SWIMMING IOT

YACHT - IT AND OT OVERVIEW

CERTivation

Overview

- Introduction
- IT and OT
- The Bridge
- ECDIS Technical 101

Why hacking yachts?

Yachts mostly privately owned or chartered

CEO’s running their business from Yachts while traveling
Celebrities like showstars, actors & others

What, if I could control the Internet access of a yacht?
What, if I have remote access to the smart devices?

Stephan Gerling @ObiWan666

I am older than the internet
Certified as “GCFA, CISSP, MCSE, CCNA, etc.”
Electronic Specialist,
several years German Aviation Army navigation system electronic specialist
More than 32 years a volunteer firefighter in my town

IT Volunteering activities
- Geraffel (group of „hacker nerds at ist best“)
- IamTheCavalry
- AG KRITIS (NGO on critical Infrastructure)
- CCI

Networks on Board

5 Networks on Board (or more)

IT

- IT Network
- Wireless Network

OT

- Bridge Network (Navigation systems Network)
- NMEA Network
- ICS Network
- KNX

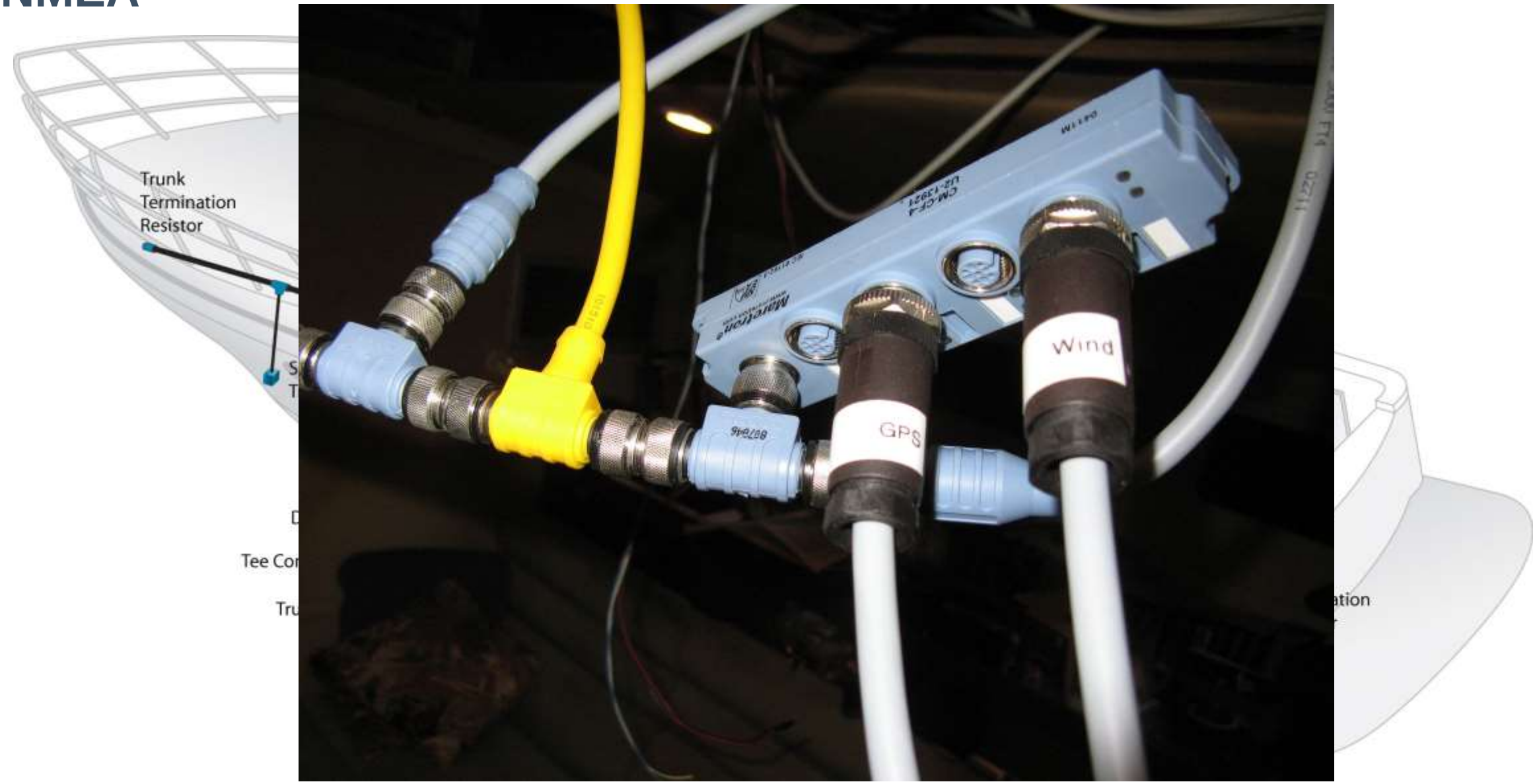
IT and OT on Yachts

Swimming IoT

Modern vessels becomme swimming IoT devices

- Vessel Traffic Service (VTS)
- Automatic identification system (AIS)
- Autopilot
- GPS
- Radar
- Camera‘s, including Thermal imaging
- Engine control and monitoring (some now cloud based) – ICS
- Internet Access
- Entertainmentsystems

NMEA



NMEA

NMEA 0183 (National Marine Electronics Association)

A combined electrical and data specification for communication between marine electronic devices, 4800 Baud speed

