UNOFFICIAL MACHINE TRANSLATION

Grant Thornton

MINISTERSTVO PRŮMYSLU A OBCHODU

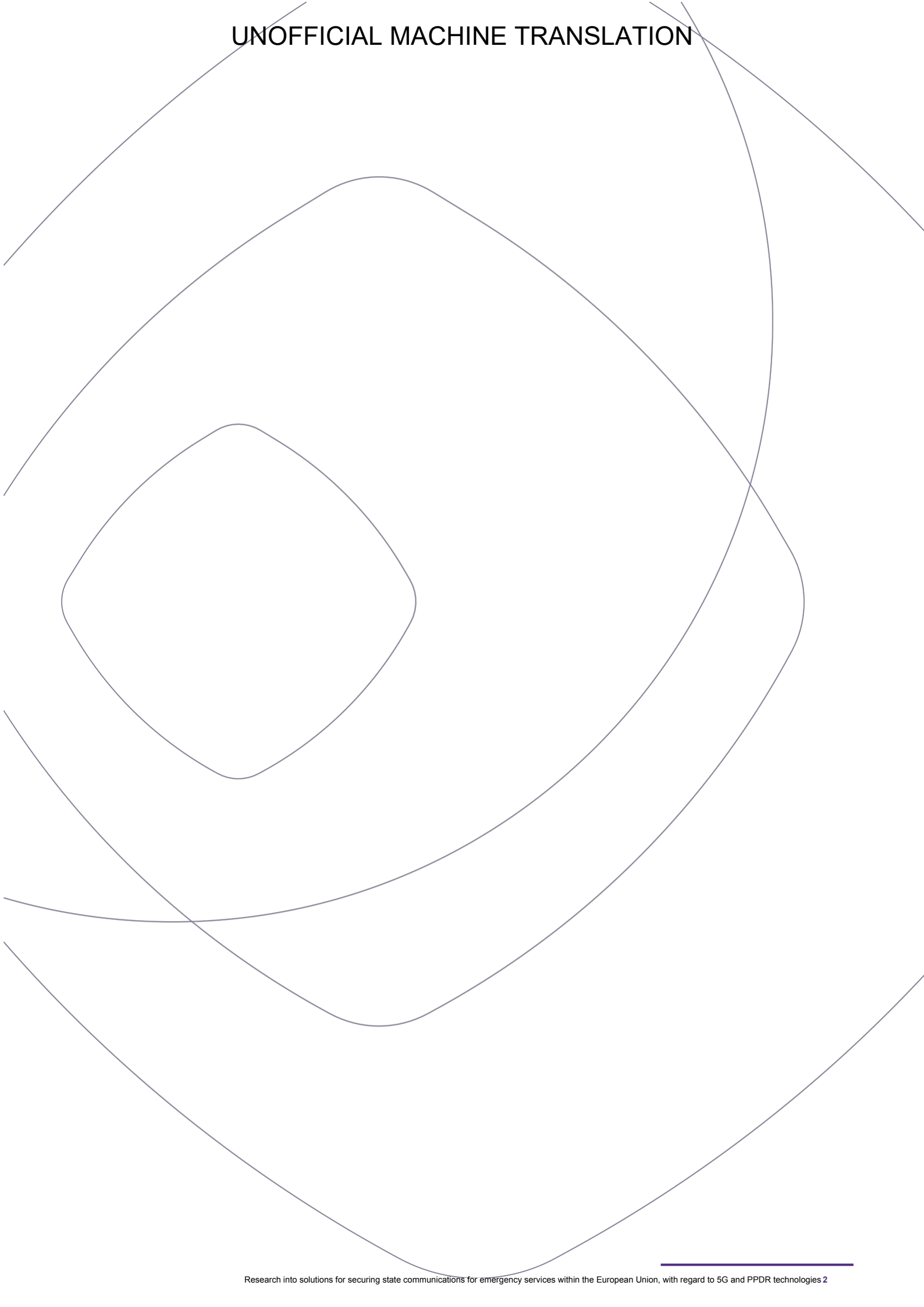
Financováno Evropskou unií
NextGenerationEU

A review of solutions for securing state communications for emergency services within the European Union, with regard to 5G and PPDR technologies

Prepared for the Ministry of Industry and Trade

[September 2024]

Národní plán obnovy



Contents

Contents

Contents

Contents

Contents

Contents

List of abbreviations and explanations

Abbreviation	Full form	Explanation
3D	Three-Dimensional	Three-dimensional
3GPP	3rd Generation Partnership Project	An organisation developing technical specifications for mobile telecommunications, including 3G, 4G and 5G standards
4G	Fourth Generation	The fourth generation of mobile networks
4K	4K	Ultra-high definition
5G	Fifth generation mobile networks	Wireless communication technology
AES	Advanced Encryption Standard	Advanced Encryption Standard
AES-128	Advanced Encryption Standard 128-bit	Advanced Encryption Standard with a 128-bit key length
API	Application Programming Interface	Application Programming Interface
AR	Augmented Reality	Augmented Reality
ARC4	Alleged RC4	Encryption algorithm for data protection
BB-PPDR	Broadband PPDR	Broadband services for PPDR
BC	Business Critical	
BDBOS	Federal Agency for Digital Radio for Authorities and Organisations with Security Responsibilities	Germany – Federal Agency for Digital Radio Communication for Security Authorities and Organisations
BDBOSG	Act on the Establishment of a Federal Agency for Digital Radio Communications for Security Authorities and Organisations	Germany – Act on the Establishment of a Federal Agency for Digital Radio Communications for Security Authorities and Organisations
BRK	Regional Security Council	
BS	Base Station	Base station
BTS	Base Transceiver Station	Base Transceiver Station
CBS	Cell Broadcast Service	A service for broadcasting messages to mobile devices in a given area
CE	Conformité Européenne	European Conformity, a mark for products meeting European standards
CEF	Connecting Europe Facility	Instrument for connecting Europe
CEPT	European Conference of Postal and Telecommunications Administrations	European Conference of Postal and Telecommunications Administrations
CO2	Carbon Dioxide	Carbon dioxide
CORE	CORE	Communication platform
CT	Computer Telephony	Computer Telephony
ČČK	Czech Red Cross	
CR	Czech Republic	
CTU	Czech Telecommunications Office	
D2D	Device-to-Device	Communication between devices
DBK	Dansk Beredskabskommunikation	Denmark – Danish emergency services communication
dBm	Decibel-milliwatts	Decibel-milliwatts

DDoS	Distributed Denial of Service	Distributed Denial of Service
DMO	Direct Mode Operation	Direct Mode Operation

DMR	Digital Mobile Radio	Standard for digital mobile communication
DoS	Denial of Service	Denial of Service
DSMD	Disaster & Safety Management	South Korea – Department of Disaster and Safety Management
DXT	Digital Exchange for TETRA	Digital Exchange for TETRA
DXTT	Digital Exchange for TETRA Transit Type	Transit digital exchange for TETRA
E2EE	End-to-End Encryption	End-to-end encryption
EADRCC	Euro-Atlantic Disaster Response Coordination Centre	Euro-Atlantic Disaster Response Coordination Centre
EDR	Unified Digital Radio System	Hungary – Unified Digital Radio System
EC	Electronic Communications	
eMBMS	Evolved Multimedia Broadcast Multicast Service	Enhanced Multicast and Broadcast Service
EMM	Enterprise Mobility Management	Enterprise Mobility Management
eMPS	Enhanced Multimedia Priority Service	Enhanced Multimedia Priority Service
ENISA	European Union Agency for Cybersecurity	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute	European Telecommunications Standards Institute
EU	European Union	
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	Evolved Universal Terrestrial Radio Access Network
GCF	Global Certification Forum	Global Certification Forum
GCSE	Group Communication System Enablers	System enabling group communication
GHz	Gigahertz	Unit of frequency
gNB	Next Generation NodeB	Next-generation base station (in 5G networks)
GNSS	Global Navigation Satellite System	Global Navigation Satellite System
GPS	Global Positioning System	Global Positioning System
HD	High Definition	High Definition
HDR	High Dynamic Range	High Dynamic Range
HEVC	High Efficiency Video Coding	High Efficiency Video Coding
HPUE	High Power User Equipment	High-performance user equipment
HW	Hardware	
Czech Fire and Rescue Service	Fire and Rescue Service of the Czech Republic	Core component of the Integrated Rescue System
iDEN	Integrated Digital Enhanced Network	Integrated Digital Enhanced Network
IDS	Intrusion Detection System	Intrusion Detection System
IDSIS	Integrated Disaster and Safety Information System	South Korea – Integrated Disaster and Safety Information System
IMEI	International Mobile Equipment Identity	International Mobile Equipment Identity
IOPS	Isolated Operations for Public Safety	Isolated Operations for Public Safety
IoT	Internet of Things	Internet of Things
IP	Internet Protocol	
IPS	Intrusion Prevention System	Intrusion Prevention System
ISLP	Integrated Services Local Point	Mobile data access
ITU	International Telecommunication Union	International Telecommunication Union
ITU-R 646 (REV.WRC 15)	ITU-R Recommendation 646 (REV.WRC 15)	ITU-R Recommendation 646 (2015 World Radiocommunication Conference revision)
Integrated Rescue System	Integrated Rescue System	

JRCC	Joint Rescue Coordination Centres	Norway – Joint Rescue Coordination Centres
JSVV	Unified Warning and Notification System	
KHS	Regional Public Health Authority	
KKB	Disaster Management Coordination Government Committee	Hungary – Government Committee for Crisis Management Coordination
KPI	Key Performance Indicator	Key Performance Indicator
KPK	Regional Contingency Plan	
KT	Korea Telecom	South Korea – Korea Telecom
KTS	Key Telephone Systems	Key Telephone Systems
KU	Regional Authority	
KVS	Regional Veterinary Administration	
KVV	Regional Military Command	
LAN	Local Area Network	Local Network
LCS	Location-Based Services	Location-based services
LFFZ	Aircraft Radio Cells	Germany – Airborne Radio Cells
LRT	LiveU Reliable Transport	LiveU's proprietary protocol for reliable data transmission
LTE	Long Term Evolution	Wireless communication standard
LTE-M	Long Term Evolution for Machines	LTE for Machines
LTE-R	Long Term Evolution for Railways	LTE for railways
Mbit/s	Megabit per second	Megabits per second
MBP	Mobile Secure Platform	
Mbps	Megabits per second	Megabits per second
MBS	Multimedia Broadcast Multicast Service	Multimedia broadcasting and multicasting
MC	Mission Critical	
MCC-ECO	Mission Critical Communication Ecosystem	Mission Critical Communication Ecosystem
MCD/MCData	Mission Critical Data	Mission-critical data communication
MCON	Multi-Operator Core Network	Network infrastructure shared by multiple operators in a hybrid model
MCPTT	Mission Critical Push to Talk	Mission-critical push-to-talk
MCS	Mission Critical Communication Systems	Mission-critical communication systems
MCV/MCVideo	Mission Critical Video	Mission-critical video communication
MCX	Mission Critical Common Functionalities	Mission-critical common functions
MDT	Mobile Data Terminal	Mobile Data Terminal
MHz	Megahertz	Unit of frequency
Mm	Millimetres	Millimetres
MMR	Ministry of Regional Development	
MNO	Mobile Network Operator	Mobile operator
MOIS	Ministry of the Interior and Safety	South Korea – Ministry of the Interior and Safety
Ms	Milliseconds	Milliseconds
MU	Emergency	
MV	Ministry of the Interior	
MVČR	Ministry of the Interior of the Czech Republic	
MVNO	Mobile Virtual Network Operator	Virtual mobile operator

