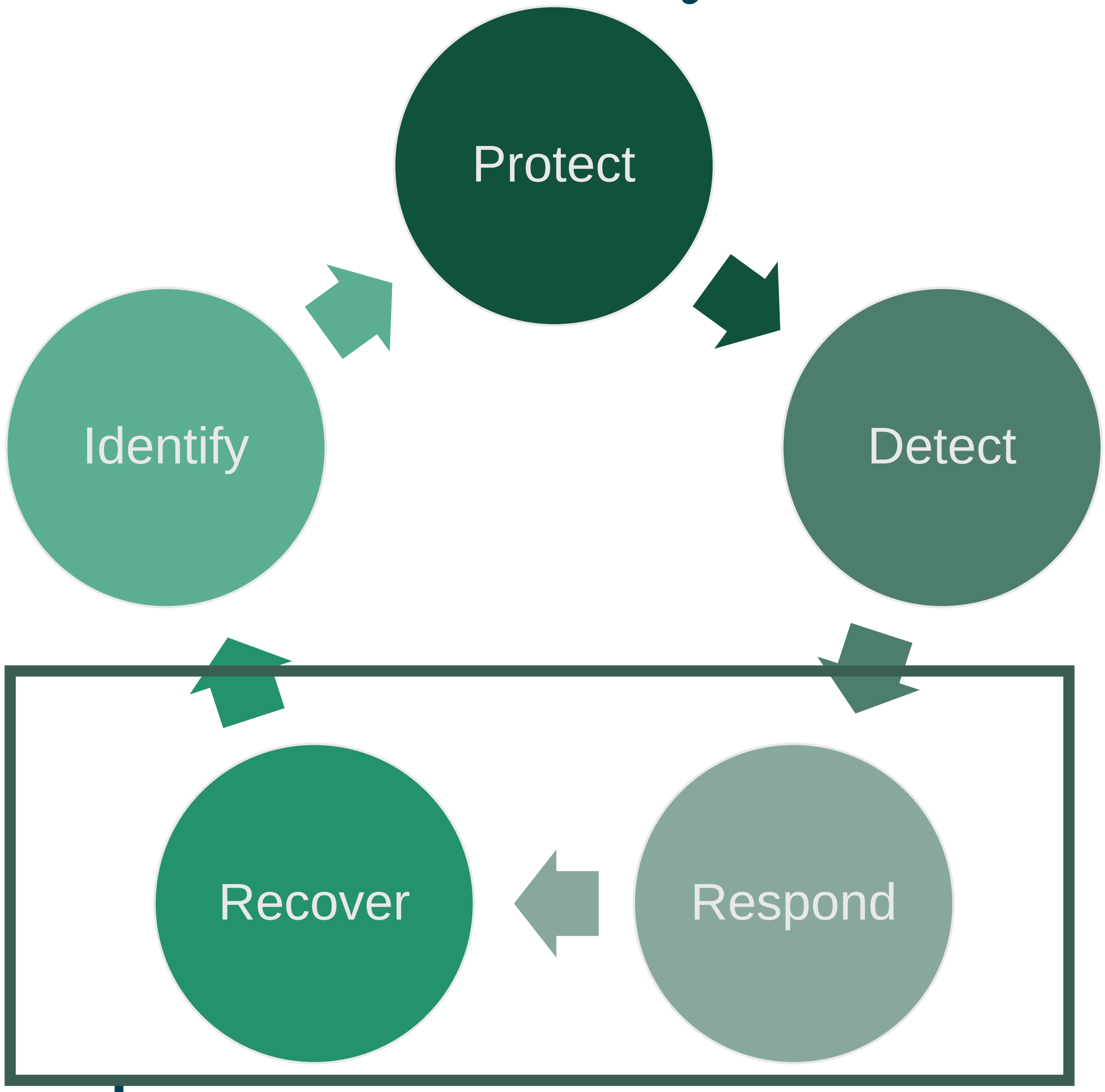
indra

Geospatial World Forum

Juan – Román Martinez Arranz

16/05/2024

Ciber-resiliency



Aspectos Clave

- It has become a key element of Information Security
- Focus: maintain operation even while receiving constant attacks
- Ensure at all times the protection of critical services to maintain operation
- Ensure at all times the Confidentiality, Integrity and Availability of Information

AI Concepts reminder

Frugality

- Ability to generate Models that work perfectly despite having a shortage of data

Robustness

- Ability of an AI Model to continue functioning correctly despite having some “anomalous” data sets, new/changing circumstances, and/or enemy attacks

Explicability

- Ability of the system to explain an AI Model and its reasoning followed to propose a solution or action or decision.

Human-in-the-loop:

- Integrate human beings into critical decision making.

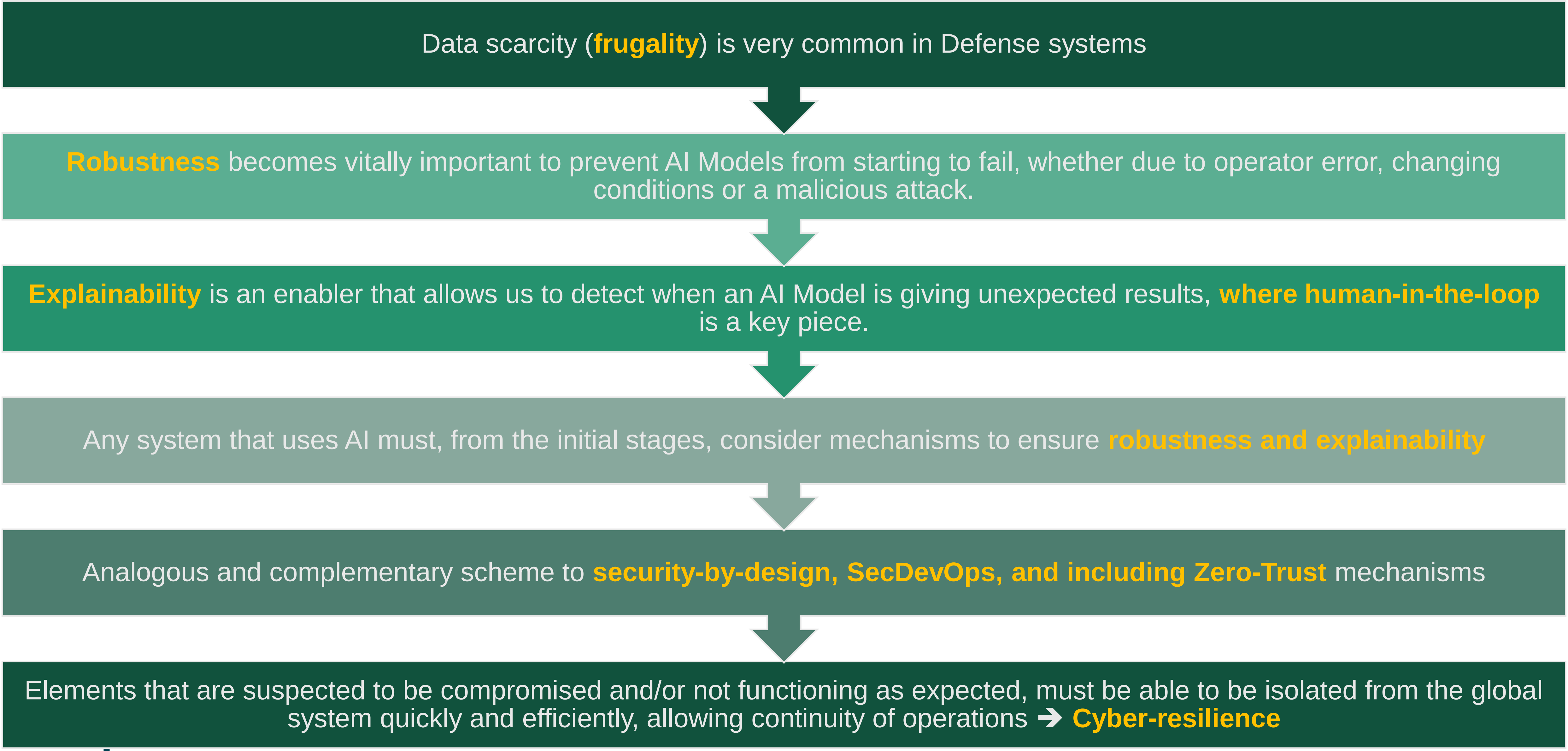
AI Digital Twin:

- Digital copy of a system to replicate behaviors, in this case, AI systems

Intelligent Data fussion

- Collection of data from different sources and types that are combined and used in AI Models to discover new threats and improve situational awareness

Our point of view



Data scarcity (**frugality**) is very common in Defense systems

Robustness becomes vitally important to prevent AI Models from starting to fail, whether due to operator error, changing conditions or a malicious attack.

Explainability is an enabler that allows us to detect when an AI Model is giving unexpected results, **where human-in-the-loop** is a key piece.

Any system that uses AI must, from the initial stages, consider mechanisms to ensure **robustness and explainability**

Analogous and complementary scheme to **security-by-design, SecDevOps, and including Zero-Trust** mechanisms

Elements that are suspected to be compromised and/or not functioning as expected, must be able to be isolated from the global system quickly and efficiently, allowing continuity of operations ➔ **Cyber-resilience**

Our Point of View

We analyze the **Confidentiality and cybersecurity** of AI to equip it with reliable mechanisms, which requires iteratively analyzing all aspects that can influence the performance of AI models (from data collection to the implementation of the model in final applications).

These considerations are even more true when we consider the ability of AI systems to resist and counter **cyberattacks** and **hybrid threats.**

Confidentiality and cybersecurity must be planned from the design phase to avoid re-planning the AI construction process, delaying the deployment of the models. Especially critical in cybersecurity situations that require the implementation of proactive countermeasures in reasonable time frames.

AI models can be attacked (intentionally or by operator error) to disrupt their inference process, which can cause critical consequences for the lives of people, society and Defense systems. The focus will be on Impact.

Our approach is to accelerate the analysis of cyber attacks on systems through machine learning using **digital twins and generative AI.**

Frugality, Robustness & Explicability on Sea Domain

Frugality

Development of algorithms for ATD/ATR through image processing.

Due to the small number of images available, the models are trained so that they are capable of detecting and recognizing targets, achieving accurate results despite said scarcity.

Escalability & Interoperability

Modular, interoperable and scalable algorithms are being developed to expand their use and functionalities.

Integration between ATD/ATR on sea domain with land and air domain systems to improve situational awareness

Robustnes y explicability

The models are capable of giving accurate results under changing conditions, such as fog, lack of light or LoS disturbed by orography. Furthermore, the developed models maintain precision in case of receiving manipulated or erroneous data. All suggested decisions are (self) explained efficiently to operators and users so that they can assess their possible use, as well as help detect when the algorithms could be failing.

MLOPS for underwater security and surveillance

Maritime and Underwater Surveillance

We work to enhance the security of ports and maritime borders, improving surveillance and security, including underwater security, taking advantage of the power of Artificial Intelligence (AI), using integrated systems capable of providing data on threat detection and analysis between 3 main elements :

- Port security infrastructure
- Advanced underwater detection systems
- Surveillance vessels with enhanced capabilities

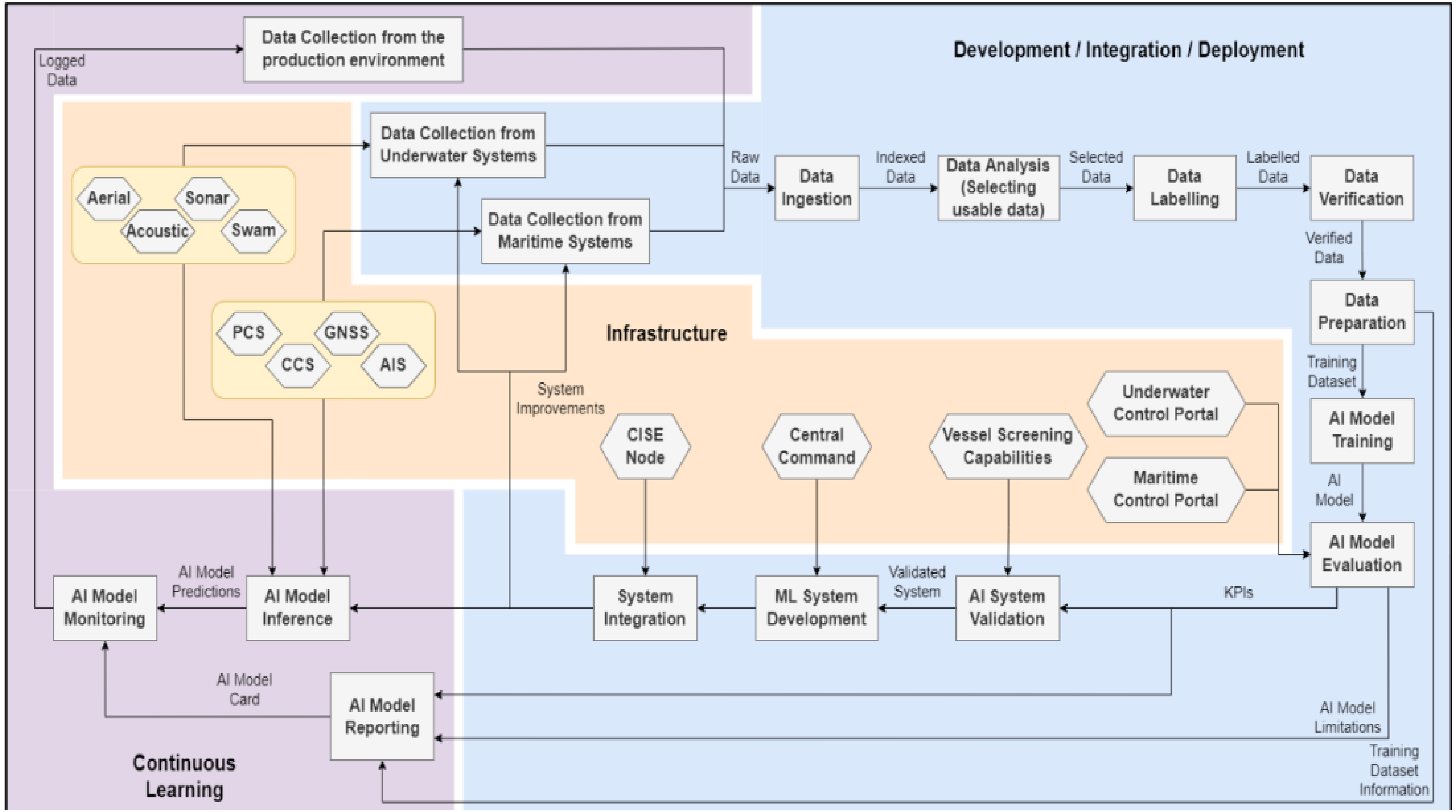
Systems

- Acoustic detection (hydrophones)
- Sonar for rapid boat hull scanning
- High resolution sonar inspection
- UUV swarm collective autonomous location

Data sources: PCS, CCS, AIS, CISE, **GNSS**

- UC1: Detection of Narco-Submarines and explosives. (Valencia)
- UC2: Detection of illegal trafficking and transportation (Elefsina and Heraklion)
- UC3: Prevention and detection of sabotage, type Nordstream (Drammen)

MLOPS for Maritime surveillance and security



Digital Twins and AI Models

Reinforcement Learning

A system that collects all information in a digital twin can help the human supervisor make proactive decisions and adjust the robustness of AI models by applying recommendations to the original machine learning process.

Security

At the same time, overall access and control of the underlying AI architecture must be secure with robust mechanisms that protect computation and storage.

Development and testing with Digital Twins

The main idea is that digital twins are created from applications or systems that run AI models. This digital environment combined with generative techniques can be used to comprehensively test, validate and verify the robustness of models against a variety of attacks and countermeasures.

Data Fusion and covert sensing

Data engineering

We work with heterogeneous data collaboratively, including the management layer that maximizes the use of resources.

The main data fusion capabilities are worked on, as well as the communication needs between the different systems involved.

Decisión Making

Using AI to improve decision support, covert detection and to help maximize covert capabilities in support of Dynamic Management

Data sources and collaboration

The set of available systems should not be limited to those found on a specific platform, and can be drawn from other sources.

The system enables synthetic reference image generation and anomaly detection to complement AI/ML-based approaches.

AI for ISR

EW

AI applied to threat monitoring and countermeasure, improving the detection of complex emitters and saturated environments as well as the application of responses.

EW+EO/IR

Image processing from electro-optical and infrared sensors and EW for defense, fusing advanced technologies and synthetic data in the development and validation of specialized algorithms.

Advanced management of Sensor

Management and synchronization of resources between sensors from different platforms for defense tasks, taking advantage of AI algorithms for analysis, monitoring, and optimized collaboration that improves the response to critical situations.

Maritime SA and Decisión-Making on Sea domain

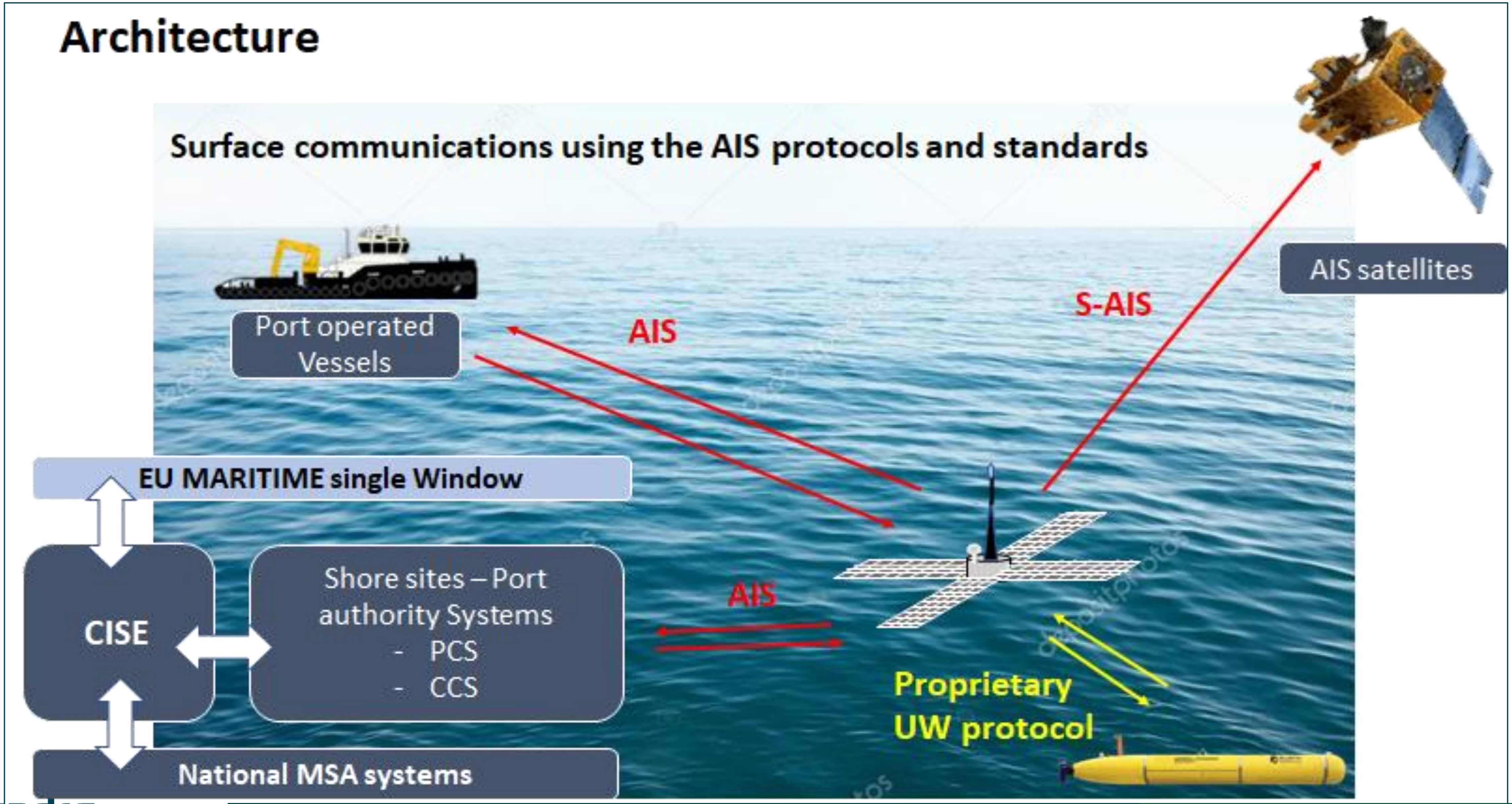
Automatisation

- Automated operation of incident management processes through Artificial Intelligence.
- Focus: Incident management and cyber defense processes.
- Detection, mitigation and response to security challenges semi-automatically or automatically.
- Support for human operators, analysts: Decision making.
- Strengthening military infrastructures and protection against advanced cyber threats.

Situational Awareness

Development and implementation of innovative theoretical foundations, methods, research prototypes and integration towards the provision of a European operational platform for the management of cyber situational awareness in real time with rapid defensive response capabilities and support for decision making of the military end users.

Maritime SA and Geospatial collaboration


Architecture
Surface communications using the AIS protocols and standards
AIS satellites
S-AIS
AIS
Port operated Vessels
EU MARITIME single Window
CISE
Shore sites – Port authority Systems
- PCS
- CCS
AIS
Proprietary UW protocol
National MSA systems

SMAUG example

SMAUG has defined three UCs, all of which have the following common features and aspects:

1. **Integration of information coming from different sources**: All SMAUG's UCs will use the information coming from PCS, CCS, GNSS, AIS as well as the data coming from the different underwater and aerial sensors and vehicles involved.

2. **Vessel Screening capacities**: All UCs will improve vessels used in ports surveillance. This improvement will be based in the definition, implementation, creation and testing process of screening capabilities and capacities of these vessels' sensors.

3. **Type of Members participating in the Use Cases**: The result of the execution of all UCs will be validated by the four **Border/Coastal** guards of the SMAUG's consortium as well as by the corresponding **Port Authority**. In this sense, every use case will have at least one national Coastal/Border Guard, a Port Authority, and Academia and Industria (SME o Large).

4. **Common Expected outcomes**: SMAUG will provide an increase of knowledge in the following disciplines during the execution of all Use cases:

- Decision making: an AI model capable to provide port operators with a proportional response or actions when a threat is detected.

- MLOps methodology: a continuous integration methodology of AI models will be used to keep a robust system ensuring retraining when diverging and being up to date to work accurately with current data**.**

- Alert generation: an AI model able to generate alerts with sensor fusion of all the information from all sources involved.

- Enhancement of C2 capabilities: Develop the capacity to detect underwater systems connected to the C2 PSIM and VTS systems that manage the security of port infrastructures and maritime traffic.1

Main Objective

The primary goal of SMAUG is to improve the underwater detection of threats in ports and their entrance routes, by means of an integrated system capable of providing data concerning threat analysis between 3 main elements: ports security infrastructure, advanced underwater detection systems and surveillance vessels. Underwater detection and location will be performed by four primary methods: i) acoustic detection, where a series of hydrophones will listen for sounds emitted by small underwater vehicles and will be processed by artificial intelligence methods, ii) rapid sonar hull scan, used to scan ships hulls and perform harbour floor scanning, iii) high resolution sonar inspection, to inspect objects in water with poor visibility and iv) collective autonomous location, where a swarm of autonomous underwater vehicles will act cooperatively. This will provide information to Artificial Intelligence modules which will improve the way detecting illicit and dangerous goods and/or of threats hidden below the water surface is currently done, taking into account sources such as Unmanned Surface Vehicle Systems, (USV), underwater remote operation vehicle (ROV), UAV (Aerial autonomous vehicle) and Port current information sources. The combination of these tools will allow SMAUG to prompt solutions capable of detecting possible threats to infrastructure or vessels, as well as identify vessels with concealed goods.

Building blocks

Maritime infaestructures security

- Port Community Systems (PCS) and Cargo Community Systems (CCS)
- **GNSS, Sentinel and Corpernicus**
- AIS

Underwater detection

- Acoustic (underwater) and Sonar (underwater)
- **Aerial (Surface)**
- Collective via Swarn (Underwater)

Combination of data sources

- Maritme C2 Portal and Underwater C2 Portal
- Central Command Portal
- CISE Node Integration

Semi/Autonomous Vessel screening

- Vessel screening capabilities improvement

Benefits of Geospatial and Maritime Collaboration

WI1: Improved security of EU land and air borders, as well as sea borders and maritime environment, infrastructures and activities, against accidents, natural disasters and security challenges such as illegal trafficking, piracy and potential terrorist attacks, cyber and hybrid threats;	
38% of all criminal activities in the EU are connected to drug trafficking. How drugs are used and are trafficked is constantly changing and the ways they are trafficked is ever-growing in technical and organisational complexity. SMAUG’s result will help reduce illegal traffic by the following improvements in 5 years. The rise in illicit cigarette consumption, particularly counterfeits, shines a spotlight on the increasing number of adult smokers who are turning to illicit tobacco, particularly as economic pressures increase. With the help of SMAUG’s solutions, a sizeable reduction of this illegal market will be feasible.	
KPI	**Target (Y5+)**
WI-KPI-1: Kilos of drugs seized	> 50%
WI-KPI-2: Kilos of illegal tobacco seized	>100%
WI-KPI-3: Shipments of illegal tobacco and drugs detected	> 50%
WI2: Improved security of maritime infrastructures and maritime transport strengthening the detection, prevention and response to illicit activities near the sea harbours by monitoring the movement and position of suspicious vessels	
The combination of the information from positioning systems based on GNSS and AIS transponders from the vessels together with the monitoring capabilities provided by Copernicus Earth observation satellites and the deployed unmanned platforms and the application of ML algorithms to the extracted data flows will enhance the situational awareness of the authorities.	
KPI	**Target (Y5+)**
WI-KPI-4: Number of unregistered boats and vessels detected	> 100%
WI-KPI-5: Number of boats and vessels departing a planned route detected	> 50%
WI3: Improved customs and supply chain security though better prevention, detection, deterrence and fight of illegal activities involving flows of goods across EU external border crossing points and through the supply chain, minimising disruption to trade flows.	
There are two methods used when unregistered vessels approach coastlines: one is to reach land by evading detection of authorities; the other is to leave the illegal goods near the coast and send the position (e.g., lat-lon) to their counterparts in the destination countries who will retrieve the illegal goods at a later date. In both situations, detecting smuggling vessels at sea is a key challenge for coastal states which may have limited resources and large search and rescue areas of responsibility.	
KPI	**Target (Y5+)**
WI-KPI-6: Increase the maritime area covered by surveillance systems in ports	>40%
WI-KPI-7: To improve intercommunication times between AIS, CISE and PCS	Real time

indra

At the core