execute unwanted action, such as changing ship navigation information.

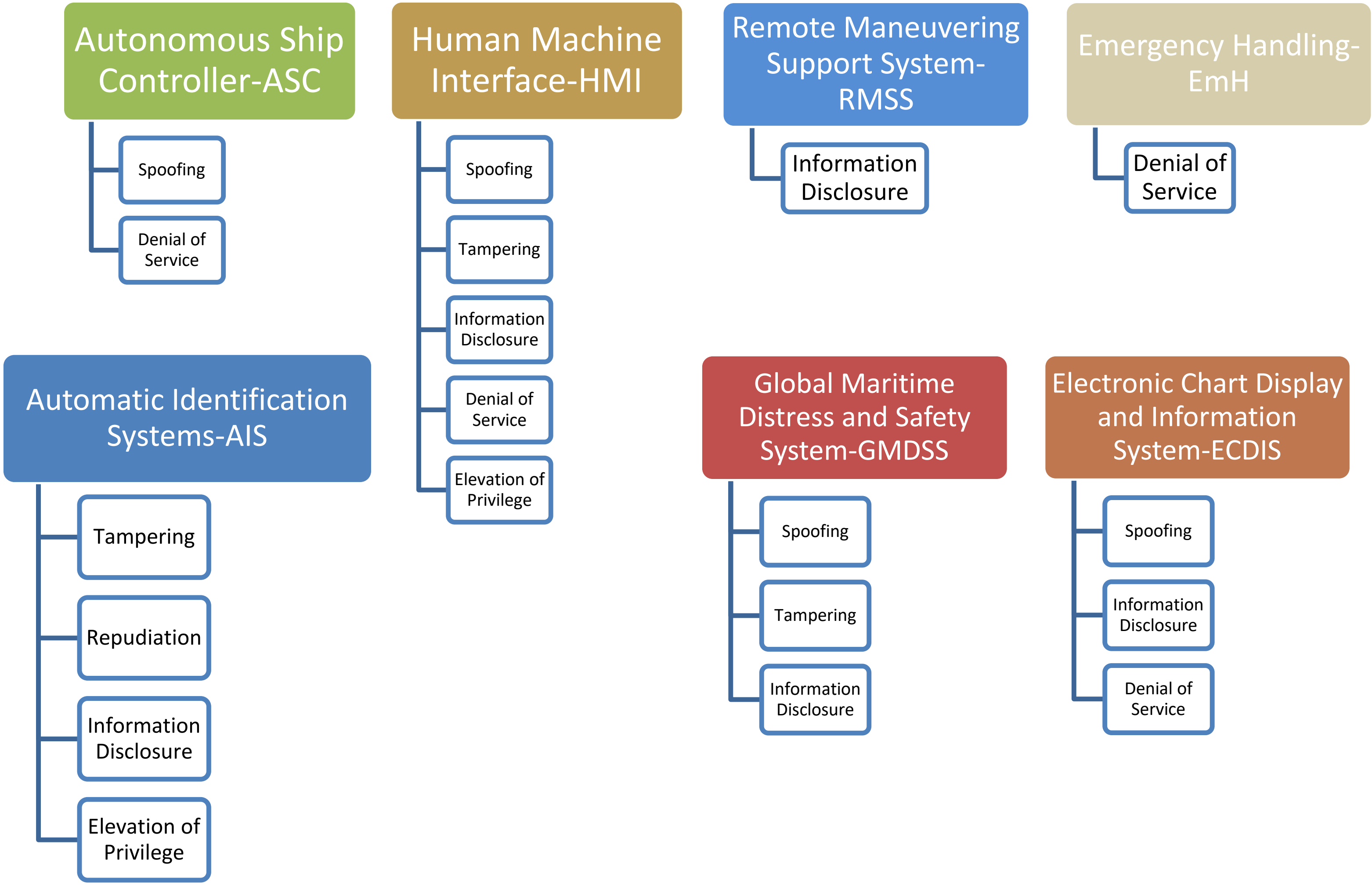
STRIDE Highly critical threats (1/2)