MoE	Ministry of the Environment

NATO	North Atlantic Treaty Organisation	North Atlantic Treaty Organisation
NB-IoT	Narrowband Internet of Things	Narrowband Internet of Things
NEA	Emergency Power Supply Systems	Germany – Emergency power supply systems
NFA	National Fire Agency	South Korea – National Fire Agency
NFC	Near Field Communication	Short-range communication
NFV	Network Functions Virtualisation	Network Functions Virtualisation
NMHH	National Media and Communications Authority	Hungary – National Media and Communications Authority
NTN	Non-Terrestrial Networks	Non-terrestrial networks
NÚKIB	National Cyber and Information Security Agency	
NVKR	National Emergency Management System	Hungary – National Emergency Management System
OEM	Original Equipment Manufacturer	Original Equipment Manufacturer
OOP	General Authorisation	Regulatory document issued by the Czech Telecommunications Office for the regulation of telecommunications
OPIS	Operations and Information Centre	
ORP	Municipality with extended powers	
OS	Operating System	Operating System
UN	United Nations	
P25	Project 25	Standard for digital radio communication
PBX	Private Branch Exchange	Private branch exchange
PČR	Czech Police	
PEGAS	PEGAS	Communication system in the Czech Republic
PIN	Personal Identification Number	Personal Identification Number
PO	Fire protection	
PPDR	Public Protection and Disaster Relief	Public Protection and Disaster Relief
ProSe	Proximity Services	Proximity Services
PRS	Public Regulated Service	Public Regulated Service
PS-LTE	Public Safety Long Term Evolution	LTE for public safety
PSTN	Public Switched Telephone Network	Public Switched Telephone Network
PTT	Push-To-Talk	Push-to-talk communication
PTZ	Pan-Tilt-Zoom	Camera pan, tilt and zoom functions
PWS	Public Warning System	Public Warning System
PZH	Prevention of major accidents	
QoS	Quality of Service	Quality of Service
RAKEL	Radio Communication for Effective Management	Sweden – Radio communication system for effective management
RAN	Radio Access Network	Radio Access System
RDP	Remote Desktop Protocol	Remote Desktop Protocol
RF OTA	Radio Frequency Over-The-Air	Radio frequency transmission over the air
RFP	Request for Proposal	Call for proposals
RSPP	Radio Spectrum Policy Programme	Radio Spectrum Policy
RSRP	Reference Signal Received Power	Reference Signal Received Power
Directorate of Information and Communication	Directorate of Information and Communication Systems Services, Ministry of Defence	

Systems Services, Ministry of Defence		
SA	Standalone	Standalone mode or system
SAR	Norwegian Search and Rescue Service	Norway – Search and Rescue Service
SCO	Centralised Protection System	
SDN	Software-Defined Network	Software-defined network
SDS	Short Data Service	Short Data Service
SIEM	Security Information and Event Management	Security Information and Event Management
SKT	SK Telecom	South Korea – Wireless telecommunications operator
SLA	Service Level Agreement	Service Level Agreement
SMUR	Mobile Emergency and Resuscitation Service	Belgium – Mobile unit for emergency medical assistance and resuscitation
SOP	Standard Operating Procedure	Standard Operating Procedure
SSHR	Administration of State Material Reserves	Ensures stocks of strategic materials
TCCA	TETRA and Critical Communications Association	Association for TETRA and Critical Communications
TDMA DMR	Time Division Multiple Access Digital Mobile Radio	Time Division Multiple Access Digital Mobile Radio
TEDS	TETRA Enhanced Data Service	Enhanced data service within the TETRA network
TETRA	Terrestrial Trunked Radio	Standard for digital radio communication
TETRAPOL	TETRAPOL	Communication system
THW	Technisches Hilfswerk	Germany – Federal Agency for Technical Relief in Disasters and Emergencies
TMO	Trunked Mode Operation	Trunked mode operation
TMO-DMO Gateway	Trunked Mode Operation – Direct Mode Operation Gateway	Gateway between trunked and direct mode operation
TVFZ	Terrestrial coverage cells	Germany – Terrestrial radio coverage
UAT	User Acceptance Testing	User acceptance testing
UHD	Ultra High Definition	Ultra High Definition
UHF	Ultra High Frequency	Ultra High Frequency
UPS	Uninterruptible Power Supply	Uninterruptible Power Supply
Zoning Decision	Planning permission	
USA	United States of America	United States of America
USB-C	Universal Serial Bus Type-C	Universal Serial Bus Type-C, a new connector standard
VHCN	Very High Capacity Network	Very High Capacity Network
VMS	Public mobile network	
VoLTE	Voice over LTE	Voice over LTE
VPN	Virtual Private Network	Virtual Private Network
VPS	Public fixed network	
Wi-Fi	Wireless Fidelity	Wireless technology
z.s.	Registered association	Legal form of the organisation
ZoEK	Electronic Communications Act	
ZÚŘ	Simplified planning procedure	
Ambulance Service	Emergency Medical Service	

Sources

The information contained in this document has been drawn from the following sources:

1 Definition of PPDR/IZS

Source	URL
Erillisverkot's safety network	https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/erillisverkot-public-safety-network

2 Definition within the Czech Republic

Source	URL
Act No. 240/2000 Coll. on crisis management and amending certain acts	https://www.zakonyprolidi.cz/cs/2000-240
Act No. 239/2000 Coll. on the Integrated Rescue System and amending certain acts	https://www.zakonyprolidi.cz/cs/2000-239
The Pegas radio communication network of the integrated rescue system and its technical and cryptographic security	https://digilib.k.utb.cz/handle/10563/38879
Annex 2B to the Announcement of a tender procedure for the granting of rights to use radio frequencies for the provision of electronic communications networks in the 700 MHz and 3400–3600 MHz frequency bands	https://ctu.gov.cz/sites/default/files/obsah/ctu/oznameni-ceskeho-telekomunikacniho-uradu-o-vyhlaseni-vyberoveho-rizeni-za-ucelem-udeleni-prav-k/obrazky/20200807-priloha2bcz.pdf
Analysis and vision of radio communication security for emergency services	F6-BP-2022-Rychetsky-Matyas-Bakalarska_Prace-Rychetsky.pdf (cvut.cz)
PUBLIC PROTECTION AND DISASTER RELIEF (PPDR)	https://cept.org/ecc/topics/public-protection-and-disaster-relief-ppdr
Decree No. 328/2001 Coll.	https://www.zakonyprolidi.cz/cs/2001-328
SECURITY STRATEGY OF THE CZECH REPUBLIC 2023	https://mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategy_of_the_Czech_Republic_2023.pdf
States of emergency	https://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-krizove-stavy-krizove-stavy.aspx?q=Y2hudW09Mg%3D%3D
Crisis management in the Czech Republic	https://www.priruckazastupitele.cz/10-krizove-rizeni-v-ceske-republice/
Ambis – Crisis Management	
External emergency plans and their relationship to civil protection	http://www.hzsmsk.cz/sklad/kraoo/publikace/PO_VHP_vztah_k_OO.doc
Terms and definitions of crisis management	https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-ke-stazeni-ff.aspx?q=Y2hudW09NQ%3D%3D
National Radiation Emergency Plan	https://sujb.gov.cz/fileadmin/sujb/docs/dokumenty/NRHP/NRHP.pdf
Integrated Rescue System documentation	https://www.hzscr.cz/clanek/dokumentace-izs-587832.aspx?q=Y2hudW09Ng%3D%3D
Act No. 127/2005 Coll. on Electronic Communications and on Amendments to Certain Related Acts (Electronic Communications Act)	https://www.zakonyprolidi.cz/cs/2005-127#f7009936
Concept for the Mobilisation of the Armed Forces of the Czech Republic	https://mocr.army.cz/images/id_40001_50000/46088/koncepce-mobilizace.pdf
Statistical Yearbooks of the Fire and Rescue Service of the Czech Republic – Statistical Yearbook 2023	https://www.hzscr.cz/clanek/statisticke-rocenky-hasicskeho-zachranneho-sboru-cr.aspx