- echo sounder
- Sonars
- Anemometer
- Gyrocompass
- Autopilot
- GPS receivers

and many other types of instruments

NMEA

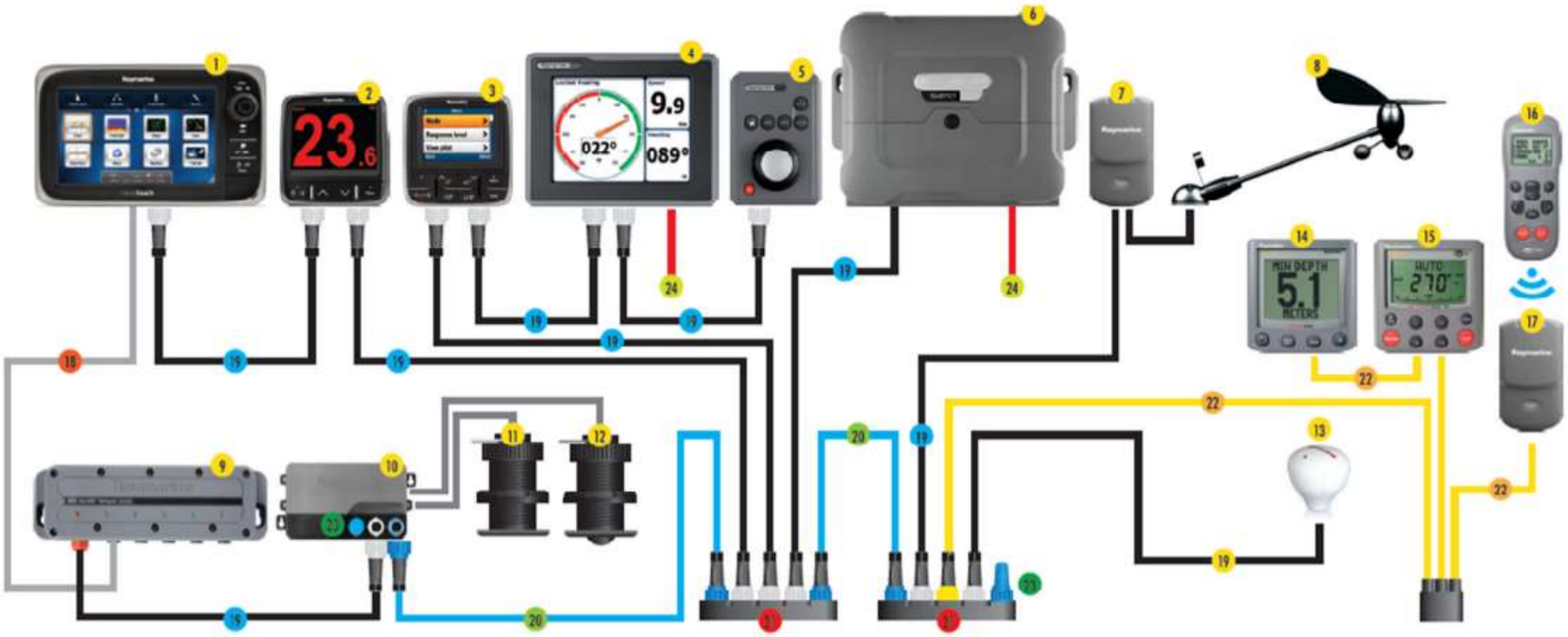
NMEA 2000

bandwidth capacities of less than 1Mbit/s

connects devices using Controller Area Network (CAN) technology originally developed for the auto industry.

NMEA 2000 network is not electrically compatible with an NMEA 0183 network

SeaTalk*ng*



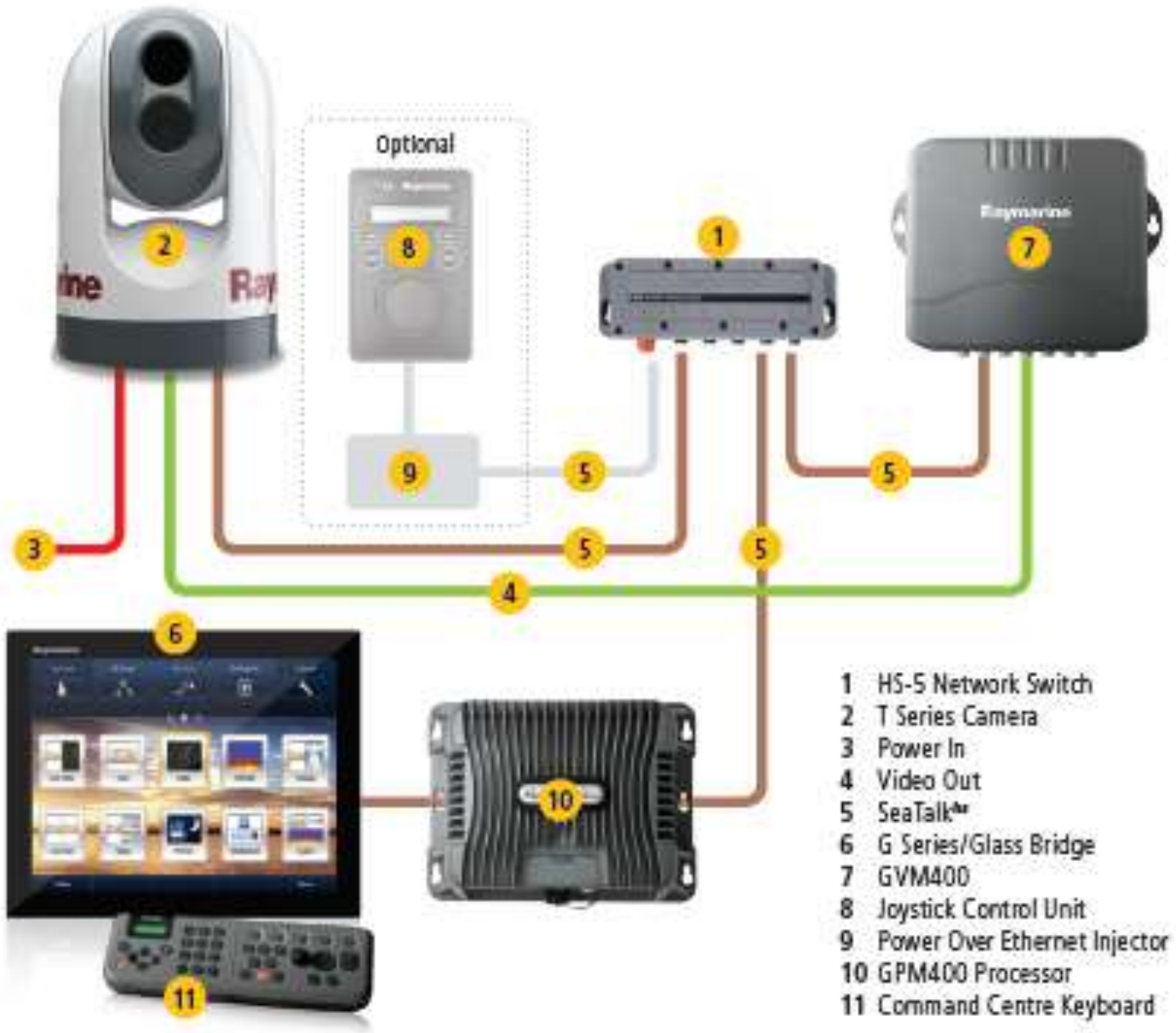
Note: Imagery for illustrative purposes only. Product images shown in suggested system diagrams are not to scale

Typical Basic SeaTalk^ng System:

1. New e Series **2.** i70 Instrument **3.** p70/p70R Autopilot **4.** ST70 Plus Instrument **5.** ST70 Plus Autopilot Keypad **6.** SPX Course Computer **7.** Pod **8.** Wind Transducer **9.** Network Switch **10.** iTC-5 **11.** Speed Transducer **12.** Depth Transducer **13.** RS130 GPS Sensor **14.** ST60+ Instrument **15.** ST6002 Autopilot **16.** SmartController **17.** Pod **18.** RayNet Cable **19.** SeaTalk^ng Spur **20.** SeaTalk^ng Backbone **21.** 5-Way SeaTalk^ng Connector **22.** SeaTalk **23.** Terminator **24.** Power Supply

http://www.raymarine.de/uploadedFiles/Products/Networking/SeaTalk/SeaTalkng.pdf

SeaTalk*hs*



http://www.raymarine.de/uploadedImages/Products/Networking/HS%20with%20HS5%20switch.jpg

IT Equipment on Board

Internet Access

- GSM
- WiFi
- SAT (Inmarsat, VSAT, Iridium, etc.)