Autonomous ship security, COINS Winter School, Finse, 2019



- Engine Automation System-EAS
  - Spoofing
  - Denial of Service
- Bridge Automation Systems-BAS
  - Spoofing
  - Denial of Service
- Shore Control Center-SCC
  - Spoofing
  - Denial of Service
- Autonomous Engine Monitoring and Control-AEMC
  - Tamperi ng
  - Denial of Service
- Engine Efficiency System-EES
  - Spoofing
  - Denial of Service
- Maintenance Interaction Systems-MIS
  - Tampering
  - Denial of Service
- Navigation Systems-NavS
  - Spoofing
  - Tampering
  - Information Disclosure
  - Denial of Service

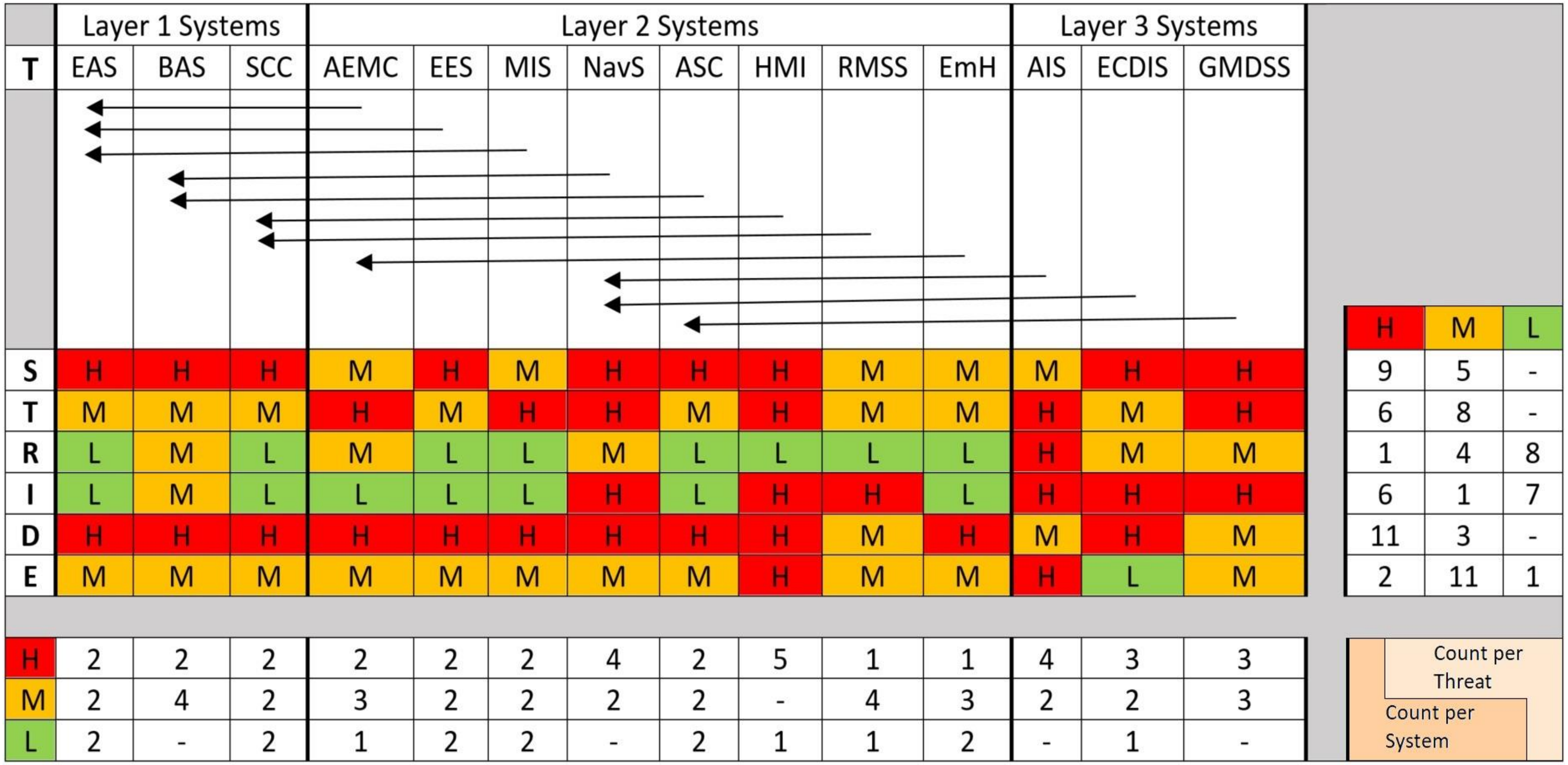
STRIDE Results (2/2)



