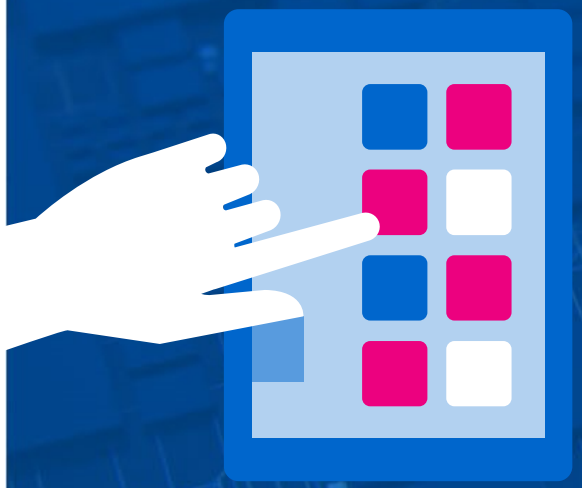
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberasiantuntijan näkemys aluksesta

Jussi Eronen

Kyberturvallisuuskeskus – kansallinen tietoturvaviranomainen



Kerää tietoa tietoturvaloukkauksista ja niiden uhkista

Tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta

Selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia sekä niiden uhkia

Arvioi ja hyväksyy järjestelmiä ja verkkoja

Ohjaa ja valvoo

- teleyritysten tietoturvallisuutta ja varautumista
- sähköisen viestinnän luottamuksellisuuden suojaa ja
- vahvojen sähköisten tunnistus- ja luottamuspalvelujen tietoturvaa

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Palvelulupaus tietoturvaloukkauksissa

Neuvomme
vahinkojen rajoittamisessa

Autamme
loukkauksen analysoinnissa

Tuemme
palautumis-toimenpiteissä

Keräämme
lisätietoja Suomesta ja maailmalta

Varoitamme
muita mahdollisia uhreja

Koordinoimme
haavoittuvuuksien korjaamista

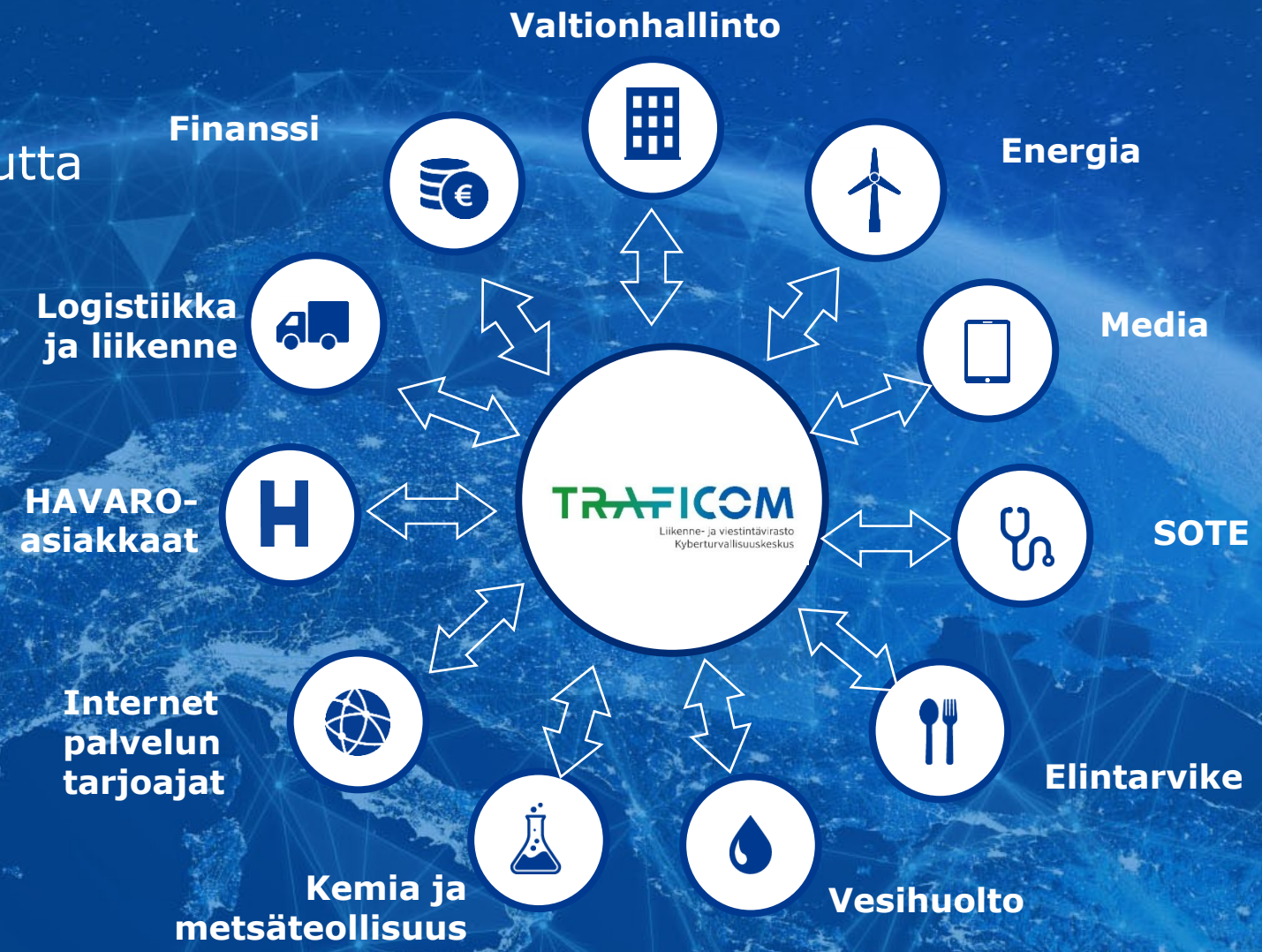
Luottamuksellisesti ja maksutta

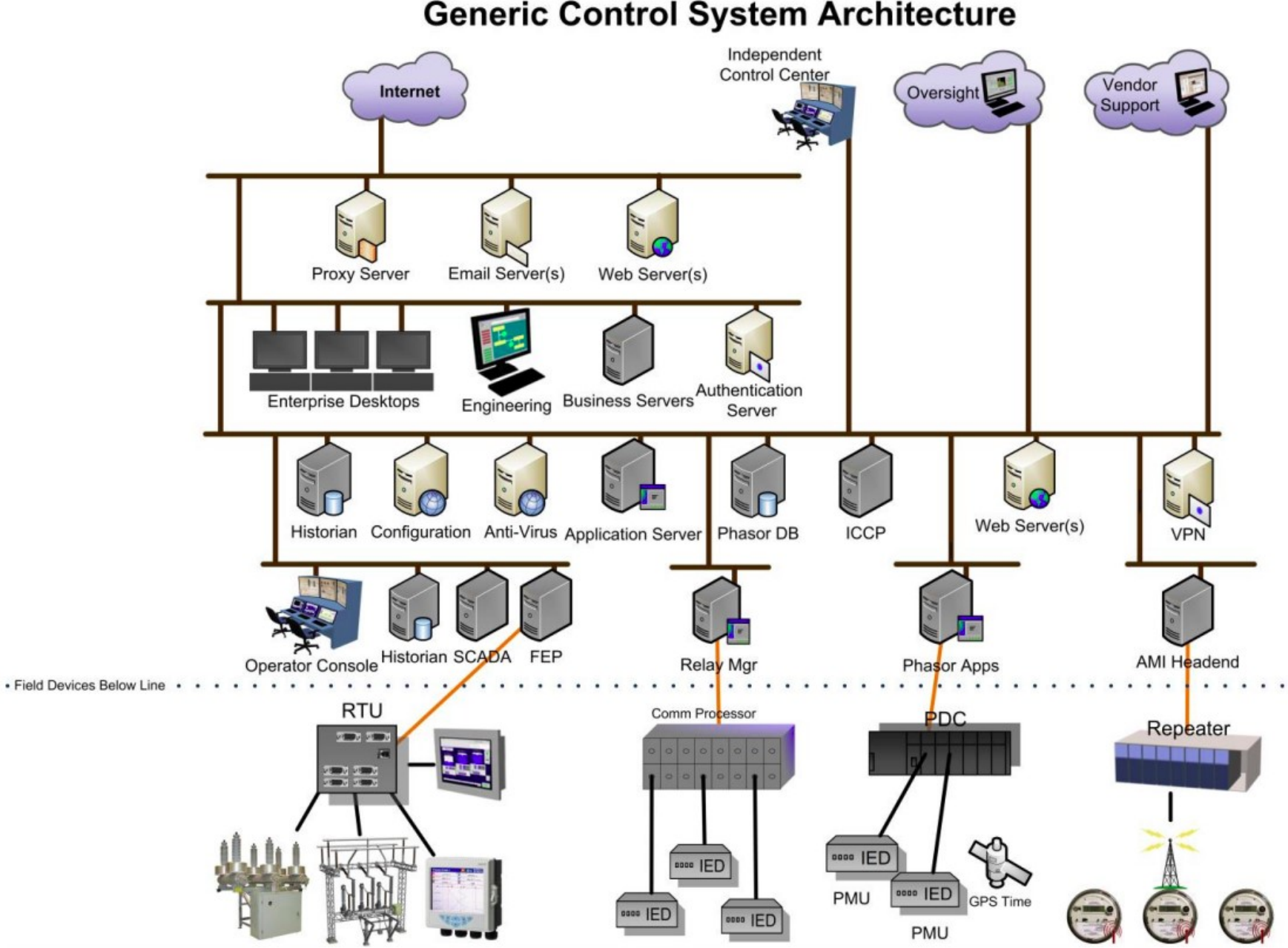
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvalliskeskuksen yhteistyöverkostoissa edistetään turvallisuutta

Kehitetään toimialojen ja yhteiskunnan kyberturvallisuutta yhdessä tietoturva-asioiden tiedonvaihtoryhmissä ISAC (Information Sharing and Analysis Centre)