On Board

- Entertainment Systems
- WiFi (Crew, Guest/Owner)
- VoIP

IT equipmen

10 Smart

1 Chart R

14 VoIP T

1 Interne

1 rack m

1 UPS

4 WiFi Ac

(Crew, G

AV equipment on Board

Smart TV

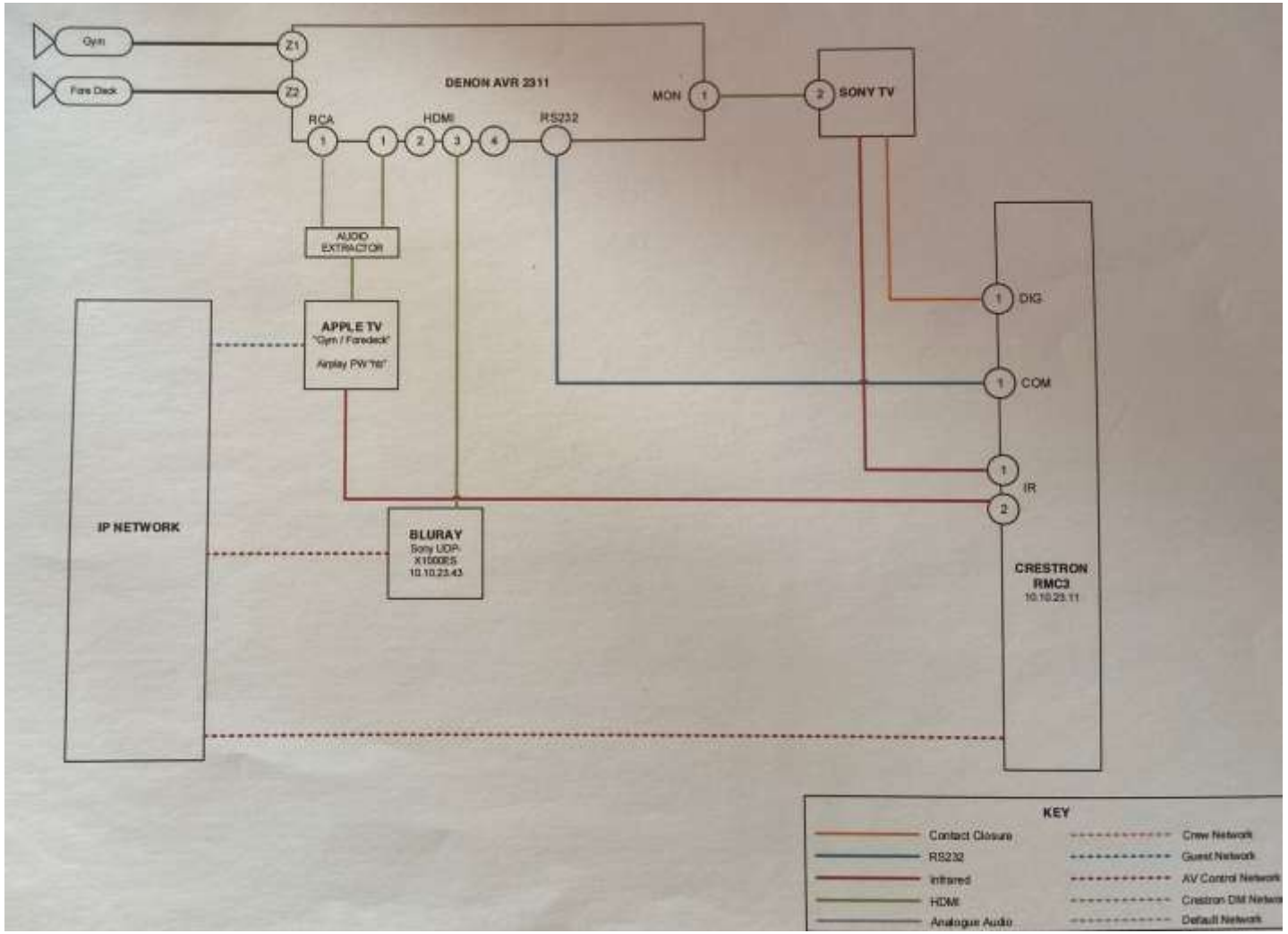
Sat Receiver

AVR

Blueray

AppleTV

Crestron



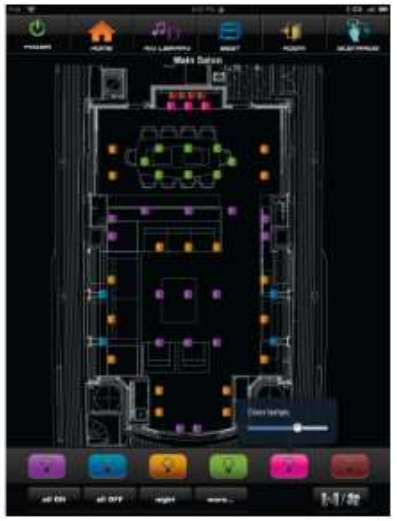
Smart Ships

Audio & Video Streaming

iPhone/iPad remote control of

- Lights
- Electric curtains
- Engine monitor
- ruder

Etc.



OT Equipment on Board

- Engine Monitoring and Control
- Propulsion
- Bowtruster
- KNX (or other Bus for Light control)
- PLC’s

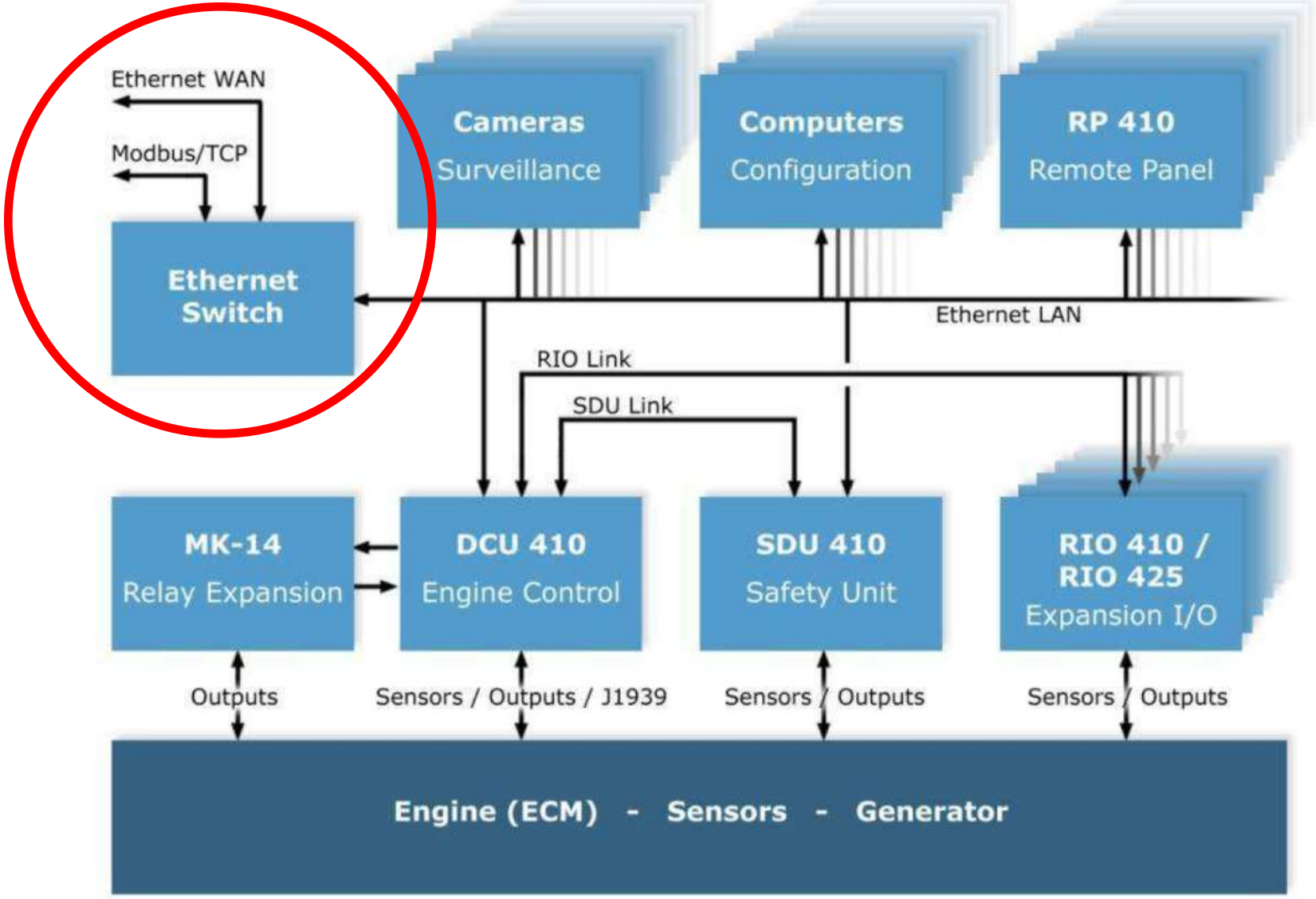
OT

ICS – Industrial Control Network – the OT part

Own Network with Computer to control

- Engine
- Sensors
- HVAC
- Water distribution
- Pumps and Valves
- Etc.

