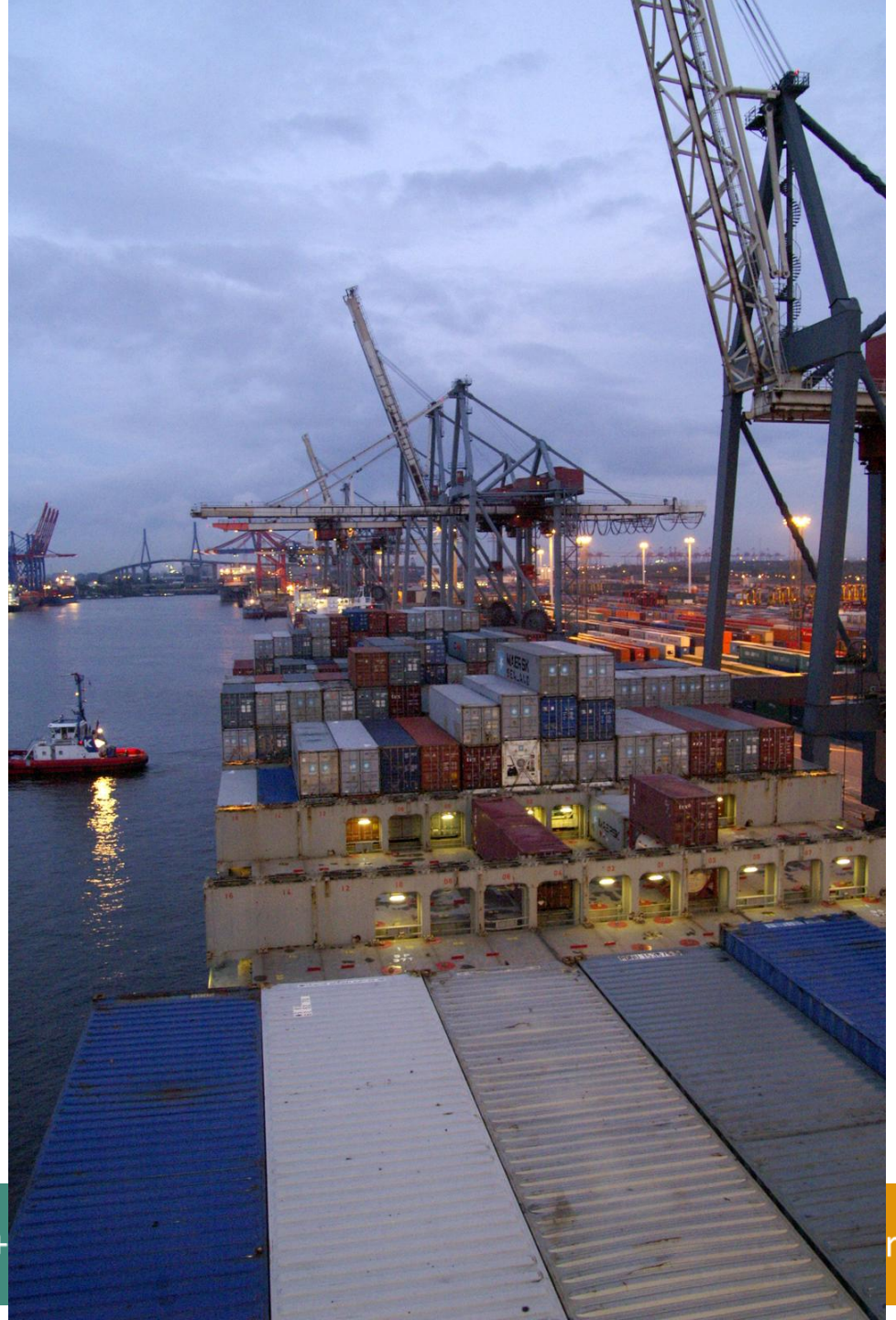
The Devil is in the Detail

PEN TEST PARTNERS

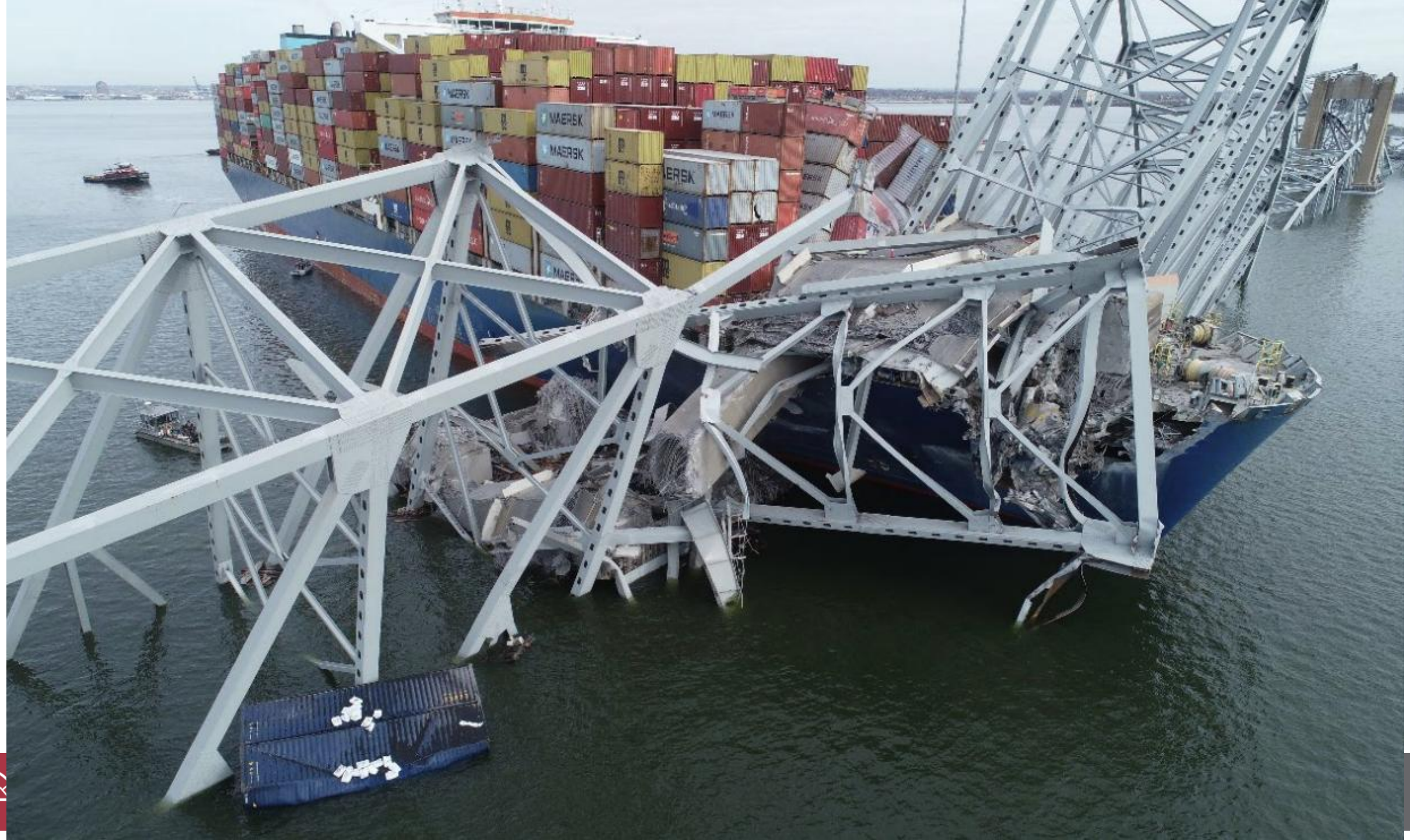


info@pentestpartners.com

+

rs

PenTestPartnersLLP


MAERSK
MAERSK

Lara Logan
@laralogan

Subscribe

The Baltimore Bridge collapse was a cyber attack and they know it. Their own intel agencies told them from the start and yet they are still denying it. Oh well. There is only one truth & nothing any of us say can change it.

6:44 PM · Mar 31, 2024 · **355.7K** Views

@CharlesleeTX1911 @Charles07788205 · Mar 31

Commercial cargo ships like the Dali cannot be remotely hacked. They could only be hacked by someone onboard using a zip drive to insert malicious code.

Their computer systems simply don't have the downlink capability necessary.

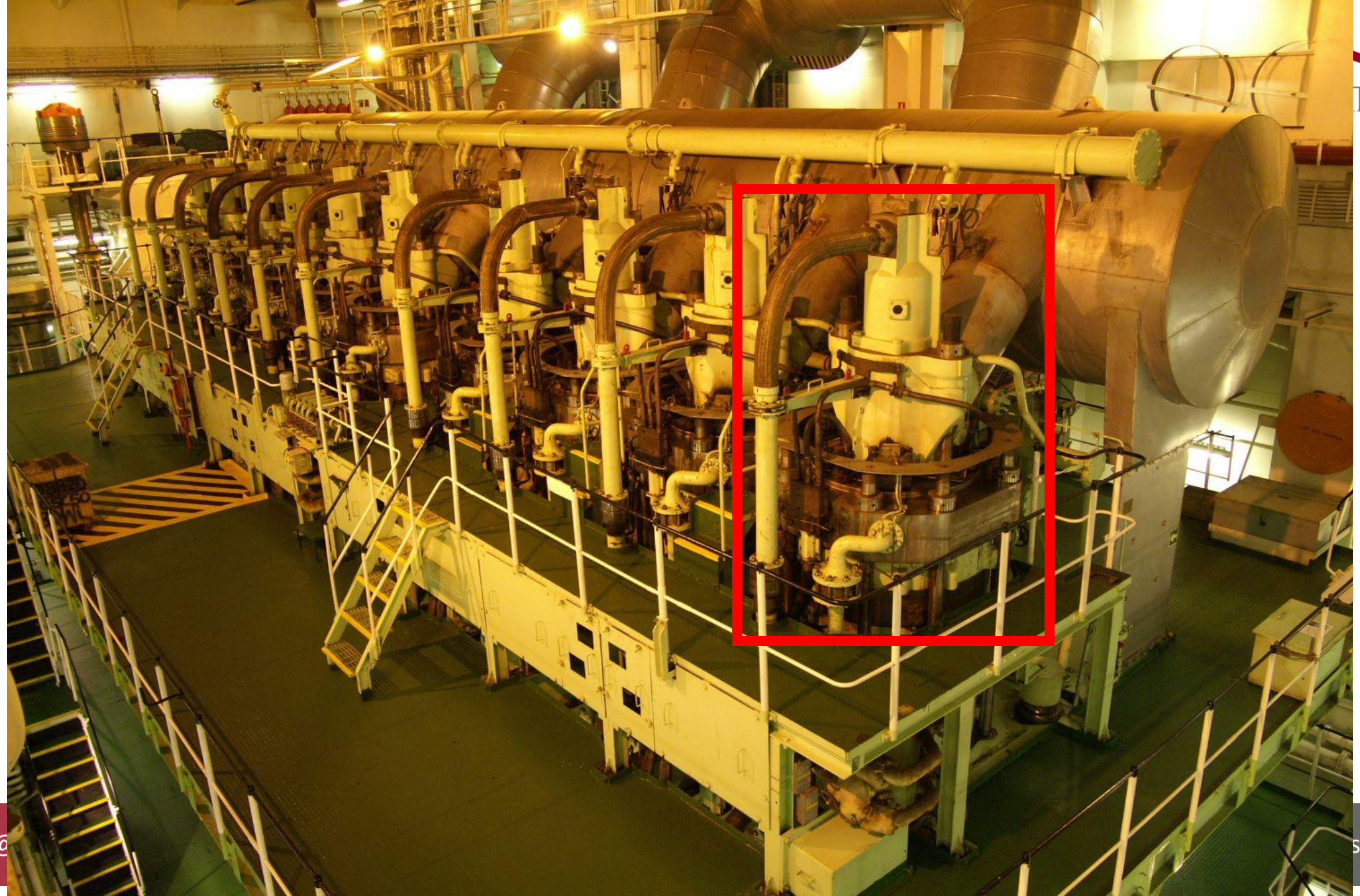
Was MV Dali hacked?

Almost certainly not.

Can ships be hacked?

Yes.

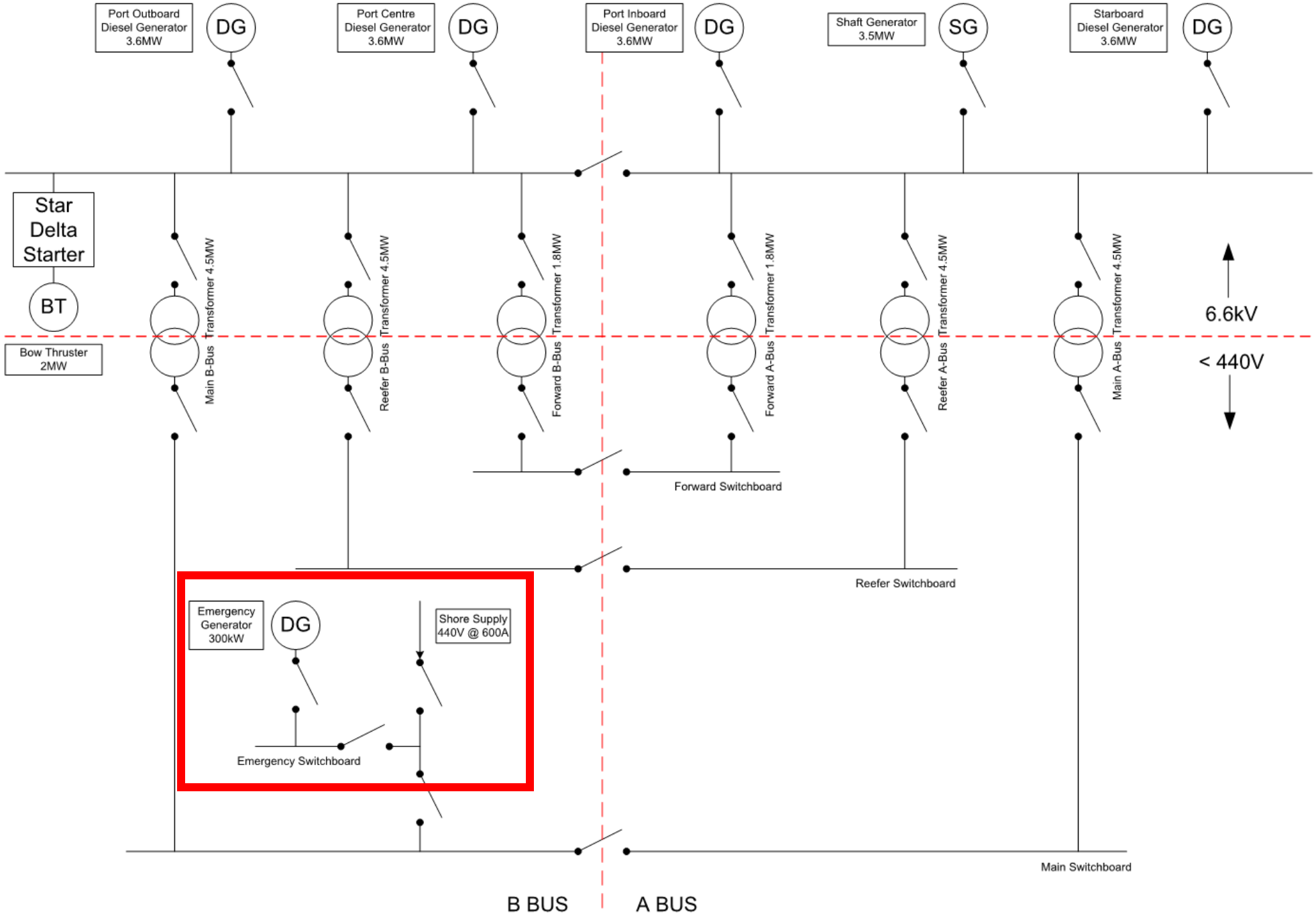

MAGNETIC
COMPASS LIGHT
WHEN NOT IN USE
OFF HEADING:PILOT WATCH
DATA
CHANGE
DIMMER
25 APRIL 2024
EMERGENCY STEERING DRILL
RECOMMENDED TURN FOR MAN OVERBOARD
Williamson turn
Rudder hard over (in an "immediate action" situation, only to the side of the casualty).
After deviation from the original course by 60°, rudder hard over to the opposite side.
When heading 20° short of opposite course, rudder to midship position and ship to be turned to opposite course.
20°
60°
0°
SYSTEM
Laden
OFF
No.2
No.1
NFU
PORT
TOKYO KEIKI
P
S
MODE
HAND
AUTO
NFU
Switch to NFU during
Emergency Steering



PEN TEST PARTNERS

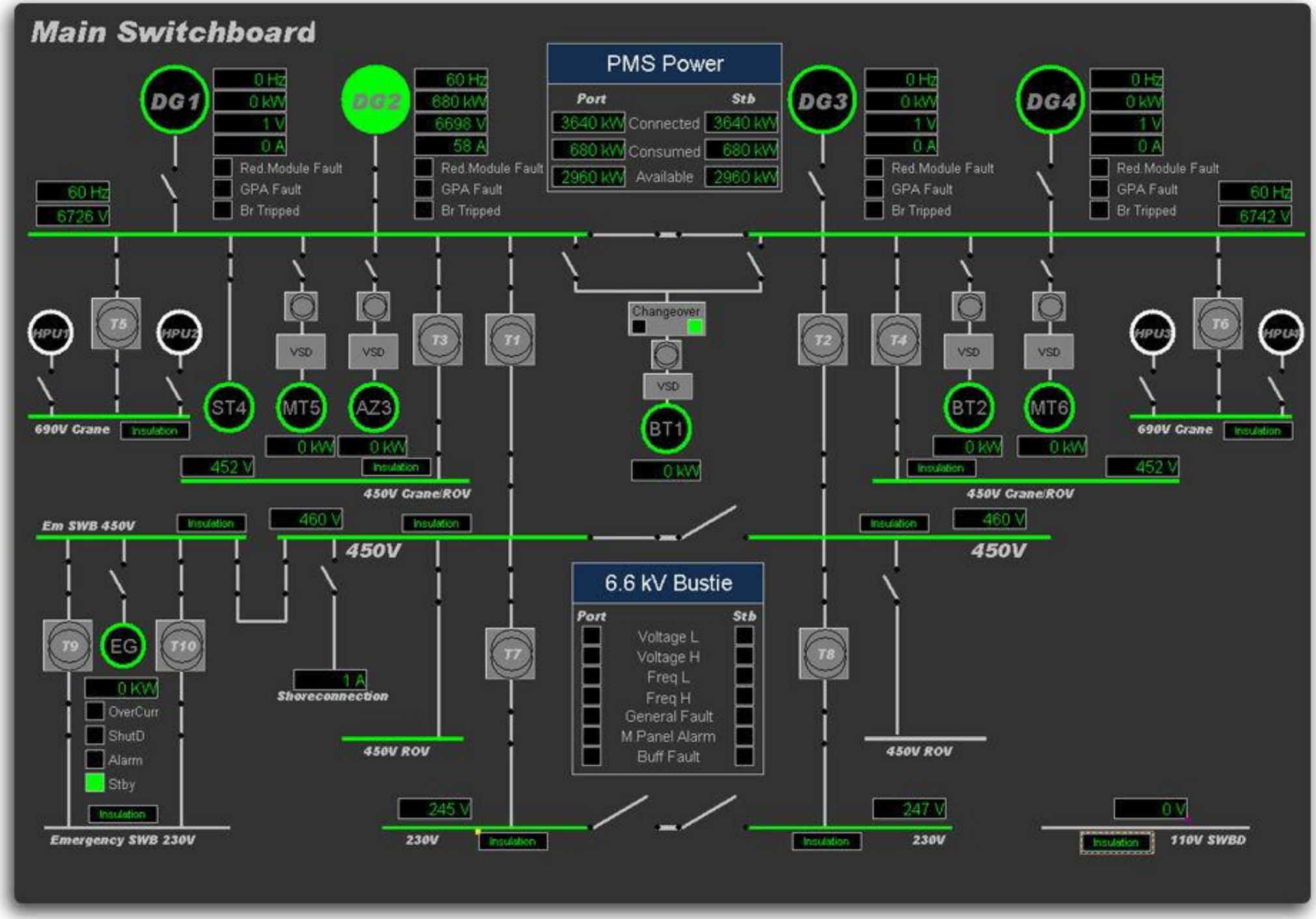
Blackout

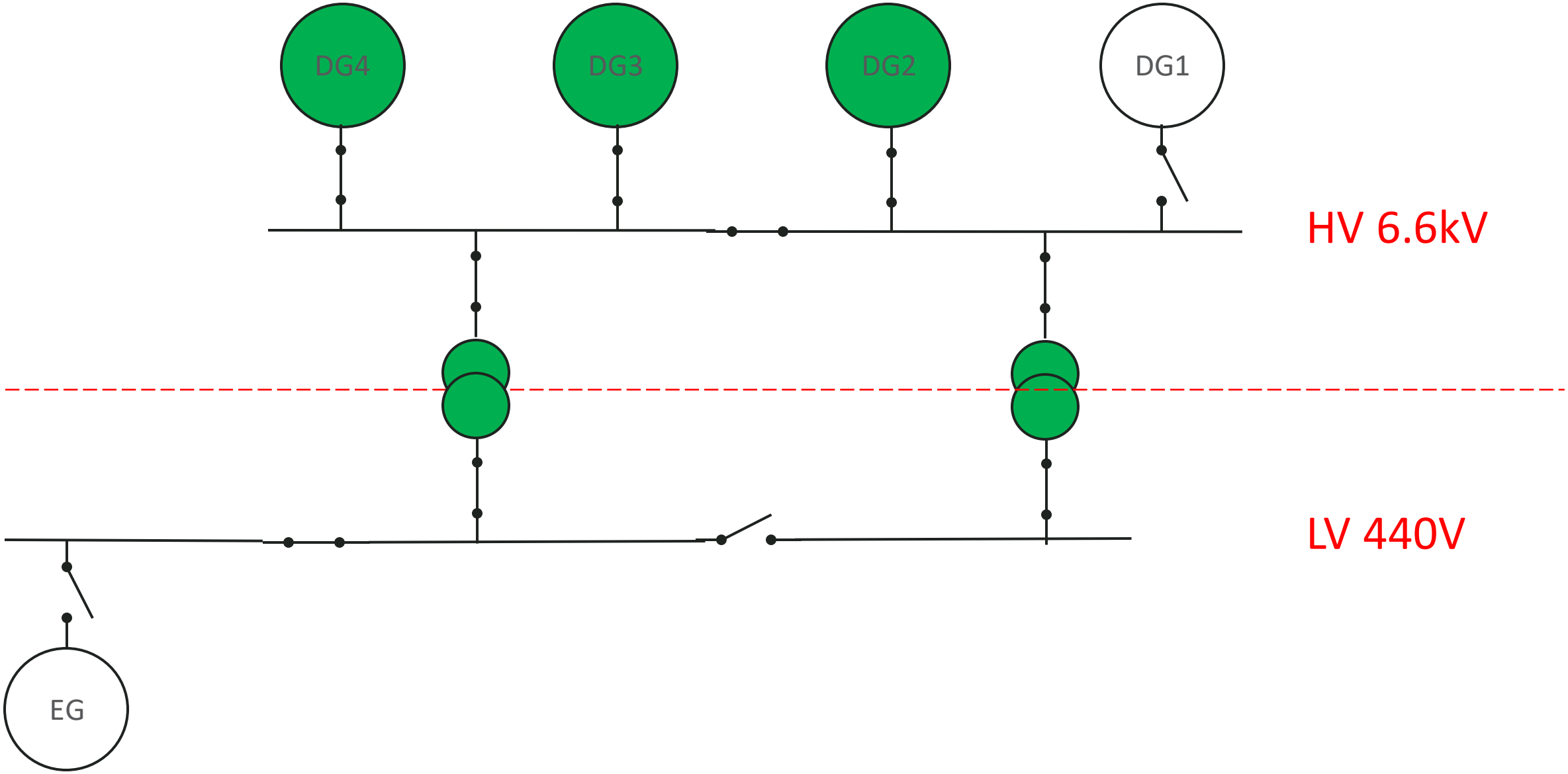
Loss of electrical power leading to loss of propulsion and steering



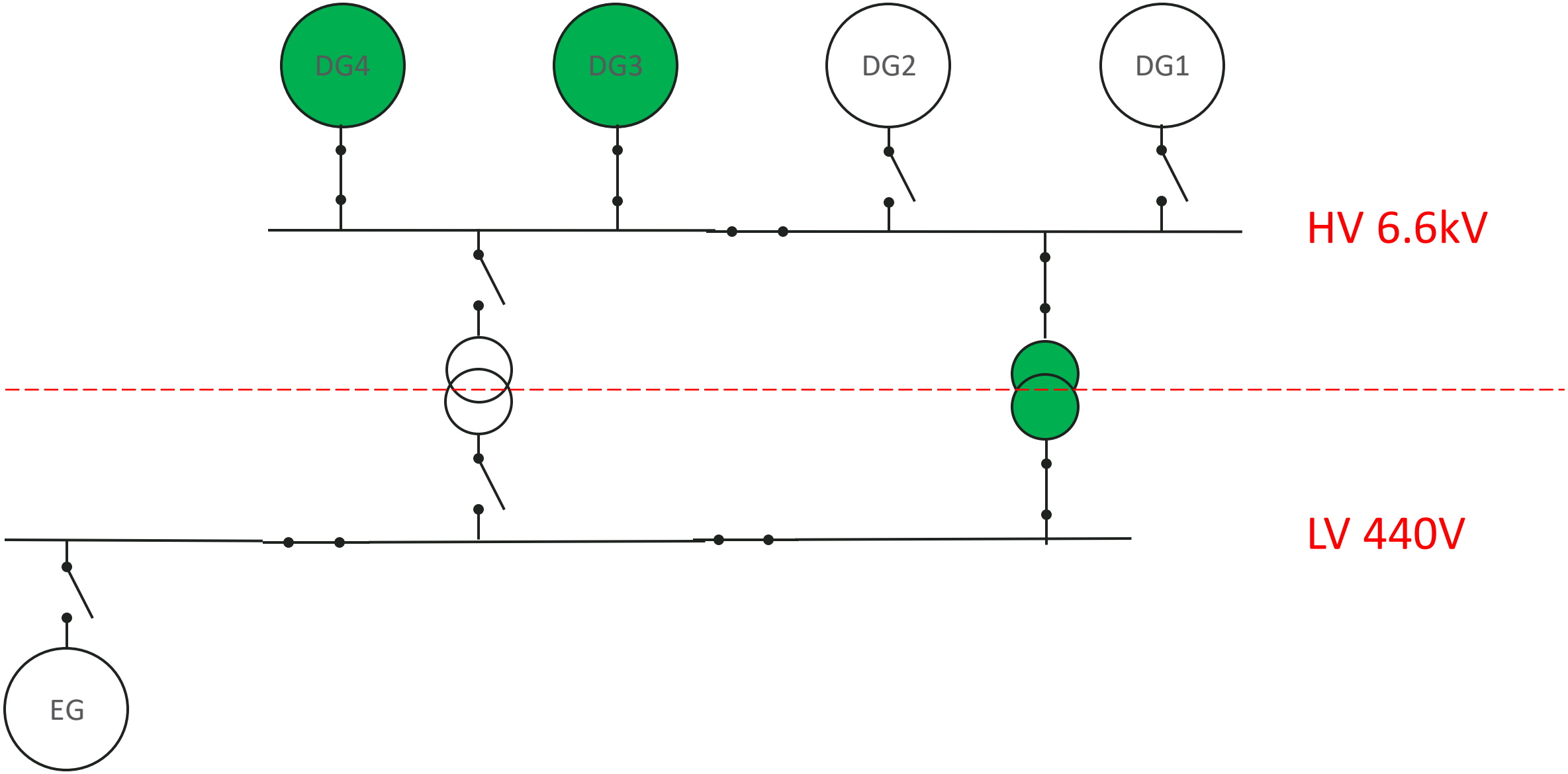
Ideal Recovery

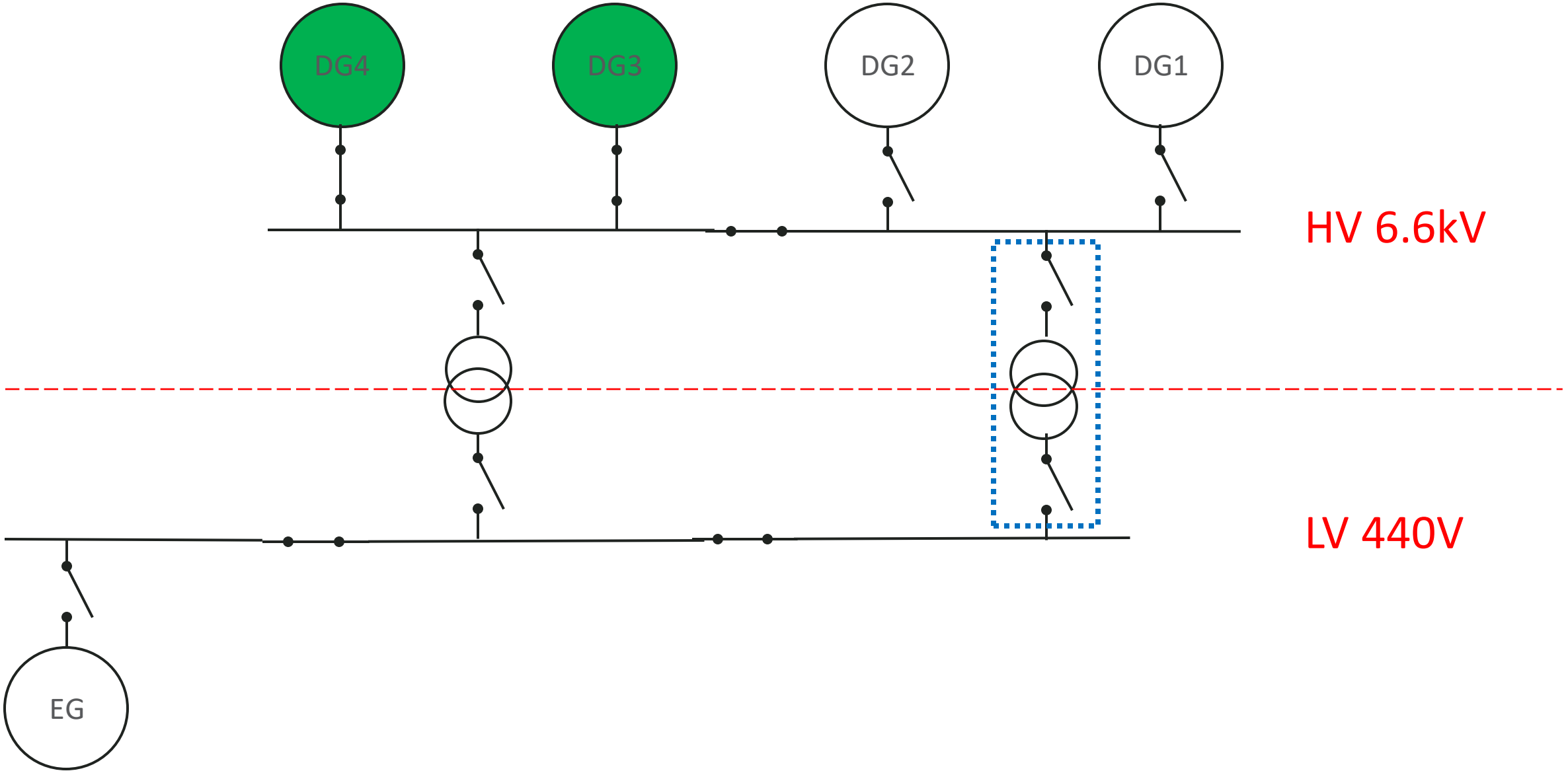
Generator trips - blackout
Emergency generator starts
Standby generator starts
Ancillaries start
Main engine can be used

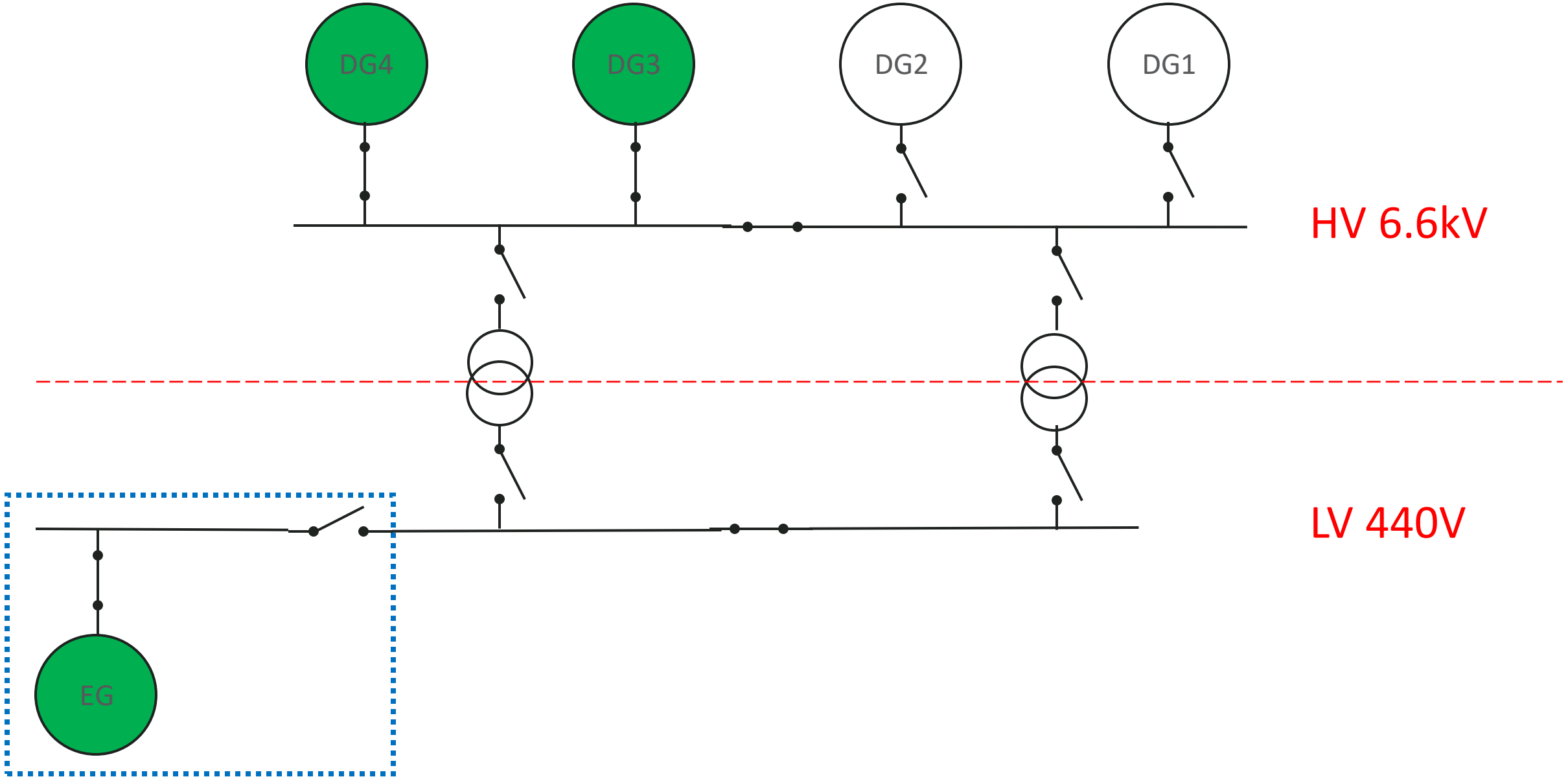

Main Switchboard
PMS Power
Port
Stb
3640 kW Connected 3640 kW
680 kW Consumed 680 kW
2960 kW Available 2960 kW
DG1
0 Hz
0 kW
1 V
0 A
Red.Module Fault
GPA Fault
Br Tripped
DG2
60 Hz
680 kW
6698 V
58 A
DG3
DG4
60 Hz
6726 V
6742 V
HPU1
HPU2
HPU3
HPU4
T5
T6
T3
T1
T2
T4
VSD
Changeover
ST4
MT5
AZ3
BT1
BT2
MT6
0 kW
452 V
460 V
690V Grane
Insulation
450V Grane/ROV
Em SWB 450V
450V
6.6 kV Bustie
Voltage L
Voltage H
Freq L
Freq H
General Fault
M.Panel Alarm
Buff Fault
T9
EG
T10
T7
T8
1 A
Shoreconnection
OverCurr
ShutD
Alarm
Stby
450V ROV
Emergency SWB 230V
245 V
247 V
230V
0 V
110V SWBD

