Penetrating the Silence: Data Exfiltration in Maritime and Underwater Scenarios

1st IEEE LCN Workshop on Maritime Communication and Security (MarCaS)

Alessandro Cantelli-Forti, *Michele Colajanni,*
Silvio Russo

Daytona Beach, FL, USA - 05 October 2023

Slide’s Stylist: Francesco Mancuso

Aim:

- We urge awareness of an unexpected attack vector (merging different paradigms).

Presentation Outline:

- Air-Gapped or Water-Gapped scenarios
- Dalayed Tollerant Networks
- The frameworks we expoited
- Validation and first results
- Conclusion and future works

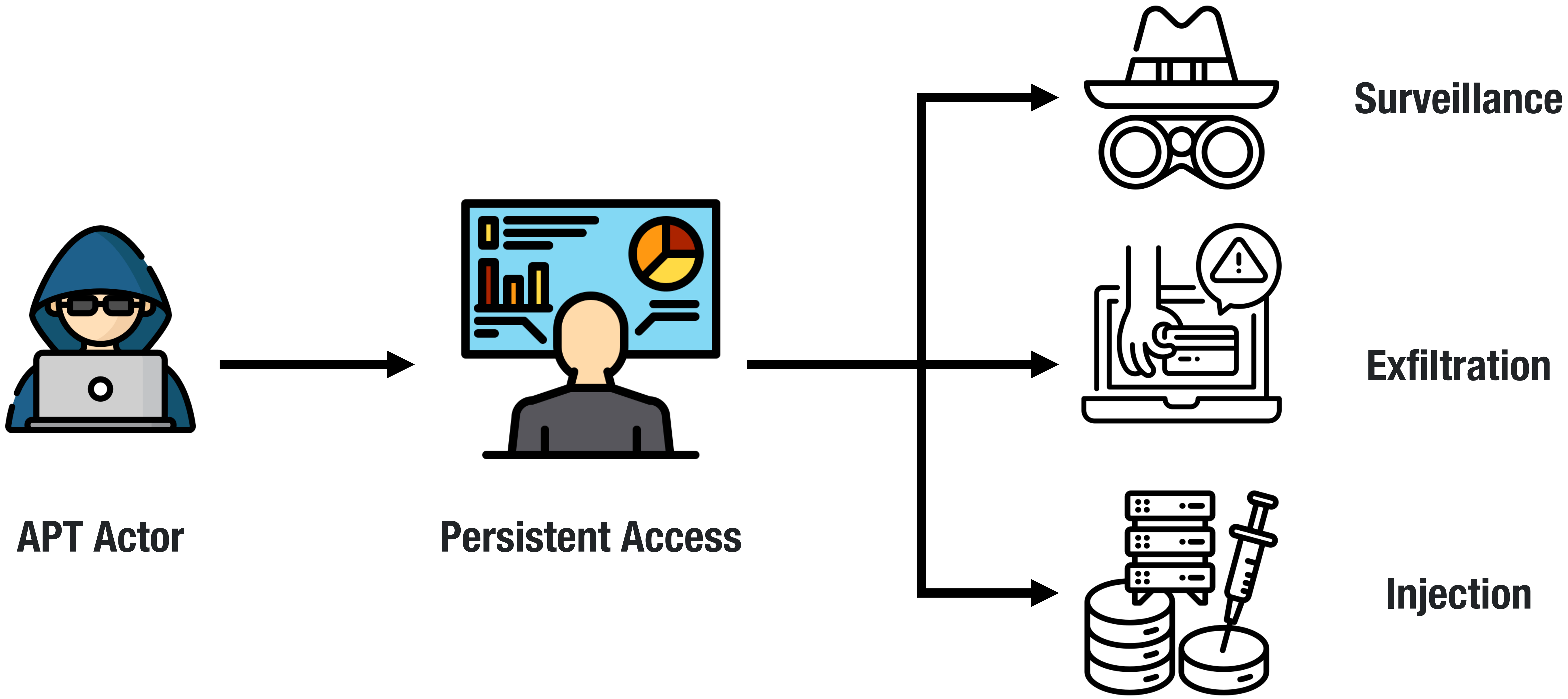
The Cyber Threats

Supply Chain Attack

- **Definition**: A supply chain attack targets vulnerabilities within the supply system, compromising legitimate software or hardware sources.
- **Stealthy Nature**: Often difficult to detect as they exploit trusted relationships.
- **Third-party Risks**: Involves the exploitation of third-party service providers or software vendors.

The Cyber Threats

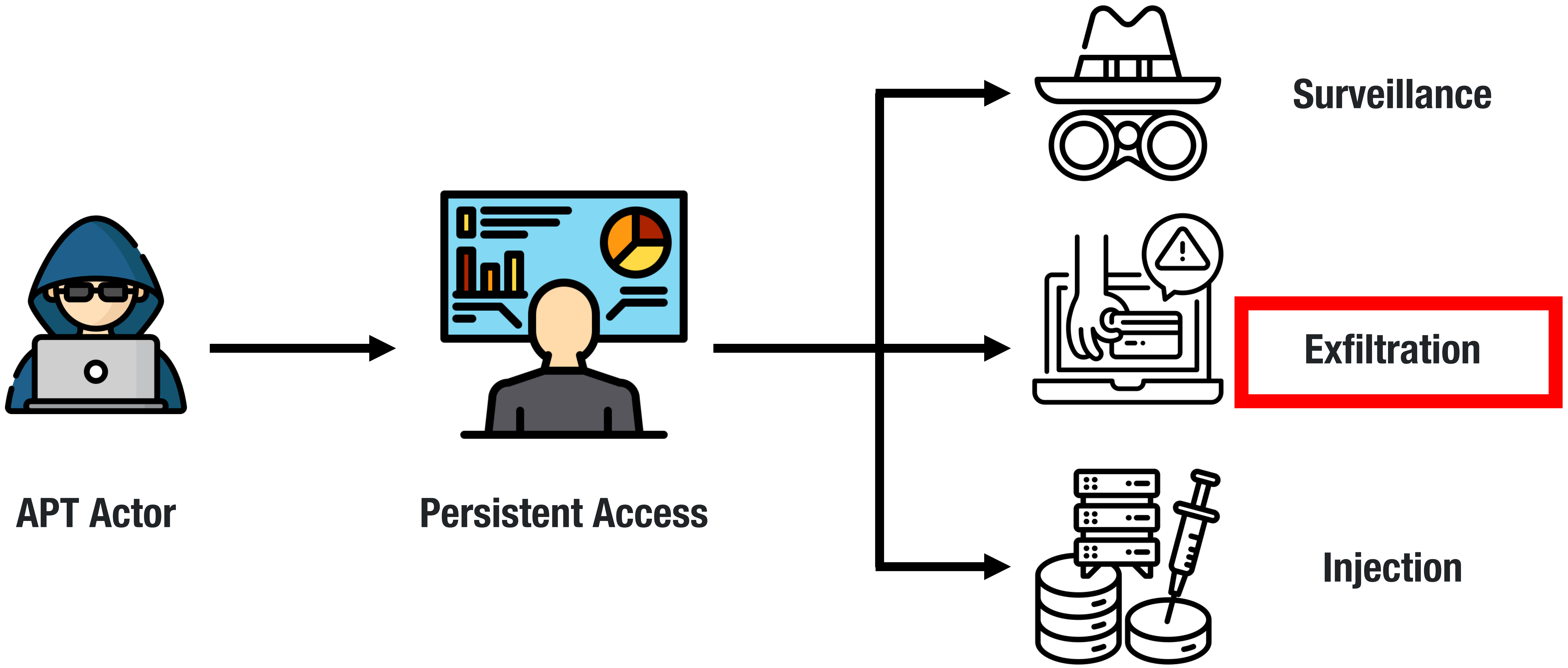
Advanced Persistent Threat



APT is a prolonged attack to gain prolonged access to a system, often for espionage or data theft.