- Autonomous Ship Controller-ASC
  - Spoofing
  - Denial of Service
- Human Machine Interface-HMI
  - Spoofing
  - Tampering
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege
- Remote Maneuvering Support System-RMSS
  - Information Disclosure
- Emergency Handling-EmH
  - Denial of Service
- Automatic Identification Systems-AIS
  - Tampering
  - Repudiation
  - Information Disclosure
  - Elevation of Privilege
- Global Maritime Distress and Safety System-GMDSS
  - Spoofing
  - Tampering
  - Information Disclosure
- Electronic Chart Display and Information System-ECDIS
  - Spoofing
  - Information Disclosure
  - Denial of Service

Security analysis summary

Autonomous ship security, COINS Winter School, Finse, 2019



	Layer 1 Systems			Layer 2 Systems								Layer 3 Systems					
T	EAS	BAS	SCC	AEMC	EES	MIS	NavS	ASC	HMI	RMSS	EmH	AIS	ECDIS	GMDSS	H	M	L
S	H	H	H	M	H	M	H	H	H	M	M	M	H	H	9	5	-
T	M	M	M	H	M	H	H	M	H	M	M	H	M	H	6	8	-
R	L	M	L	M	L	L	M	L	L	L	L	H	M	M	1	4	8
I	L	M	L	L	L	L	H	L	H	H	L	H	H	H	6	1	7
D	H	H	H	H	H	H	H	H	H	M	H	M	H	M	11	3	-
E	M	M	M	M	M	M	M	M	H	M	M	H	L	M	2	11	1
H	2	2	2	2	2	2	4	2	5	1	1	4	3	3			
M	2	4	2	3	2	2	2	2	-	4	3	2	2	3			
L	2	-	2	1	2	2	-	2	1	1	2	-	1	-			

Count per Threat

Count per System

S	T	R	I	D	E

Agenda

- Cyber-enabled ship: aim of the project
- Cyber-enabled ship systems
- Digging deeper to the architecture…
- Security analysis of OT systems
- **Maritime Architecture Framework – MAF**
- Towards a Cyber-physical Range – C-ES testbed
- Ongoing and future work

Maritime Architecture Framework-MAF

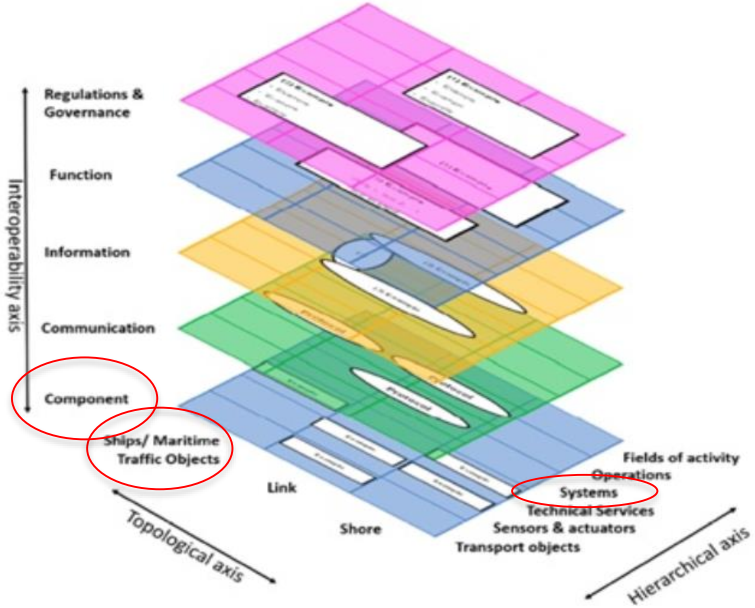
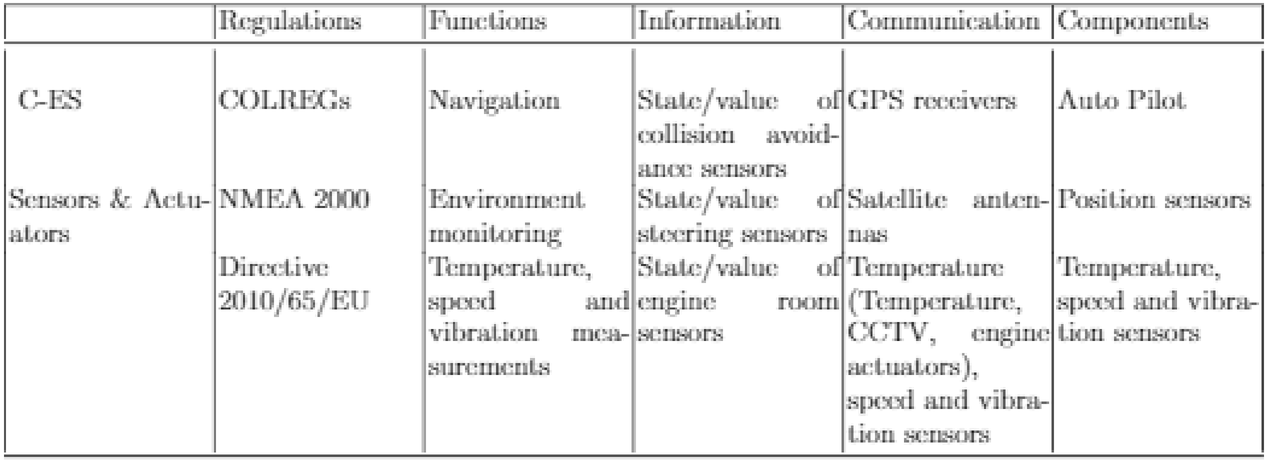