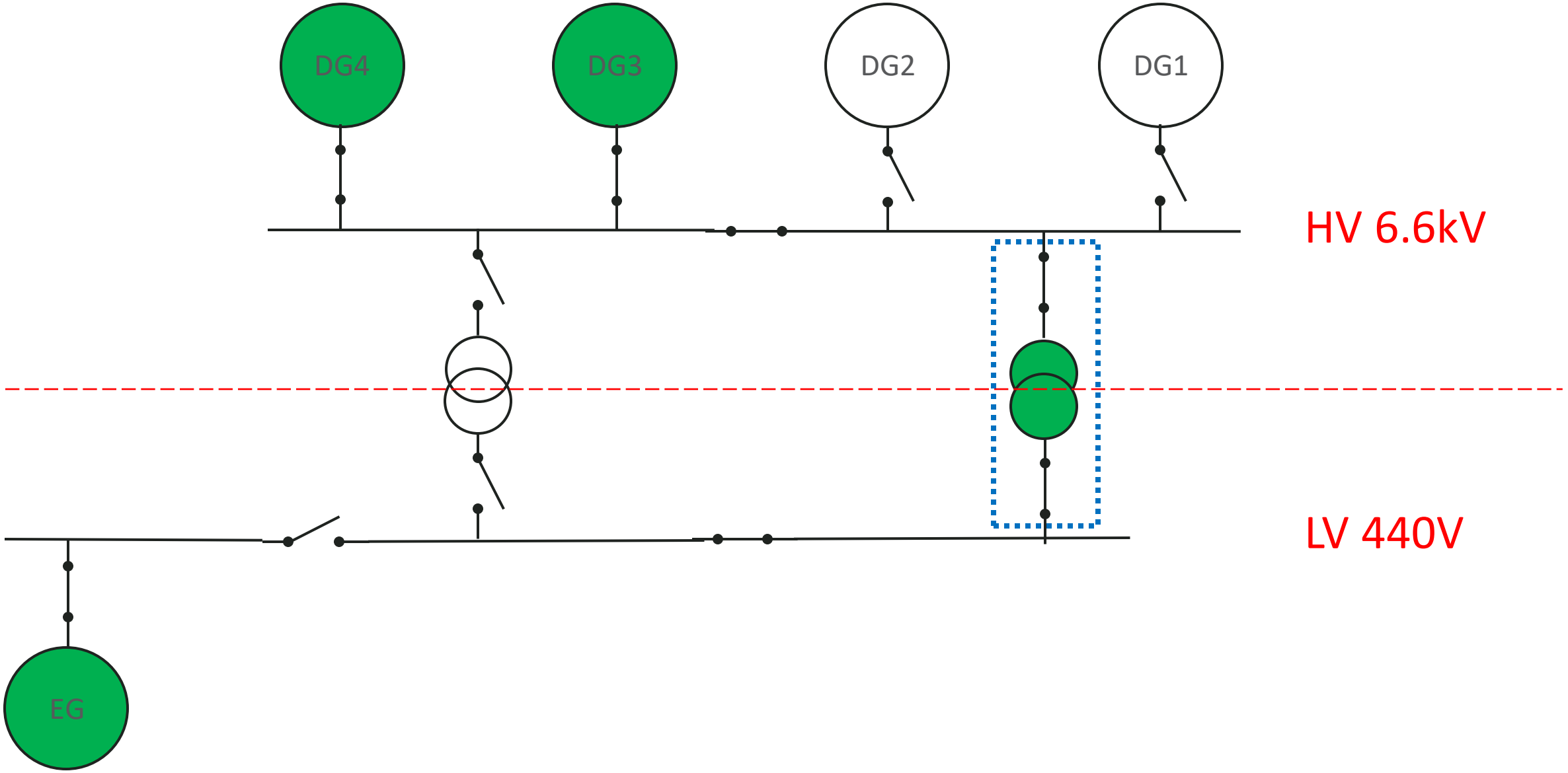


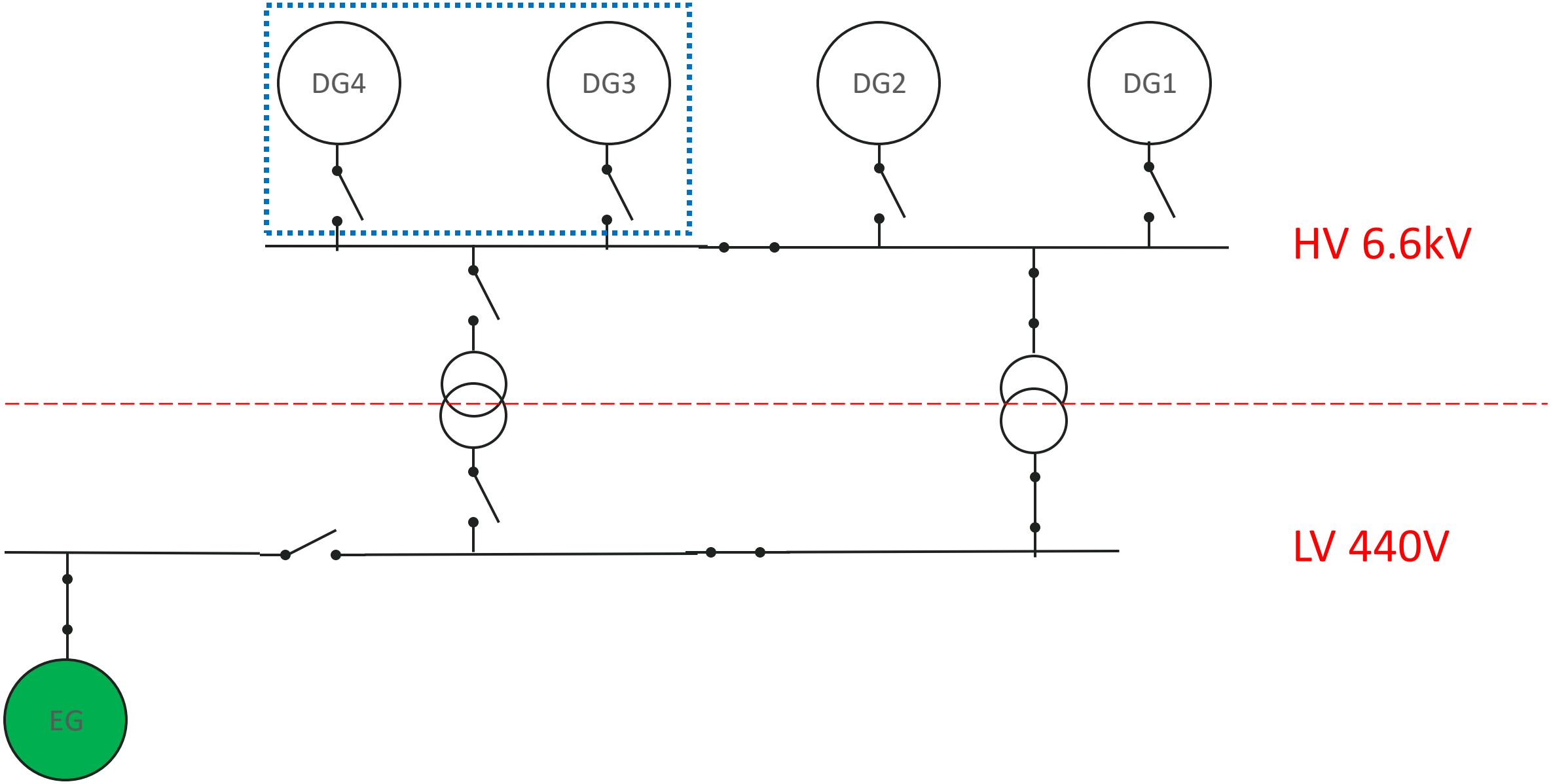
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

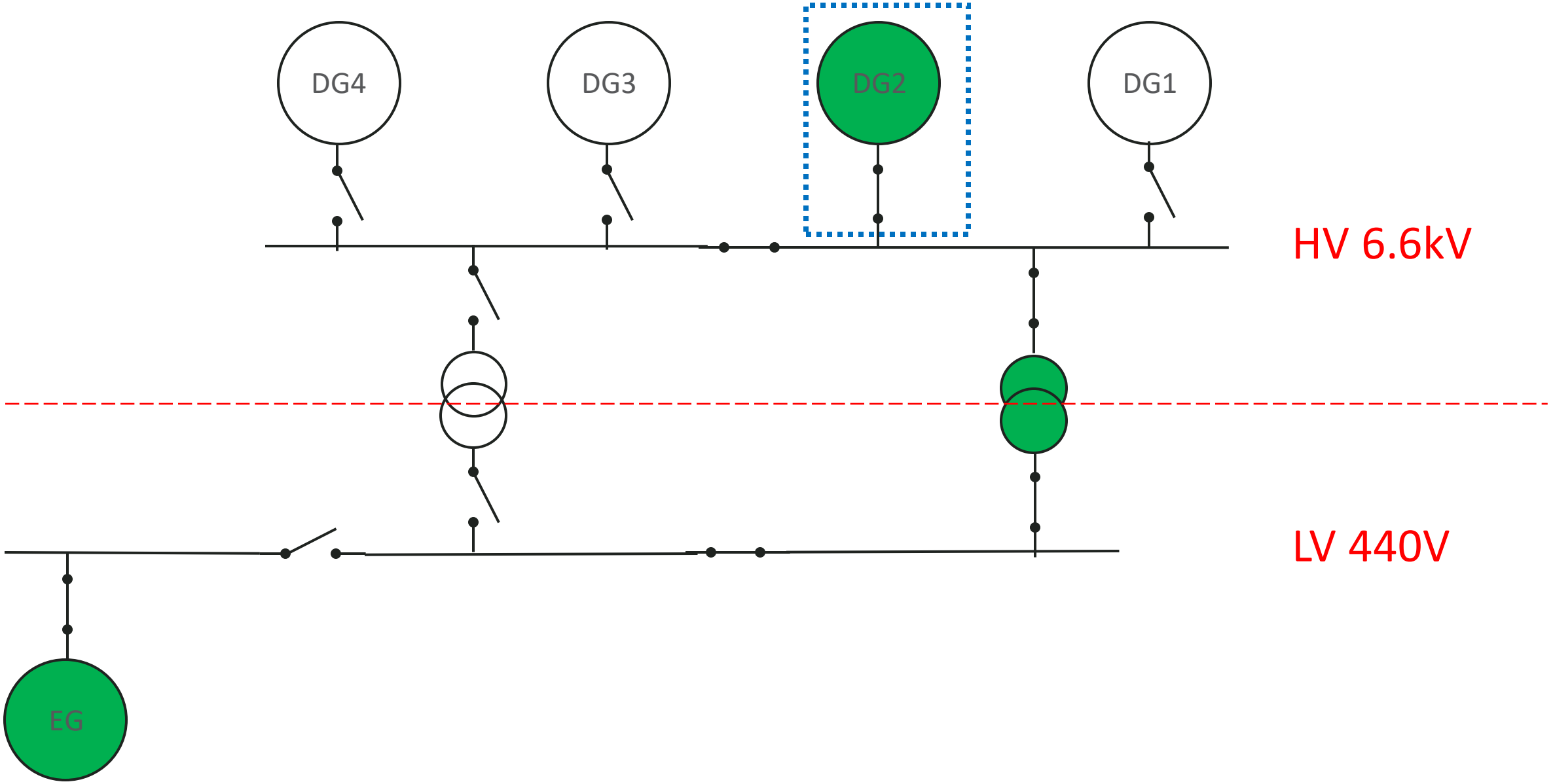

DG4
DG3
DG2
DG1
HV 6.6kV
LV 440V
EG


DG4
DG3
DG2
DG1
HV 6.6kV
LV 440V
EG


DG4
DG3
DG2
DG1
HV 6.6kV
LV 440V
EG


DG4
DG3
DG2
DG1
HV 6.6kV
LV 440V
EG


DG4
DG3
DG2
DG1
HV 6.6kV
LV 440V
EG

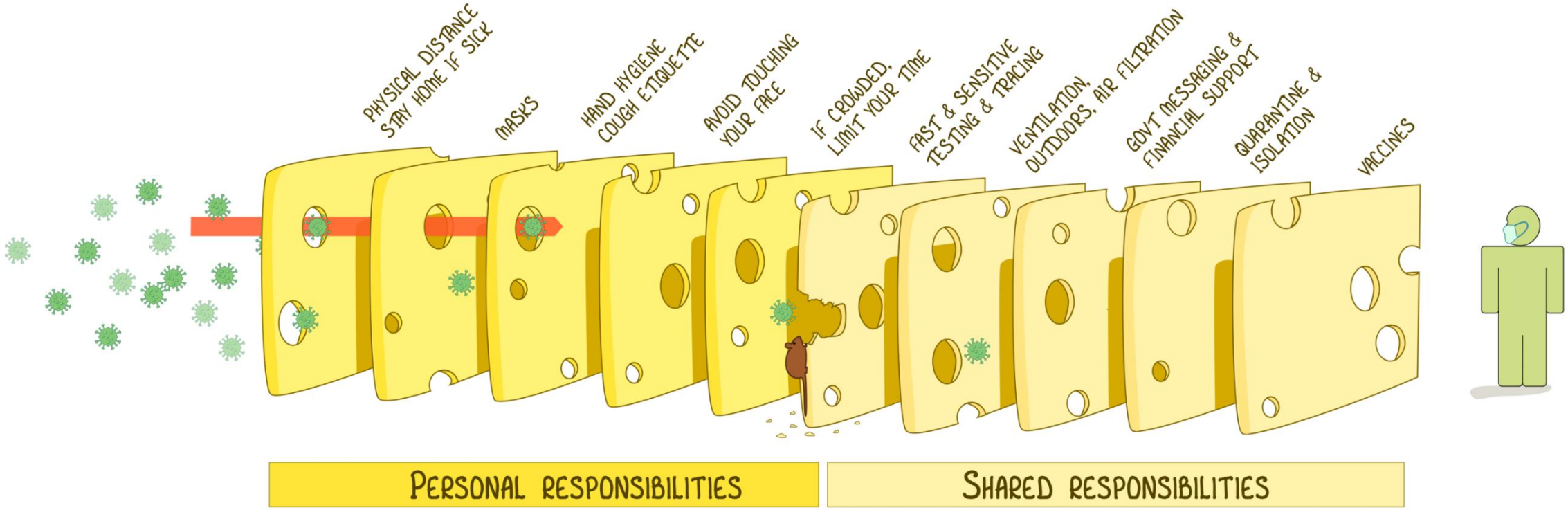

DG4
DG3
DG2
DG1
HV 6.6kV
LV 440V
EG

MV Dali Recovery

Transformer trips – blackout 1
Emergency generator starts
Transformer manually restored
Both generators trip – blackout 2
Standby generator starts
Ancillaries start
~~Main engine can be used~~

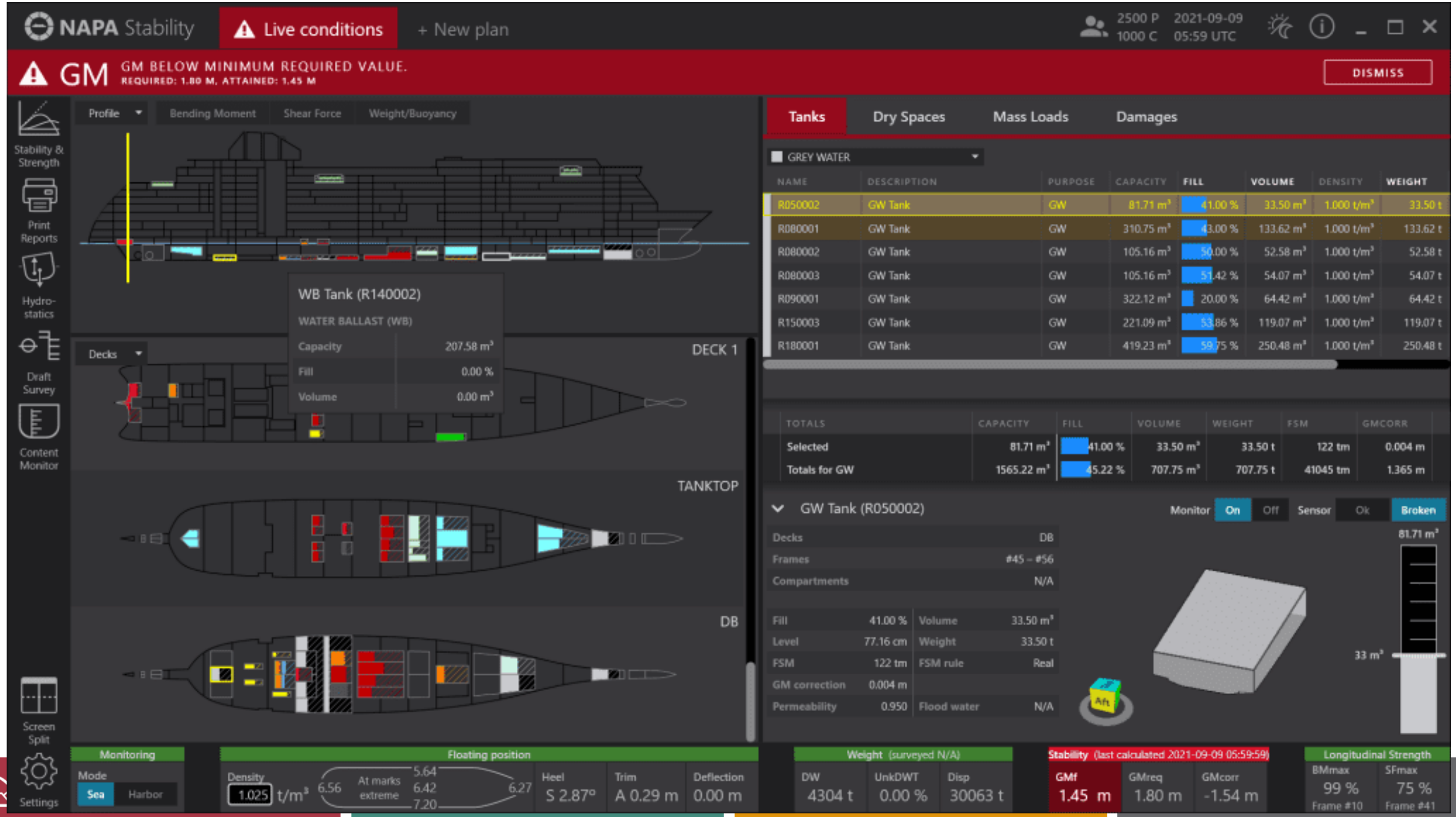
The Swiss Cheese Respiratory Virus Pandemic Defence

Recognising that no single intervention is perfect at preventing spread



Each intervention (layer) has imperfections (holes).
Multiple layers improve success.

Ian M Mackay
virologydownunder.com
With thanks to Jody Lanard, Katherine Arden & the Uni of Qld
Based on the Swiss cheese model of accident causation, by James T Reason, 1990
version 3.0
update: 24oct2020


NAPA Stability
Live conditions
+ New plan
2500 P 2021-09-09
1000 C 05:59 UTC
GM
GM BELOW MINIMUM REQUIRED VALUE.
REQUIRED: 1.80 M, ATTAINED: 1.45 M
DISMISS
Stability & Strength
Print Reports
Hydro-statics
Draft Survey
Content Monitor
Screen Split
Settings
Profile
Bending Moment
Shear Force
Weight/Buoyancy
WB Tank (R140002)
WATER BALLAST (WB)
Capacity 207.58 m³
Fill 0.00 %
Volume 0.00 m³
Decks
DECK 1
TANKTOP
DB
Tanks
Dry Spaces
Mass Loads
Damages
GREY WATER
NAME DESCRIPTION PURPOSE CAPACITY FILL VOLUME DENSITY WEIGHT
R050002 GW Tank GW 81.71 m³ 41.00 % 33.50 m³ 1.000 t/m³ 33.50 t
R080001 GW Tank GW 310.75 m³ 43.00 % 133.62 m³ 1.000 t/m³ 133.62 t
R080002 GW Tank GW 105.16 m³ 50.00 % 52.58 m³ 1.000 t/m³ 52.58 t
R080003 GW Tank GW 105.16 m³ 51.42 % 54.07 m³ 1.000 t/m³ 54.07 t
R090001 GW Tank GW 322.12 m³ 20.00 % 64.42 m³ 1.000 t/m³ 64.42 t
R150003 GW Tank GW 221.09 m³ 53.86 % 119.07 m³ 1.000 t/m³ 119.07 t
R180001 GW Tank GW 419.23 m³ 59.75 % 250.48 m³ 1.000 t/m³ 250.48 t
TOTALS CAPACITY FILL VOLUME WEIGHT FSM GMCORR
Selected 81.71 m³ 41.00 % 33.50 m³ 33.50 t 122 tm 0.004 m
Totals for GW 1565.22 m³ 45.22 % 707.75 m³ 707.75 t 41045 tm 1.365 m
GW Tank (R050002)
Monitor On Off Sensor Ok Broken
Decks DB
Frames #45 – #56
Compartments N/A
Fill 41.00 % Volume 33.50 m³
Level 77.16 cm Weight 33.50 t
FSM 122 tm FSM rule Real
GM correction 0.004 m
Permeability 0.950 Flood water N/A
81.71 m³
33 m³
Aft
Monitoring
Mode Sea Harbor
Floating position
Density 1.025 t/m³
6.56 At marks extreme 5.64 6.42 7.20 6.27
Heel S 2.87°
Trim A 0.29 m
Deflection 0.00 m
Weight (surveyed N/A)
DW 4304 t
UnkDWT 0.00 %
Disp 30063 t
Stability (last calculated 2021-09-09 05:59:59)
GMf 1.45 m
GMreq 1.80 m
GMcorr -1.54 m
Longitudinal Strength
BMmax 99 % Frame #10
SFmax 75 % Frame #41

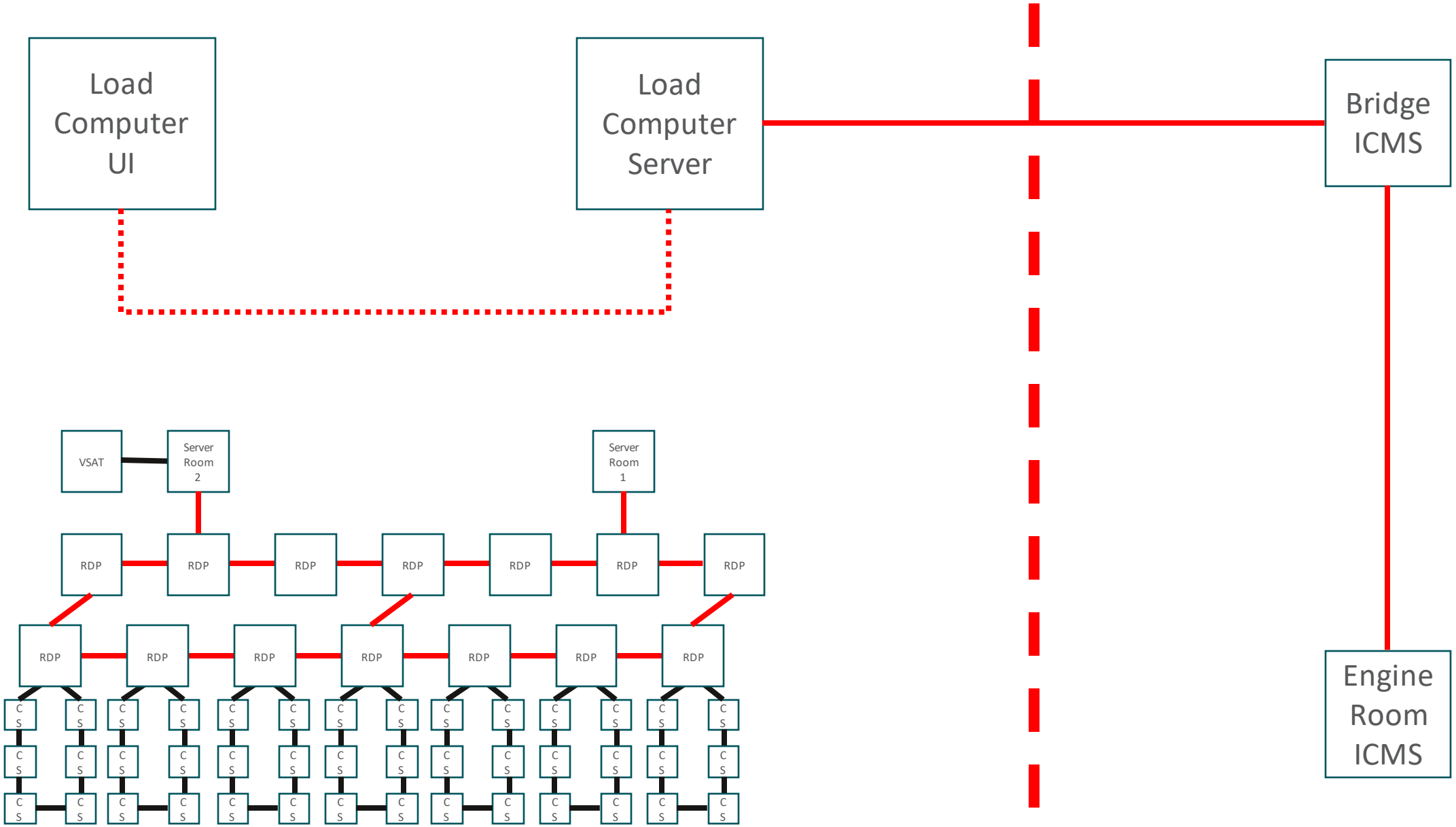
Integrated Control and Monitoring System

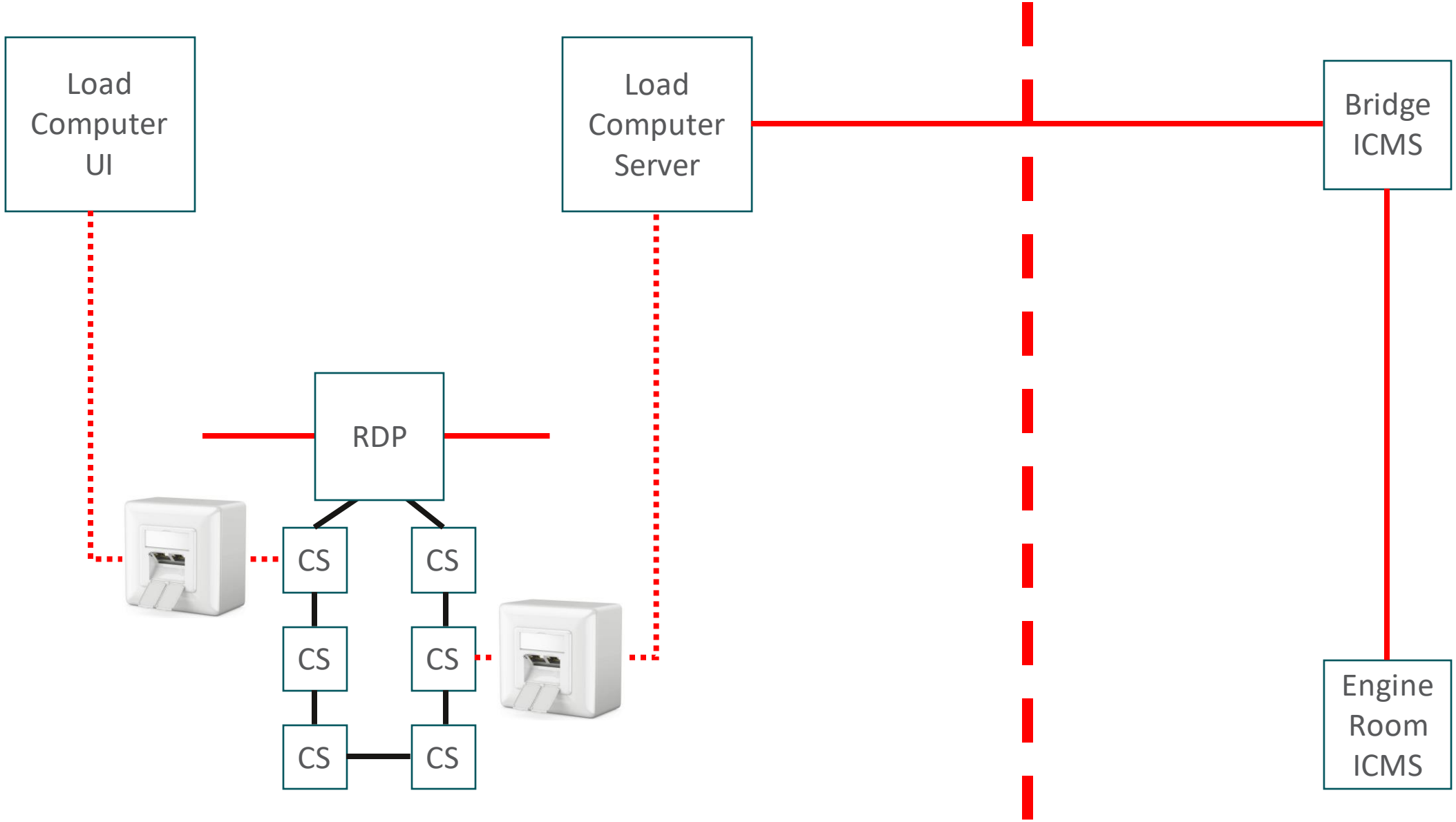
info@pentestpartners.com

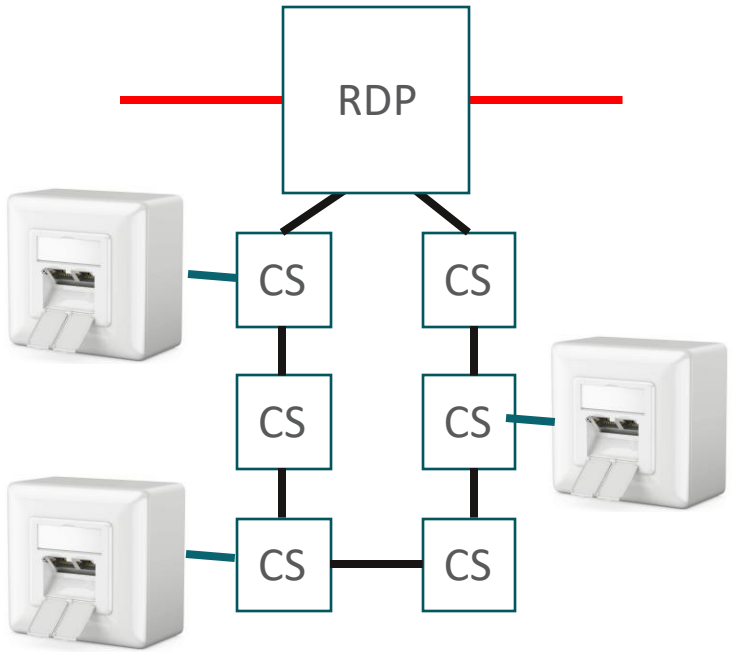
+44 (0)20 3095 0500

@PenTestPartners

PenTestPartnersLLP

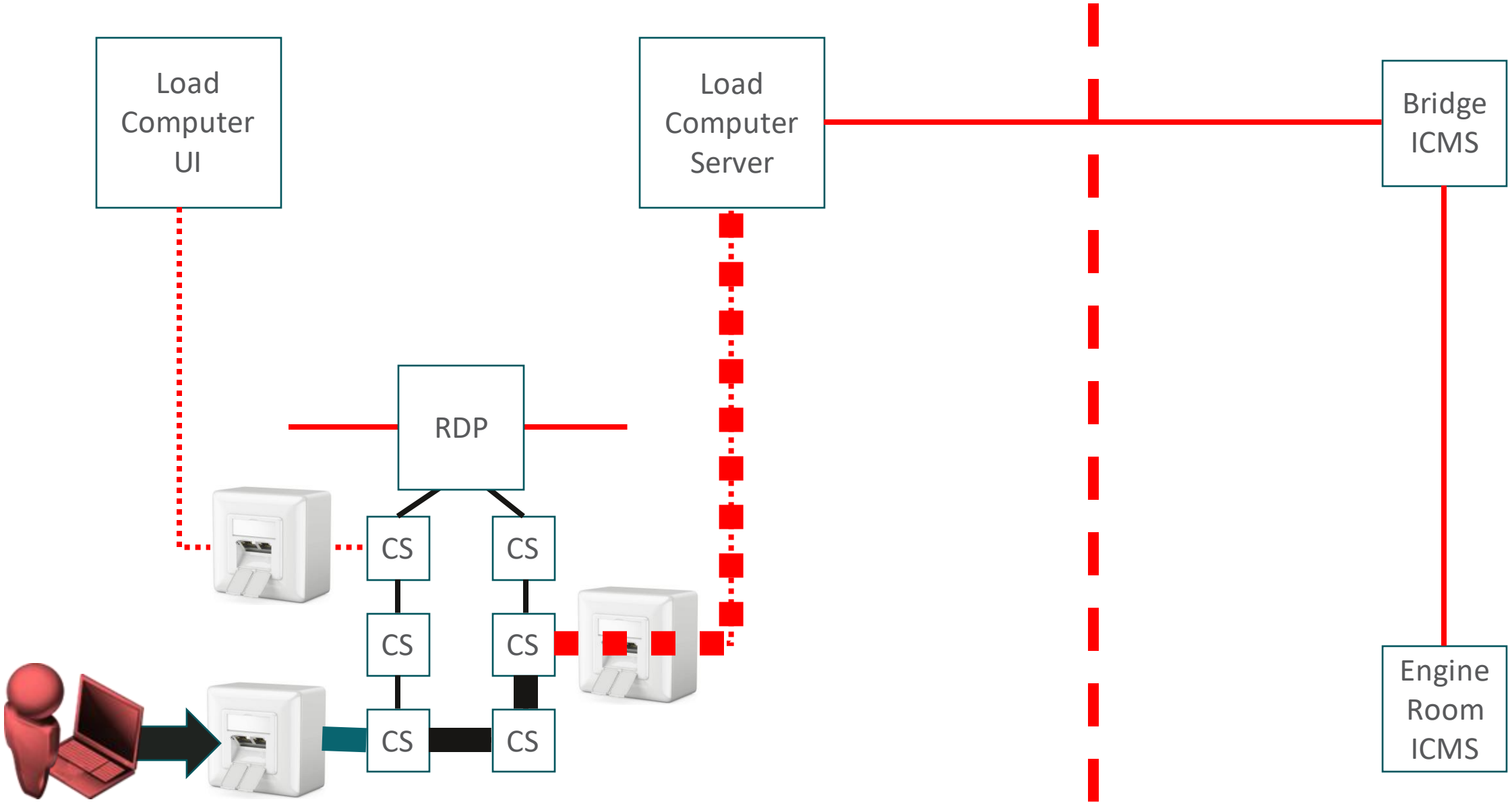

Load Computer UI
Load Computer Server
Bridge ICMS
Engine Room ICMS
VSAT
Server Room 2
Server Room 1
RDP
CS


Load Computer UI
Load Computer Server
Bridge ICMS
RDP
CS
CS
CS
CS
CS
CS
Engine Room ICMS



Unassigned wall-ports need 802.1x

Or you go into the tar pit!

