



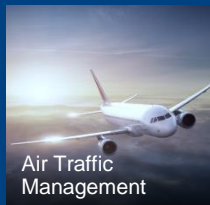
FREQUENTIS
FOR A SAFER WORLD

Security & Safety-Challenges im sicherheitskritischen Umfeld

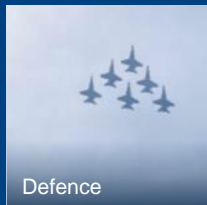
Ing. Philipp Lellek

Dipl.-Ing. Gianluca Raberger

We set standards
in control centres
worldwide



Air Traffic
Management



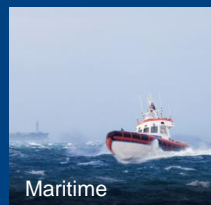
Defence



Public
Safety



Public
Transport

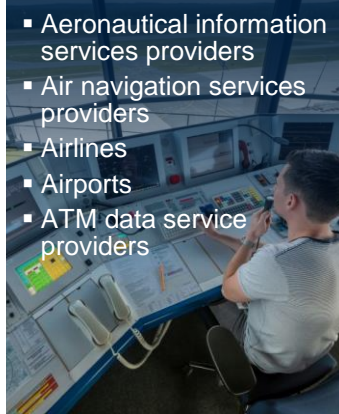


Maritime

Safety-critical control centre solutions – across industries



Civil

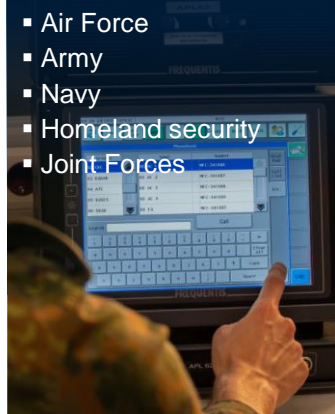


- Aeronautical information services providers
- Air navigation services providers
- Airlines
- Airports
- ATM data service providers

Air Traffic Management



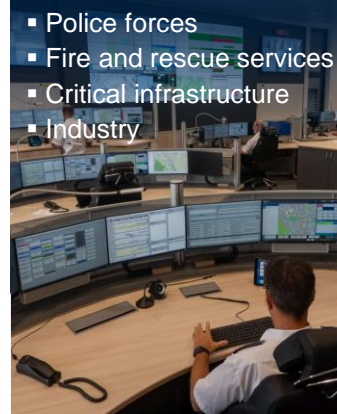
Defence



- Air Force
- Army
- Navy
- Homeland security
- Joint Forces



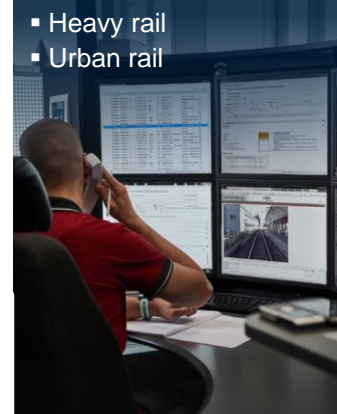
Public Safety



- Police forces
- Fire and rescue services
- Critical infrastructure
- Industry



Public Transport

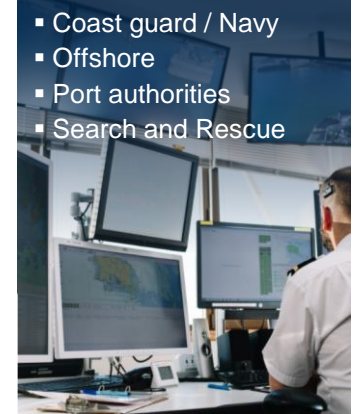


- Heavy rail
- Urban rail

Public Safety & Transport



Maritime




- Coast guard / Navy
- Offshore
- Port authorities
- Search and Rescue

Contributing significantly to the successful completion of safety tasks

A strong network around the world


30,000+
working positions using
Frequentis solutions

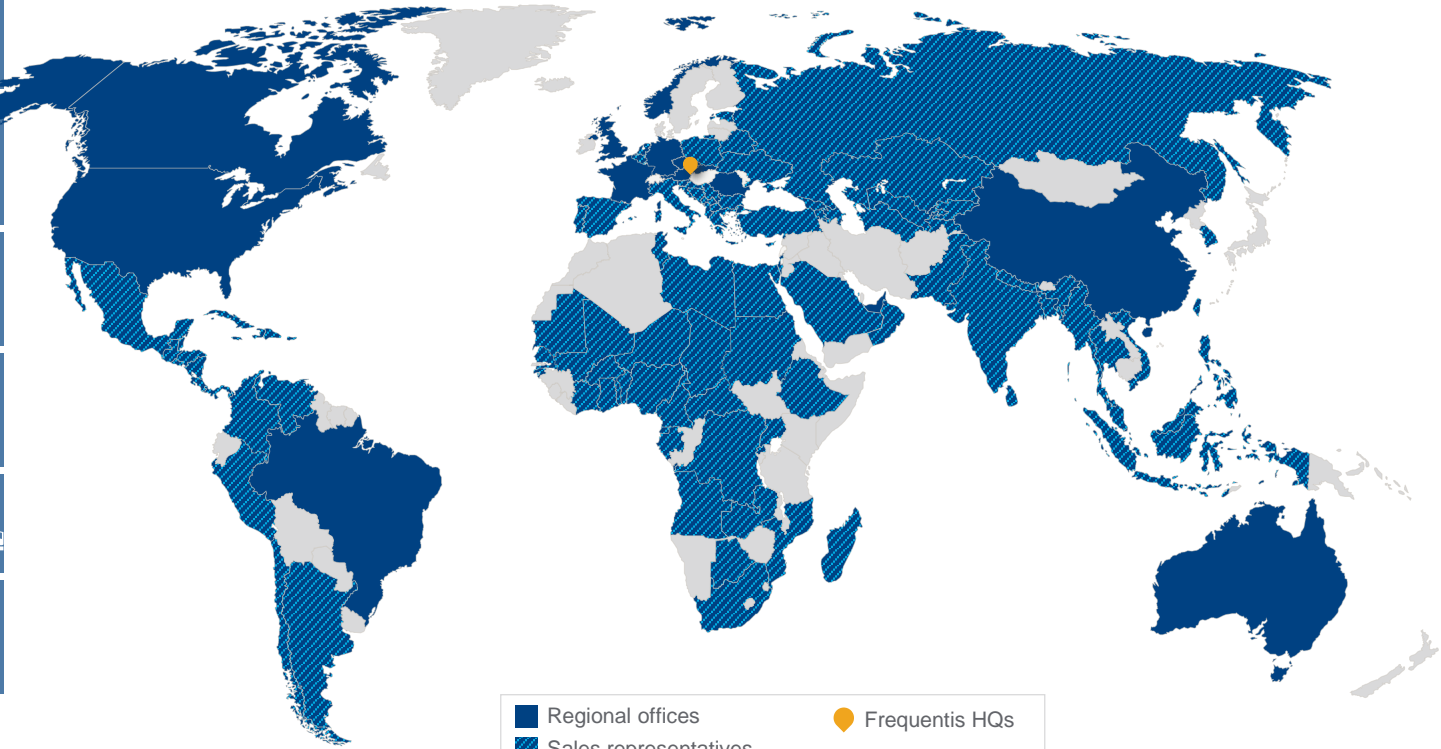
500+ customers **140** countries

90%
of all air passengers globally are
served by Frequentis customers 

33%
of the world safer with
Frequentis networks

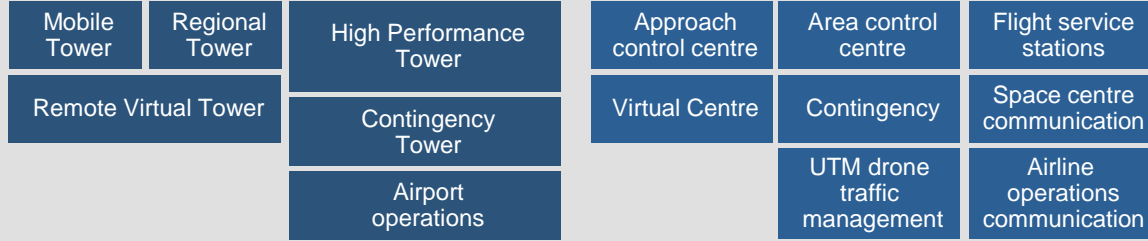
#1 in GSM-R
dispatcher terminals 

240,000 km
protecting the largest
maritime coastline 



Air Traffic Management – solutions overview

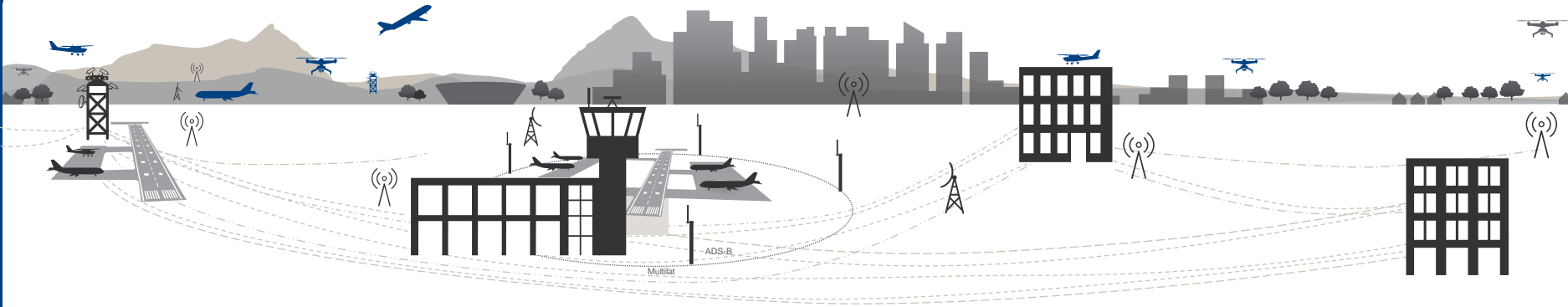
- ▶ Communication
- ▶ Automation
- ▶ Surveillance



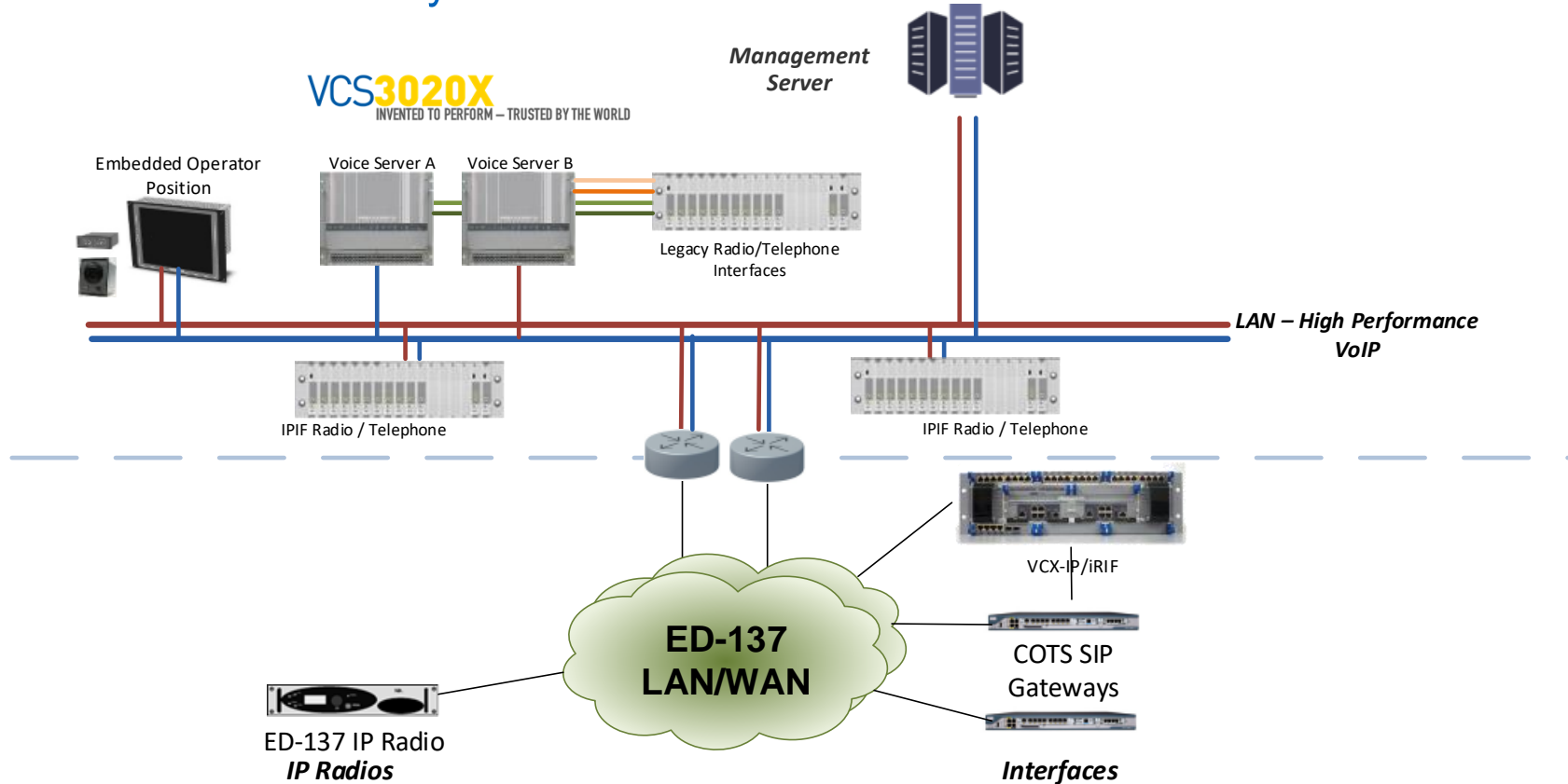
▶ Information Mgmt.

- Flight planning
- Data mgmt.
- NOTAM mgmt.
- Electronic Publications & Charting
- Digital briefing
- Messaging / SWIM

▶ Networks



Voice Communication System Architecture



Framework and standards

Keeping the system secure and safe during operation

Legal frameworks

- E.U. NIS directive 2016
- U.S. Homeland Security Act and NIPP 2013
- AU: Security of Critical Infrastructure Act 2018
- SGP: Cybersecurity Bill 2018

Standards

- NIST Cyber Security Framework for Critical Infrastructures
- ISO 2700x Information Security Management
- IEC 62443 Industrial system security
- **ED 205 Aeronautical Information systems security**

Best practises

- CIS benchmarks, CIS controls
- BSIMM software security framework
- Next Generation 9-1-1 Security (NG-SEC)
- ENISA guidelines
- ASD Top 4 Mitigation Strategies

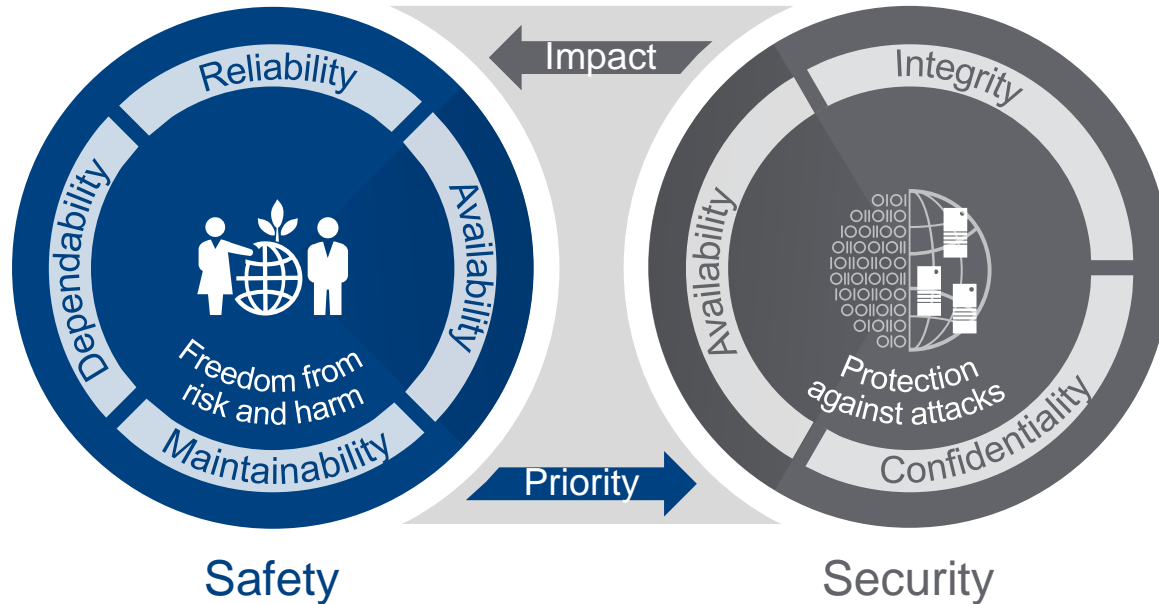
Due care

Prime responsibility of the system operator

Common interest and collaborative effort of system operator, integrator and vendors

Safety and security need to go hand in hand

Safety is the primary goal - security is a prerequisite



Safety and security need to go hand in hand

Finding the right balance



Integrated safety and security methodology

Examples of customer requirements

With potential safety impact

Patching times

“Updates to **remediate critical vulnerabilities** shall be provided within a shorter period than other updates, **within at least three (3) days**”

Testing of Patches

“**All** security-related **service packs, patches, and hot-fixes** shall be **tested** and **applied to all servers on a regular basis.**”

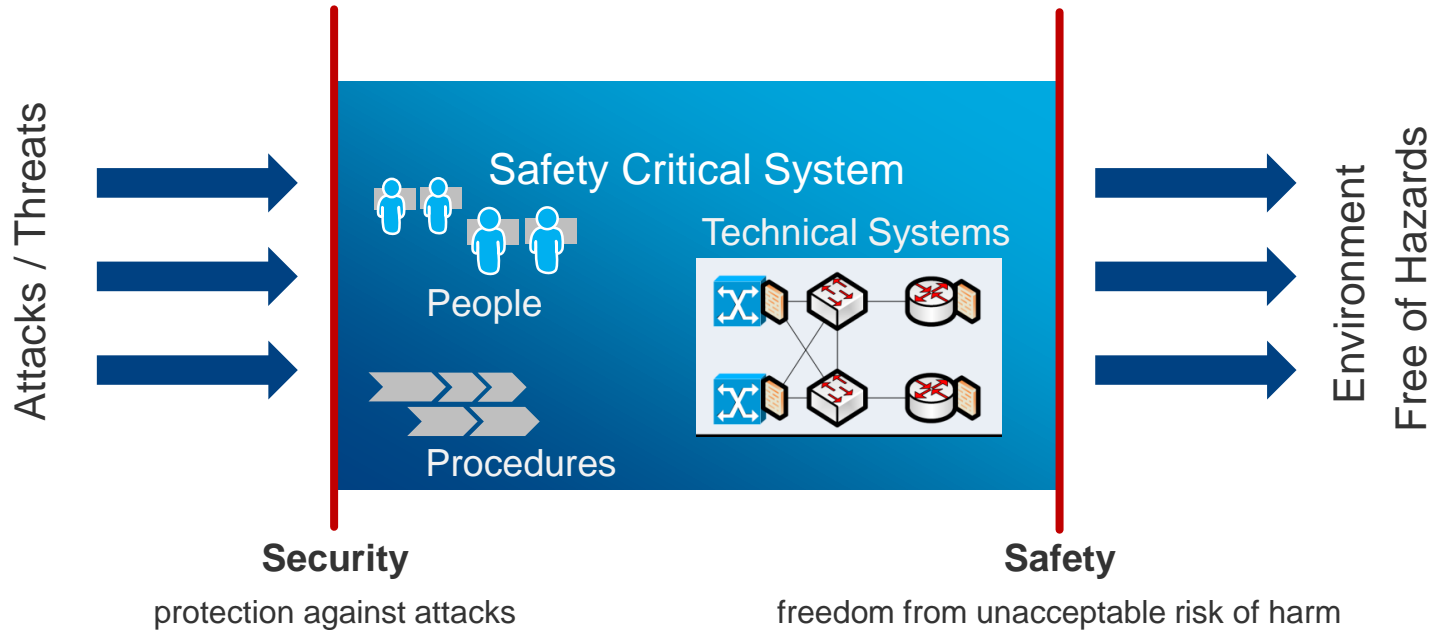
Malware Protection

“The cybersecurity requirements for [...] must include at least the following: Advanced, up-to-date and **secure management of malware and virus protection** on servers and workstations.”

Authentication

“The system should **implement multifactor authentication for local access.**”

Managing Safety and Security



Security impacts Safety
Safety has priority over Security

What are the challenges?

Any change needs an impact assessment, an updated safety case, complete test evidence, and a formal approval!



Rare, long planned updates



Frequent, short term patching



A patch for a critical vulnerability was published today, we need to patch our system asap!



Any change needs an impact assessment, an updated safety case, complete test evidence

Rare, long

Joint impact assessment of critical vulnerabilities and threat scenarios

short term patching

a critical vulnerability has been published, we need to patch our system today!



Safety relevant processes must never be stopped without a human intervention!



Fail-safe



Fail-secure



Antivirus and intrusion protection shall stop suspicious processes!



proc
stop

**Whitelisting approach
on safety critical components**

**Blacklisting approach (Anti Virus)
on supporting components**

intrusion
shall stop
processes
tely!



Security & Safety take aways

There is no “one fits all” solution

Security Risk Assessment

Priority on identification of most critical threat scenarios

For legacy systems > reassess the basics > verify assumptions

Joint assessment of security requirements

Security shall not increase safety risk or weaken established controls

i.e. Breaking segmentation in favour of centralised services > Re-evaluate zoning concept

Example of safety aligned technical controls

If something cannot be blocked, ensure extended monitoring & auditing is in place
i.e. Automatic brute force account lockout > trigger alert instead > if possible also rate limit

If data at rest encryption is not possible, ensure enforced physical protection is in place
i.e. Unlock requires physical presence of admin > delaying automatic system recovery > raise critical alert instead



FREQUENTIS

FOR A SAFER WORLD

Air Traffic
Management

Defence

Public
Safety

Public
Transport

Maritime