Fig. 2: MAF cube

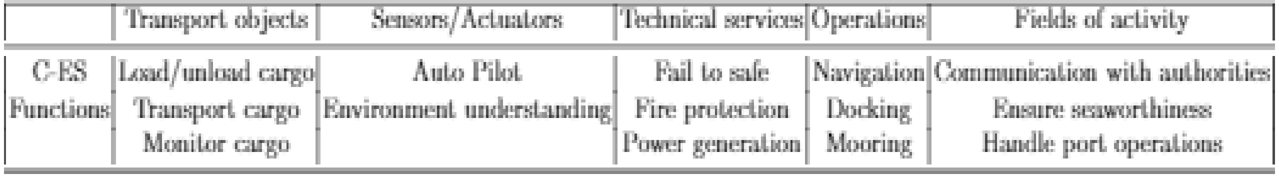
- Identify vessel's cyber-physical systems
- Clarify their interconnections, dependencies and interdependencies

Maritime Architecture Framework-MAF



	Regulations	Functions	Information	Communication	Components
C-ES	COLREGs	Navigation	State/value of collision avoidance sensors	GPS receivers	Auto Pilot
Sensors & Actuators	NMEA 2000	Environment monitoring	State/value of steering sensors	Satellite antennas	Position sensors
	Directive 2010/65/EU	Temperature, speed and vibration measurements	State/value of engine room sensors	Temperature (Temperature, CCTV, engine actuators), speed and vibration sensors	Temperature, speed and vibration sensors

