Internet auf See?
Cybersecurity auf Schiffen

(Ein)Blick in die Maritime IT

admeritia

Ihr Ansprechpartner

admeritia

Internet auf See?

(Ein)Blick in die Maritime IT

Und was das mit Security zu tun hat.

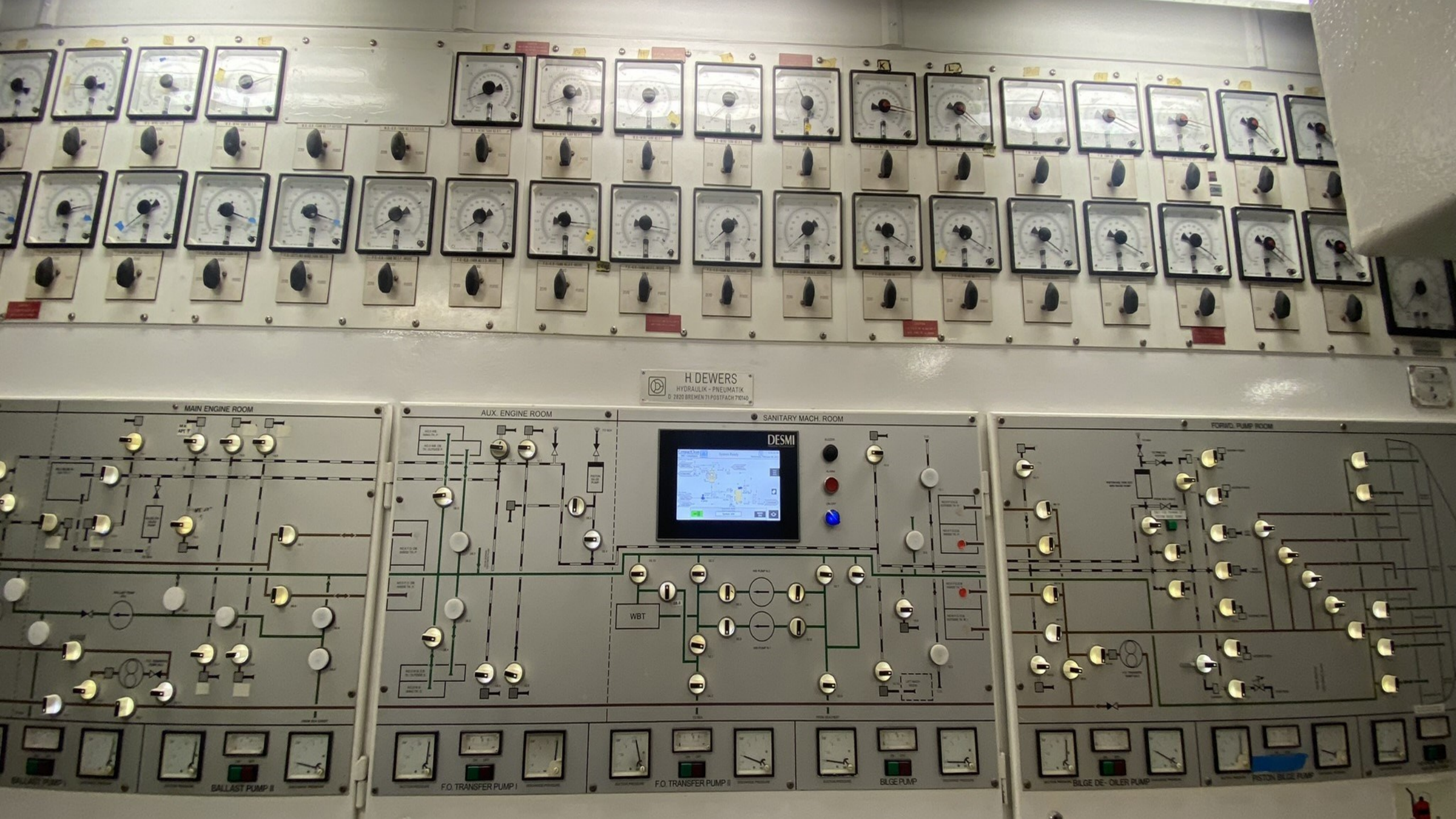
Stephan Gerling

OT Cyber Security Consultant

admeritia GmbH

stephan.gerling@admeritia.de

@ObiWan666


H. DEWERS
HYDRAULIK – PNEUMATIK
D 2820 BREMEN 71 POSTFACH 710140
MAIN ENGINE ROOM
AUX. ENGINE ROOM
SANITARY MACH. ROOM
FORW'D. PUMP ROOM
DESMI
WBT
BALLAST PUMP II
F.O. TRANSFER PUMP I
F.O. TRANSFER PUMP II
BILGE PUMP
BILGE DE - OILER PUMP
PISTON BILGE PUMP

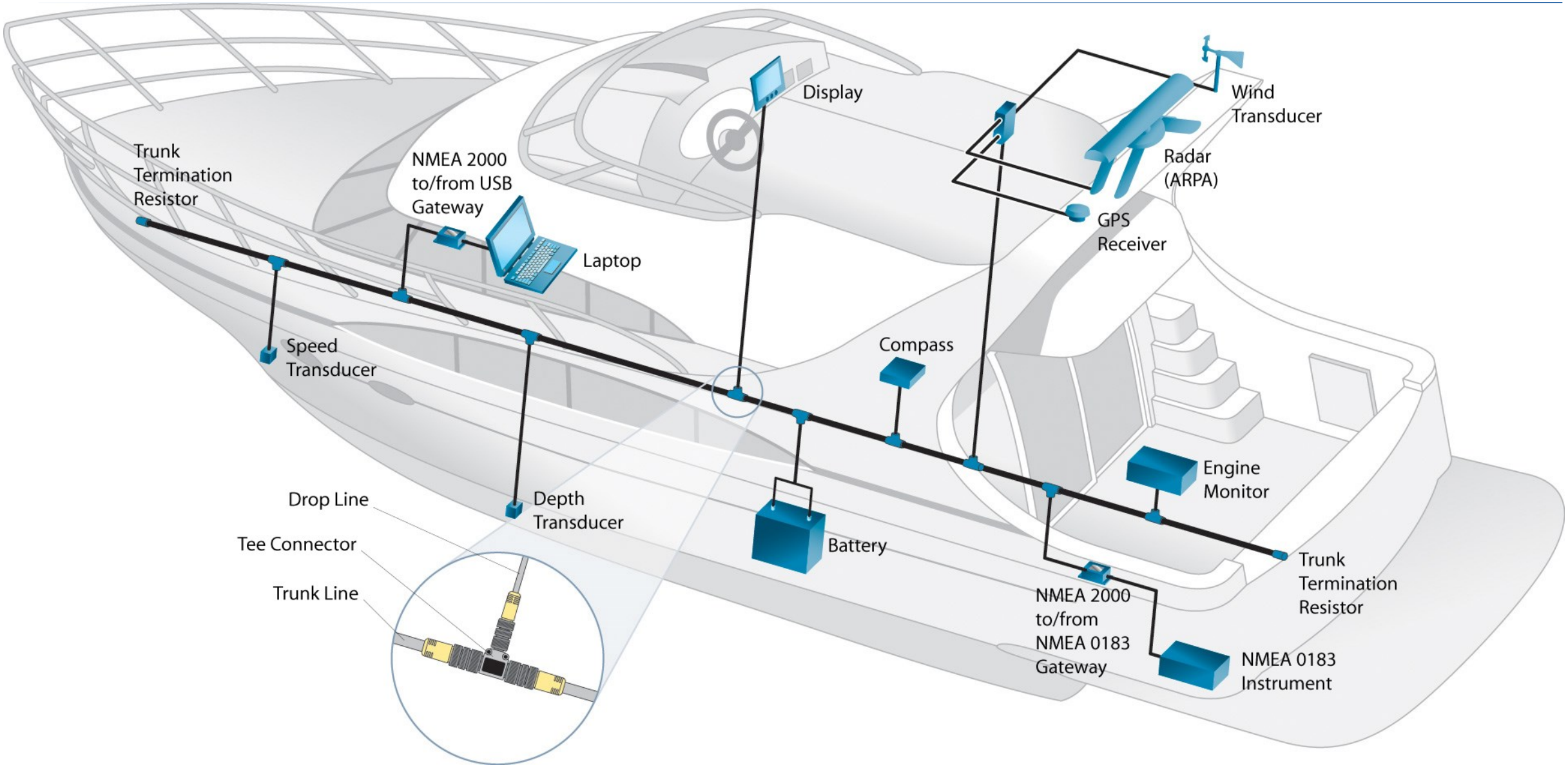
Ich liebe meinen Job

admeritia

Maritim	Radar – AIS – GPS – ECDIS – etc.
IT	Crew – Gäste - Owner – Office-IT Entertainment (Audio-Video)
OT	Antrieb – Steuerung – Energie – Stabilizer – Spezial Equipment