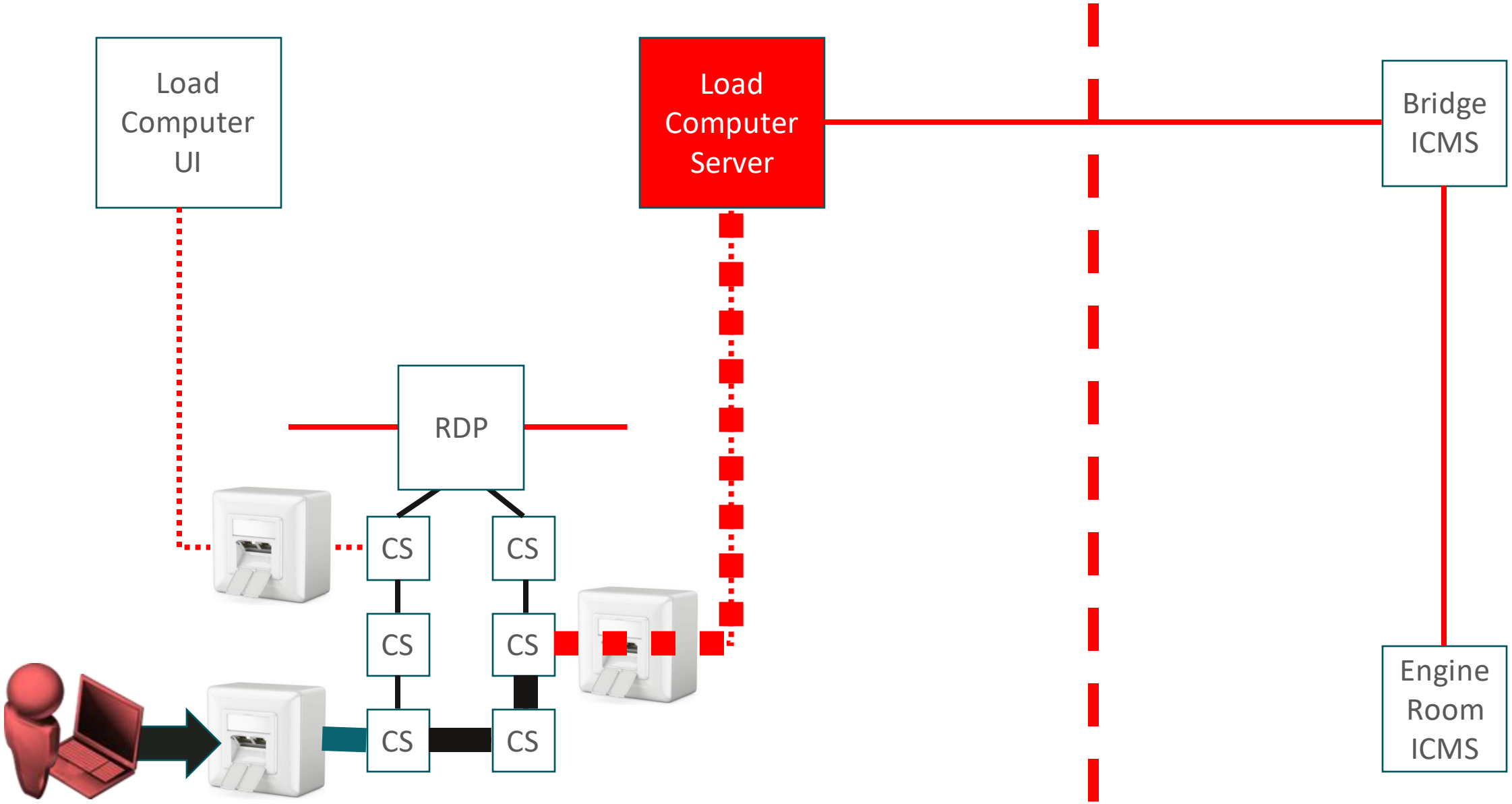

Load Computer UI
Load Computer Server
Bridge ICMS
RDP
CS
CS
CS
CS
CS
CS
Engine Room ICMS

[redacted] - Notepad

File Edit Format View Help

Windows Registry Editor Versior

[HKEY_LOCAL_MACHINE\software\mi
"AutoAdminLogon"="1"
"DefaultUserName"=[redacted]
"DefaultPassword"=[redacted]


Load Computer UI
Load Computer Server
Bridge ICMS
RDP
CS
CS
CS
CS
CS
CS
Engine Room ICMS

Published March 2024

REPORT MARINE 2024/05

Loss of propulsion and near grounding of Viking Sky, Hustadvika, Norway 23 March 2019

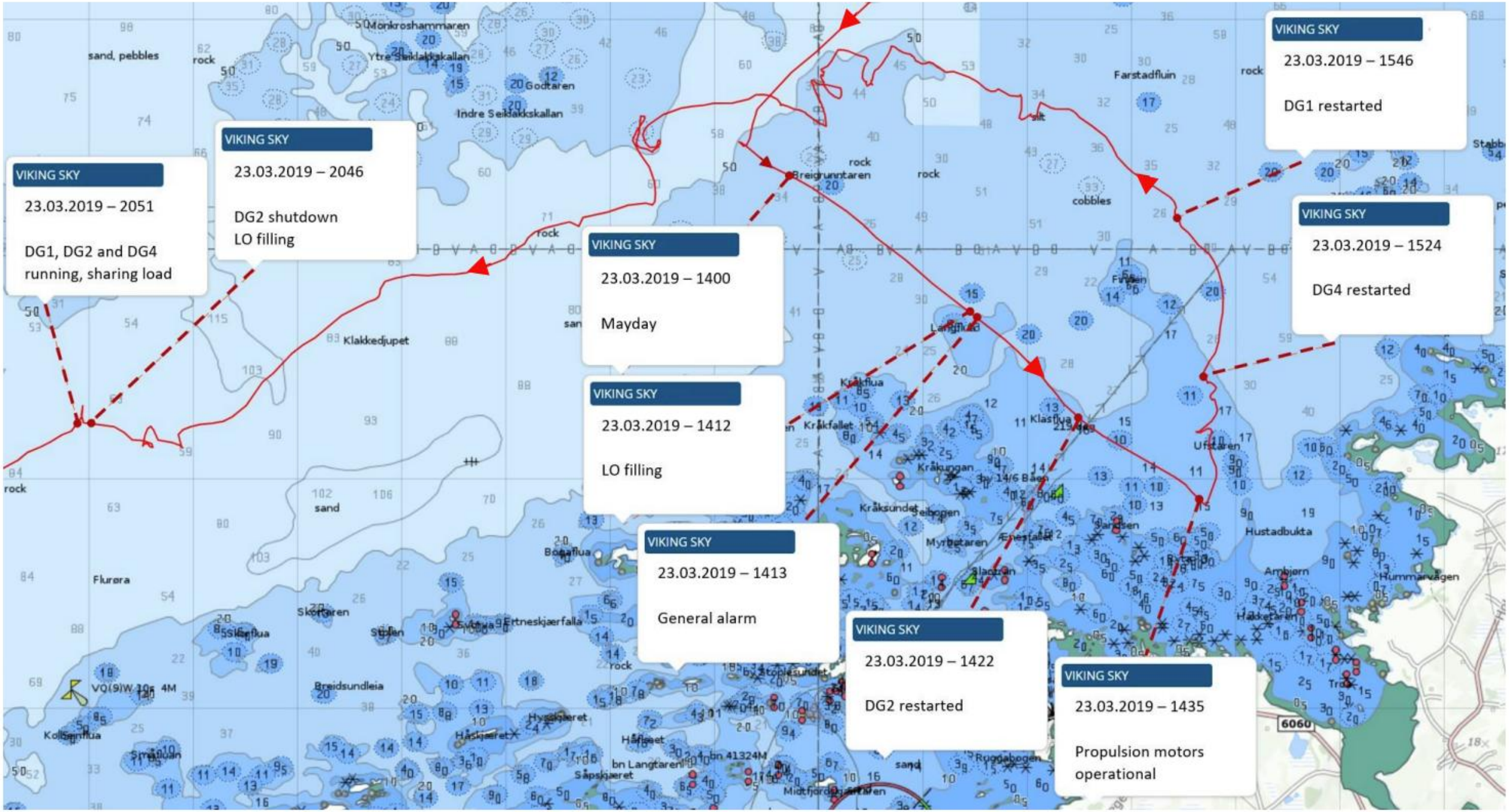


Figure 15: Events during restoration of power. Source: The Norwegian Coastal Administration AIS / NSIA

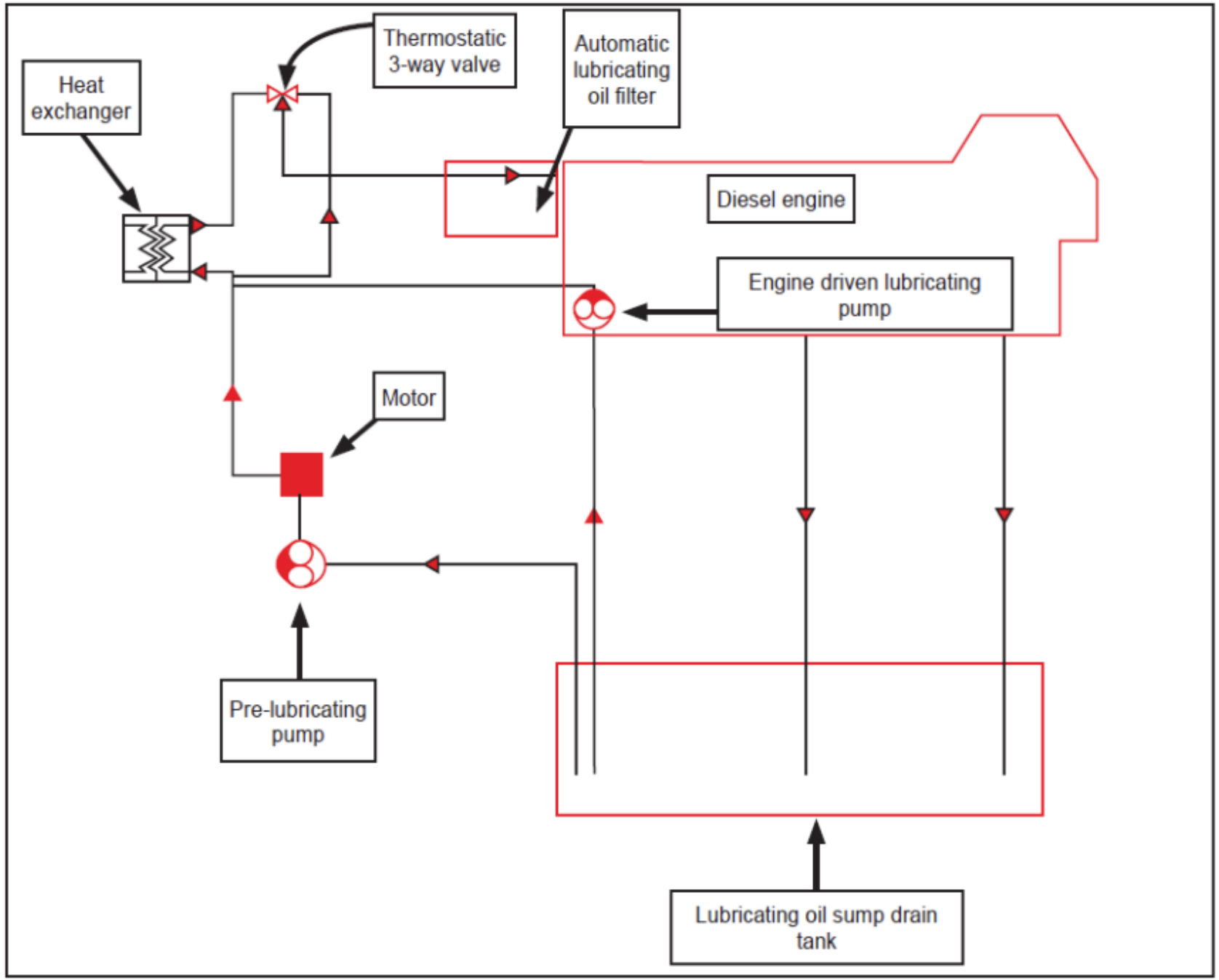


Figure 30: Schematic drawing of the diesel generator lubricating oil system. Illustration: NSIA

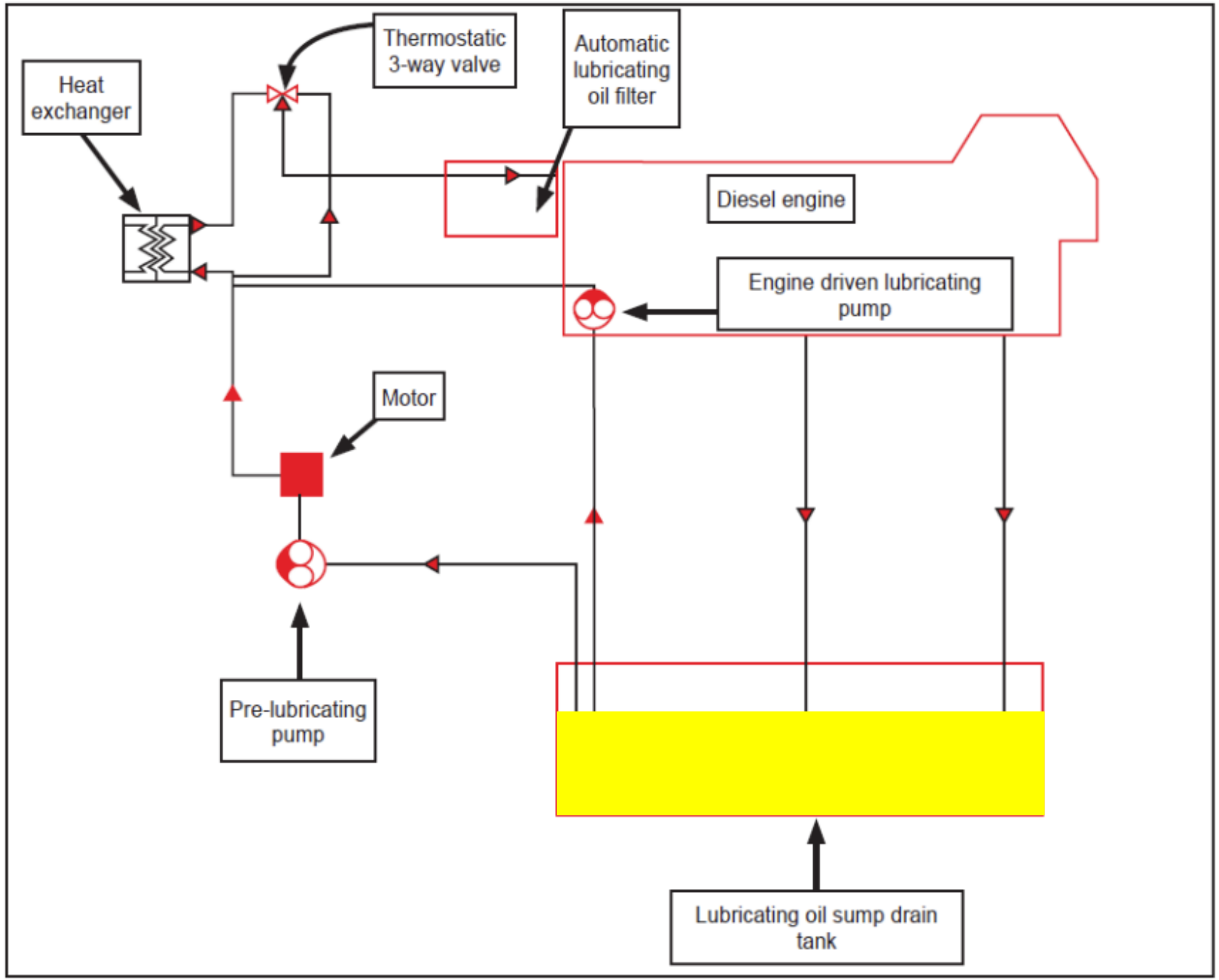


Figure 30: Schematic drawing of the diesel generator lubricating oil system. Illustration: NSIA

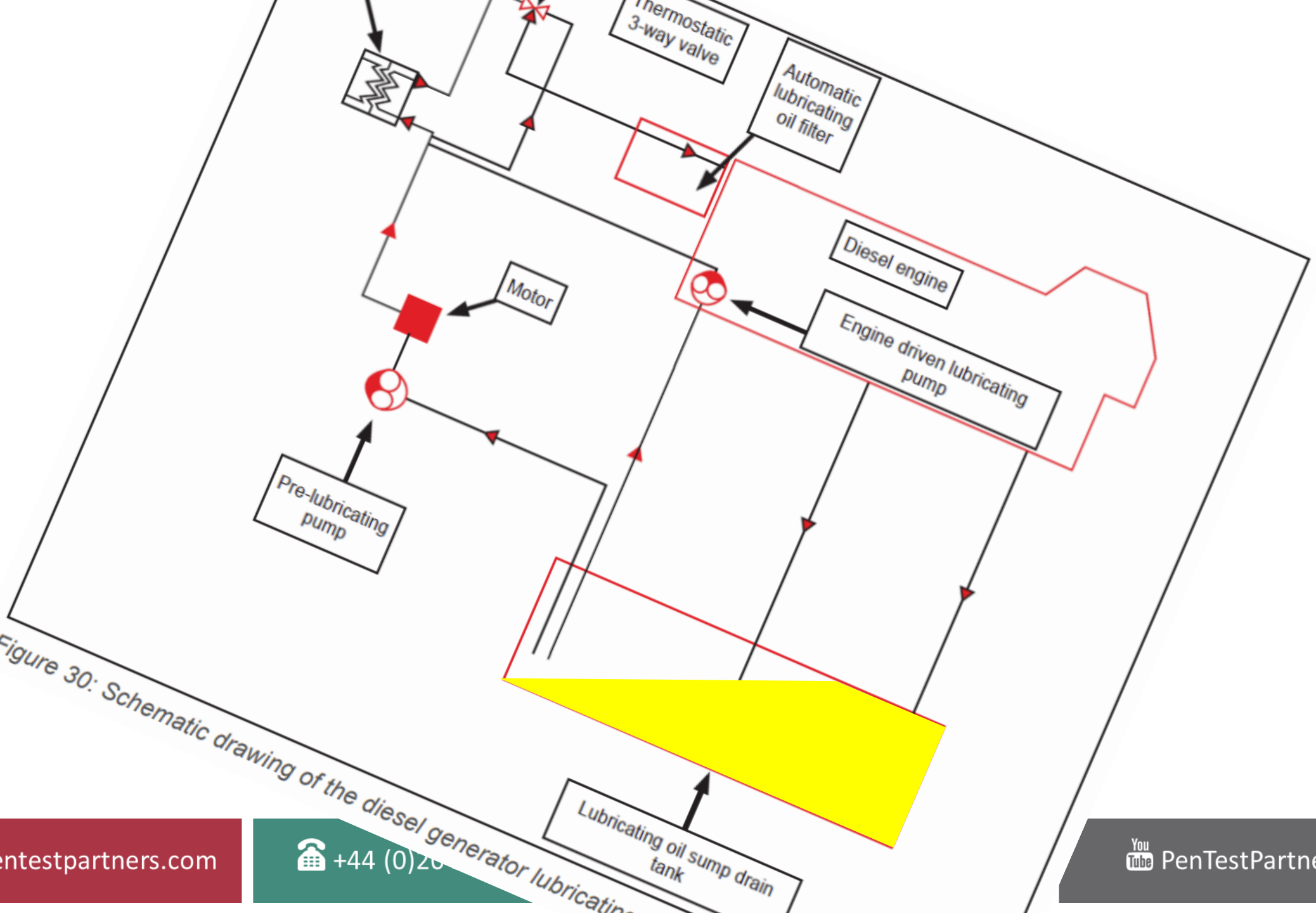
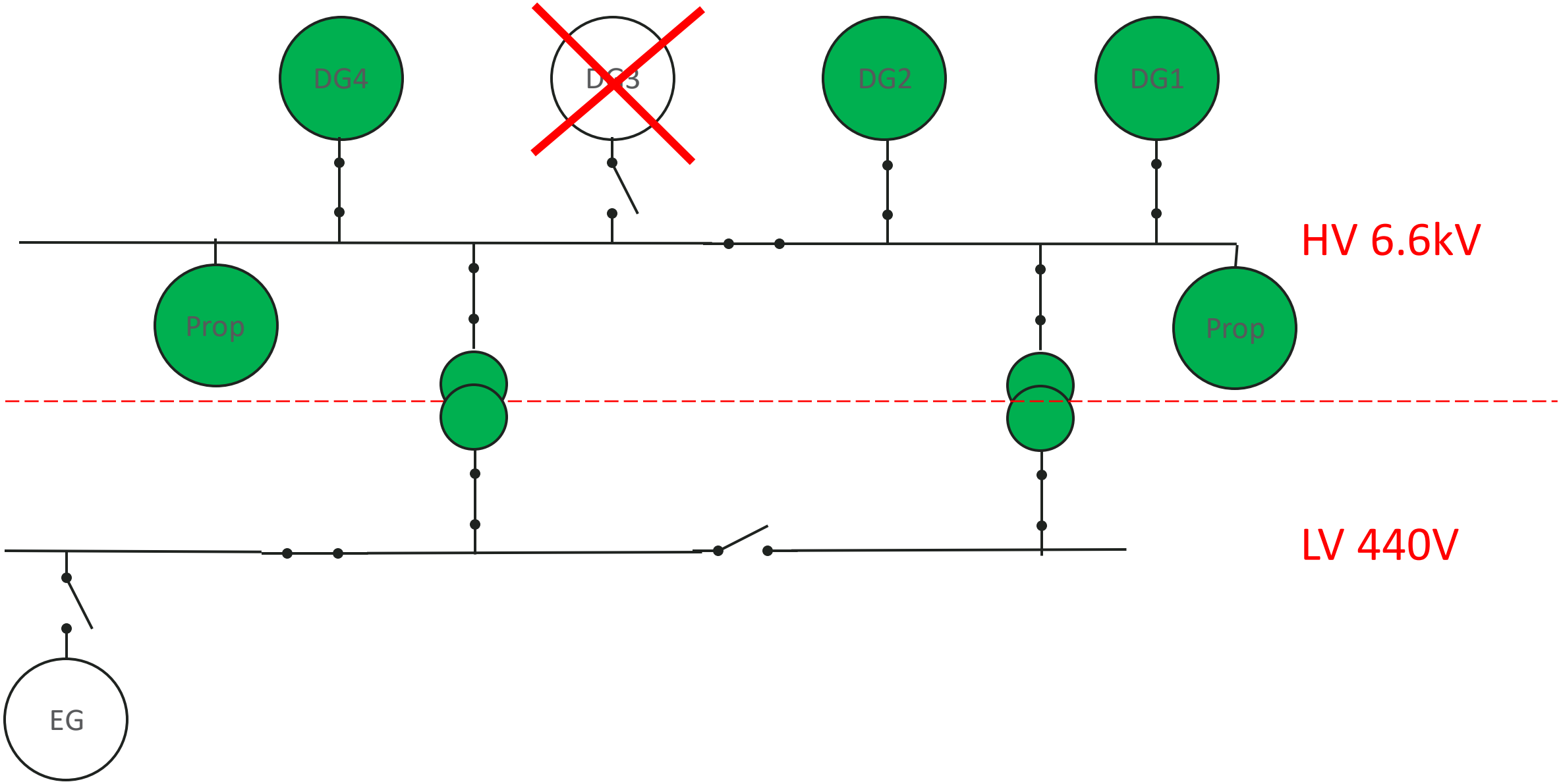
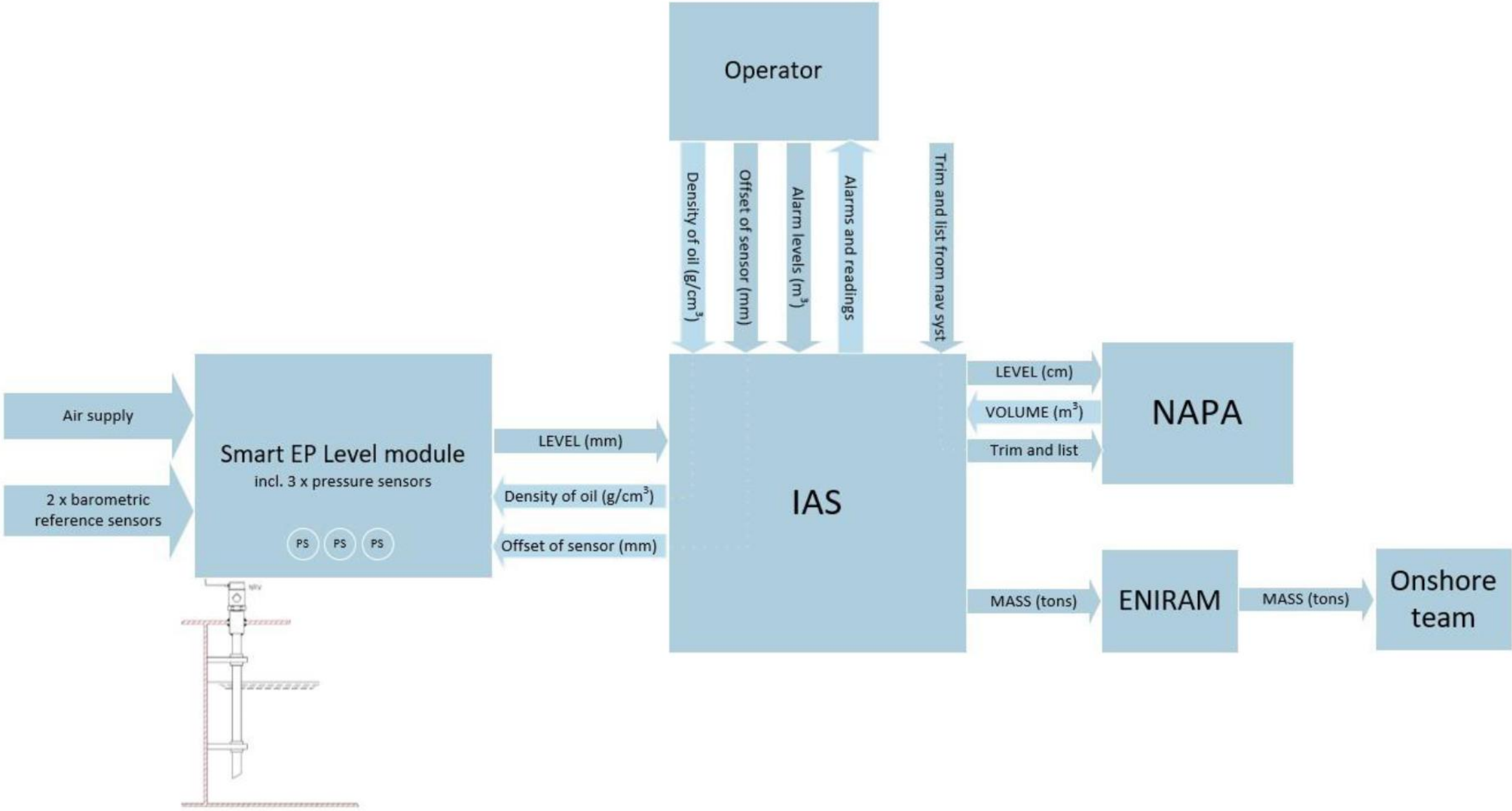
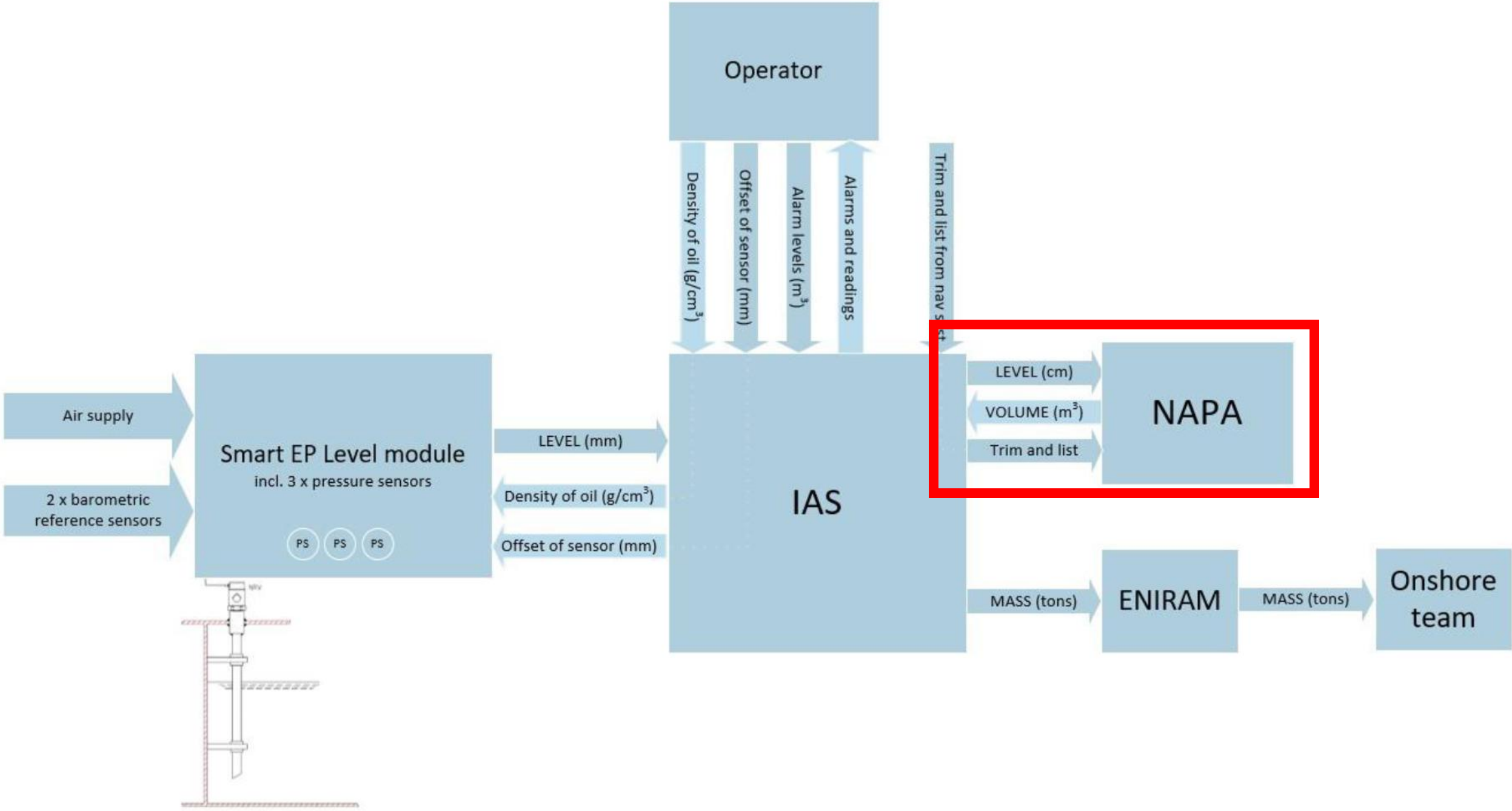
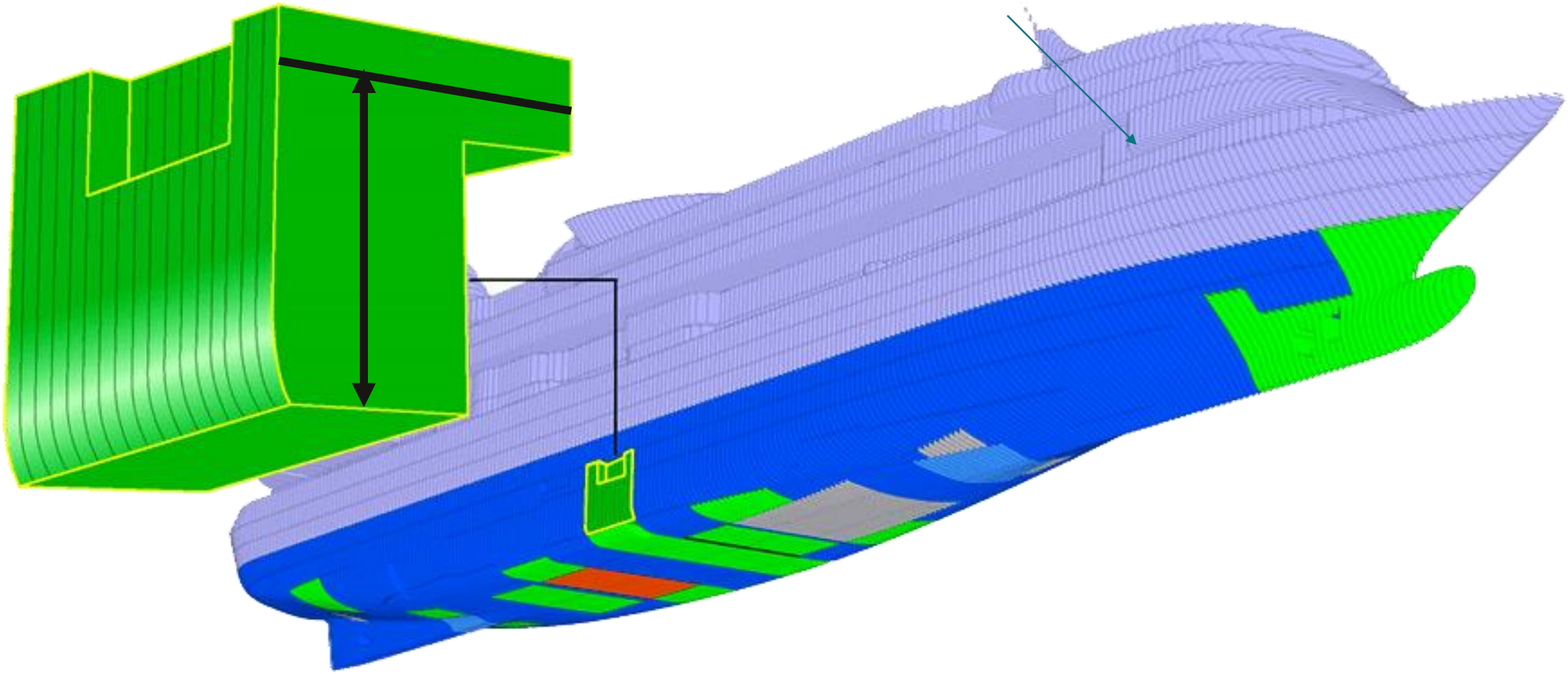


Figure 30: Schematic drawing of the diesel generator lubricatin


DG4
DG3
DG2
DG1
HV 6.6kV
Prop
Prop
LV 440V
EG


Operator
Density of oil (g/cm³)
Offset of sensor (mm)
Alarm levels (m³)
Alarms and readings
Trim and list from nav syst
Air supply
2 x barometric reference sensors
Smart EP Level module
incl. 3 x pressure sensors
PS
PS
PS
LEVEL (mm)
Density of oil (g/cm³)
Offset of sensor (mm)
IAS
LEVEL (cm)
VOLUME (m³)
Trim and list
NAPA
MASS (tons)
ENIRAM
MASS (tons)
Onshore team

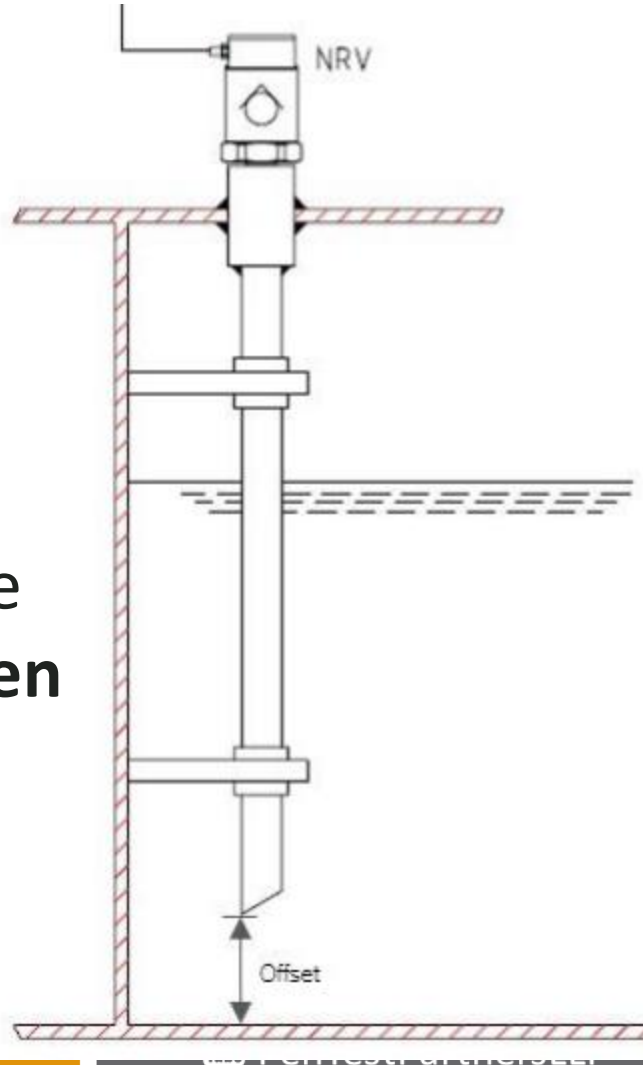

Operator
Density of oil (g/cm³)
Offset of sensor (mm)
Alarm levels (m³)
Alarms and readings
Trim and list from nav s
Air supply
2 x barometric reference sensors
Smart EP Level module
incl. 3 x pressure sensors
PS
PS
PS
LEVEL (mm)
Density of oil (g/cm³)
Offset of sensor (mm)
IAS
LEVEL (cm)
VOLUME (m³)
Trim and list
NAPA
MASS (tons)
ENIRAM
MASS (tons)
Onshore team