Figure 1. Interoperability axis of the C-ES



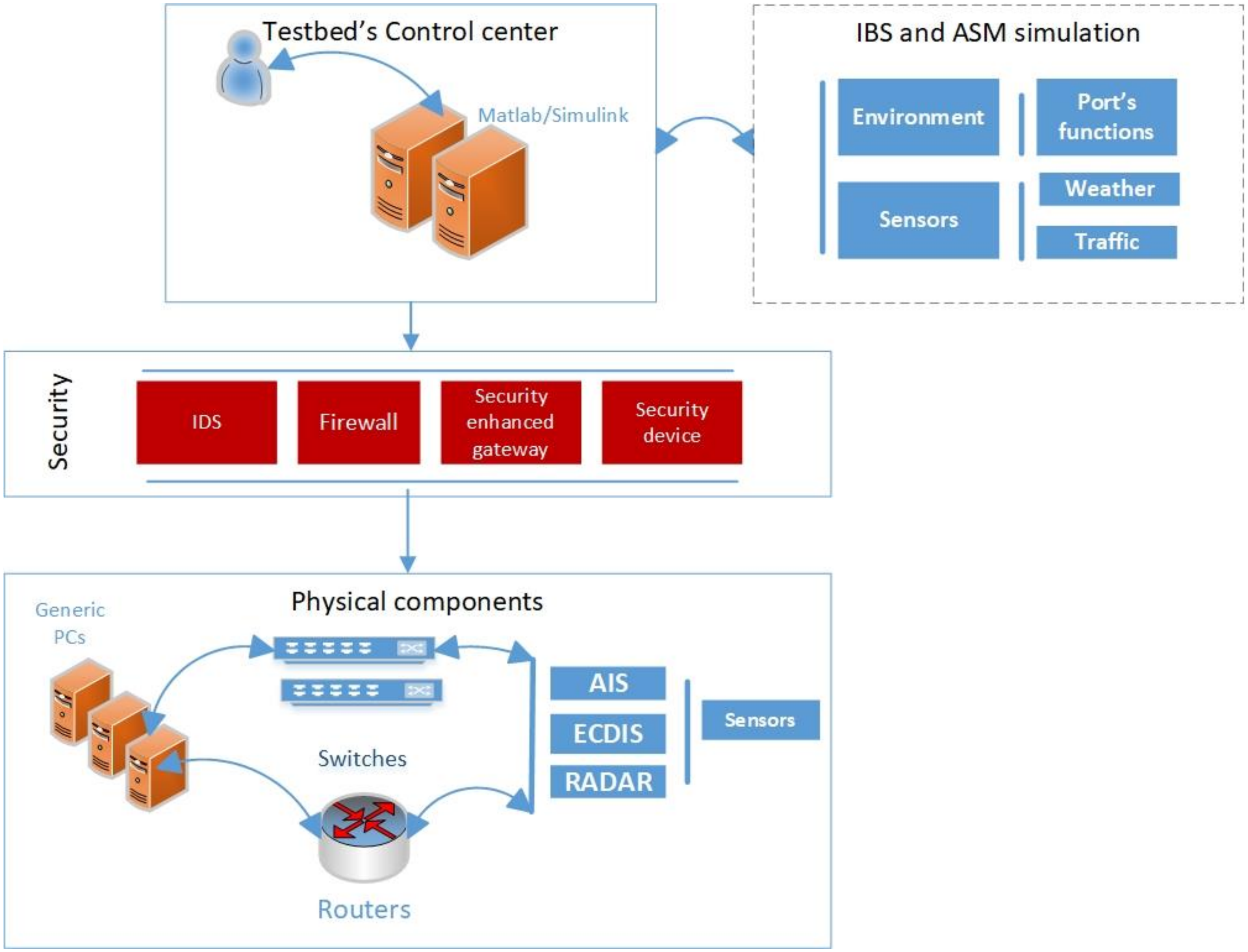
	Transport objects	Sensors/Actuators	Technical services	Operations	Fields of activity
C-ES	Load/unload cargo	Auto Pilot	Fail to safe	Navigation	Communication with authorities
Functions	Transport cargo	Environment understanding	Fire protection	Docking	Ensure seaworthiness
	Monitor cargo		Power generation	Mooring	Handle port operations

Figure 2. Hierarchical axis of the C-ES

Agenda

- Cyber-enabled ship: aim of the project
- Cyber-enabled ship systems
- Digging deeper to the architecture…
- Security analysis of OT systems
- Maritime Architecture Framework – MAF
- **Towards a Cyber-physical Range – C-ES testbed**
- Ongoing and future work

Towards a Cyber-physical Range: A use case for the C-ES



Ongoing and future work

- Currently we are working on the security requirements elicitation for the C-ES using SecureTropos methodology.

- As future work, we will implement the aforementioned testbed and we will define an appropriate risk assessment method that combines safety and security risks aiming to propose a secure system architecture.

○ *Publications*: 1) Cyber-attacks against the autonomous ship, *Georgios Kavallieratos, Sokratis Katsikas and Vasileios Gkioulos, CyberICPS 2018, Barcelona*
2) Towards a Cyber-physical Range, *Georgios Kavallieratos, Sokratis Katsikas and Vasileios Gkioulos,* AsiaCCS 2019*, New Zealand*

Thank you!
Questions?