erster Überblick

admeritia

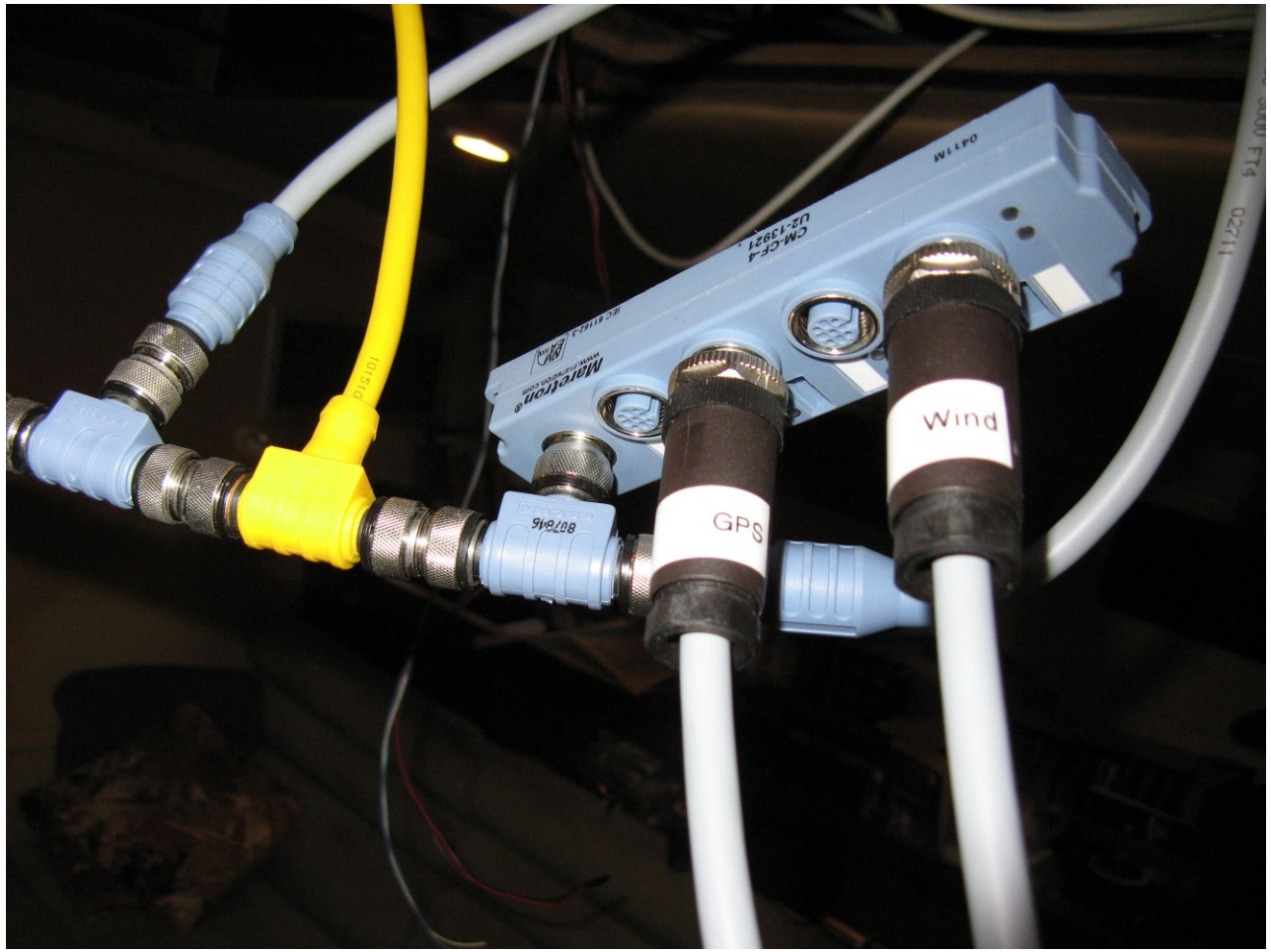


admeritia

Verkabelung

- NMEA 0183 - seriell
- NMEA 2000 – SAE J1939

Farbe	Name	Spannung	Funktion
weiß	CAN-High	+ 2,5V	Signal
blau	CAN-low	- 2,5V	Signal
metallisch	-		Abschirmung
rot	V+	+ 12V	Spannungsversorgung
schwarz	V-	0V	Spannungsversorgung



Satcom

admeritia

Satcom

- Offshore internet via SATCOM
- Problem Patching?
- Viele “vulnerable” Geräte immer noch Online
- Wird vermehrt durch STARLINK ersetzt
- WiFi to shore bis >15NM möglich

admeritia

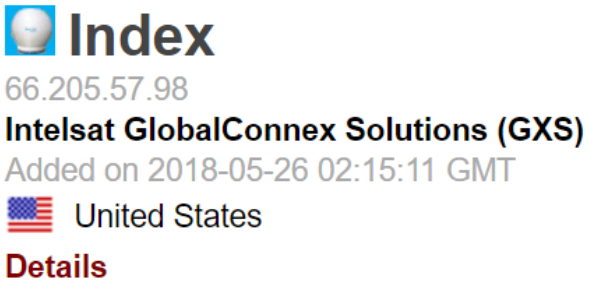
Online suche auf Shodan.io

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

admeritia

Oh, was hab ich den hier?

“stabilized Digital Antenna System”




```
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
```

- “Cobham Seatel MXP Webserver”
- Optimierter Suchbegriff: “Server: Micro Digital Webserver”

Search “Server: Micro Digital Webserver”

admeritia

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

TOP ORGANIZATIONS

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
```

Index

Frage:

Was sind die wichtigsten Tools eines Angreifers?

Antwort:

- Benutzerhandbuch
- F12 oder “view source” im Browser

RTFM

Im Handbuch steht:”username” & “password”

- Dealer: seatel3
- SysAdmin: seatel2
- User: seatel1

admeritia

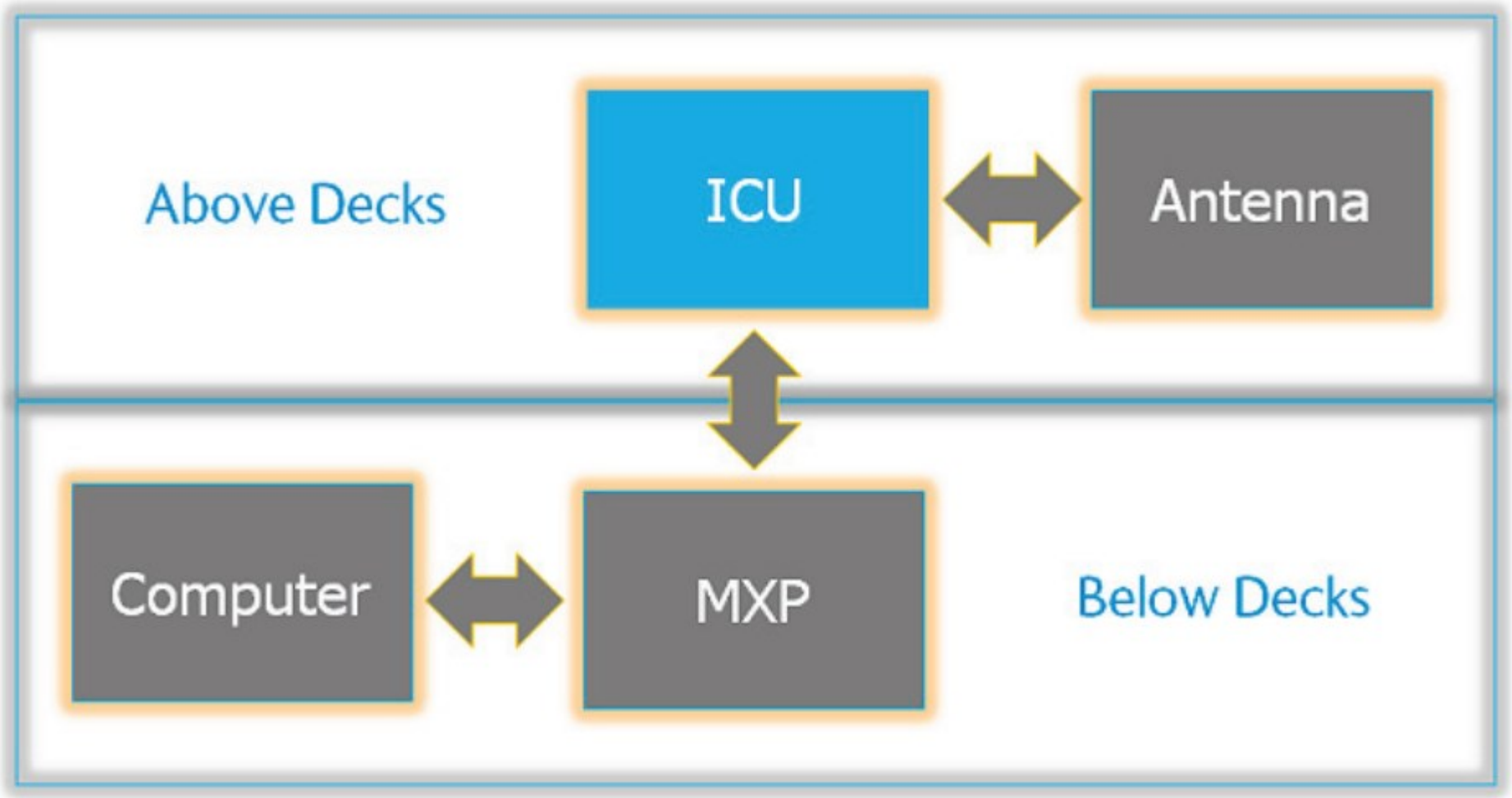
Login Seite mit F12 oder “view source” anschauen:

/js/userLogin.js