- riskianalyysit
- ohjeistukset
- tutkimukset
- tiedonvaihto



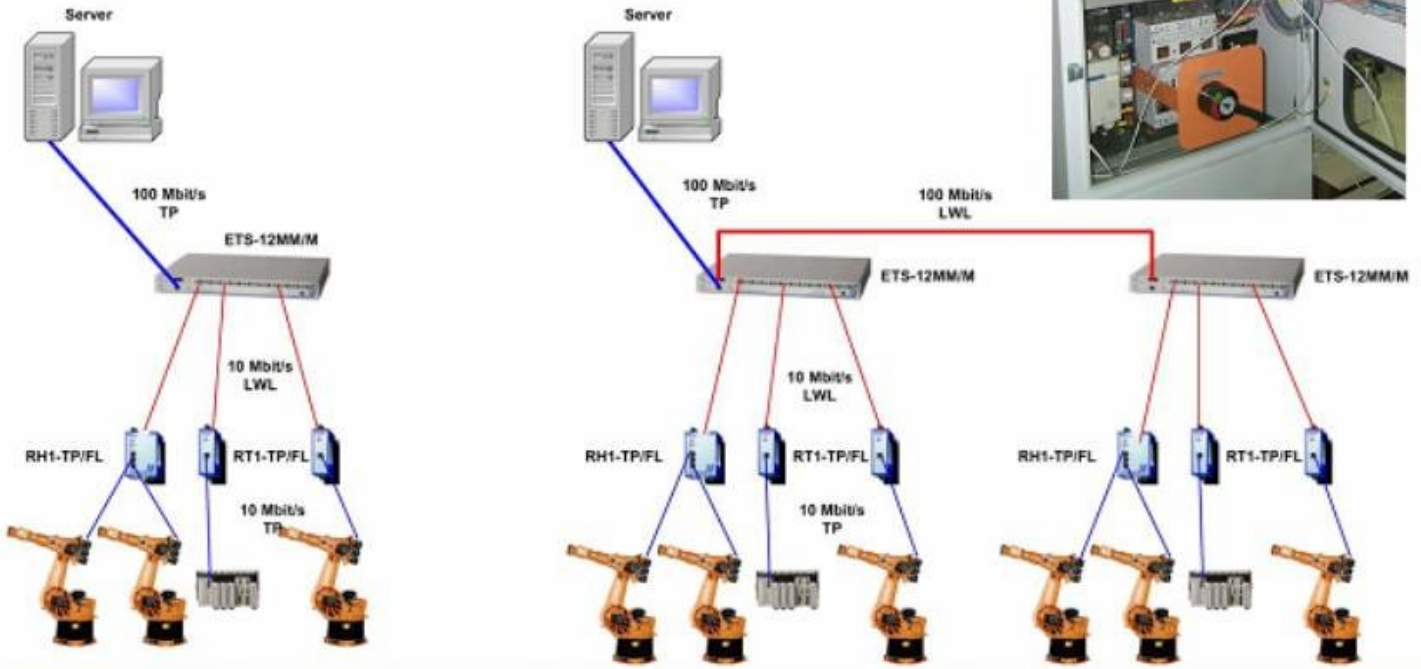


https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

HIRSCHMANN

OPEL Welding Robots Network

Automation and Network Solutions



Slide 23

https://wwsinternational.com.au/Hirschmann/industPP.htm

HIRSCHMANN

Hydropower Plant Network

Automation and Network Solutions

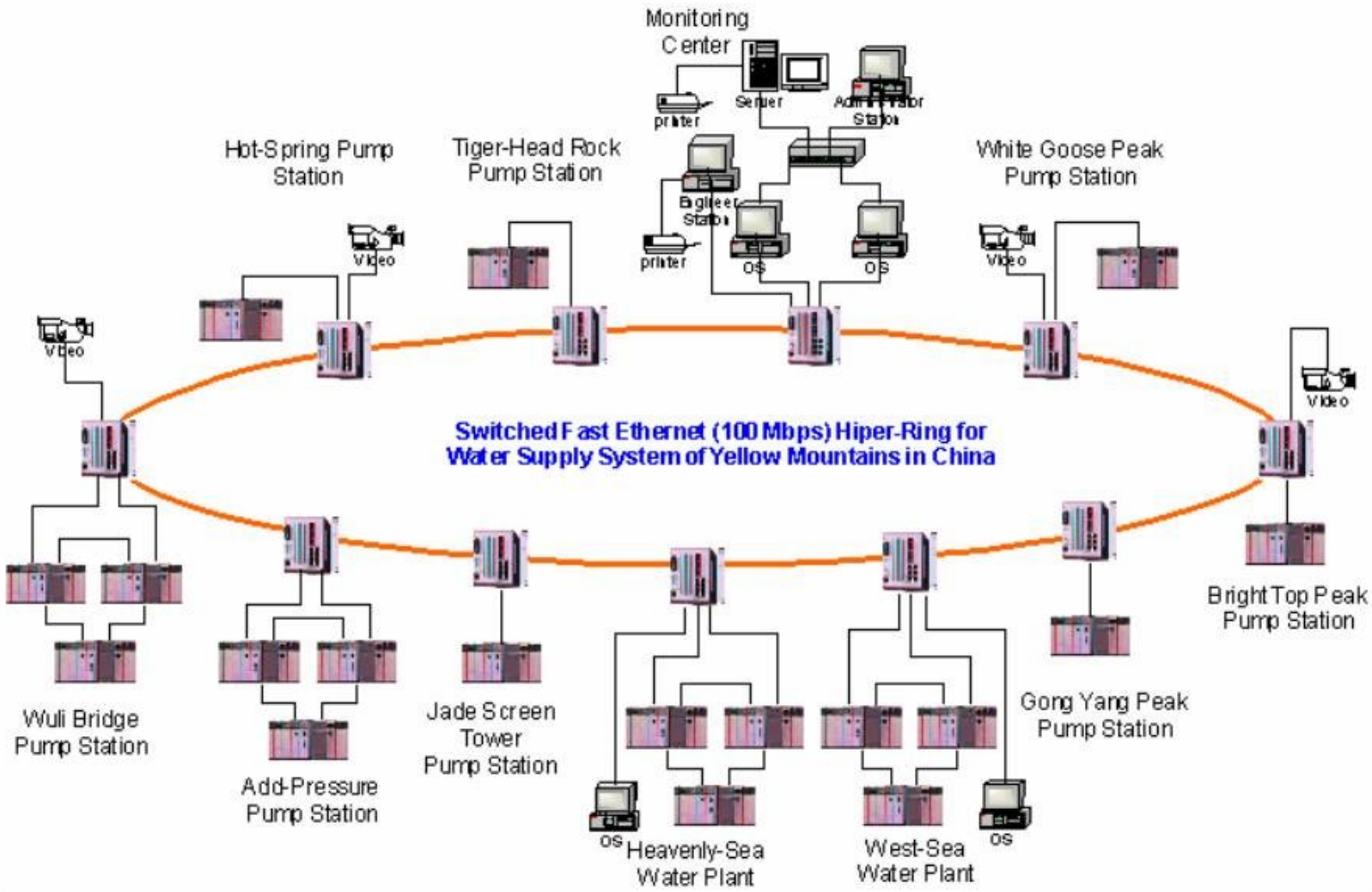
Slide 46

https://wwsinternational.com.au/Hirschmann/industPP.htm

HIRSCHMANN

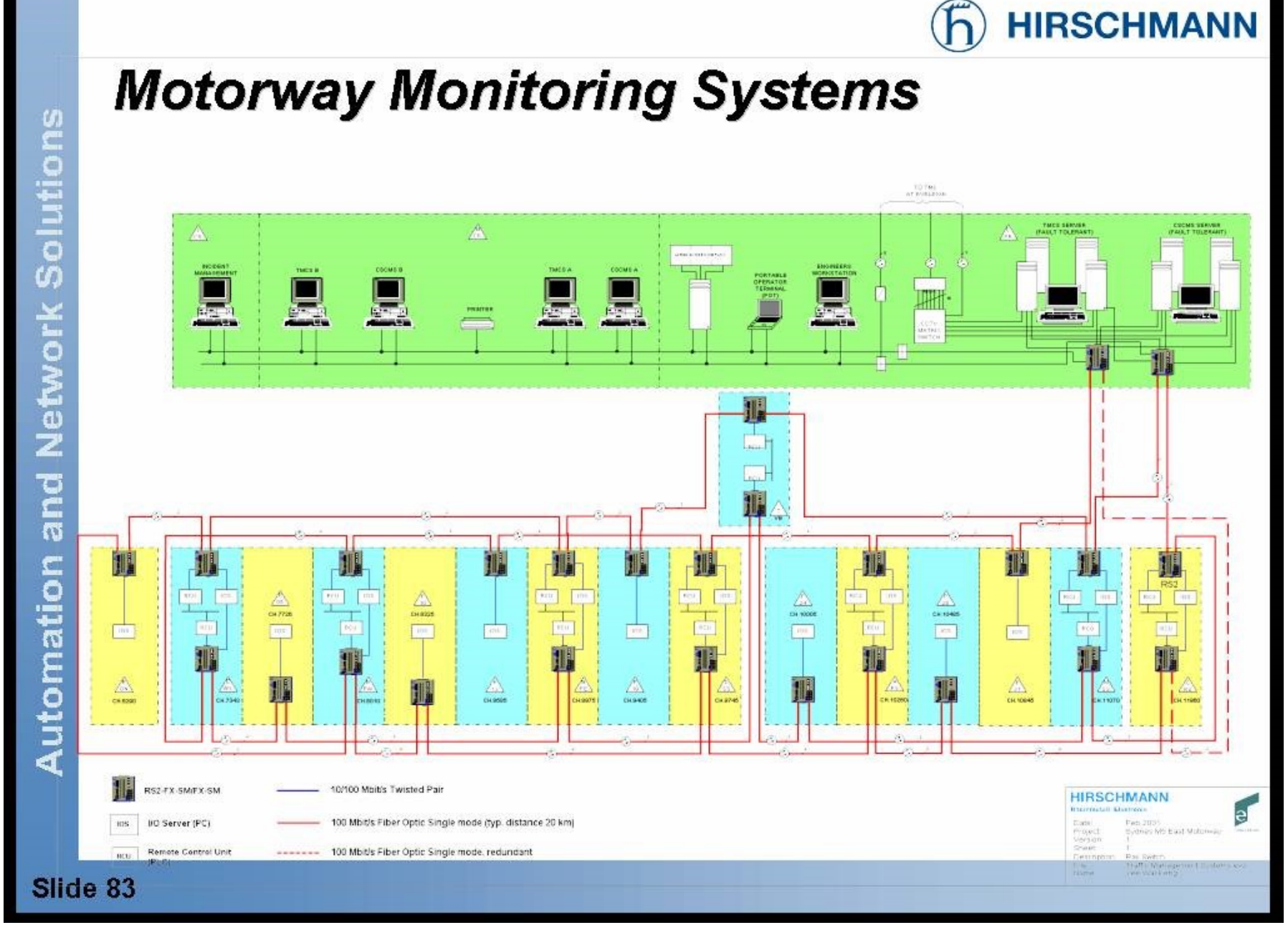
Huangsan Water Supply Project

Automation and Network Solutions