3 Definitions abroad

Source	URL
Authorities and organisations with security responsibilities	https://abes-online.com/publikationen/fachbeitraege/behoerden-und-organisationen-mit-sicherheitsaufgaben/
The Federal Agency for Technical Relief	https://www.bmi.bund.de/SharedDocs/behoerden/DE/thw.html
Belgium – Civil Protection	https://portal.cor.europa.eu/divisionpowers/Pages/Belgium-Civil-protection.aspx
Safety and prevention	https://www.belgium.be/en/justice/safety_and_prevention
Belgium Civil Protection	https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system/belgium_en
ORGANISATION IN THE EVENT OF AN EMERGENCY IN THE FIELD	https://centredecrise.be/fr/que-font-les-autorites/gestion-de-crise/organisation-lors-dune-situation-durgence-sur-le-terrain
PUBLIC SAFETY IN FINLAND	https://www.businessfinland.fi/4a845c/globalassets/ict-digi-maritime/bf_publicsafetyfromfinland_jointoffering_web.pdf
Rescue Act - 29 April 2011/379	https://www.finlex.fi/fi/laki/ajantasa/2011/20110379#P112
Rescue Services – a trusted safety authority	https://turvallisuuskomitea.fi/pelastustoimi-luotettu-turvallisuusviranomainen/
Future broadband public safety communication in Finland: Virve 2.0	https://vimeo.com/657514644
The role of mobile network operators in next-generation public safety services	https://acris.aalto.fi/ws/portalfiles/portal/97753446/1_s2.0_S0308596122001914_main.pdf
Units/institutions/structures subordinate to /in coordination with/ within the Ministry of the Interior	https://www.mai.gov.ro/en/organisation/units-institution-or-structures-subordinated/
COUNTY CENTRE FOR MANAGEMENT AND COORDINATION OF INTERVENTIONS – C.J.C.C.I.	https://isujis.ro/interventie/centrul-operational/centrul-judetean-de-conducere-si-coordonare-interventiei-c-j-c-c/
General Inspectorate for Emergency Situations (IGSU) (Romania)	https://www.devex.com/organizations/general-inspectorate-for-emergency-situations-igsu-romania-127756
The national disaster management system in Romania	https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system/romania_en
RO-ALERT System	https://ro-alert.ro/en/about-ro-alert-2/
Welcome to the Norwegian Sea Rescue Society	https://rs.no/english/
Critical-Communications-Today – Tetra Today Issue 36 2017	https://flickread.com/edition/html/index.php?pdf=5892e9cf3843f#27
TOWARDS A FUTURE-PROOF MISSION-CRITICAL COMMUNICATION ECOSYSTEM FOR PUBLIC SAFETY	https://www.capgemini.com/insights/research-library/towards-a-future-proof-mission-critical-communication-system-for-public-safety/
Hungary – Management of dangerous situations	https://www.katasztrofavedelem.hu/26424/veszlyhelyzetek-kezelse
Hungary – Management of dangerous situations	https://tudastar.mk.uni-pannon.hu/ff/10-vesz/veszhelyzet.xhtml
The Norwegian Search and Rescue Service	
A Brief Overview of the Norwegian – SEARCH RESCUE	https://www.jwc.nato.int/application/files/8716/3280/9240/issue37_1 3.pdf
Emergency Services in Norway	https://www.lifeinnorway.net/emergency-services/
Prevention-centric disaster and safety management systems of the Republic of Korea	https://www.preventionweb.net/news/prevention-centric-disaster-and-safety-management-systems-republic-korea
Republic of Korea – Roles and Functions of the Ministry of the Interior and Safety (MOIS) Disaster and Safety Management Department (DSMD)	

4 Legislation and regulations for the European Union and the Czech Republic

Source	URL

Annex 2B to the Notice of a tender procedure for the granting of rights to use radio frequencies for the provision of electronic communications networks in the 700 MHz and 3400–3600 MHz frequency bands	https://ctu.gov.cz/sites/default/files/obsah/ctu/oznameni-ceskeho-telekomunikacniho-uradu-o-vyhlaseni-vyberoveho-rizeni-za-ucelem-udeleni-prav-k/obrazky/20200807-priloha2bcz.pdf
5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.6.0 Release 16)	https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf

5 Emergency situations and communication in emergency situations

Source	URL
PSTN (public switched telephone network)	https://www.techtarget.com/searchnetworking/definition/PSTN
Telecom Basics, Second Edition – Private Telephone Systems	https://www.globalspec.com/reference/79234/203279/private-telephone-systems
The use of mobile applications in the public sector, with a focus on police forces in the Czech Republic	https://dspace5.zcu.cz/bitstream/11025/53405/1/DP.pdf
Secure mobile platform	https://katalog.polac.cz/Record/POLAC.119184/Description
VPN	https://www.eset.com/cz/vpn-pojem/
10 reasons to switch to digital DMR radios and radio networks	https://www.hyt.cz/10-duvodu-proc-prejit-digitalni-dmr-radiostanice/
Unified warning and notification system, end-user devices	https://www.hzscr.cz/clanek/jednotny-system-varovani-a-vyrozumeni-koncove-prvky.aspx
A straightforward introduction to satellite communications	https://www.inmarsat.com/en/insights/corporate/2023/a-straightforward-introduction-to-satellite-communications.html
Comparison of Tetra and Tetrapol – Ministry of the Interior of the Czech Republic	https://www.mvcr.cz/soubor/srovnani-tetra-tetrapol-pdf.aspx
RF / Bluetooth – Standards-based vs Proprietary Design	https://www.optimatech.net/knowledge-center/RF-Bluetooth-Standards-Based-vs-Proprietary-Design.aspx
Radio communication solutions for the Internet of Things (IoT)	https://www.technickytydenik.cz/rubriky/archiv/prostredky-radiove-komunikace-pro-internet-veci-iot_42579.html

6 Technological options for solutions

Source	URL
Ensuring critical communication with a secure national symbiotic network	https://www.ericsson.com/en/reports-and-papers/white-papers/ensuring-critical-communication-with-a-secure-national-symbiotic-network
Security and Interoperability in Next Generation PPDR Communication Infrastructures	https://cordis.europa.eu/project/id/313296

7 Opportunities for further technological development

Source	URL
Study to determine the broadband frequency spectrum demand of German public safety organisations in mobile broadband networks.	https://www.bdbos.bund.de/DE/Aufgaben/DigitalfunkBOS/Frequenzbedarf/frequenz.retten.leben_node.html
Mapping Interoperable EU PPDR Broadband Communication Applications and Technology	https://cordis.europa.eu/project/id/700380/
TOWARDS A FUTURE-PROOF MISSION-CRITICAL COMMUNICATION ECOSYSTEM FOR PUBLIC SAFETY	https://www.capgemini.com/insights/research-library/towards-a-future-proof-mission-critical-communication-system-for-public-safety/

8 Examples of PPDR network solutions abroad

Source	URL
The role of mobile network operators in next-generation public safety services	https://acris.aalto.fi/ws/portalfiles/portal/97753446/1_s2.0_S0308596122001914_main.pdf

Virve 2 mobile strategy 2023	https://www.erillisverkot.fi/wp-content/uploads/2023/05/virve-2-mobile-strategy-2023-versio-1.2f_eng.pdf
PPDR Rugged Handheld Device for heavy use v1.0	https://www.erillisverkot.fi/wp-content/uploads/2023/06/ppdr-rugged-handheld-device-for-heavy-use_nccom-whitepaper_signed-1.pdf
VIRVE – nationwide public safety network in Finland	https://www.securelandcommunications.com/customerstories/virve-nationwide-public-safety-network-in-finland
Airbus signs Agnet 800 MC-PTT contract with the Virve 2.0 programme to support migration to broadband Virve services	https://www.securelandcommunications.com/news/airbus-signs-agnet-800-mc-ptt-contract-with-virve-2.0-programme-to-support-migration-to-broadband-virve-services
How to plan your migration from TETRA to 4G/5G mission-critical broadband	https://www.securelandcommunications.com/hubfs/pdf/Migration-from-TETRA-to-4G-5G-mission-critical-broadband-Airbus-white-paper.pdf?hstc=2408687.623a566d6352f2809909f26a872d847b.1717755692651.1717755692651.1717755692651.1&hssc=2408687.3.1717755692652&__hsfp=1195774571
What is Virve 2.0?	https://blogg.telia.se/app/uploads/sites/4/2020/03/Bl%C3%A5ljusn%C3%A4t-Finland.pdf
TOWARDS A FUTURE-PROOF MISSION-CRITICAL COMMUNICATION ECOSYSTEM FOR PUBLIC SAFETY	https://www.capgemini.com/wp-content/uploads/2022/04/Whitepaper-Mission-critical-communications-for-Public-Safety.pdf
The public safety network Virve continues to operate whilst undergoing renewal during the 2020s	https://www.erillisverkot.fi/en/virve-radio-network/
For TETRA Specialists – Data Services and facilities	https://tcca.info/tetra/for-tetra-specialist/data-services-and-facilities/
Hungary - Government Decree No. 346/2010 (28 December) on networks for government purposes	https://net.jogtar.hu/jogszabaly?docid=a1000346.kor
Rakel – nationwide public safety network in Sweden	https://www.securelandcommunications.com/customerstories/rakel-nationwide-tetra-public-safety-network-in-sweden
Act on Electronic Communications Services (917/2014; amendments up to 1207/2020 included)	https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf
Rescue Act (379/2011)	https://www.finlex.fi/fi/laki/ajantasa/2011/20110379
Act on Public Procurement and Concession Contracts (1397/2016)	https://www.finlex.fi/fi/laki/ajantasa/2016/20161397
Section 31 Procurement of Virve 2.0 network coverage surveys and measures to improve coverage	https://vakehyva.cloudnc.fi/fi-FI/Viranhaltijat/Tietohallintojohtaja/Virve_20_verkon_kuuluvuuskartoituksien_j(12651)
Act on Security Network Operations in Public Administration	https://finlex.fi/fi/laki/alkup/2015/20150010
ATRID – Belgium	https://www.astrid.be
Law of 8 June 1998 on radio communications for emergency and security services	https://etaamb.openjustice.be/fr/loi-du-08-juin-1998_n1998000389.html
BDBOS	https://www.bdbos.bund.de/DE/Home/home_node.html
BOS Digital Radio FAQ	https://www.bdbos.bund.de/SharedDocs/Downloads/DE/Publikationen/faq-broschuere.html
South Korea – Disaster and Safety Communication Network Act	https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%9E%AC%EB%82%9C%EC%95%88%EC%A0%84%ED%86%B5%EC%8B%A0%EB%A7%9D%EB%B2%95/(18206,20210608)
South Korea – Regulations on the operation and use of disaster safety communication networks	https://law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000189 691
South Korea – Anti-Terrorism Act for the Protection of the People and Public Safety	https://law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EB%AF%BC%EB%B3%B4%ED%98%B8%EC%99%80%EA%B3%B5%EA%B3%B5%EC%95%88%EC%A0%84%EC%9D%84%EC%9C%84%ED%95%9C%ED%85%8C%EB%9F%AC%EB%B0%A9%EC%A7%80%EB%B2%95#:~:text=URL%3A%20https%3A%2F%2Flaw.go.kr%2F%25EB%25B2%2595%25EB%25A0%25B9%2F%25EA%25B5%25AD%25EB%25AF%25BC%25EB%25B3%25B4%25ED%2598%25B8%25EC%2599%2580%25EA%25B3%25B5%25EA%25B3%25B5%25EC%2595%2588%25EC%25A0%2584%25EC%259D%2584%25EC%259C%2584%25ED%2595%259C%25ED%258