```
if(t=="Dealer"){if(r=="true"){e="MenuDealerGx.html"}else{e="MenuDealer.html"}}else
if(t=="SysAdmin"){if(r=="true"){e="MenuSysGx.html"}else{e="MenuSys.html"}}else
if(t=="User"){if(r=="true"){e="MenuEuNCGx.html"}else{e="MenuEuNC.html"}}
```

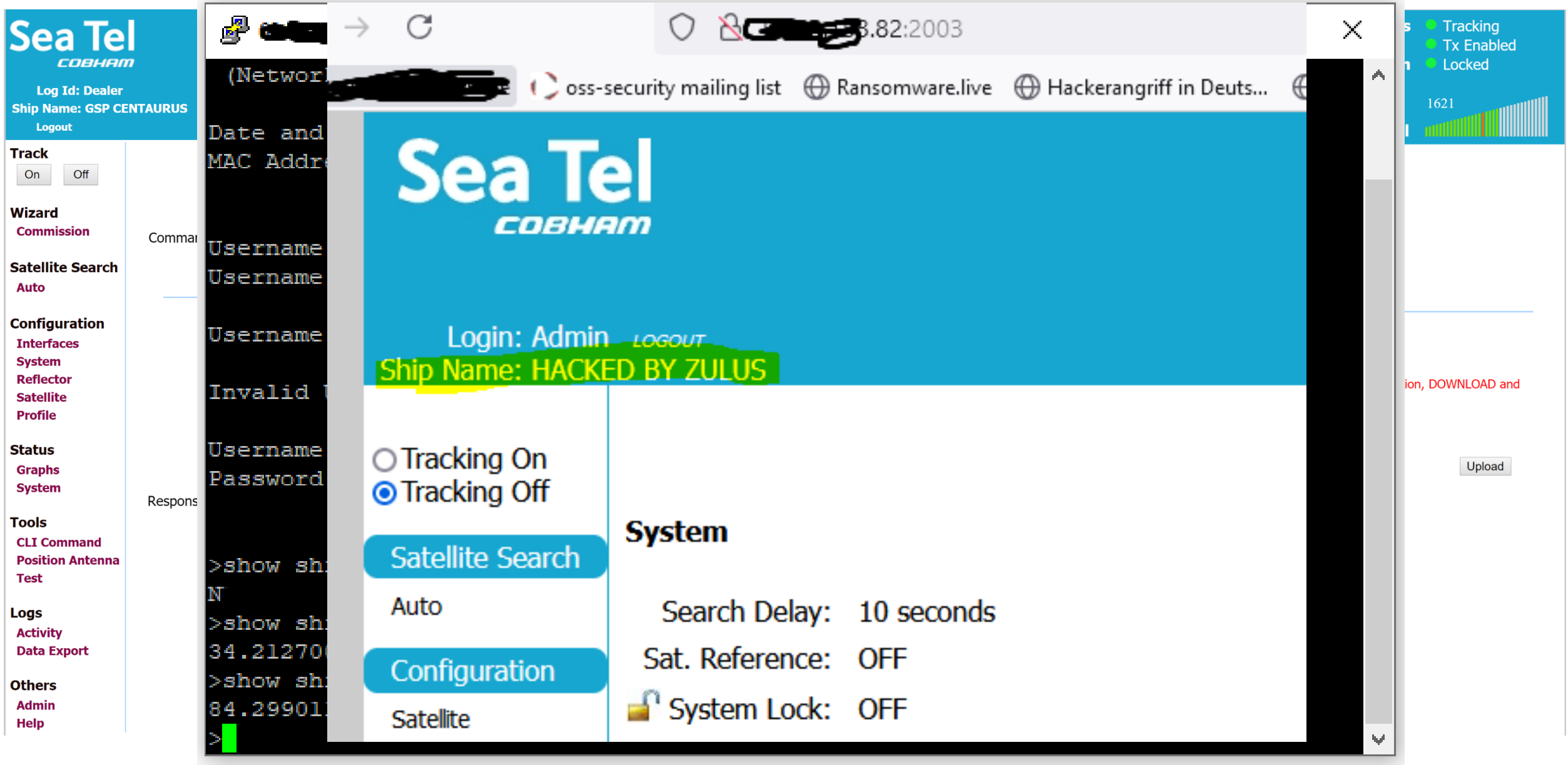
SatCom

admeritia



Cobham Seatel Satcom

admeritia



admeritia

CVE-2018-16114
- Auth bypass in Cobham Seatel
Patch verfügbar

“Cobham_seatel_inifile-dump.py”
auf meinem Github verfügbar:
https://github.com/ObiWan666/maritime

```
[SATELLITE_FAV:0]
DESCRIPTION = INOVSAT
LON = 22.0 W
FREQ = 1328.737
SKEW = 0.0
BAND = 2
TX_POL = V
SEARCH_PATTERN = SPIRAL
REFLECTOR = PRIMARY_REFLECTOR
LNB = XPOL
# ****************ICU1 INI************
# ************************************
# IMPORTANT: DO NOT MODIFY THIS SECTION
[REVISION]
INI_MAJOR = 1
INI_MINOR = 2
INI_TIMESTAMP = 2675566445
# ************************************

[HARDWARE]
TYPE = ICU

[VERSION]
MXP = 179 (Build:224945)
MXP_BUILD_DATE = Dec 15 2017, 11:03:06
ICU = 179 (Build:224945)
ICU_BUILD_DATE = Dec 15 2017, 11:03:06
MDB_RUNNING = 2.07
```

admeritia

Locomarine Yachtrouter

- High power WIFI Booster for long distance connectivity (15+ NM)
- High power 4G/3G/2G module (30+ Nautical miles)

The control software (PC/Android/iOS)

admeritia

The control software

admeritia

- App nutzt FTP
- Download “YachtRouterGen3.xml
- Änderungen in dieser XML
- FTP upload
- Hardcoded credentials!!!
- WLAN SSID und Password in XML

344	98.416854	10.80.0.1	10.81.255.254	FTP	109	Response: 220 YachtRouterMiniB FTP server (MikroTik 6.24) ready
345	98.418233	10.81.255.254	10.80.0.1	FTP	65	Request: USER loco
346	98.418601	10.80.0.1	10.81.255.254	TCP	60	21→21418 [ACK] Seq=56 Ack=12 Win=14600 Len=0
347	98.418976	10.80.0.1	10.81.255.254	FTP	86	Response: 331 Password required for loco
348	98.419067	10.81.255.254	10.80.0.1	FTP	81	Request: PASS SecureConnectingUser
349	98.451857	10.80.0.1	10.81.255.254	TCP	60	21→21418 [ACK] Seq=88 Ack=39 Win=14600 Len=0

Firmware enthält Passwort

admeritia