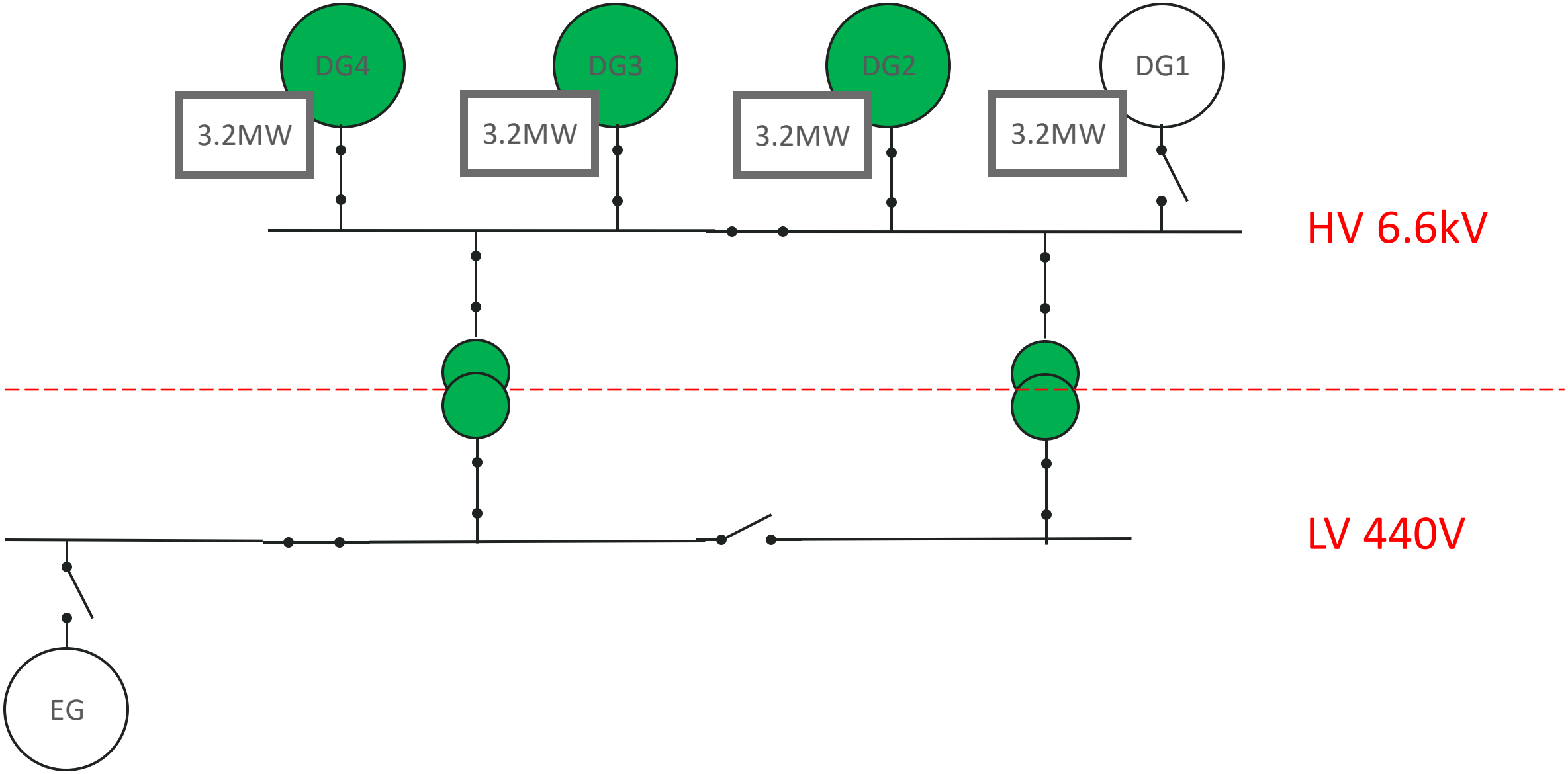


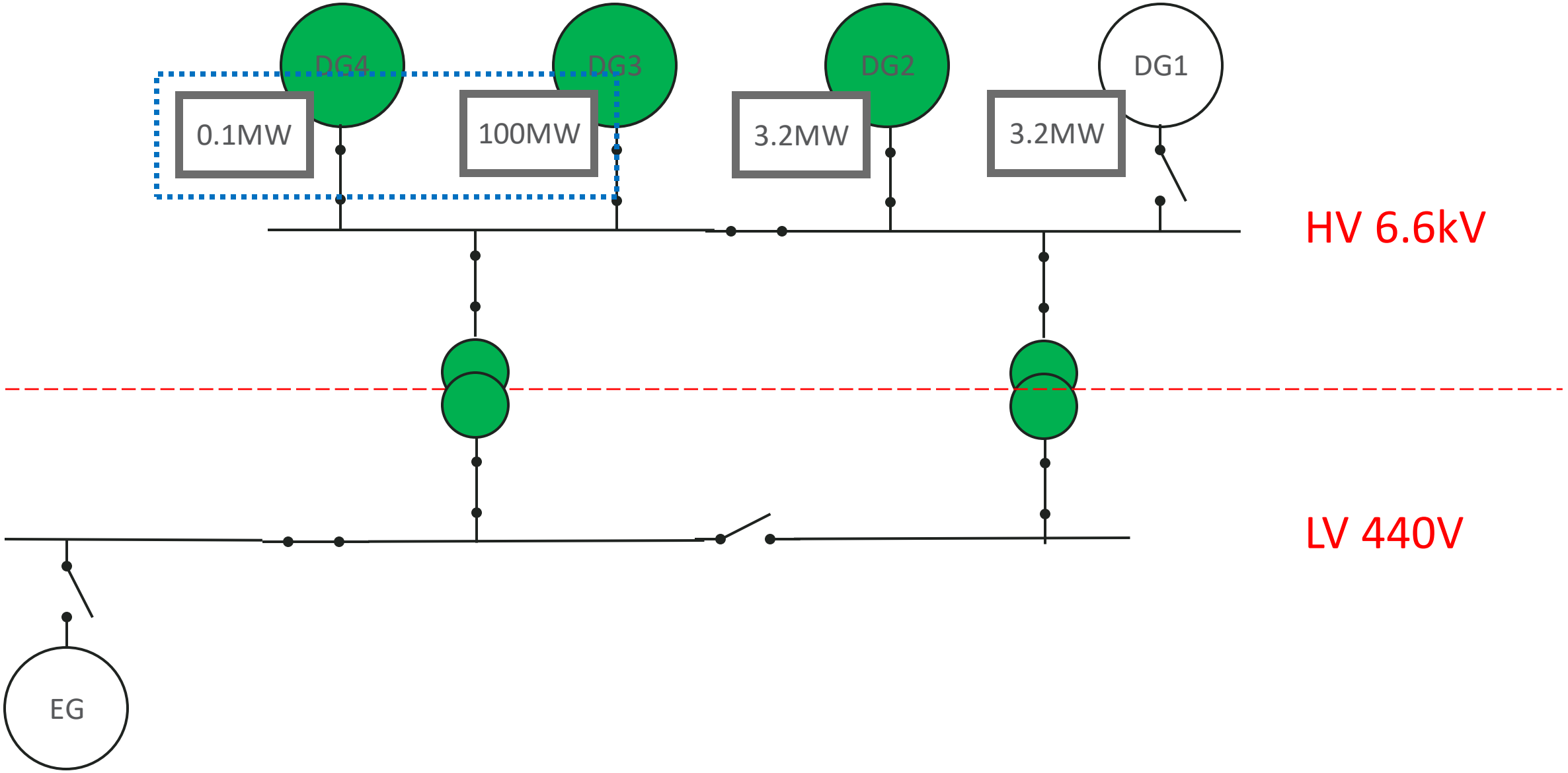
The following operator inputs were required for remote monitoring of the sump tanks:

- Offset of the sensor tube (mm)
- Density of the oil (g/cm3)
- Alarm levels (m3)

These values could be adjusted in the IAS by any of the engineers, with **no means of identifying what had been changed, by whom, when or why**.




DG4
DG3
DG2
DG1
3.2MW
3.2MW
3.2MW
3.2MW
HV 6.6kV
LV 440V
EG


DG4
DG3
DG2
DG1
0.1MW
100MW
3.2MW
3.2MW
HV 6.6kV
LV 440V
EG

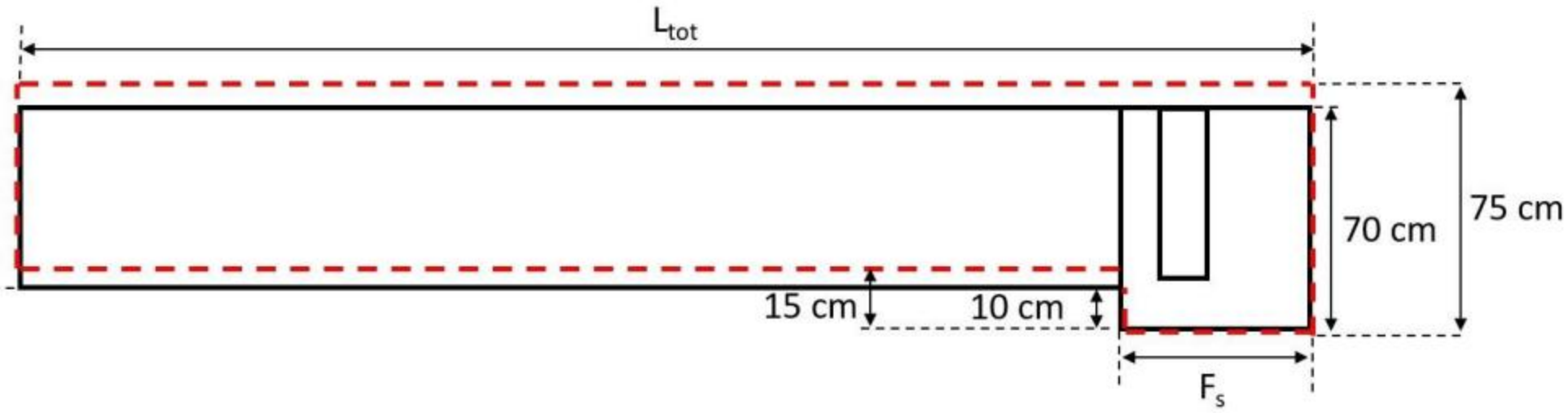
The installation of the sensor system in the lube oil sump tank is shown. In addition to the external air supply, the module requires input from **two barometric reference sensors** for measurement correction.

There were approximately 150 audible alarms in total. 88 were tank level warnings that returned to normal condition within 2 minutes. These warnings were likely caused by a short term pressure fluctuation at one of the barometric reference sensors.

It was identified that the aft draft sensor was sending erroneous readings to NAPA. This was affecting the level correction done by NAPA and thus also led to wrong volume calculations.

The investigation has identified that there was an error in the 3D model geometry. This caused an error in the calculations.

The volume calculation will return a value 568 litres less than the actual oil volume.



The remote tank level monitoring system was complex, and the measurements were inaccurate and unreliable. The crew had gradually lost confidence in the remote monitoring system.

The investigation has found that the fleet of Viking cruise vessels was operated for years without the crew or shoreside personnel knowing the correct lube oil sump tank filling levels or alarm setpoints.

Unable to determine lube oil levels

Didn’t know what lube oil levels should be…

Inputs:

NAPA software

3D tank models

Barometric pressure

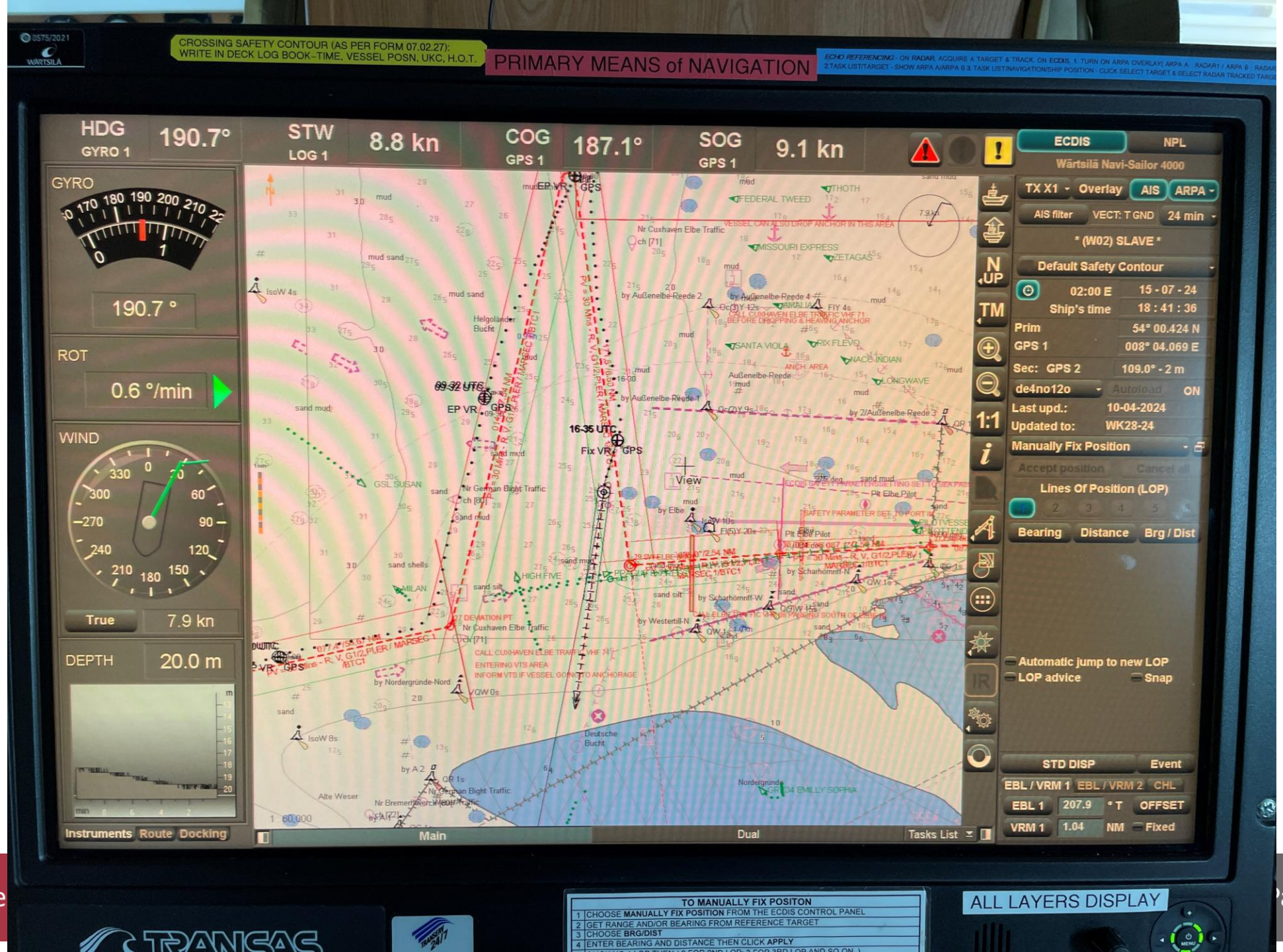
Offset

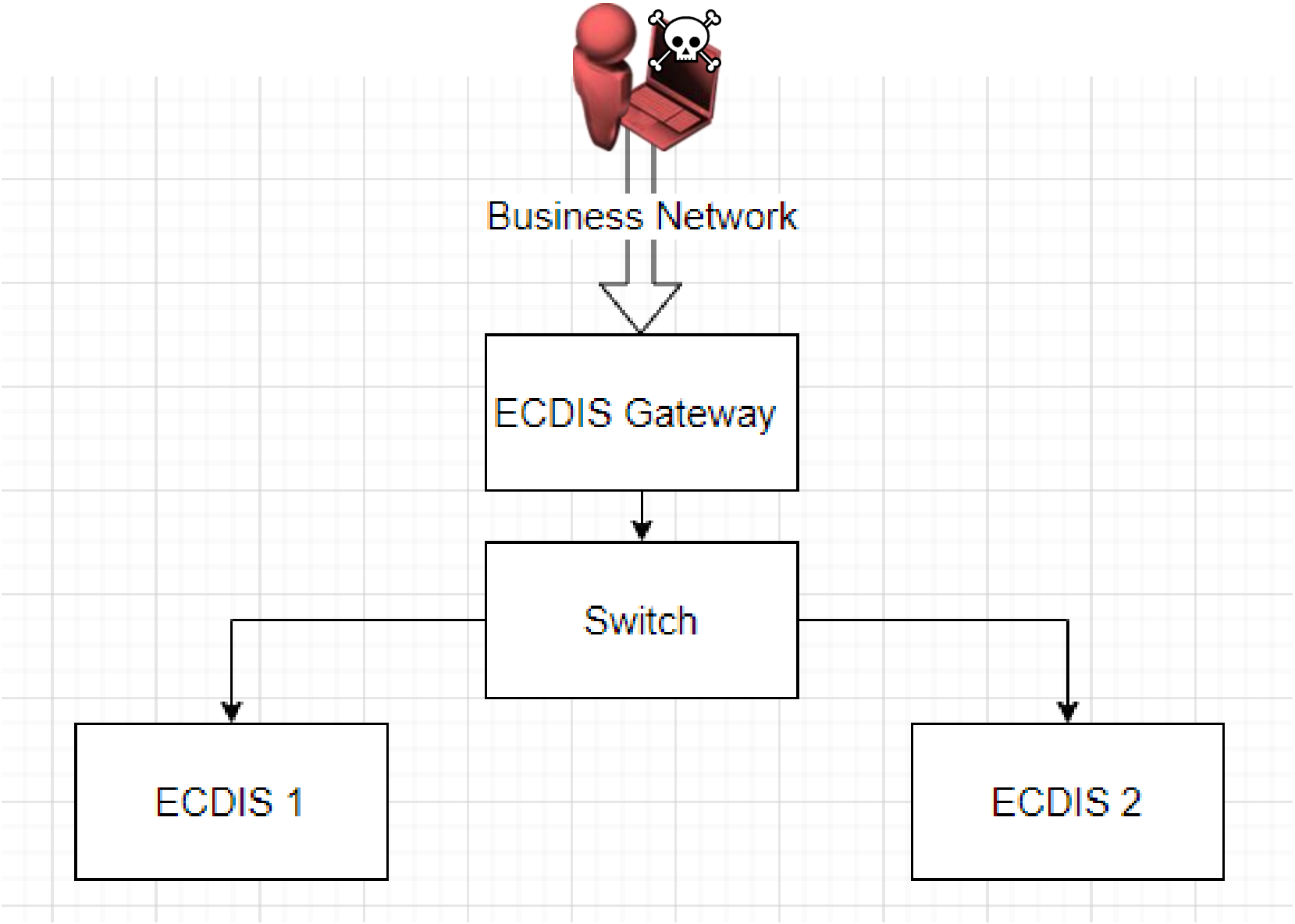
Oil density

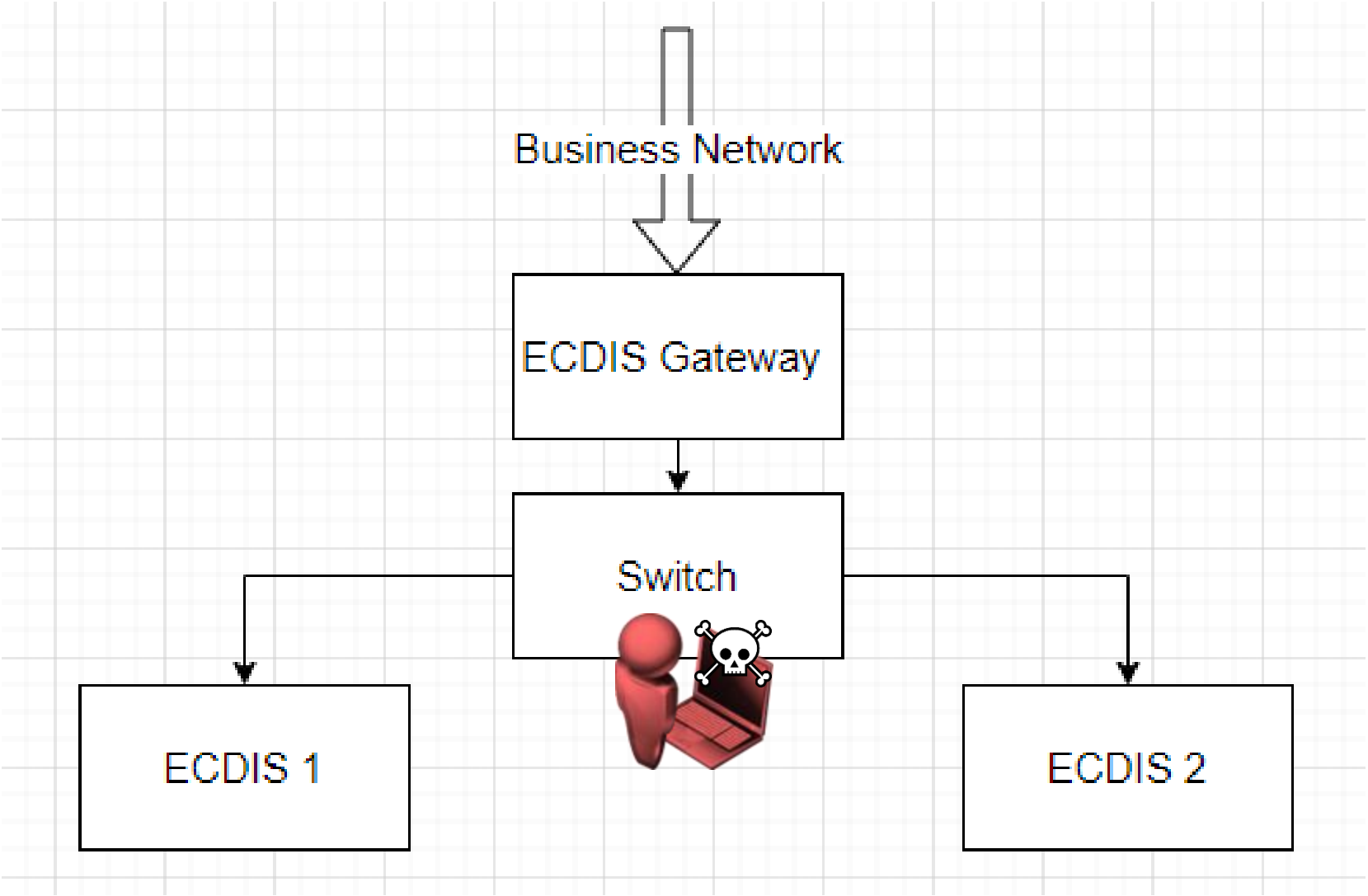
Heel and trim

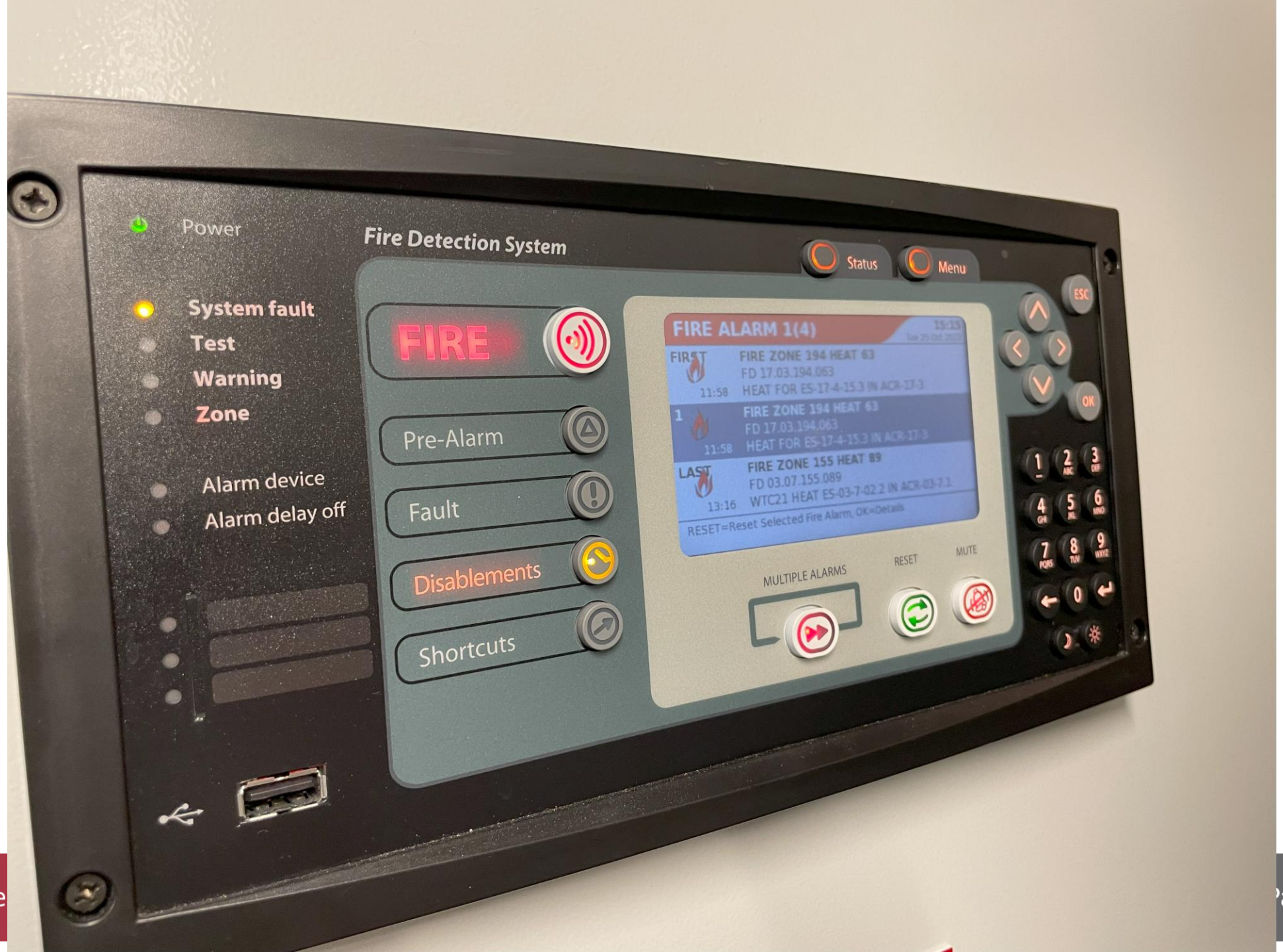
Can the crew of a modern vessel possibly understand exactly how these systems work?


FURUNO
SSAS & LRIT
CURRENT PASSAGE CHARTS
ACTIVE CHARTS


CROSSING SAFETY CONTOUR (AS PER FORM 07.02.27):
WRITE IN DECK LOG BOOK–TIME, VESSEL POSN, UKC, H.O.T.
PRIMARY MEANS of NAVIGATION
HDG GYRO 1 190.7°
STW LOG 1 8.8 kn
COG GPS 1 187.1°
SOG GPS 1 9.1 kn
GYRO
190.7 °
ROT
0.6 °/min
WIND
True 7.9 kn
DEPTH 20.0 m
Instruments Route Docking
Main
Dual
Tasks List
ECDIS NPL
Wärtsilä Navi-Sailor 4000
TX X1 Overlay AIS ARPA
AIS filter VECT: T GND 24 min
* (W02) SLAVE *
Default Safety Contour
02:00 E 15 - 07 - 24
Ship's time 18 : 41 : 36
Prim 54° 00.424 N
GPS 1 008° 04.069 E
Sec: GPS 2 109.0° - 2 m
de4no12o Autoload ON
Last upd.: 10-04-2024
Updated to: WK28-24
Manually Fix Position
Accept position Cancel all
Lines Of Position (LOP)
Bearing Distance Brg / Dist
Automatic jump to new LOP
LOP advice Snap
STD DISP Event
EBL / VRM 1 EBL / VRM 2 CHL
EBL 1 207.9 ° T OFFSET
VRM 1 1.04 NM Fixed
TO MANUALLY FIX POSITON
1 CHOOSE MANUALLY FIX POSITION FROM THE ECDIS CONTROL PANEL
2 GET RANGE AND/OR BEARING FROM REFERENCE TARGET
3 CHOOSE BRG/DIST
4 ENTER BEARING AND DISTANCE THEN CLICK APPLY
ALL LAYERS DISPLAY


Business Network
ECDIS Gateway
Switch
ECDIS 1
ECDIS 2


Business Network
ECDIS Gateway
Switch
ECDIS 1
ECDIS 2


Power
Fire Detection System
Status
Menu
System fault
Test
Warning
Zone
Alarm device
Alarm delay off
FIRE
Pre-Alarm
Fault
Disablements
Shortcuts
FIRE ALARM 1(4)
FIRST
FIRE ZONE 194 HEAT 63
FD 17.03.194.063
11:58
HEAT FOR ES-17-4-15.3 IN ACR-17-3
1
FIRE ZONE 194 HEAT 63
FD 17.03.194.063
11:58
HEAT FOR ES-17-4-15.3 IN ACR-17-3
LAST
FIRE ZONE 155 HEAT 89
FD 03.07.155.089
13:16
WTC21 HEAT ES-03-7-02.2 IN ACR-03-7.1
RESET=Reset Selected Fire Alarm, OK=Details
MULTIPLE ALARMS
RESET
MUTE
ESC
OK

csvload.scr - Notepad

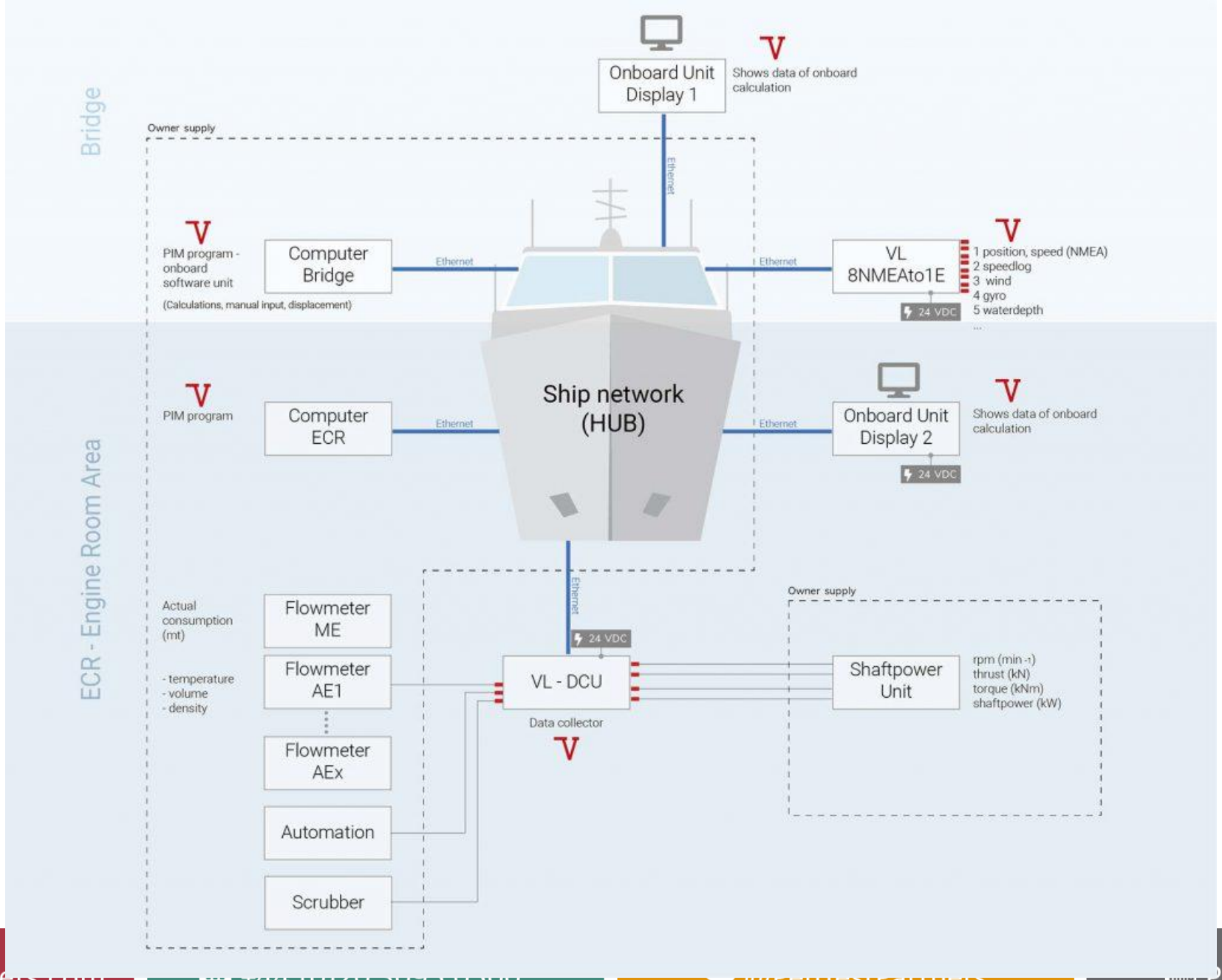
File Edit Format View Help

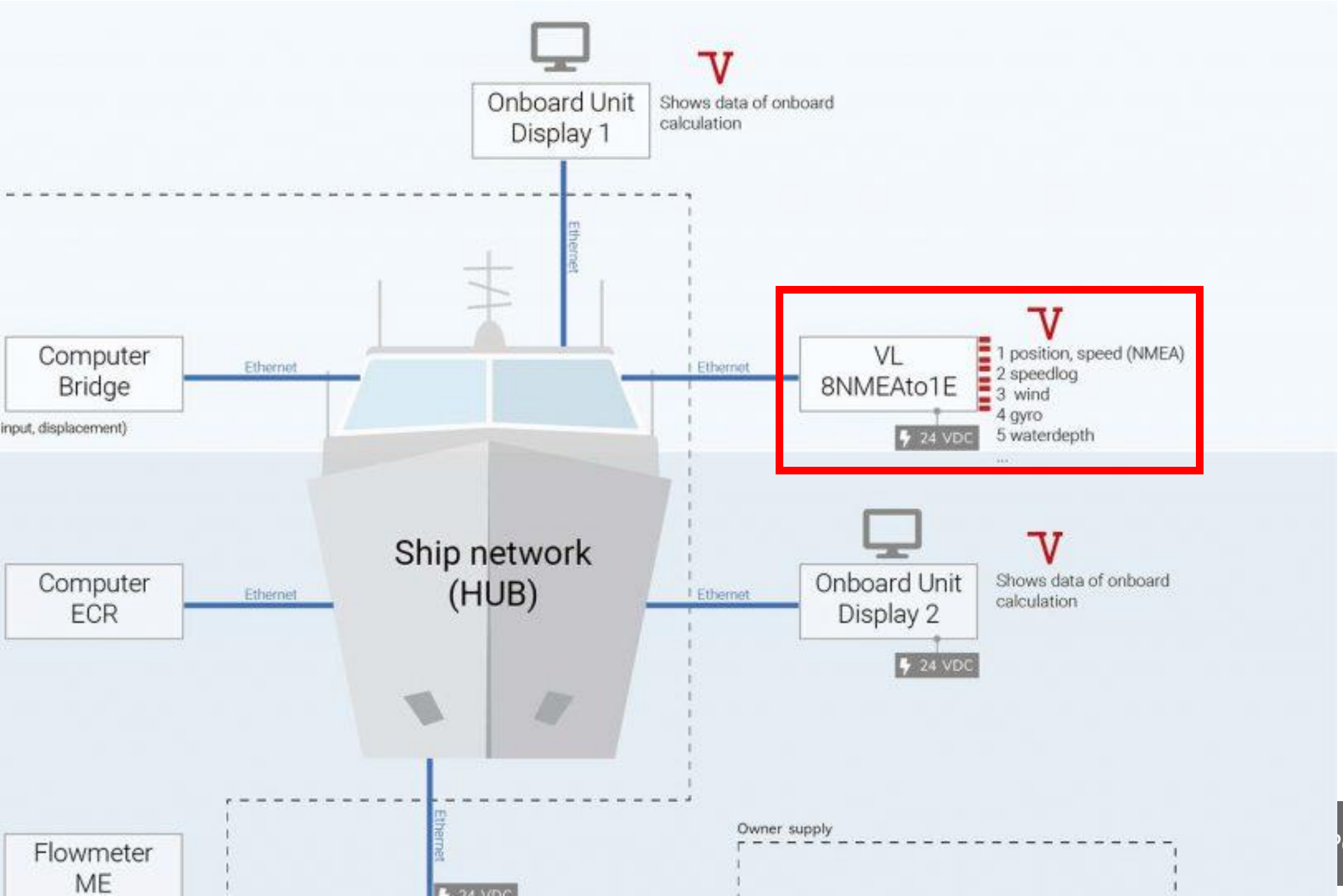
```
open scp://CS5000:[redacted]@192.168.200.161/ -hostkey=*
get -latest /mnt/sd/modbus-tcpip/*.csv ccp.csv
exit
```

```
CS5000@192.168.1.4's password:
$ whoami
CS5000
$ cat /etc/shadow
root:$                                  ':10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
backup:$                                [.:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
vdradmin                                  /:10933:0:99999:7:::
CS5000:$                                  10965:0:99999:7:::
$
```

Many systems are redundant to hardware failure, power loss, even fire and flooding – but not cyber-attack.