	5%258C%25EB%259F%25AC%25EB%25B0%25A9%25EC%25A7%2580%25EB%25B2%2595%0AVisible%3A%200%25%20
Pro-M Prepares for the Future of Critical Communications in Hungary	https://www.criticalcommunicationsreview.com/ccr/news/100645/pro-m-prepares-for-the-future-of-critical-communications-in-hungary
4iG Group to sell DIGI mobile infrastructure	https://www.4ig.hu/4ig-group-to-sell-digi-mobile-infrastructure
5G-based Public Protection and Disaster Relief (PPDR 5G)	https://digital-strategy.ec.europa.eu/en/news/5g-based-public-protection-and-disaster-relief-ppdr-5g
Pro-M Zrt. Targets 2025 for Next-Generation Public Safety Broadband Network in Hungary	https://www.criticalcommunicationsreview.com/critical-iot/news/113057/pro-m-zrt-targets-2025-for-next-generation-public-safety-broadband-network-in-hungary
EDR – nationwide public safety network in Hungary	https://www.securelandcommunications.com/customerstories/edr-nationwide-public-safety-network-in-hungary
NATIONAL MEDIA AND INFOCOMMUNICATIONS AUTHORITY, HUNGARY RADIO SPECTRUM STRATEGY	https://english.nmhh.hu/document/219290/nmhh_radio_spektrum_strategy_2021_2025.pdf
Project 101094972–21-HU-DIG-PPDR 5G	https://prod5.assets-cdn.io/event/8792/assets/8317407177-d0d34f68e2.pdf
Hungary – Act C of 2003 on electronic communications	https://net.jogtar.hu/jogszabaly?docid=a0300100.tv
Hungary - 12/2011. (XII. 16.) NMHH decree on the order of frequency management for non-civilian purposes, as well as organisations falling within the scope of frequency management for non-civilian purposes	https://net.jogtar.hu/jogszabaly?docid=a1100012.nmh
Hungary - 7/2012. (26 January) NMHH decree on certain official procedures of civil frequency management	https://net.jogtar.hu/jogszabaly?docid=a1200007.nmh
Hungary - Government Decree No. 346/2010 (28 December) on networks for government purposes	https://net.jogtar.hu/jogszabaly?docid=a1000346.kor

9 Security threats

Source	URL
PUBLIC PROTECTION AND DISASTER RELIEF (PPDR)	https://www.cept.org/ecc/topics/public-protection-and-disaster-relief-ppdr
PPDR Communications: A NATO Perspective	https://www.itu.int/dms_pub/itu-r/oth/0a/0e/r0a0e00005b0001pdfe.pdf
International Disaster Relief	https://www.studentsummit.cz/wp-content/uploads/2021/02/International-Disaster-Relief_compressed.pdf
Lisbon Treaty	https://cept.org/files/10424/The%20Lisbon%20Treaty%20(art.%20196).docx
REPORT ON THE STATE OF CYBER SECURITY IN THE CZECH REPUBLIC FOR 2022	https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf
SECURITY IN 5G SPECIFICATIONS – Controls in 3GPP Security Specifications (5G SA)	https://cybercompetence.sk/wp-content/uploads/dokumenty/kniznica/schemy_specifikacie/ENISA-5G_Security_Specifications.pdf
Action Plan for Combating Terrorism 2022	https://www.czdefence.cz/clanek/akcni-plan-boje-proti-terorismu-2022
AMBIS – CRISIS MANAGEMENT	
Annual Report of Military Intelligence for 2023	https://vzcr.cz/uploads/41-Vyrocni-zprava-2023.pdf

10 Application possibilities

Source	URL
PPDR Rugged Handheld Device for heavy use v1.0	https://www.nodnett.no/siteassets/aktuelt/ppdr-rugged-handheld-device-for-heavy-use-nccom-whitepaper.pdf

TOWARDS A FUTURE-PROOF MISSION-CRITICAL COMMUNICATION ECOSYSTEM FOR PUBLIC SAFETY	https://www.capgemini.com/wp-content/uploads/2022/04/Whitepaper-Mission-critical-communications-for-Public-Safety.pdf
The shortest critical path to Next-Generation Public Safety Networks	https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/documents/critical-communications-world.pdf
Accelerating towards next-generation mission-critical services	https://www.pwc.com/m1/en/services/consulting/documents/ccw-2023-mission-critical-communication-paper.pdf

Executive summary

This research paper examines aspects of secure and reliable communication for the Integrated Rescue System (IRS) in European Union countries, with an emphasis on the use of modern technologies such as 5G networks and PPDR (Public Protection and Disaster Relief) systems. Security and emergency communications are a key element in the state's effective response to emergencies and crisis situations. They ensure the smooth and reliable exchange of information between emergency and security services, such as the Czech Police, the Fire and Rescue Service and the Emergency Medical Service.

Given growing challenges, such as more frequent natural disasters, terrorist threats and technological accidents, it is essential that communication systems are not only secure and resilient, but also flexible and capable of responding rapidly to new threats and needs. The research therefore focuses on analysing the current state of technology, specific international implementations, and identifying technologies and approaches that could be effectively utilised in the Czech Republic.

Examples of communication system implementations in Finland and Germany demonstrate how modern technologies enhance the security and reliability of crisis communication. These findings may inspire and lead to the introduction of similar systems in the Czech context.

The aim is to assess the possibilities for integrating these technologies into the existing emergency response structures in the Czech Republic, with the assessment placing emphasis on interoperability, security and the overall effectiveness of the systems. This document provides an overview of the possibilities for modernising crisis communication in the Czech Republic, taking into account global trends and new security challenges.

Conclusion to Chapter 1:

- PPDR represents a set of activities focused on public protection and crisis management. In the Czech Republic, these activities are carried out through the IZS, which ensures the coordination of rescue and security services, such as the Police of the Czech Republic, the Fire and Rescue Service and the Emergency Medical Service.
- In the Czech legal framework, the term IZS is used, whilst the term PPDR is not explicitly defined in Czech law. In an international context, PPDR focuses more on the technological and communication aspects of public protection, whereas the IZS in the Czech Republic represents a comprehensive system for coordinating rescue and security services.
- To ensure reliable and secure communication between IZS units, it is essential to use specific frequency bands, including the implementation of modern technologies such as 5G. These technologies provide higher capacity and data transfer speeds, which is key to the effective management of crisis situations and ensuring the safety of the population.

Conclusion to Chapter 2:

- Given the growing security threats and technological challenges, the modernisation of PPDR systems and communication infrastructure is necessary. The transition to broadband and 5G technologies will bring higher speeds, capacity and reliability of communication, and will improve the IZS's ability to respond to crisis situations and ensure public safety.
- The Integrated Rescue System (IRS) in the Czech Republic focuses on public protection and crisis management, thereby enabling a coordinated response to threats such as terrorism, cyber-attacks, natural disasters and pandemics. This system involves cooperation between key components, such as the Fire and Rescue Service, the Police of the Czech Republic and the Emergency Medical Service.
- Given the growing security threats and technological challenges, the modernisation of the IZS's communications infrastructure is essential. The transition to broadband and 5G technologies will bring higher speeds, capacity and reliability of communication, which will improve the ability of IZS units to respond effectively to crisis situations and ensure public safety.

Conclusion to Chapter 3:

- The organisation of emergency services varies considerably from country to country, depending on their legislative, geographical and organisational conditions. The basic principles – public protection and crisis management – remain similar, but individual countries adapt their systems to specific needs and available resources.
- Compared to foreign systems, such as the IZS in Germany or Finland, the Czech IZS is more centralised and emphasises unified coordination across the whole country. Despite regionalisation abroad, where there is greater autonomy at the regional level, centralisation and unified management at the national level are key in the Czech Republic.

- Different countries have varying approaches to the implementation of 5G and PPDR, with some states, such as Germany and France, emphasising advanced encryption standards and security measures, whilst others focus on ensuring interoperability between systems.

Conclusion to Chapter 4:

- The auction of spectrum in the 700 MHz band, announced by the Czech Telecommunications Office (ČTÚ), was a step towards the development of 5G networks and the provision of priority services for public safety and emergency communications in the Czech Republic, and also established the conditions for national roaming and the provision of priority broadband PPDR services.
- The auction of spectrum in the 700 MHz band, announced by the CTO, represents a significant step towards the development of 5G networks in the Czech Republic. This step not only supports the development of modern telecommunications technologies but also ensures priority services for public safety and emergency communications. Part of this auction involved setting out the conditions for national roaming and the provision of priority broadband services for the Integrated Rescue System (IRS) units.
- This legal framework and its technical standards are a key factor in ensuring secure and reliable communication between emergency services. Thanks to these legislative measures, which set out rules for the operation and maintenance of communication systems, it is possible to ensure interoperability and effective cooperation between the various emergency and security services. The legislation also supports the implementation of modern technologies, such as 5G.

Conclusion to Chapter 5:

- Communication between emergency services is facilitated by various types of communication systems, such as fixed networks, mobile networks, TETRAPOL IP, DMR and other technologies. Each of these systems has specific characteristics and limitations that affect their use in emergency situations.
- Networks such as TETRAPOL and TETRA offer secure and reliable communication thanks to their closed infrastructure and hardware encryption, which ensures the protection of sensitive information and enables effective coordination during crisis events. Public networks and satellite communications provide wider coverage and flexibility, but entail greater risks in terms of service quality and security, particularly during high-traffic crisis situations. Overall, effective crisis communication requires a combination of different types of communication systems that complement one another and ensure robust and reliable connections across various scenarios and conditions.
- Various crisis situations, such as natural disasters, terrorist attacks or technological accidents, require specific communication strategies. In the event of natural disasters, it is essential to quickly inform the public about evacuation plans and safety measures, whilst in the case of terrorist threats, the priority is to ensure secure and encrypted communication between emergency services.

Conclusion to Chapter 6:

- The analysis shows that modernising the PPDR communication platform is essential. The proposed approaches, including the implementation of a broadband PPDR network, the combination of existing networks with commercial networks, and the development of proprietary infrastructure in cooperation with the armed forces, represent a step towards ensuring more robust and flexible emergency communications. The use of modern technologies such as 5G, digital radio networks and advanced encryption standards offers the potential to increase the capacity, security and reliability of communications.
- Future technological innovations, such as artificial intelligence, the Internet of Things or augmented reality, can further improve the ability of emergency services to respond to crisis situations. For example, AI can analyse large volumes of data to predict crisis situations, whilst AR can help emergency responders navigate the terrain more effectively by visualising key information.
- A network interconnecting multiple technologies, encompassing both government and commercial infrastructure, represents the optimal solution for ensuring reliable and effective crisis communication. This approach ensures that communications remain functional even during outages or periods of increased demand for capacity. At the same time, it enables the integration of advanced features such as precise positioning or real-time video transmission.

Conclusion to Chapter 7:

- The development of broadband networks, such as LTE and 5G, brings new possibilities for fast and reliable emergency communications, including the integration of advanced applications and data services. The transition to 5G technology enables the deployment of innovative applications.
- In the field of security, blockchain technology also offers a solution, which can ensure the transparency and integrity of data during crisis situations, thereby contributing to the protection of sensitive information.
- The introduction of these innovative technologies can significantly improve the ability of emergency services to respond to crisis situations and enhances their preparedness and effectiveness in protecting the public.