```
static yrEngine()
{
  yrEngine.RouterConfig_Username = "loco";
  yrEngine.RouterConfig_Password = "SecureConnectingUser";
  yrEngine.RouterConfig_FtpPath = "ftp://10.80.0.1/YachtRouterGen3.xml";
  yrEngine.RouterSupportInfo_FtpPath = "ftp://10.80.0.1/SupportInfo.png";
  yrEngine.extenderIdentity = "YR_WIFI_EXTENDER";
  yrEngine.rootExtenderDHCPServer = "dhcpBACKBONE";
  yrEngine.bridgePrefix = "bridgeEoip_";
  yrEngine.routingMarkPrefix = "markAlwaysON_";
  yrEngine.virtualApPrefix = "wifiAlwaysON_";
  yrEngine.virtualApSecurityProfilePrefix = "SecurityProfile_";
  yrEngine.eoipTunnelPrefix = "eoipTunnel_";
  yrEngine.shipPhysicalWifiInterface = "shipPhysical";
  yrEngine.defaultPassword = "12345678";
  yrEngine.rootIpAddress = "10.90.";
```

Und es kommt noch schlimmer!

NMAP scan on the puplic IP

- Router os= Mikrotik Router OS
- Winbox Management 8291/TCP
- API access of the Yachtrouter exe 8728/TCP (API)

- Portscan from Internet:
- PORT STATE SERVICE
- 21/tcp open ftp
- 22/tcp open ssh
- 53/tcp open domain
- 2000/tcp open cisco-sccp
- 8291/tcp open unknown

Remote support

admeritia

Yacht Router model & serial nun

How do they know the IP addres

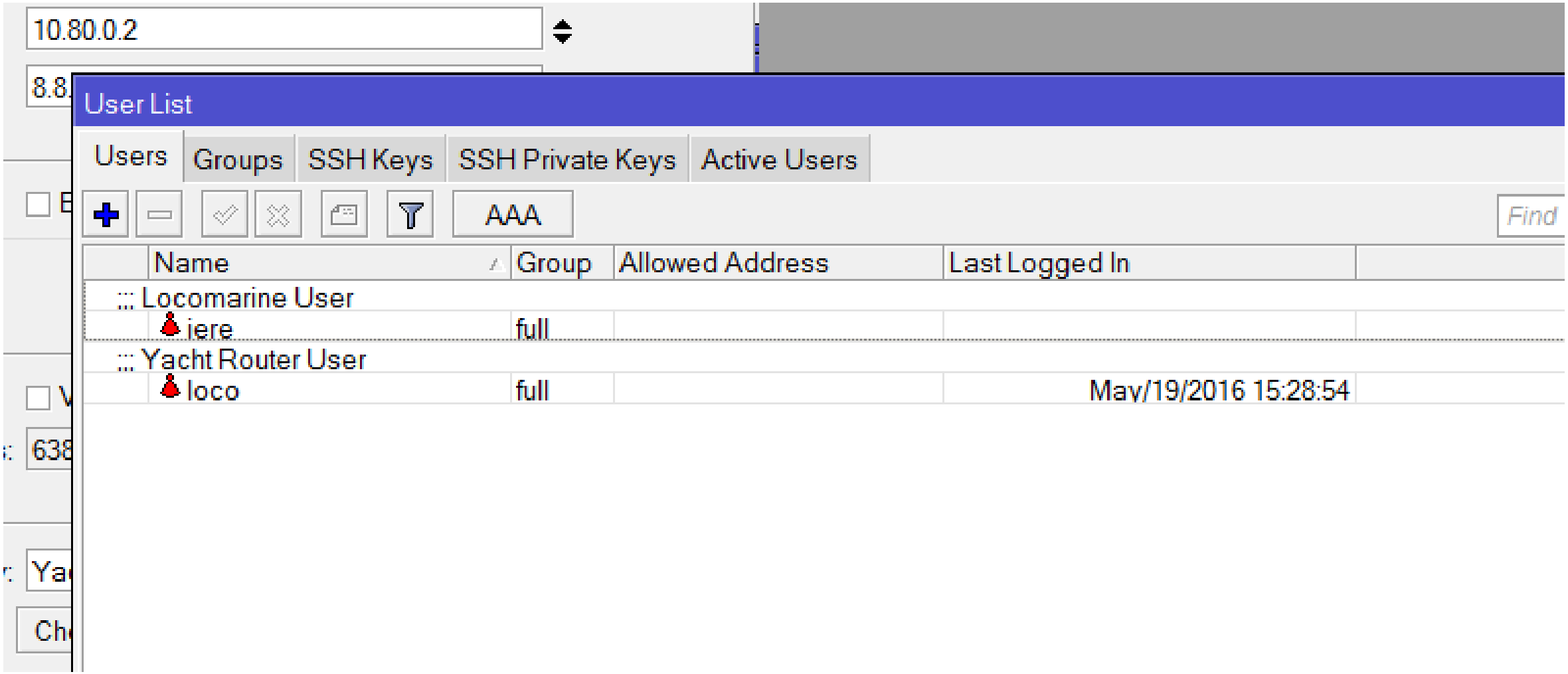
```
or=0
..!done../ping.=address=5.10.88.130.=count=5..!r
et-loss=100..!re.=seq=1.=status=no route to hos
 host.=sent=3.=received=0.=packet-loss=100..!re.
```

Whois IP 5.10.88.130

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" fla

% Information related to '5.10.88.128 - 5.10.88.135'

% Abuse contact for '5.10.88.128 - 5.10.88.135' is 'abuse@softlay

inetnum:        5.10.88.128 - 5.10.88.135
netname:        NETBLK-SOFTLAYER-RIPE-CUST-BO1663-RIPE
descr:          LOCOMARINE DOO
country:        HR
admin-c:        BO1663-RIPE
tech-c:         BO1663-RIPE
status:         ASSIGNED PA
mnt-by:         MAINT-SOFTLAYER-RIPE
created:        2013-07-25T18:27:47Z
last-modified:  2013-07-25T18:27:47Z
source:         RIPE
```

Issue #4 – Winbox Management

admeritia



Issue #4 – Winbox Management Cracking

admeritia

MKBRUTUS v1.0.0

Password bruteforcer for MikroTik devices or boxes running RouterOS
Site: https://github.com/mkbrutusproject/MKBRUTUS

Or use CVE-2018-14847 (works on Mikrotik 6.42 or below)
https://github.com/BigNerd95/WinboxExploit

$ python3 WinboxExploit.py 192.168.0.1

- User: the user
- Pass: StrengGeheim

Vendor response

admeritia

- Security issues reported in June 2017 to vendor
- 2 bugs intensely fixed
- New Apps and router firmware versions were developed
- In November finaly released
- Permission from vendor to present
- CVE-2017-17673 requested

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17673

Hersteller Patch

admeritia

- Hersteller hat die Lücken geschlossen

Und was genau wurde gemacht?

- .Net application ist nun obfuskiert
- FTP wurde durch SSH ersetzt

WTF - Security by obscurity – wirklich?

Obfuscated code

admeritia

```
ICSharpCode.Decompiler.DecompilerException: Error decompiling System.String YR.Core.yrEngine/MyUserInfo::getPassword()
 ---> System.NullReferenceException: Object reference not set to an instance of an object.
   at ICSharpCode.Decompiler.CecilExtensions.GetPopDelta(Instruction instruction, MethodDefinition methodDef)
   at ICSharpCode.Decompiler.ILAst.ILAstBuilder.StackAnalysis(MethodDefinition methodDef)
   at ICSharpCode.Decompiler.ILAst.ILAstBuilder.Build(MethodDefinition methodDef, Boolean optimize, DecompilerContext context)
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(IEnumerable`1 parameters)
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(MethodDefinition methodDef, DecompilerContext context, IEnumera
   --- End of inner exception stack trace ---
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(MethodDefinition methodDef, DecompilerContext context, IEnumera
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateMethod(MethodDefinition methodDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddTypeMembers(TypeDeclaration astType, TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateType(TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddTypeMembers(TypeDeclaration astType, TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateType(TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddType(TypeDefinition typeDef)
   at ICSharpCode.ILSpy.CSharpLanguage.DecompileType(TypeDefinition type, ITextOutput output, DecompilationOptions options)
   at ICSharpCode.ILSpy.TextView.DecompilerTextView.DecompileNodes(DecompilationContext context, ITextOutput textOutput)
   at ICSharpCode.ILSpy.TextView.DecompilerTextView.<>c__DisplayClass31_0.<DecompileAsync>b__0()
```

Da war doch noch was…..

admeritia

```
// YR.Core.yrEngine
using ...

public class yrEngine
```

```
RouterConfig_Username = "loco";
```

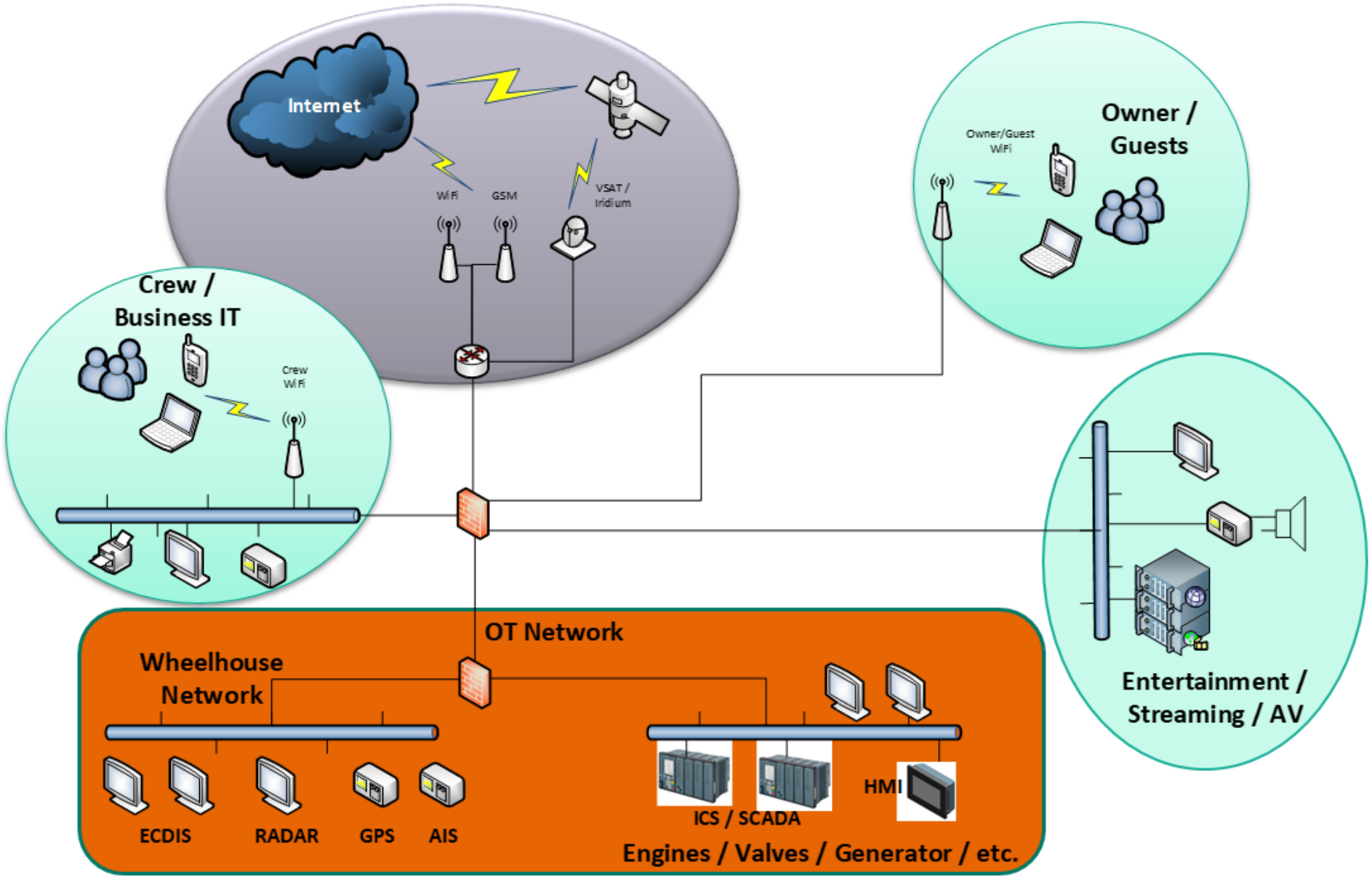
```
RouterConfig_Password = "ySyteMJwWuyAyMu84D";
```

```
public static string RouterConfig_FtpPath = "ftp://10.80.0.1/YachtRouterGen3.xml";

public static string RouterSupportInfo_FtpPath = "ftp://10.80.0.1/SupportInfo.png";

public static string extenderIdentity = "YR_WIFI_EXTENDER";

public static string rootExtenderDHCPServer = "dhcpBACKBONE";

public static string bridgePrefix = "bridgeEoip_";
```

Zusammenfassend

admeritia

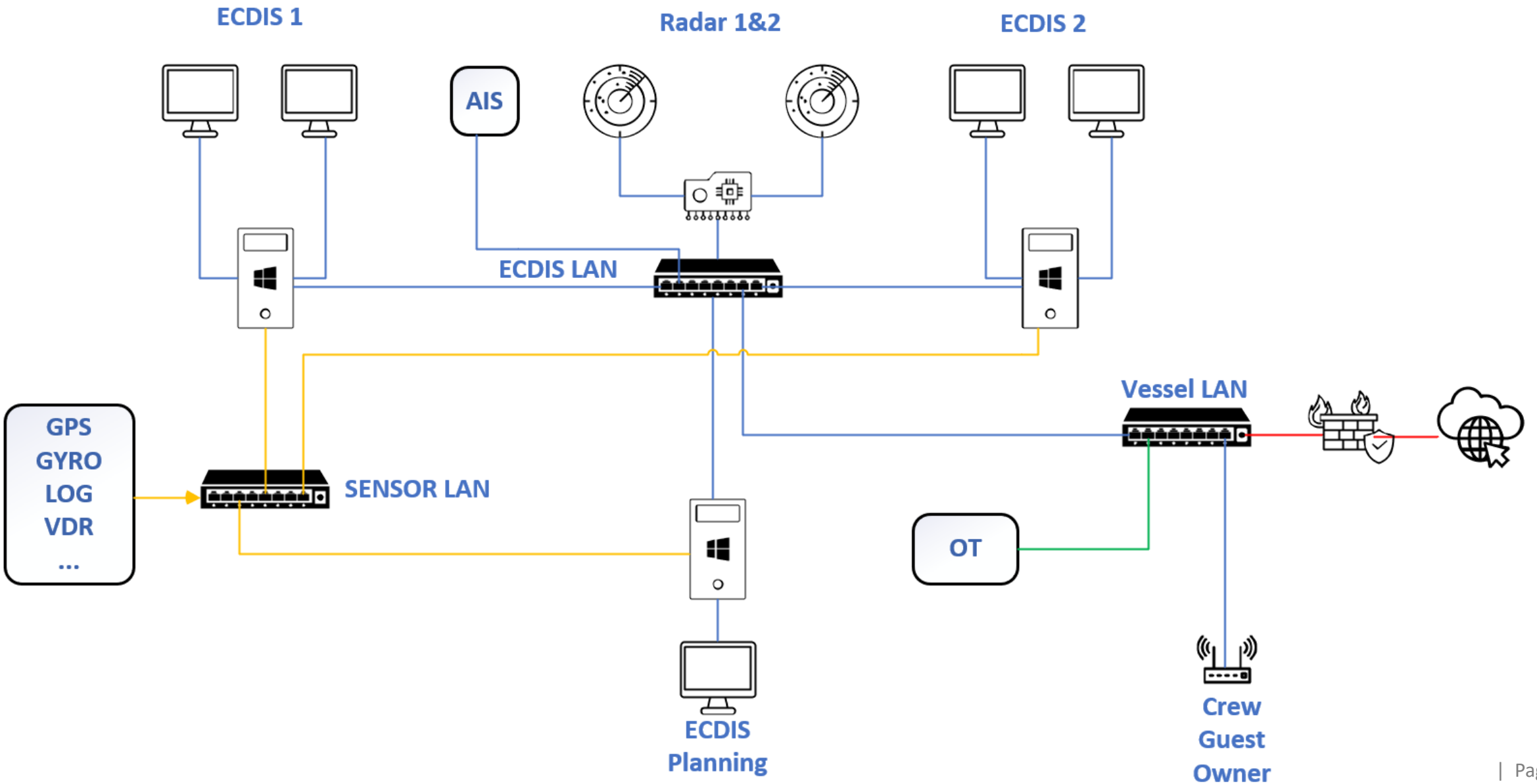
- SSH ersetzt FTP - gut
- Obfuscated Exe + DLL in Windows Version - schlecht
- Android APK not obfuscated - schlecht
- iOS Version nicht getested
- Hardcoded credentials in yrEngine - schlecht
- Aus dem Internet SSH & Winbox offen - schlecht


Internet
Wi Fi
GSM
VSAT / Iridium
Owner / Guests
Owner/Guest WiFi
Crew / Business IT
Crew Wi Fi
Entertainment / Streaming / AV
OT Network
Wheelhouse Network
ECDIS
RADAR
GPS
AIS
ICS / SCADA
HMI
Engines / Valves / Generator / etc.

Ein Blick hinter die Kulisse

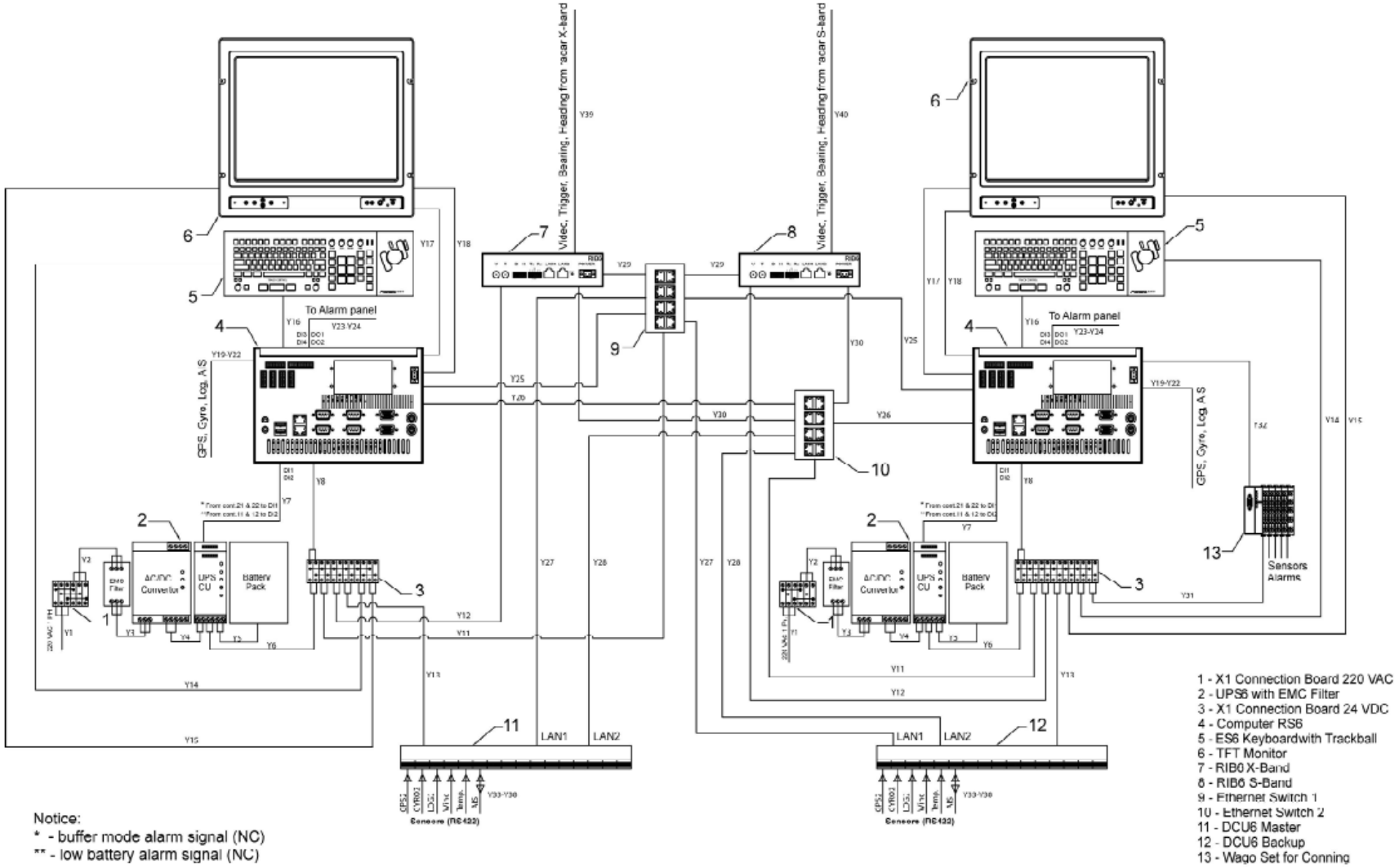
Electronic Chart Display - ECDIS

Navigationssysteme



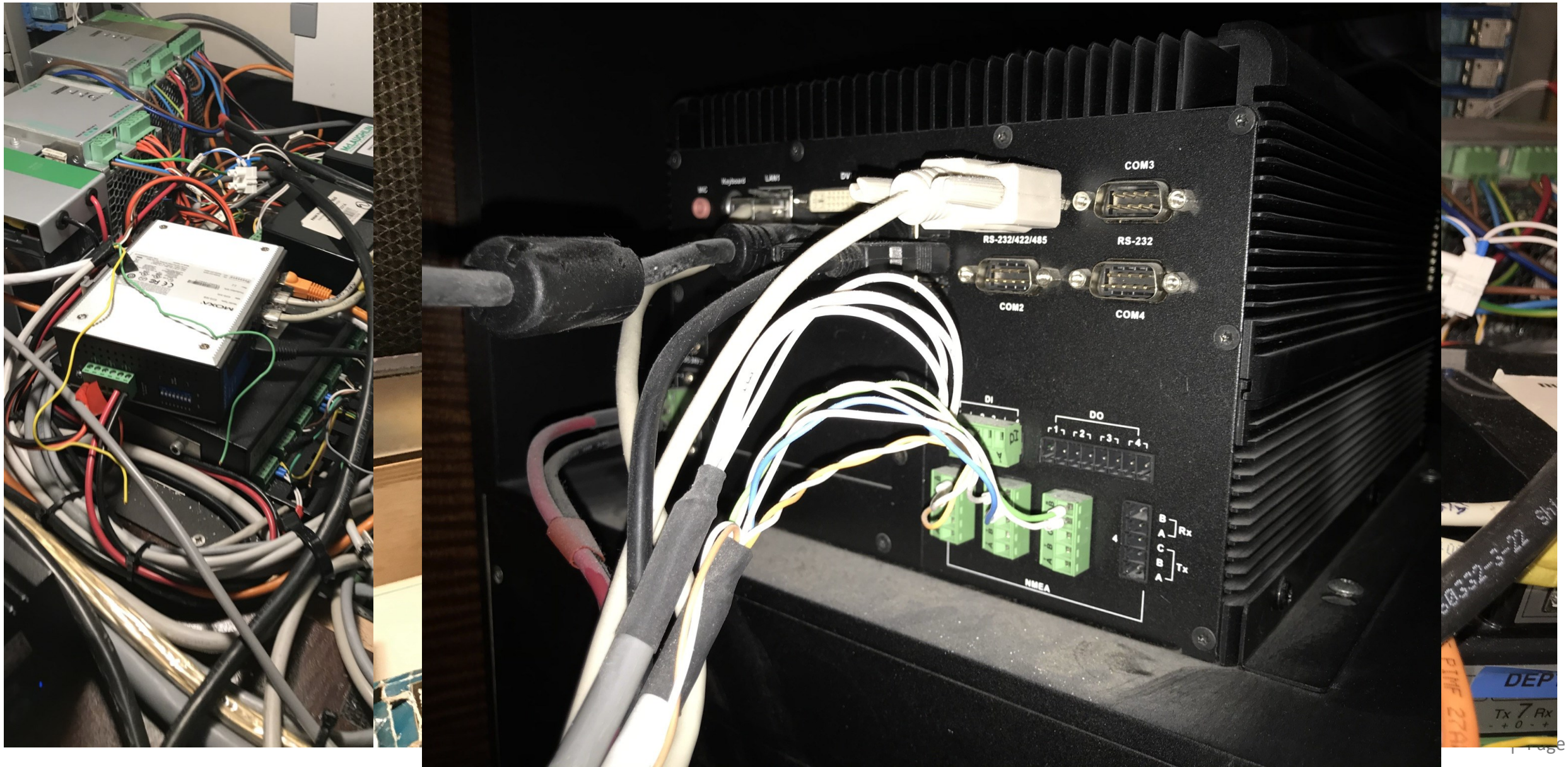
Electronic Chart Display - ECDIS

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

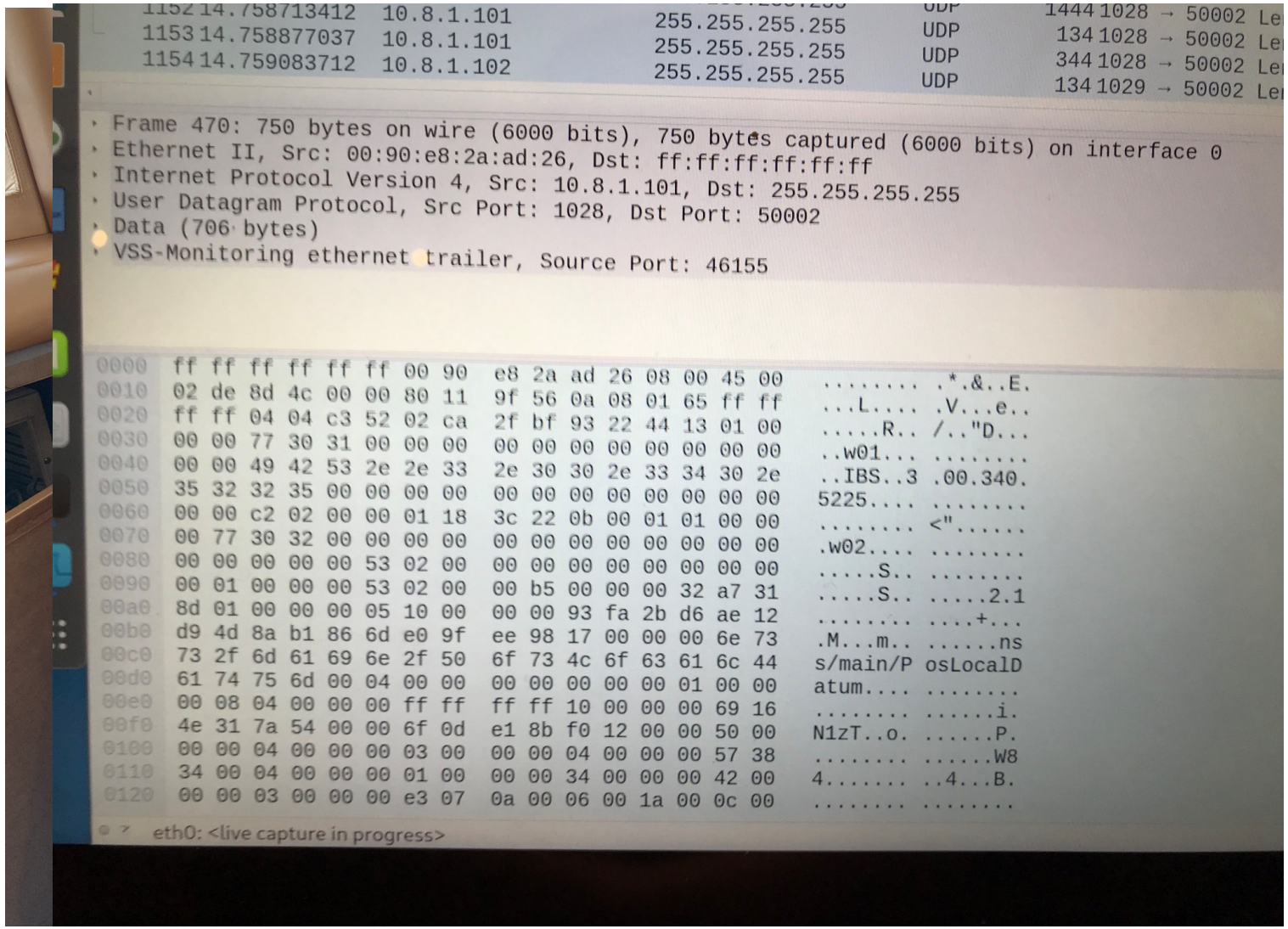
Ein Blick hinter die Kulisse



Navigationsnetz

admeritia

- Oft legacy (WinXP/Win7)
- Vorsicht beim Pentest
- Besser nur passiv Mithören!



Von klein bis groß

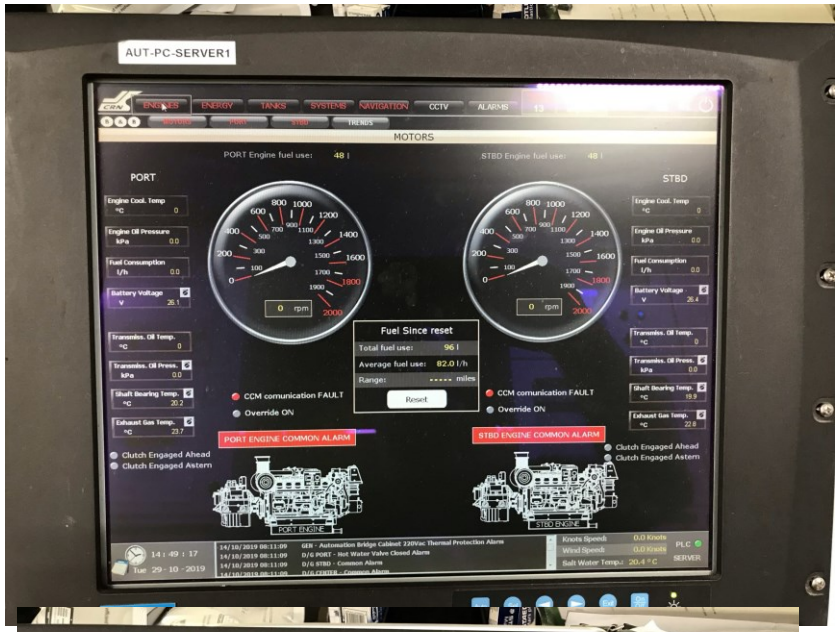
admeritia

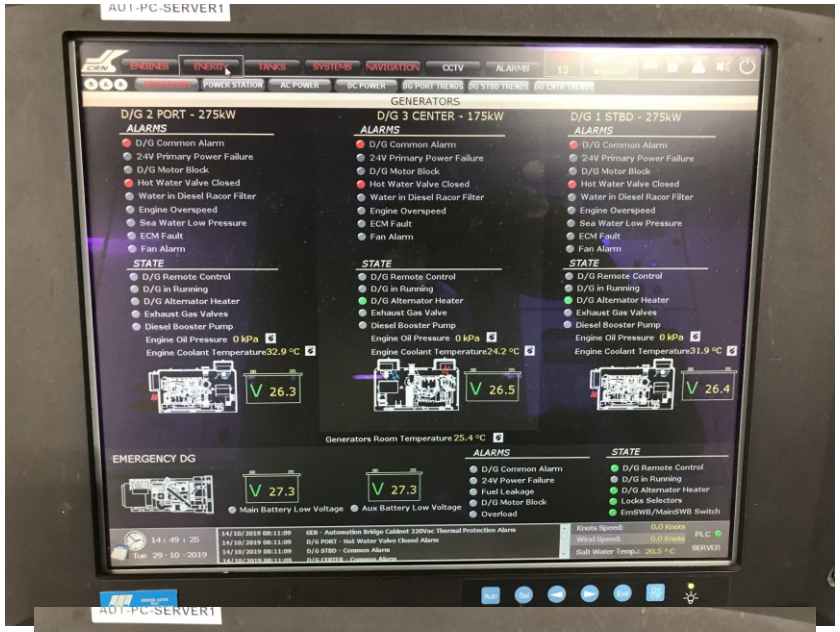
admeritia

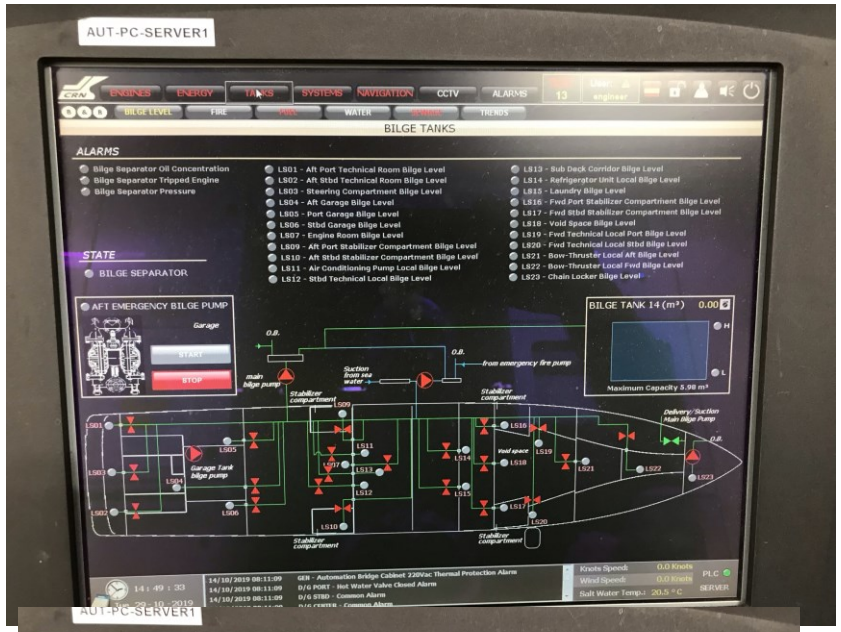
- Maschinenraum
- Energie
- Und vieles mehr

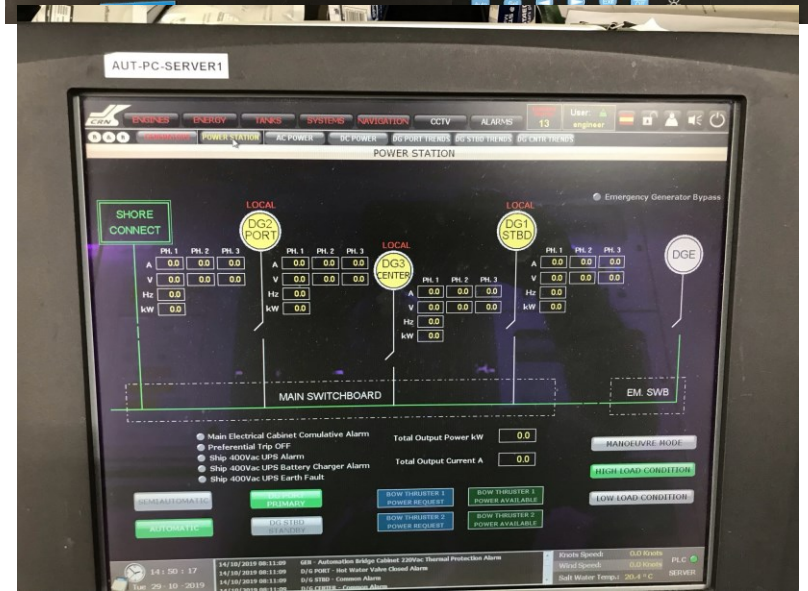
Ein Blick hinter die Kulisse

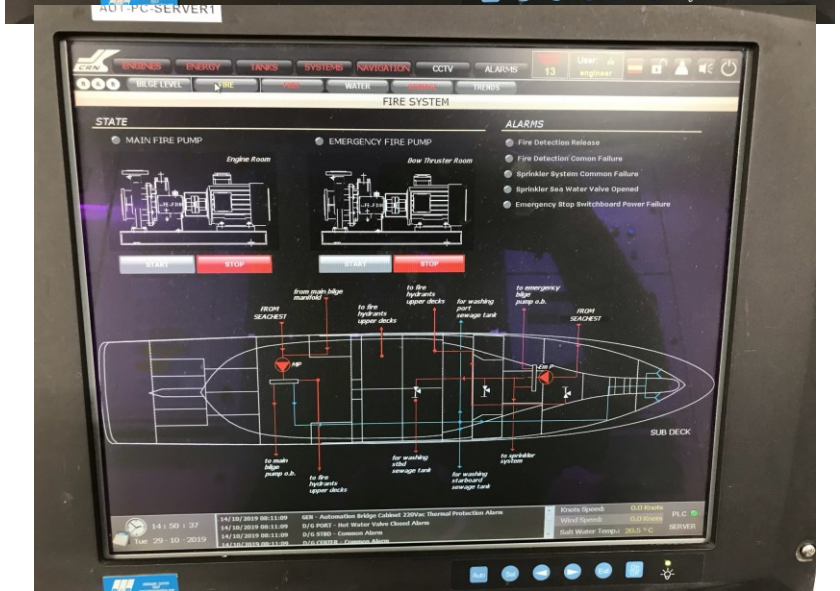
admeritia

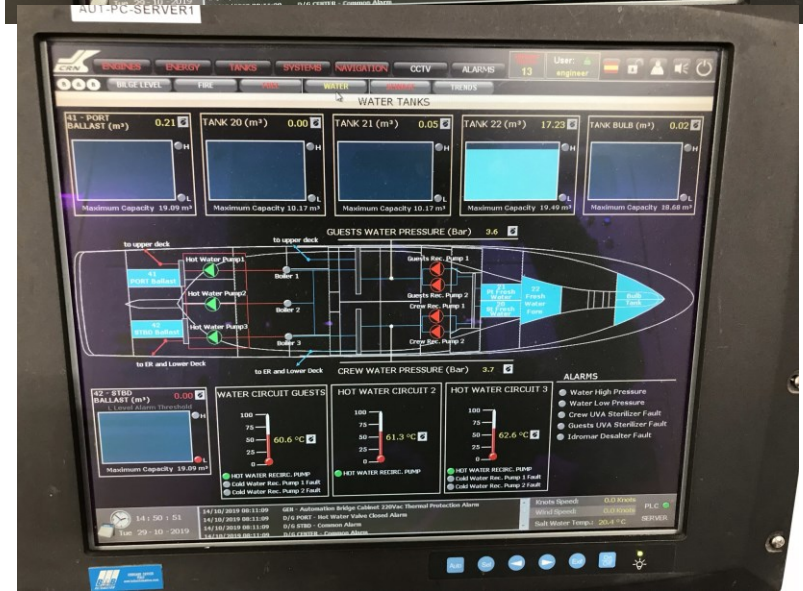












admeritia

Der Hauptzweck besteht darin, ein Schiff durch die Steuerung des Antriebssystems

in einer bestimmten Position zu halten

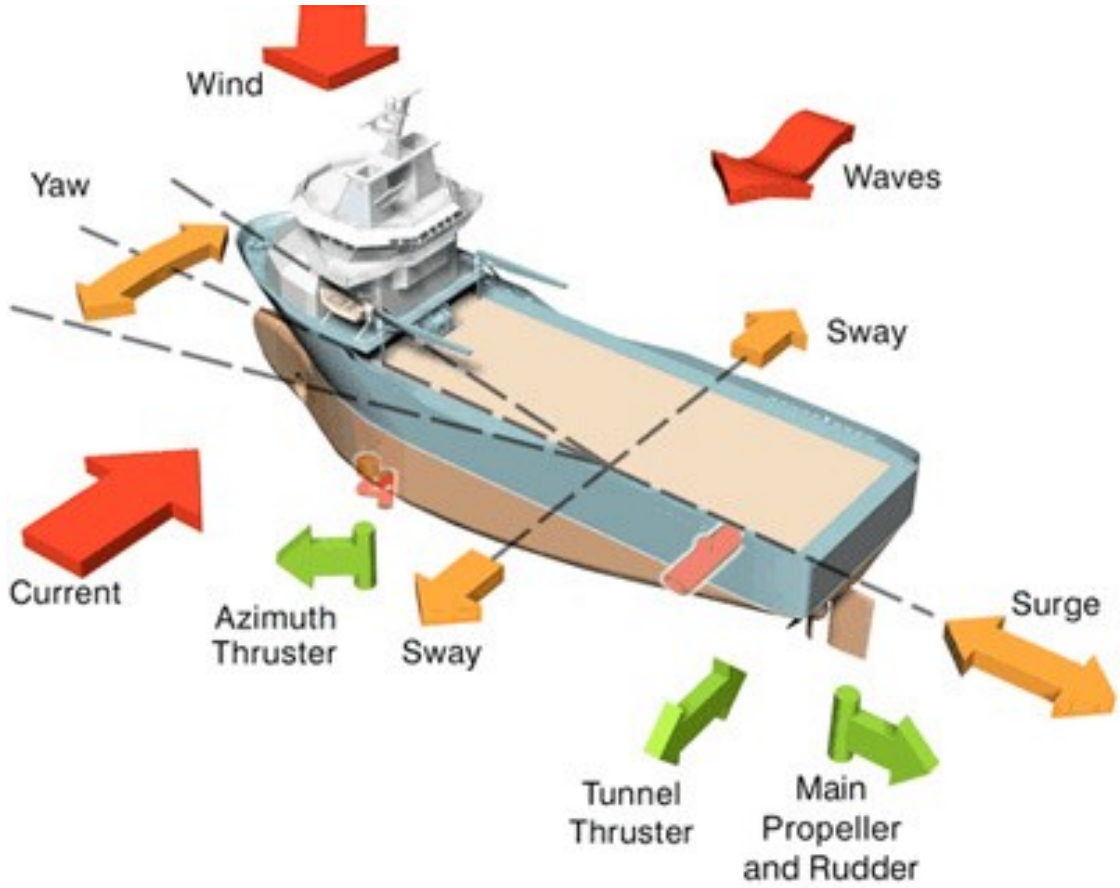
Operationen durchzuführen, ohne seine Position zu verändern

admeritia

Schiffe

- yaw (Gieren/Schlingern)
- pitch (Nicken/Stampfen)
- roll (Rollen/Wanken)

- Sway (lateral movement)
- Surge (linear movement)
- Heave (vertical movement)



4 Klassen definiert

Alle Klasse DP1-DP3 gemeinsam:

- Automatische und manuelle Position & Kurs Steuerung

Fehlertoleranz:

Class 1

- Keine Redundanz. Positionsverlust kann beim Ausfall **einer** Komponente auftreten

Class2

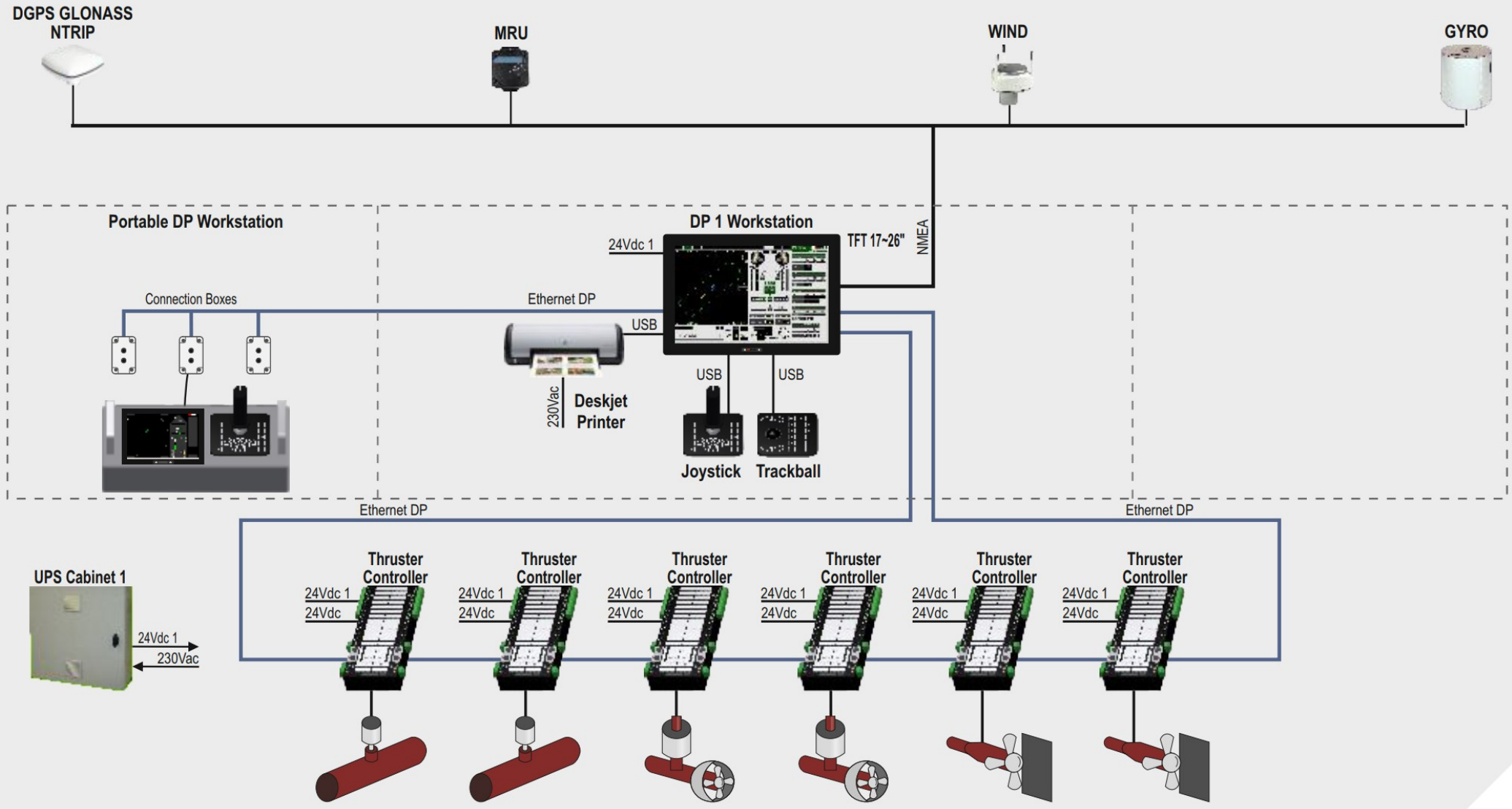
- Kein Positionsverlust bei Ausfall **einer** Aktiven Komponente wie „thrusters, generators, switchbords, remote control valves, etc“
- keine redundanten Systeme

Class 3

- Kein Positionsverlust bei Ausfall **jeweils einer** Aktiven Komponente wie „thrusters, generators, switchbords, remote control valves, etc“ sowie Brand oder Flutung der Segmente.
- mehrfach redundante Systeme and Segmentierten Orten

Dynamic Positioning

DP0



Compliance vorgaben

Maritime Safety Committee & International Maritime Organization

- Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems
- MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management.

IACS - International Association of Classification Societies

- - UR E22 Computer-based systems
- - UR E26 Cyber resilience of ships
- - UR E27 Cyber resilience of on-board systems and equipment
- - Rec 166 - Recommendation on Cyber Resilience

Contact

Questions?

Thank you for
your attention!

Mail:
stephan.gerling@admeritia.de

LinkedIn:
linkedin.com/in/stephan-gerling-11a010/

Socials:
@obiwan666

SECURITY UNTER KONTROLLE:
security-unter-kontrolle.de/

Monthly „Security-Briefing für HardHats“:
admeritia.de/hardhats

Blog:
fluchsfriction.medium.com