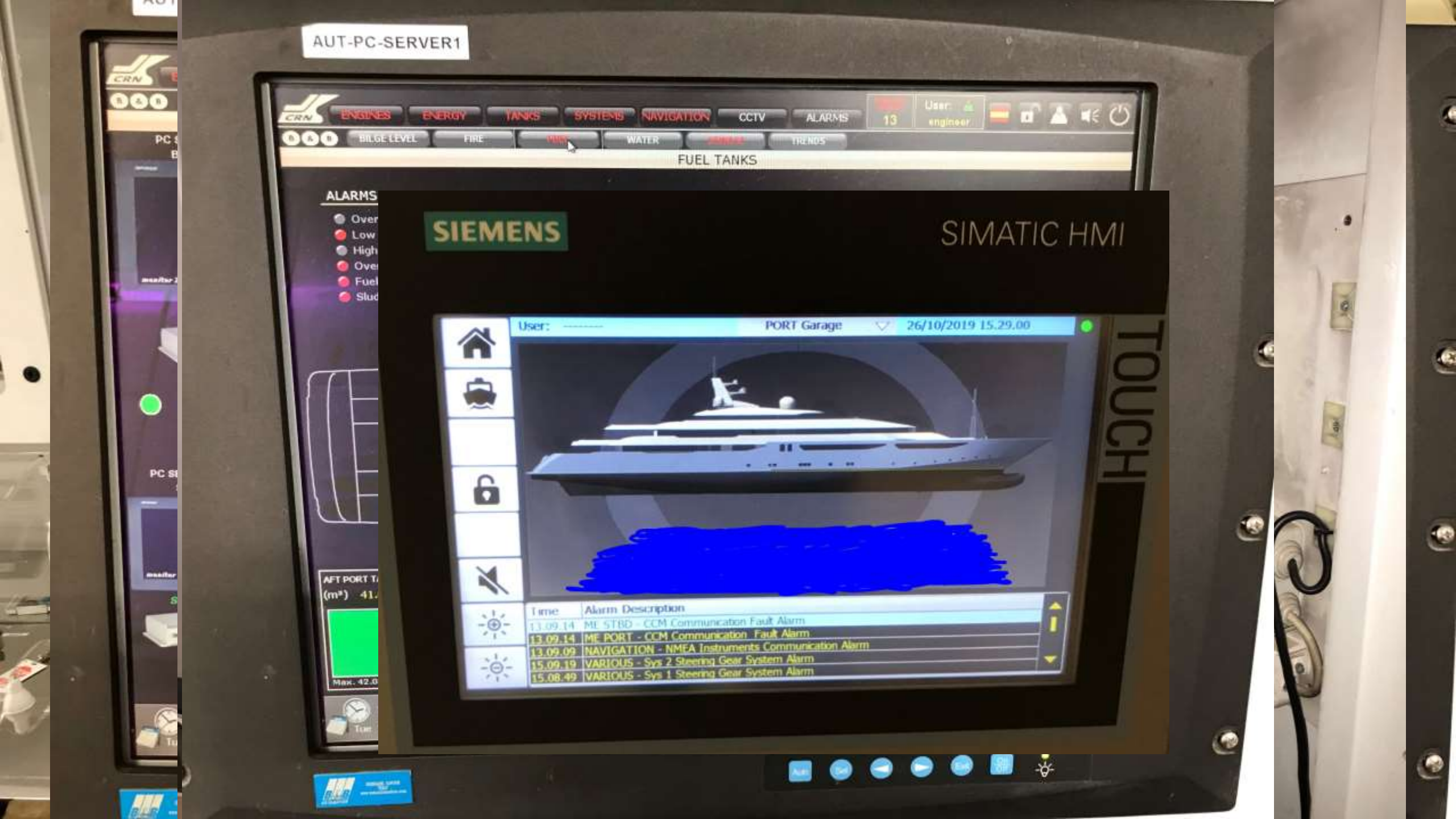
Engine Control units

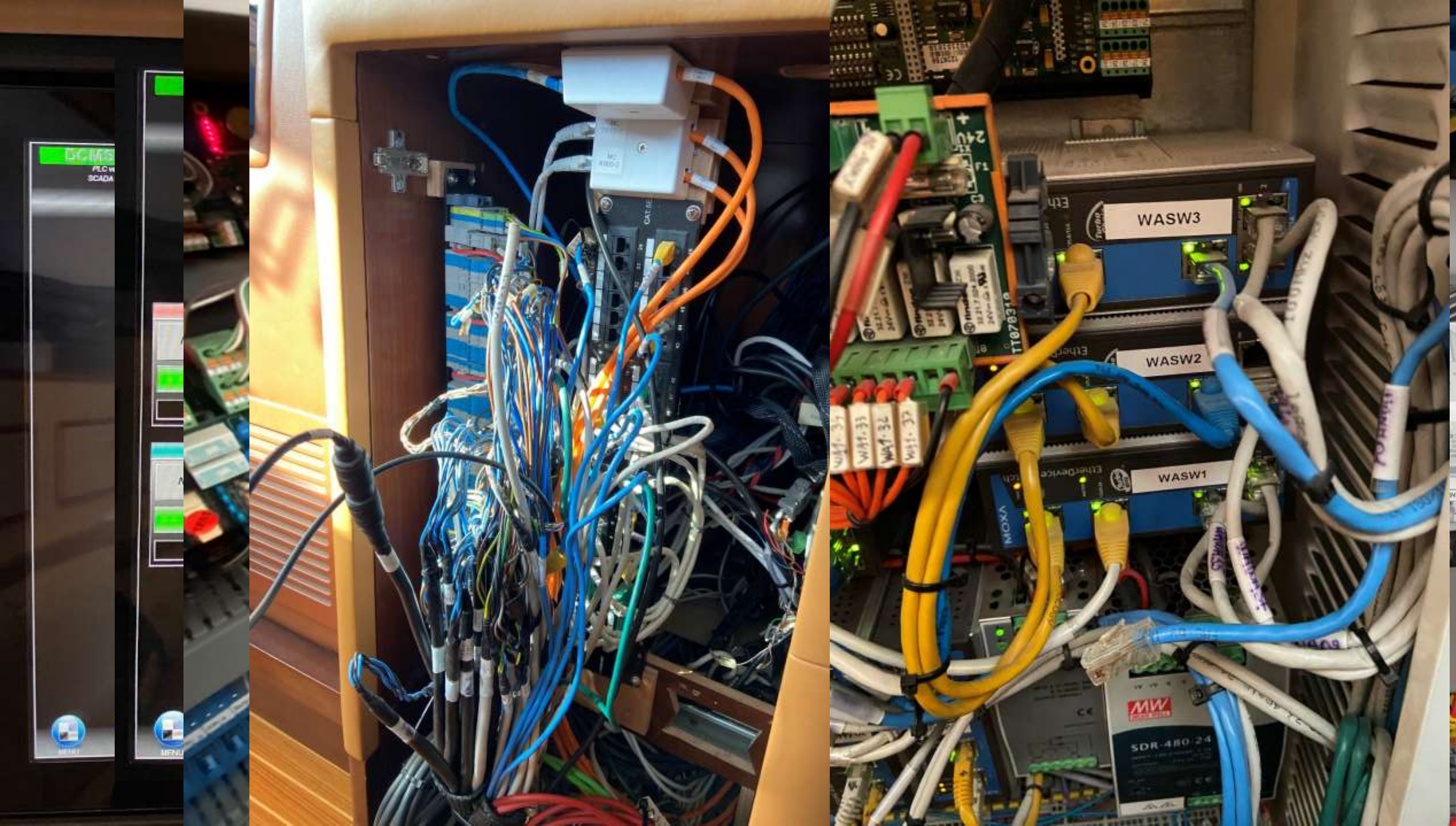


Auto Maskin 400_Series_Installation_and_Configuration__Manual_2_11.pdf

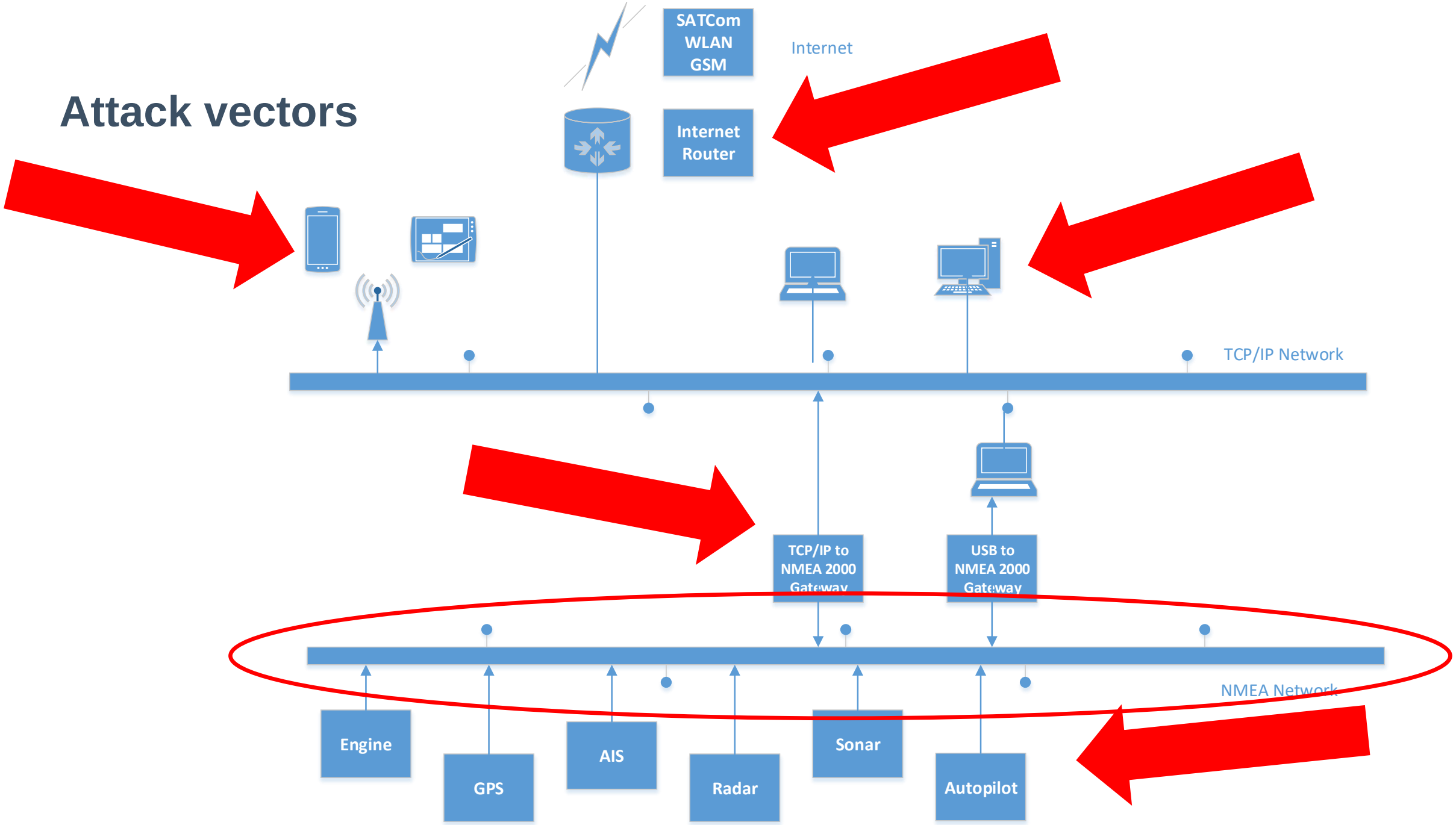
ECU
Remote Panel
Safety Unit
Etc.

Mostly Connected to the Ethernet like a MTU wired remote control for engines and bow-thruster


AUT-PC-SERVER1
ENGINES
ENERGY
TANKS
SYSTEMS
NAVIGATION
CCTV
ALARMS
13
User:
engineer
BILGE LEVEL
FIRE
WATER
TRENDS
FUEL TANKS
ALARMS
SIEMENS
SIMATIC HMI
User:
PORT Garage
26/10/2019 15.29.00
TOUCH
Time
Alarm Description
13.09.14 ME STBD - CCM Communication Fault Alarm
13.09.14 ME PORT - CCM Communication Fault Alarm
13.09.09 NAVIGATION - NMEA Instruments Communication Alarm
15.09.19 VARIOUS - Sys 2 Steering Gear System Alarm
15.08.49 VARIOUS - Sys 1 Steering Gear System Alarm