Conclusion to Chapter 8:

- An overview of the implementation of PPDR networks in various countries shows that approaches to these technologies vary significantly depending on local legislative frameworks, technological capabilities and the operational needs of emergency services. Examples from Germany, France, the United Kingdom and Sweden provide valuable insights into how different countries have adapted their communication systems to specific national conditions.
- In Germany, for example, the BDBOS broadband network has been implemented, providing digital radio communication for all emergency services with a high level of encryption and security. In France, a broadband PPDR network based on LTE technology has been introduced, enabling real-time voice and data transmission. The United Kingdom has implemented the ESN network, utilising 4G and 5G technologies, which is interoperable with other systems and enables a wide range of advanced features, such as location tracking and video conferencing. Sweden uses the TETRA network, which offers a high level of security and resistance to interference.
- These examples highlight that the successful implementation of PPDR networks depends on adaptation to local conditions, whilst also providing inspiration for the future development of emergency communications in the Czech Republic.

Conclusion to Chapter 9:

- Cyber threats and terrorist attacks pose significant risks to the communication systems of emergency services. With the increasing complexity and interconnectedness of systems, particularly during the transition to 5G technology, these threats are becoming more frequent and sophisticated. Cyberattacks, such as ransomware, phishing or DDoS, can seriously disrupt the availability and security of emergency communications, whilst terrorist attacks may target physical infrastructure, leading to widespread outages.
- To minimise these threats, it is essential to implement comprehensive security measures. This includes securing network infrastructure through advanced encryption standards, regular threat monitoring and the protection of critical systems. Physical protection of infrastructure, including the security of base stations and data centres, is just as important as preventing technical failures through regular maintenance and modernisation.
- Contingency planning and preparedness for natural disasters ensure that communications remain operational even under the most challenging conditions. At the same time, ongoing staff training and awareness-raising in the field of cybersecurity are necessary to minimise human error and enhance the overall preparedness of emergency services for potential security threats.

Conclusion to Chapter 10:

- The application capabilities of communication systems are key to the effective functioning of the IZS. The difference between commercial and critical systems is fundamental – whilst commercial systems target a broad spectrum of users and prioritise profitability, critical systems designed for PPDR emphasise reliability, security and resilience. Communication systems for emergency services, such as MC systems, require specialised infrastructure that supports continuous availability and data security.
- Current technological capabilities include digital radio networks, mobile communication systems and advanced encryption technologies. Future innovations, such as artificial intelligence, the Internet of Things and augmented reality, have the potential to further improve the efficiency and response capabilities of emergency services in crisis situations.
- To ensure secure and effective communication, it is essential not only to integrate these technologies but also to link them into a robust and flexible system capable of meeting the specific requirements of critical operations. The implementation of such technologies will play a crucial role in the future of emergency communications.

Based on international experience, the following objectives can be set for the communication networks of emergency services in the Czech Republic:

- **Development of in-house communication networks:** Modernisation of communication technologies through the implementation of 5G and PPDR technologies will ensure fast and reliable communication, including backup solutions using a secure private communication network.
- **Interoperability:** It is necessary to ensure compatibility with international systems and standards for effective cooperation in crisis situations at a global level.
- **Security and encryption:** The introduction of advanced encryption standards and other security measures is essential for protecting sensitive data and ensuring the security of communication systems.
- **Research and development:** Increasing investment in research and development in the field of secure communications is key to supporting innovation and the long-term improvement of the communication infrastructure of the emergency services.

These measures should enhance the efficiency, security and preparedness of the emergency services for crisis situations in the Czech Republic.

Management summary

This research focuses on the aspects of secure and reliable communication for the Integrated Rescue System units in European Union countries, emphasising the use of modern technologies such as 5G networks and Public Protection and Disaster Relief (PPDR) systems. Crisis communication is a key element in ensuring an effective state response to emergencies and crisis situations. It facilitates the smooth and reliable exchange of information between rescue and security services, such as the Czech Police, the Fire and Rescue Service, and the Emergency Medical Service.

Given the growing challenges such as more frequent natural disasters, terrorist threats, and technological failures, communication systems must be not only secure and resilient but also flexible and capable of quickly responding to new threats and needs. Therefore, this research focuses on analysing the current state of technology, specific foreign implementations, and identifying technologies and approaches that could be effectively utilised in the Czech Republic.

Examples of communication system implementations in Finland and Germany demonstrate how modern technologies enhance the security and reliability of crisis communication. These insights can inspire and lead to the introduction of similar systems in the Czech context.

The aim is to assess the possibilities for integrating these technologies into the existing IZS structures in the Czech Republic, with an emphasis on interoperability, security, and overall system efficiency. This document provides an overview of the possibilities for modernising crisis communication in the Czech Republic, taking into account global trends and emerging security challenges.

Conclusion to Chapter 1:

- PPDR represents a set of activities focused on public protection and crisis management. In the Czech Republic, these activities are carried out through the Integrated Rescue System, which ensures the coordination of rescue and security units such as the Czech Police, the Fire and Rescue Service, and the Emergency Medical Service.
- In the legislative framework of the Czech Republic, the term IZS is used, whilst PPDR is not explicitly defined in Czech law. Internationally, PPDR focuses more on the technological and communication aspects of public protection, whereas IZS in the Czech Republic represents a comprehensive system for coordinating rescue and security services.
- To ensure reliable and secure communication between IZS units, it is essential to use specific frequency bands, including the implementation of modern technologies such as 5G. These technologies provide higher capacity and faster data transmission, which is crucial for effective crisis management and ensuring public safety.

Conclusion to Chapter 2:

- Given the increasing security threats and technological challenges, the modernisation of PPDR systems and communication infrastructure is essential. The transition to broadband and 5G technologies will provide higher speed, capacity, and communication reliability, enhancing the ability of the IZS to respond to crisis situations and ensure public safety.
- The IZS in the Czech Republic focuses on public protection and crisis management, enabling a coordinated response to threats such as terrorism, cyberattacks, natural disasters, and pandemics. This system involves cooperation between key units such as the Fire and Rescue Service, the Czech Police, and the Emergency Medical Service.
- Due to growing security threats and technological challenges, the modernisation of the communication infrastructure for the IZS is crucial. The transition to broadband and 5G technologies will increase speed, capacity, and reliability, improving the ability of IZS units to effectively respond to crisis situations and safeguard the population.

Conclusion to Chapter 3:

- The organisation of IZS units varies significantly across countries, depending on their legislative, geographical, and organisational conditions. The basic principles—public protection and crisis management—remain similar, but each country adapts its systems to specific needs and available resources.
- Compared to foreign systems, such as the IZS in Germany or Finland, the Czech IZS is more centralised and emphasises unified coordination across the entire country. Despite regionalisation abroad, where there is greater

autonomy at the regional level, centralisation and unified management at the national level are key in the Czech Republic.

- Different countries have various approaches to implementing 5G and PPDR technologies, with some nations, such as Germany and France, focusing on advanced encryption standards and security measures, whilst others prioritise ensuring interoperability between systems.

Conclusion to Chapter 4:

- The 700 MHz frequency auction announced by the Czech Telecommunications Office (ČTÚ) was a step towards the development of 5G networks and the provision of priority services for public safety and emergency communications in the Czech Republic. It also set the conditions for national roaming and the provision of priority broadband services for PPDR.
- The 700 MHz frequency auction announced by the Czech Telecommunications Office (ČTÚ) represents a significant step towards the development of 5G networks in the Czech Republic. This step not only supports the advancement of modern telecommunications technologies but also ensures priority services for public safety and emergency communications. Part of this auction involved establishing conditions for national roaming and the provision of priority broadband services for Integrated Rescue System (IZS) units.
- This legal framework and its technical standards are essential factors in ensuring secure and reliable communication among IZS units. Thanks to these legislative measures, which establish rules for the operation and maintenance of communication systems, interoperability and effective cooperation between various rescue and security services can be ensured. The legislation also promotes the implementation of modern technologies, such as 5G.

Conclusion to Chapter 5:

- Communication between IZS units is facilitated by various types of communication systems, such as fixed networks, mobile networks, TETRAPOL IP, DMR, and other technologies. Each of these systems has specific features and limitations that affect their use in crisis situations.
- Networks such as TETRAPOL and TETRA offer secure and reliable communication due to their closed infrastructure and hardware encryption, which ensures the protection of sensitive information and enables efficient coordination during crisis events. Public networks and satellite communications provide broader coverage and flexibility but pose higher risks in terms of service quality and security, especially during high-traffic crisis situations. Overall, for effective crisis communication, it is necessary to combine various types of communication systems that complement each other and provide robust and reliable connections in different scenarios and conditions.
- Different crisis scenarios, such as natural disasters, terrorist attacks, or technological failures, require specific communication strategies. During natural disasters, it is crucial to quickly inform the public about evacuation plans and safety measures, whilst in the case of terrorist threats, the priority is to ensure secure and encrypted communication between emergency services units.

Conclusion to Chapter 6:

- The analysis shows that modernising the communication platform for PPDR is essential. Proposed measures, including the implementation of a broadband PPDR network, combining existing networks with commercial ones, and developing proprietary infrastructure in cooperation with the military, represent a step towards ensuring more robust and flexible crisis communication. The use of modern technologies such as 5G, digital radio networks, and advanced encryption standards offers the potential to increase communication capacity, security, and reliability.
- Future technological innovations, such as artificial intelligence, the Internet of Things, or augmented reality, can further enhance the capabilities of IZS units in responding to crisis situations. For instance, AI can analyse large volumes of data to predict crisis scenarios, whilst AR can help rescuers navigate the terrain more effectively by visualising important information.
- A network that integrates multiple technologies, encompassing both government and commercial infrastructure, represents the optimal solution for ensuring reliable and effective crisis communication. This approach guarantees that communication remains operational even during outages or periods of high demand. It also allows for the integration of advanced features such as precise location tracking or real-time video transmission.

Conclusion to Chapter 7:

- The development of broadband networks, such as LTE and 5G, opens up new possibilities for fast and reliable crisis communication, including the integration of advanced applications and data services. The transition to 5G technology enables the deployment of innovative applications.
- In terms of security, blockchain technology offers the potential to ensure transparency and data integrity during crisis situations, thereby contributing to the protection of sensitive information.

- The implementation of these innovative technologies can significantly enhance the capabilities of emergency services units in responding to crisis situations, increasing their preparedness and effectiveness in safeguarding the population.

Conclusion to Chapter 8:

- An overview of the implementation of PPDR networks in various countries shows that approaches to these technologies differ significantly depending on local legislative frameworks, technological capabilities, and the operational needs of emergency services. Examples from Germany, France, the United Kingdom, and Sweden provide valuable insights into how different countries have adapted their communication systems to specific national conditions.
- For example, Germany implemented the BDBOS broadband network, which ensures digital radio communication for all emergency services units with a high level of encryption and security. France introduced a broadband PPDR network based on LTE technology, allowing real-time voice and data transmission. The United Kingdom implemented the ESN network, utilising 4G and 5G technologies, which is interoperable with other systems and offers a wide range of advanced features, such as location tracking and video conferencing. Sweden uses the TETRA network, which offers a high level of security and resistance to interference.
- These examples highlight that the successful implementation of PPDR networks depends on adapting to local conditions, whilst also providing inspiration for the future development of crisis communication in the Czech Republic.