ENIRAM DTA - TRIM
-2.0
-1.5
-1.0
-0.5
0.0
0.5
1.0
1.5
2.0
FORE
AFT
F0.64 M
0.03 M
TO OPTIMUM
ENIRAM ELA
90%
75%
60%
45%
30%
DG 1
DG 2
DG 3
DG 4
ENIRAM DTA - LIST
-2.00
-1.00
0.00
1.00
2.00
P0.39 °
16:08:58 UTC
ENIRAM QSA
40
50
60
70
80
90
100
110
120
130
98 RPM
1.0 RPM
TO OPTIMUM

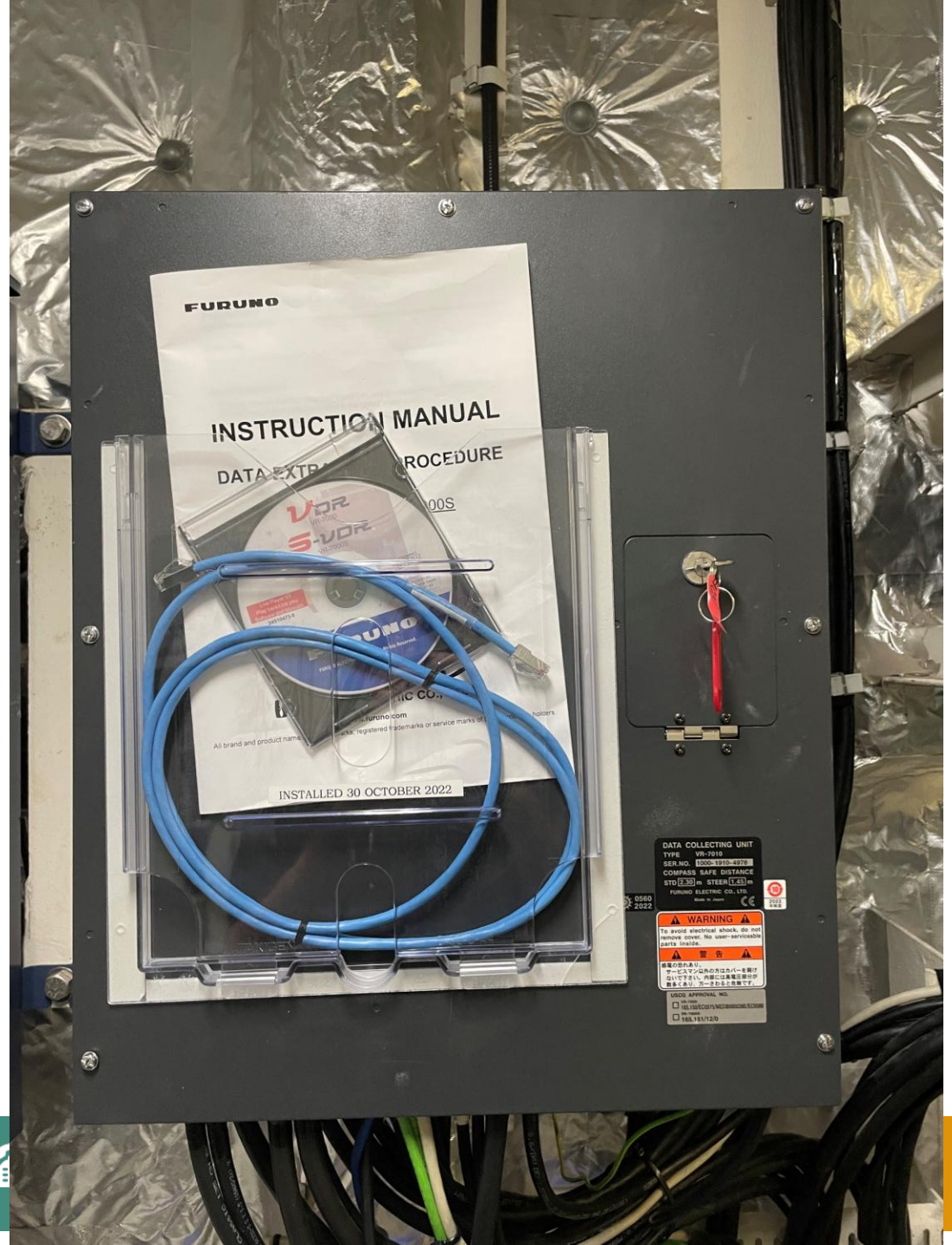

Bridge
Onboard Unit Display 1
Shows data of onboard calculation
Owner supply
Ethernet
PIM program - onboard software unit
(Calculations, manual input, displacement)
Computer Bridge
Ethernet
Ethernet
VL 8NMEAto1E
1 position, speed (NMEA)
2 speedlog
3 wind
4 gyro
5 waterdepth
...
24 VDC
ECR - Engine Room Area
PIM program
Computer ECR
Ethernet
Ship network (HUB)
Ethernet
Onboard Unit Display 2
Shows data of onboard calculation
24 VDC
Ethernet
Owner supply
Actual consumption (mt)
- temperature
- volume
- density
Flowmeter ME
Flowmeter AE1
Flowmeter AEx
Automation
Scrubber
24 VDC
VL - DCU
Data collector
Shaftpower Unit
rpm (min -1)
thrust (kN)
torque (kNm)
shaftpower (kW)

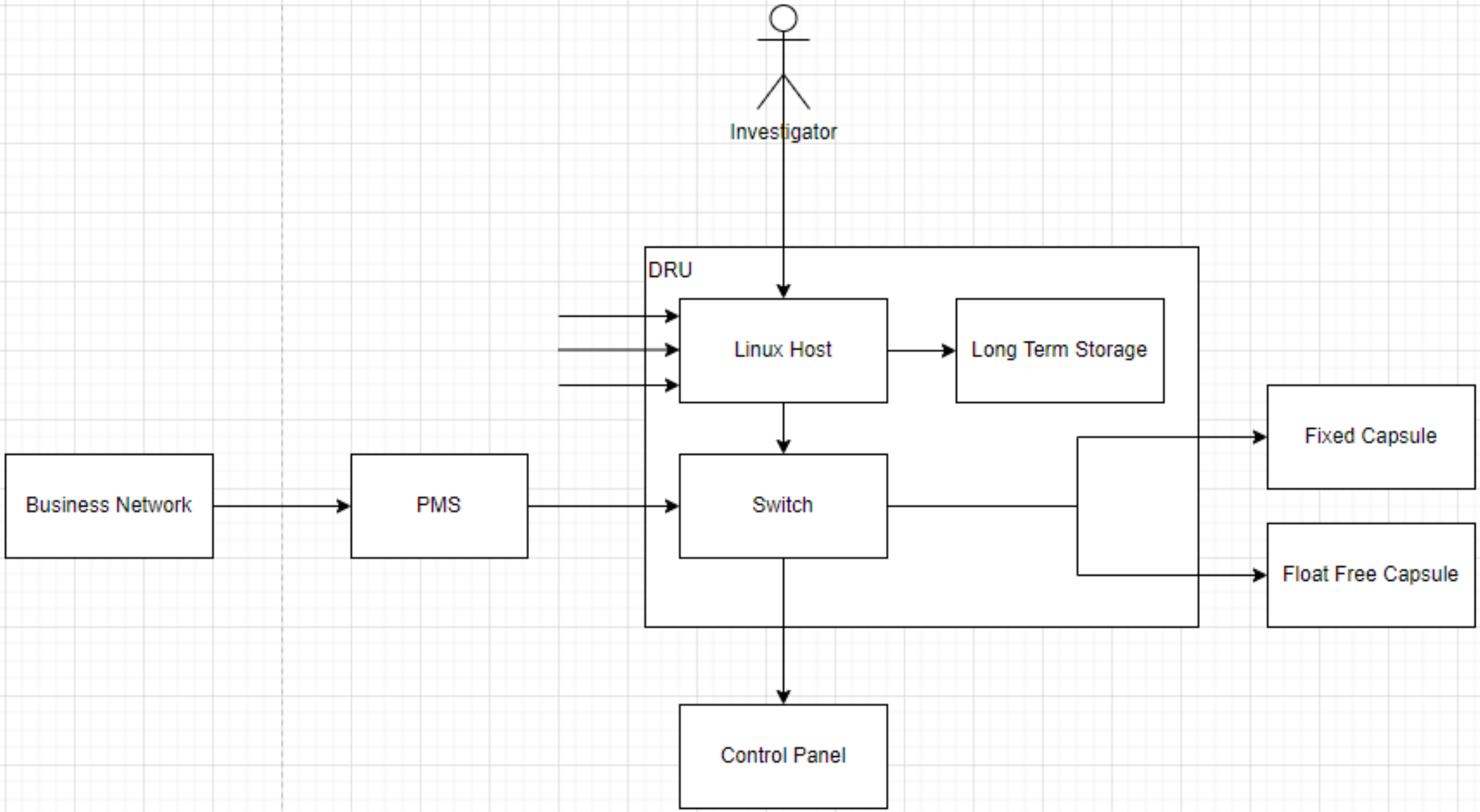

Onboard Unit
Display 1
Shows data of onboard calculation
Ethernet
Computer
Bridge
input, displacement)
Ethernet
Ethernet
VL
8NMEAto1E
24 VDC
1 position, speed (NMEA)
2 speedlog
3 wind
4 gyro
5 waterdepth
...
Ship network
(HUB)
Computer
ECR
Ethernet
Ethernet
Onboard Unit
Display 2
24 VDC
Shows data of onboard calculation
Ethernet
Flowmeter
ME
Owner supply

Voyage Data Recorder

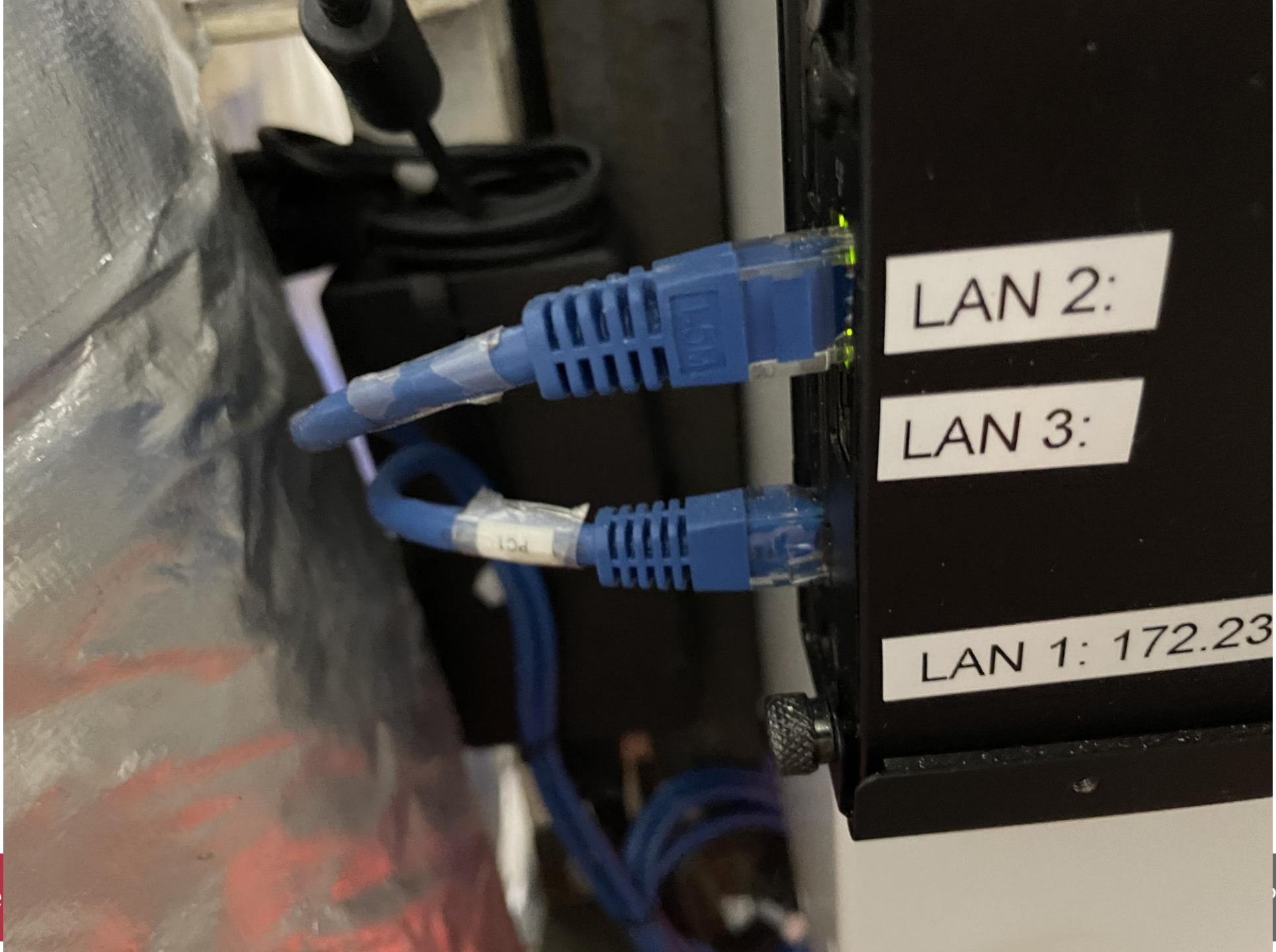
@PenTestPartners

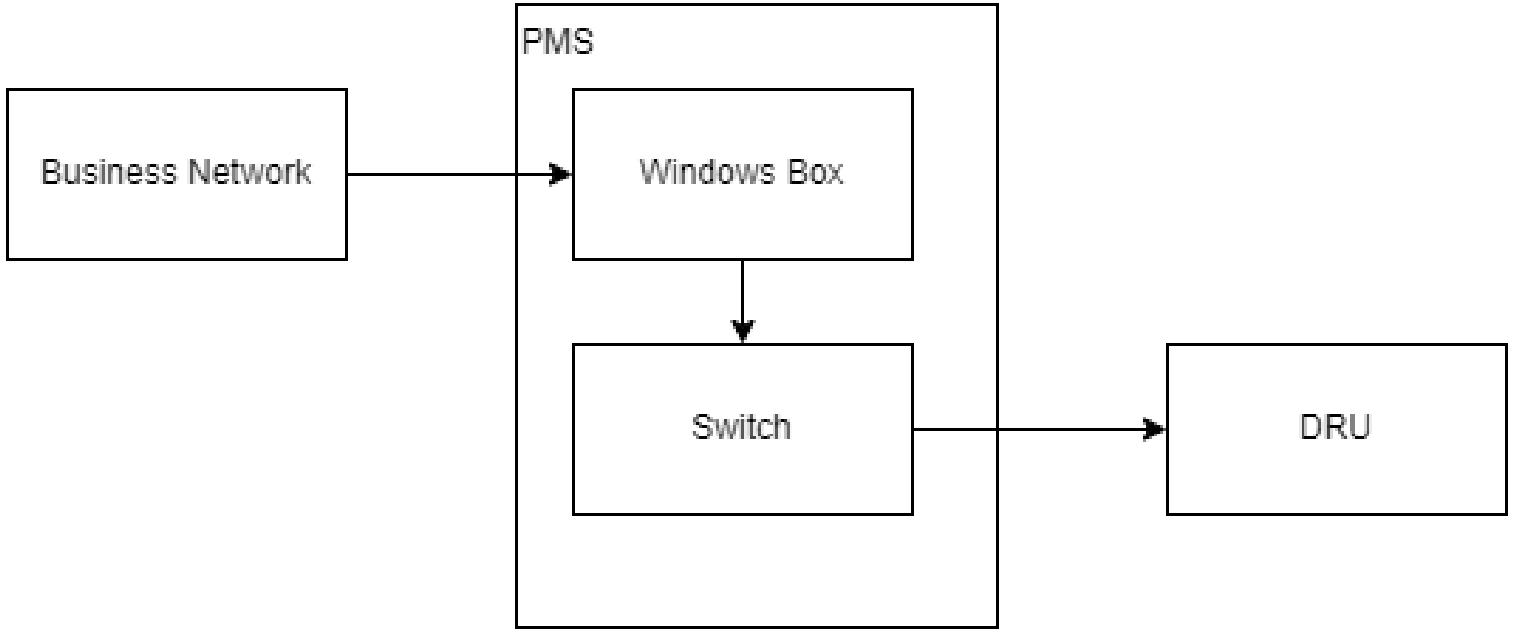
PenTestPartnersLLP

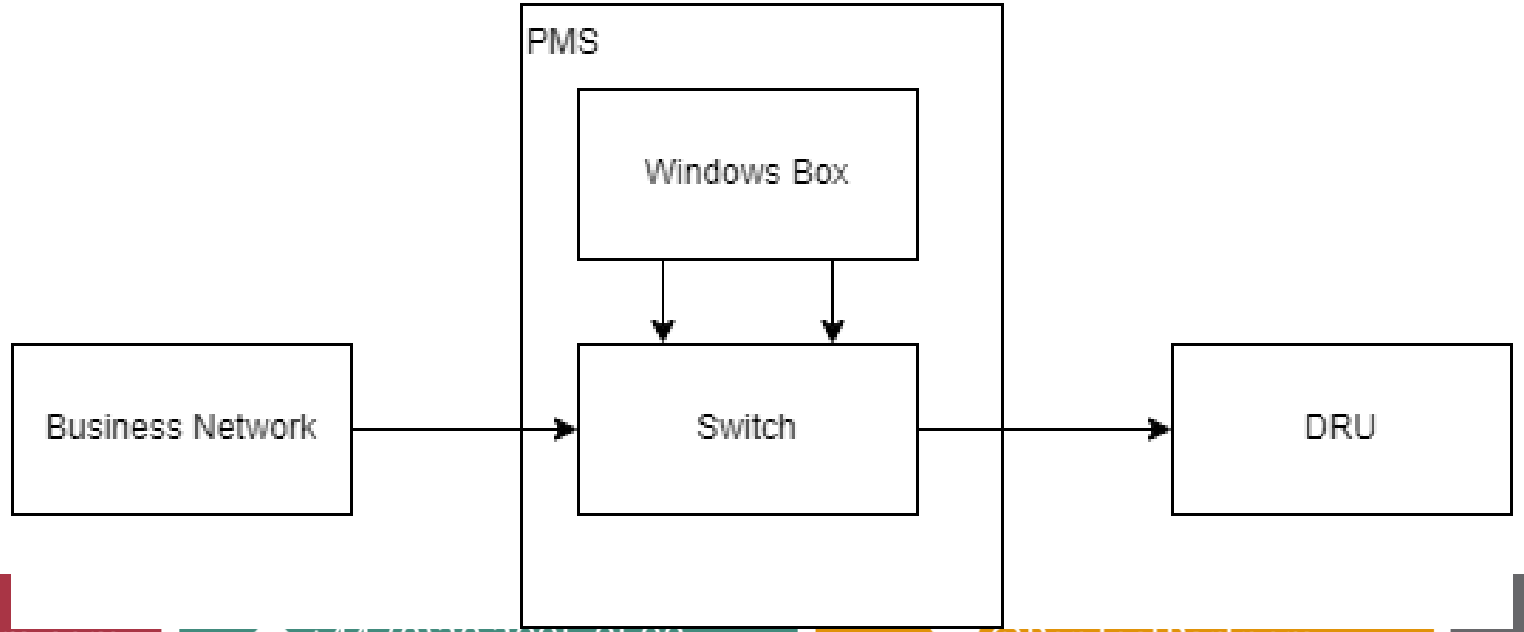

FURUNO
INSTRUCTION MANUAL
INSTALLED 30 OCTOBER 2022
DATA COLLECTING UNIT
TYPE VR-7010
COMPASS SAFE DISTANCE
FURUNO ELECTRIC CO., LTD.
WARNING

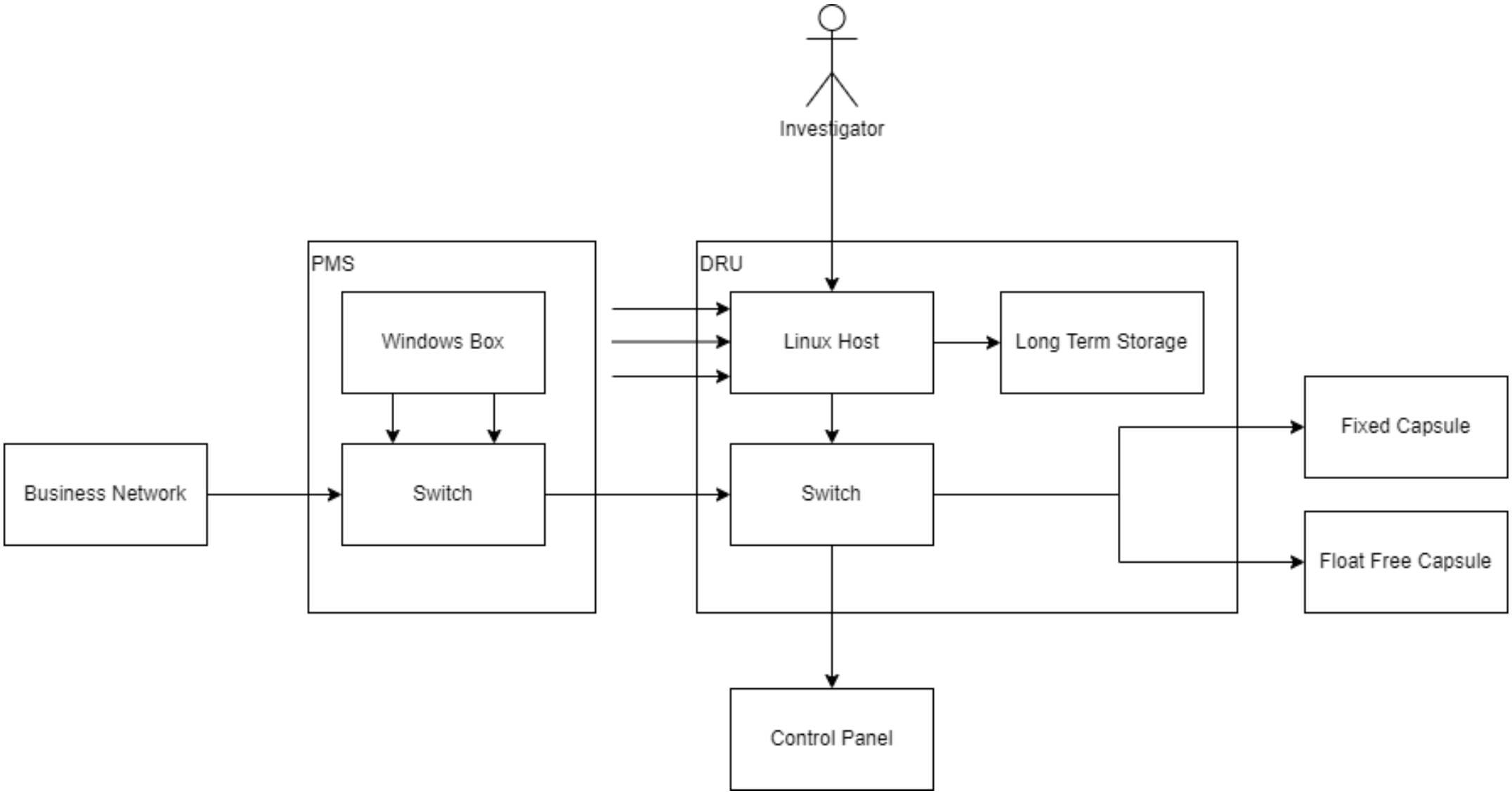

Investigator
DRU
Linux Host
Long Term Storage
Business Network
PMS
Switch
Fixed Capsule
Float Free Capsule
Control Panel


ThinkStation
P340
Veinland
IP: 172.23.23.11
-F1
-G1
-X0
-X2
PULS
DIMENSION
Output DC 24V 5A


LAN 2:
LAN 3:
LAN 1: 172.23

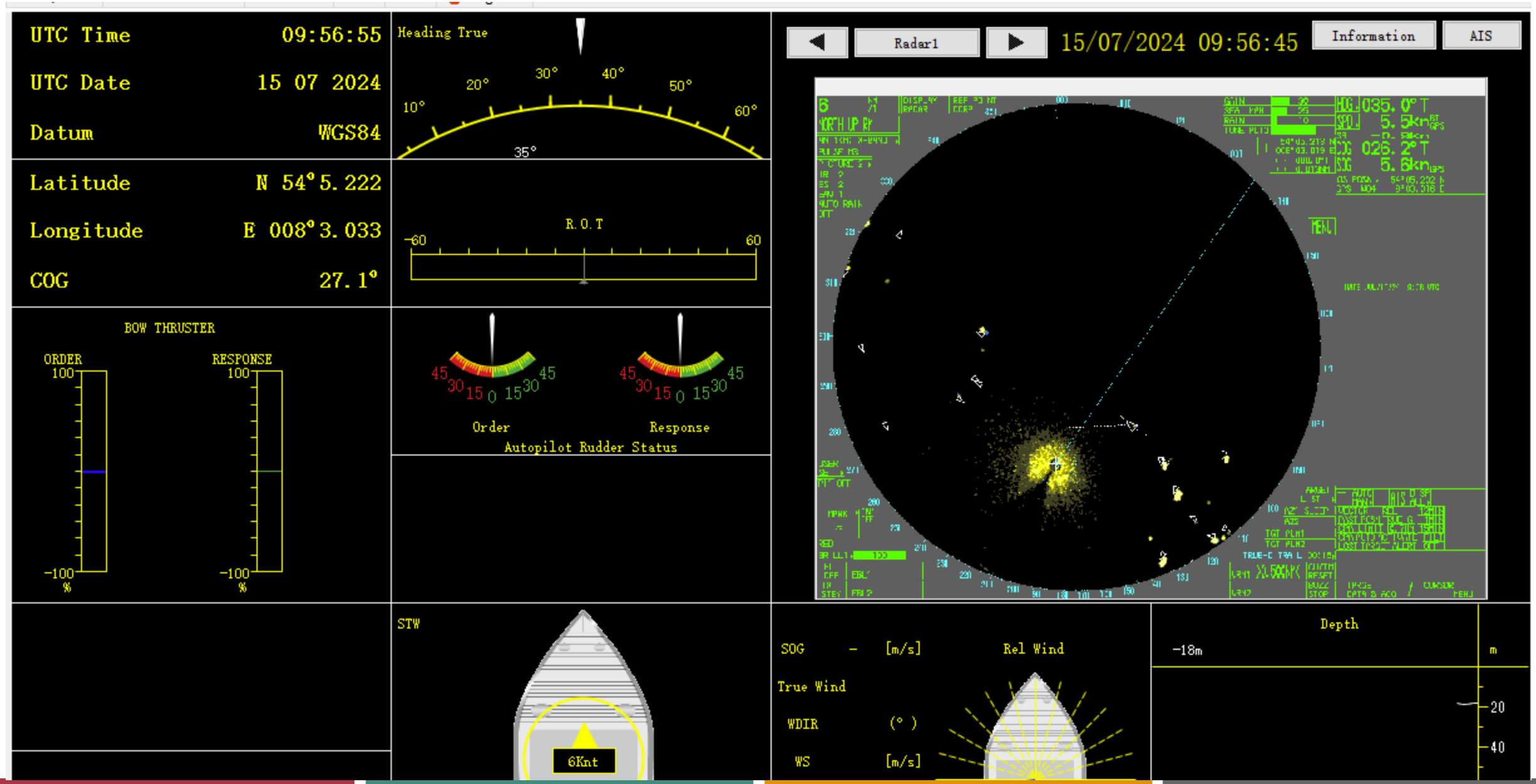

PMS
Business Network
Windows Box
Switch
DRU


PMS
Windows Box
Business Network
Switch
DRU



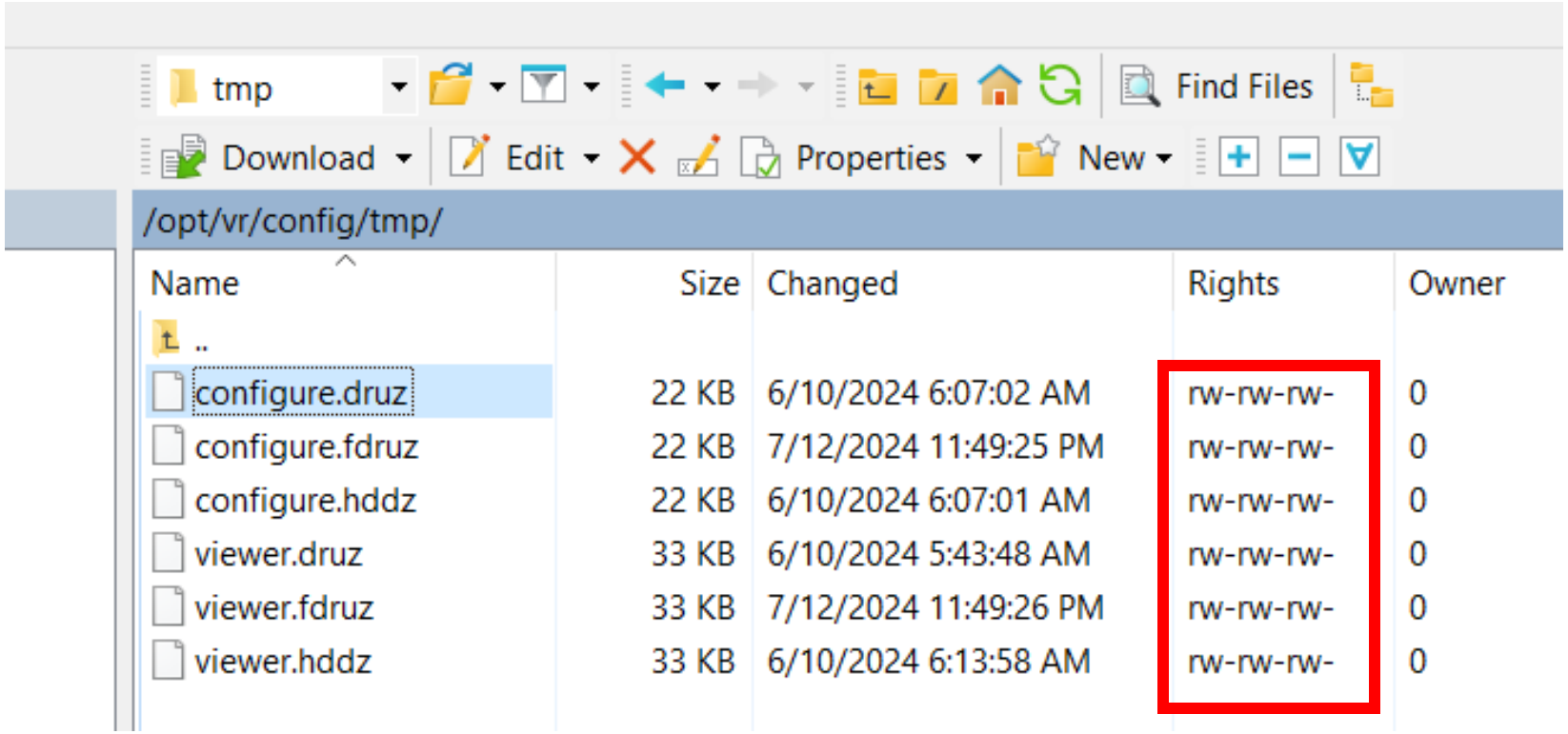
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.6.1	9c:dc:71:c1:59:9b	13	780	Hewlett Packard Enterprise
10.0.0.2	00:d0:1d:06:63:03	1	60	FURUNO ELECTRIC CO., LTD.
10.0.0.100	00:e0:27:26:0b:31	1	60	DUX, INC.
10.0.0.101	90:2e:16:d1:c3:d6	1	60	LCFC(HeFei) Electronics Technology co., ltd
10.0.0.120	00:d0:1d:11:98:62	2	120	FURUNO ELECTRIC CO., LTD.
10.0.0.130	00:d0:1d:11:98:f3	1	60	FURUNO ELECTRIC CO., LTD.
10.0.0.140	00:02:9f:04:95:3c	1	60	L-3 Communication Aviation Recorders
10.0.0.150	00:06:cb:1b:01:d0	1	60	Jotron Electronics A/S
10.0.6.23	00:15:5d:e1:c3:04	3	180	Microsoft Corporation


UTC Time 09:56:55
UTC Date 15 07 2024
Datum WGS84
Latitude N 54° 5.222
Longitude E 008° 3.033
COG 27.1°
Heading True
10° 20° 30° 40° 50° 60°
35°
R.O.T
-60 60
BOW THRUSTER
ORDER
RESPONSE
100
-100
%
45 30 15 0 15 30 45
Order
Response
Autopilot Rudder Status
Radar1
15/07/2024 09:56:45
Information
AIS
STW
6Knt
SOG - [m/s]
True Wind
WDIR (°)
WS [m/s]
Rel Wind
Depth
-18m
m
20
40

```java
public static String decryptoString(byte[] bArr) {
    LOGGER.debug("##### Call VDR_AES_Decrypt #####");
    if (linkedDLL) {
        return VDR_AES_Decrypt(bArr);
    }
    LOGGER.fatal("Can't call native method.");
    return null;
}
```

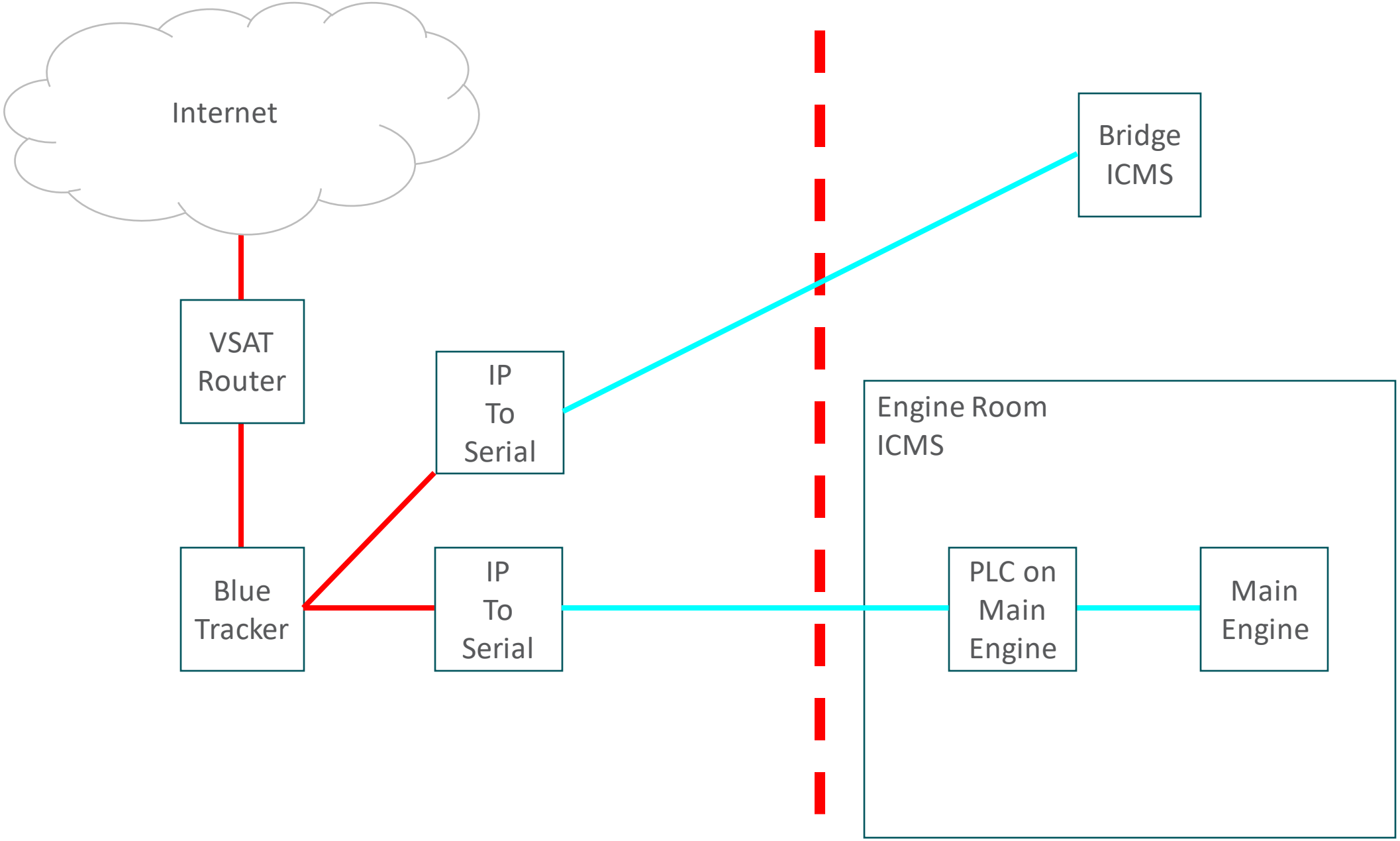
```
[net.FileTransporter:retrieveFile:L?] - Get [/opt/vr/data/onindb/config/conf
[util.VDRSecurityJNI:decryptoString:L?] - ##### Call VDR_AES_Decrypt #####
[util.VDRSecurityJNI:decryptoString:L?] - ##### Call VDR_AES_Decrypt #####
[net.FileTransporter:createDestinationClient:L?] - Host name : 10.0.0.100
[net.FileTransporter:createDestinationClient:L?] - Login name : ftp-reader
[net.FileTransporter:createDestinationClient:L?] - Password : [redacted]
[net.FileTransporter:createDestinationClient:L?] - Timeout : 180000
```