WASW3
WASW2
WASW1
SDR-480-24

Attack vectors

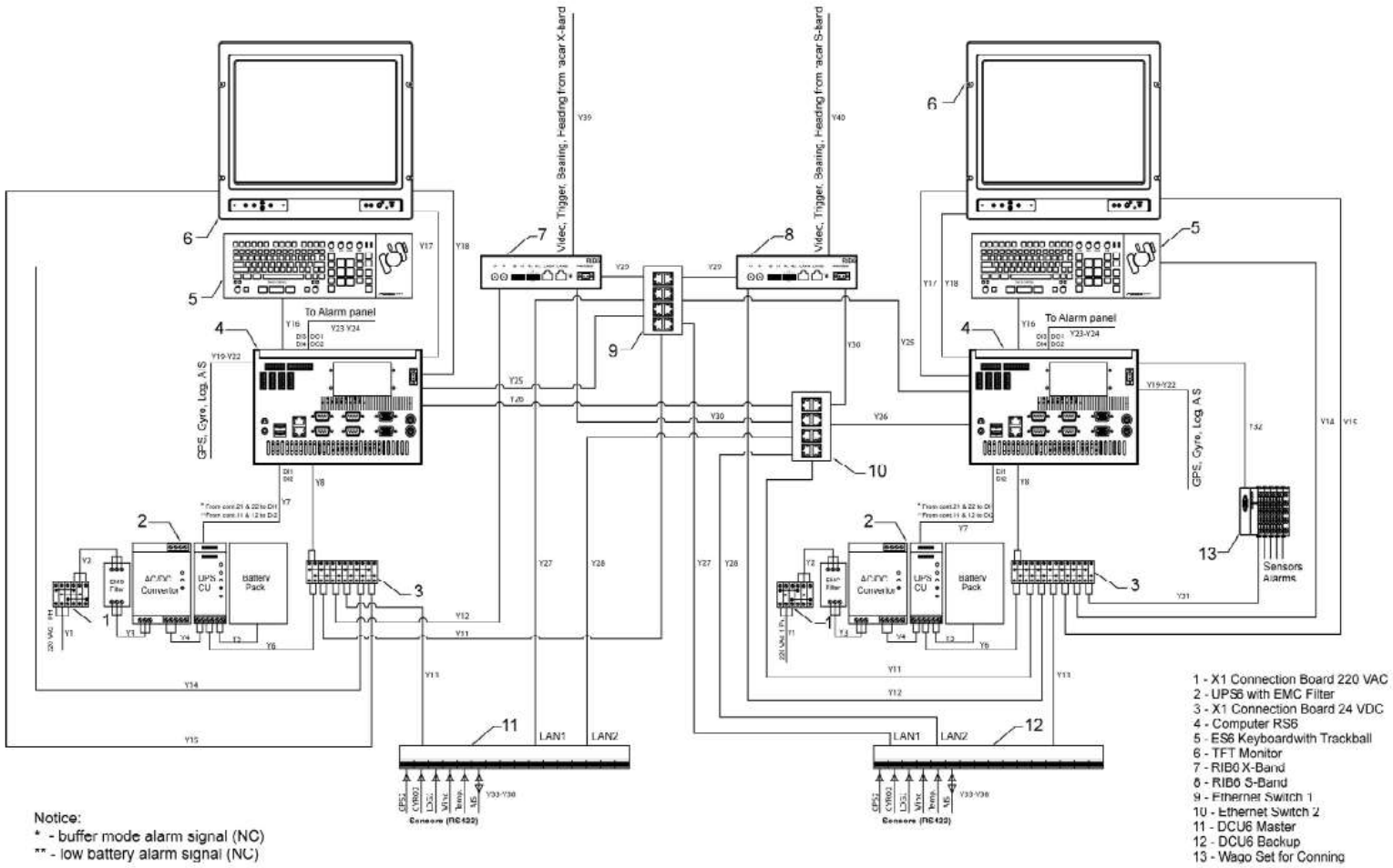


The Bridge

The Bridge

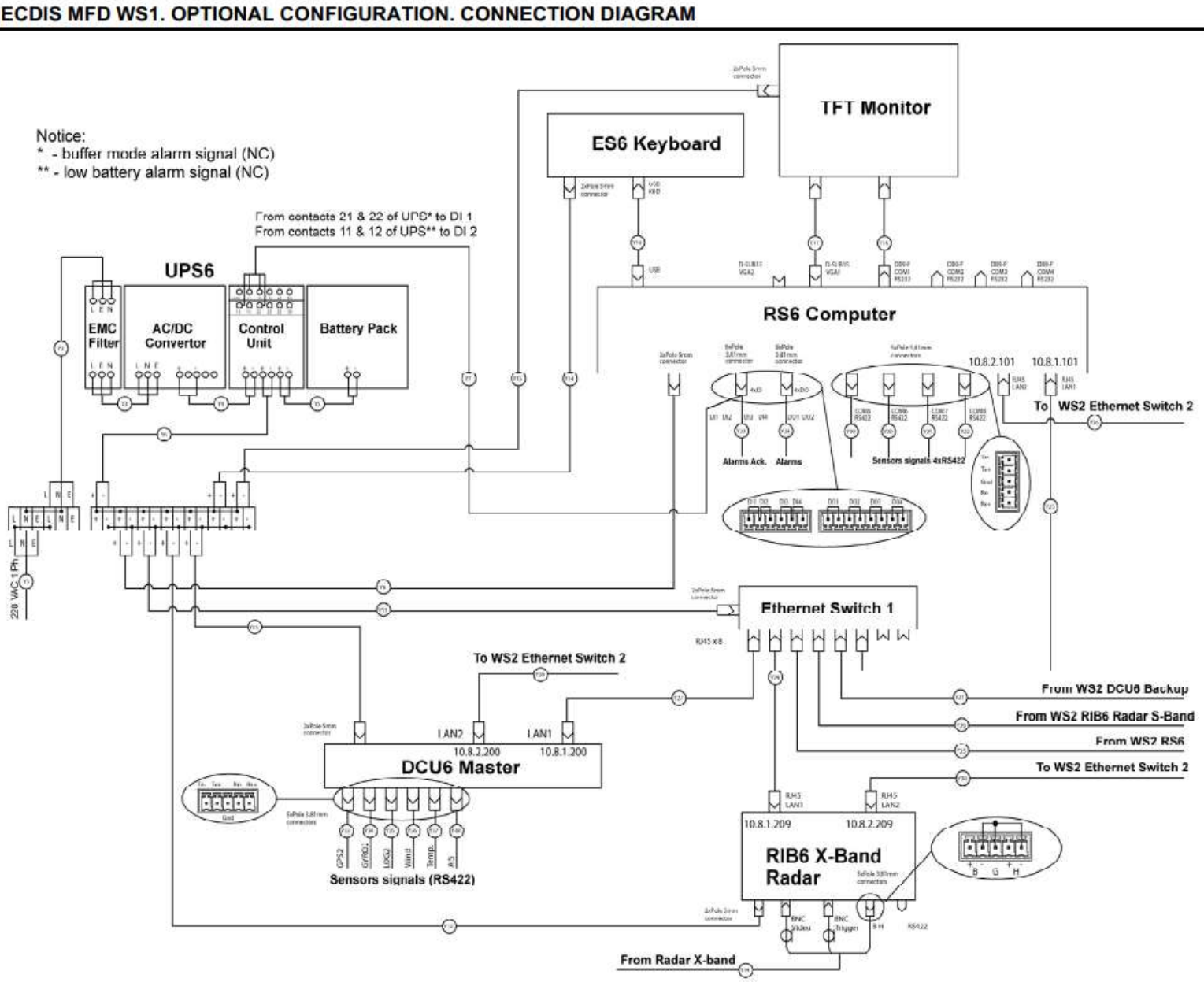
Bridge Network Diagram (Transas Navisailor)

NS 4000/4100 ECDIS MFD (WS1 AND WS2). OPTIONAL CONFIGURATION. BLOCK DIAGRAM



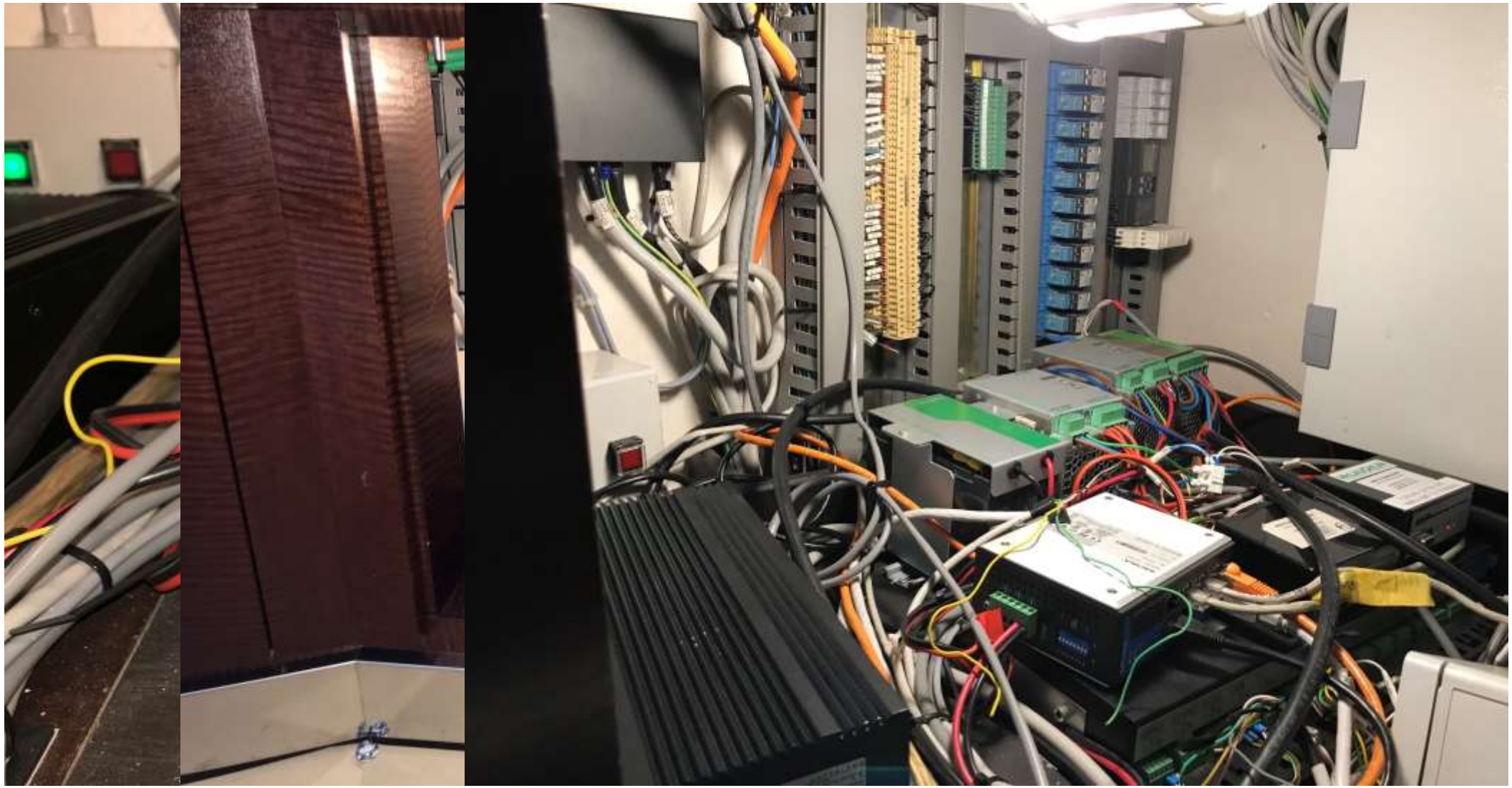
https://www.marinsat.com/marinsat/dosyalar/dosya/NS4000_4100_ECDIS_Installation_Guide_eng.pdf

Bridge



https://www.marinsat.com/marinsat/dosyalar/dosya/NS4000_4100_ECDIS_Installation_Guide_eng.pdf

Bridge Network reality

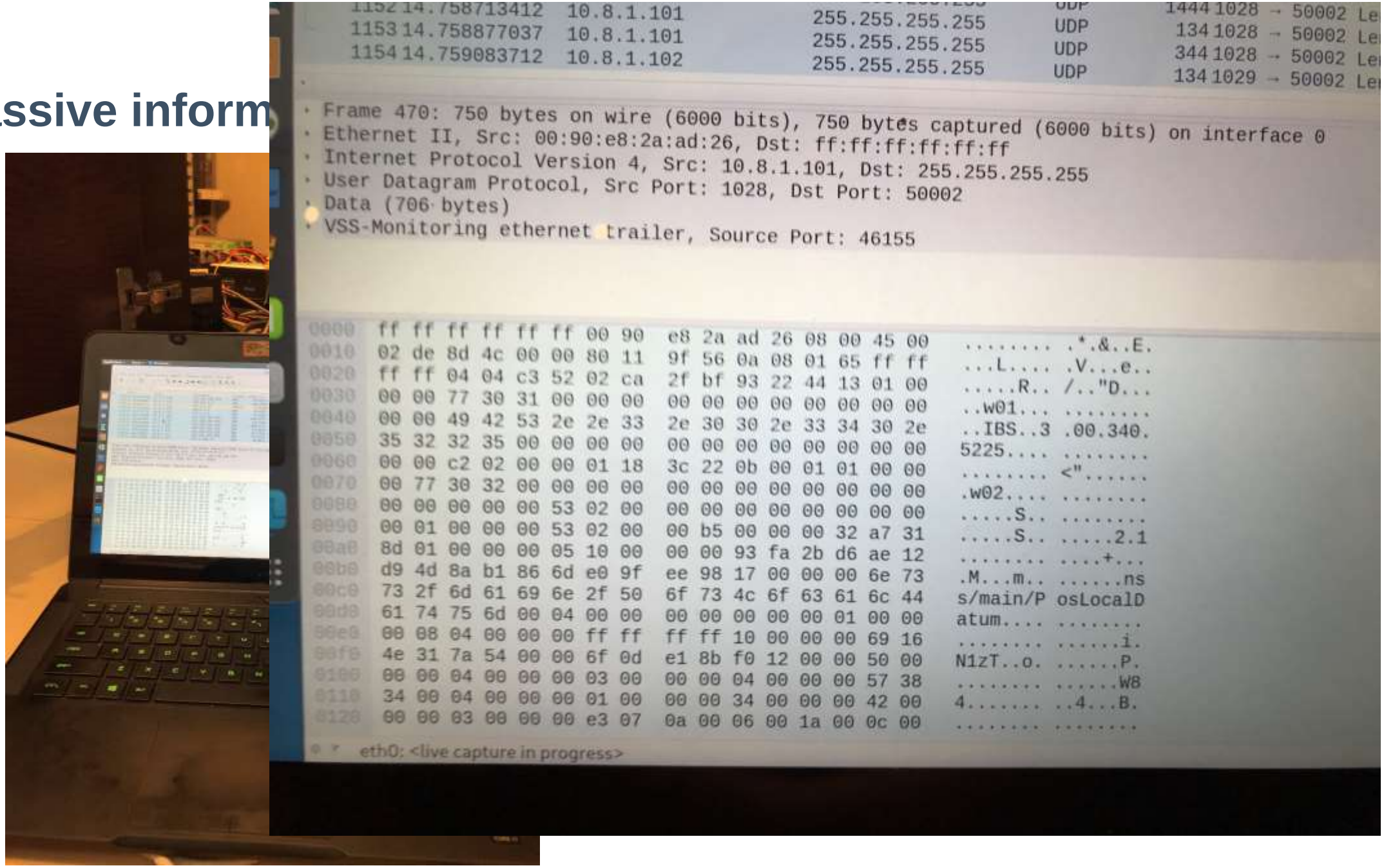


Warning

Attach passively to the network (no active connection)

- Under Linux read only NIC config (no arp, no ip, no dhcp….)
- Don’t NMAP the Network (legacy systems sometimes break)
- Disconnect nothing unless u know what you do
- Always ask the Captain before you do something

Passive inform



OT devices

Electronic Chart Display and Information System (ECDIS)

ECDIS is a geographic information system used for nautical navigation displays information from:

- Electronic Navigational Charts (ENC)
- or Digital Nautical Charts (DNC)

integrates position information

- Position
- Heading
- speed

sensors which could interface with an ECDIS are radar, Navtex, Automatic Identification Systems (AIS), and depth sounders.

ECDIS


HDG
GYRO 1
277.4°
STW
LOG 1
0.0 kn
COG
GPS 1
215.8°
SOG
GPS 1
0.0 kn
Overscale
SF CNT
End of watch
ECDIS
Default Safety Contour
Route Data
Current SOG
ETA
(Ship)
TTG
DWOL
PTA
Quick calculation
STG (kn)
PTA (Ship time)
STD DISP
Event
EBL 2
OFFSET
VRM 2
Fixed
Main
Dual
AIS
Charts
Config
Tasks
Tasks List
Depth in Metres
TRANSAS

ECDIS

default credentials

ECDIS

NMEA data

ECDIS

Network Time Protocol Server

Network Time Protocol Server

ZNT-100 Network Time Protocol Server

ZNT-100 NTP Server receives the time information from GPS and synchronization the internal clock and transmits the received time information to external equipment using NTP.

ZNT-100 NTP Server

90 x 137 x 42mm / 0.5kgs

Brochure

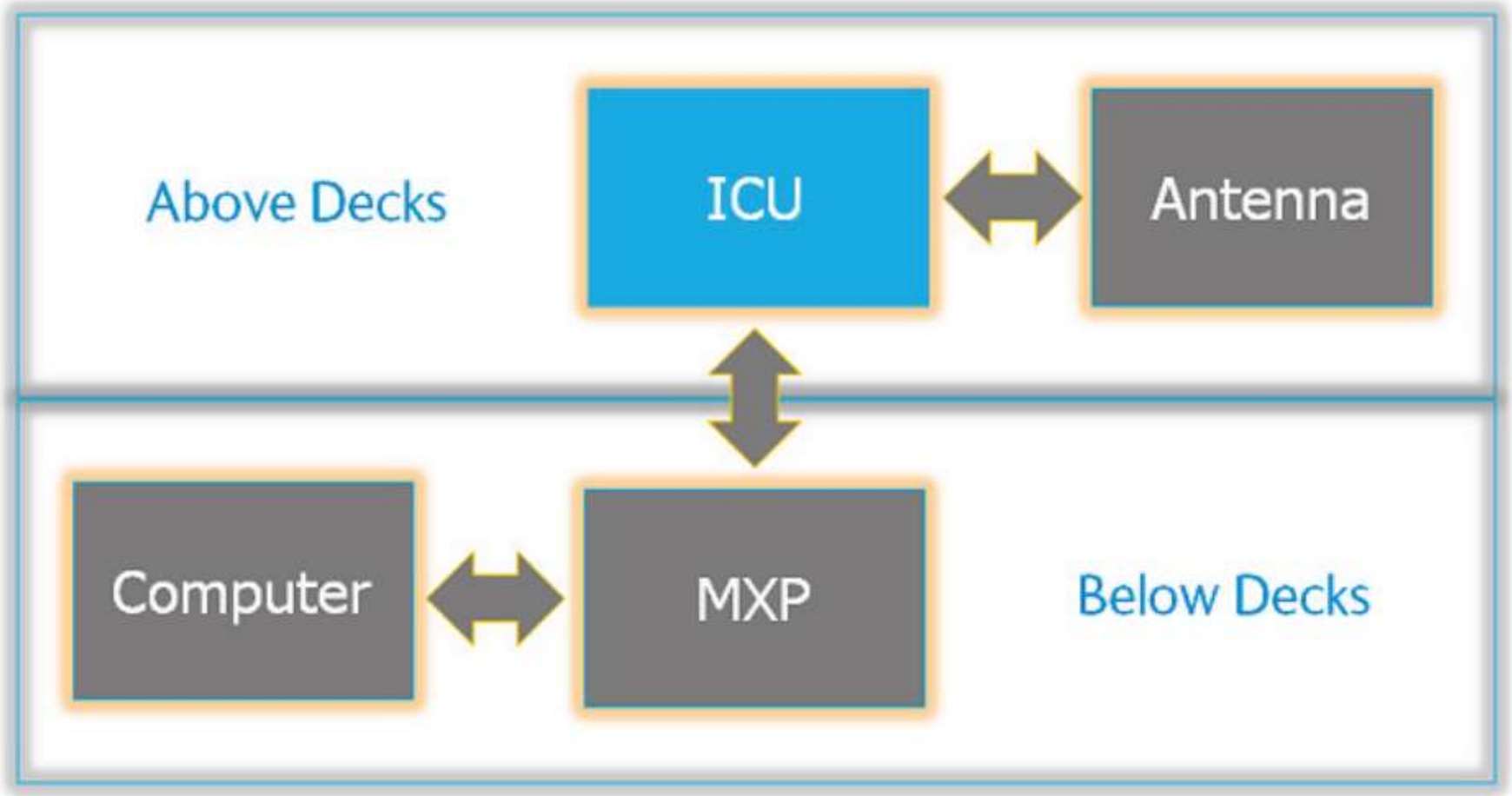
Satcom

Satcom

- Offshore internet acces via Satcom
- Patching ?
- Many old Versions still online

SatCom


Sea Tel
COBHAM


Above Decks
ICU
Antenna
Computer
MXP
Below Decks

Satcom

Shodan.io search hint’s for possible vulnerable devices

- “Sailor 900”
- “Inmarsat Solutions”
- “Telenor Satellite”
- “Commbox”
- org:"Intelsat GlobalConnex Solutions (GXS)“
- org:"Telenor UK Ltd"

Satcom

Was shodan surfing for other Satcom Boxes !
“stabilized Digital Antenna System” result paid my attention

- Results in Cobham MXP Webserver
- Shodan Query for “Server: Micro Digital Webserver” gives better result

Index
66.205.57.98
Intelsat GlobalConnex Solutions (GXS)
Added on 2018-05-26 02:15:11 GMT
United States
Details

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

2018

Shodan | Developers | Book | View All...

SHODAN

Server: Micro Digital Web Server

Explore | Downloads | Reports | Developer Pricing | En

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

21

TOP COUNTRIES

United States	8
Brazil	5
Italy	2
United Kingdom	2
Singapore	1

TOP SERVICES

HTTP	17
HTTP (8080)	3
HTTPS	1

Index

66.205.57.98

Intelsat GlobalConnex Solutions (GXS)

Added on 2018-05-26 02:15:11 GMT

United States

Details

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

Index

217.173.54.10

Telenor UK Ltd

Added on 2018-05-26 00:24:52 GMT

United Kingdom

Details

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

2020

SHODAN | Downloads | Pricing | "Server: Micro Digital Web Server"

TOTAL RESULTS

19

TOP COUNTRIES

United States	12
Malaysia	2
Japan	1
Italy	1
Hong Kong	1

More...

TOP PORTS

80	15
49153	1
14265	1
8088	1
8082	1

Download Results | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Index
216.236.194.4
SES
United States

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

Index
74.114.107.214
Global Data Systems
United States, Krotz Springs

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

Index
216.236.193.212
SES

```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
```

Satcom OSINT

~~Did u know? Shodan.io has a Live Shiptracker~~

~~URL: Shiptracker.shodan.io~~

Last year, SHODAN has switched off access to the shiptracker.

VSAT provider uses IP masquerading (NAT) to minimize exposure to Internet

- Device not visible to internet or shodan
- Gives the Owner/Crew Deceptive security
- Vulnerabilities still there, VSAT provider “could” exploit it

Cobham Seatel Satcom RTFM

RTFM ! In the manual: default usename and password

- Dealer
- seatel3

- SysAdmin
- seatel2

- User
- seatel1

What’s next?

- ECDIS Protocol decoder for wireshark
- Release all my tools on Github
- https://github.com/ObiWan666/maritime

Linkedin: ***Stephan Gerling***
Twitter: ***@ObiWan666***
E-Mail: ***ObiWan666@eclipso.de***
https://github.com/ObiWan666/maritime

THANK YOU FOR JOINING THIS PRESENTATION.

www.certivation.com

CERTivation