Conclusion to Chapter 9:

- Cyber threats and terrorist attacks pose significant risks to the communication tools of IZS units. With the increasing complexity and interconnectedness of systems, particularly during the transition to 5G technologies, these threats are becoming more frequent and sophisticated. Cyberattacks, such as ransomware, phishing, or DDoS, can severely disrupt the availability and security of crisis communication, whilst terrorist attacks can target physical infrastructure, leading to widespread outages.
- To minimise these threats, it is crucial to implement comprehensive security measures. This includes securing network infrastructure through advanced encryption standards, regular threat monitoring, and protection of critical systems. Physical protection of infrastructure, including securing base stations and data centres, is just as important as preventing technical malfunctions through regular maintenance and modernisation.
- Crisis planning and preparation for natural disasters ensure that communication remains operational even in the most challenging conditions. Continuous staff training and awareness in the field of cybersecurity are also necessary to minimise human error and enhance the overall preparedness of IZS units for potential security threats.

Conclusion to Chapter 10:

- The application possibilities of communication systems are key to the effective operation of IZS units. The distinction between commercial and critical systems is fundamental—whilst commercial systems target a broad spectrum of users and prioritise profitability, critical systems intended for PPDR emphasise reliability, security, and resilience. Communication systems for IZS units, such as MC systems, require specialised infrastructure that supports continuous availability and data security.
- Current technological capabilities include digital radio networks, mobile communication systems, and advanced encryption technologies. Future innovations, such as artificial intelligence, the Internet of Things, and augmented reality, have the potential to further enhance the efficiency and responsiveness of IZS units in crisis situations.
- Ensuring secure and efficient communication requires not only the integration of these technologies but also their integration into a robust and flexible system capable of meeting the specific requirements of critical operations. The implementation of such technologies will play a crucial role in the future of crisis communication.

Based on international experience, the following objectives can be set for the communication networks of IZS units in the Czech Republic:

- **Development of independent communication networks:** Modernising communication technologies through the implementation of 5G and PPDR technologies will ensure fast and reliable communication, including backup solutions using secure private communication networks.
- **Interoperability:** It is essential to ensure compatibility with international systems and standards for effective cooperation in crisis situations on a global level.
- **Security and encryption:** The introduction of advanced encryption standards and other security measures is necessary to protect sensitive data and ensure the security of communication systems.
- **Research and development:** Increasing investment in research and development in the field of secure communication is crucial for supporting innovation and the long-term improvement of the communication infrastructure for IZS units.

These measures should enhance the efficiency, security, and preparedness of IZS units for crisis situations in the Czech Republic.

Introduction

Public Protection and Disaster Response (PPDR) communication is a key component of the state's response capabilities to various emergencies, including natural disasters, terrorist attacks and technological accidents. Ensuring reliable and resilient communication between the various components of emergency and security services, such as the police, fire services, medical services and others, is essential for the effective management of these crisis situations. Today, the growing number and complexity of such events present a challenge that must be addressed through modern technological solutions.

This study focuses on analysing the current technologies used in the field of public safety and disaster response communications within the European Union, with a particular emphasis on the use of 5G networks. 5G technology offers significant advantages in terms of speed, capacity and data transmission security, which are key factors for the successful implementation of PPDR systems. Combining 5G networks with existing emergency communication systems can significantly enhance the ability to respond effectively to emergencies and ensure a high level of public protection.

This study examines various approaches and technological solutions implemented in foreign emergency communication systems, such as those in Finland, Germany, South Korea and other countries. The analysis of foreign use-cases provides best practices that can also be applied in the context of the Czech Republic. The study focuses on identifying the factors that contribute to the effectiveness and resilience of these systems, whilst also seeking to identify potential risks and challenges that may arise during their implementation in a local environment.

1 Definition of PPDR/IZS

1.1 Definition of PPDR

Public Protection and Disaster Relief (PPDR) is an acronym denoting activities and services aimed at public protection and emergency management. Translated, PPDR means 'Public Protection and Disaster Relief'. This term encompasses a wide range of activities aimed at ensuring the safety of the population and an effective response to crisis situations, such as natural disasters, technological accidents and terrorist attacks.

In the Czech Republic, this acronym is not defined in legislation. The Czech legal framework does not contain a direct definition of PPDR, but related activities are regulated in several laws, for example in Act No. 239/2000 Coll. on the Integrated Rescue System and Act No. 240/2000 Coll. on Crisis Management.

The term PPDR as such is defined in European documents and standards, which provide a framework for the harmonisation and interoperability of emergency communication systems between EU Member States[1] .

The European Union has a strategy for PPDR communications[2] aimed at modernising and harmonising the radio spectrum and technologies across Member States. A key objective is the transition to broadband networks, which will enable better information sharing and increase the effectiveness of emergency response operations. The strategy includes the use of the 700 MHz band for PPDR broadband services, which is intended to ensure sufficient capacity for data transmission, including video and voice services.

The implementation of 5G technologies in PPDR communications is a further step in this strategy[3], as 5G offers higher transmission speeds, lower latency and greater reliability, which is crucial for emergency communications. In the Czech Republic, for example, these strategies are embodied in the 5G spectrum auction.

1.2 Definition of the Integrated Rescue System

In the Czech Republic, PPDR is implemented through the IZS. This system is comprehensive and involves the coordination of both core and extended units that cooperate in managing emergencies. The core components of the IZS include the Fire and Rescue Service of the Czech Republic, the Police of the Czech Republic, the Emergency Medical Service and Fire Protection Units. The extended components then include the armed forces, other armed security forces, public health authorities, emergency response services, civil protection facilities and non-profit organisations.

Most European countries have their own versions of integrated rescue systems, which involve the coordination of various rescue service components, the armed forces and other specialised units. These systems may differ in name, organisation and scope, but they all share similar objectives and functions.

1.3 Means for delivering PPDR services

1.3.1 Frequency spectrum

The frequency spectrum is a key element in ensuring PPDR services, as it enables the transmission of signals between the various components of the emergency response system. In the Czech Republic, specific frequency bands are reserved for the IZS components. These bands ensure reliable and secure communication between IZS components during crisis situations. Harmonisation of these bands at European level

[1] https://www.cept.org/ecc/topics/public-protection-and-disaster-relief-ppdr

[2] https://www.cept.org/ecc/topics/public-protection-and-disaster-relief-ppdr

[3] https://eur-lex.europa.eu/eli/dir/2018/1972/oj

enables effective cross-border cooperation and interoperability, which is essential for managing cross-border crisis situations. Dedicated frequency bands for emergency services are therefore vital for ensuring an effective crisis response and coordination between emergency services.

1.3.2 Use of frequency bands – dedicated and shared

The use of frequency bands for emergency services includes both dedicated and shared bands, enabling effective and flexible emergency communications. Dedicated frequency bands, such as the 380–385 MHz band for the PEGAS/TETRAPOL IP network, are reserved specifically for the needs of the emergency services and provide a high level of reliability and security due to the absence of commercial traffic. Shared frequency bands, such as 700 MHz and 3400–3600 MHz, which are also used for commercial mobile services, offer additional capacity and flexibility. Shared bands can be dynamically allocated according to current needs and utilise QoS technology to ensure priority access to PPDR services in emergency situations, thereby enabling effective communication between emergency services. This combined approach ensures that emergency services always have reliable means of communication available for the effective management of emergencies.

1.3.3 Types of networks used by IZS/PPDR services – public and private networks

Both public and private networks are used to provide PPDR services.
Public networks are operated by commercial operators; they offer wide coverage and high capacity thanks to modern technologies such as 2G, LTE and 5G, but may face challenges with prioritisation and security during emergencies due to the obligation to provide a publicly available electronic communications service.
Private networks are specifically reserved for the internal needs of central and local government, and the needs of emergency and security services. Depending on their configuration, these networks also provide greater reliability, security and the ability to prioritise traffic. Critical infrastructure obligations often apply to these networks as well.

2 Definition within the Czech Republic

PPDR in the Czech Republic focuses on public protection and the management of emergencies and crisis situations through the coordinated activities of the components of the Integrated Rescue System (IZS). This system is fundamental to an effective response to various types of crises.

The Czech Republic's Security Strategy identifies a number of security threats and sources of instability that have a direct impact on the need for effective public protection and disaster response systems. The main threats include terrorism, cyber-attacks, hybrid threats, natural disasters, technological accidents and pandemics. These threats require a robust and interoperable communications infrastructure that will enable a rapid and coordinated response from the Integrated Rescue System (IRS).

In view of these threats, it is crucial that PPDR systems are modernised and integrated, thereby enhancing the Czech Republic's ability to effectively manage crisis situations. For example, cyber attacks and hybrid threats require advanced protection of communication networks, whilst natural disasters and technological accidents place an emphasis on rapid and reliable communication between emergency services.

Changes in the security environment place new demands on communications infrastructure. The Czech Republic is preparing for the end of support for the TETRAPOL system, as support for TETRAPOL has been paid for by the Czech Republic until 2035. The modernisation of PPDR systems involves a transition to broadband communication technologies, which will offer higher capacity, speed and reliability of communication.

Investments in the modernisation of PPDR systems therefore reflect the need to adapt to the changing security environment. A modern and interoperable communications infrastructure will enable better coordination of emergency services, a faster response to crisis situations and an increase in the overall safety of the population.