The Cyber Threats

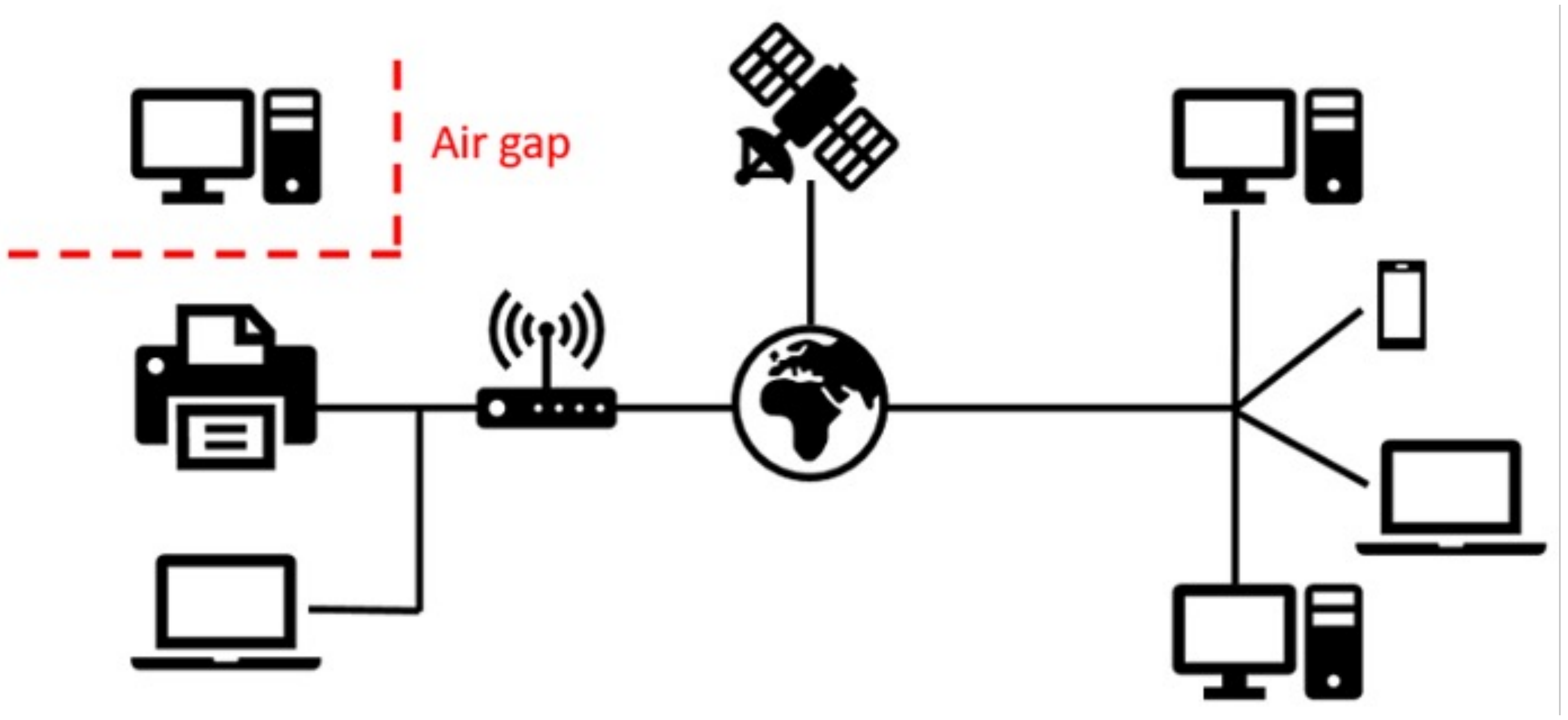
Advanced Persistent Threat



APT is a prolonged attack to gain prolonged access to a system, often for espionage or data theft.

Air-Gapped System

A security measure for high-security environments



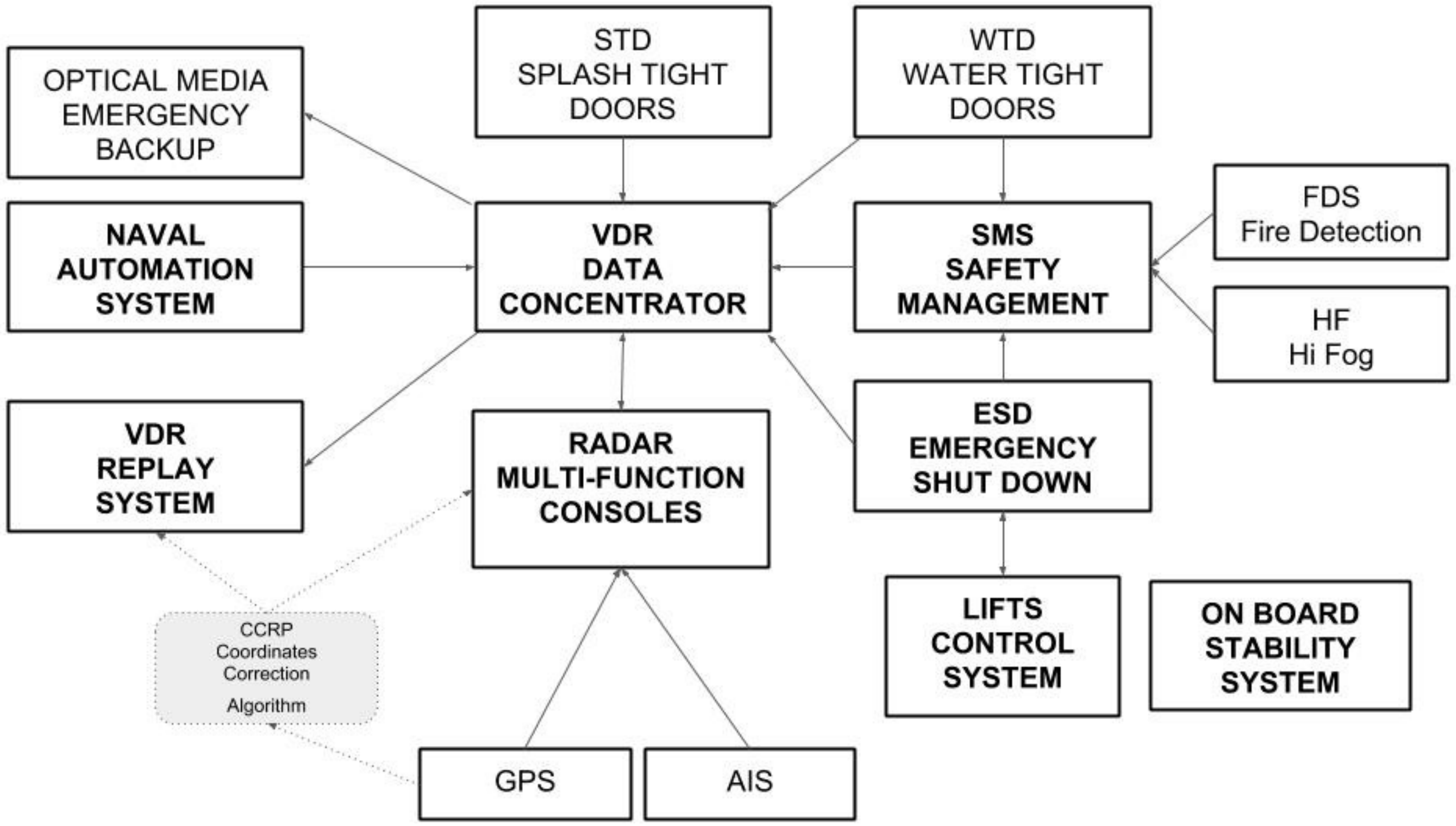
- Physically isolating certain computers or an entire network from unprotected systems

- Without any external communication, an APT can neither receive command and control signals nor transmit data to and from the victim network.