Slide 60

https://wwsinternational.com.au/Hirschmann/industPP.htm

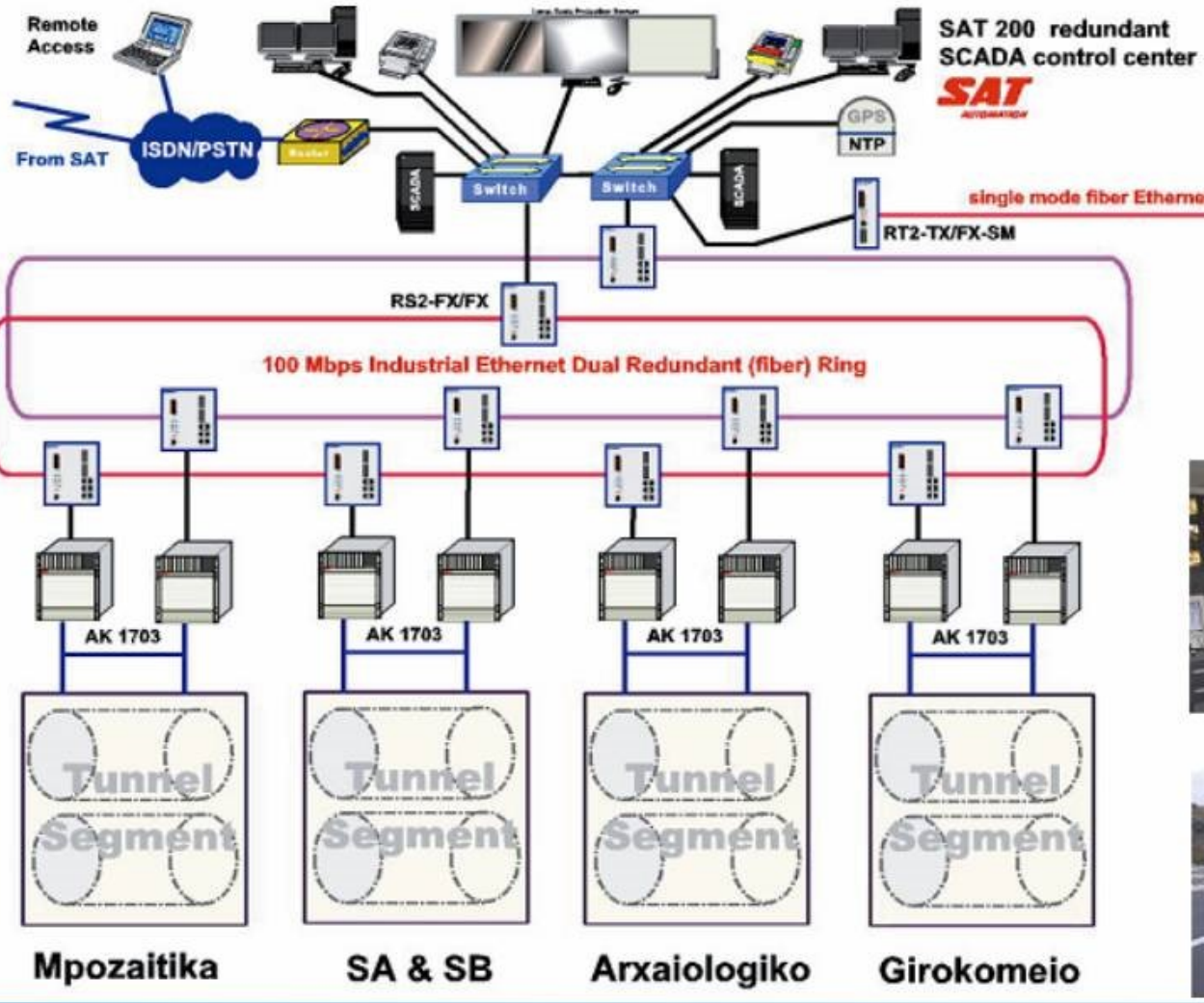


https://wwsinternational.com.au/Hirschmann/industPP.htm

HIRSCHMANN

Patras Highway Monitoring Systems

Automation and Network Solutions

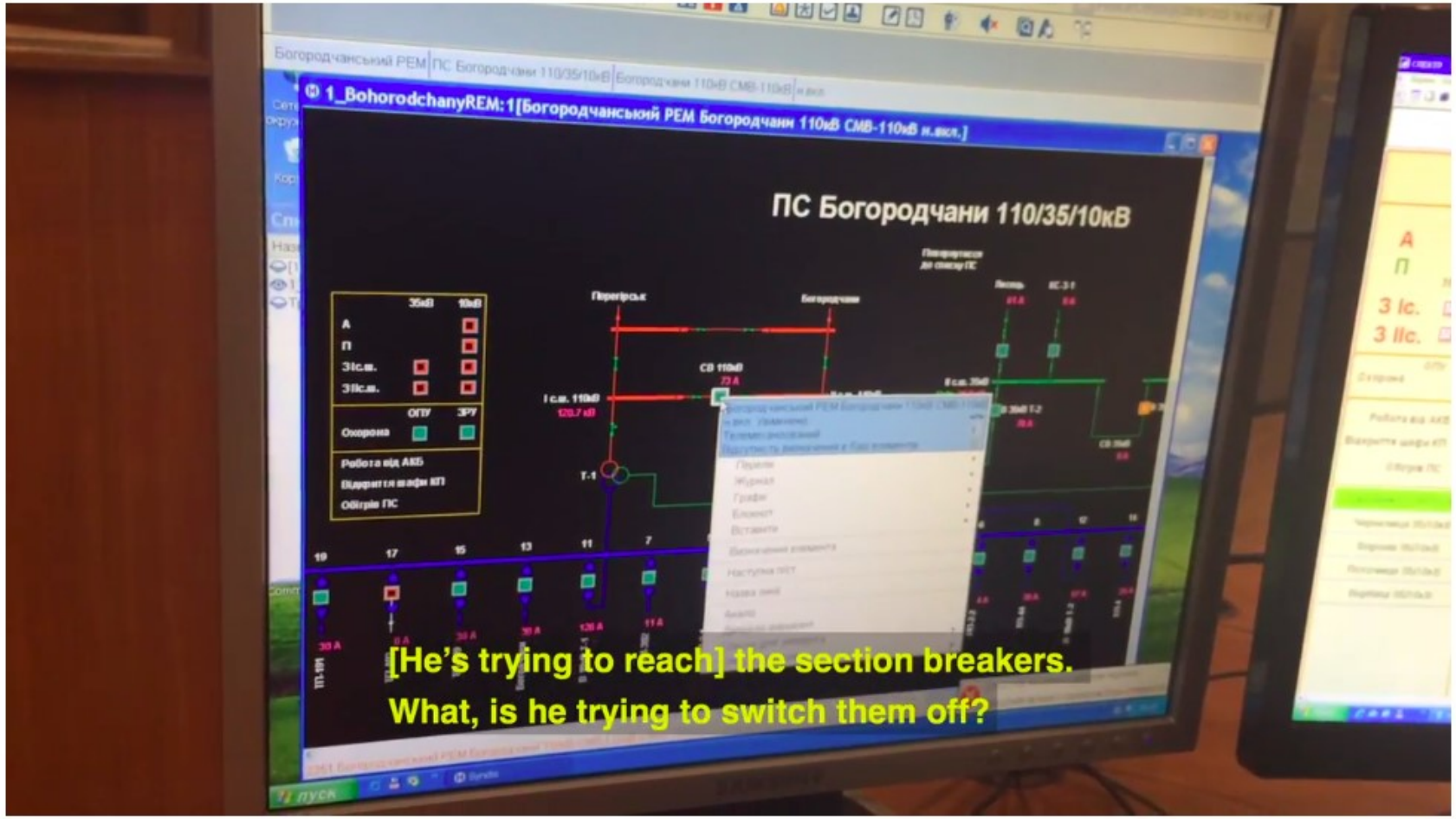


Slide 85

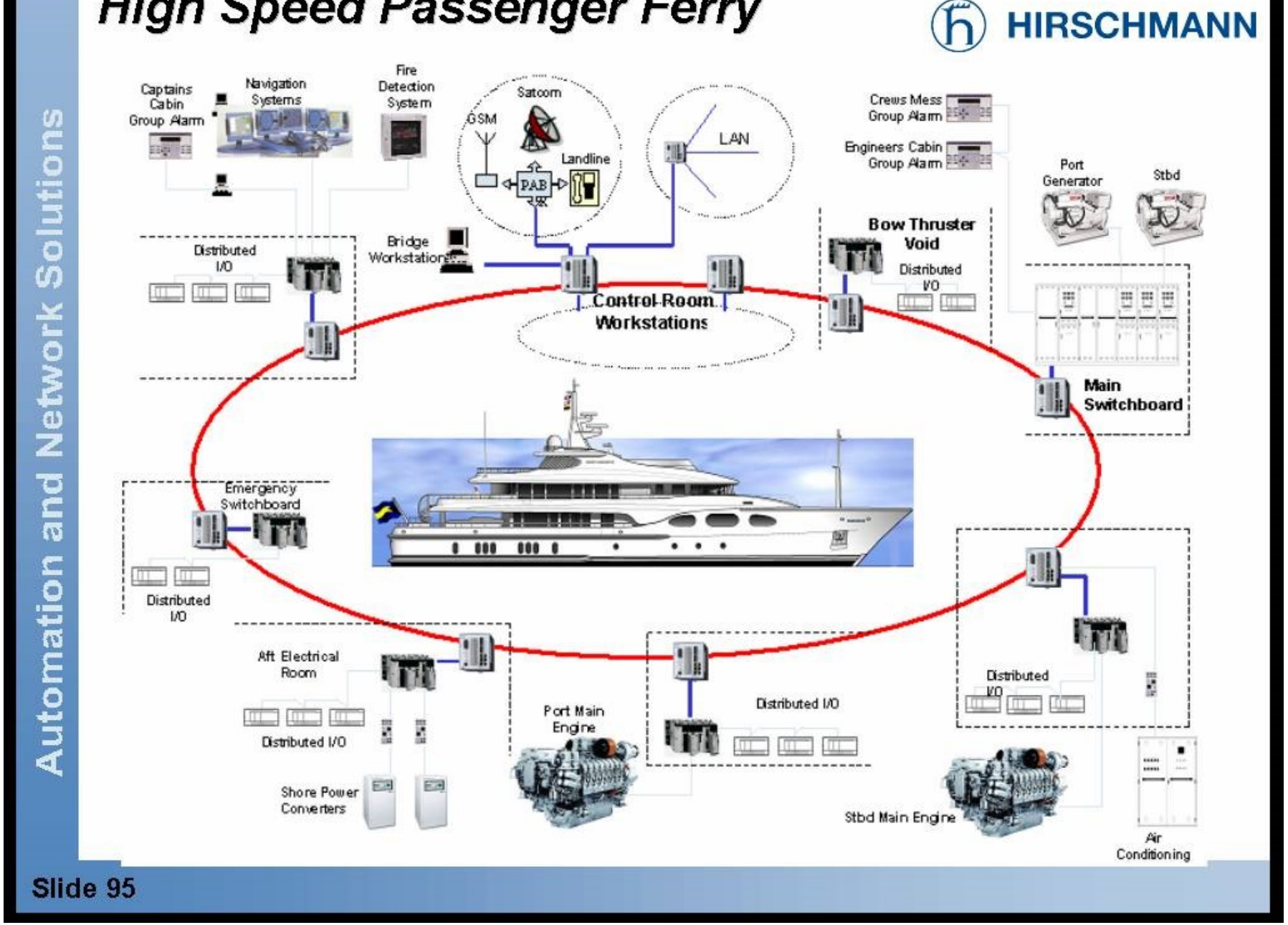
https://wwsinternational.com.au/Hirschmann/industPP.htm

Watch Hackers Take Over the Mouse of a Power-Grid Computer

As intruders caused a blackout by hijacking the network of a Ukrainian energy company, spooked engineers recorded this video.



https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/



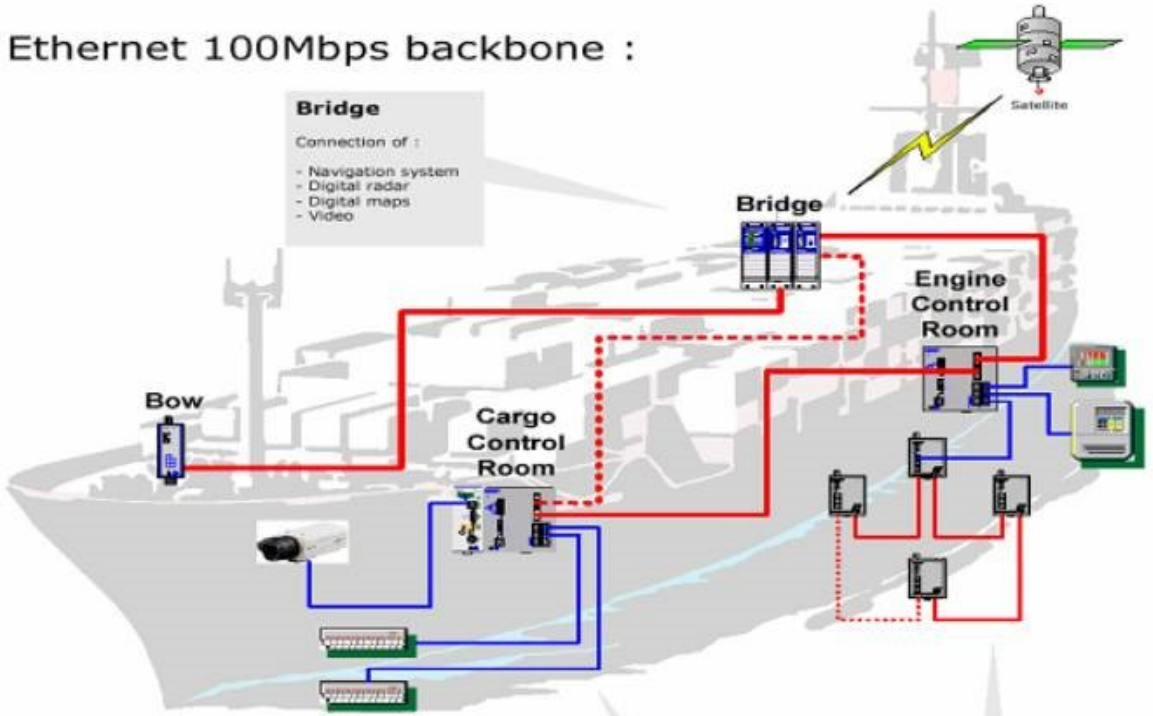
https://wwsinternational.com.au/Hirschmann/industPP.htm

Ship Control Network

HIRSCHMANN

Automation and Network Solutions

Ethernet 100Mbps backbone :



Bridge

Connection of :

- Navigation system
- Digital radar
- Digital maps
- Video

R-ViP Tx
Rail Video/Ethernet Converter

RS2-STX/FX
Rail Switch 4x10/100 + 1x100BFX

RS2-FX/FX(Navy)
Rail Switch 5x10/100 + 2x100BFX

MICE 2000 Series
- MS2108-2 Basic Switch Unit
- MM2-2FXM3/2TX1 Media Module 2x10/100 + 2x100BFX
- MM2-4TX1 Media Module 4x10/100

Cargo Control Room

Connection of :

- PLC
- Remote I/O
- Video

Engine Control Room

Connection of :

- PLC
- Remote I/O
- Local Bus System
- Video

Slide 98

https://wwsinternational.com.au/Hirschmann/industPP.htm

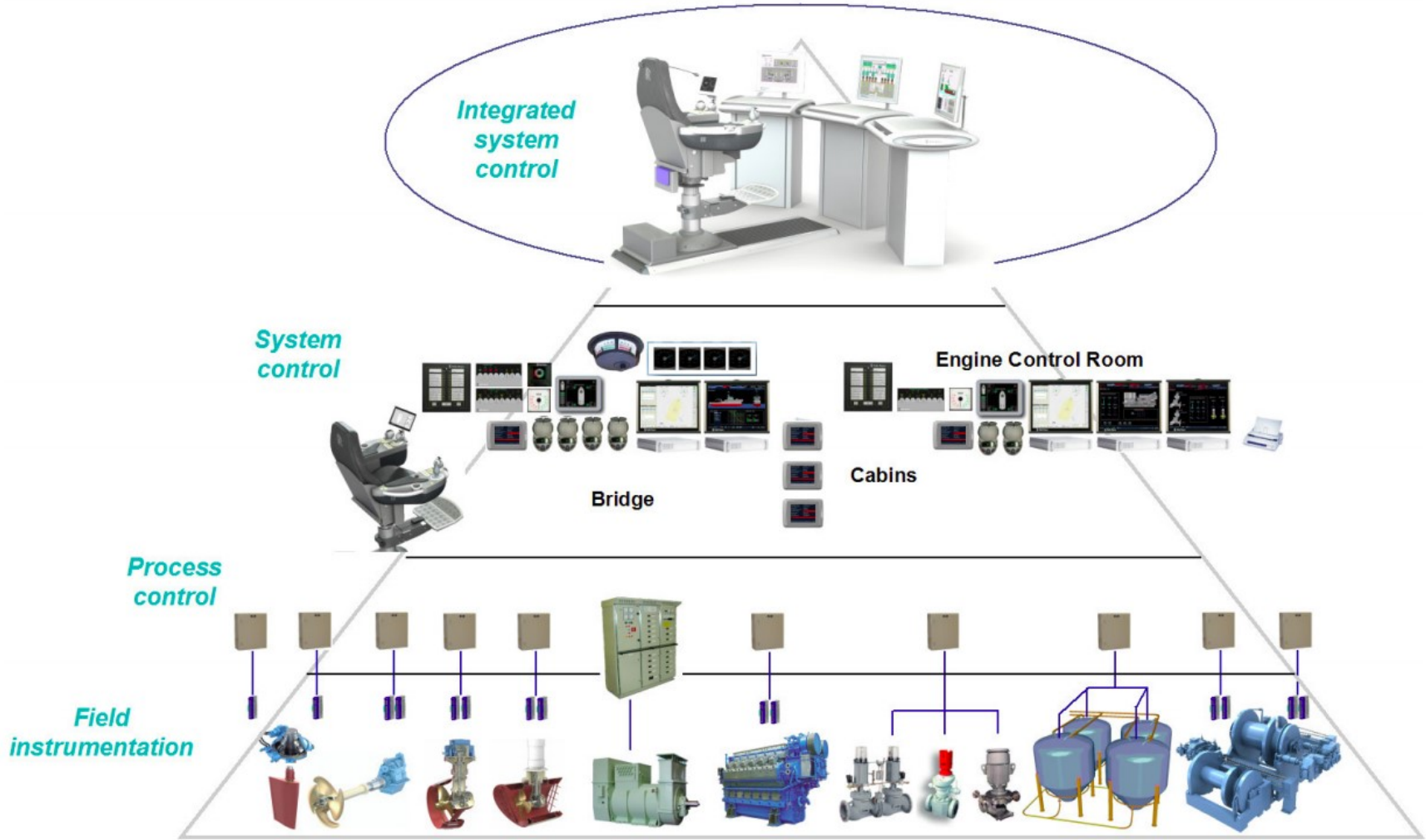
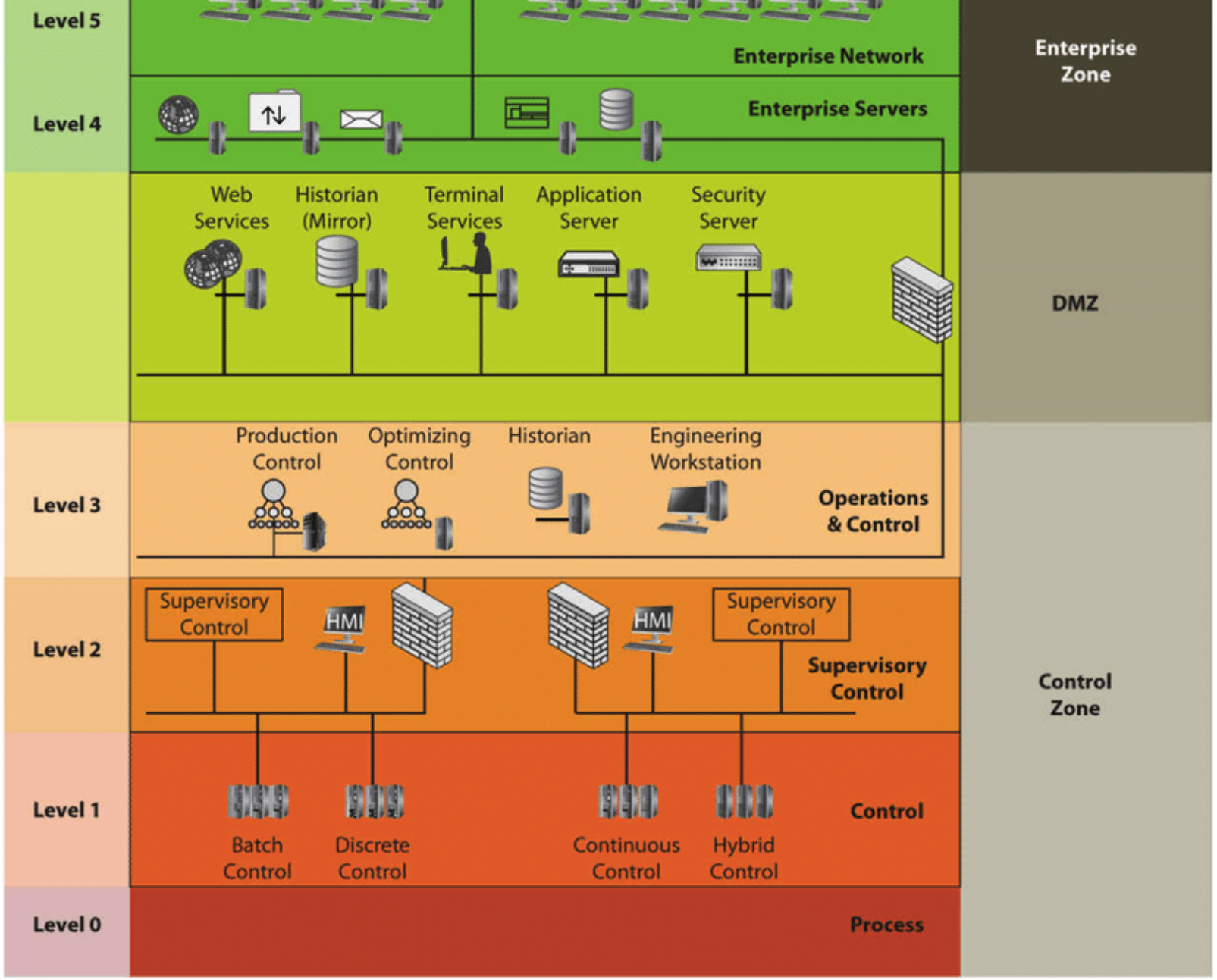
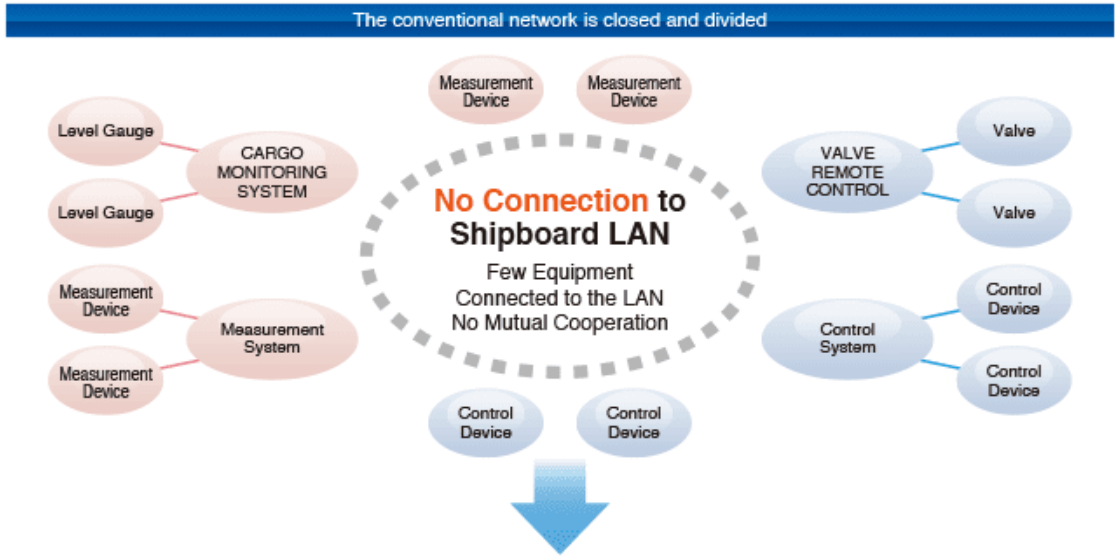


Figure 5 Common Control Platform for all Products

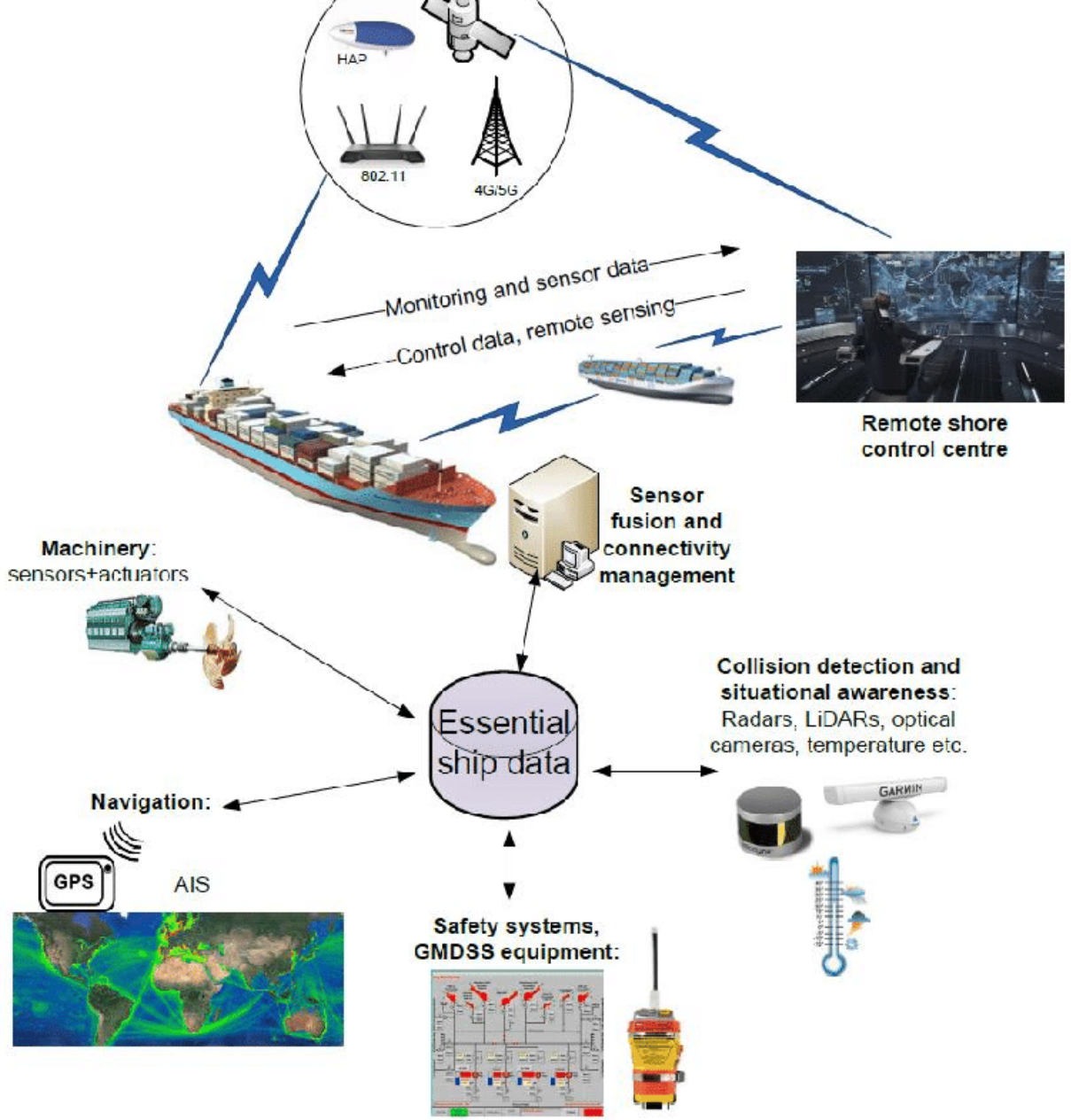
https://dynamic-positioning.com/proceedings/dp2007/design_hansen.pdf



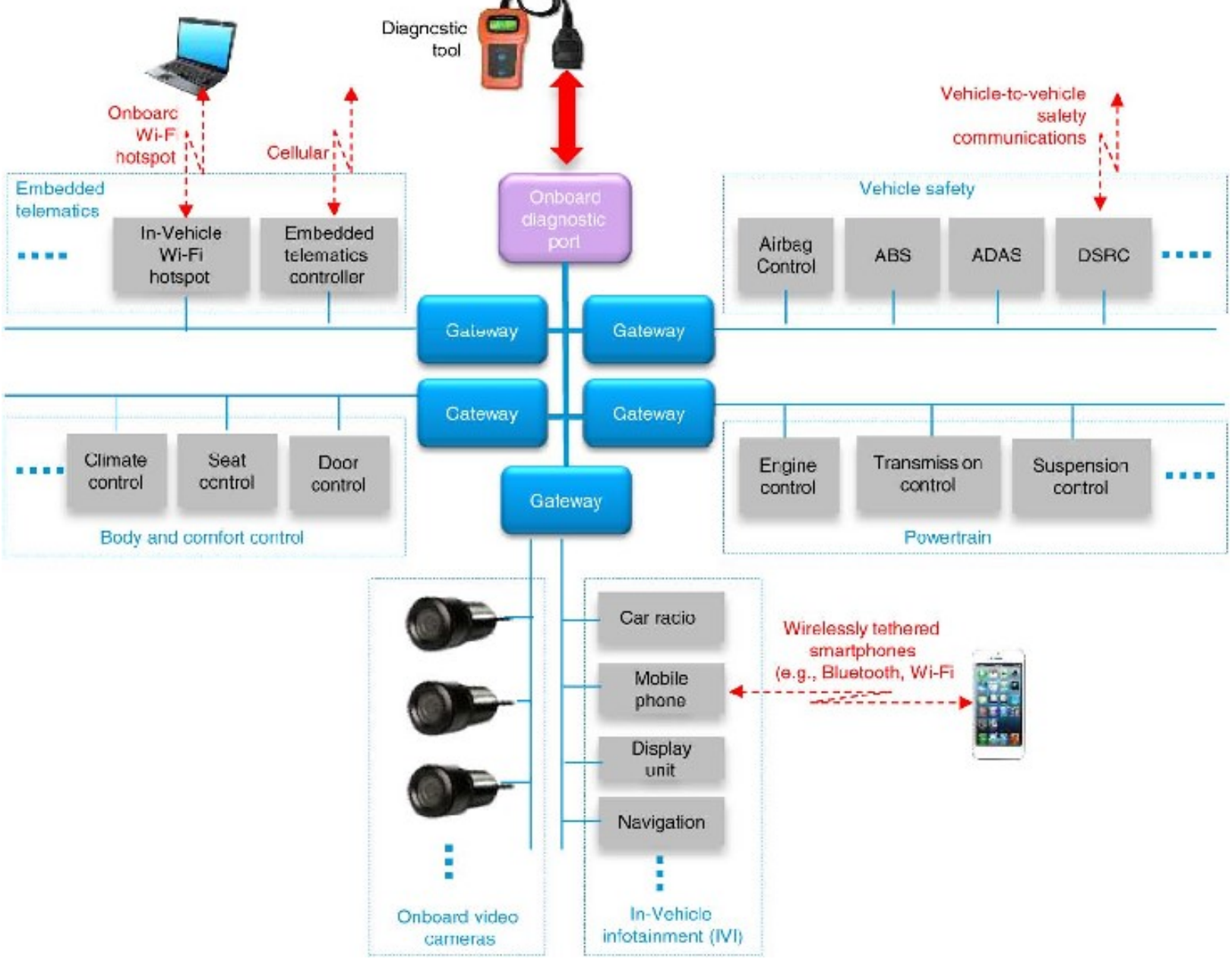
Experience and Lessons in Building an ICS Security Testbed, https://ieeexplore.ieee.org/document/8850804



https://www.musasino.biz/smartnetwork



Connectivity for autonomous ships: Architecture, use cases, and research challenges, https://ieeexplore.ieee.org/document/8191000



Defending Connected Vehicles Against Malware: Challenges and a Solution Framework, https://ieeexplore.ieee.org/document/6720160

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Miller and Valasek's full arsenal includes functions that at lower speeds fully kill the engine, abruptly engage the brakes, or disable them altogether. The most disturbing maneuver came when they cut the Jeep's brakes, leaving me frantically pumping the pedal as the 2-ton SUV slid uncontrollably into a ditch. The researchers say they're working on perfecting their steering control—for now they can only hijack the wheel when the Jeep is in reverse. Their hack enables surveillance too: They can track a targeted Jeep's GPS coordinates, measure its speed, and even drop pins on a map to trace its route.

ANDY GREENBERG/WIRED

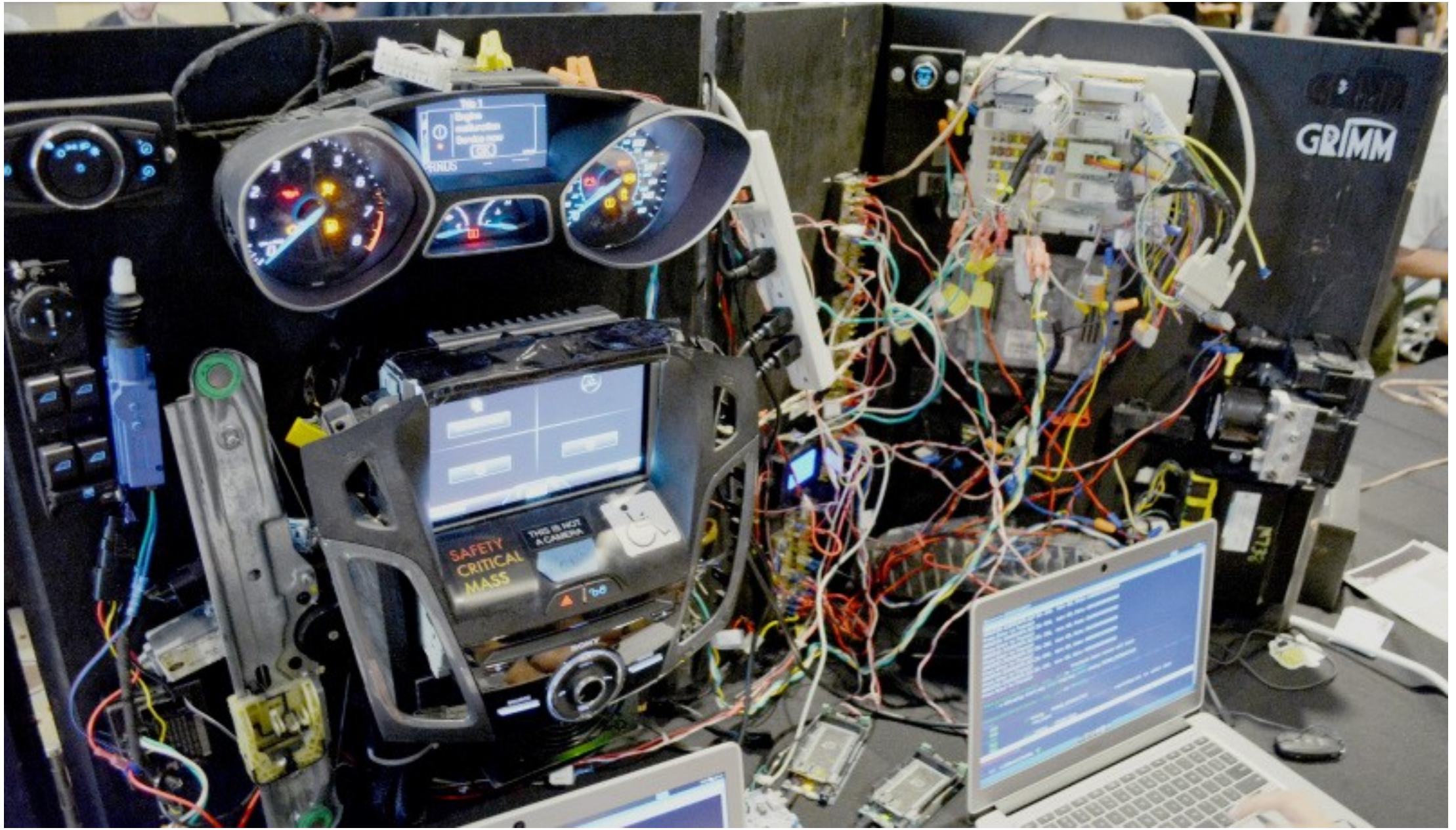
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

KIM ZETTER 07.30.09 04:51 PM

Smart Parking Meters Hacked — Free Parking For All!

LAS VEGAS – Scofflaws could hack the smart cards that access electronic parking meters in large cities around the United States, researchers are finding. The smart cards pay for parking spots, and their programming could be easily changed to obtain unlimited free parking.

https://www.wired.com/2009/07/parking-meters/



https://hackaday.com/2018/08/11/car-hacking-at-def-con-26/

MARKET NEWS JULY 31, 2015 / 12:40 AM / 5 YEARS AGO

UPDATE 1-Researcher says can hack GM's OnStar app, open vehicle, start engine

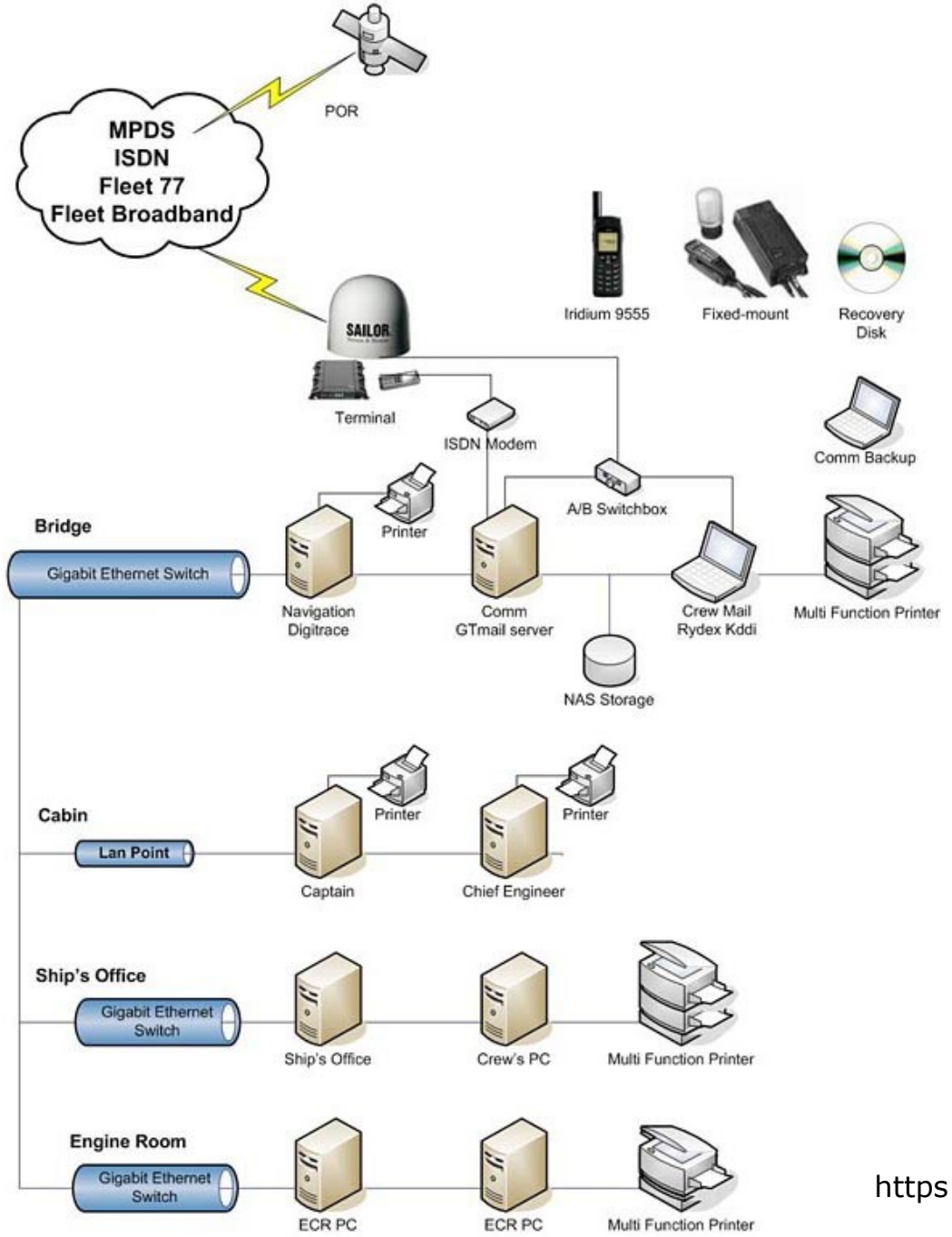
3 MIN READ

(Adds that GM plans to release an update for the app)

By Jim Finkle and Bernie Woodall

BOSTON/DETROIT, July 30 (Reuters) - A researcher is advising drivers not to use a mobile app for General Motors Co's OnStar vehicle communications system, saying hackers can exploit a security flaw in the product to unlock cars and start engines remotely.

https://www.reuters.com/article/gm-hacking/update-1-researcher-says-can-hack-gms-onstar-app-open-vehicle-start-engine-idUSL1N10A3XK20150730

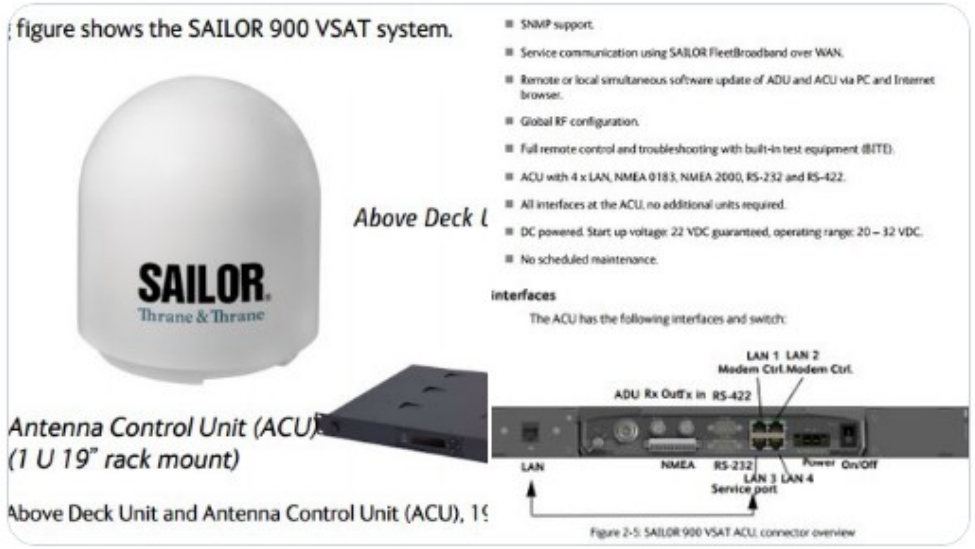


https://qzs.com.sg/maritime-it-shipboard-support/

x0rz @x0rz · Jul 18, 2017

Replying to @x0rz

If you want to know more about these systems, here is the documentation for the SAILOR 900 VSAT livewire-connections.com/sites/default/… (PDF) #HackingShips



4 93 166

x0rz @x0rz · Jul 18, 2017

Duuuuuude, default creds everywhere. I'm connected to a motherfucking ship as admin right now. Hacking ships is easy 😌

In the following map you can see all the open AIS receivers we identified
green dots and the last available position of unique vessels represented

AIS receivers look something like this:

They can easily be bought on Amazon for a price that ranges between $300 and $2,000, depending on their class and additional capabilities. Sometimes they are already provided with USB or Ethernet sockets in order to push or serve the collected data to an external system. Sometimes they are directly made available on the Internet through a serial port server provided with 3G, mobile or other satellite connections.

bly noticed two tracks around the Equator line: we believe that
ordinates of GPS receivers of vessels that were not able to est

Looking through the Internet Census data, **we identified more than 360 AIS receivers with around 160 of them still active** and responding. These receivers are distributed all over the globe and are constantly logging AIVDM/ AIVDO and similar messages over an open TCP port that varies depending on the vendor of the serial port server or other equipment used.

https://blog.rapid7.com/2013/04/29/spying-on-the-seven-seas-with-ais/

RESEARCH | DECEMBER 9, 2015

Maritime Security: Hacking into a Voyage Data Recorder (VDR)

By **Ruben Santamarta**

In 2014, IOActive disclosed a series of attacks that affect multiple SATCOM devices, some of which are commonly deployed on vessels. Although there is no doubt that maritime assets are valuable targets, we cannot limit the attack surface to those communication devices that vessels, or even large cruise ships, are usually equipped with. In response to this situation, IOActive provides services to evaluate the security posture of the systems and devices that make up the modern integrated bridges and engine rooms found on cargo vessels and cruise ships. [1]

https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/

PEN TEST PARTNERS
Penetration testing and security services

BLOG: MARITIME CYBER SECURITY

Speed 2 – The Poseidon Adventure – Part One

Andrew Tierney
08 Sep 2020

That change in trim alone could cause a capsize.

If the change in ballast wasn't enough to sink the vessel by itself, when a list had started to develop, send a NMEA message to the autopilot, commanding a turn to starboard.

Or, send a helm message commanding the same turn direction

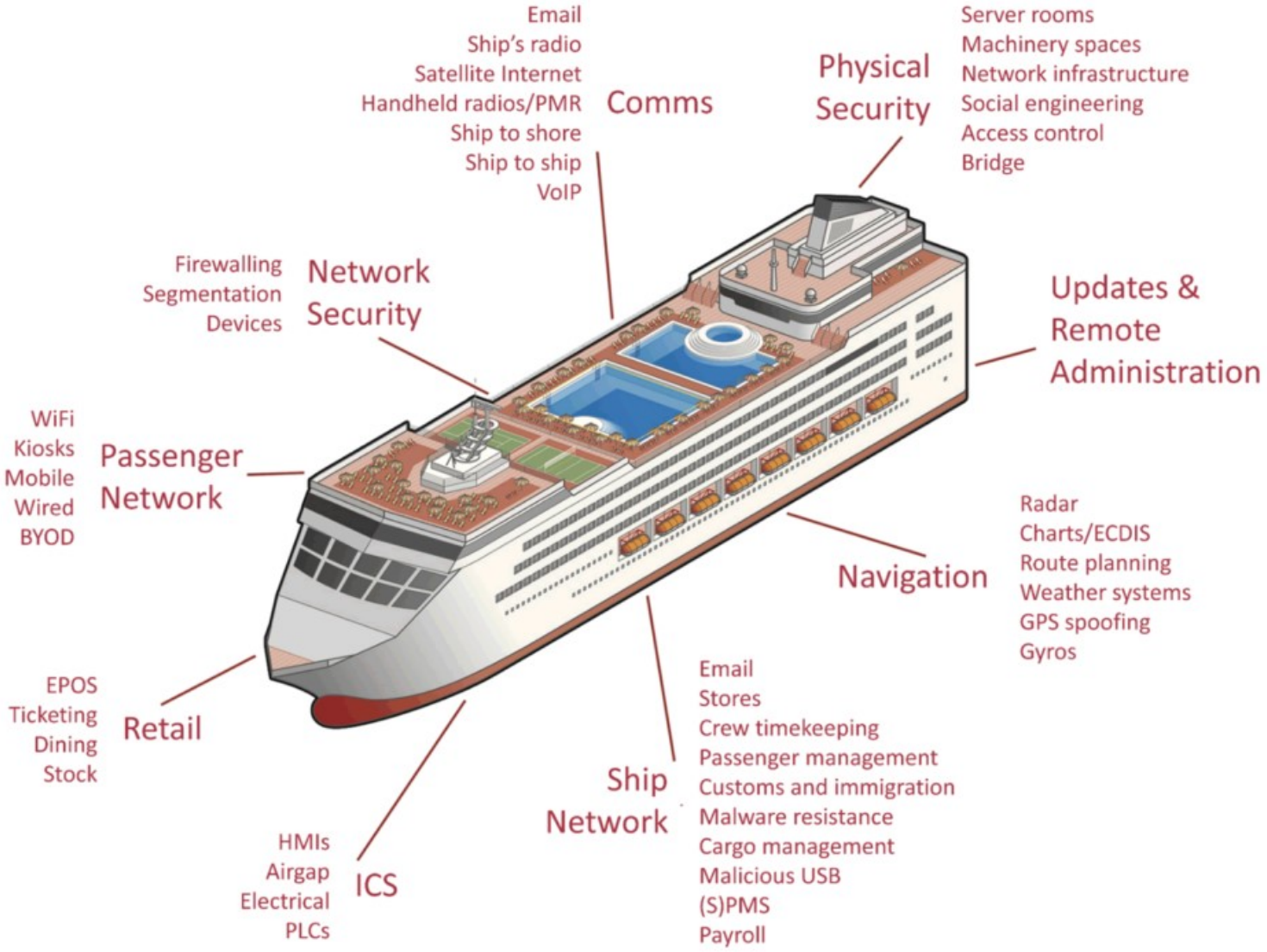
The list, combined with the change in stability when turning, is likely to cause a capsize

Sound far-fetched? Read up on the MV Cougar Ace car carrier incident if you're not convinced what ballast changes can do to ships:

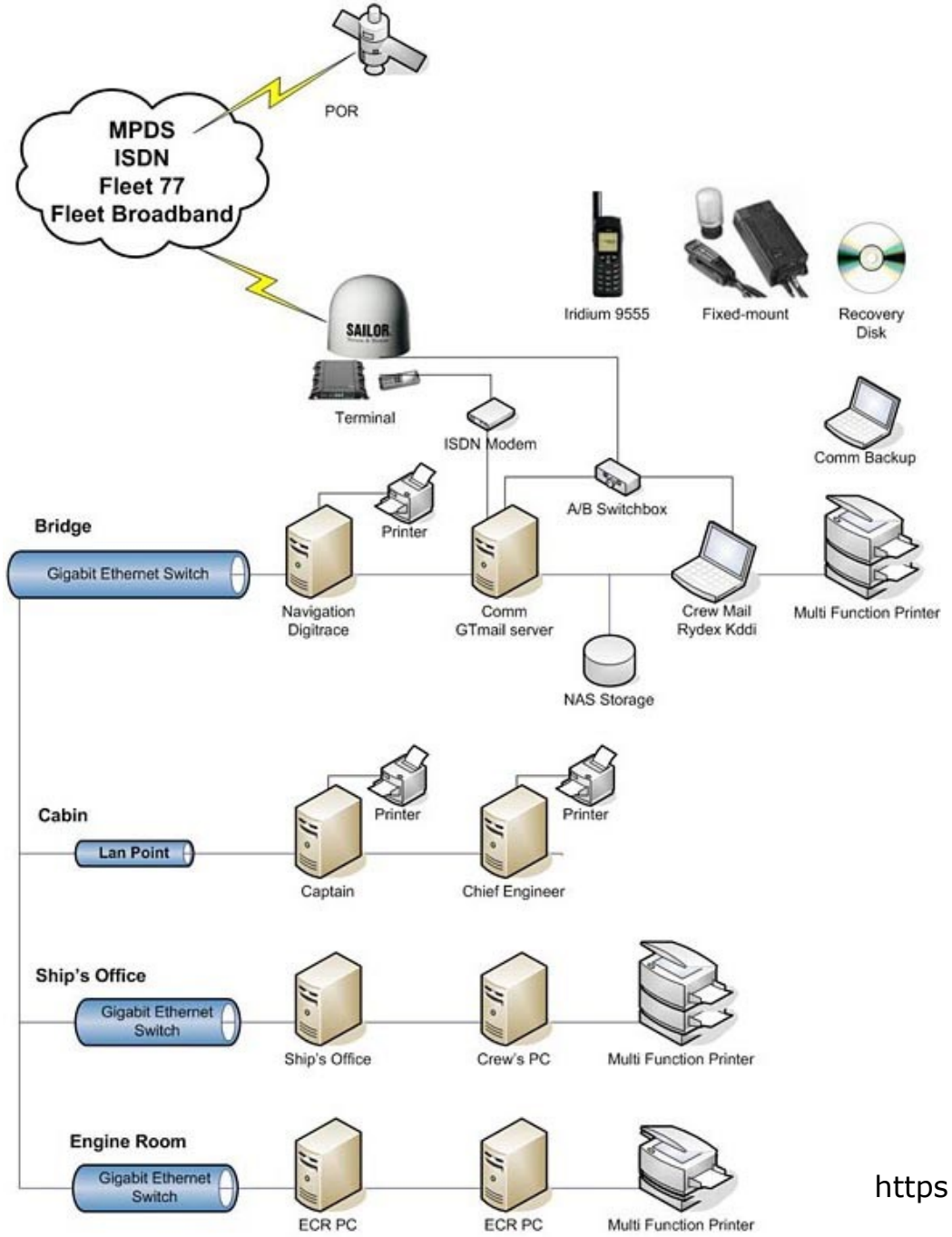
https://en.wikipedia.org/wiki/MV_Cougar_Ace – $117M of vehicles had to be crushed as a result, even though the ship wasn't lost.

https://www.pentestpartners.com/security-blog/sinking-a-ship-and-hiding-the-evidence/
https://www.pentestpartners.com/security-blog/speed-2-the-poseidon-adventure-when-cruise-ships-attack-part-1/

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus



https://www.pentestpartners.com/security-blog/speed-2-the-poseidon-adventure-when-cruise-ships-attack-part-1/

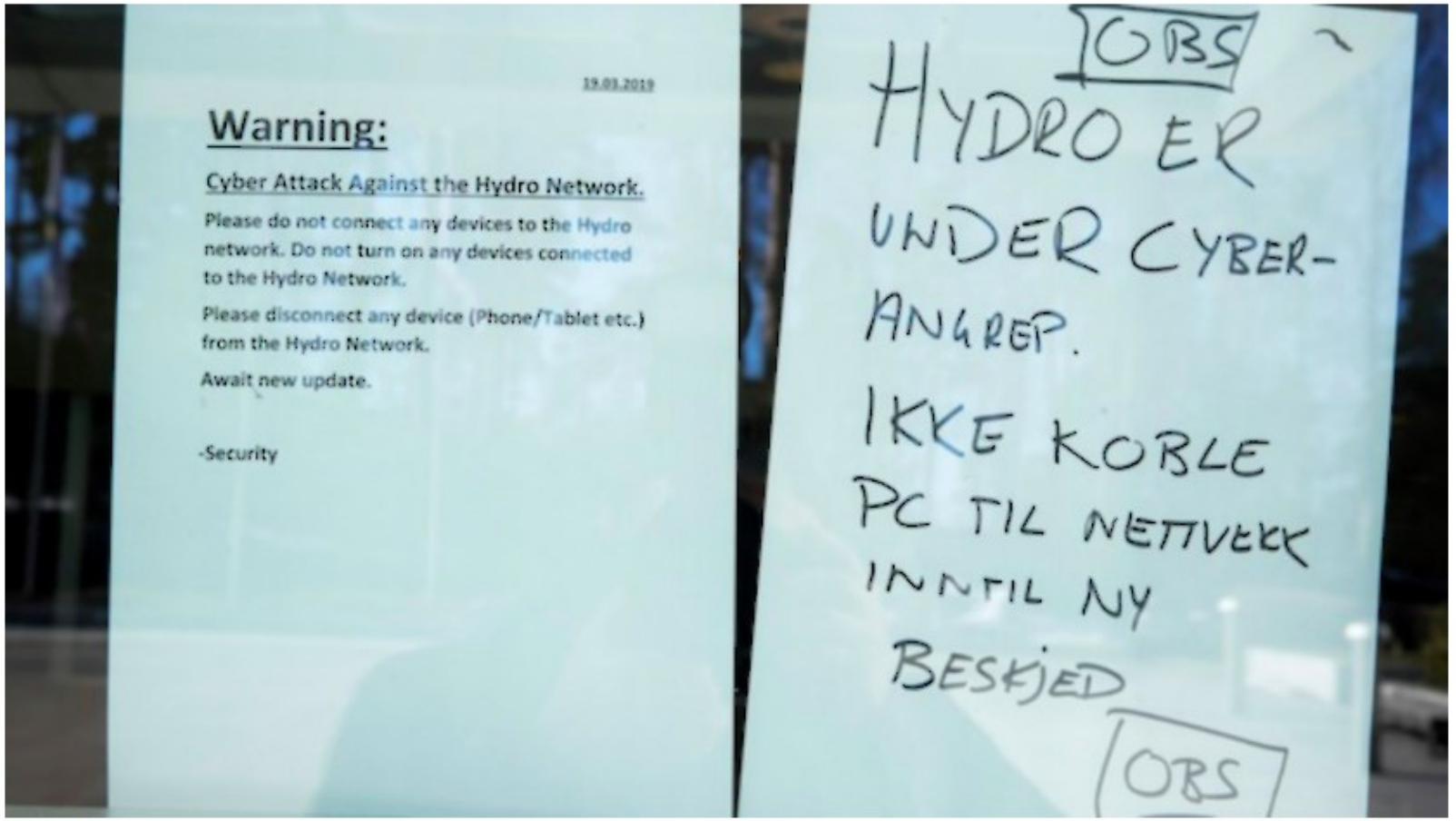


https://qzs.com.sg/maritime-it-shipboard-support/

LockerGoga Ransomware Sends Norsk Hydro Into Manual Mode

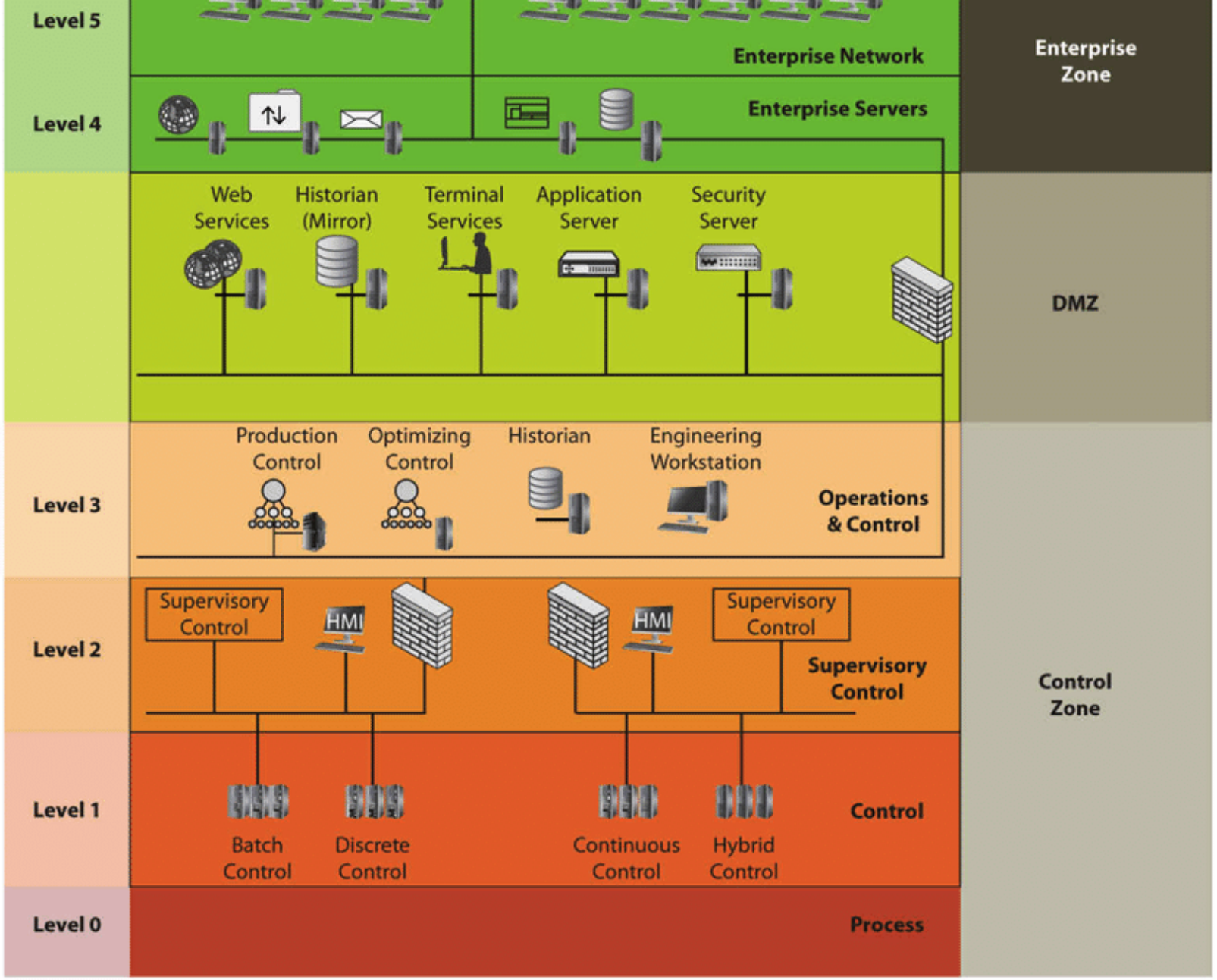
By Ionut Ilascu

March 19, 2019 09:48 AM 1



One of the largest aluminum producers in the world, Norsk Hydro, has been forced to switch to partial manual operations due to a cyber attack that is allegedly pushing LockerGoga ransomware.

https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/

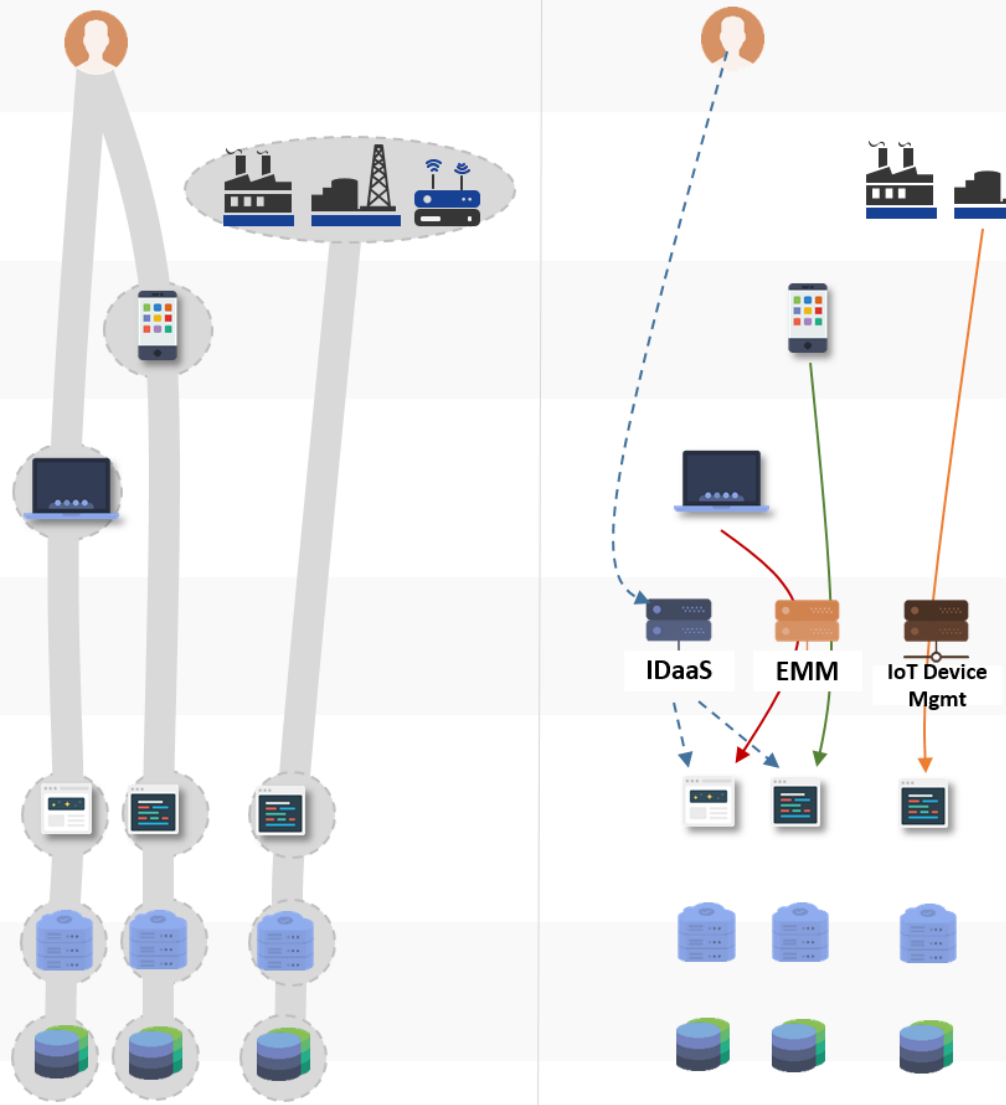


Experience and Lessons in Building an ICS Security Testbed, https://ieeexplore.ieee.org/document/8850804

Example of achieving Zero Trust through network micro-segmentation

Example of achieving Zero Trust through an identity-centric approach

Example of Roots of Trust anchors for enabling Zero Trust by Design



A corporate badge: used for both physical and logical access

Ruggedized Secure Element: used for securing credentials and cryptographic functions

Secure Element or TEE: used for securing credentials and performing cryptographic functions in a secure enclave

Trusted Platform Module: used for securing credentials and performing cryptographic functions securely

Hardware Security Module: tamper-proof hardware for securing credentials and performing cryptographic functions

https://www.linkedin.com/pulse/zero-trust-design-haider-iqbal

Kiitos

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus