Edith Cowan University
School of Science

Improving Critical Infrastructure Security

Dr Ahmed Ibrahim

Outline

- Critical Infrastructure
- Security Concerns
- Research at ECU
- Port Security
- Research Challenges

What is Critical Infrastructure?

What is “Critical” Infrastructure? (USA)

United States of America, Patriot Act of 2001, **Critical Infrastructure** is defined as:

> *“systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”*

https://www.congress.gov/bill/107th-congress/house-bill/3162

What is “Critical” Infrastructure? (Singapore)

Singapore, Cybersecurity Act, Section 7(1):

*“a **Critical Information Infrastructure** is a computer or a computer system located wholly or partly in Singapore, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore.”*

https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx

What is “Critical” Infrastructure? (Sri Lanka)

Sri Lanka, Cyber Security Bill 2019, Section 17:

An institution is said to have **Critical Information Infrastructure**:

“(a) the disruption or destruction of the computer system or computer program would have serious impact on the national security, public health, public safety, confidentiality, or economic well –being of citizens, or the effective functioning of the government or the economy of Sri Lanka; and

(b) the computer program or the computer system is located wholly or partly in Sri Lanka.”

https://www.cert.gov.lk/documents/Cyber%20Security%20Bill.pdf

Critical Infrastructure Sectors

1. Communications
2. Data storage or processing
3. Defence industry
4. Energy
5. Financial services and markets
6. Food and grocery
7. Health care and medical
8. Higher education and research
9. Space technology
10. Transport
11. Water and sewerage

Security of Critical Infrastructure Act 2018

No. 29, 2018

8E Meaning of *critical infrastructure sector asset*

(1) An asset is a ***critical infrastructure sector asset*** if it is an asset that relates to a critical infrastructure sector.

Deeming—when asset relates to a sector

(10) For the purposes of this Act, each of the following assets is taken to relate to the transport sector:

(a) a critical port;

(b) a critical freight infrastructure asset;

(c) a critical freight services asset;

(d) a critical public transport asset;

(e) a critical aviation asset.

Critical Infrastructure Characteristics

- Multiple Systems
- Provides Essential Services
- National Security
- Public Health and Safety
- Economic wellbeing

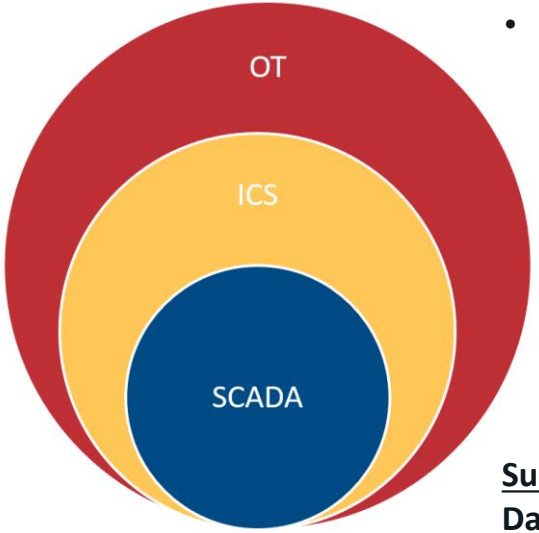
Operational Technology (OT)

*"Programmable systems or devices that interact with the **physical environment** (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.*

Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms."

NIST SP 800-37 Rev. 2

OT vs ICS vs SCADA

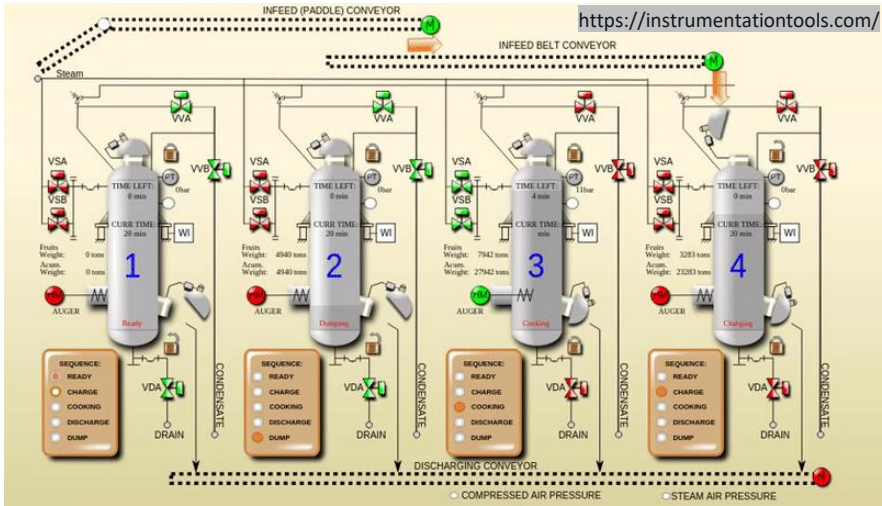


Industrial Control Systems

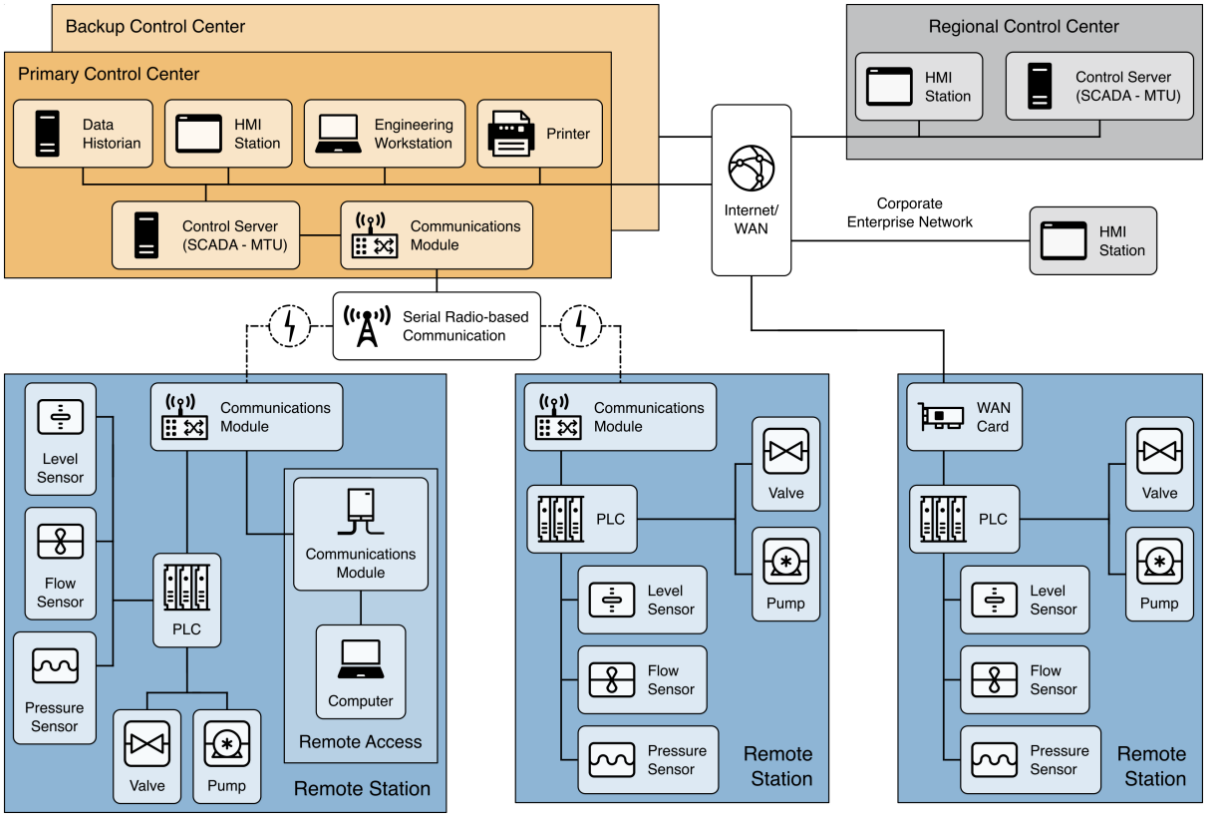
- Conveyor belt
- Power consumption
- Valve pressures

Supervisory Control And Data Acquisition

1. Central command centre
2. Local control systems
3. Communication systems

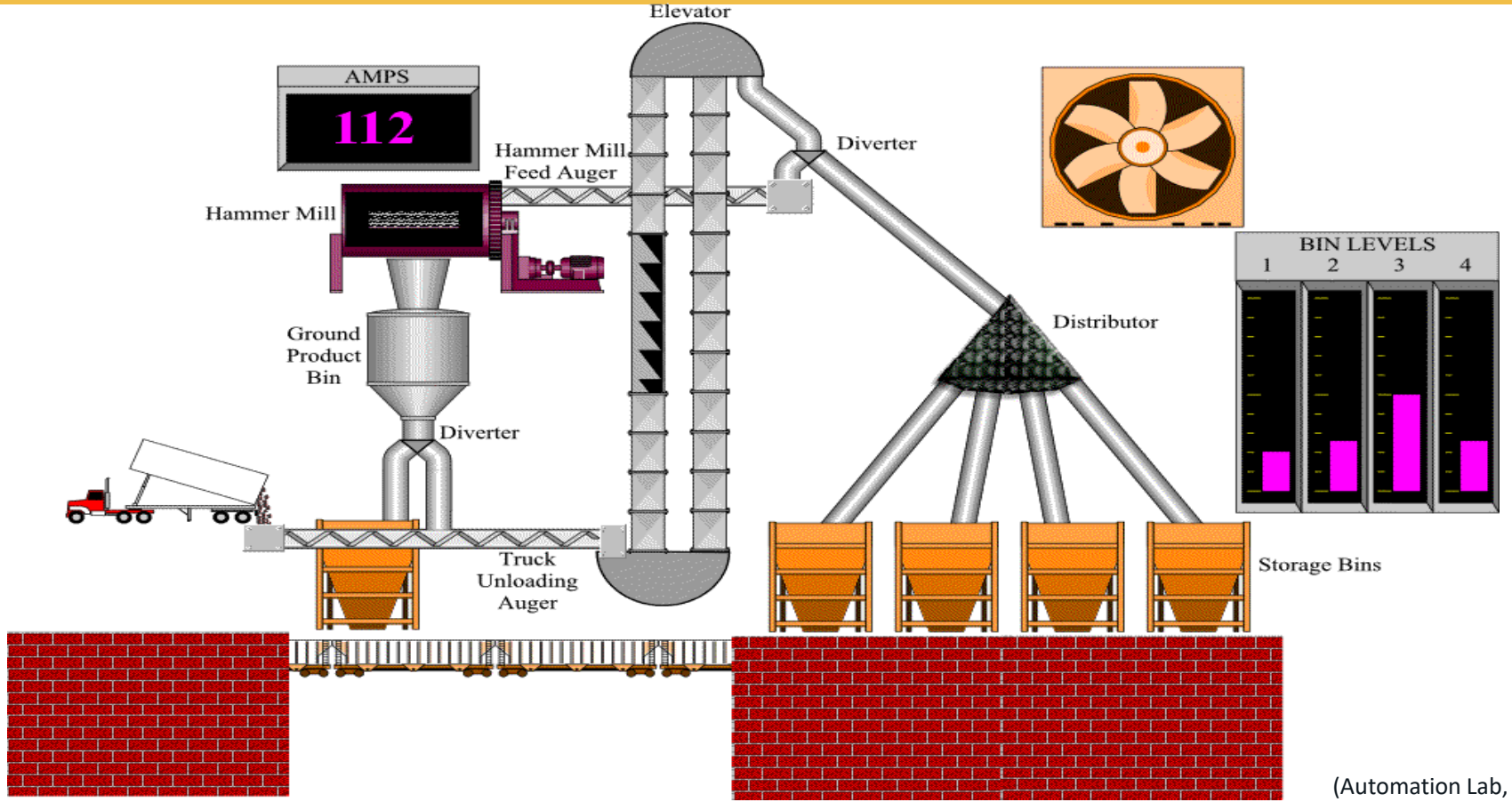


SCADA System Implementation Example



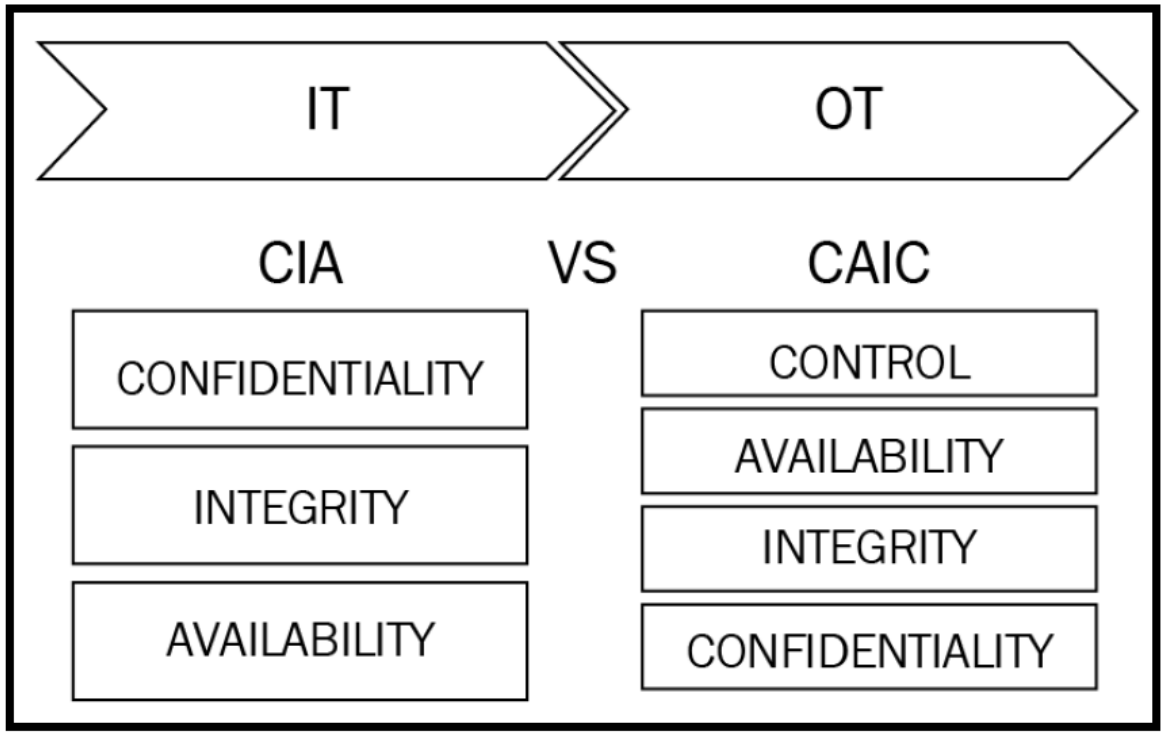
SP 800-82 Rev. 3 (Draft) (2022, p12)

Industrial Automation



(Automation Lab, IIT Delhi)

Divergent Priorities of IT and OT

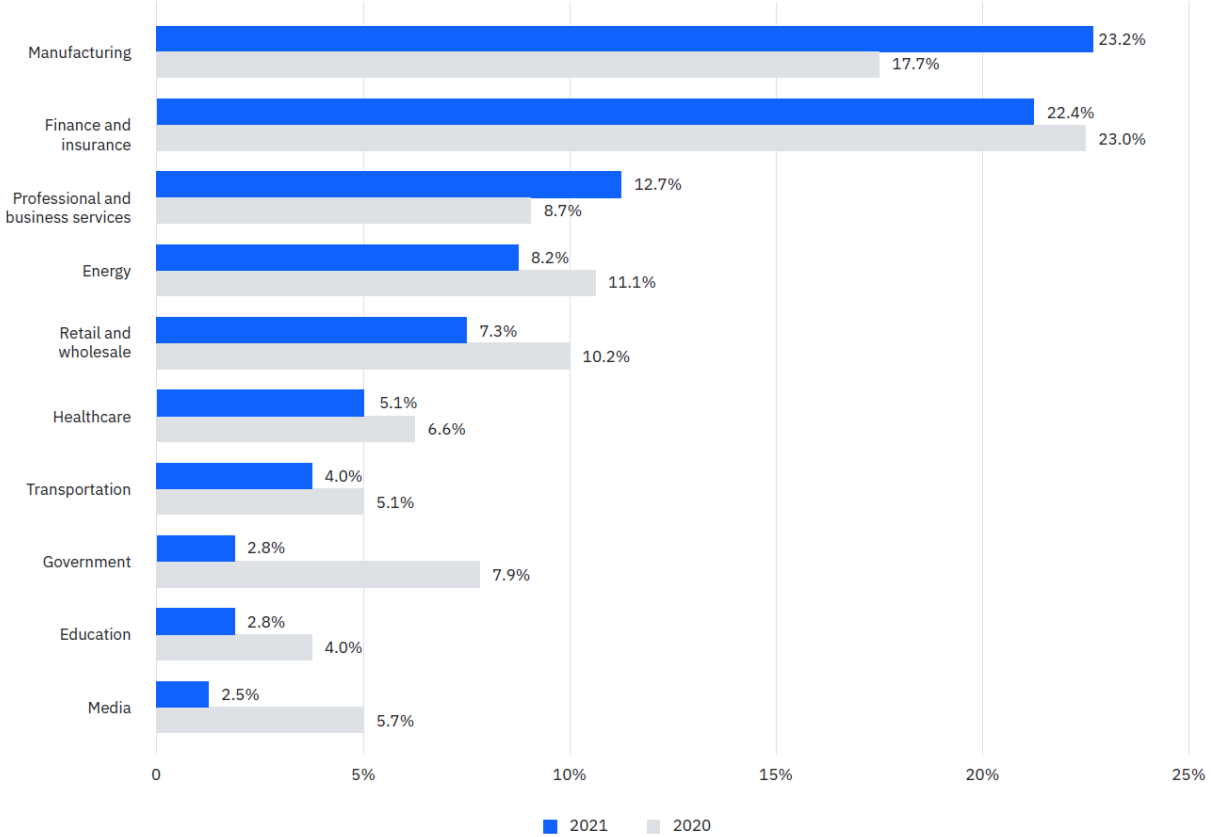


Bhattacharjee (2018, p26)

Threat Sources (US-Cert, CISA)

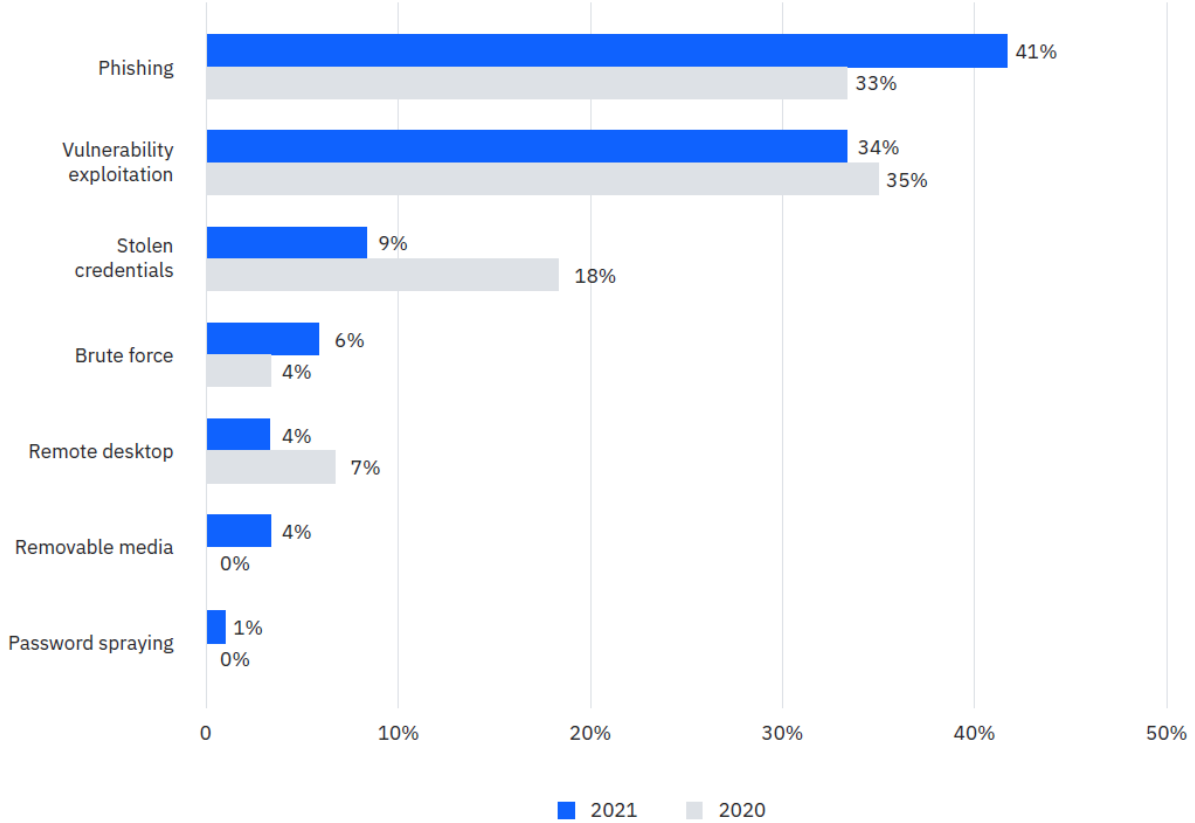
- National Governments
- Terrorists
- Industrial Spies
- Organized Crime Groups
- Hacktivists
- Hackers

Breakdown of attacks on the top 10 industries, 2021 vs 2020

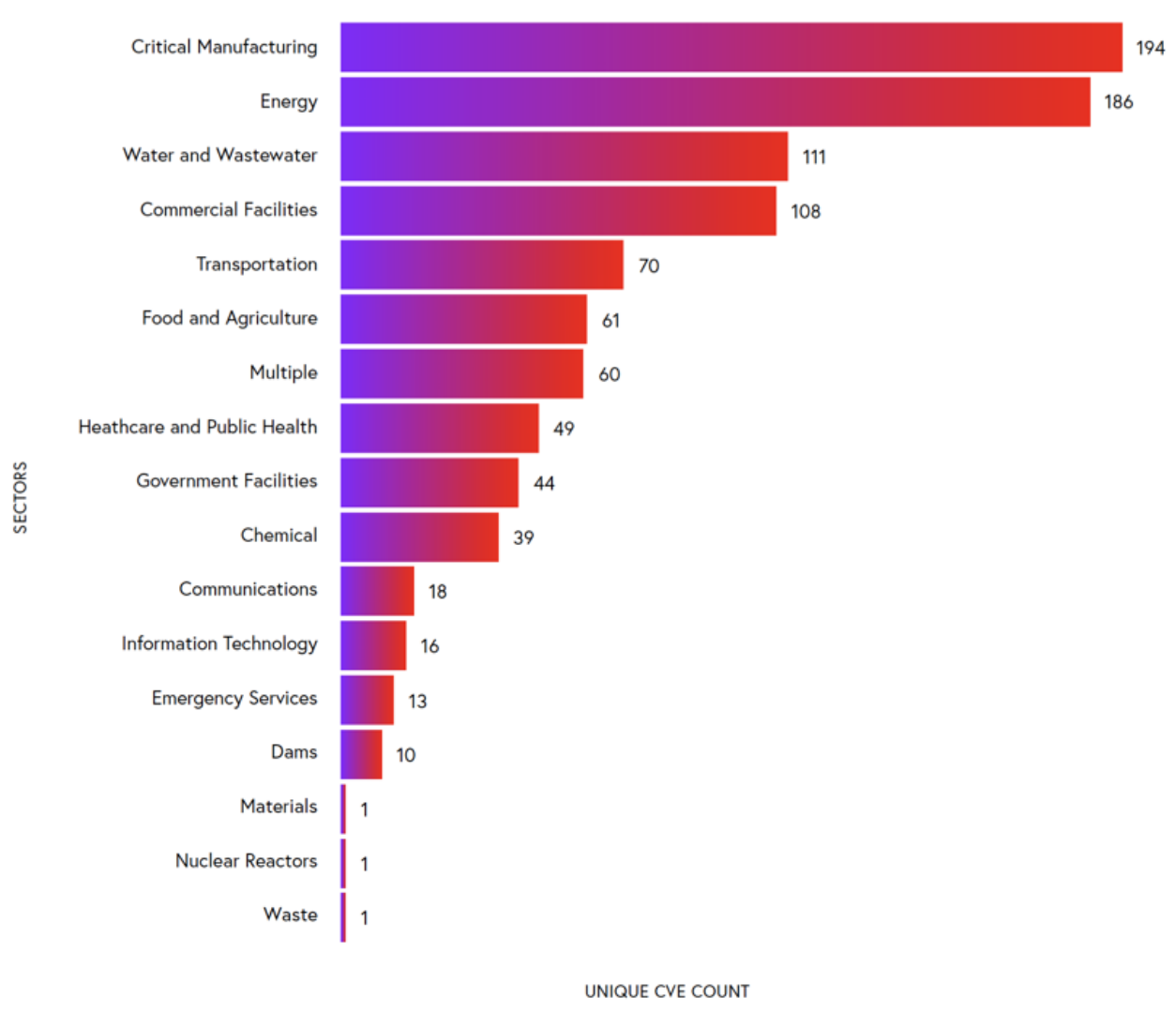


IBM (2022, p42)

Top infection vectors, 2021 vs 2020



IBM (2022, p16)



Vulnerabilities per sector

Claroty (2021, p19)

Top 5 ICS Cyber Attacks

1. ICS Insider
2. IT Insider
3. Common Ransomware
4. Targeted Ransomware
5. Zero-Day Ransomware

FireEye (Ginter, 2018)

History of ICS Incidents (Hamsley & Fisher, 2018, p2-3)

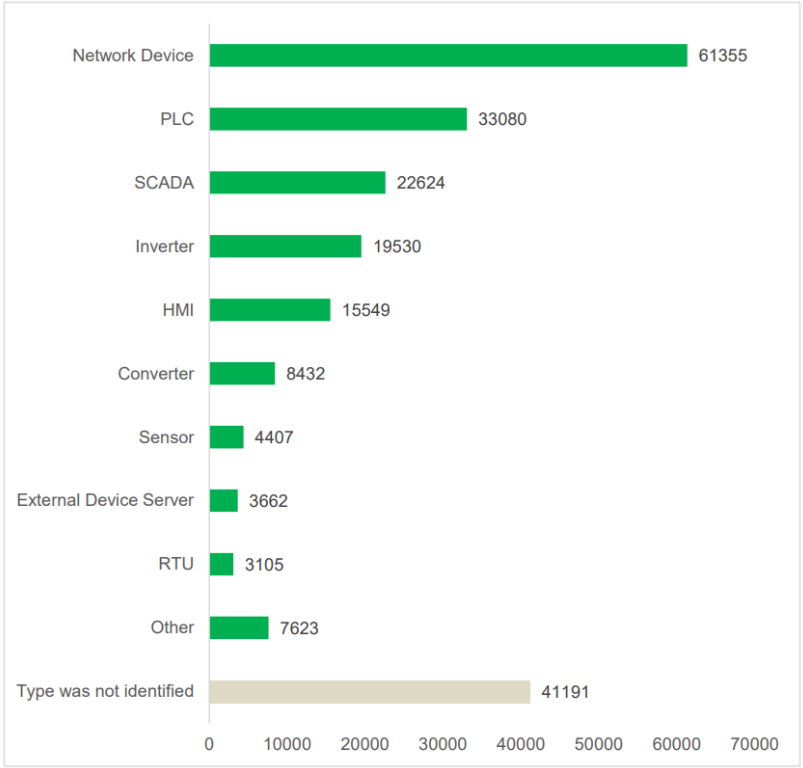
Table 1. ICS cyber-incident timeline.

Year	Type	Name	Description
1903	Attack	Marconi Wireless Hack	Marconi's wireless telegraph presentation hacked with Morse code.
2000	Attack	Maroochy Water	A cyber-attack caused the release of more than 265,000 gallons of untreated sewage.
2008	Attack	Turkey Pipeline Explosion (not quite cyber)	Did attackers use a security camera's vulnerable software to gain entrance into a pipeline's control network?
2010	Malware	Stuxnet	The world's first publically known digital weapon.
2010	Malware	Night Dragon	Attackers used sophisticated malware to target global oil, energy, and petrochemical companies.
2011	Malware	Duqu/ Flame/Gauss	Advanced and complex malware used to target specific organizations, including ICS manufacturers.
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identified an active series of cyber-intrusions targeting the natural gas pipeline sector.
2012	Malware	Shamoon	Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.
2013	Attack	Target Stores	Hackers initially gained access to Target's sensitive financial systems through a third-party that maintained its HVAC ICSs, costing Target $309M.
2013	Attack	New York Dam	The U.S. Justice Department claims Iran conducted a cyber-attack on the Bowman Dam in Rye Brook, NY.
2013	Malware	Havex	An ICS-focused malware campaign.

Table 2. ICS cyber-incident timeline (continued).

Year	Type	Name	Description
2014	Attack	German Steel Mill	A steel mill in Germany experienced a cyber-attack resulting in massive damage to the system.
2014	Malware	Black Energy	Malware that targeted human-machine interfaces (HMIs) in ICSs.
2014	Campaign	Dragonfly/Energetic Bear No. 1	Ongoing cyber-espionage campaign primarily targeting the energy sector.
2015	Attack	Ukraine Power Grid Attack No. 1	The first known successful cyber-attack on a country's power grid.
2016	Attack	"Kemuri" water company	Attackers gained access to hundreds of the programmable logic circuits (PLCs) used to manipulate control applications, and altered water treatment chemicals.
2016	Malware	Return of Shamoon	Thousands of computers in Saudi Arabia's civil aviation agency and other Gulf State organizations wiped in a second Shamoon malware attack.
2016	Attack	Ukraine Power Grid Attack No. 2	Cyber-attackers tripped breakers in 30 substations, turning off electricity to 225,000 customers in a second attack.
2017	Malware	CRASHOVERRIDE	The malware used to cause the Ukraine power outage was finally identified.
2017	Group	APT33	A cyber-espionage group targeting the aviation and energy sectors.
2017	Attack	NotPetya	Malware that targeted the Ukraine by posing as ransomware, but with no way to pay a ransom to decrypt altered files.
2017	Campaign	Dragonfly/Energetic Bear No. 2	Symantec® claims energy sector is being targeted by a sophisticated attack group.
2017	Malware	TRITON/Trisis/ HatMan	Industrial safety systems in the Middle East targeted by sophisticated malware.

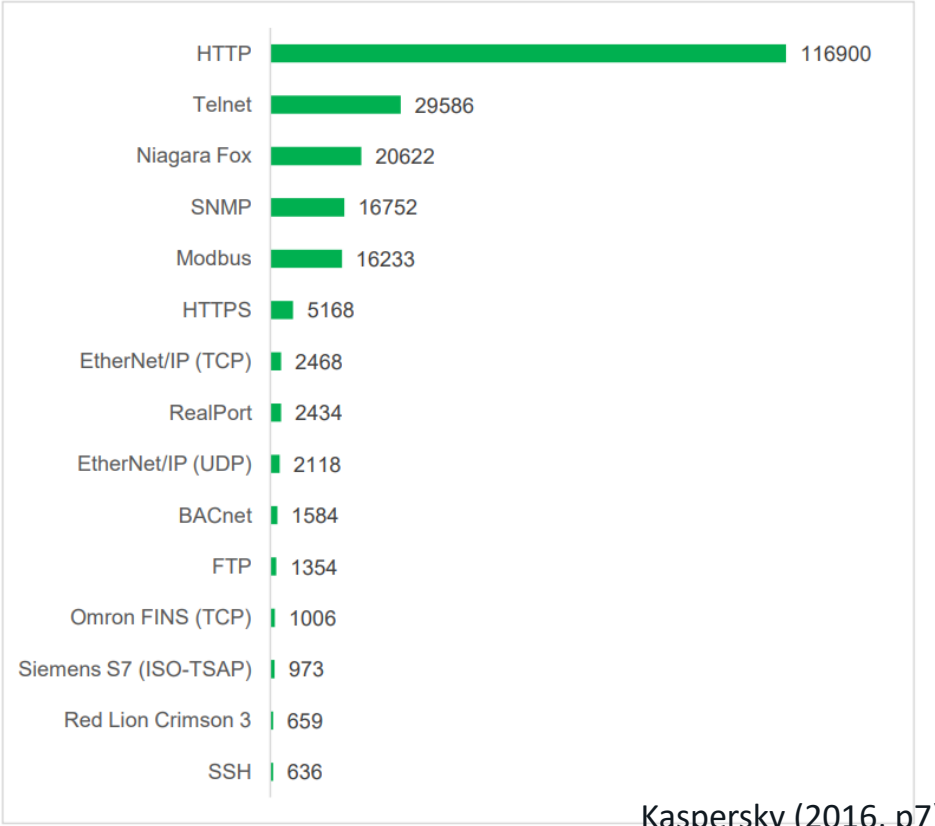
Industrial Components



Kaspersky (2016, p6)

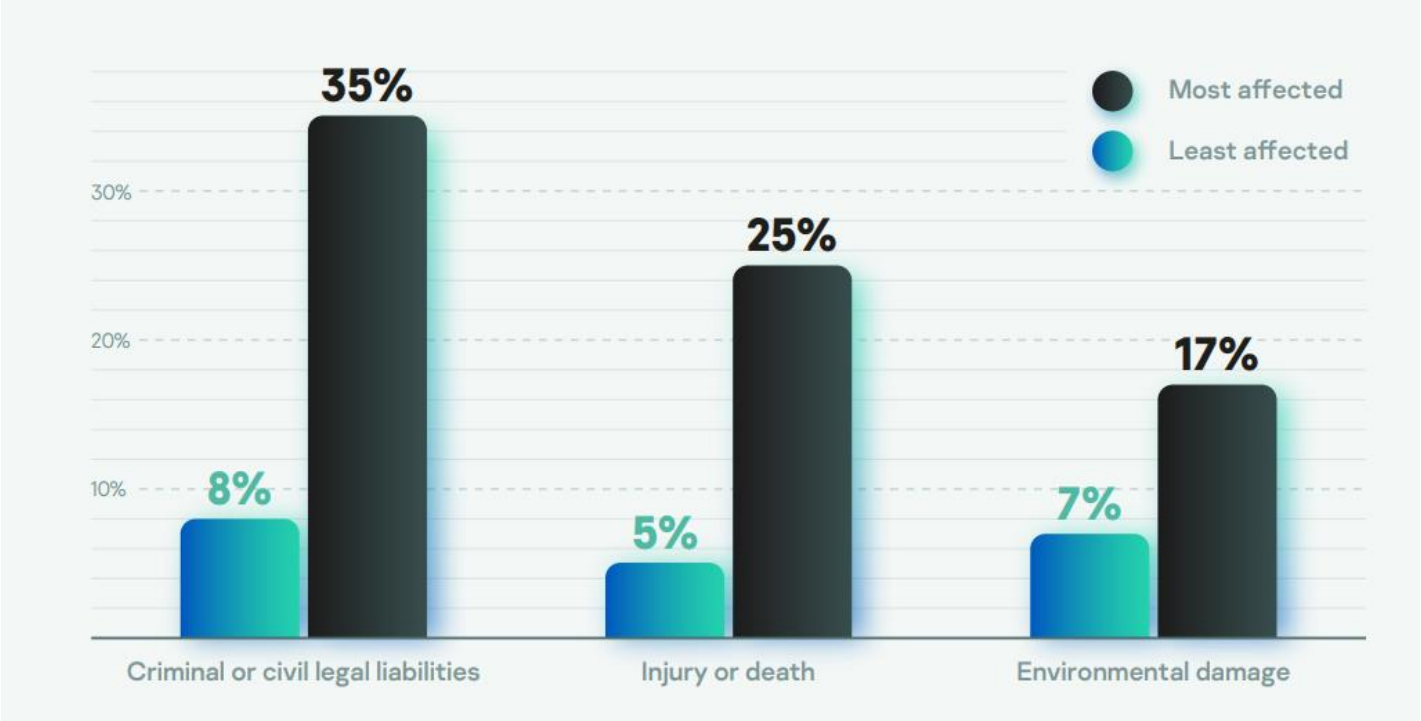
Industrial Protocols

88% are insecure by design



Kaspersky (2016, p7)

Consequences of OT/ICS intrusions / breaches



Kaspersky (2022, p9)

Critical Infrastructure Security Research at ECU

Critical Infrastructure Security Training

Industrial Control Systems Training

- Cyber Security Practices and Ethical Hacking
- Technical and Non-Technical Participants

Red VS Blue Team Exercise

- Chemical Processing Plant
- Virtual Environment (enterprise/OT network and assets)
- Documentation (outdated intentionally)
- Devices (vulnerable intentionally)
- Management team (useful to some extent)

Critical Infrastructure Security Research @ ECU

ECU Security Research Institute

Securing Critical Infrastructure

Ongoing PhD:

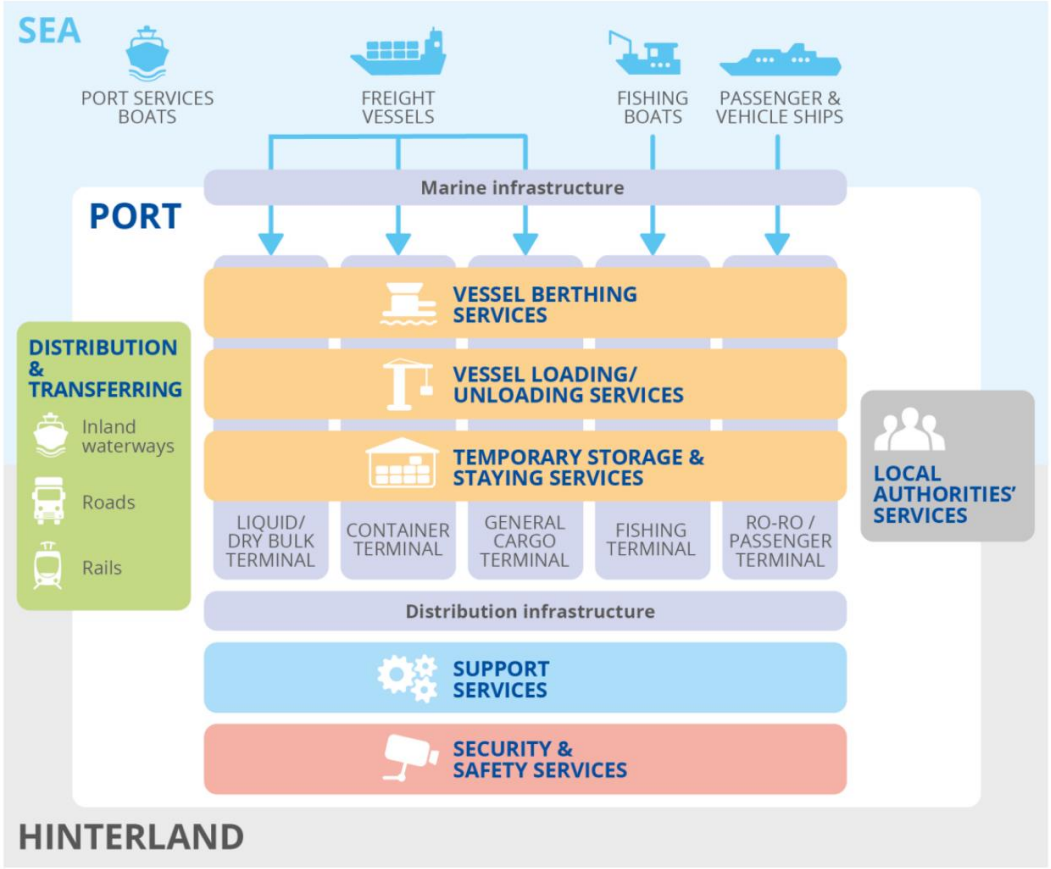
- Malware Detection in Cyber-Physical Systems (CPS)
- Mining SCADA Alarm Analysis by Autonomous Operator to Identify Cyber-Physical Attacks

Funded Research:

- Multi-factor Authentication in Medical Contexts for Pharmaceutical Dispensary Functions
- Cyber Range for Port Security

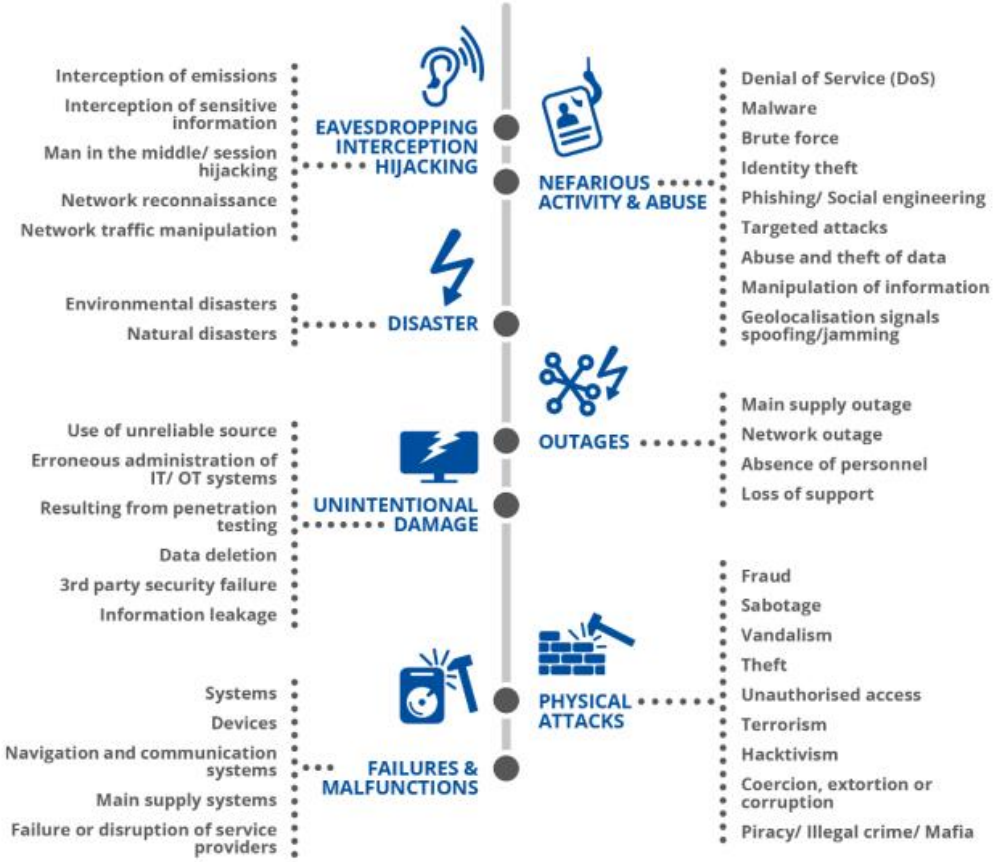
Port Security

Port Services and Infrastructure



ENISA (2019, p16)

Threat Taxonomy



ENISA (2019, p27)

Cyber attacks related to ports

Table 2
Cyberattacks in maritime transport industry.

Firm	Type of operator	Type of cyberattack	Year	Source
Islamic Republic of Iran Shipping Lines	Shipping line	Cyberattack	2011	Torbati and Saul, (2012); Hayes (2016)
Japanese and Korean shipbuilding	Ship builder	Advanced phishing attacks Persistent threat	2013	Hayes (2016); Shaikh (2017); ICS (2018)
Maritime industry in South Korea	Shipping line Port operator	Cyberattack	2016	Shaikh (2017); Nichols (2016)
Maersk line and Maersk group's APM Terminals	Shipping line Port operator	Malware Cyber extortion	2017	Jensen (2017); Fosen (2019)
BW Group	Shipping operator Floating gas infrastructure	Hacktivism	2017	Fosen (2019)
FedEx	Logistics company	Wiper virus for deleting data	2017	McKevitt (2017)
Clarkson Plc	Shipbroker	Hacktivism	2017	Kennard (2019)
Port of Barcelona	Port operator	Ransomware attack	2018	Aharoni (2018)
COSCO terminal in Long Beach Port	Port operator	Ransomware attack	2018	Aharoni (2018); Fosen (2019)
US Port of San Diego	Port operator	Cybersecurity incident Ransomware attacks	2018	The Institute of Marine Engineering, Science and Technology (2018)
Total Quality Logistics (TQL)	Logistics company Freight broker	Data phishing attempt	2020	TQL (2020); Forde (2020)
Toll Group	Freight forwarder	Ransomware attack	2020	Otago Daily Times (2020)

Senarak (2021, p24)

Traffickers using hackers to import drugs into major Europe ports

Europol disclose that drug traffickers have recruited hackers to help them smuggle shipments of contraband into major ports including Antwerp

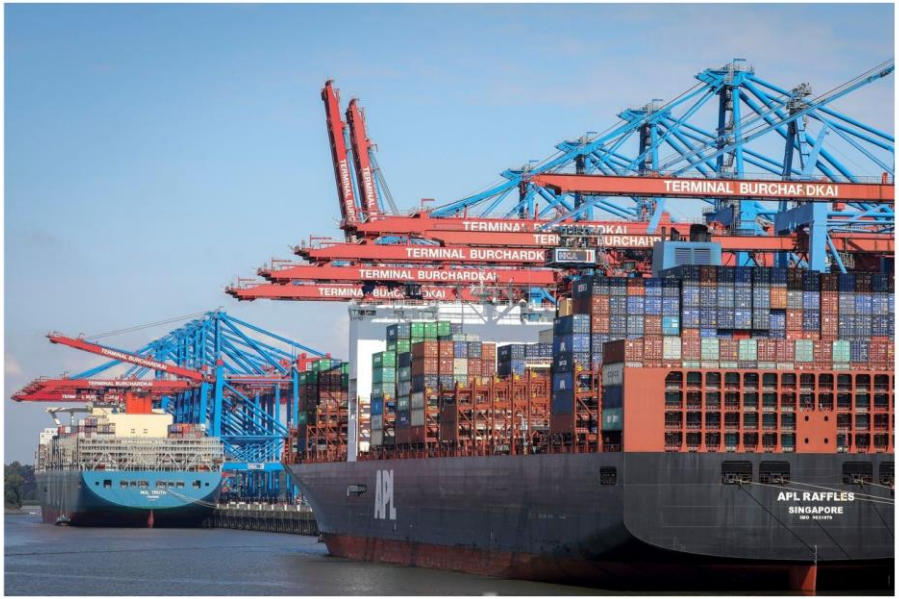
By Colin Freeman
16 October 2013 • 3:30pm

2020

LOGISTICS REPORT

Global Maritime Regulator Hit by Cyberattack

International Maritime Organization is the second shipping entity attacked by hackers in the past week



The frequency of cyberattacks against the maritime sector has increased this year, underscoring weaknesses in security systems at companies that are major carriers of global goods trade.

PHOTO: FOCKE STRANGMANN/EPA-EFE/REX/SHU/EPA/SHUTTERSTOCK

By Costas Paris Follow

Updated Oct. 1, 2020 11:30 am ET

French shipping giant CMA CGM suffers data breach

Jessica Haworth 21 September 2021 at 12:40 UTC
Updated: 21 September 2021 at 14:50 UTC

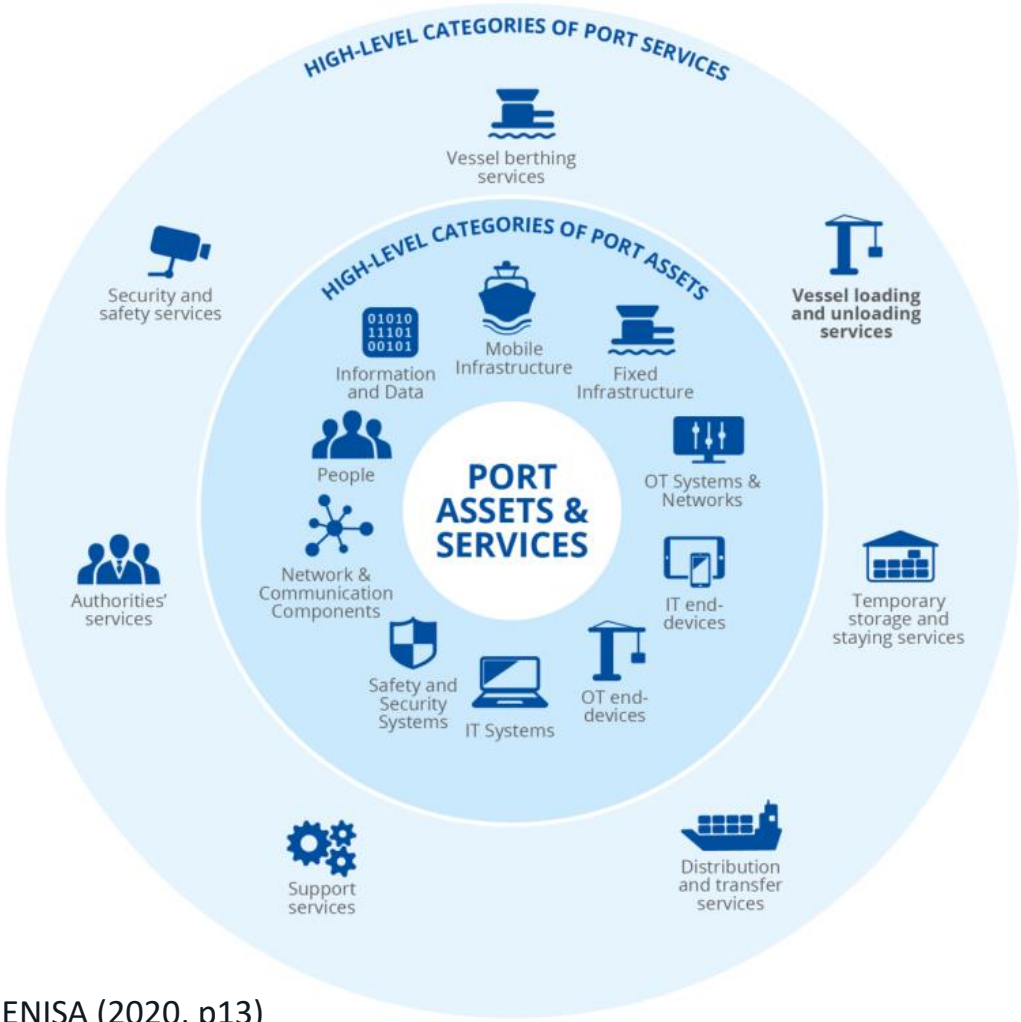
Data Breach | Data Leak | Maritime

Customer data impacted by security incident

French shipping company CMA CGM has announced it has suffered a data breach.

The container transportation and maritime giant, based in Marseille, revealed in a security advisory that customers' names, email addresses, phone numbers, and employment information have been leaked.

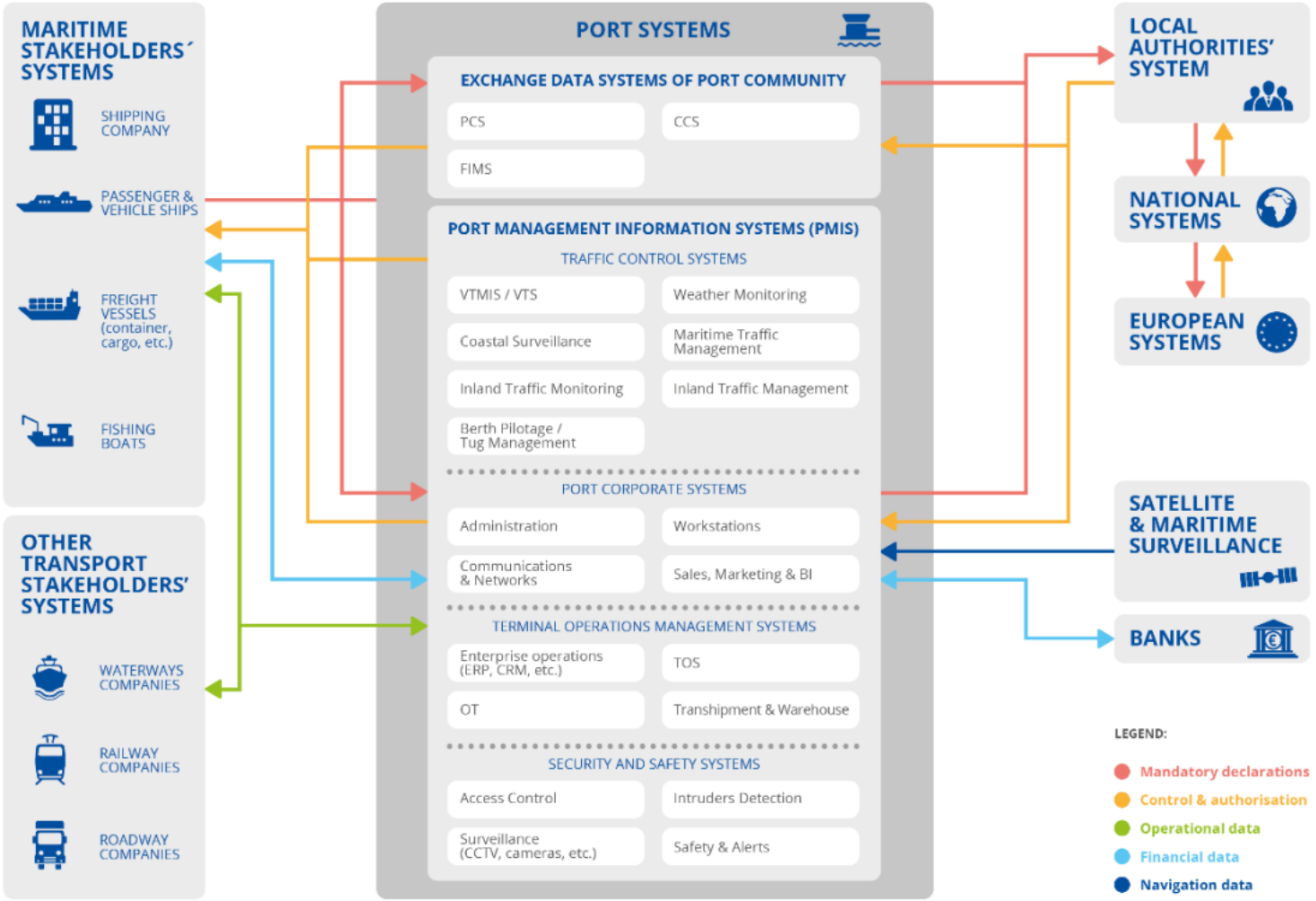
It has not yet been confirmed how many individuals were affected by the incident, but CMA CGM said that its operations were not affected.



High-level categories of port assets and services

ENISA (2020, p13)

Port Systems Data Flows



ENISA (2019, p18)

Research Challenges

Research Challenges

1. Different ports function differently
2. Capturing cyber-physical aspects
3. Time synchronisation across various systems
4. Capturing and measuring human factors
5. Lack of specific datasets

Feel free to get in touch and connect

Email: **ahmed.ibrahim@ecu.edu.au**

Twitter: @**ai8rahim**