Data Exfiltration

In a Vessel’s sensor network

Common Naval bridge network schema



- Given the **increasing reliance** on networked systems and **digital technologies** in modern vessels,

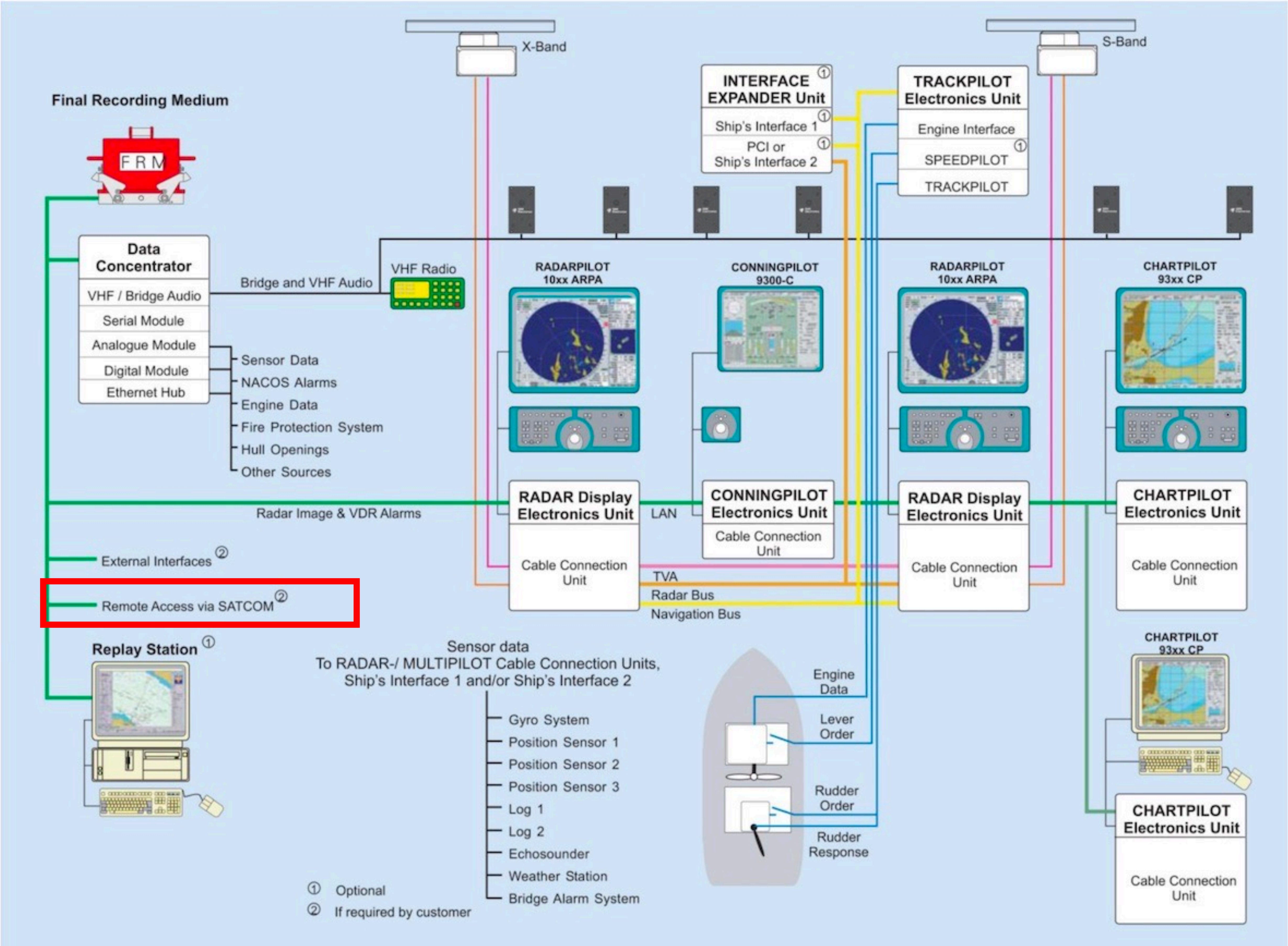
- We investigate the feasibility of data exfiltration attacks in maritime vessels, which we define of as potential “**water-gapped**” environments,

- The **data connection of personal devices** like smartphones is exploited by means of the misuse of store-and-forward, opportunistic networks.

Data Exfiltration

In a Vessel’s sensor network

Common Naval bridge network schema (SAM’s Electronics)



- In a vessel’s sensor network, the attack surface **can be defended** notably due to its limited connectivity,
- Restricted to satellite or occasionally High-Frequency radio Internet Protocol (HF-IP).

Other Contexts

Ingenious methods for data exfiltration or Side Channel attack

- They **exploit** aspects like electromagnetic analysis, LED analysis of network equipment, screen brightnes, video card's fans, network cables (as radio transmitters), and even thermometers, microphones, or accelerometers.

- All these attack **strategies are ineffective** in a «physically» isolated context such as the maritime environment.

- They require the **simultaneous** presence of a transmitting source and a receiving entity through «unconventional» transmission media.

- **The data connection of personal devices like smartphones is exploited by means of the misuse of store-and-forward, opportunistic networks such as OFN.**

Offline Finding Networks

Opportunistic use of COTS devices

- OFNs, these **spontaneous**, **crowdsourced**, and **opportunistic** networks for mobile object location

- Used for locating personal items, such as keys, wallets, or vehicles (or spouses!) **without the need for direct internet access**, while maintaining a low energy footprint

- They leverages the internet data connection with **nearby portable devices** and their geolocation services.

- They transmit Bluetooth Low Energy (BLE) signals, which are relayed on the internet by ubiquitous smart devices

- To **expoit** OFN networks for this purpos we must gain the ability to **control data transit** through the opportunistic network

- **Heinrich et al.** [1] have successfully **emulated** an Apple “AirTag” device by programming a common microcontroller or a Linux system with BLE - HCI.

- **Braunlein** [2] has proposed the transmission of a limited-length payload, such as a message by **tampering** with the transmission of “announcement keys”

- In the standard scenario, the data payload is composed of the position provided by a passing device.

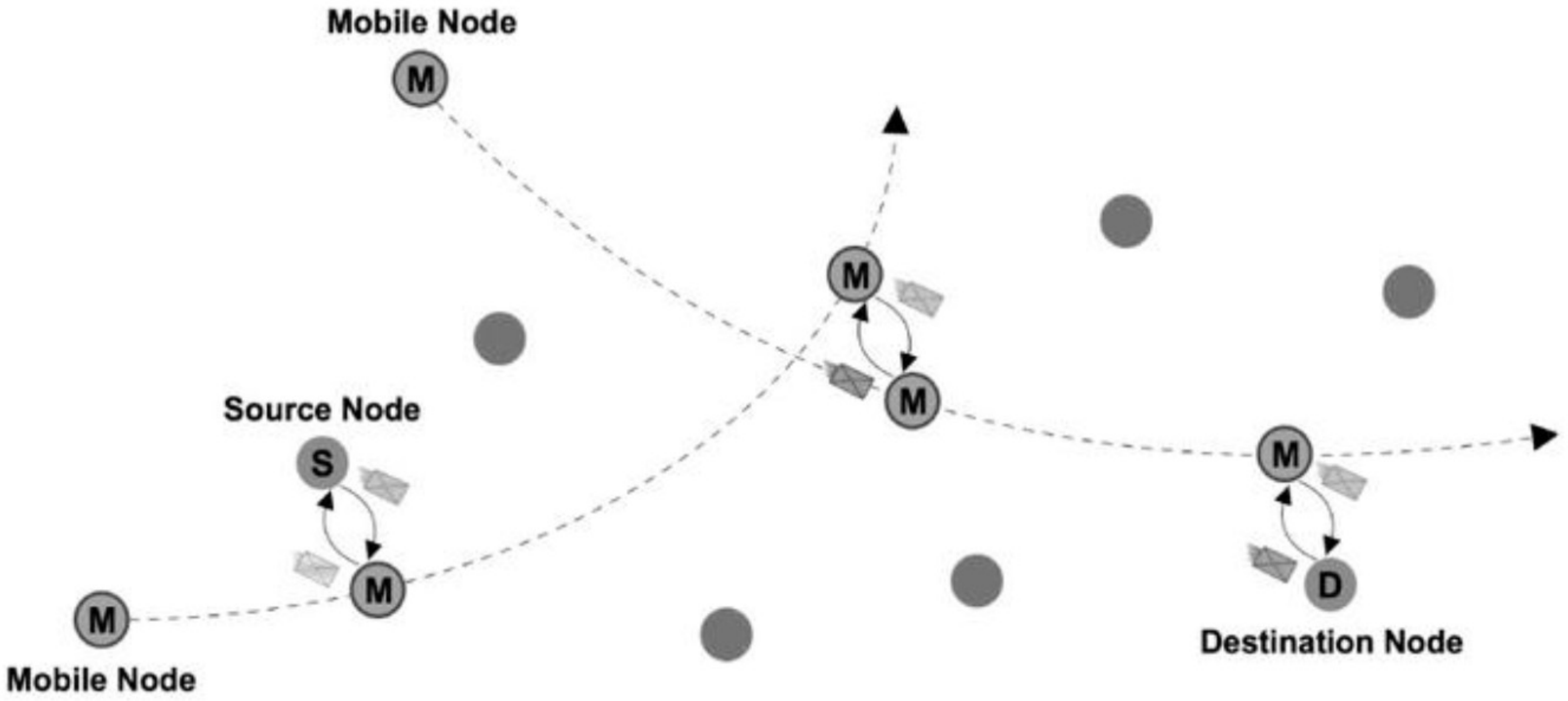
- Announcement keys can carry encoded messages: a portion of the advertisement keys is fixed and used as an identifier for “inoculated” messages.

- The remaining portion of the keys as “variables” for data reconstruction by means of heuristic search.

[1] A.Heinrich,M.Stute,T.Kornhuber,andM.Hollick,“Who can devices?» [2]F. Braunlein, “Send My: Arbitrary data transmission via Apple’s Find My network

Offline Finding Networks

Are store and forward “Delayed Tollerant Networks”



CCDCOE

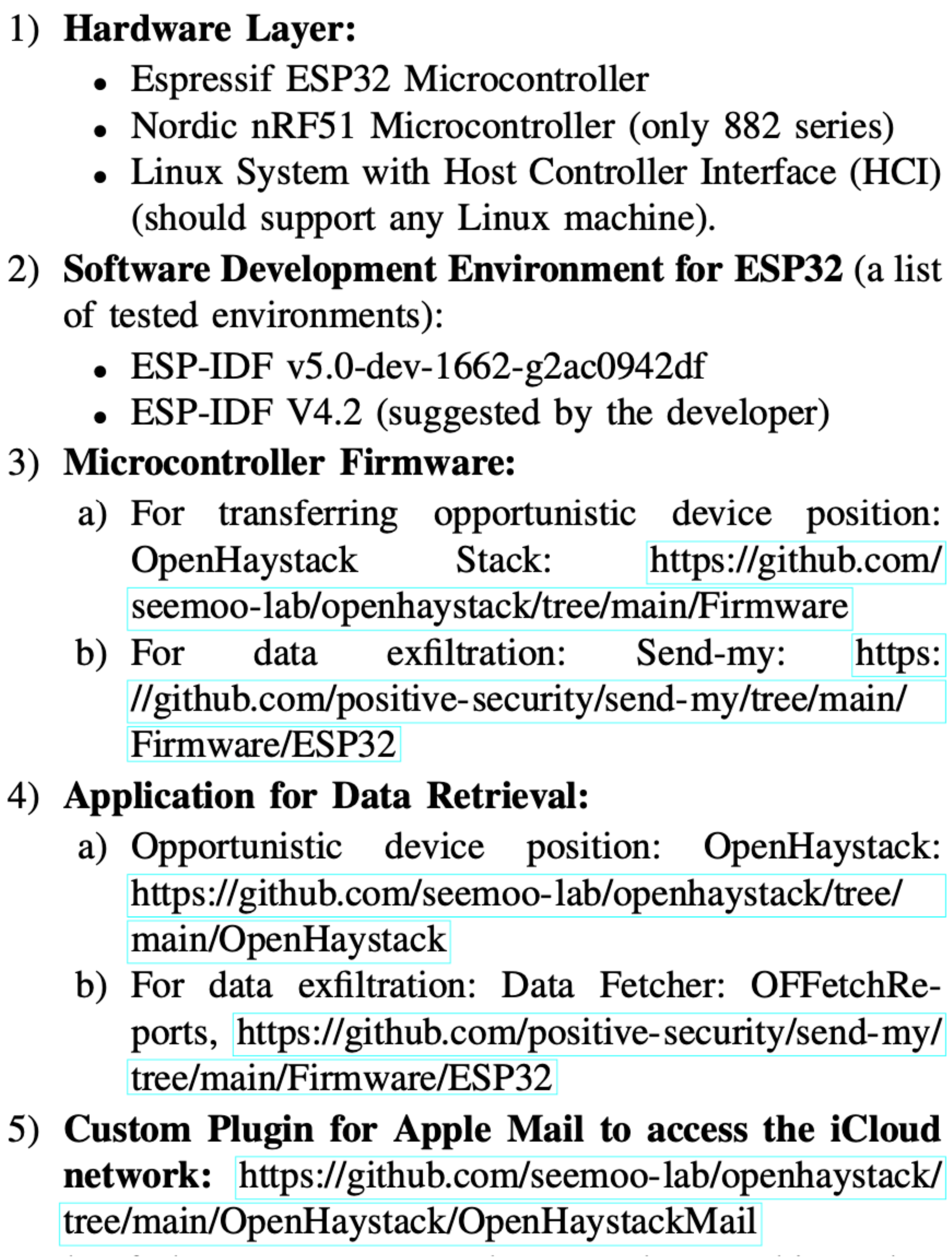
Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

Existing systemside channel attacks are not conceived to exfiltrate data from a maritime , due to the inherent physical isolation

[1] Battlefield Digital Forensics: Digital Intelligence and Evidence Collection in Special Operations (NATO Cooperative Cyber Defence Centre Of Excellence et al.)
[2] SOF on Trial. The Technical and Legal Value of Battlefield Digital Forensics in Court (Mancini, Monti, Panico)

Experimental Set-Up

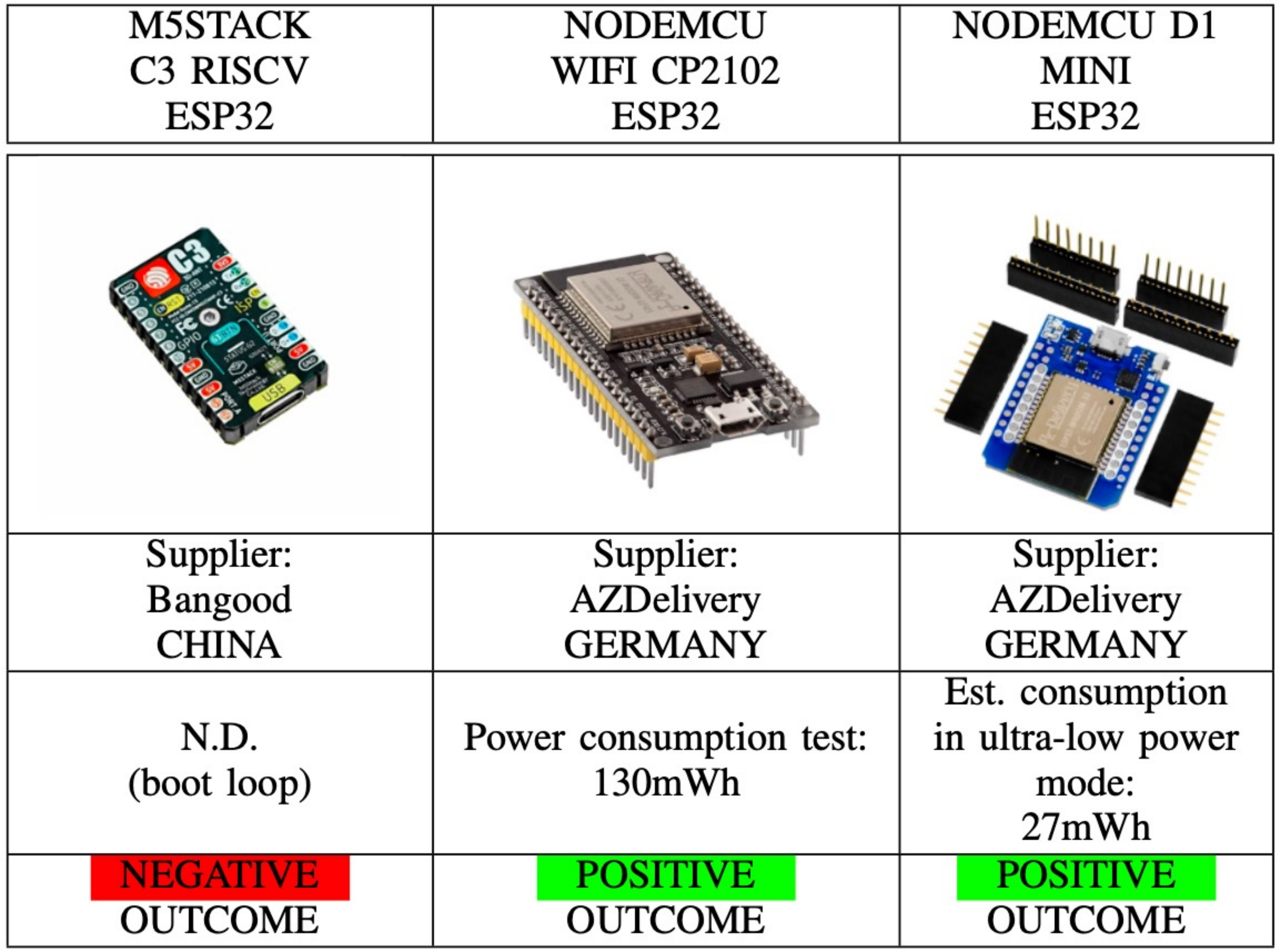
high-level architecture and software building blocks



1) **Hardware Layer:**
   - Espressif ESP32 Microcontroller
   - Nordic nRF51 Microcontroller (only 882 series)
   - Linux System with Host Controller Interface (HCI) (should support any Linux machine).
2) **Software Development Environment for ESP32** (a list of tested environments):
   - ESP-IDF v5.0-dev-1662-g2ac0942df
   - ESP-IDF V4.2 (suggested by the developer)
3) **Microcontroller Firmware:**
   a) For transferring opportunistic device position: OpenHaystack Stack: https://github.com/seemoo-lab/openhaystack/tree/main/Firmware
   b) For data exfiltration: Send-my: https://github.com/positive-security/send-my/tree/main/Firmware/ESP32
4) **Application for Data Retrieval:**
   a) Opportunistic device position: OpenHaystack: https://github.com/seemoo-lab/openhaystack/tree/main/OpenHaystack
   b) For data exfiltration: Data Fetcher: OFFetchReports, https://github.com/positive-security/send-my/tree/main/Firmware/ESP32
5) **Custom Plugin for Apple Mail to access the iCloud network:** https://github.com/seemoo-lab/openhaystack/tree/main/OpenHaystack/OpenHaystackMail

ESP32 Microcontrollers

Details of our testbed

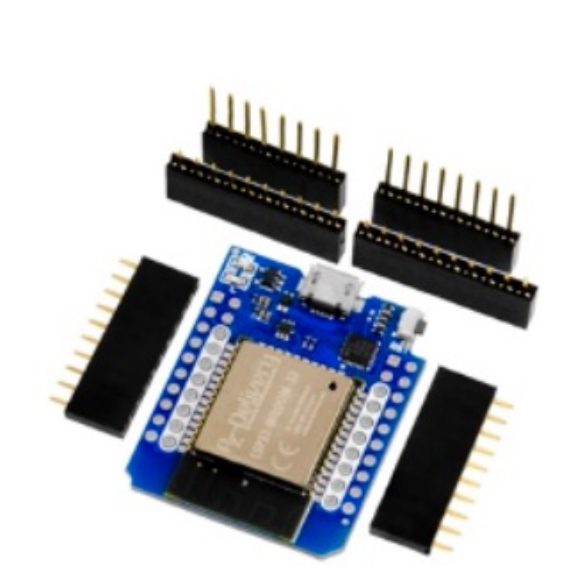


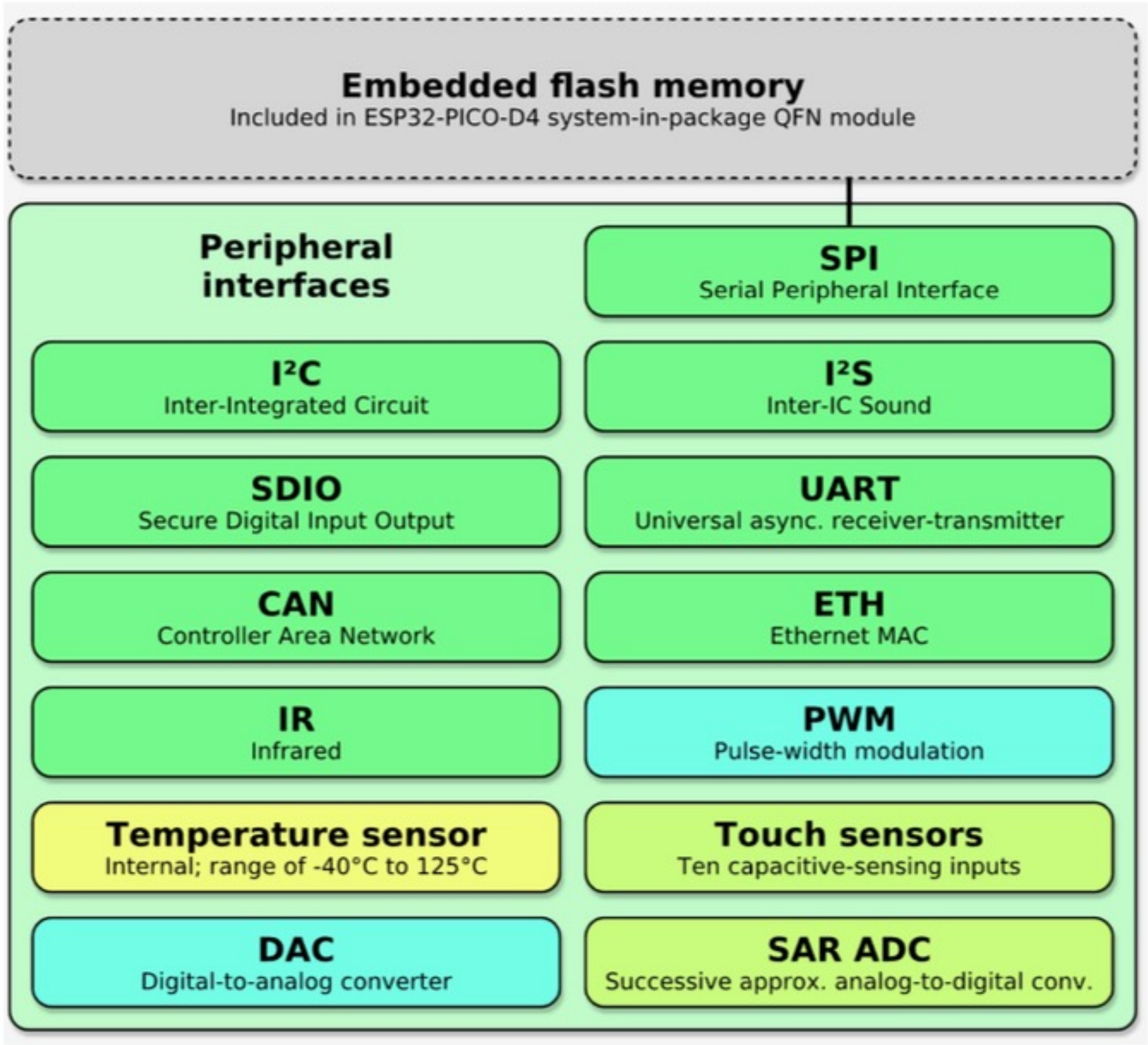
M5STACK C3 RISCV ESP32	NODEMCU WIFI CP2102 ESP32	NODEMCU D1 MINI ESP32
Supplier: Bangood CHINA	Supplier: AZDelivery GERMANY	Supplier: AZDelivery GERMANY
N.D. (boot loop)	Power consumption test: 130mWh	Est. consumption in ultra-low power mode: 27mWh
🟥 NEGATIVE OUTCOME	🟩 POSITIVE OUTCOME	🟩 POSITIVE OUTCOME

- To expoit OFN networks for this purpos we must gain the ability to control data transit through the opportunistic network

ESP32 Microcontrollers

Details of our testbed

M5STACK C3 RISCV ESP32	NODEMCU WIFI CP2102 ESP32	NODEMCU D1 MINI ESP32
		
Supplier: Bangood CHINA	Supplier: AZDelivery GERMANY	Supplier: AZDelivery GERMANY
N.D. (boot loop)	Power consumption test: 130mWh	Est. consumption in ultra-low power mode: 27mWh
NEGATIVE OUTCOME	POSITIVE OUTCOME	POSITIVE OUTCOME



Embedded flash memory
Included in ESP32-PICO-D4 system-in-package QFN module

Peripheral interfaces

SPI
Serial Peripheral Interface

I²C
Inter-Integrated Circuit

I²S
Inter-IC Sound

SDIO
Secure Digital Input Output

UART
Universal async. receiver-transmitter

CAN
Controller Area Network

ETH
Ethernet MAC

IR
Infrared

PWM
Pulse-width modulation

Temperature sensor
Internal; range of -40°C to 125°C

Touch sensors
Ten capacitive-sensing inputs

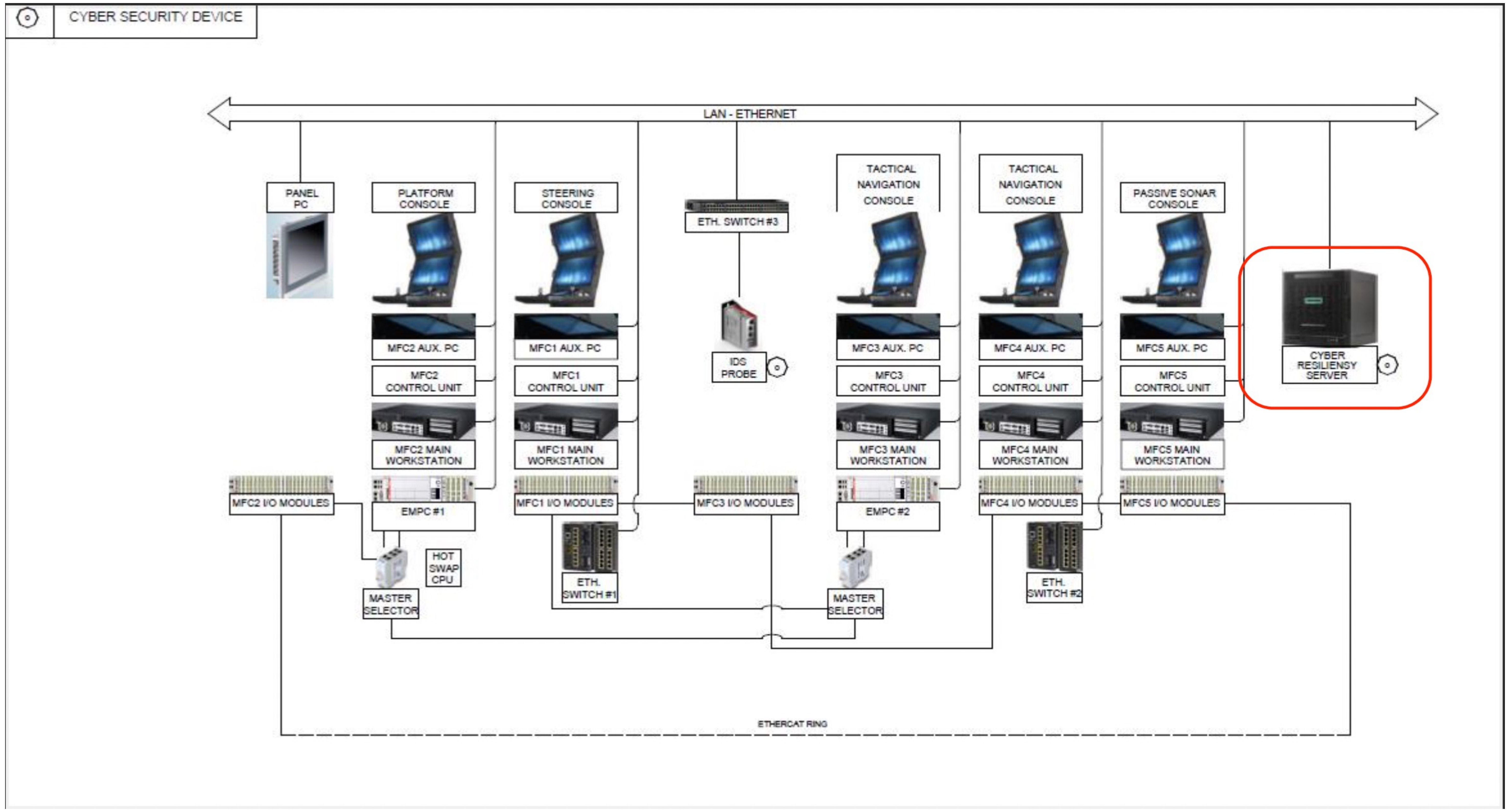
DAC
Digital-to-analog converter

SAR ADC
Successive approx. analog-to-digital conv.

- To expoit OFN networks for this purpos we must gain the ability to control data transit through the opportunistic network

APT HIDE AND SEEK: UNDERWATER COVERT THREATS

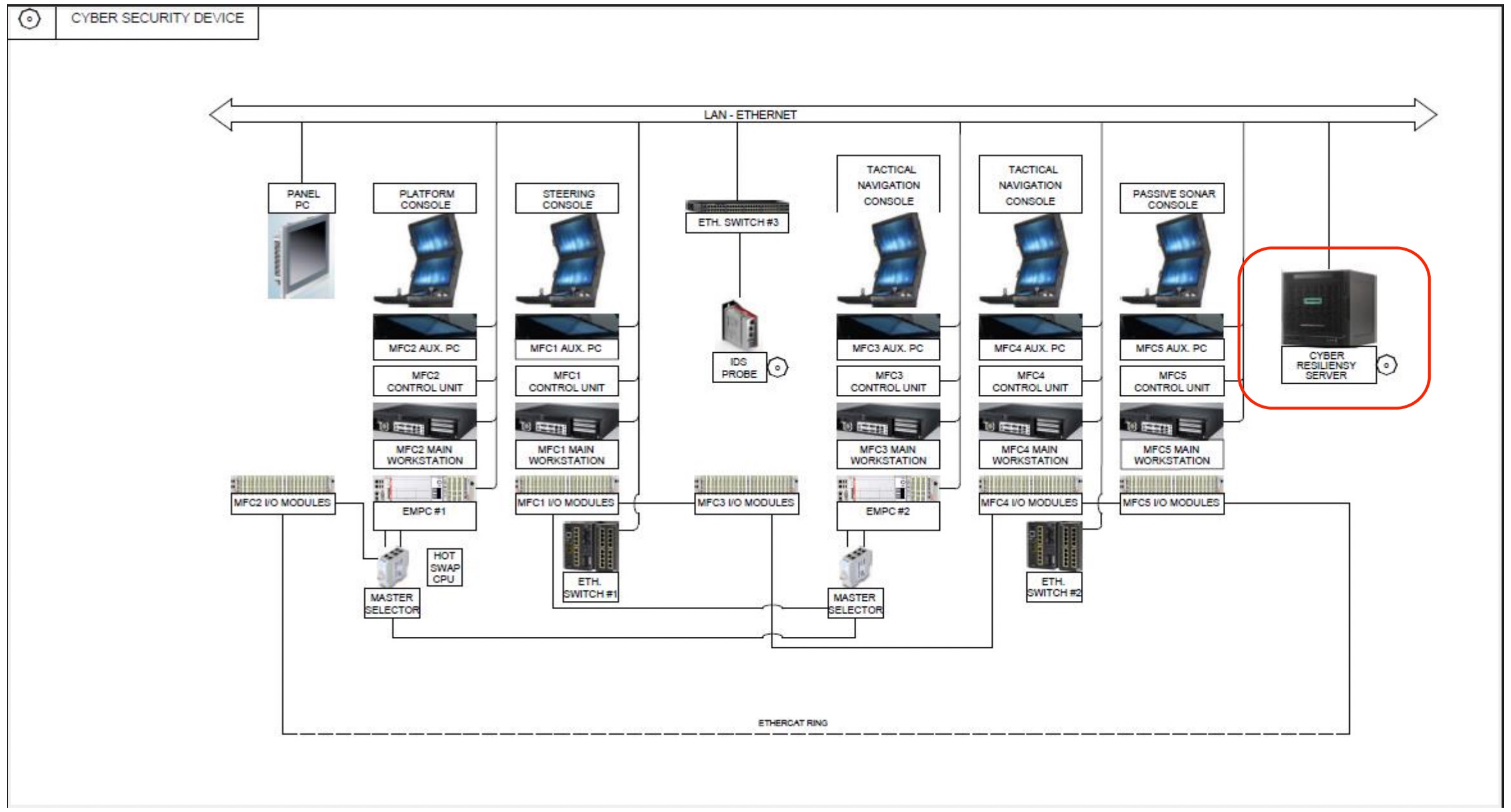
Penetreating the Silence



- Field tests were conducted in October 2021 inside the Integrated Submarine Systems built by DRASS Group, Livorno, Italy.

APT HIDE AND SEEK: UNDERWATER COVERT THREATS

Field tests were conducted in October 2021 inside the Integrated Submarine Systems built by DRASS Group, Livorno, Italy.



- Continuously broadcasting a single 42byte NMEA $GPGLL message containing pre-saved latitude and longitude data.

APT HIDE AND SEEK: UNDERWATER COVERT THREATS

Threat of the Unfaithful or Unaware sailor

- Continuously broadcasting a single 42byte NMEA $GPGLL message containing pre-saved latitude and longitude data.

- $GPGLL,4205.8344,N,01146.5951,E, 170001.00,A,A*6C

- An iPhone without internet connection was also placed inside the hull for around 20 minutes.

- After the smartphone was able to connect back to the internet the full message was extracted at RaSS National Lab, Pisa in almost exactly 60 minutes.

APT HIDE AND SEEK: UNDERWATER COVERT THREATS

More field tests in September 2023

- Smartphone was placed outside the hull (door open for mainenance) at **~200meters using ~20mW .**
- Still **positive** results exfiltrating NMEA data of alarms.
- Exfiltrate **one message at the time**. No ack of reception.

Conclusion..

- The **feasibility** of hardware and/or software (only) for data exfiltration over spontaneous and opportunistic network channels can be achieved.
- Attempting to **anticipate** the next moves of a potential adversary is crucial
- Rigorous device management policies, conducting regular security audits, and enforcing physical security
- **Final goal:** systems should be periodically scrutinized, considering the potential for even sporadic emission of low-energy BLE packets (consider cognitive attack solutions).

…and future work

- ..can only be undertaken for the verification of the Key Performance Indicators (KPIs) of the proposed attack:
- Measurement of the maximum **throughput**
- Average **latency** of message propagation, as a function of the number of opportunistic hosts present.
- Maximum and minimum **permanence** of a message in the cloud; degree, and degradation prediction of the messages over time.
- **Range** of the BLE radio in function of the boundary conditions (more submarines!?).

This work was partially supported by the project “SER- ICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGener- ationEU.

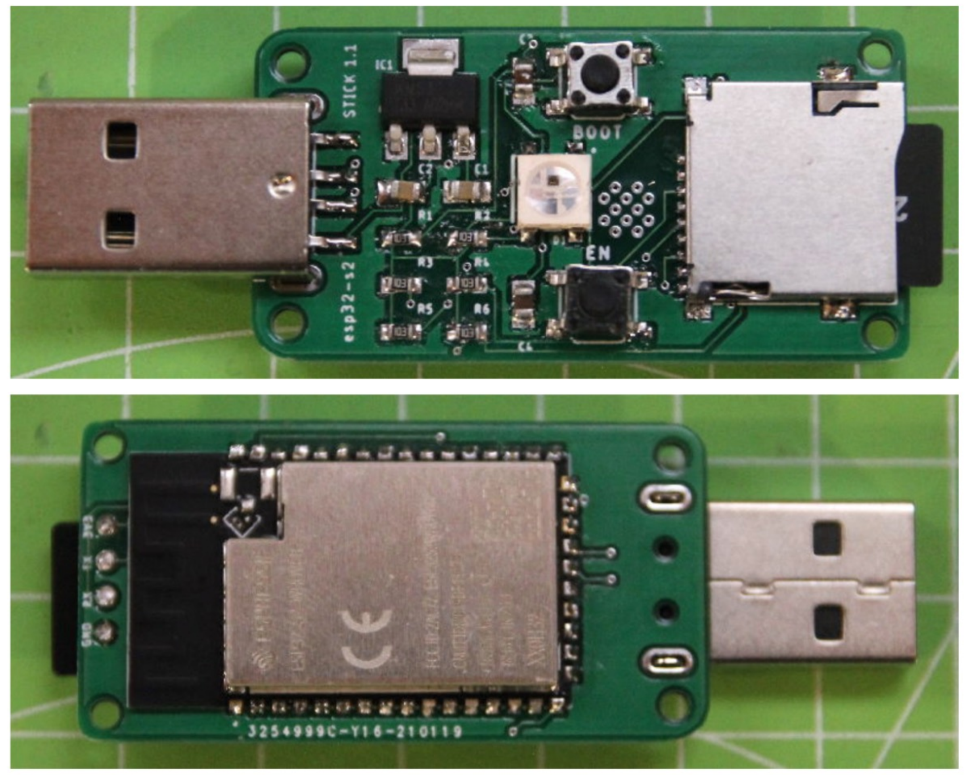
…and future offensive research

- envision micro-antennas, turned or 3D printed,
- Demo can be pushed to **consume only 27mWh**. We can adopt cognitive and stealth techniques to activate transmission and reduce.
- Specific **coding scheme** and data compression for energy-efficient exfiltration of predictable data like navigational waypoints
- **Range** of the BLE radio in function of the boundary conditions (more submarines!?).

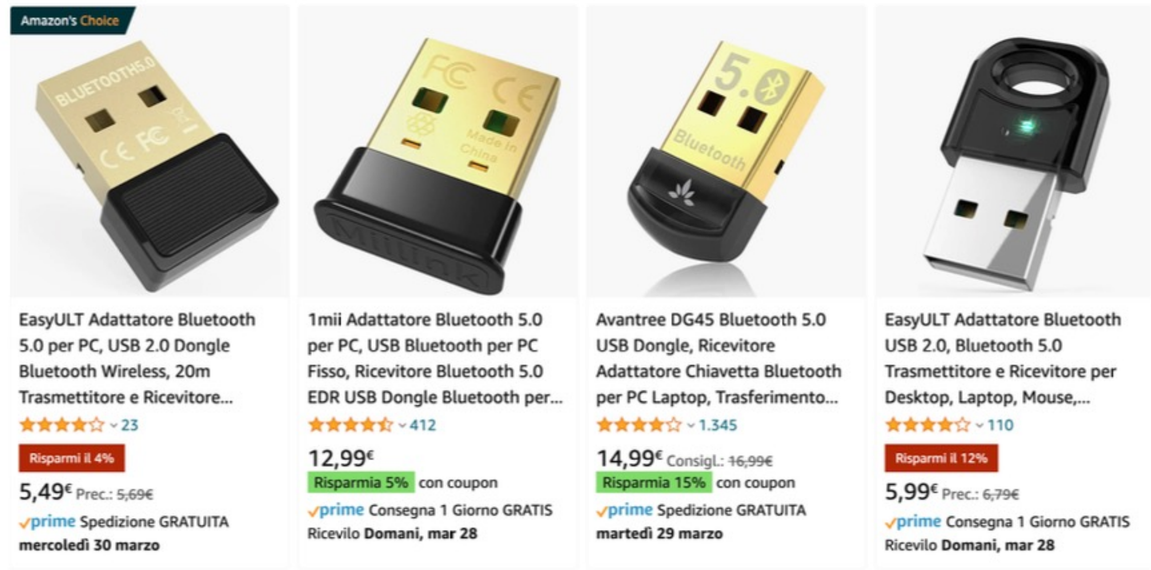
This work was partially supported by the project “SER- ICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGener- ationEU.

…and future offensive research

- Fancy ways to mess with hardware…



*ESP32Stick bought on dark-net market



Amazon's Choice

EasyULT Adattatore Bluetooth 5.0 per PC, USB 2.0 Dongle Bluetooth Wireless, 20m Trasmettitore e Ricevitore...
★★★★☆ 23
Risparmi il 4%
5,49€ Prec.: ~~5,69€~~
✓prime Spedizione GRATUITA
mercoledì 30 marzo

1mii Adattatore Bluetooth 5.0 per PC, USB Bluetooth per PC Fisso, Ricevitore Bluetooth 5.0 EDR USB Dongle Bluetooth per...
★★★★☆ 412
12,99€
Risparmia 5% con coupon
✓prime Consegna 1 Giorno GRATIS
Ricevilo **Domani, mar 28**

Avantree DG45 Bluetooth 5.0 USB Dongle, Ricevitore Adattatore Chiavetta Bluetooth per PC Laptop, Trasferimento...
★★★★☆ 1.345
14,99€ Consigl.: ~~16,99€~~
Risparmia 15% con coupon
✓prime Spedizione GRATUITA
martedì 29 marzo

EasyULT Adattatore Bluetooth USB 2.0, Bluetooth 5.0 Trasmettitore e Ricevitore per Desktop, Laptop, Mouse,...
★★★★☆ 110
Risparmi il 12%
5,99€ Prec.: ~~6,79€~~
✓prime Consegna 1 Giorno GRATIS
Ricevilo **Domani, mar 28**

This work was partially supported by the project “SER- ICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGener- ationEU.

Q&A

Thanks for your attention and for the sun today in Florida!

🏠 http://labrass.cnit.it

✉ alessandro.cantelli.forti@cnit.it