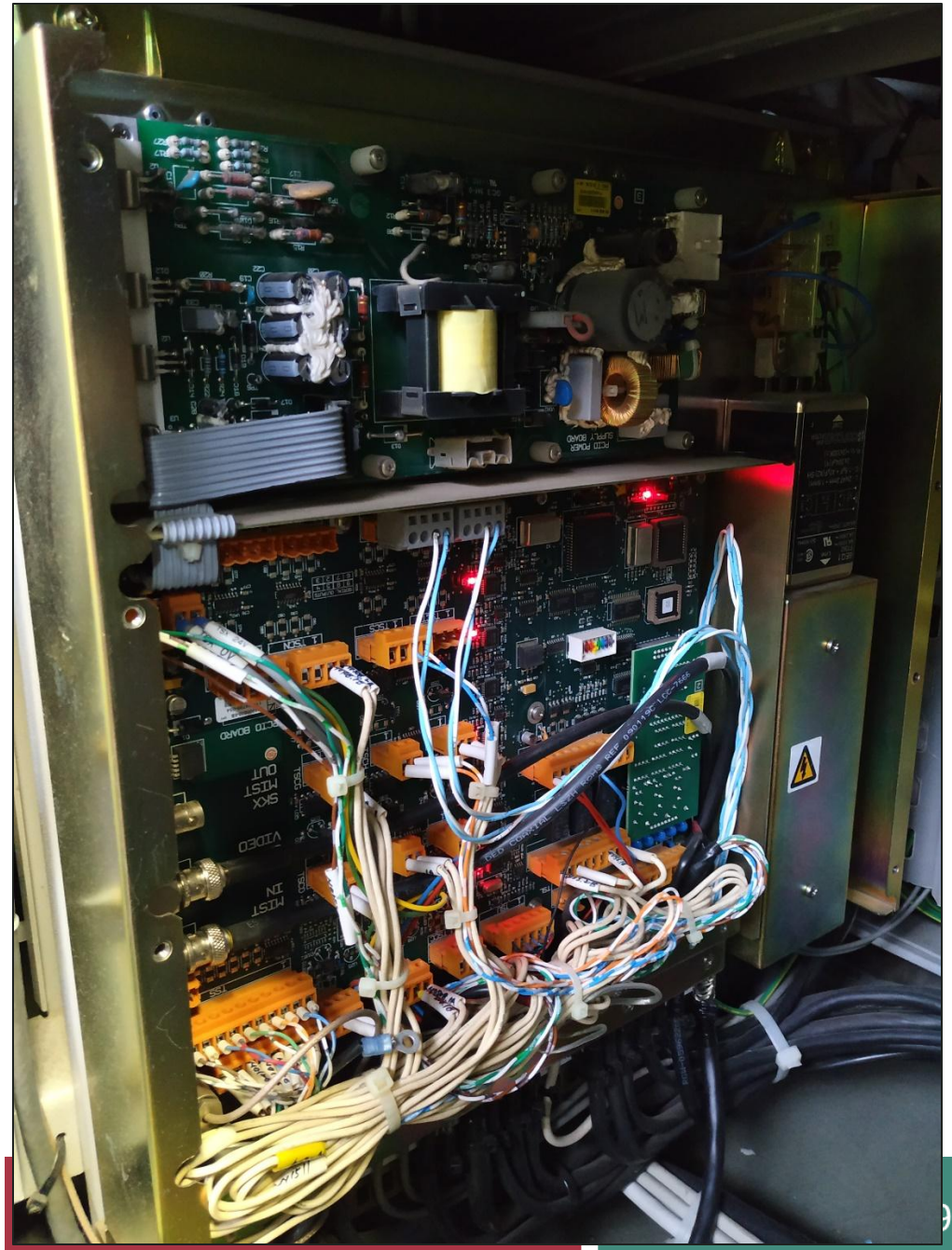

tmp
Find Files
Download
Edit
Properties
New
/opt/vr/config/tmp/
Name
Size
Changed
Rights
Owner
..
configure.druz 22 KB 6/10/2024 6:07:02 AM rw-rw-rw- 0
configure.fdruz 22 KB 7/12/2024 11:49:25 PM rw-rw-rw- 0
configure.hddz 22 KB 6/10/2024 6:07:01 AM rw-rw-rw- 0
viewer.druz 33 KB 6/10/2024 5:43:48 AM rw-rw-rw- 0
viewer.fdruz 33 KB 7/12/2024 11:49:26 PM rw-rw-rw- 0
viewer.hddz 33 KB 6/10/2024 6:13:58 AM rw-rw-rw- 0

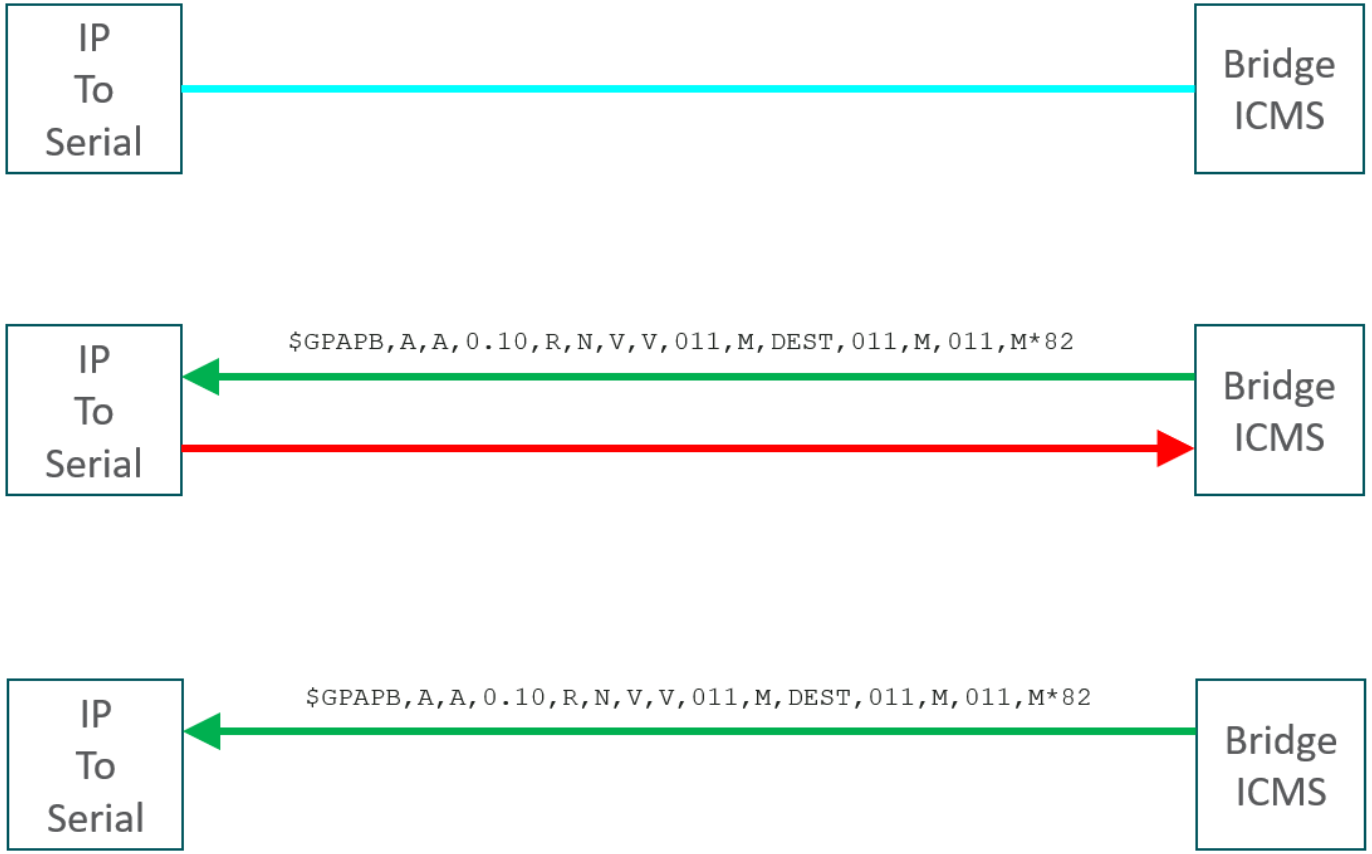
A broken VDR doesn't have immediate safety impact…

But it can stop you sailing due to regulatory reasons…

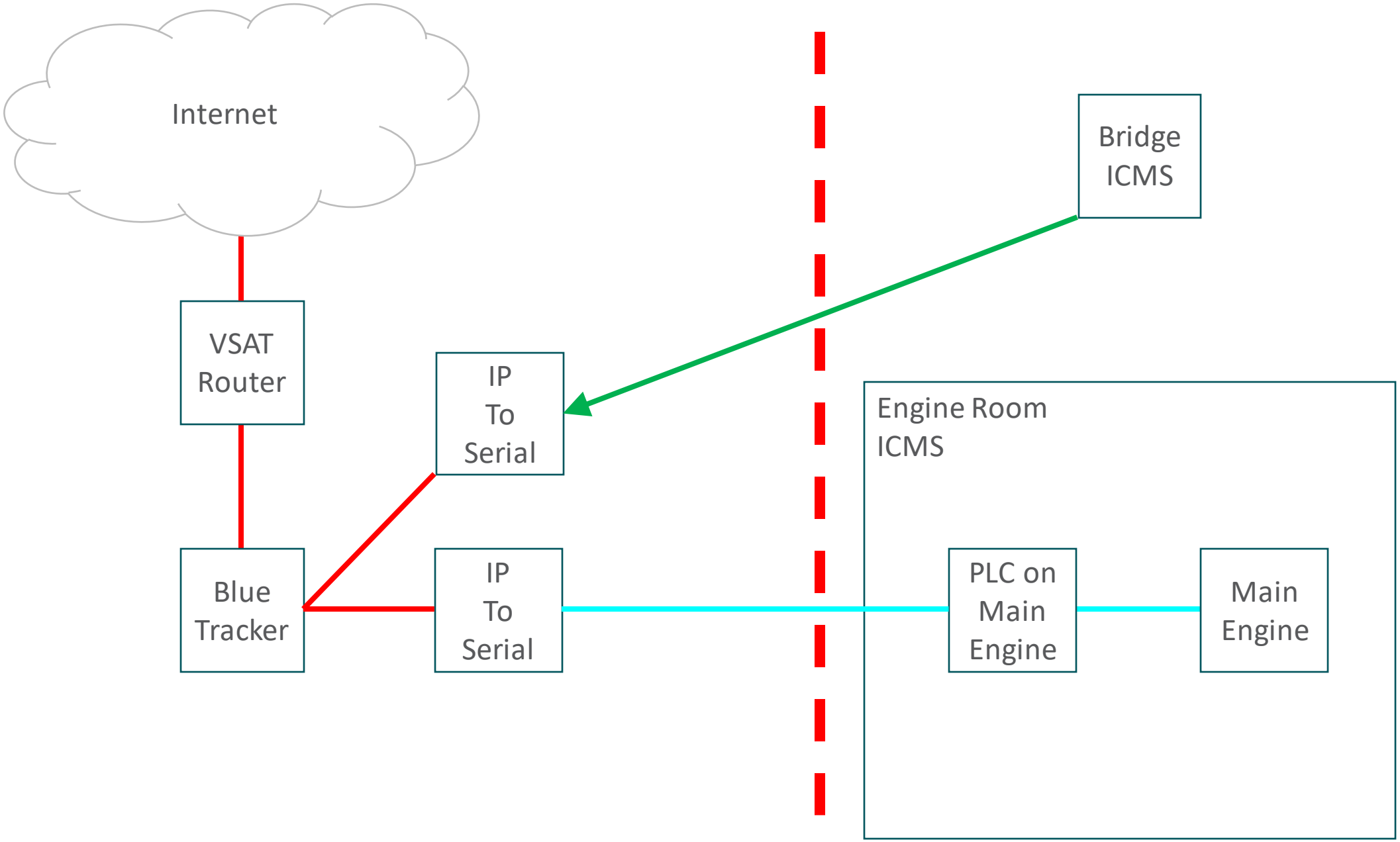

12-48 VDC
RESET
10/100M
Ethernet
MOXA
NPort 5110
Serial Device Server
Ready
Link
Tx/Rx
Port 1 RS-232


Internet
VSAT Router
Blue Tracker
IP To Serial
IP To Serial
Bridge ICMS
Engine Room ICMS
PLC on Main Engine
Main Engine





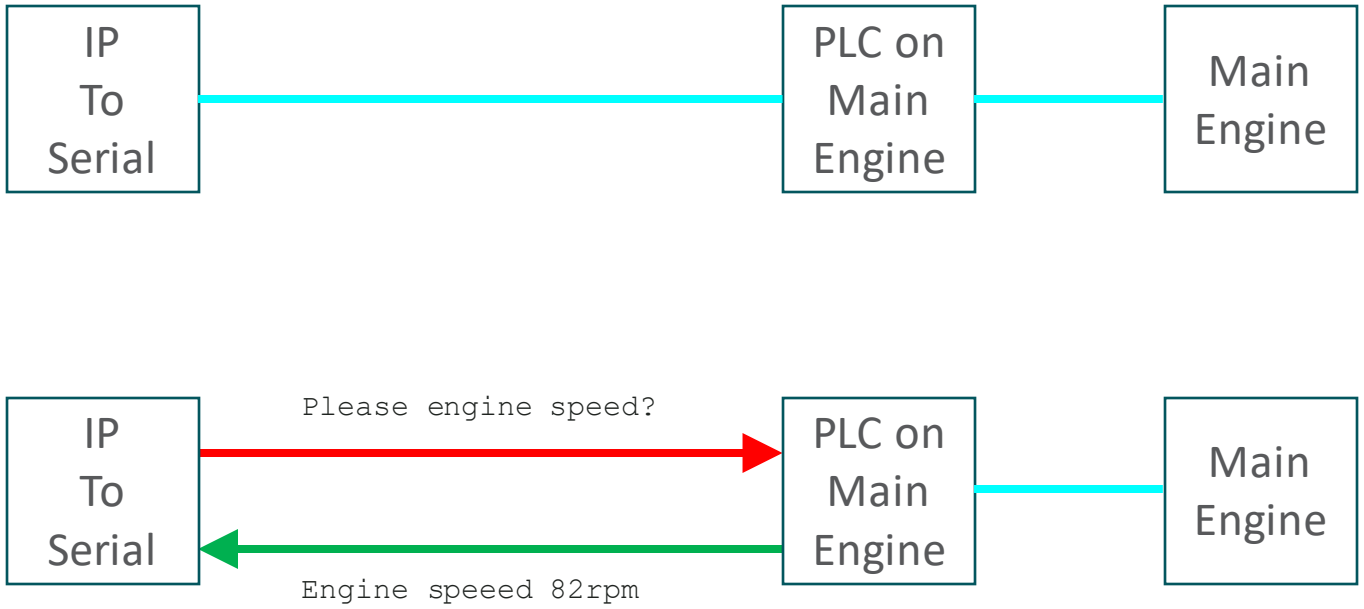
Transmit only works!


Internet
Bridge ICMS
VSAT Router
IP To Serial
Engine Room ICMS
Blue Tracker
IP To Serial
PLC on Main Engine
Main Engine

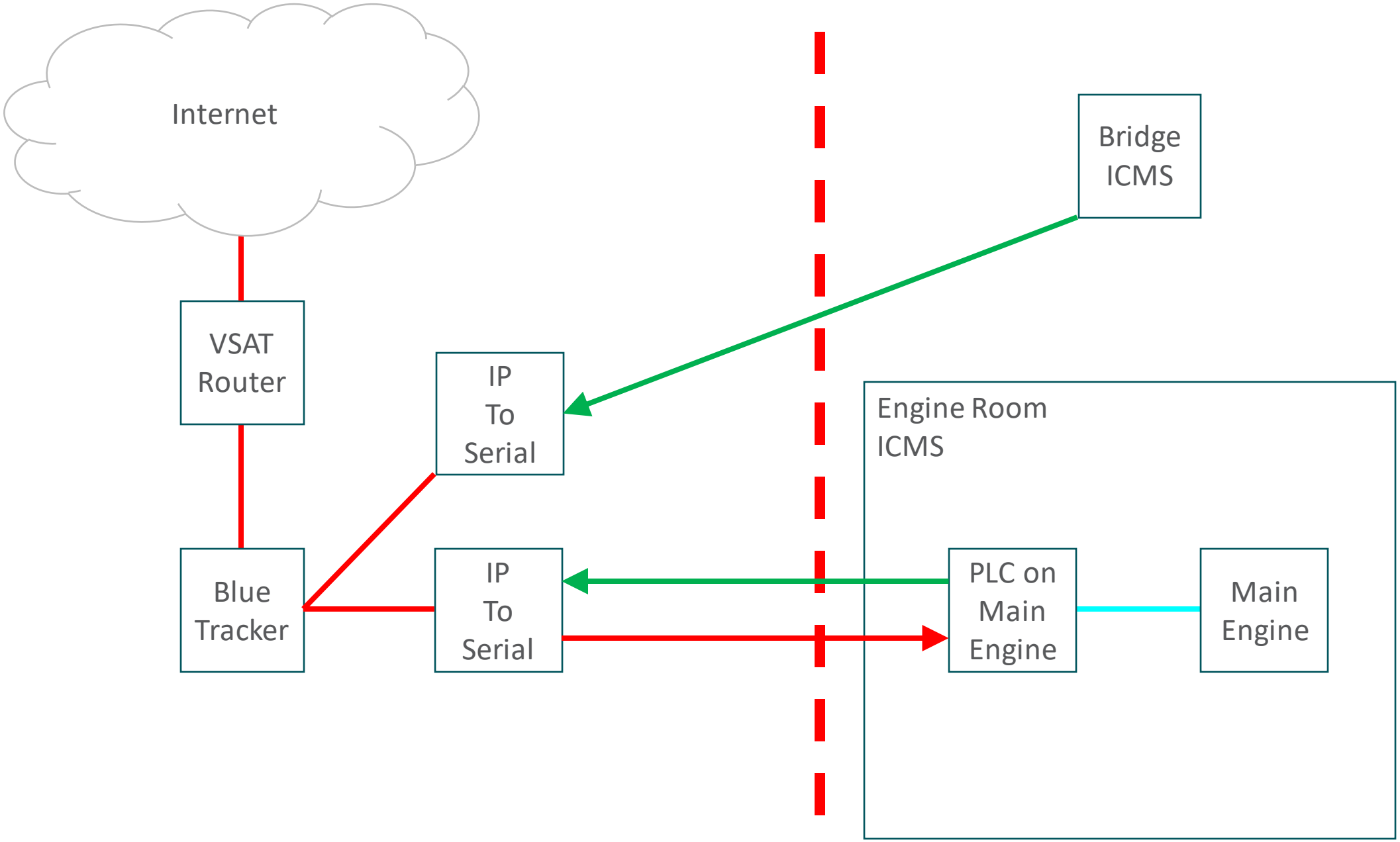
```
17:08:12 +00:21.064  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 250 1223 1175 1197 ... }
17:08:13 +00:22.064  0000 01 03 00 64 00 03 44 14                    ...d..D.
17:08:13 +00:22.064  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0064 N: 3
17:08:14 +00:22.150  0000 01 03 06 00 00 01 A4 00 00 61 6A           .........aj
17:08:14 +00:22.150  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 0 420 0 }
17:08:15 +00:23.172  0000 01 03 00 68 00 4B 84 21                    ...h.K.!
17:08:15 +00:23.172  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0068 N: 75
17:08:15 +00:23.210  0000 01 03 96 01 40 00 46 01 7C 01 06 01 11 00 3F 00  ....@.F.|.....?.
17:08:15 +00:23.306  0010 FC 00 F1 01 1A 02 1F 01 E2 02 1B 02 0C 02 07 01  ........□.......
                     0020 E9 02 0F 02 19 01 D5 01 DE 01 99 01 AB 01 9F 00  □.....□.□.......
                     0030 FF 00 E9 00 F7 02 A8 02 BB 02 A8 02 92 02 A8 02  ..□.............
                     0040 A8 02 9C 02 9C 01 8F 01 CB 01 54 02 CF 02 D9 02  ........ˢ.T.ç.□.
                     0050 C5 02 CF 02 CF 02 CF 02 D9 02 D9 01 17 01 17 01  ł.ç.ç.ç.□.□.....
                     0060 17 02 A8 02 A8 02 A8 02 B2 02 A8 02 A8 02 A8 02  ................
17:08:15 +00:23.420  0070 92 01 0E 01 0E 01 0E 0E 22 0E 72 0E B8 0E EB 0E  ........".r...□.
                     0080 B8 0E 91 0E C2 0E 72 12 51 12 2A 0F A9 0B 40 01  ......r.Q.*...@.
                     0090 46 01 48 01 44 00 00 FF FE 02 0C                 F.H.D......
17:08:15 +00:23.420  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 320 70 380 262 ... }
17:08:16 +00:24.421  0000 01 03 00 00 00 64 44 21                    .....dD!
```

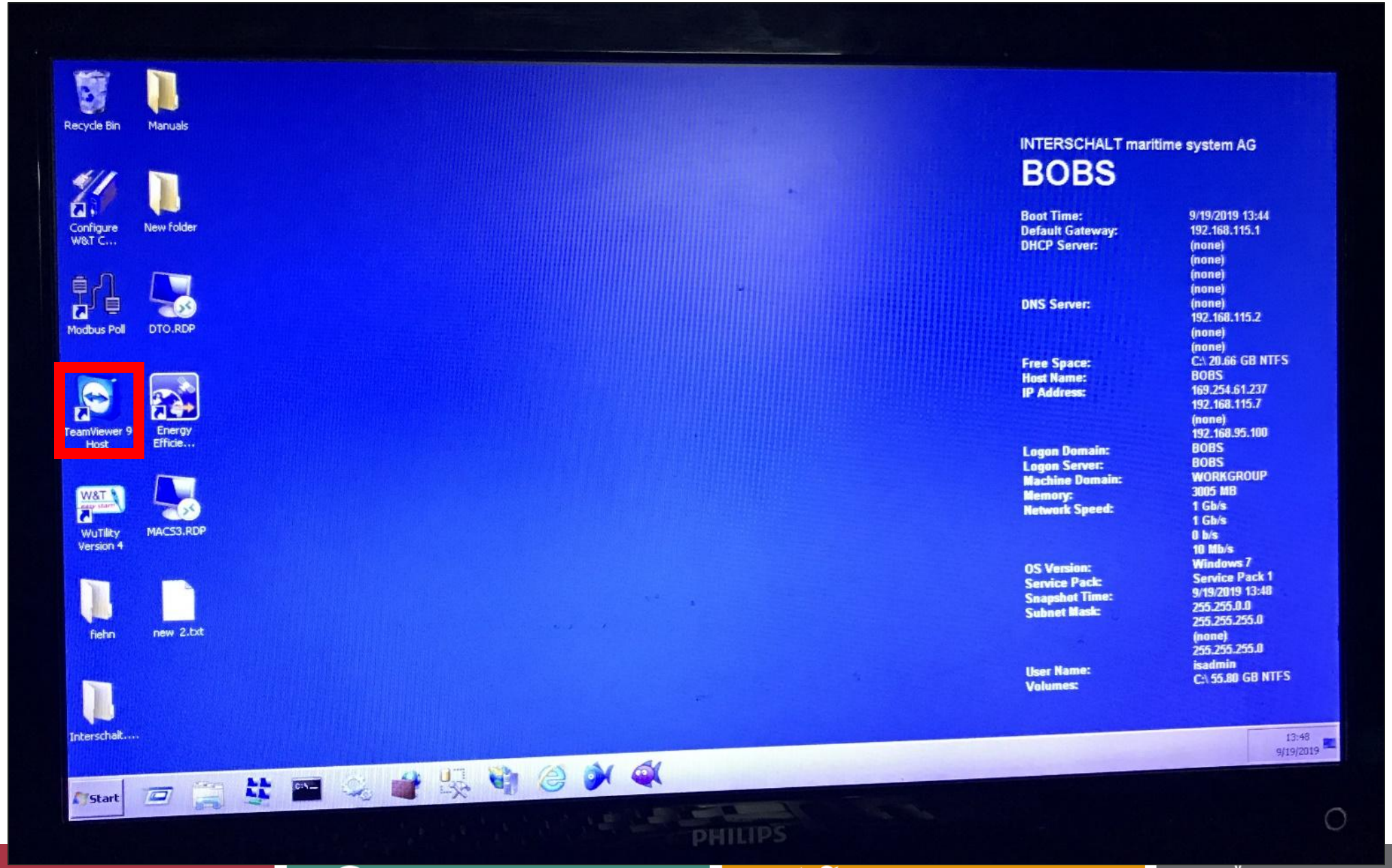

```
[+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0064 N: 3
0000 01 03 06 00 00 01 A4 00 00 61 6A                    .........aj
[+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 0 420 0 }
0000 01 03 00 68 00 4B 84 21                    ...h.K.!
[+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0068 N: 75
```

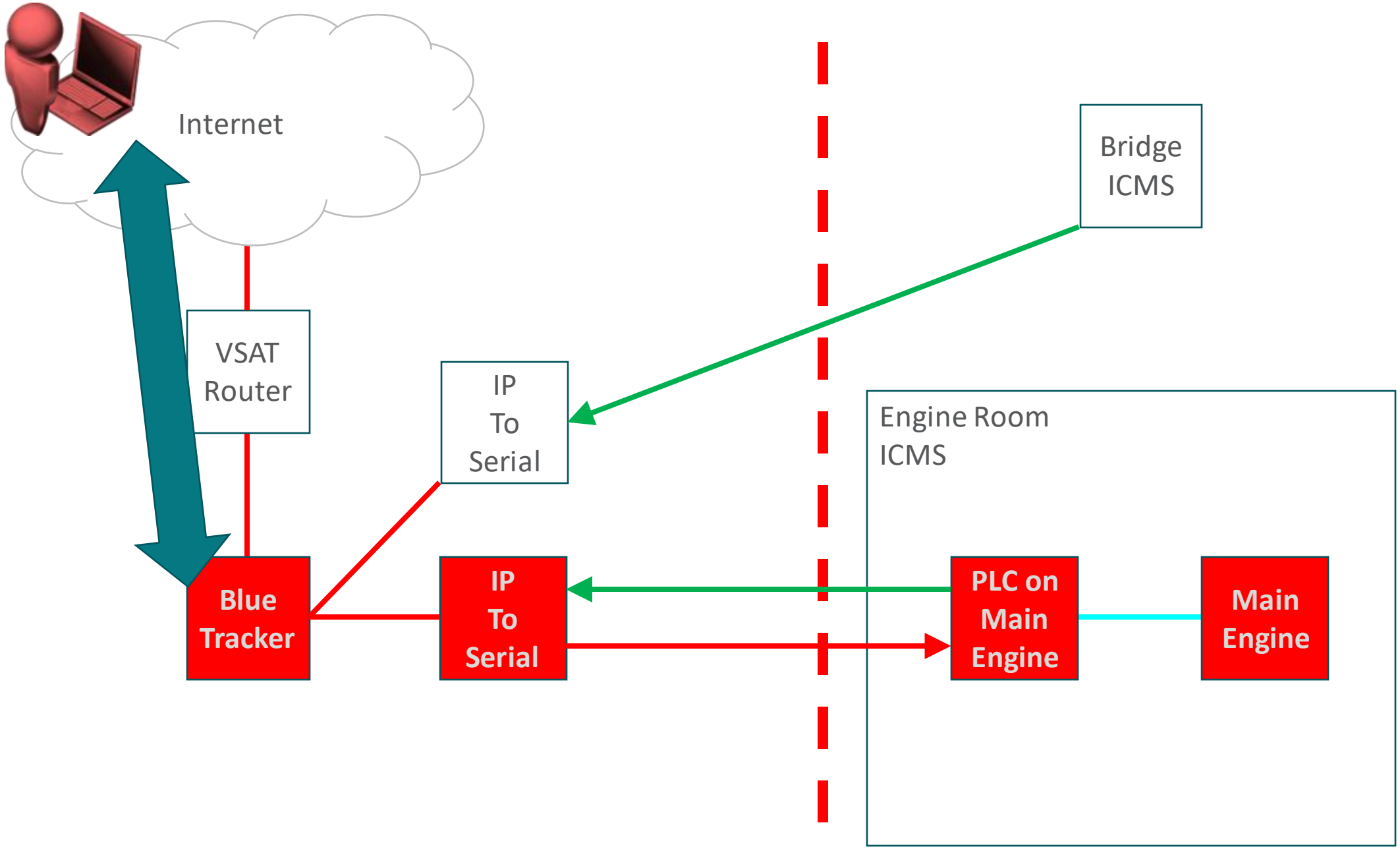

```
17:08:16 +00:24.764  00C0 44 01 57 0B 09 00 00 00 00 01 7C AF 3F      D.W.......|.?
17:08:16 +00:24.764  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 250 1223 1175 1197 ... }
17:08:17 +00:25.765  0000 01 03 00 64 00 03 44 14                    ...d..D.
17:08:17 +00:25.765  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0064 N: 3
17:08:17 +00:25.838  0000 01 03 06 00 00 01 A4 00 00 61 6A           .........aj
17:08:17 +00:25.838  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 0 420 0 }
17:08:18 +00:26.838  0000 01 03 00 68 00 4B 84 21                    ...h.K.!
17:08:18 +00:26.838  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0068 N: 75
17:08:18 +00:26.913  0000 01 03 96 01 40 00 46 01 7C 01 06 01 11 00 3F 00  ....@.F.|.....?.
```

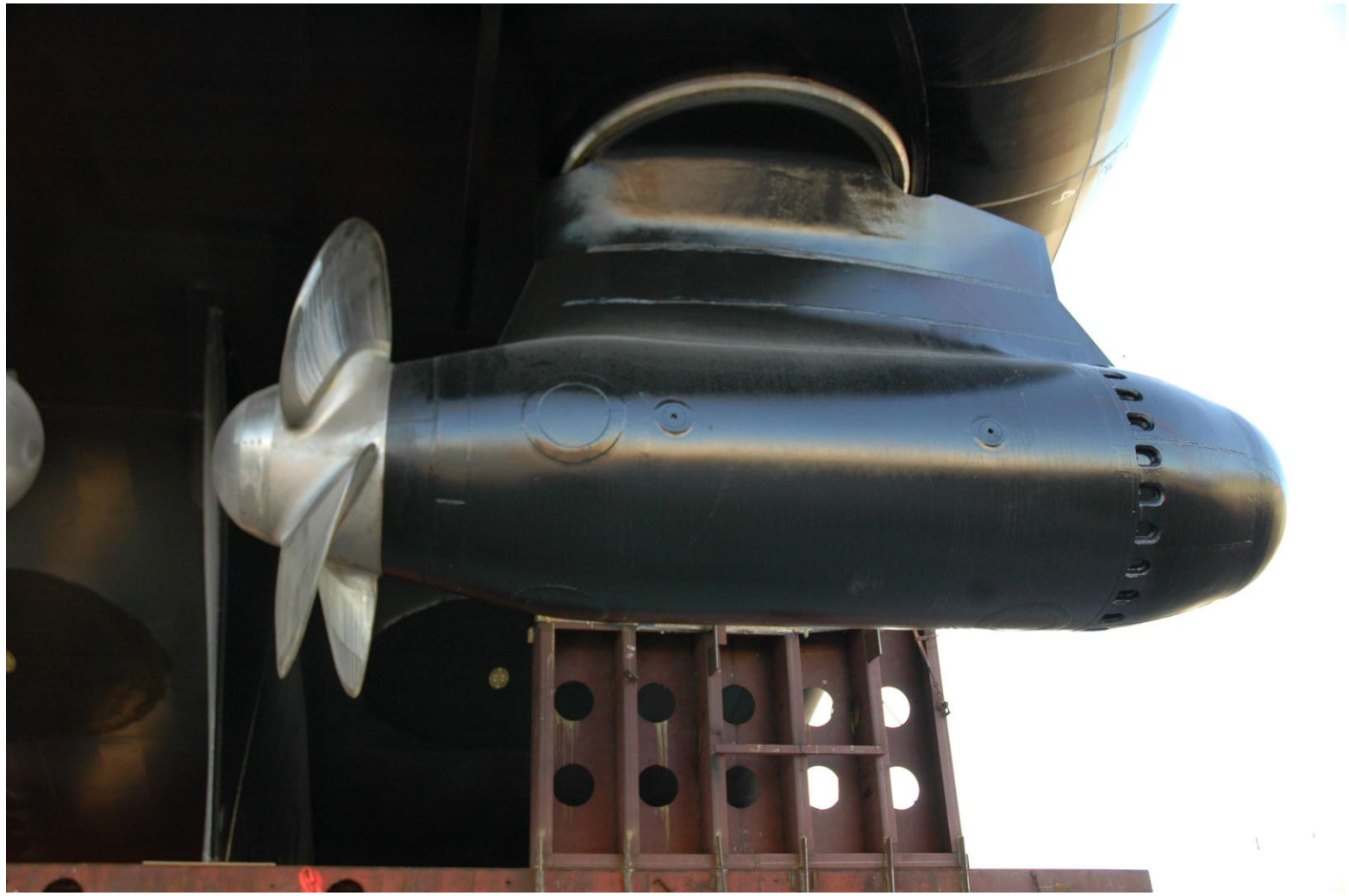


Modbus – request/reply
Needs transmit/receive

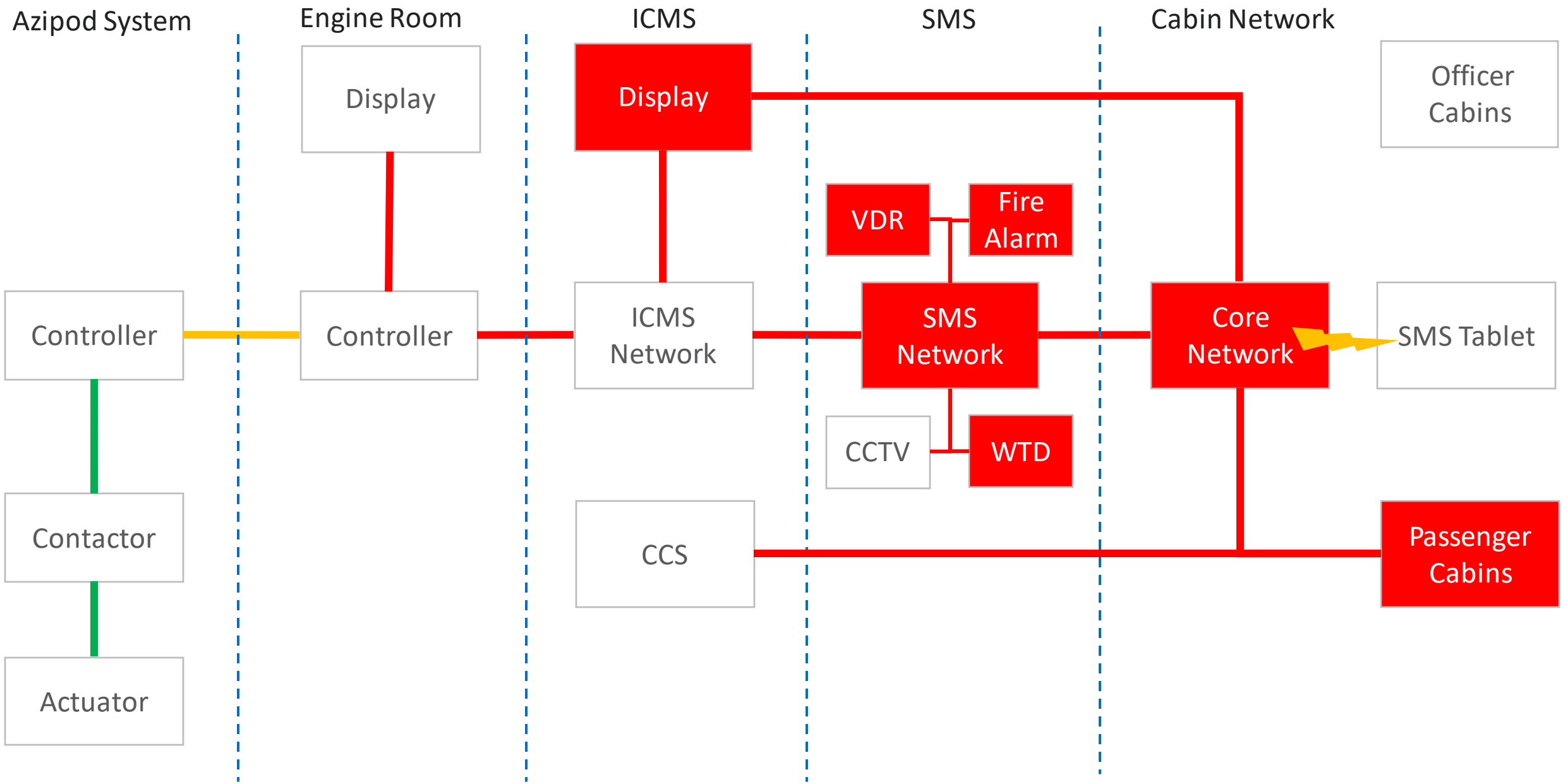

Internet
Bridge ICMS
VSAT Router
IP To Serial
Engine Room ICMS
Blue Tracker
IP To Serial
PLC on Main Engine
Main Engine


Recycle Bin
Manuals
Configure W&T C...
New folder
Modbus Poll
DTO.RDP
TeamViewer 9 Host
Energy Efficie...
WuTility Version 4
MACS3.RDP
fiehn
new 2.txt
Interschalt....
Start
INTERSCHALT maritime system AG
BOBS
Boot Time: 9/19/2019 13:44
Default Gateway: 192.168.115.1
DHCP Server: (none)
(none)
(none)
(none)
DNS Server: (none)
192.168.115.2
(none)
(none)
Free Space: C:\ 20.66 GB NTFS
Host Name: BOBS
IP Address: 169.254.61.237
192.168.115.7
(none)
192.168.95.100
Logon Domain: BOBS
Logon Server: BOBS
Machine Domain: WORKGROUP
Memory: 3005 MB
Network Speed: 1 Gb/s
1 Gb/s
0 b/s
10 Mb/s
OS Version: Windows 7
Service Pack: Service Pack 1
Snapshot Time: 9/19/2019 13:48
Subnet Mask: 255.255.0.0
255.255.255.0
(none)
255.255.255.0
User Name: isadmin
Volumes: C:\ 55.80 GB NTFS
13:48
9/19/2019
PHILIPS

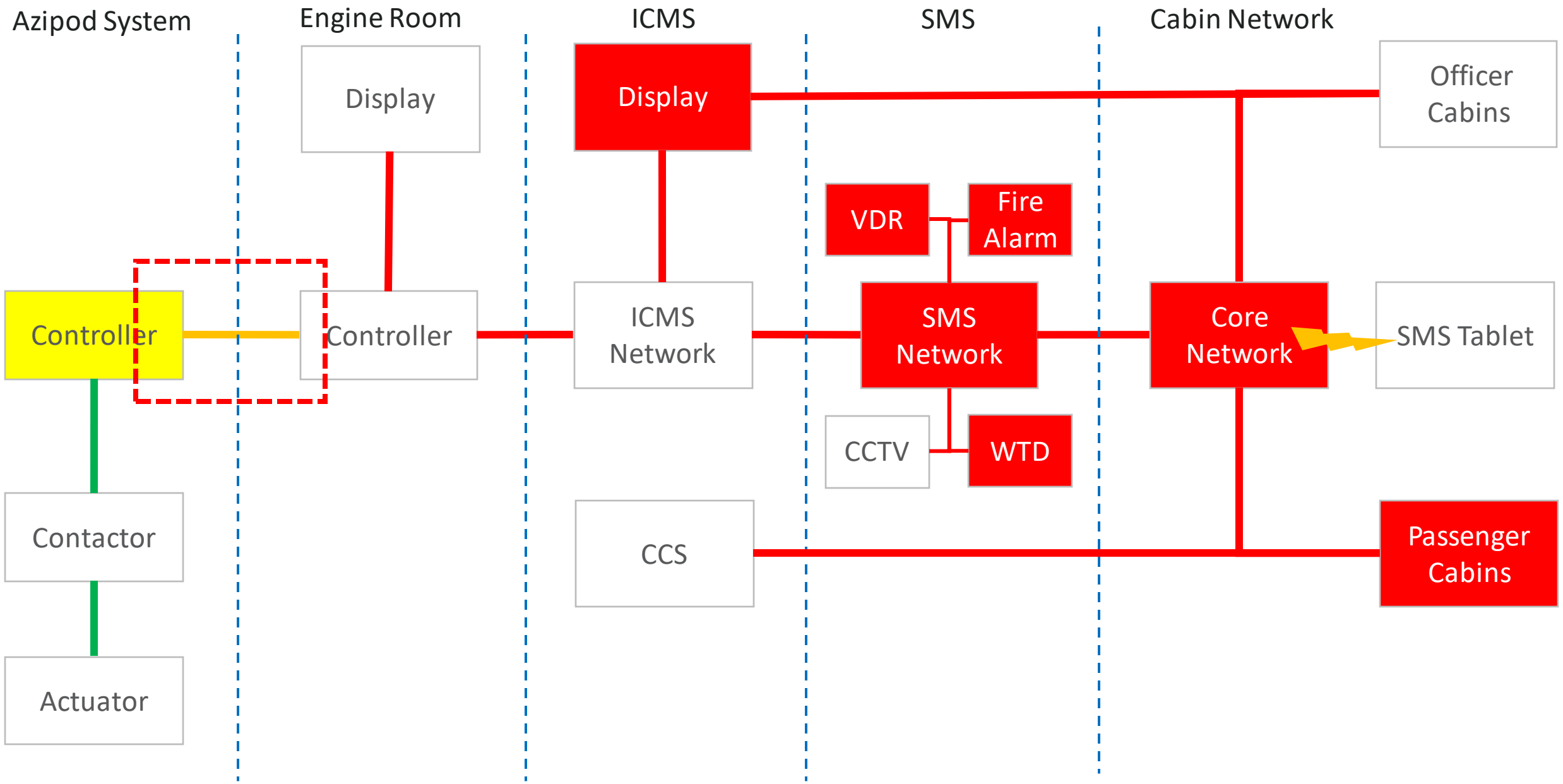

Internet
Bridge
ICMS
VSAT
Router
IP
To
Serial
Engine Room
ICMS
Blue
Tracker
IP
To
Serial
PLC on
Main
Engine
Main
Engine



Azipods



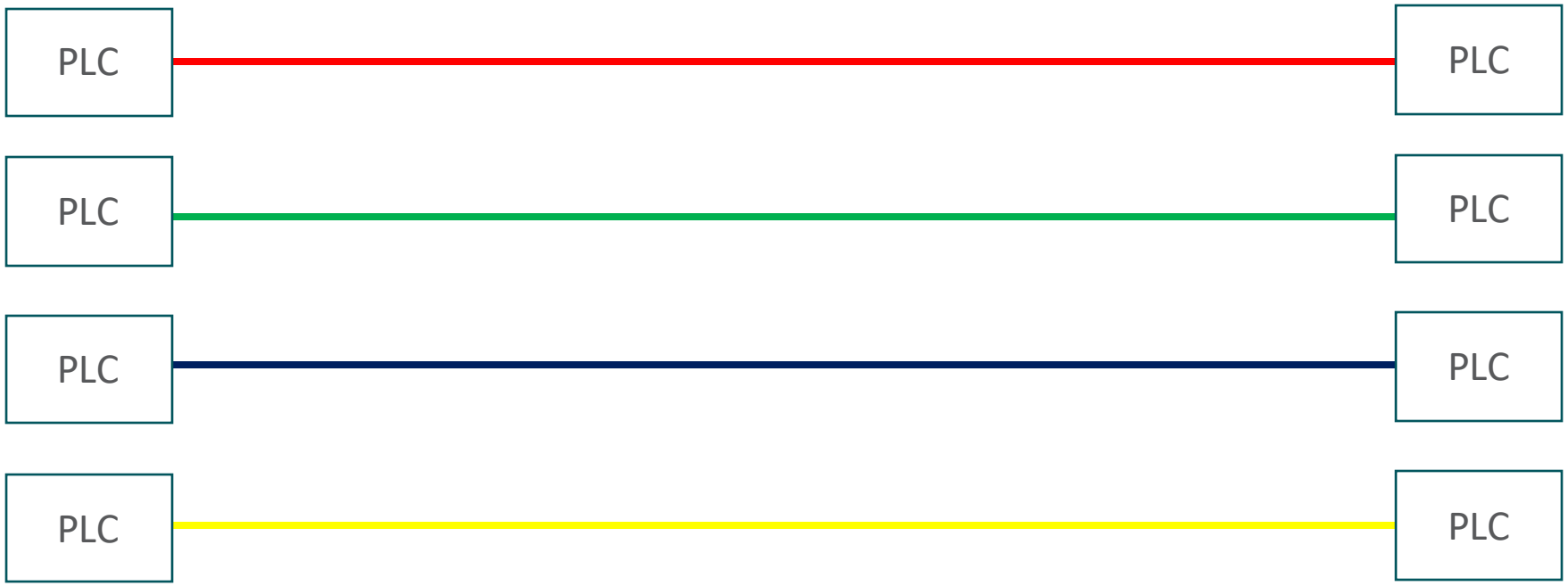
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP



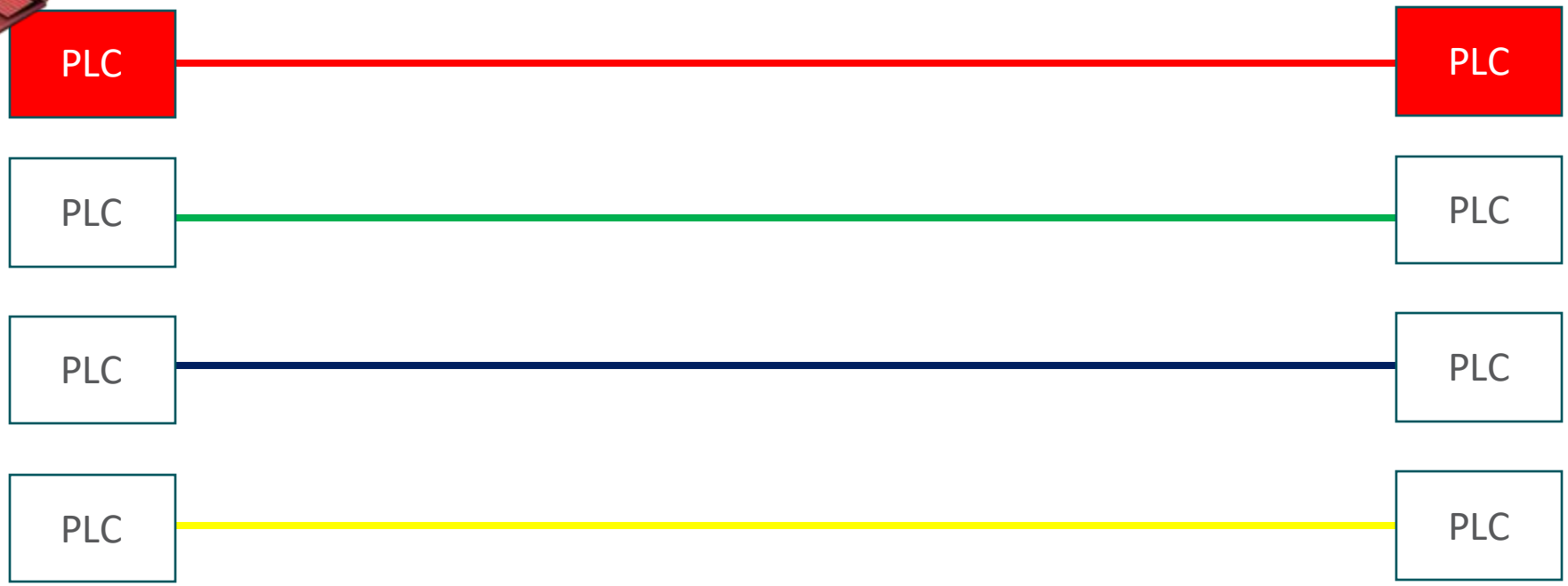
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

“The azipods are connected to the ICMS by serial and for monitoring only”

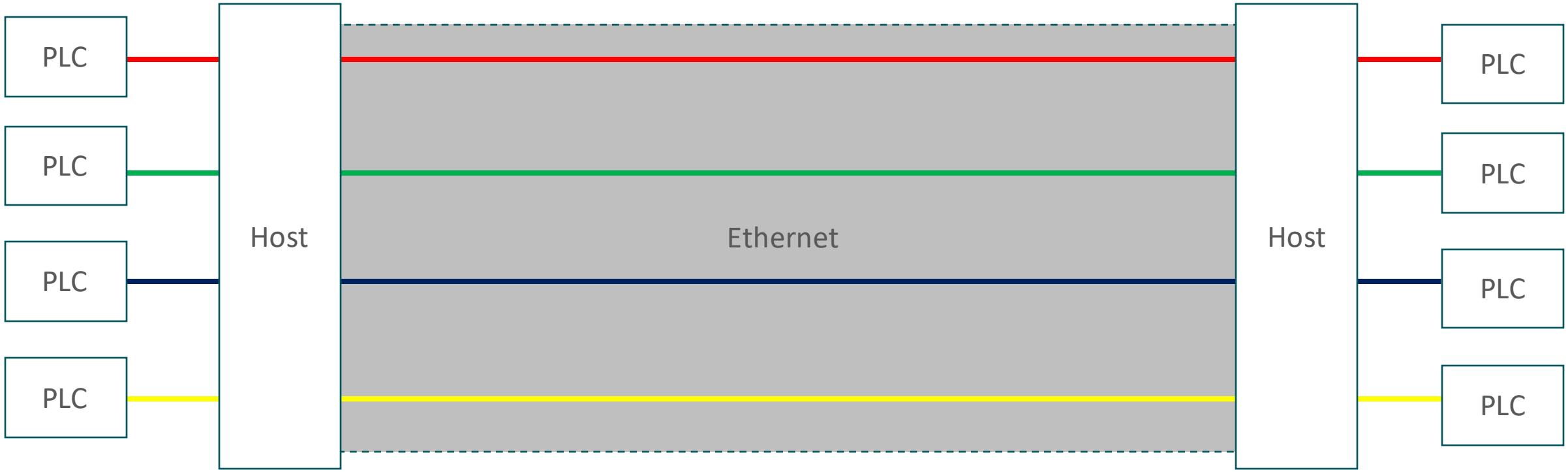
Discrete Serial



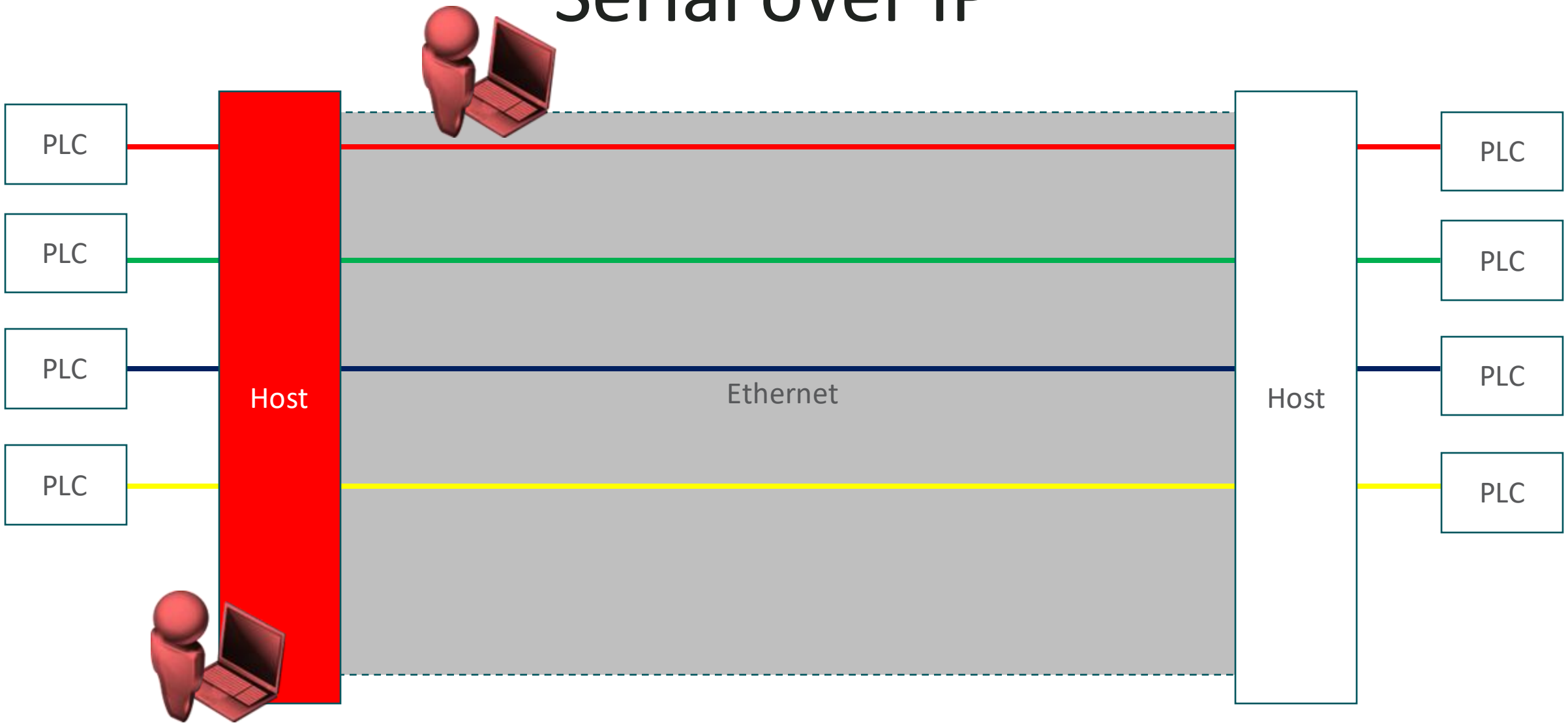
Discrete Serial



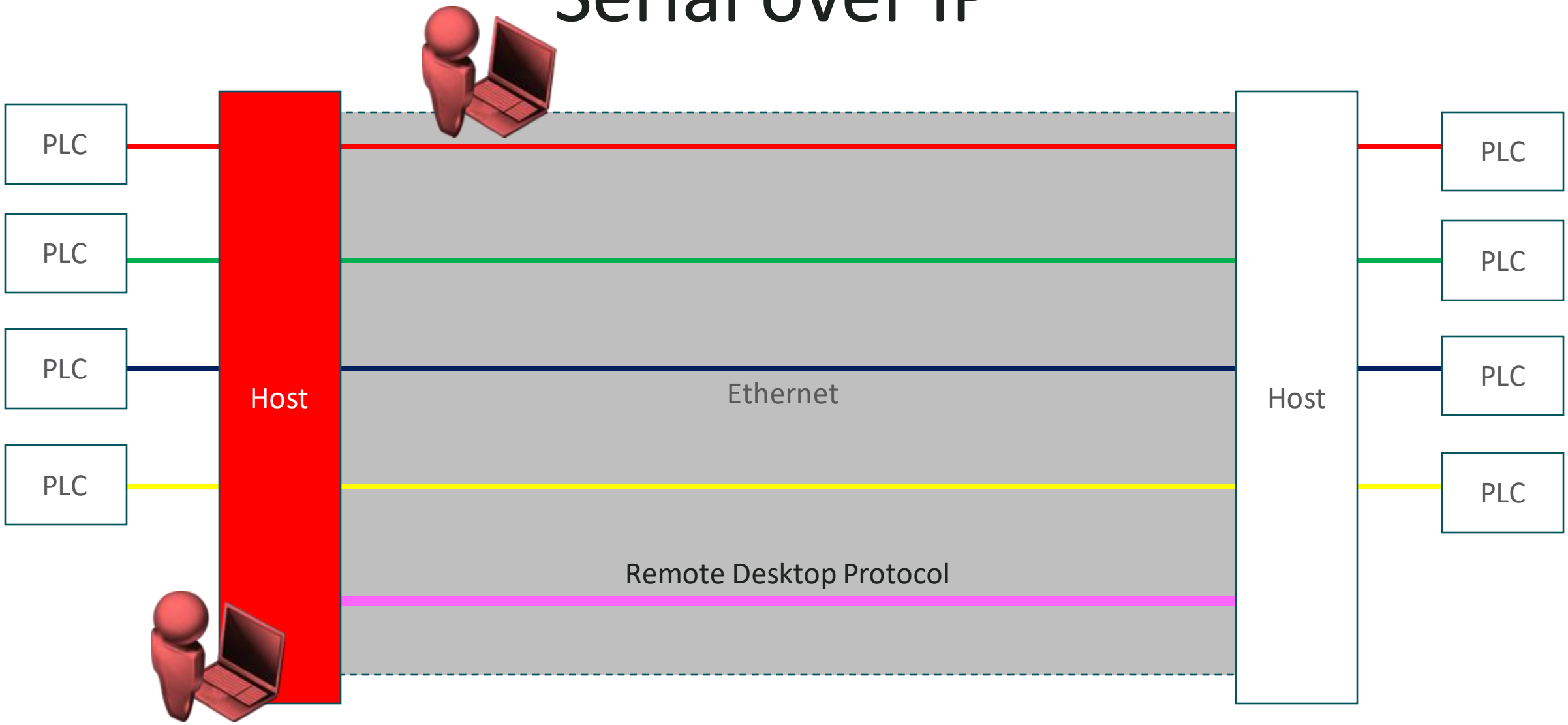
Serial over IP



Serial over IP

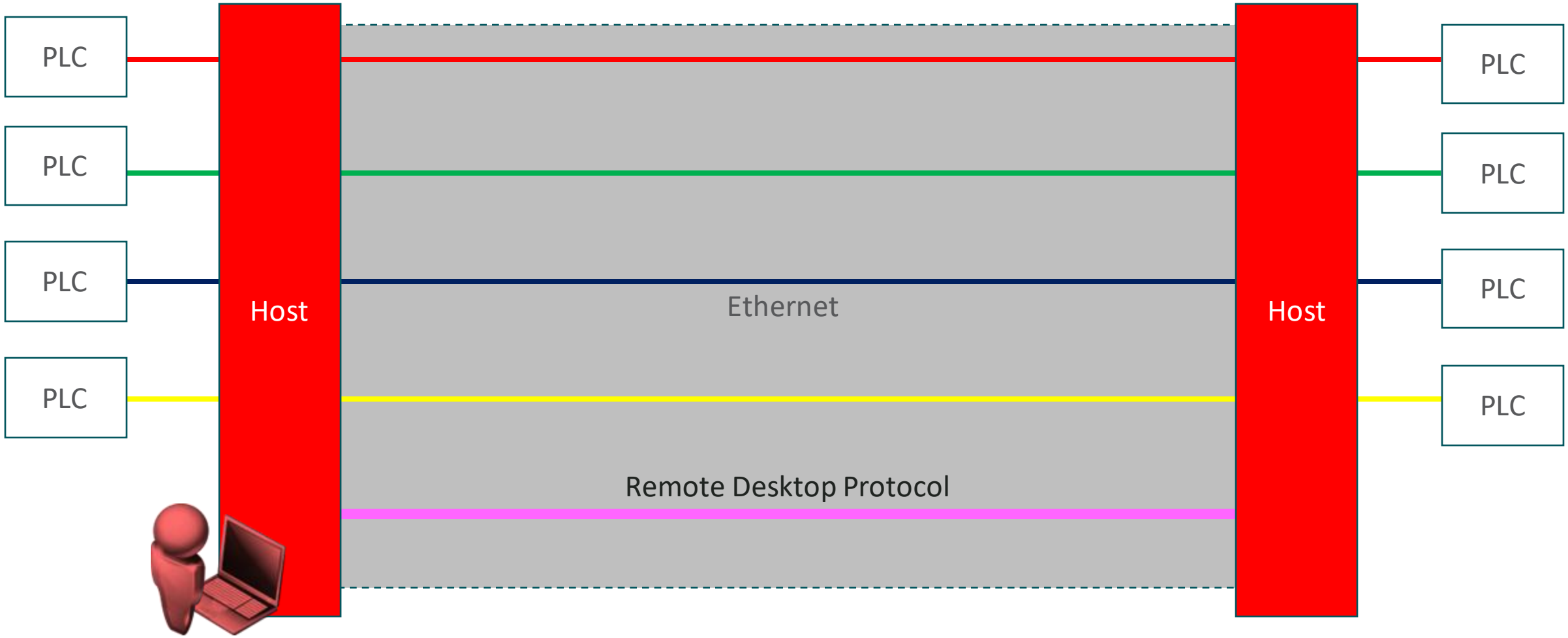


Serial over IP



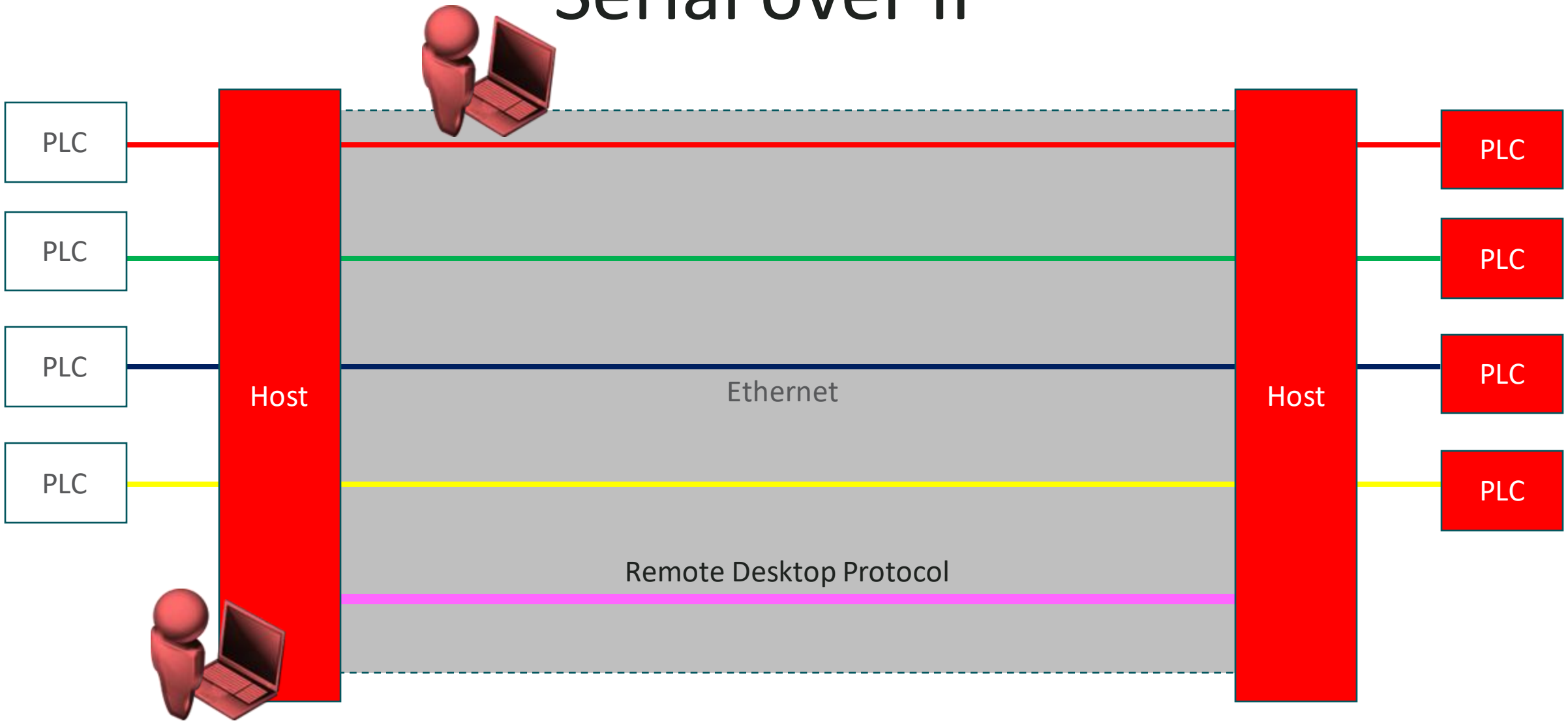
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

Serial over IP



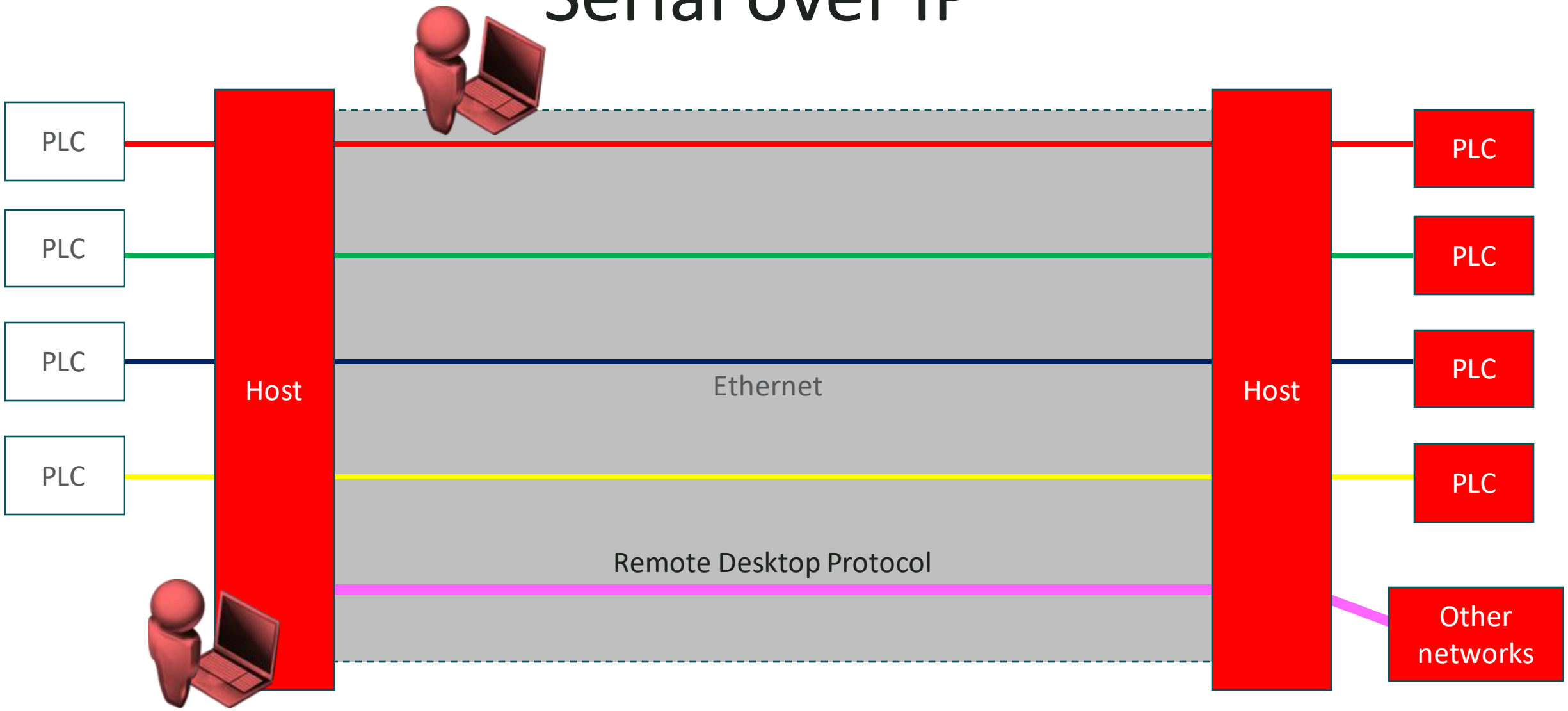
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

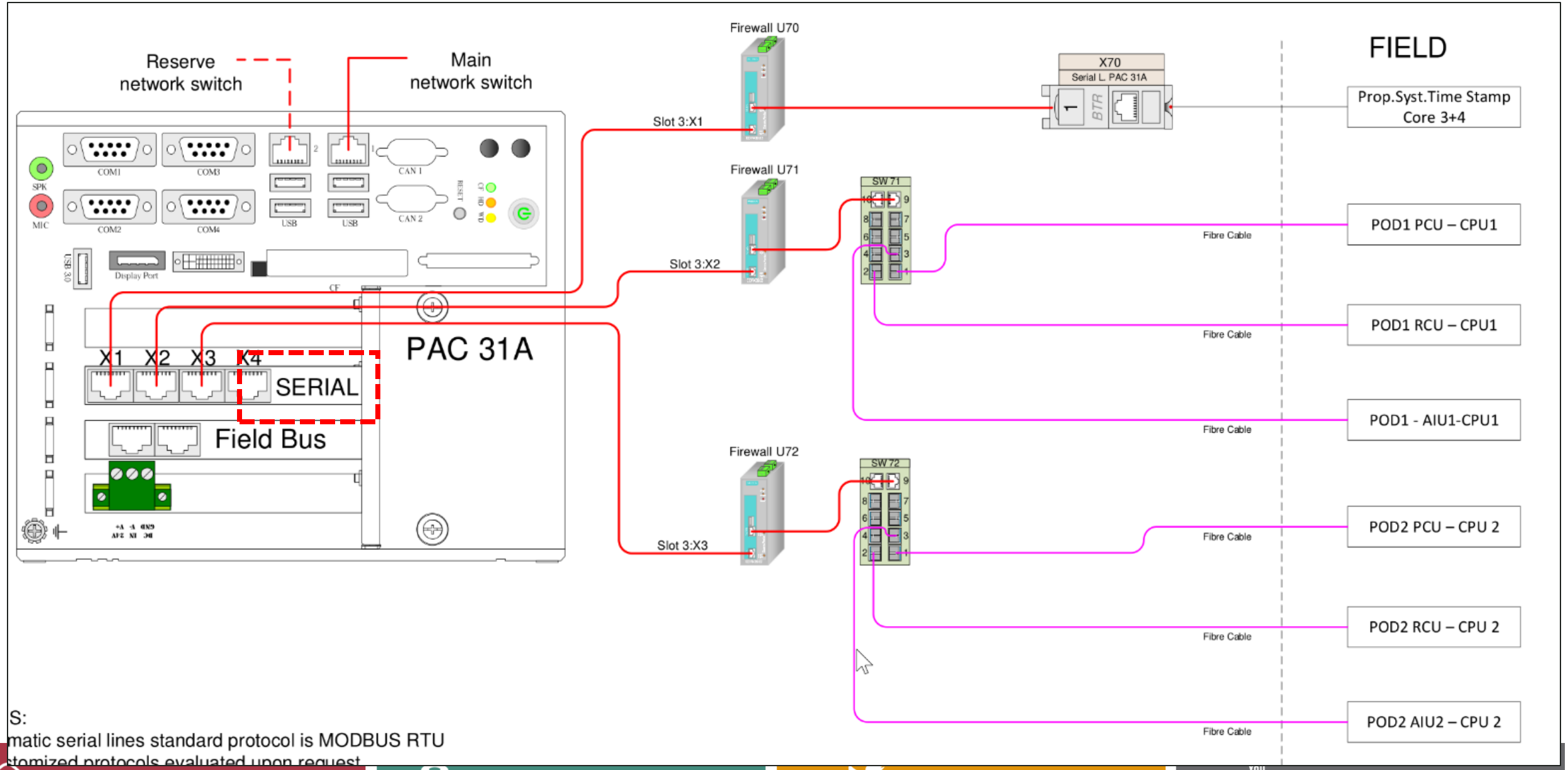
Serial over IP



info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP

Serial over IP





S:
matic serial lines standard protocol is MODBUS RTU
tomized protocols evaluated upon request

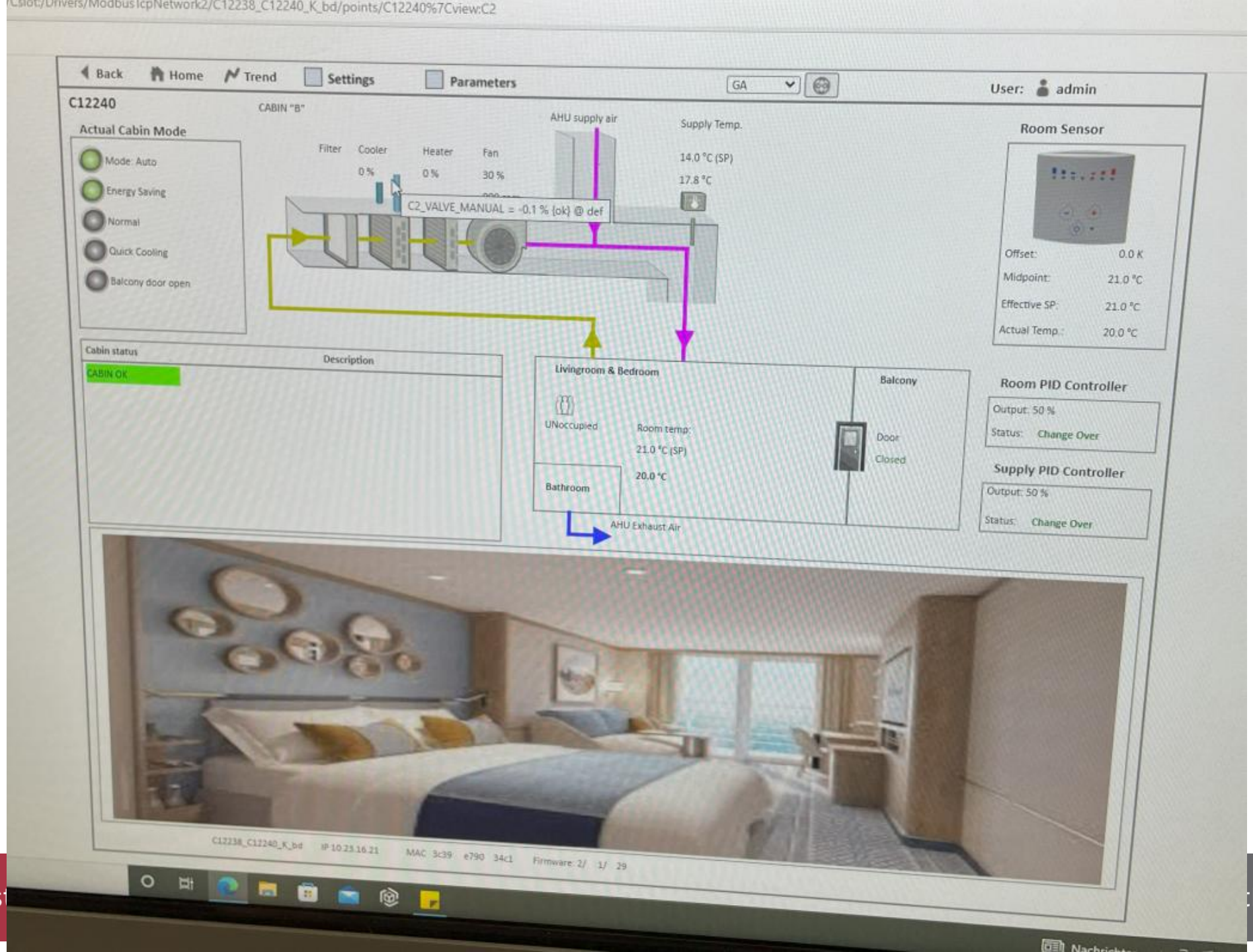
[redacted] - Remote Desktop Connection

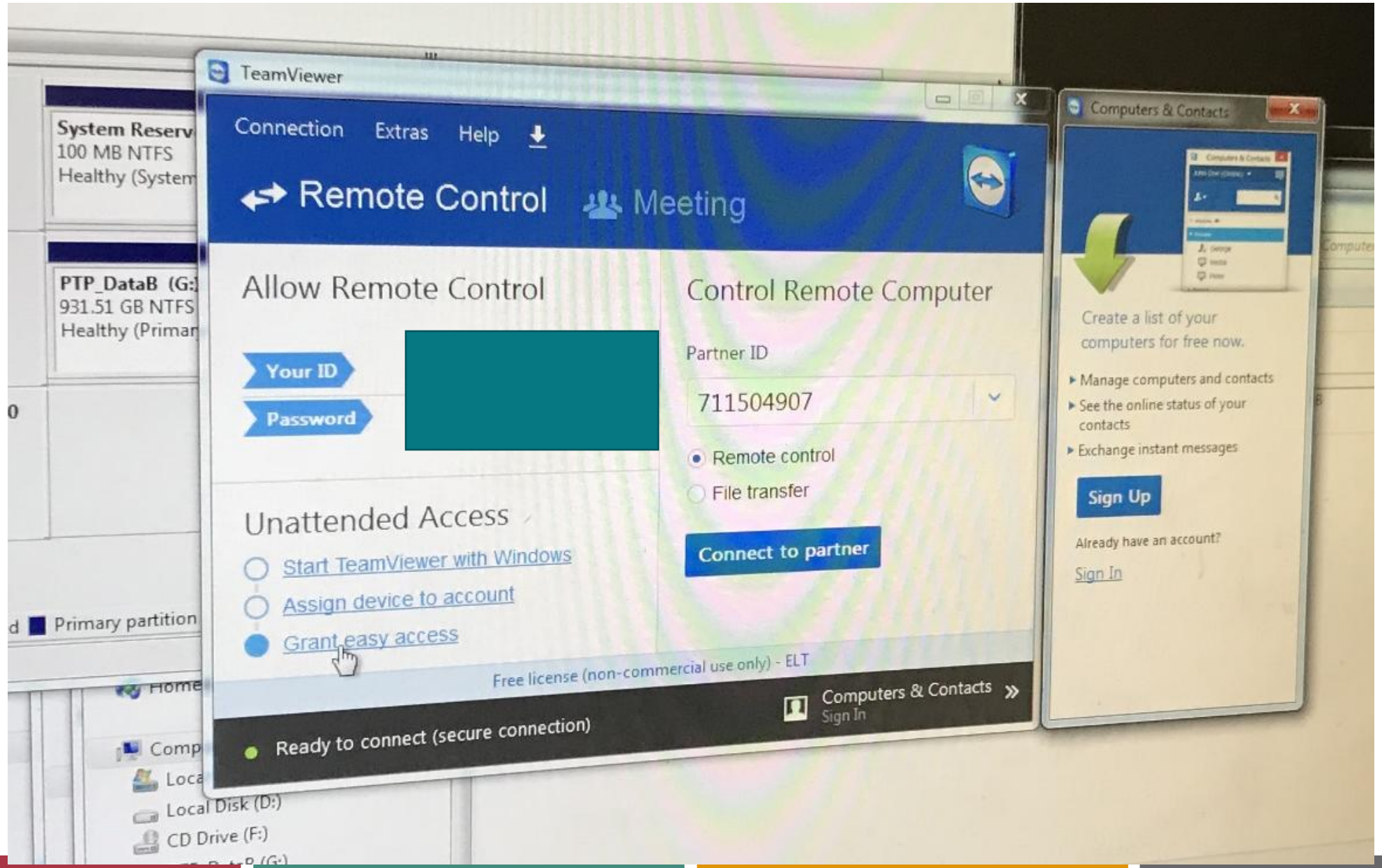
Select Administrator: CMD

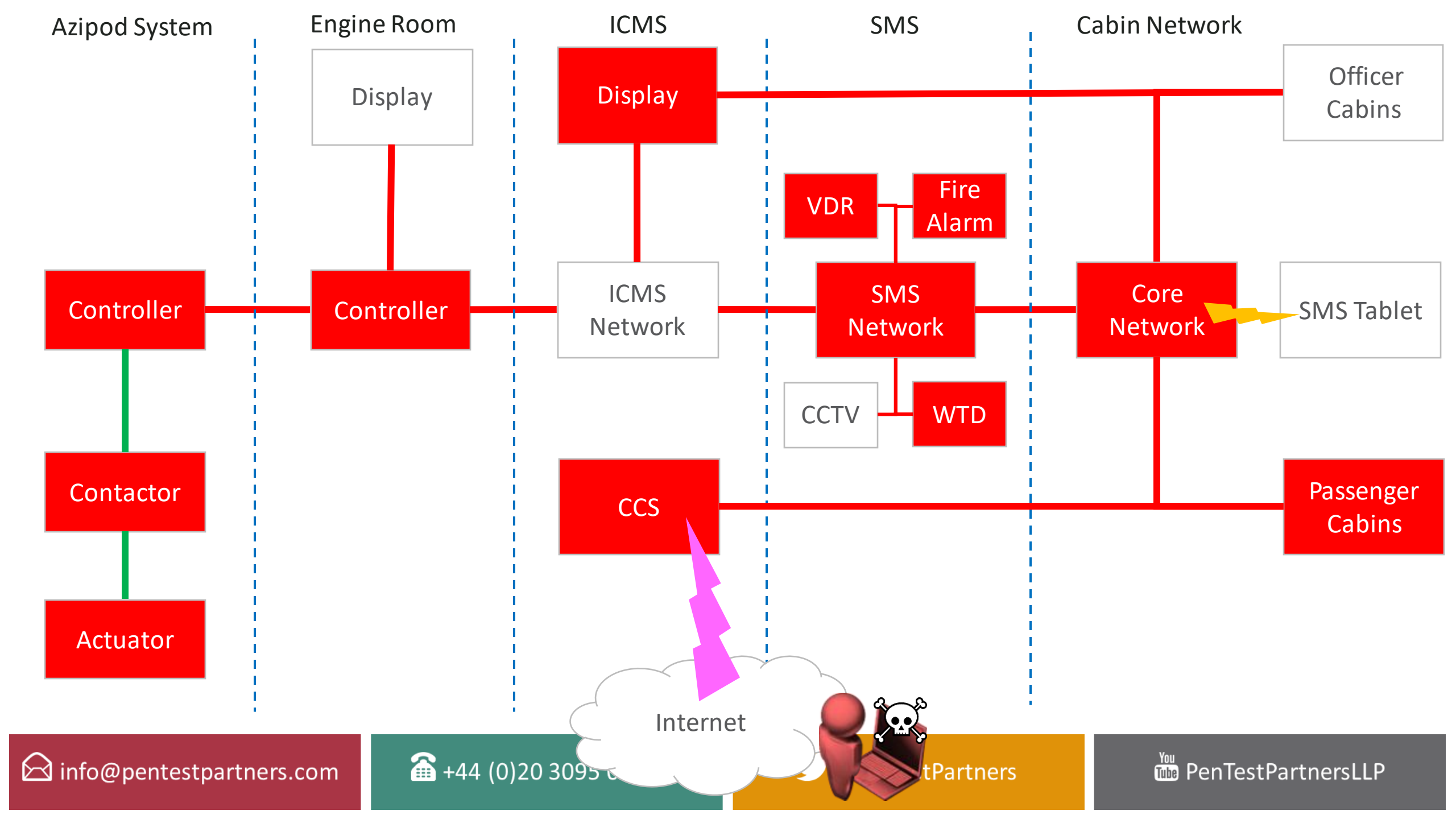
```
C:\Users\Operator>reg save hklm\security security.save
The operation completed successfully.

C:\Users\Operator>reg save hklm\system system.save
The operation completed successfully.

C:\Users\Operator>ipconfig

Windows IP Configuration


Ethernet adapter Fieldbus:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter POD2 PCU AIU2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2538:b70d:46e4:5907%16
   IPv4 Address. . . . . . . . . . . : 192.168.62.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter POD1 PCU AIU1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::44c1:e572:875e:9788%8
   IPv4 Address. . . . . . . . . . . : 192.168.61.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Prop Syst Time Stamp Core 3_4:
```

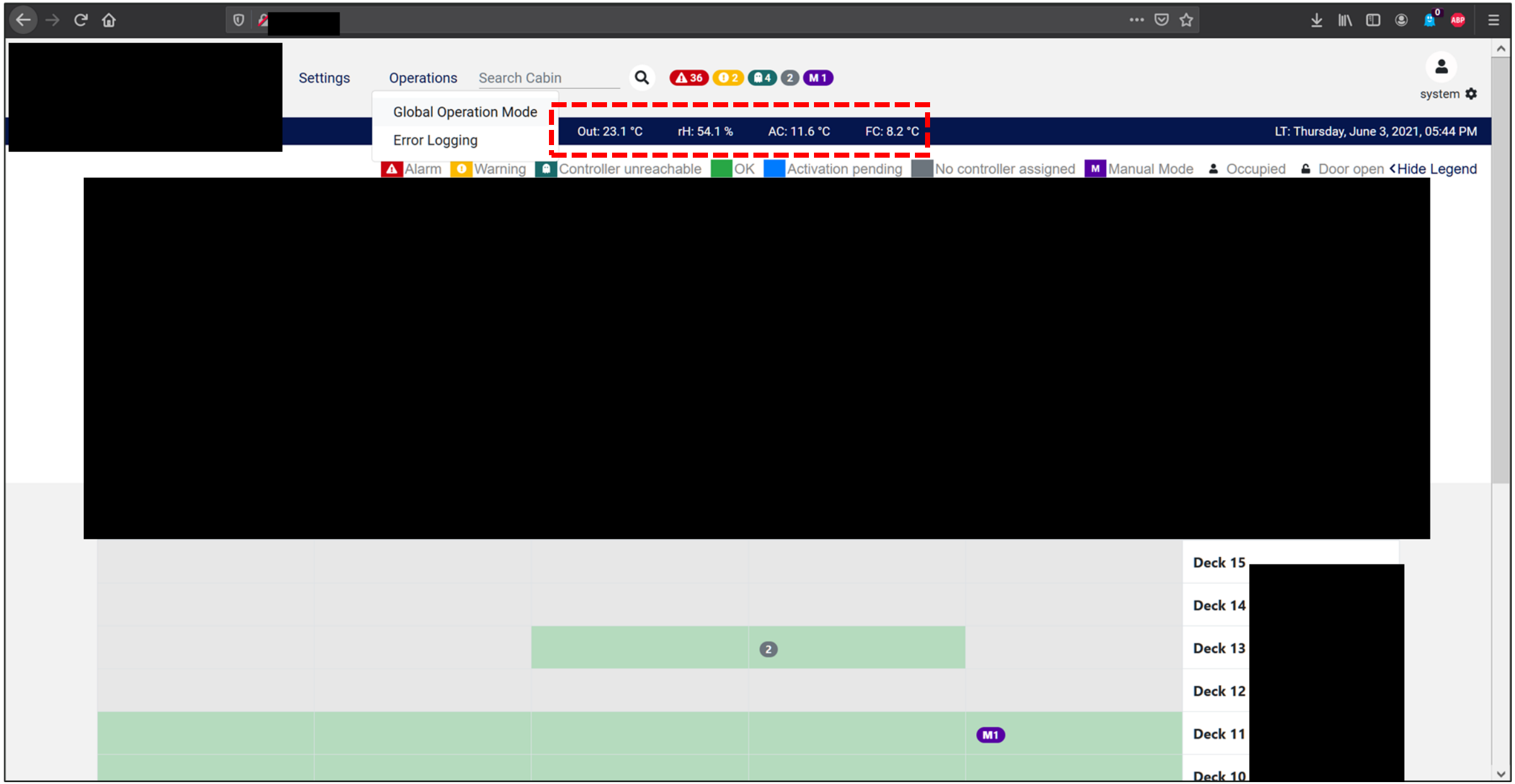
But you are still on the ship?

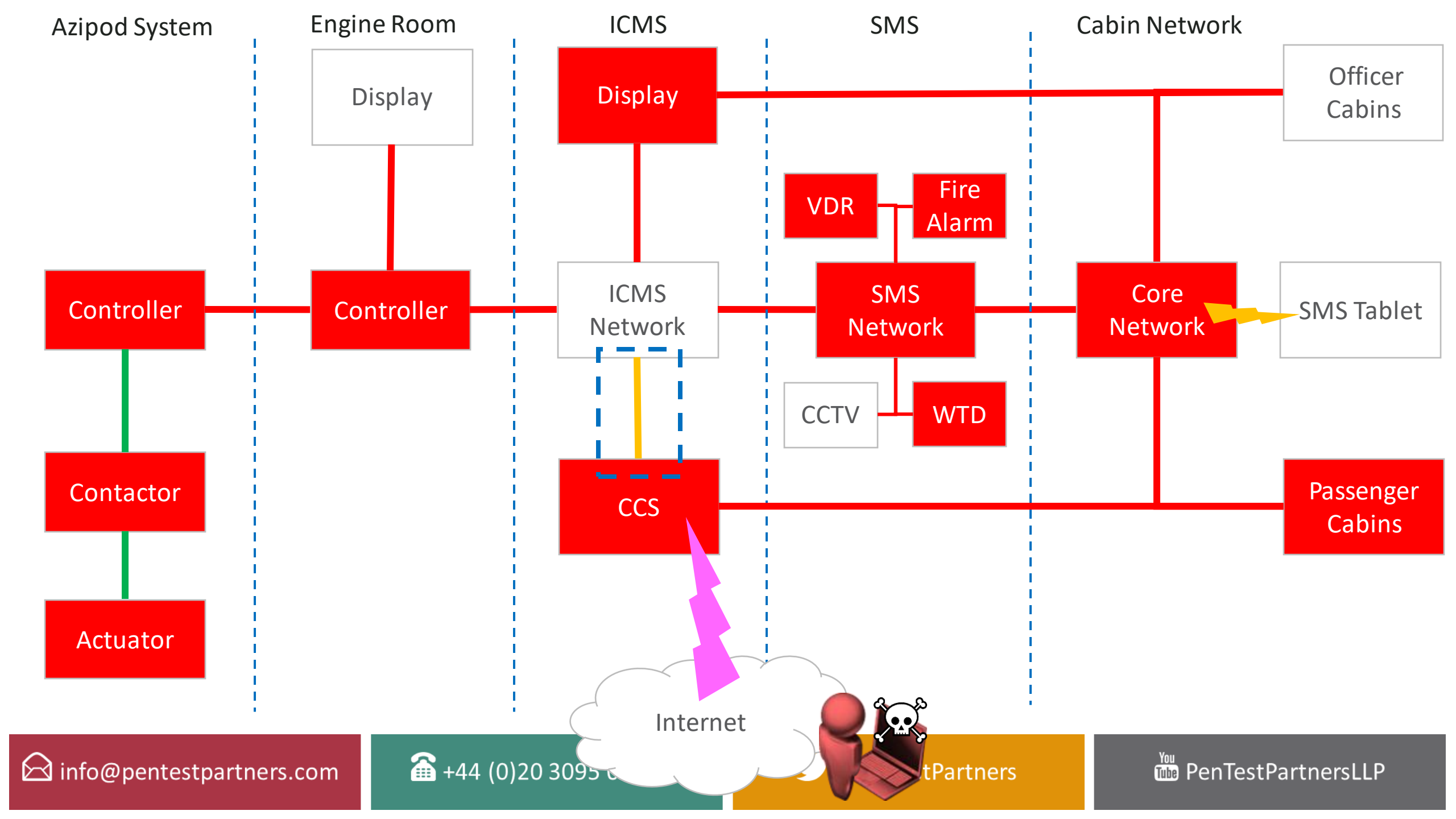
info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP


Back
Home
Trend
Settings
Parameters
GA
User: admin
C12240
CABIN "B"
Actual Cabin Mode
Mode: Auto
Energy Saving
Normal
Quick Cooling
Balcony door open
Filter
Cooler
Heater
Fan
0 %
0 %
30 %
AHU supply air
Supply Temp.
14.0 °C (SP)
17.8 °C
C2_VALVE_MANUAL = -0.1 % {ok} @ def
Room Sensor
Offset: 0.0 K
Midpoint: 21.0 °C
Effective SP: 21.0 °C
Actual Temp.: 20.0 °C
Cabin status
Description
CABIN OK
Livingroom & Bedroom
UNoccupied
Room temp:
21.0 °C (SP)
20.0 °C
Bathroom
AHU Exhaust Air
Balcony
Door
Closed
Room PID Controller
Output: 50 %
Status: Change Over
Supply PID Controller
Output: 50 %
Status: Change Over


TeamViewer
Connection
Extras
Help
Remote Control
Meeting
Allow Remote Control
Your ID
Password
Control Remote Computer
Partner ID
711504907
Remote control
File transfer
Connect to partner
Unattended Access
Start TeamViewer with Windows
Assign device to account
Grant easy access
Free license (non-commercial use only) - ELT
Ready to connect (secure connection)
Computers & Contacts
Sign In
Computers & Contacts
Create a list of your computers for free now.
Manage computers and contacts
See the online status of your contacts
Exchange instant messages
Sign Up
Already have an account?
Sign In
System Reserv
100 MB NTFS
Healthy (System
PTP_DataB (G:)
931.51 GB NTFS
Healthy (Primar
Primary partition
Local Disk (D:)
CD Drive (F:)

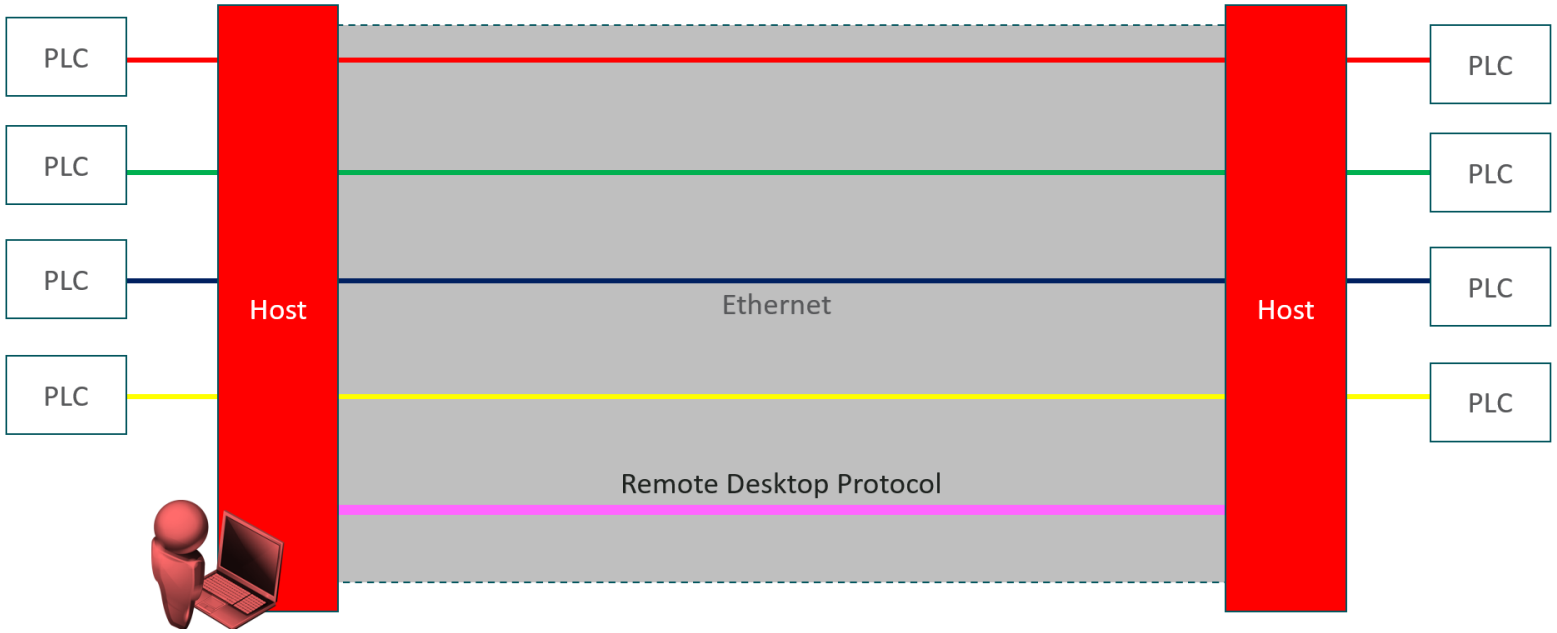

Azipod System
Engine Room
ICMS
SMS
Cabin Network
Display
Display
Officer Cabins
VDR
Fire Alarm
Controller
Controller
ICMS Network
SMS Network
Core Network
SMS Tablet
CCTV
WTD
Contactor
CCS
Passenger Cabins
Actuator
Internet
info@pentestpartners.com
+44 (0)20 3095
tPartners
PenTestPartnersLLP


Settings
Operations
Search Cabin
36
2
4
2
M 1
system
Global Operation Mode
Error Logging
Out: 23.1 °C
rH: 54.1 %
AC: 11.6 °C
FC: 8.2 °C
LT: Thursday, June 3, 2021, 05:44 PM
Alarm
Warning
Controller unreachable
OK
Activation pending
No controller assigned
Manual Mode
Occupied
Door open
Hide Legend
Deck 15
Deck 14
Deck 13
Deck 12
Deck 11
Deck 10
2
M1

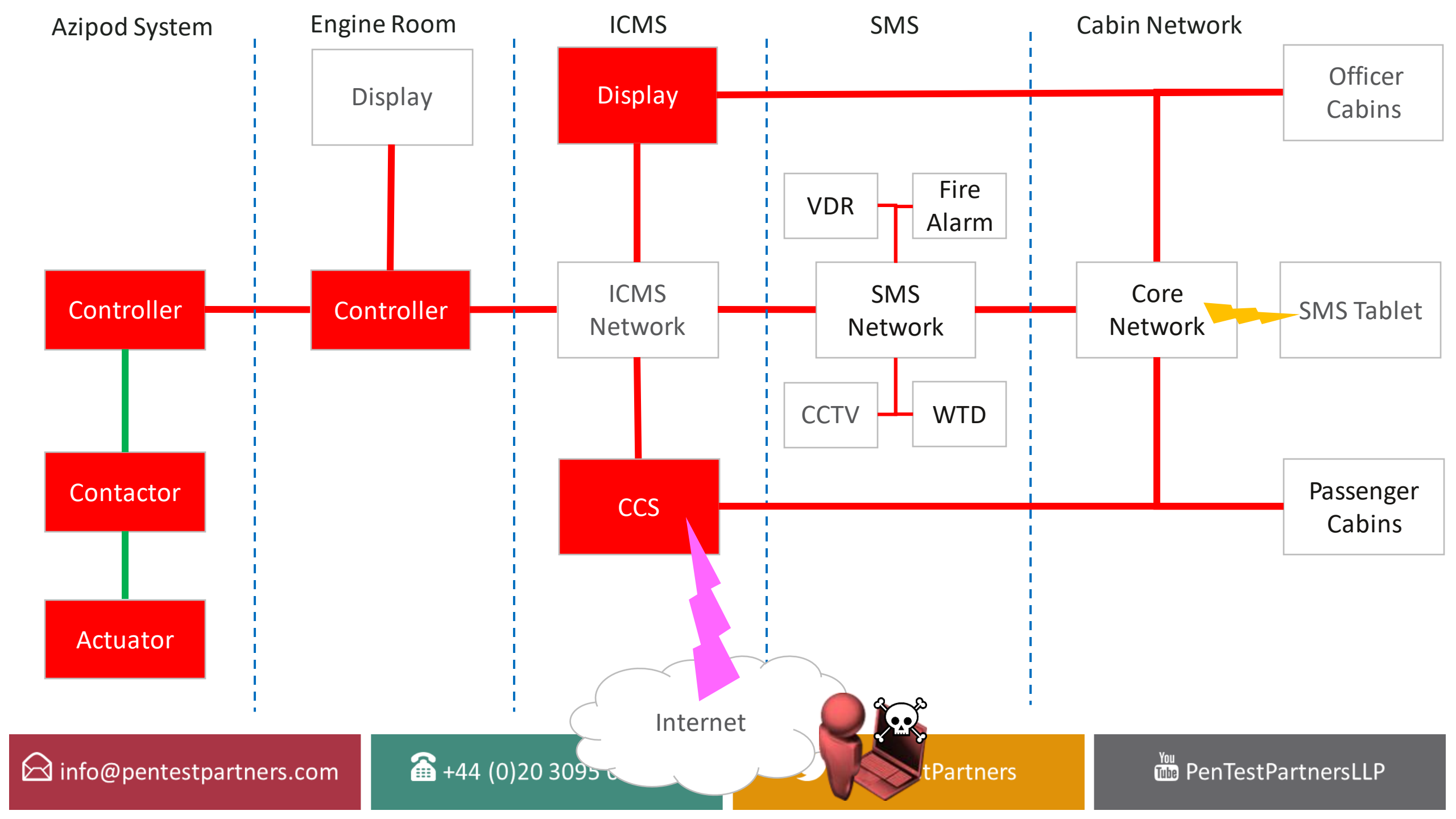

Azipod System
Engine Room
ICMS
SMS
Cabin Network
Display
Display
Officer Cabins
VDR
Fire Alarm
Controller
Controller
ICMS Network
SMS Network
Core Network
SMS Tablet
CCTV
WTD
Contactor
CCS
Passenger Cabins
Actuator
Internet
info@pentestpartners.com
+44 (0)20 3095
tPartners
PenTestPartnersLLP

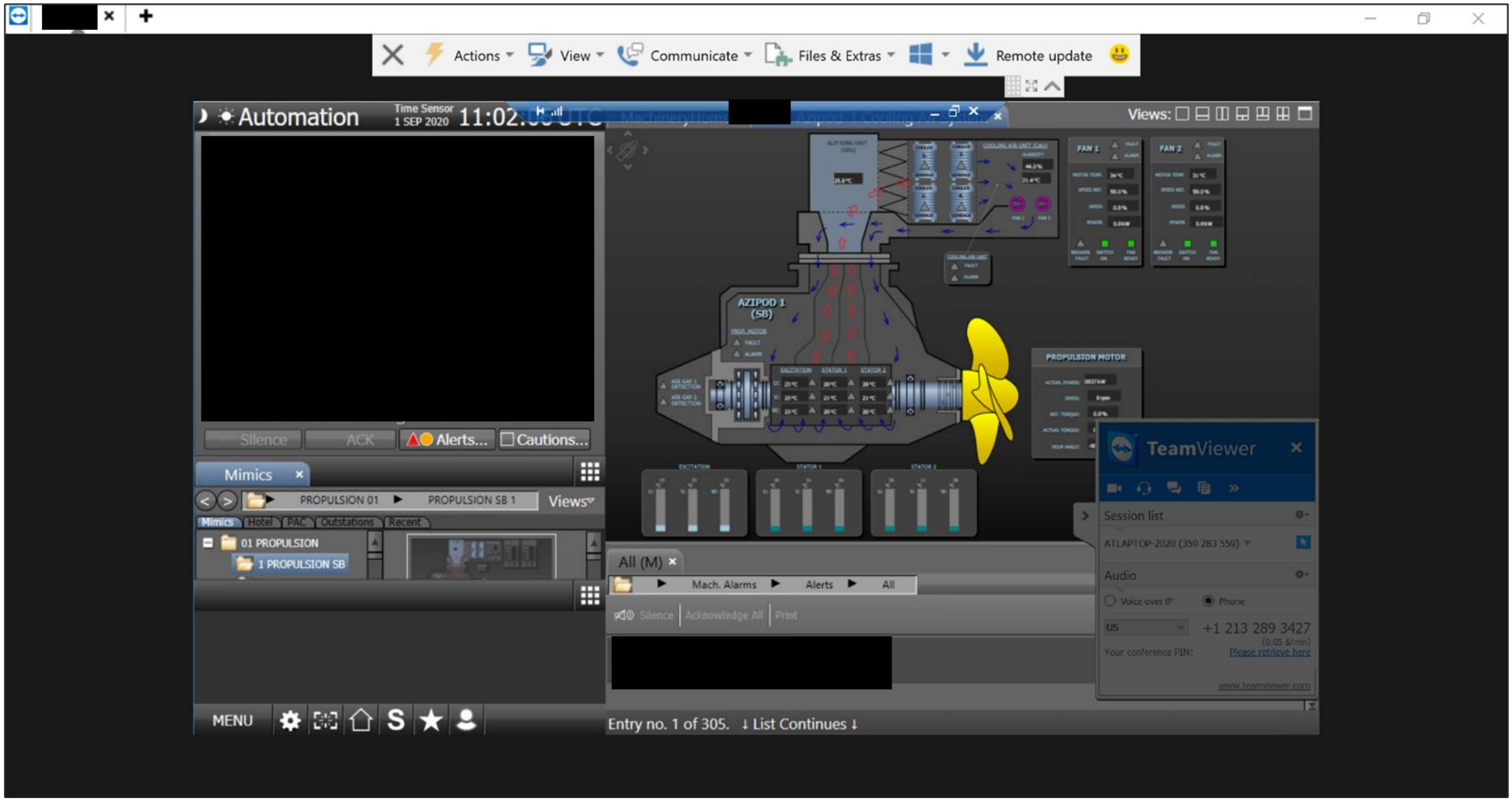
```
17:08:12 +00:21.064  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 250 1223 1175 1197 ... }
17:08:13 +00:22.064  0000 01 03 00 64 00 03 44 14                          ...d..D.
17:08:13 +00:22.064  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0064 N: 3
17:08:14 +00:22.150  0000 01 03 06 00 00 01 A4 00 00 61 6A                 .........aj
17:08:14 +00:22.150  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 0 420 0 }
17:08:15 +00:23.172  0000 01 03 00 68 00 4B 84 21                          ...h.K.!
17:08:15 +00:23.172  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0068 N: 75
17:08:15 +00:23.210  0000 01 03 96 01 40 00 46 01 7C 01 06 01 11 00 3F 00  ....@.F.|.....?.
17:08:15 +00:23.306  0010 FC 00 F1 01 1A 02 1F 01 E2 02 1B 02 0C 02 07 01  ................
                     0020 E9 02 0F 02 19 01 D5 01 DE 01 99 01 AB 01 9F 00  ................
                     0030 FF 00 E9 00 F7 02 A8 02 BB 02 A8 02 92 02 A8 02  ................
                     0040 A8 02 9C 02 9C 01 8F 01 CB 01 54 02 CF 02 D9 02  ........‘.T.ç.Ù.
                     0050 C5 02 CF 02 CF 02 CF 02 D9 02 D9 01 17 01 17 01  Å.ç.ç.ç.Ù.Ù.....
                     0060 17 02 A8 02 A8 02 A8 02 B2 02 A8 02 A8 02 A8 02  ................
17:08:15 +00:23.420  0070 92 01 0E 01 0E 01 0E 0E 22 0E 72 0E B8 0E EB 0E  ........".r...ë.
                     0080 B8 0E 91 0E C2 0E 72 12 51 12 2A 0F A9 0B 40 01  ......r.Q.*...©.
                     0090 46 01 48 01 44 00 00 FF FE 02 0C                 F.H.D......
17:08:15 +00:23.420  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 320 70 380 262 ... }
17:08:16 +00:24.421  0000 01 03 00 00 00 64 44 21                          .....dD!
17:08:16 +00:24.421  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0000 N: 100
17:08:16 +00:24.551  0000 01 03 C8 00 FA 04 C7 04 97 04 AD 02 44 01 3A 01  ..È...Ú.....D.:.
                     0010 C5 00 00 00 00 00 00 FF FF 00 00 00 1E 00 00 01  Å...............
                     0020 44 00 B4 01 46 01 48 01 44 01 00 04 2C 00 2B 00  D...F.H.D...,.+.
                     0030 48 00 32 01 04 02 F8 01 EA 02 F8 01 E0 03 16 01  H.2.....ê...Ö...
                     0040 FE 00 2B 01 06 01 02 01 07 01 B9 01 BD 01 BD 01  ..+.............
17:08:16 +00:24.665  0050 BF 01 BD 01 BB 01 C5 01 BA 01 AC 01 BF 01 BB 01  ......Å.........
                     0060 BE 00 96 00 7E 00 8F 01 EA 01 15 01 16 01 18 03  ....~...ê.......
                     0070 7B 03 73 03 76 03 74 03 79 03 80 03 77 03 7B 03  {.s.v.t.y...w.{.
                     0080 7B 03 67 03 77 03 76 03 76 00 F9 00 8C 00 8C 02  {.g.w.v.v.......
                     0090 62 02 E4 01 40 01 68 00 8C 00 8C 02 80 03 20 01  b.ä...h....... .
                     00A0 36 01 C2 00 96 00 BE 02 44 02 E4 01 4A 01 4A 01  6.......D.ä...J.
                     00B0 04 00 C8 02 F8 03 0C 01 4A 01 5E 01 47 01 49 01  ..È.....J.^.G.I.
17:08:16 +00:24.764  00C0 44 01 57 0B 09 00 00 00 00 01 7C AF 3F           D.W.......|.?
17:08:16 +00:24.764  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 250 1223 1175 1197 ... }
17:08:17 +00:25.765  0000 01 03 00 64 00 03 44 14                          ...d..D.
17:08:17 +00:25.765  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0064 N: 3
17:08:17 +00:25.838  0000 01 03 06 00 00 01 A4 00 00 61 6A                 .........aj
17:08:17 +00:25.838  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Reply) { 0 420 0 }
17:08:18 +00:26.838  0000 01 03 00 68 00 4B 84 21                          ...h.K.!
17:08:18 +00:26.838  [+] MODBUS-RTU Dev: 1 Fn: 3 Read Holding Registers (Request) Addr: 0x0068 N: 75
17:08:18 +00:26.913  0000 01 03 96 01 40 00 46 01 7C 01 06 01 11 00 3F 00  ....@.F.|.....?.
```

Serial over IP



info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP


Azipod System
Engine Room
ICMS
SMS
Cabin Network
Display
Display
Officer Cabins
VDR
Fire Alarm
Controller
Controller
ICMS Network
SMS Network
Core Network
SMS Tablet
CCTV
WTD
Contactor
CCS
Passenger Cabins
Actuator
Internet
info@pentestpartners.com
+44 (0)20 3095
tPartners
PenTestPartnersLLP


Actions
View
Communicate
Files & Extras
Remote update
Automation
Time Sensor
1 SEP 2020
Views:
AZIPOD 1
(SB)
FAN 1
FAN 2
PROPULSION MOTOR
Silence
ACK
Alerts...
Cautions...
Mimics
PROPULSION 01
PROPULSION SB 1
Views
Mimics
Hotel
PAC
Outstations
Recent
01 PROPULSION
1 PROPULSION SB
All (M)
Mach. Alarms
Alerts
All
Silence
Acknowledge All
Print
TeamViewer
Session list
ATLAPTOP-2020 (359 283 559)
Audio
Voice over IP
Phone
US
+1 213 289 3427
(0.05 $/min)
Your conference PIN:
Please retrieve here
www.teamviewer.com
MENU
Entry no. 1 of 305.
List Continues

Physical medium
Protocol
Data carried
Dependencies between systems

“Aligning the holes” by stopping systems working can have massive impact.

Increased crew workload can have devastating effects under the wrong conditions.

It is becoming impossible for crew to understand exactly how all systems work.

Understanding the data flows and dependencies between systems is vital for security.

Thanks!

Any questions?

Twitter: @cybergibbons

info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP