BRITISH APCO

Working in Partnership to Improve Public Safety Technology

TCCA

TETRA

TRUSTED · ALWAYS · EVERYWHERE

TETRA and sustainability of TETRA standard and equipment

Mladen Vratonjić TCCA Board Chair &
Francesco Pasquali, Leonardo, TCCA TIG Chair

Critical communications for all professional users

TCCA Mission

Provide a platform for the exchange of information and experience between members

Drive the evolution of critical communications worldwide

Promote the critical communications market and solutions to a global audience.

About us

We support open and standardised mobile critical communications technologies and complementary applications.

3GPP Market Representation Partner.

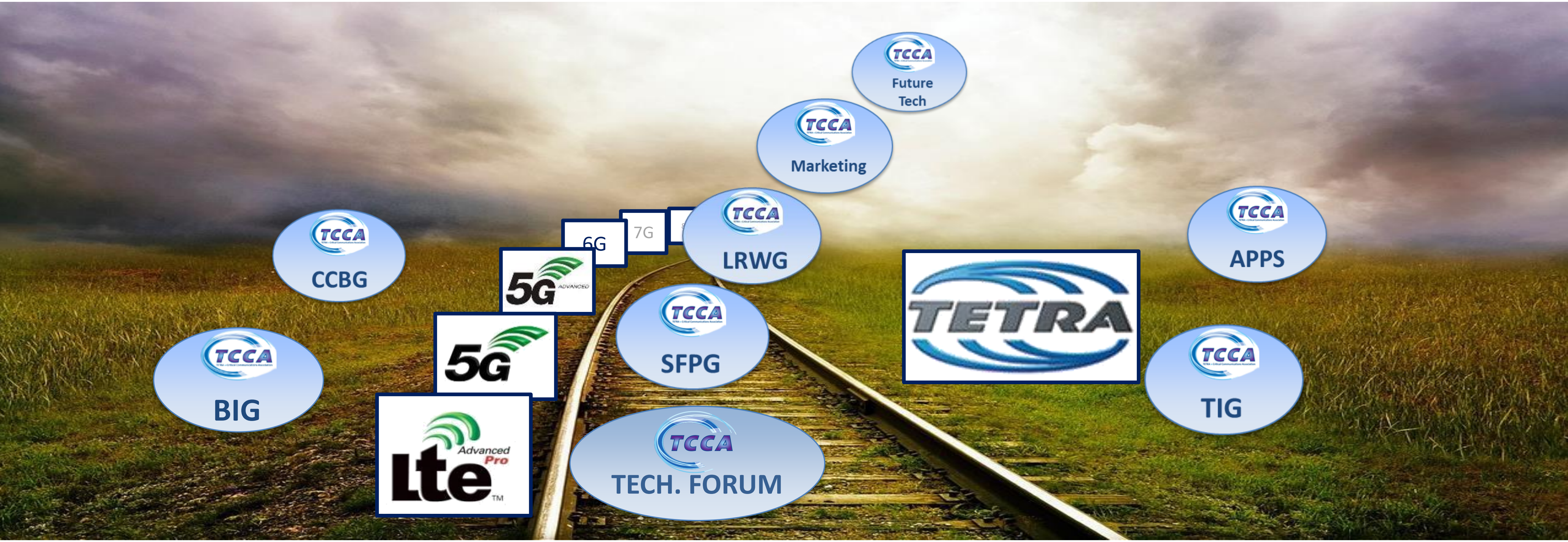
Catalysing competitive multivendor markets worldwide through open standards.

Our members include users, operators, industry and other stakeholders globally all sharing knowledge and experience.

Collaborative working across the critical communications ecosystem to develop and drive the most effective solutions for all.

Critical communications for all professional users

Continuous Evolution



Critical communications for all professional users

TCCA

TETRA evolves and have a long-term future

- □ ~~You may have heard somewhere TETRA is close to its end of life~~ FALSE

- □ One or more specific TETRA network might be close to End of Life (EOL), but **this is not due to the technology itself or lack of support from the industries,** but simply to investment strategies of individual organisations

- □ TETRA is an **alive & kicking** and still **evolving** technology with a brilliant future

FACTS

- □ **<u>TETRA is NOT close to its EOL or End of Support (EOS) as a technology</u>**

FACTS

- □ All TETRA industries continuously confirm their **commitment on TETRA** with new products, new features and new standardisation efforts

FACTS

- □ TETRA industries everyday sign contract taking **long term commitments** on TETRA product **maintenance** (e.g. up to 15-20 years for mass transit systems)

FACTS

- □ TETRA is **cutting-the-edge** technology, continuously renewed to face up with new challenges on which you can **invest today with TRUST**

FACTS

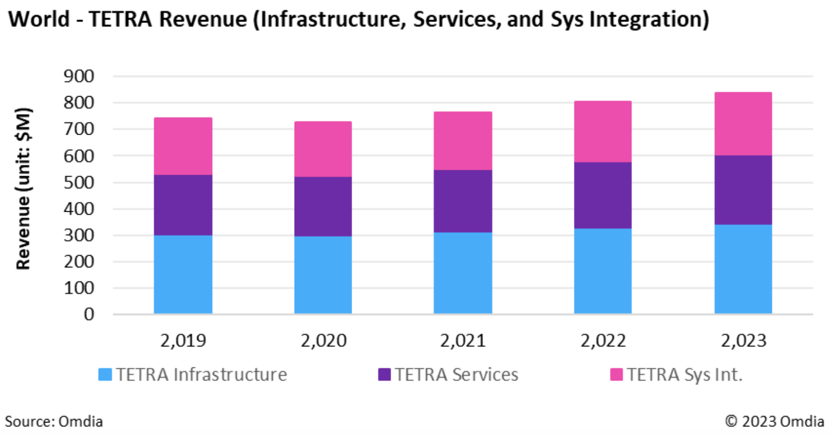
Including but not limited to:

AIRBUS
LEONARDO
DAMM
Critical communication made easy
MOTOROLA SOLUTIONS
sepura
ROHILL
Hytera
FEP
FUNK-ELECTRONIC piciorgros GMBH

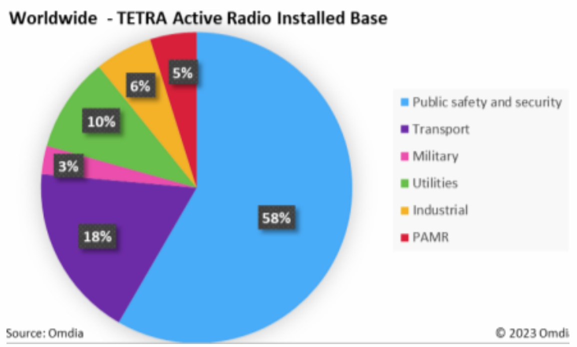
Critical communications for all professional users

TETRA market grows across all verticals…

- ❑ The constant growth of TETRA market observed in the past few years will continue (CAGR ~ 4.6%)
- ❑ After pandemic downturn, TETRA market had a rebound with an upturn mainly driven by business-critical sectors as Transport (+4.6%), Utilities (+3.7%) and Industrial (+6%)
- ❑ TETRA continues to be widely adopted in all main critical comms market sectors
- ❑ The progressive Broadband adoption with different models is so far mainly restricted to the Public Security and Safety (PSS) sector


World - TETRA Revenue (Infrastructure, Services, and Sys Integration)

Source: Omdia
© 2023 Omdia

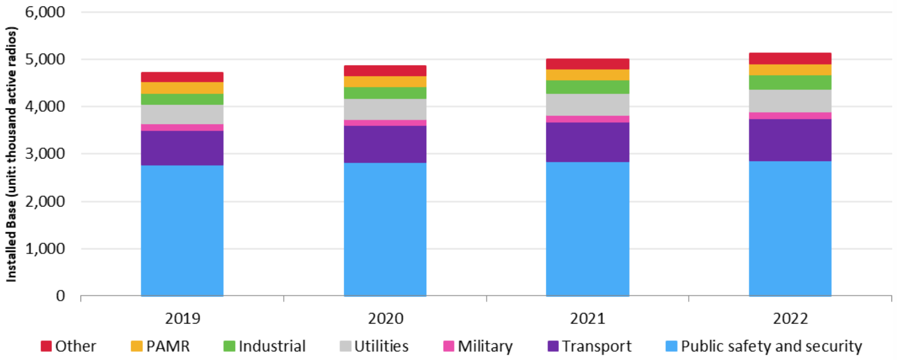

Worldwide - TETRA Active Radio Installed Base

Source: Omdia
© 2023 Omdi

…and geographies

- ❑ In many countries the hybrid approach exploiting the complementarity of TETRA and Broadband will be the chosen model in the medium/long term
- ❑ In Europe a few countries recently selected or confirmed TETRA for their national PSS networks (e.g. Romania, Slovenia). Others are expected to do the same soon
- ❑ In many verticals voice and low throughput data apps are still the main focus and narrowband dedicated networks are still regarded as the best solutions
- ❑ TETRA still is the technology of reference in many sectors (e.g. mass transit) in Asia (CAGR +2.1%) and Americas (CAGR +2%)

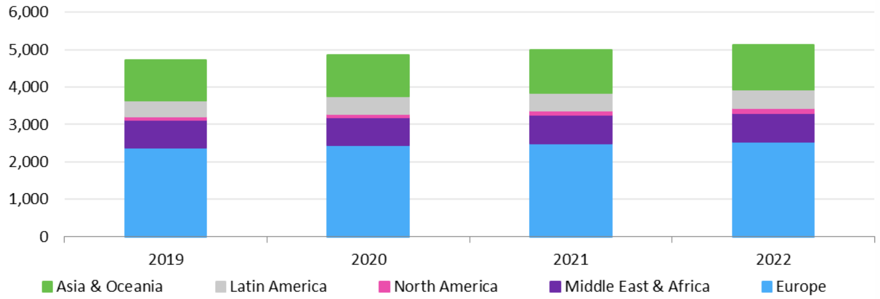
World - TETRA installed base split by user application area



Source: Omdia

© 2023 Omdia

World - TETRA Installed Base
(unit: thousands of active radios)

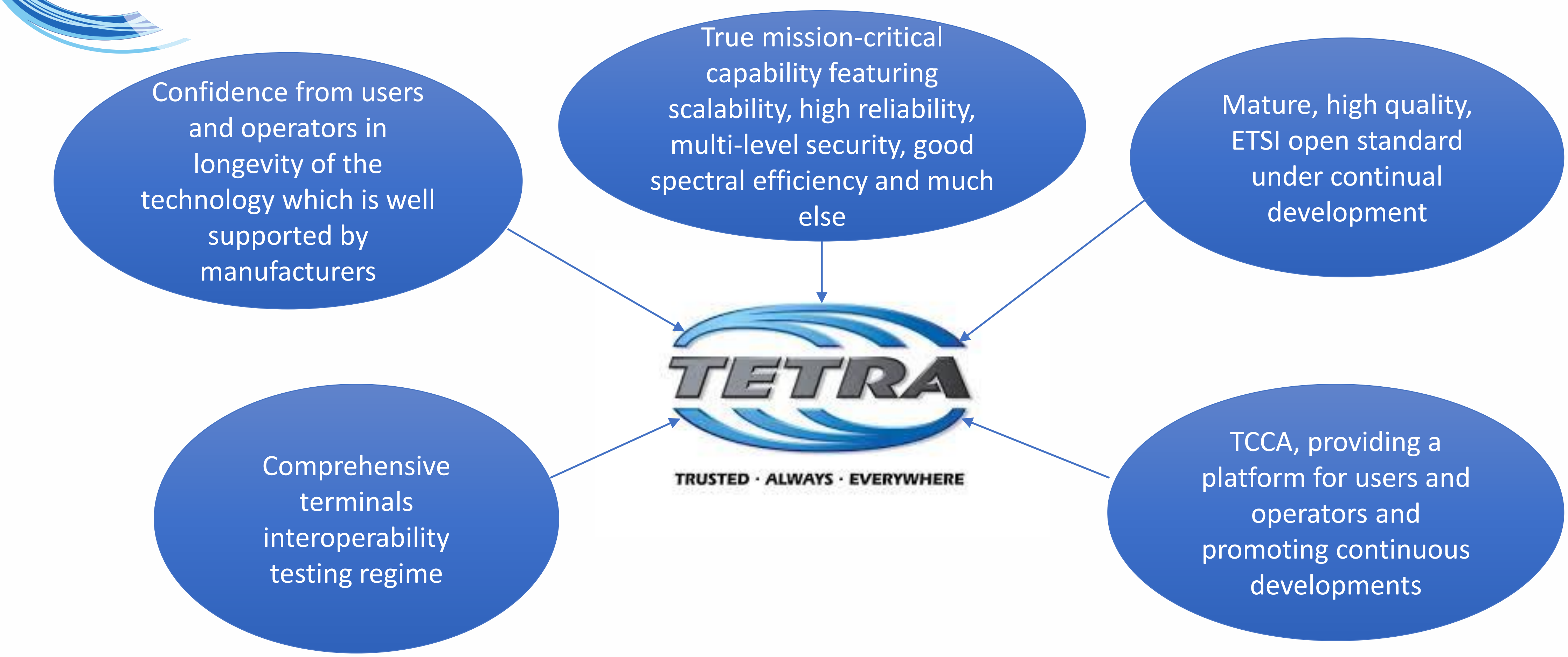


Source: Omdia

© 2023Omdia

Overview of the TETRA environment

Why has TETRA been so successful and why does it have a long term future?



Confidence from users and operators in longevity of the technology which is well supported by manufacturers

True mission-critical capability featuring scalability, high reliability, multi-level security, good spectral efficiency and much else

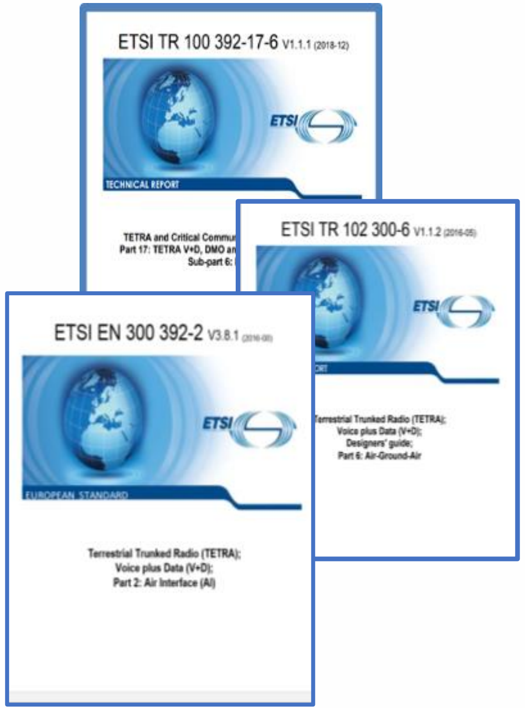
Mature, high quality, ETSI open standard under continual development

Comprehensive terminals interoperability testing regime

TCCA, providing a platform for users and operators and promoting continuous developments

What is the TETRA standard?

- **An ETSI standard, TETRA consists of 19 parts and defines:**
- **Three major TETRA interfaces**
  - Air Interface
  - Peripheral Equipment Interface
  - Inter-Systems Interface & IWF
- **Services and functions**
  - Security, Interoperability between TETRA and critical comms broadband, Harmonized radio conformance specifications, Direct Mode Operation, CODEC, short data service, pre-emptive priority, DGNA, SIM, etc)
- The standard consists of 142 current specifications and 37 technical reports, all of which are available freely on the ETSI website **https://www.etsi.org/standards-search#page=1&search=tetra**



ETSI TR 100 392-17-6 V1.1.1 (2018-12)

TECHNICAL REPORT

TETRA and Critical Commu
Part 17: TETRA V+D, DMO an
Sub-part 6:

ETSI TR 102 300-6 V1.1.2 (2016-05)

Terrestrial Trunked Radio (TETRA);
Voice plus Data (V+D);
Designers' guide;
Part 6: Air-Ground-Air

ETSI EN 300 392-2 V3.8.1 (2016-08)

EUROPEAN STANDARD

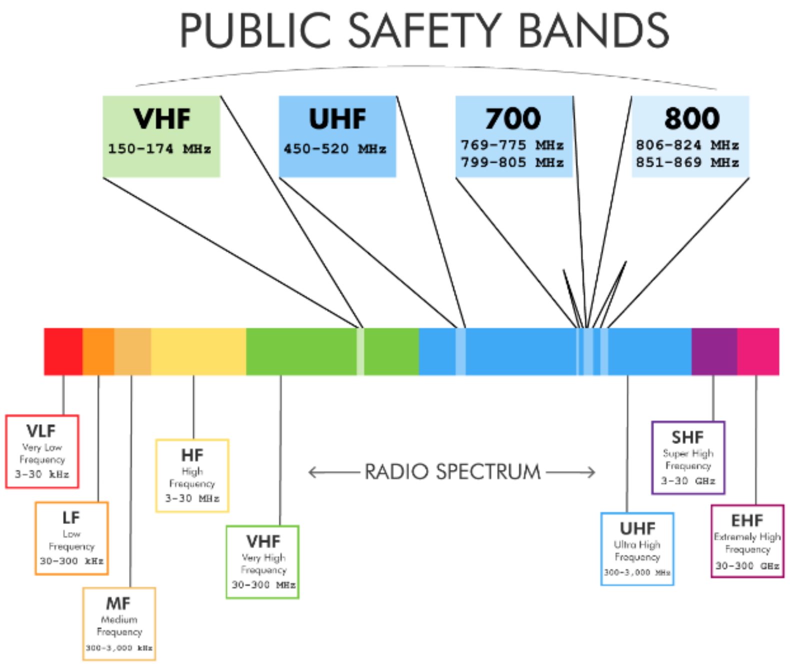
Terrestrial Trunked Radio (TETRA);
Voice plus Data (V+D);
Part 2: Air Interface (AI)

Frequency extension

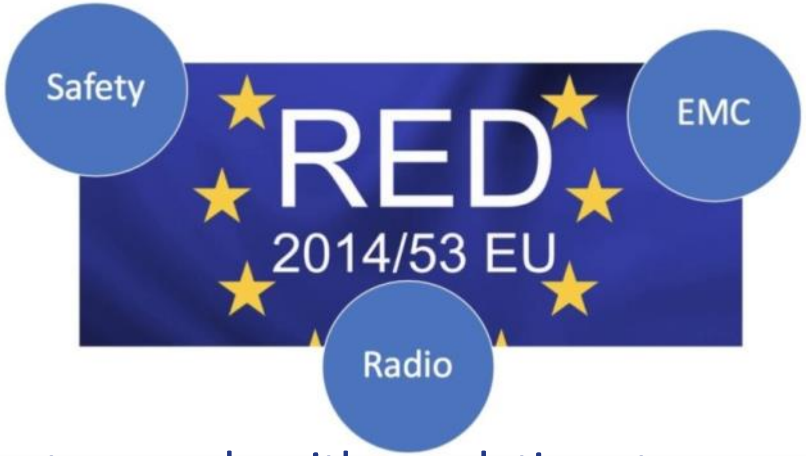
TETRA was originally developed for the UHF frequency bands with a frequency bounds of 300 to 1000 MHz

There was a need to provide a VHF version which would be preferable and more economical for use in very rural areas as well as areas where there was no suitable UHF spectrum available.

Extensive testing was carried out and proved that TETRA could operate in the VHF band so the lower limit was reduced to 138 MHz



TETRA Radio Compliance



- Like all radio systems, TETRA has to comply with regulations to ensure that its transmissions do not interfere with other services.
- The regulations were previously covered by the European R &TTE(Radio and Telecommunications Terminal Equipment) 1999/5/EC Directive and there were TETRA specifications based on these which were used for conformance testing
- These have now been replace by the RED (Radio Equipment Directive) 2014/53/EU and new specifications have had to be written especially for TETRA equipment

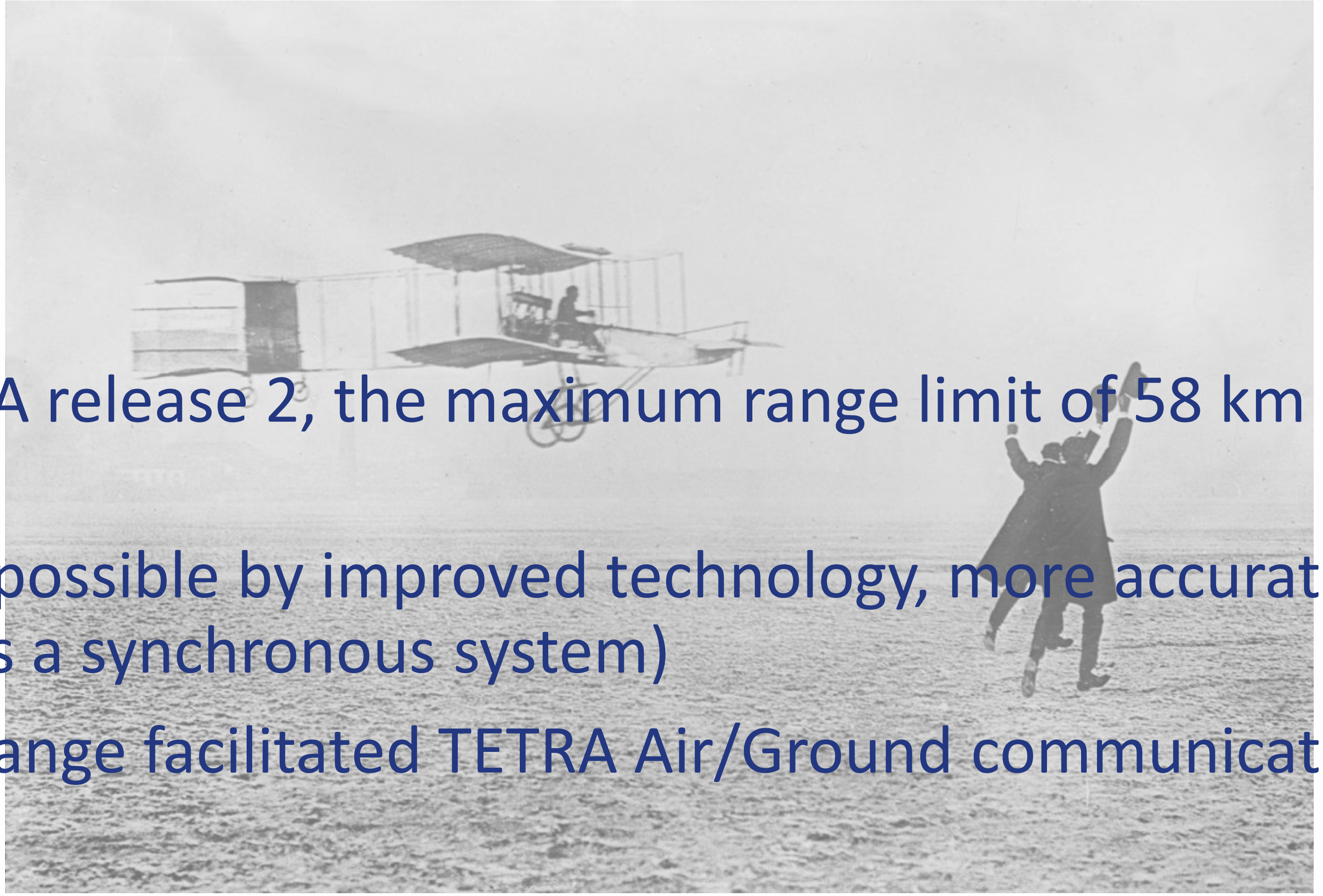
Group Addressed Packet Data

- One of TETRA's most important features is the ability to make group voice and SDS calls which is fast and economical and allows "all informed" groups
- Therefore it was considered a great step forward to have the same facility for the packet data service and would allow a single data message to reach a group which would improve efficiency
- The project is extremely complex and has taken a long time to develop. **It is near to completion**
- The effect of using GAPD would be to add a small overhead to each message (content identifiers allowing the MS to choose which data streams it wishes to accept) but is outweighed by much higher efficiency

TOO LATE?

- **If TETRA continues to provide mission critical speech and secure low bandwidth data in areas that 3GPP systems do not cover, this can be part of the solution to make data transfer more effective**

Base Station Range Extension



As part of TETRA release 2, the maximum range limit of 58 km was improved to 83km

This was made possible by improved technology, more accurate system timing (TETRA is a synchronous system)

The increased range facilitated TETRA Air/Ground communications

Interworking between TETRA and Critical Broadband systems

3GPP have developed Mission-Critical applications for operation on LTE (4G) and later technologies (5G on)

Interworking with Land Mobile Radio (primarily for TETRA and P25) added to the specifications in Rel-16 Interworking specifications provided for speech services (MCPTT) and Short Data Service (MCData)

The facilities that are included in the Interworking specification are:

Group attachment: Group controlled by MCPTT system

Group call: Groups controlled by either TETRA or MCPTT system

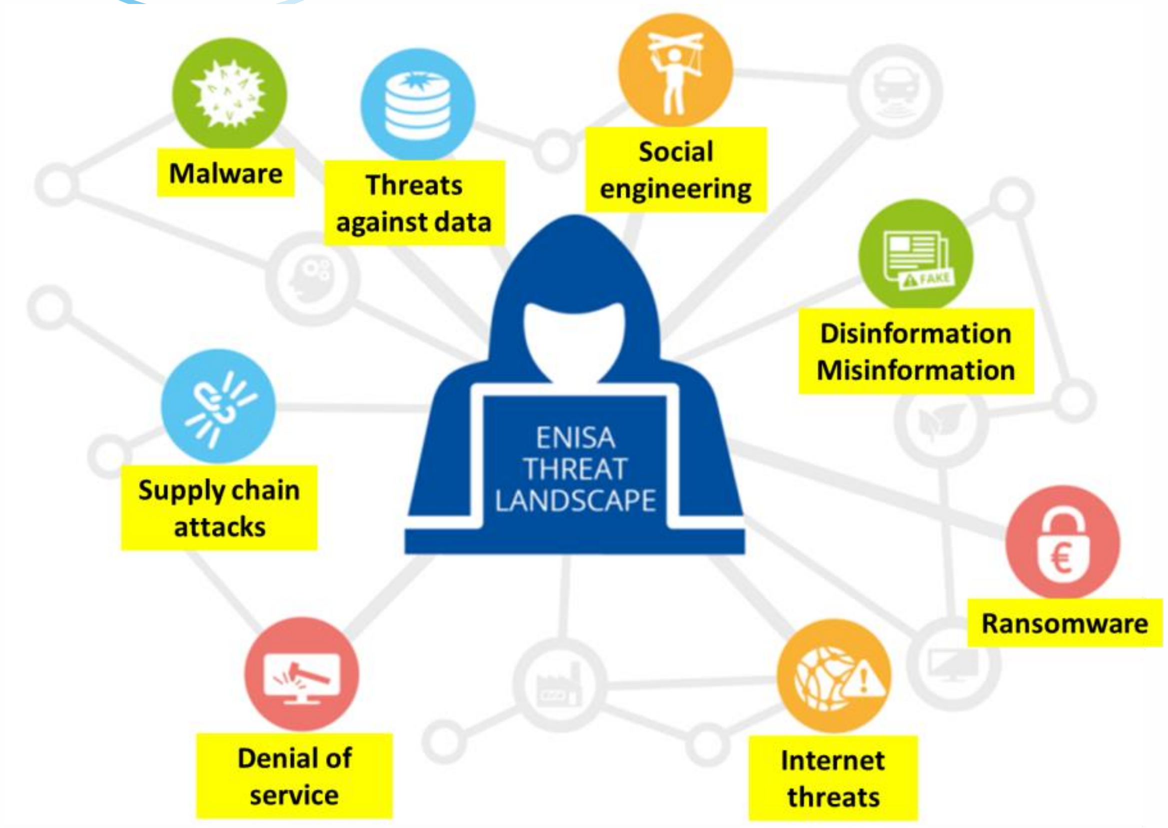
Individual/private call: Originated or terminated in the TETRA system

Emergency call: Group or individual

Short data messages: Originated or terminated in TETRA system, Individual or group destination

Encrypted communications

Increasing Risk of Cyber Attacks



Source: “ENISA Threat Landscape 2022”, European Union Agency for Cybersecurity, November 2022

- Increasing risk of brute force attacks
  - Cost of computing power reducing exponentially
  - Quantum computers on the horizon
- Expanding attack planes
  - Increasing connectivity
  - Opening up the traditionally closed environment
- Volatile geopolitical environment

Keeping TETRA secure to 2040 and beyond

- □ **TETRA** already provides an **OUTSTANDING** level of **SECURITY**
- □ Nonetheless considering TETRA lifetime will last for at least the next 10-15 years, new growing cyber threats and the progress of technology in terms of computational power…
- □ TETRA is being
  - □ **upgraded** with new additional **POST QUANTUM CRYPTOGRAPHY** algorithms
  - □ designed and deployed according to cutting-edge **CYBER RESILIENCE** methodologies

Keeping TETRA secure to 2040 and beyond

Encryption is a key factor for security, but even if it is efficient and reliable, cyber resilience of TETRA networks is much more…

A holistic strategy is needed for the whole life cycle of TETRA networks

- Secure by design
- Secure by configuration
- Secure by operation

New Air interface security algorithms

Air interface encryption has been a cornerstone of TETRA making the most vulnerable part of the system difficult to attack. The current algorithms were designed in the 1990s and have served very well in providing confidentiality to users data, protecting signalling and identities

To keep TETRA security futureproofed. in 2019, TCCE embarked on the development of new algorithms with longer keys which will provide extremely good long term protection against attack even with the future advent of quantum computers

The existing algorithms have a basic key length of 80 bits although some algorithms have shortened keys to comply with export control regulations

The new keys have a basic length of 192 bits with a shortened version for export control. At the same time identity encryption has been greatly strengthened and other aspects of the encryption. Authentication and key management system improved

The specifications for both the exiting algorithm set and the new algorithm set are being published as the strength of the encryption rests solely on the key and not the design of the algorithm

Data Applications: TETRA or Broadband: does it matter?

TETRA Data
“superpowers”

Automation
Work Management
Location tracking
Telemetry
Database lookup
etc...

Different
application
contexts

Most operational
data can be handled
through TETRA

Critical user
operational data are
not consumer data

TETRA can enable data
Centric and automated
operations

TETRA can be
complemented through
Broadband for video and
imagery transmission

Hybrid Data:
Best of Both Worlds

Conclusions

- TETRA has proved itself to be the “GoTo” technology for critical communications users over the past 25 years and has an extensive range of well tried and trusted functionalities which are required just as much today.
- Because it has been continually developed and enjoys strong industry support TETRA is future proofed and enjoys the users’ confidence in its longevity and relevance.
- Interworking solutions between TETRA and MC Broadband systems will be very important over the medium term and will give users the maximum choice in future migration plans, whether temporary or on a long-term basis.
- Many users have no requirements for MC broadband services so TETRA remains their choice of technology for Critical Communications.

- Work is ongoing both within ETSI TC TCCE, in 3GPP and also in several TCCA working groups TF, SFPG, CCBG to ensure that users have the most relevant mission critical solutions available to them.
- TETRA is still showing very good sales growth in many different verticals and so its future seems as bright as ever.
- TETRA shows every sign of being in use and still under development well towards the end of the next decade.

Critical communications for all professional users

BRITISH APCO
Working in Partnership to Improve Public Safety Technology

TCCA

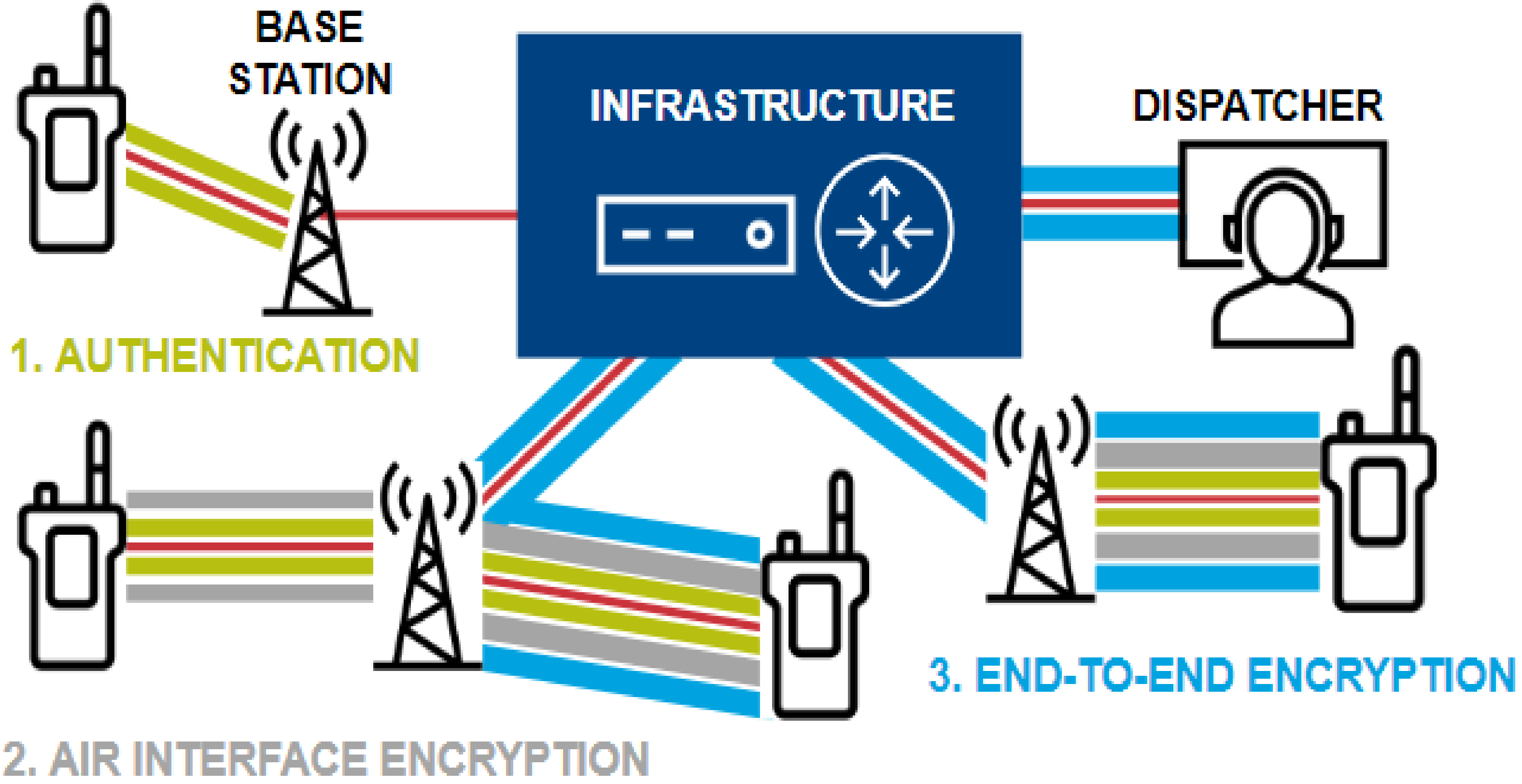
TETRA
TRUSTED · ALWAYS · EVERYWHERE

TETRA Security Vulnerabilities

Critical communications for all professional users

TETRA: Highly Secure Communications

Multiple Layers of TETRA Security



+

- Security best practices
- Holistic cyber security strategy

EQUIPMENT & SUBSCRIPTION DISABLE/ENABLE

Critical communications for all professional users

The Research Disclosures

Source Wikipedia

In August 2023, a group of Dutch security researchers published papers describing a set of findings relating to TETRA security.

The research findings were made public by Midnight Blue in August 2023 at Black Hat USA, and subsequent security conferences, after a responsible disclosure process.

The researchers’ findings all apply to air interface encrypted systems. End-to-end encryption was not examined in the research, and generally uses well known public domain algorithms such as AES128 or AES256, or government owned algorithms.

TEA1 problem

- The main finding is about the TEA1 encryption algorithm which internally reduces the effective length of the encryption key, thus requiring less effort than expected to recover the reduced key and decrypt communications.

- No issues were found with the TEA2 algorithm, and it is considered to be safe for continued use.

Source Wikipedia

TEA1 was conceived in the mid-1990s to be easily exportable. The key reduction was therefore needed to comply with the Wassenaar Arrangement signed by many countries – 42 at present – limiting the exports of military and 'dual use' (military and civilian applications) technologies, which includes cryptography. In the TEA1 algorithm design, the key length was reduced to an equivalent of 32 bits to permit worldwide export according to the Arrangement. The actual value of the equivalent key length had not been public before the Midnight Blue publication, but the status of TEA1 as an export-friendly variant was public.

TEA1 problem 2

HOLISTIC APPROACH

The mitigation steps should be results of a risk analysis – holistic approach.

A possible solution is to go to a different algorithm, e.g. an existing algorithm such as TEA2 or TEA3 where available, or a new algorithm such as TEA5, 6 or 7, or

To use End-to-End encryption.

TEA2 and TEA3 use 80 bit keys without any reduction in the key length, but deployment of these algorithms is more restricted than TEA1. The new algorithms TEA5 and TEA6 use 192 bit keys without any reduction but are also restricted in where they can be deployed. The new algorithm TEA7 has an effective key length reduction to 56 bits and will be available in many countries as per the Wassenaar Arrangement.

Additional algorithms

In 2019, ETSI TCCE started work on developing additional algorithms, to keep TETRA safe for another generation (even if quantum computing becomes a realistic threat). Three algorithms have been designed to fulfil the same three different purposes as the original algorithm set. **They will soon be made public.**

https://www.etsi.org/newsroom/press-releases/2293-etsi-releases-tetra-algorithms-to-public-domain-maintaining-the-highest-security-for-its-critical-communication-standard

- TEA5==TEA2 This algorithm has the same management rules as before
- TEA6==TEA3 Designed for PPDR/critical infrastructure where TEA5 is not permitted
- TEA7==TEA1/4 For use where export control regulations would not permit TEA6
- TAA2 Authentication and key management algorithms including new identity encryption

Other findings

- The research also found a weakness of the identity encryption that could allow an attacker to discover the numerical identities (SSIs) of the users (**not the personal identities of the users themselves**). Direct Mode Operation (DMO) uses a different mechanism and is not vulnerable to this attack.

  The additional encryption algorithms, TEA5, TEA6 and TEA7 have been designed together with a different authentication and key management algorithm set TAA2 which uses a different identity encryption process which is not vulnerable to the attack. Migration to TAA2 would completely solve the issue. TAA2 is implemented when migrating to TEA5, TEA6 or TEA7.

- Finally, the research also contained two secondary findings, which can be solved by a software upgrade of mobile stations. Despite the low probability of either attack being carried out in a real system environment, changes have been made in the TETRA standard to mitigate these findings and these are no longer considered to be an issue.

Recommended actions

- Any TETRA system operator or user should work with their national cyber-security agencies and with their suppliers to assess whether the findings provide a material risk to their system operation. This will depend on their specific threats and threat actors, and the consequences of the threats being acted upon.
- The findings that are not related to algorithms, only require a software update to completely mitigate, and some suppliers already have updates available.
- Transition to a new algorithm is complex, and system operators should consult their suppliers to investigate implications and timescales.
- TCCA Working Groups have already input significantly on addressing these issues, and further information is available to TCCA members here (log in required).
- ETSI TCCE will make the primitives of all TETRA Air Interface cryptographic algorithms* available as part of the TETRA documentation set but will maintain confidential handling of the full set of documentation applying to such algorithms.

*In this case the primitives of the algorithms relate to the algorithm specification and not any example code or test data.

The Critical Communications Event of the Year

TCCA
CRITICAL
COMMUNICATIONS
WORLD 2024

PLATINUM SPONSOR
MOTOROLA SOLUTIONS

GOLD SPONSOR
ERICSSON

PRESENTED BY
TCCA

in TCCA Critical Communications World

X @critcommsseries

14-16 May 2024, Dubai World Trade Centre,
Dubai, United Arab Emirates

www.critical-communications-world.com

TCCA

Thank you!
Questions?

mladen.vratonjic@tcca.info
francesco.pasquali@leonardo.com

Critical communications for all professional users