Maritime Cybersecurity:

Some Machine Learning contributions faced with an increasingly digital sector

Clet Boudehenn

Naval Cyber Chair – French Naval Academy

Who am I ?

Ph. D. Student – French Naval Academy – Chair of Naval Cyber Defense

- **Research Laboratory**

- **Collaboration with engineering schools, French Navy and defense Industry.**

- **Several research fields:**
  - Cyber protection
  - Cyber resilience
  - Cyber defense

Maritime context

Maritime trade : main place for worldwide goods exchange

- **90% of world trade** (by volume)

- **80%** (by value)

- **290 tons of goods every second**

- more than **50,000 merchant ships** sailing in international waters.

Maritime context: *an increasingly digital sector*

Computer systems (IT & OT) are now everywhere on board !

Complex set of industrial and on- board systems :
ICS (Industrial Control Systems),
SCADA (Supervisory Control and Data Acquisition),
GNSS (Global Navigation Satellite System).

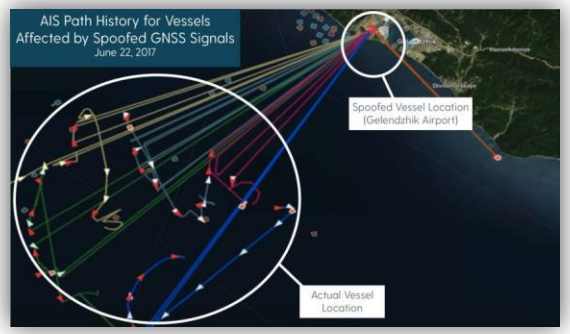
These systems are no cyber secured by design and carry a plenty of vulnerabilities.

Increase of cyber attacks on *CPS* (Cyber Physical Systems) ***GPS*** (Global Positioning System) **and *AIS*** (Automatic Identification System).

Navals Systems – GNSS Vulnerabilities

New security challenges have emerged

- *GPS Jamming*
- *GPS Spoofing*



Spoofed vessel in the Black Sea (22-24 June 2017)

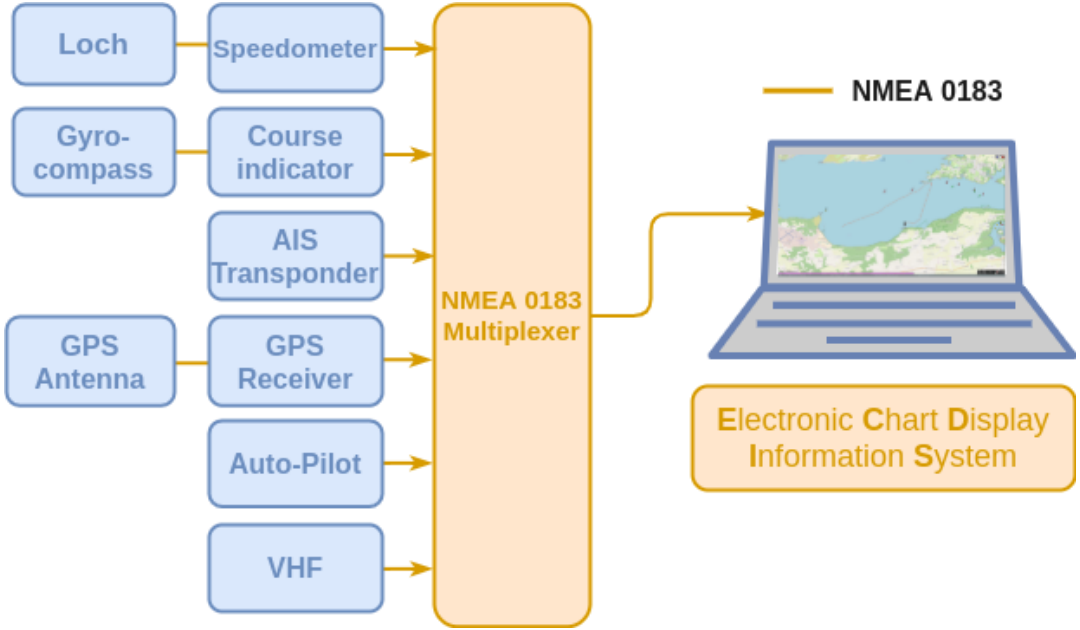
British tanker boarded by Iranian Coastguard in the Persian Guld

Possible impacts and consequences :

- Navigation discrepancies : potential groudings (in narow waters or channels).
- Violation of foreign territorial waters, potential boardings.

Architecture of the navigation systems – NMEA standard

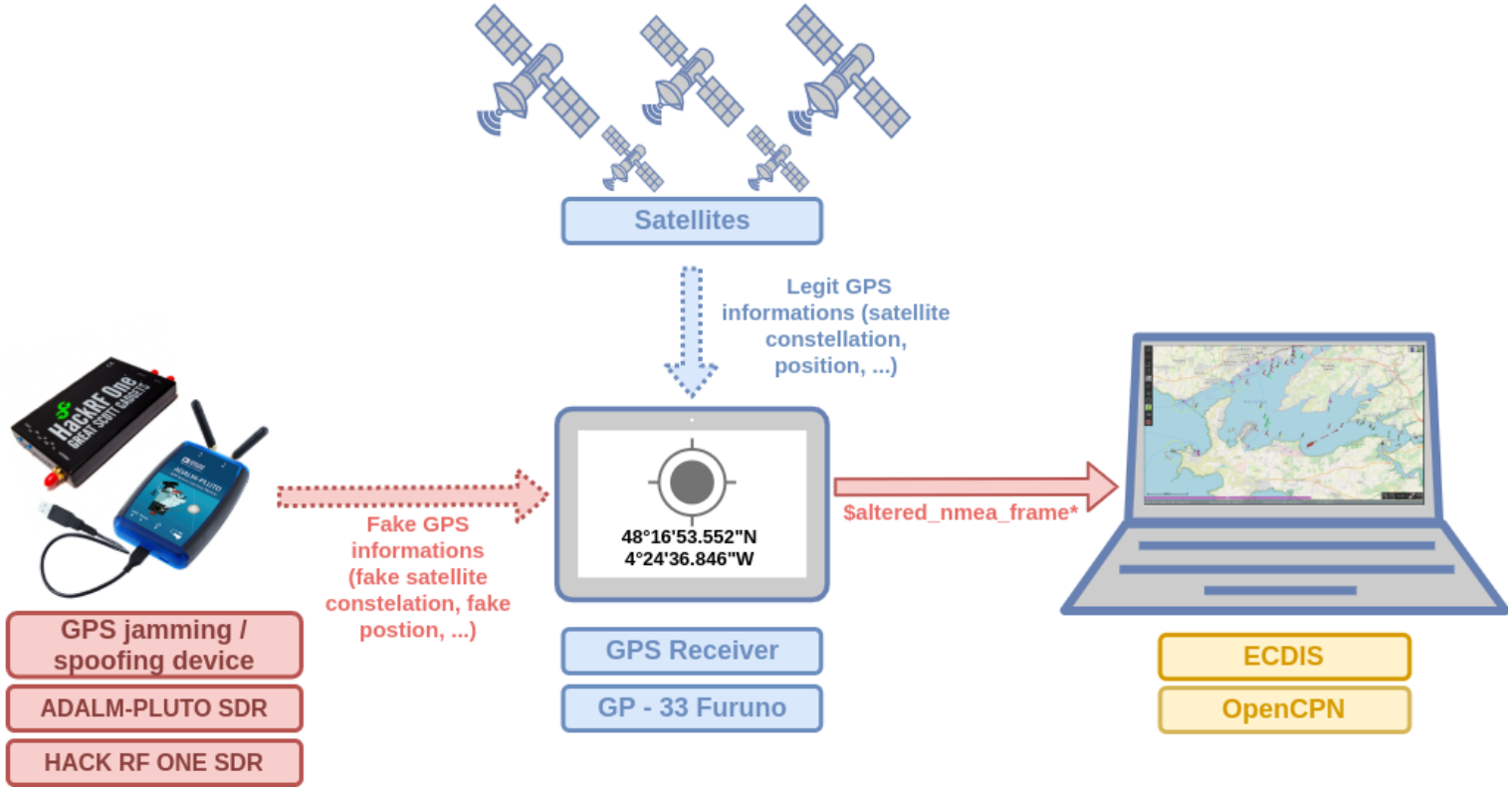
Modern merchant ships are composed of a various complex systems to ensure functional and operational requirements for navigation.



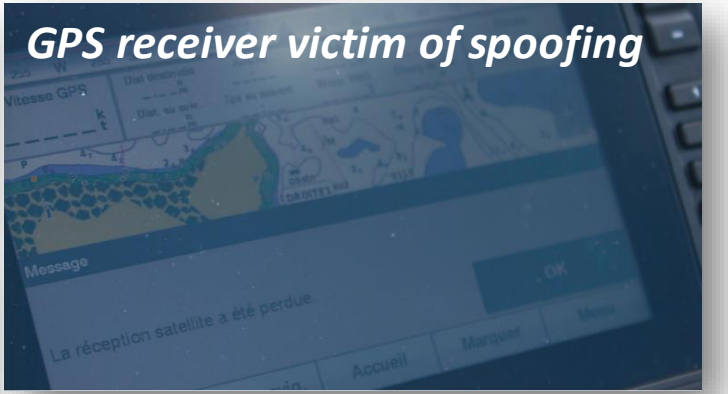
AAM	Waypoint Arrival Alarm (GPS)
GGA	Global Positioning fix data (GPS)
GLL	Latitude / Longitude data (GPS)
RMC	Recommended Minimum data (GPS)
RMB	Recommended Minimum data (GPS)
RPM	Revolutions (GPS)
RSA	Rudder Sensor Angle (GPS)
VTG	Track Made Good and Ground Speed (GPS)
ZDA	Time and Date (GPS)

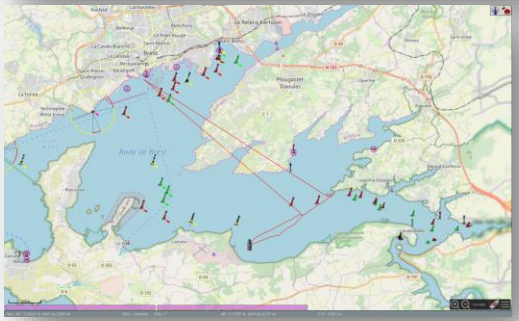
All NMEA-compatible devices can send or receive and interpret data sent using the standard **(NMEA-0183** and **NMEA-2000).**

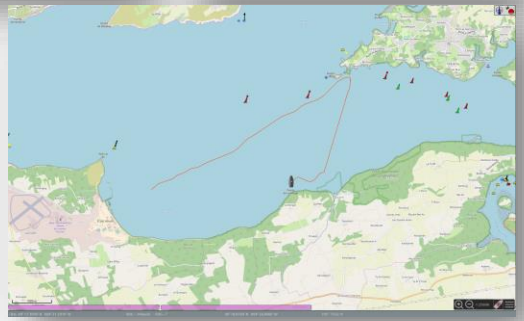
External attack on GNSS (in theory)



Let's practice!

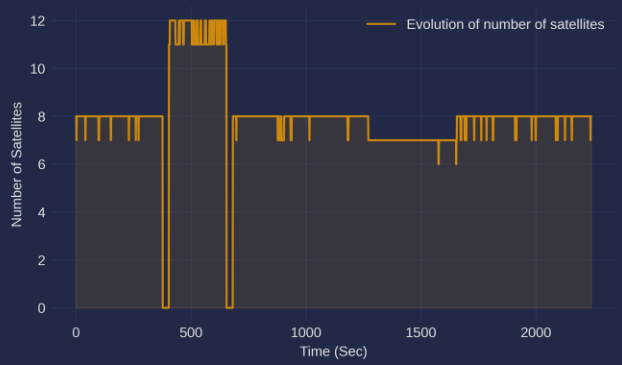




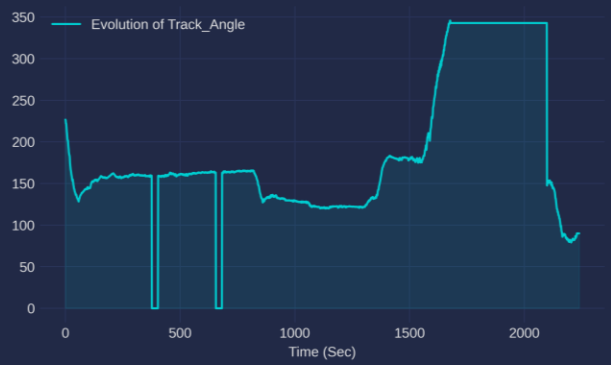


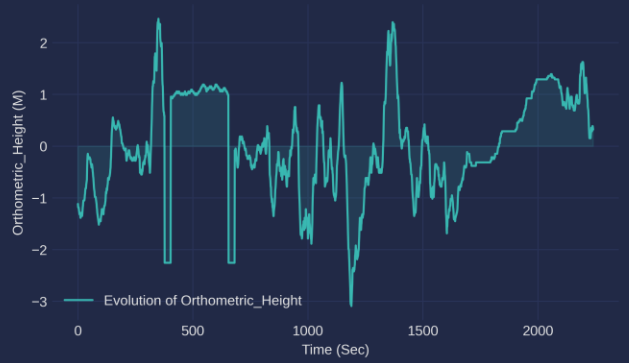
Generation of spoofing scenarios

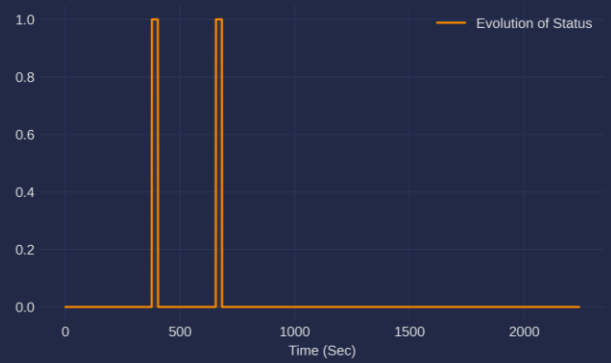
GPGGA_Evolution_Decoy_1



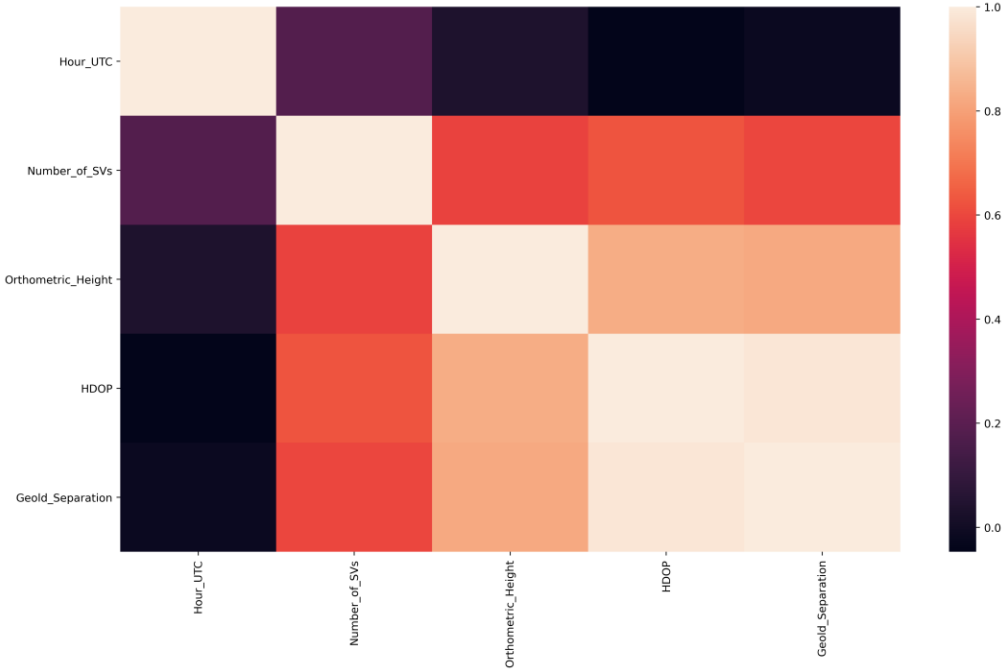
_Decoy_1

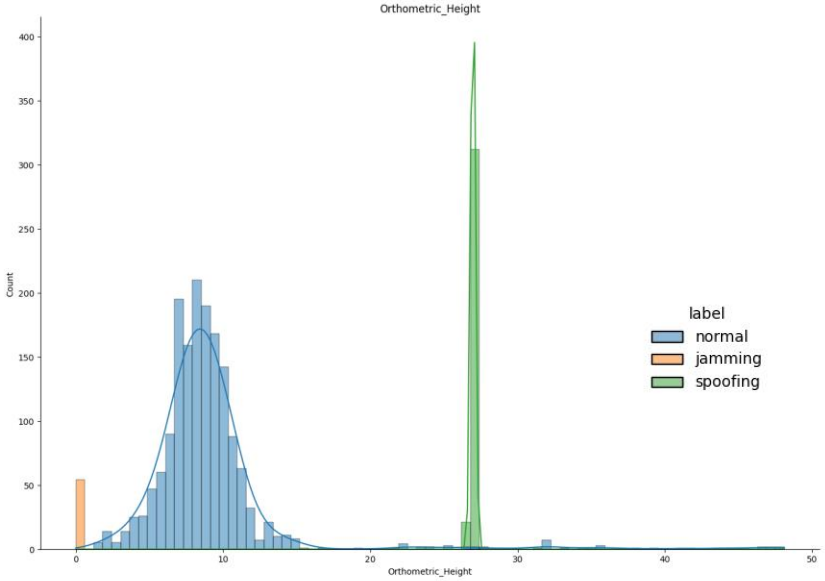




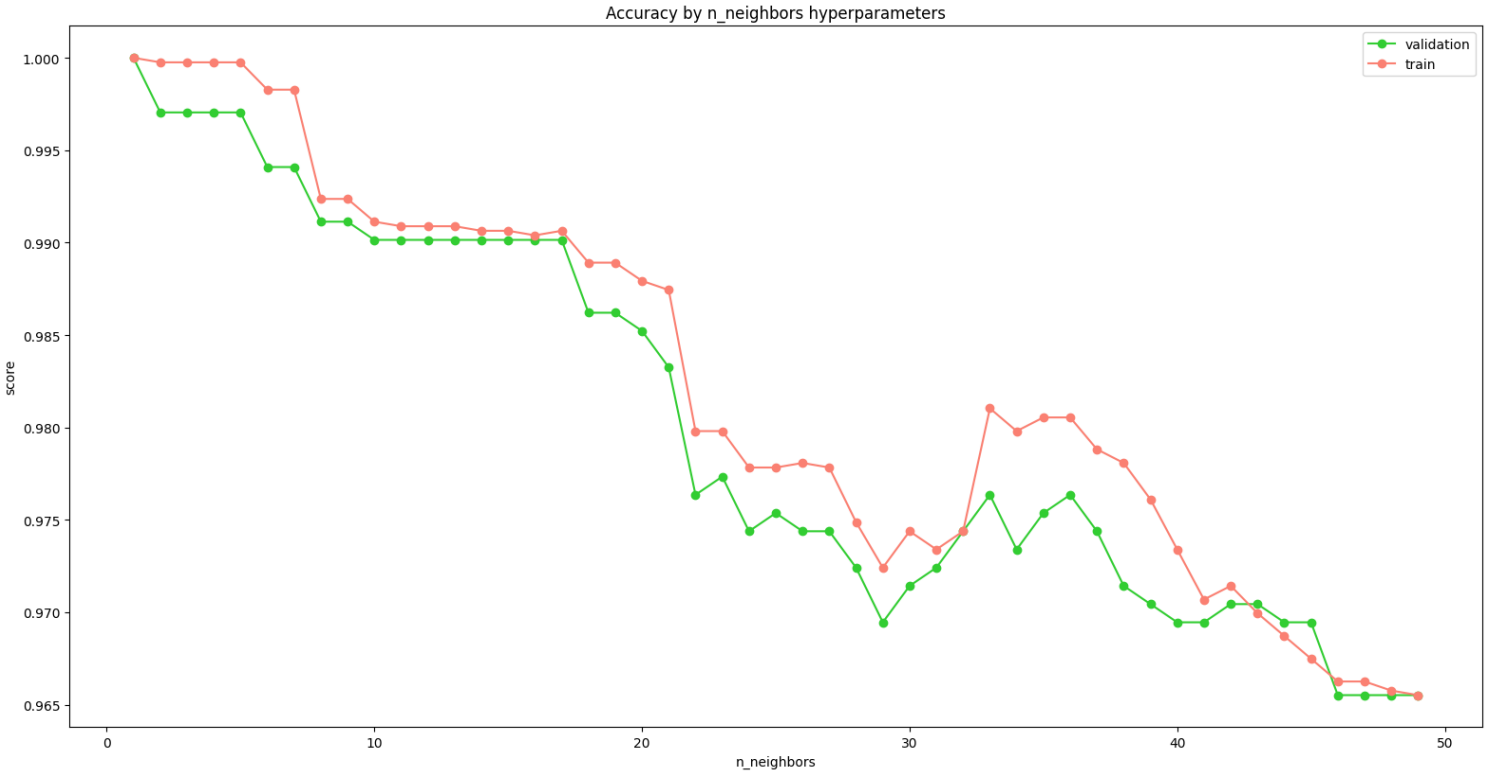


Selection of relevant features





Supervised Learning



Supervising Learning Results

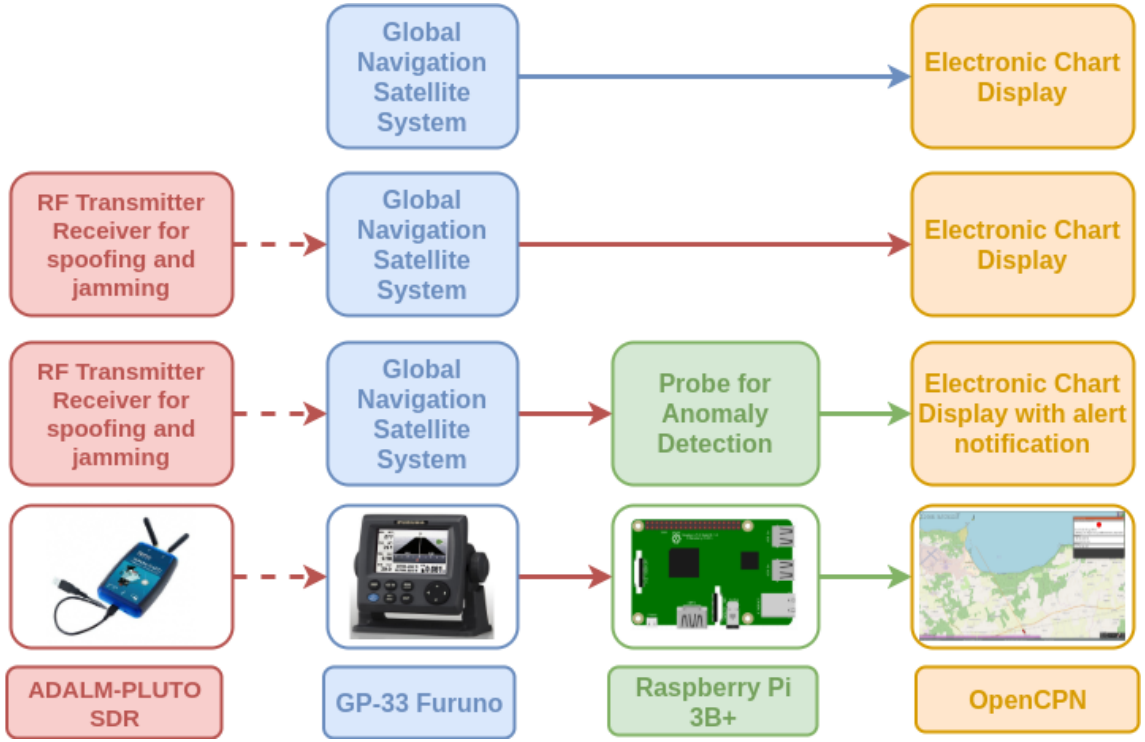
Accuracy Scores according to several algorithms

(mean of 20 iterations + cross validation)

$$\frac{TP + TN}{TP + TN + FP + FN}$$

Spoofing_Method	GPS_Sentence_ID	SVM_RBF	SVM_Linear	SVM_Ploy_2	SVM_Poly_3	SVM_Sigmoid	NN	KNN	Bayes
Decoy_Spoofing	"RMC"	96.6667	98.0381	98.1714	99.2190	74.4000	98.8581	98.4190	97.523
Decoy_Spoofing	"GGA"	99.0189	99.0377	99.0377	99.0377	98.8302	98.9434	98.9057	77.962
Offset_Spoofing	"RMC"	92.6598	98.5155	98.4742	98.6186	91.8351	98.5155	98.5773	98.783
Offset_Spoofing	"GGA"	99.0103	98.9878	99.1753	99.0103	98.6598	99.0928	98.8247	65.216
Static_Spoofing	"RMC"	99.4000	99.0727	99.0727	99.00	98.8545	98.9636	98.8545	75.781
Static_Spoofing	"GGA"	99.0545	99.0545	99.0545	99.1636	98.8909	99.1273	98.80	59.854
Staight_Spoofing	"RMC"	96.76	96.96	97.60	97.2800	94.2200	98.4400	97.70	98.58
Straight_Spoofing	"GGA"	99.02	98.96	99.02	99.0200	96.3000	98.9200	98.46	76.82

Proposed detection methodology



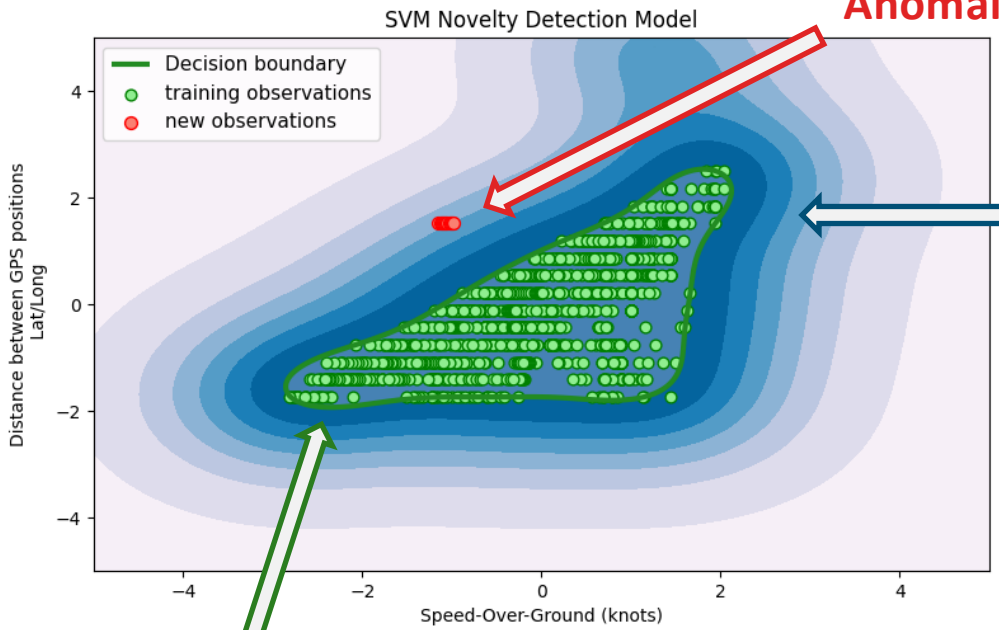
1 **Native architecture**

2 **+ External cyber attack /!\ /!**

3 **+ Cybersecurity components**

Low-cost embedded device for anomaly detection and warning plugin directly on ECDIS.

Novelty Detection with One-Class SVM



Anomalies (due to spoofing)

Train dataset

Expected normal behavior

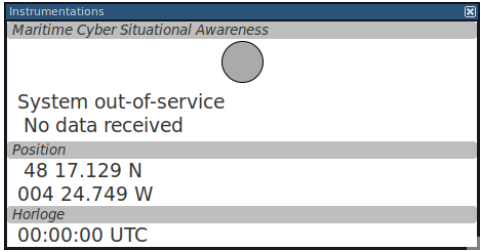
Example of learning with NMEA data

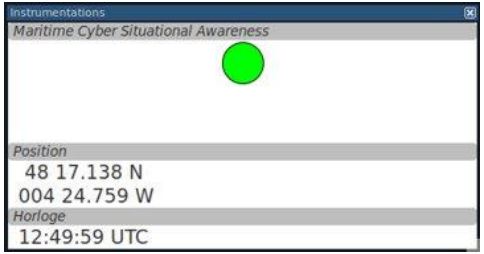
Unsupervised Learning Results

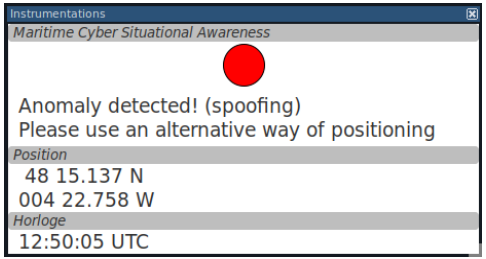
Accuracy Scores according to several novelty detection algorithms

Spoofing_Distance	GPS_Sentence_ID	*OneClass SVM*	*Local Outlier Factor*	*Isolation Forest*
250 yards	"RMC"	99.69	99.78	92.96
100 yards	"RMC"	99.16	99.531	92.78
10 yards	"RMC"	99.004	97.4869	88.412
5 yards	"RMC"	98.40	89.564	76.89
1 yards	"RMC"	97.28	87.82	72.023

Concept of a warning system for navigation charts



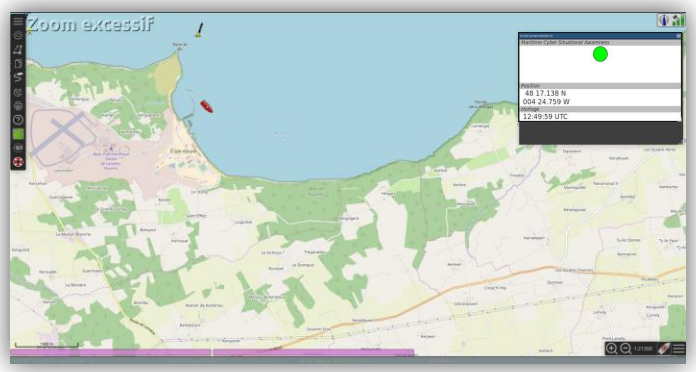


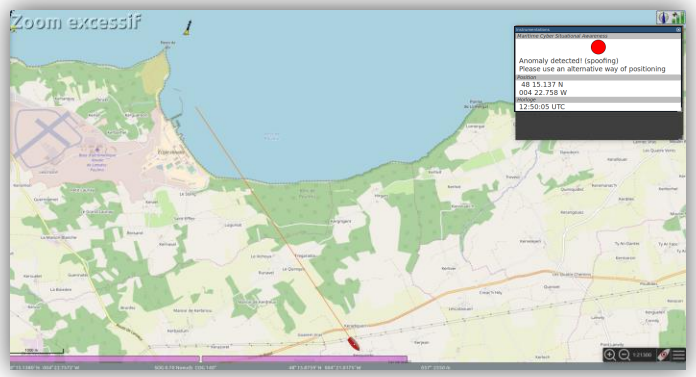


[Gray Status] :
Indicates if there is a problem or reception failure from GPS systems.

[Green Status] :
Indicates if nothing is abnormal.

[Red Status] :
Indicates if a potential cyber attack occures.





Operational Technology Vulnerabilities

Simatic S7-300 & S7-400 and I/O module

Possible attacks on ICS :

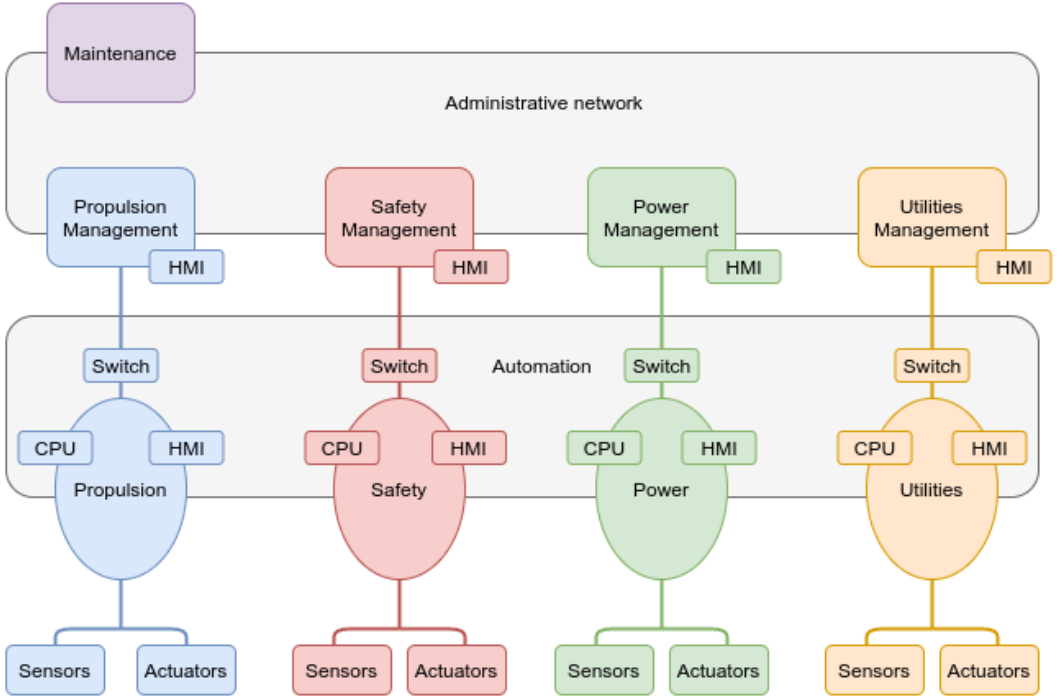
- Reconnaissance
- Authentication bypass
- Brute-force
- Command injection and response
- Denial of service
- Memory read and write logic
- Man in the middle (MITM)
- Attacks against PLC firmware

Naval systems have seen an increase of **Intrusion Detection Systems's** deployment.

But there is a lack of training data to improve the cyber-security on board.

Architecture of the automatic layer of naval systems

Modern merchant ships are composed of a various complex systems to ensure functional and operational requirements.

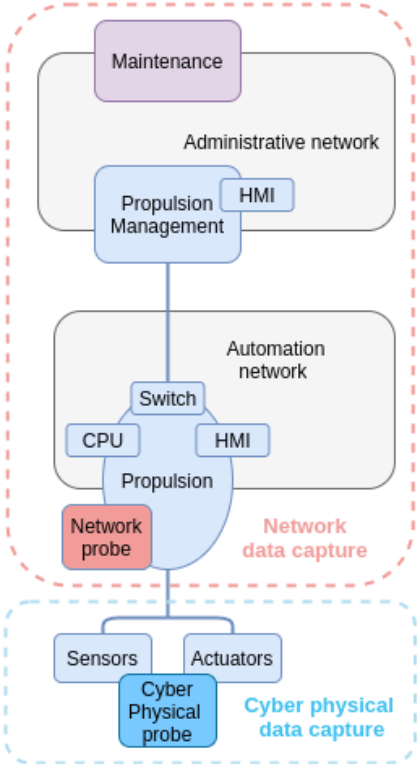


Automatic layer compoments :

- **ICS** (Industrial Control Systems)
- **DCS** (Distribution Control Systems)
- **PLC** (Programmable Logic Controler)
- **HMI** (Human-Machine Interfaces)
- **I/O Modules** : Sensors and actuators

To respond of the lack of training data, **this architecture is simulated by a virtual environment and different physical components.**

Method to extract data from ICS flow



A data extraction strategy is developed **to improve the performance of anomaly detection algorithms based on cyber physical alert.**

Network flow collection

+

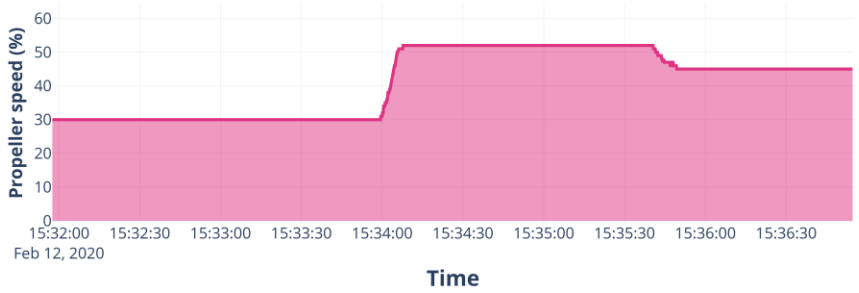
Anomaly correlation

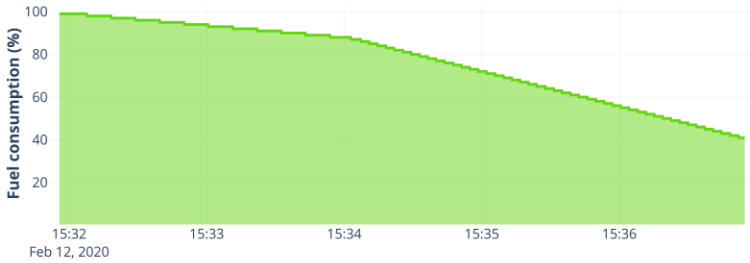
Cybernetic flow collection

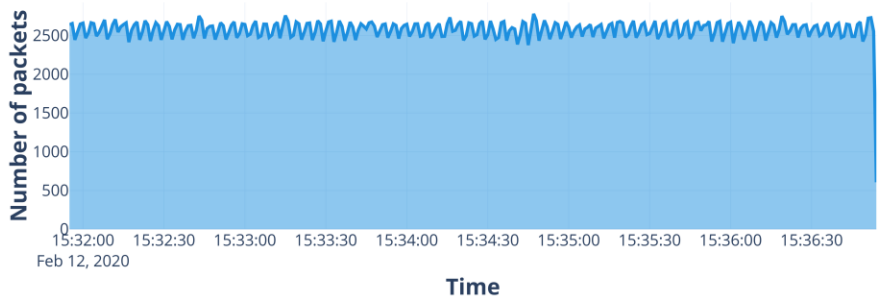
Extraction of propulsion management cybernetic flow

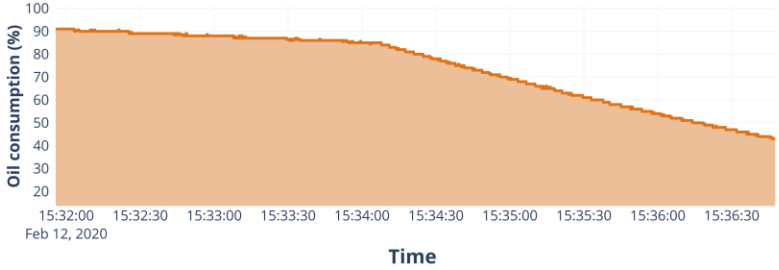
- Sensors / actuators and network traffic correlation (**normal behavior**)

Evolution of sensors, actuators and network traffic (number of packets)





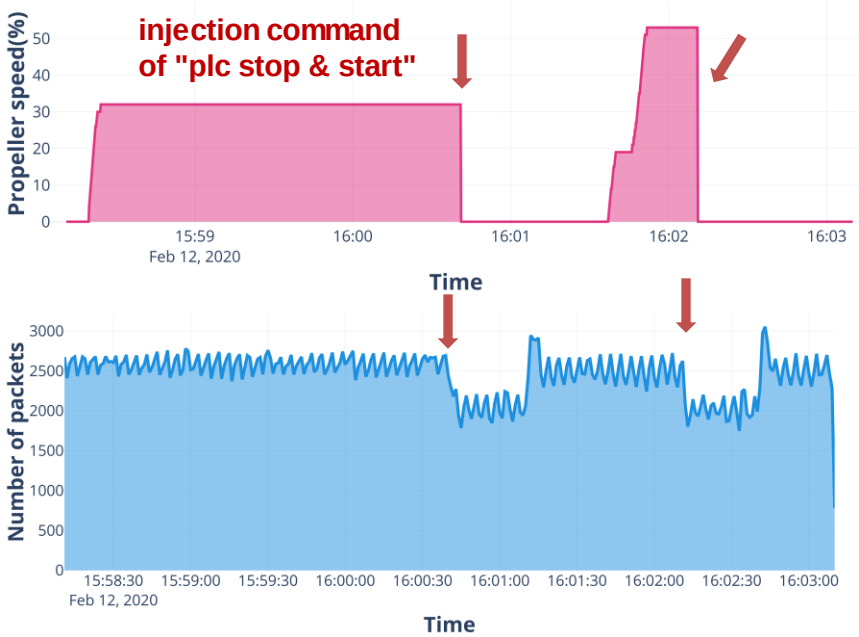


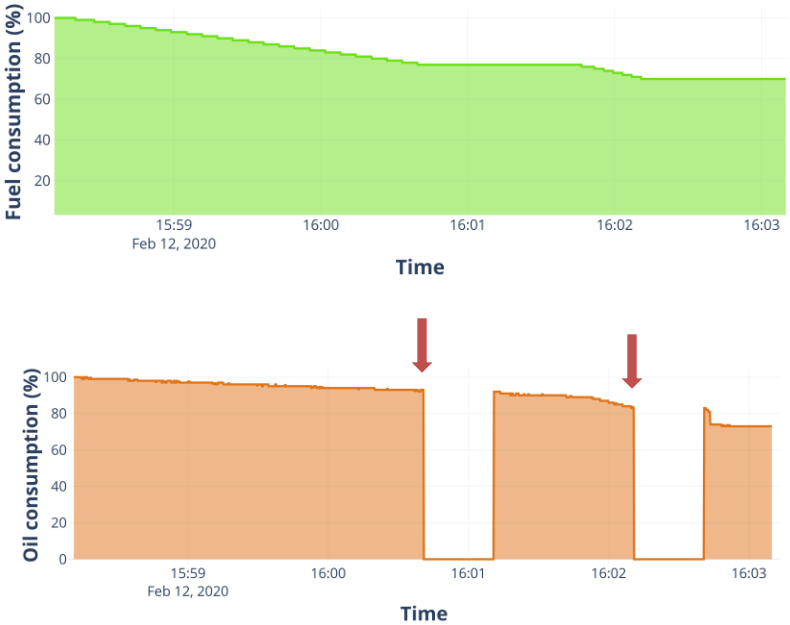


Attacks example on propulsion management system

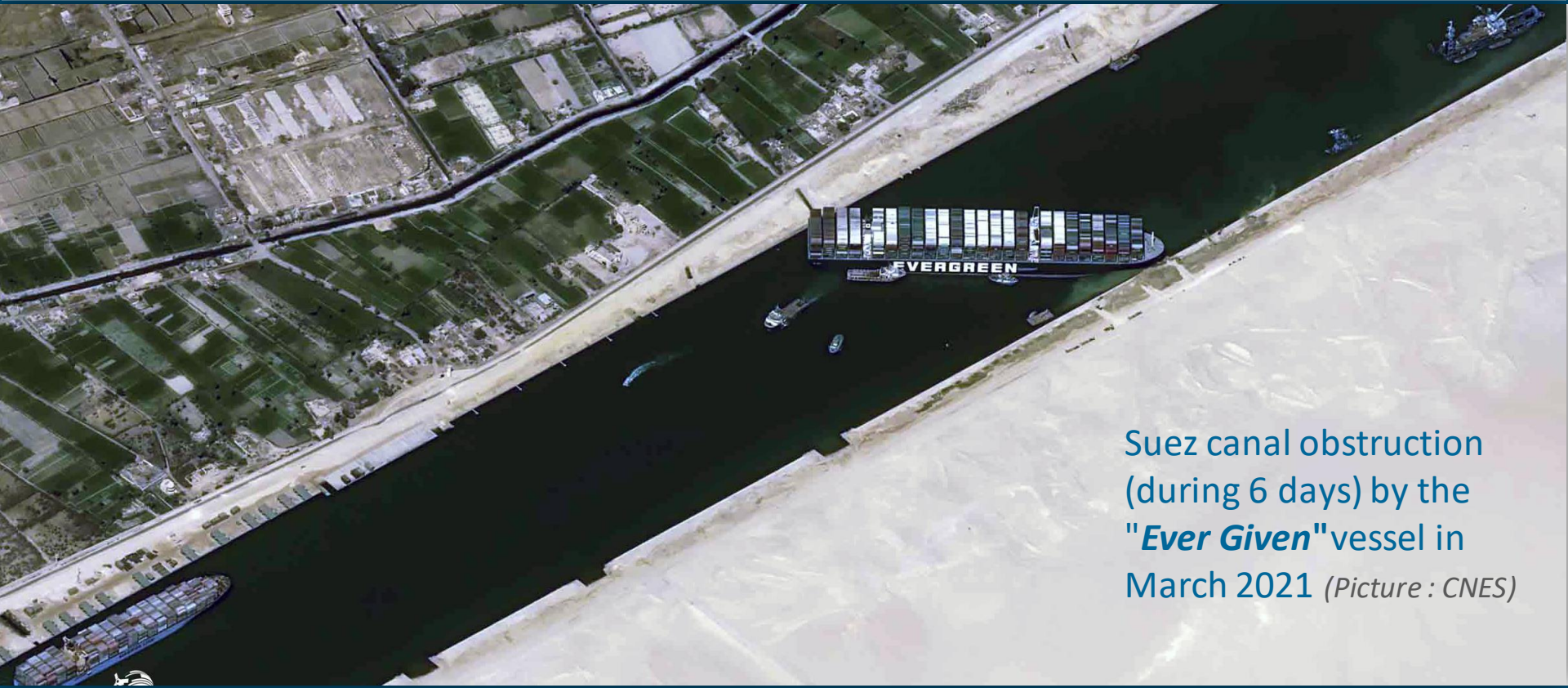
- Sensors / actuators and network traffic correlation (**plc "stop & start" behavior**)

Evolution of sensors, actuators and network traffic (number of packets)





And what about now ?



Suez canal obstruction (during 6 days) by the "***Ever Given***" vessel in March 2021 *(Picture : CNES)*

Questions ?