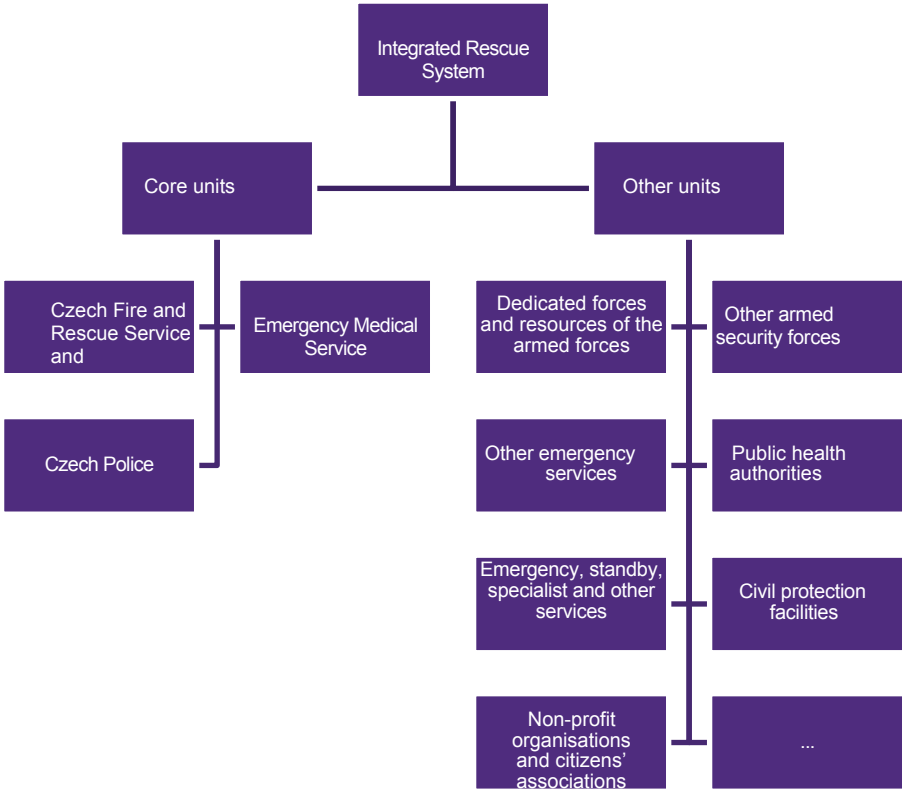
2.1 Components of the Integrated Rescue System (IRS)

The Integrated Rescue System of the Czech Republic is a comprehensive structure comprising multiple components that work together to ensure public safety and the effective management of emergencies. The IZS is designed to enable a rapid and coordinated response to various types of crisis situations, including natural disasters, technical accidents, terrorist attacks and other emergencies that may endanger the lives, health or property of citizens.

One of the main advantages of the IZS is its ability to link various organisations and institutions into a single functional unit capable of responding effectively to crisis situations. This system includes both core units, which are key to day-to-day rescue operations, and other specialised units that are deployed during larger-scale or specific crises.

Under Act No. 239/2000 Coll., on the Integrated Rescue System, IZS units are divided into basic and other units. The basic IZS units ensure round-the-clock readiness to receive reports of emergencies, assess them and carry out immediate intervention at the scene of the emergency. Mutual communication refers to the coordinated approach of these components in preparing for emergencies and in carrying out rescue and recovery operations. The IZS components also perform key tasks in accordance with the Crisis Act.

Further details on the organisation and activities of the Integrated Rescue System are specified in Decree No. 328/2001 Coll., on certain details regarding the provision of the Integrated Rescue System. This decree sets out specific rules and procedures that the IZS units must adhere to.



Structure of the Integrated Rescue System

2.1.1 Core components of the IZS

The basic components of the IZS include:

- The Fire and Rescue Service of the Czech Republic (HZS ČR), including fire protection units – organised to provide comprehensive coverage of the region
- The Police of the Czech Republic (PČR)
- Emergency medical service providers

2.1.1.1 Fire and Rescue Service of the Czech Republic (HZS ČR)

The Fire and Rescue Service of the Czech Republic is a core component of the Integrated Rescue System and the coordinator of rescue operations and civil protection. The HZS ČR is responsible for responding to fires, chemical and radiological accidents, road traffic accidents and other emergencies. In addition, it carries out preventive activities and training aimed at improving public safety.

The Fire and Rescue Service of the Czech Republic is a unified emergency service whose primary task is to protect lives, health, the environment, animals and property from fires and other emergencies. It contributes to ensuring the safety of the Czech Republic by carrying out tasks relating to fire protection, civil protection, civil emergency planning, crisis management and other tasks in accordance with the law. These activities are defined in particular by Act No. 320/2015 Coll. on the Fire and Rescue Service, Act No. 133/1985 Coll. on Fire Protection and Act No. 239/2000 Coll. on the Integrated Rescue System. The Fire and Rescue Service of the Czech Republic falls under the remit of the Ministry of the Interior.

The history of the Fire and Rescue Service of the Czech Republic dates back to the civil defence system, specifically to the 75th Rescue and Training Base in Olomouc of the Czech Army, which was established in 1991. During 2000, a detached rescue battalion was established there, stationed at the Hlučín garrison. In 2004, this battalion formed the basis of the newly established 157th Rescue Battalion. By a resolution of the Czech Government dated 22 October 2007 and following the approval of the restructuring of the Ministry of Defence of the Czech Republic, the 157th Rescue Battalion was transferred to the Fire and Rescue Service of the Czech Republic, and on 1 January 2009, the Rescue Unit of the Fire and Rescue Service of the Czech Republic was established.

The headquarters of the Rescue Unit of the Fire and Rescue Service of the Czech Republic is located in Hlučín, and the unit has two rescue companies – one in Jihlava and the other in Zbiroh. The rescue companies are equipped for a wide range of rescue operations, from dealing with the aftermath of natural disasters to providing assistance during industrial accidents.

In some documents, the Fire and Rescue Service is referred to as the 'Fire Protection Unit' (JPO), which is understood to mean an organised body comprising professionally trained personnel, firefighting equipment and material resources for fire protection. Given that the outbreak of a fire or other emergency cannot be ruled out anywhere in the Czech Republic, the JPO system has been established to ensure effective assistance across the whole of the Czech Republic within a specified time limit, using a specific number of personnel and resources (firefighters, firefighting equipment and other fire protection resources). Currently, this assistance is provided by 247 units of the Fire and Rescue Service of the Czech Republic, 93 corporate fire and rescue units, 6,063 municipal volunteer fire brigades and 89 corporate volunteer fire brigades. Due to the rapid development of new technologies, industrial growth and urban changes, the Joint Fire and Rescue Service faces new challenges to which it must respond. In this context, a long-term priority for the Czech Fire and Rescue Service is the renewal of the existing equipment used by fire and rescue units.

In 2023, there were 7,826 firefighters registered with the Fire and Rescue Service of the Czech Republic, 3,148 firefighters in corporate fire and rescue services, and 1,150 firefighters in corporate voluntary fire brigades, and 79,468 firefighters in municipal voluntary fire brigades.

The following units fall under the Fire and

Rescue Service of the Czech Republic:

Director General

Ministry of the Interior – General Directorate of the

Fire and Rescue Service of the Czech Republic

Fire and Rescue Service of the City of Prague

Central Bohemia Regional

Fire Service South

Bohemia Regional Fire

Service Plzeň Regional

Fire Service Karlovy Vary

Regional Fire Service Ústí

nad Labem Regional Fire

Service Liberec Regional

Fire Service

Fire and Rescue Service of the

Hradec Králové Region Fire and

Rescue Service of the

Pardubice Region

Fire and Rescue Service of the Vysočina Region

Fire and Rescue Service of the

South Moravian Region Fire and

Rescue Service of the Olomouc

Region

Fire and Rescue Service of the

Moravian-Silesian Region Fire

and Rescue Service of the Zlín

Region Rescue Unit of the Fire

and Rescue Service of the

Czech Republic Secondary

Vocational School of Fire

Protection and Higher
Vocational School of Fire
Protection
Technical Institute of Fire Protection
Fire Protection Schools in Frýdek-Místek Fire
and Rescue Service of the Czech Republic
School and Training Facilities Institute of
Civil Protection
Service and Repair Facility of the Fire and
Rescue Service of the Czech Republic
Czech National Committee of the CTIF
Police and Firefighters Foundation
Fire Protection Exhibition in Zbiroh Prague
Castle Fire Protection Unit

2.1.1.2 Fire protection units assigned to provide comprehensive coverage of the region

Fire protection units include both professional and voluntary fire brigades. Professional units form part of the Fire and Rescue Service of the Czech Republic and operate at national level, whilst voluntary fire brigades, organised at local level, provide support during operations and often act as the first responders to minor fires and other incidents.

The fire service system is designed to ensure effective assistance across the whole of the Czech Republic within a specified time limit, with sufficient personnel and resources. This system ensures that the protection of property and lives is not limited solely to the capabilities of individual municipalities, but is guaranteed at national level. Fire protection units respond not only to fires, but also to road traffic accidents, leaks of hazardous substances, natural disasters and other emergencies.

The organisation and activities of fire protection units are governed by Act No. 133/1985 Coll., on fire protection, and Decree of the Ministry of the Interior No. 247/2001 Coll., which sets out the conditions for comprehensive coverage of the territory of the Czech Republic by fire protection units. Government Regulation No. 172/2001 Coll., implementing the Act on Fire Protection, defines the operational districts and support points of fire protection units. Each cadastral area of a municipality is assigned appropriate fire protection coverage by fire protection units according to the level of risk, ensuring rapid and effective assistance during emergencies throughout the territory of the Czech Republic.

Professional fire protection units, specifically the Fire and Rescue Service of the Czech Republic, are subordinate to the Ministry of the Interior. This ministry provides the legislative framework, funding and overall coordination of the activities of the Fire and Rescue Service of the Czech Republic. Voluntary fire brigades are organised at the municipal level; municipalities are responsible for their funding and equipment, and they cooperate with the Fire and Rescue Service of the Czech Republic.

The basic principle of the organisation of the fire protection unit system[4] is that each municipal cadastral area is, according to its level of risk, assigned appropriate fire protection coverage, which guarantees:

the response time of fire and rescue units, determined by the operational capacity of the units according to their type,

the number of fire and rescue service personnel and resources (number of fire and rescue service units and their equipment, number of firefighters) that will arrive at the scene of the incident by a specified time.

Level of risk in the municipality	Number of fire and rescue service units and their response time to the scene
I	A: 2 firefighting units within 7 minutes and a further 1 firefighting unit within 10 minutes B: 1 firefighting unit within 7 minutes and a further 2 firefighting units within 10 minutes
II	A: 2 firefighting units within 10 minutes and a further 1 unit within 15 minutes B: 1 firefighting unit within 10 minutes and a further 2 units within 15 minutes
III	A: 2 fire engines within 15 minutes and a further 1 fire engine within 20 minutes B: 1 fire engine within 15 minutes and a further 2 fire engines within 20 minutes
IV	A: 1 fire brigade within 20 minutes and a further 1 fire brigade within 25 minutes

Basic table of fire brigade unit coverage across the Czech Republic

1 Fire brigade unit – one fire brigade unit

2 Fire brigade unit – two

fire brigade units min –

minutes

Počet JPO podle kategorie * vojenské hasičské jednotky

	2019	2020	2021	2022	2023
HZS ČR - JPO I	245	245	246	246	247
JSDH obcí	6 698	6 389	6 288	6 232	6 063
JPO II	237	241	244	244	244
JPO III	1 356	1 380	1 386	1 403	1 407
JPO V	5 105	4 768	4 658	4 585	4 412
HZS podniků - JPO IV	96	95	96	92	93
z toho VHJ*	16	16	17	16	17
JSDH podniků - JPO VI	136	108	102	100	89

[4] https://www.hzscr.cz/clanek/jednotky-po-961839.aspx?q=Y2hudW09Mg%3D%3D

A fire brigade system established in accordance with this principle guarantees a basic level of assistance provided by fire brigades and is referred to as the territorial coverage of the Czech Republic by fire brigades (hereinafter “territorial coverage”). Comprehensive coverage is based on Section 65(6) and Annex No. 1 of Act No. 133/1985 Coll., on fire protection, as amended; it is further regulated by Section 1 and Annex No. 1 of Decree of the Ministry of the Interior No. 247/2001 Coll., on the organisation and activities of fire protection units, as amended by Decree No. 226/2005 Coll., Section 5 of Government Regulation No. 172/2001 implementing the Act on Fire Protection, as amended by Government Regulation No. 498/2002 Coll.

Druh události	2019	2020	2021	2022	2023	Index %
počet mimořádných událostí	130 229	143 500	142 197	151 619	153 275	101
počet ostatních činností	17 237	18 325	19 607	19 364	18 653	96
Celkem	147 466	161 825	161 804	170 983	171 928	101

The growing number of incidents handled by the Fire and Rescue Service (https://www.hzscr.cz/soubor/informacni-servis-statistiky-rocenka-2023-pdf.aspx)

Types of incidents handled in 2023 (https://www.hzscr.cz/soubor/informacni-servis-statistiky-rocenka-2023-pdf.aspx)

Negativní vlivy u zásahů

Druh negativního vlivu	2019	2020	2021	2022	2023	Index %
Pozdní příjezd JPO						
špatná funkce ohlašovny požárů	8	7	7	12	5	42
selhání spojovacích prostředků	143	241	232	170	230	135
pozdní ohlášení oproti zpozorování	6	7	4	9	8	89
pozdní vyhlášení poplachu oproti ohlášení	14	8	6	7	13	186
pozdní výjezd oproti vyhlášení poplachu	61	102	115	99	104	105
obtížná cesta na místo zásahu	385	313	372	360	510	142
selhání vozidla na cestě	11	15	16	10	9	90
přivolaná místní jednotka nevyjela k požáru	71	64	62	47	24	51
pozdní přivolání dalších JPO	3	3	0	0	2	x
jiné	46	60	49	70	70	100

In conclusion, one of the findings from the 2023 Statistical Yearbook of the Fire and Rescue Service of the Czech Republic ((https://www.hzscr.cz/soubor/informacni-servis-statistiky-rocenka-2023-pdf.aspx)) concerning factors adversely affecting operations.

(Source: https://www.hzscr.cz/soubor/informacni-servis-statistiky-rocenka-2023-pdf.aspx)

2.1.1.3 Czech Police (PČR)

The Police of the Czech Republic plays a key role in ensuring public order and safety. The PČR is responsible for the prevention and suppression of criminal activity, the protection of citizens’ property and health, and assistance in rescue and disaster relief operations.

The police also provide support to other components of the Integrated Rescue System (IRS) in the coordination and management of operations.

The Police of the Czech Republic is a unified armed security force established under Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended. Its task is to protect the safety of persons and property, maintain public order and prevent crime. It also performs tasks under the Code of Criminal Procedure and other tasks in the field of internal order and security entrusted to it by laws, European Community regulations and international treaties that form part of the legal order of the Czech Republic.

The Police of the Czech Republic is subordinate to the Ministry of the Interior. It comprises the Police Presidium, units with nationwide jurisdiction, regional police directorates and units established within the regional directorates. The Act establishes 14 regional police directorates, whose territorial jurisdictions correspond to the territorial jurisdictions of the 14 regions of the Czech Republic.

2.1.1.4 Emergency Medical Service (EMS)

The Emergency Medical Service is responsible for providing urgent medical assistance during emergencies. The EMS provides pre-hospital care, transport of patients to healthcare facilities and support during mass casualty incidents. Its work is crucial for saving lives and minimising the health consequences of crisis situations.

The Emergency Medical Service (EMS) is a medical service which, in response to an emergency call, provides pre-hospital emergency care to people with serious health conditions or whose lives are in immediate danger. The availability of the emergency medical service is ensured by a plan covering the region with dispatch bases. This plan determines the number and location of dispatch bases according to the demographic, topographical and risk parameters of individual municipalities and city districts, so that the scene of the incident can be reached from the nearest dispatch base within a response time of 20 minutes[5] .

The main conditions governing the operation of the emergency medical service are defined in Act No. 374/2011 Coll., on the emergency medical service, and related implementing decrees. The EMS falls within the remit of the regions, with service providers being publicly funded organisations established by individual regions and methodologically supervised by the Ministry of Health.

2.1.2 Other armed and rescue services

Other IZS units provide planned assistance on request during rescue and clearance operations. Other IZS units include, for example:

Municipal/city police

Dedicated forces and resources of the armed

forces Other armed security forces Other

rescue services

Armed Forces of the Czech Republic

Public health authorities

Emergency, standby, specialist and other services

The Czech Red Cross rescue team Civil protection

facilities

Non-profit organisations and citizens' associations that can be utilised for rescue and clearance work, e.g. the Association of Volunteer Rescuers of the Czech Republic, z.s.

Czech Mountain Rescue Service

Czech Red Cross Water Rescue

Service Czech Red Cross Rock

Rescue Service

Specialist medical facilities at university hospital level for the provision of specialist care (these become part of the Integrated Rescue System during states of emergency).

[5] https://www.zakonyprolidi.cz/cs/2011-374

2.1.2.1 Army of the Czech Republic

The Czech Armed Forces are one of the key other components of the Integrated Rescue System, providing support during rescue and clearance operations. The Czech Armed Forces are involved in crisis management and civil protection, with their role defined by Act No. 219/1999 Coll., on the Armed Forces of the Czech Republic. The Czech Armed Forces are primarily involved in rescue operations upon request – they are called upon to provide their specific capabilities, resources and specialist personnel to deal with emergencies and crisis situations.

The main role of the Czech Armed Forces within the Integrated Rescue System is:

To provide specialist and technical assistance during large-scale natural disasters, such as floods, forest fires, earthquakes and other natural disasters.

Assisting in the evacuation of the population from endangered areas and providing humanitarian aid.

Assisting in the clean-up following chemical, biological, radiological and nuclear incidents.

Support in ensuring logistics, transport and communications in crisis situations. Cooperation

with other components of the Integrated Rescue System (IRS) in fulfilling tasks to protect

the population and property. Assistance in identifying and addressing hybrid cyber

threats/attacks.

The Czech Armed Forces are equipped with specialised units and equipment that are ready for rapid deployment when required. These units include, for example, engineering units capable of carrying out technical interventions, building temporary bridges and removing obstacles, and chemical units trained to respond to hazardous substance leaks.

Cooperation between the Czech Army and other components of the Integrated Rescue System is coordinated through crisis management teams at various levels of central and local government. This coordination ensures the effective use of all available resources and expertise in dealing with crisis situations and emergencies.

2.1.3 Coordination and communication within the Integrated Rescue System

Effective coordination between the various components of the Integrated Rescue System is essential for the successful management of crisis situations. A key element of this coordination is a reliable and secure communications infrastructure that enables the rapid and accurate exchange of information. In the Czech Republic, the PEGAS/TETRAPOL IP radio communication network is used for this purpose, providing secure communication between the components of the Integrated Rescue System.

The main coordinator of the activities of the Czech Integrated Rescue System is the Czech Fire and Rescue Service. This role is established by Act No. 239/2000 Coll., on the Integrated Rescue System, and regulated in more detail by Decree No. 328/2001 Coll., on certain details of the operation of the Integrated Rescue System. The Ministry of the Interior coordinates and develops emergency communications (both voice and text) to ensure connection to the core components of the Integrated Rescue System via the numbers 112, 150, 155 and 158. It takes measures to ensure accessibility for people with disabilities, collects information on the quality of emergency communications and cooperates with other ministries and EU bodies.

2.1.3.1 Communication needs of the Integrated Rescue System

The communication needs of the IZS units relate to the performance of their activities in accordance with the law, defined conditions and operational procedures. These needs evolve with technological developments in communication infrastructure and security standards. Historically, these needs were met through separate voice and data services, which are now increasingly being integrated thanks to advanced technologies.

The management of the Integrated Rescue System is divided into 14 regions, which corresponds to the division of regional control centres and the management of communication networks. Private networks (PEGAS/TETRAPOL IP, DMR and TETRA) and relayed communications are interconnected at the control centre level (the control centre has access to all available networks within the region, but the systems are not interconnected) or at the level of the incident commander, who is equipped with multiple communication terminals. Control centres are interconnected via the public fixed network (VPS) and the public mobile network (VMS), as well as with each other. Data services are available only at the control centre level (fixed data network) or, to a limited extent, to certain users (e.g. the Police of the Czech Republic) in the form of the so-called Mobile Secure Platform and mobile data services. From a crisis communication perspective, data services currently play only a limited supporting role due to legislation that has not been updated for a long time.

Mobile communications for the Integrated Rescue System (IRS) units are currently provided by several unconnected communication solutions. The current concept of the communication infrastructure for security and rescue services is based on a historical model, where the key task of the communication infrastructure was to ensure secure voice communication between individual IRS units, which

was primarily provided by the TETRAPOL system (operated in the Czech Republic as the PEGAS/TETRAPOL IP network). In addition to this system, other analogue and digital radio networks such as DMR, TETRA and mobile operators' services are also used to a limited extent.

2.1.3.2 Material reserves in the Czech Republic

Material reserves are a key component of the Czech Republic's crisis management. Their administration falls within the remit of the State Material Reserves Administration (SSHR), which maintains stocks of strategic materials and raw materials needed to manage crisis situations such as natural disasters, technical accidents or other emergencies. Material reserves include, for example, food, petroleum products, medical supplies and other essential raw materials that can be rapidly mobilised to ensure the stability and security of the state.

The SSHR is governed by Act No. 97/1993 Coll., on the Competence of the State Material Reserves Administration. This Act defines the scope and method of securing state material reserves, their replenishment and renewal, and stipulates that the SSHR is subordinate to the Government of the Czech Republic and coordinates its activities with other crisis management bodies and the Integrated Rescue System (IZS).

Material reserves are stored in strategically located warehouses throughout the country, enabling their rapid and effective deployment in crisis situations. The SSHR is also responsible for updating and managing stocks to ensure they meet current needs and are always ready for use.

The material reserves also include the resources necessary for managing crisis situations, ranging from fuel to essential equipment.

2.2 Legislative framework for PPDR/IZS

The legislative framework for PPDR/IZS services in the Czech Republic is set out in several laws and regulations, which together ensure the organisation, coordination and technical support of the IZS. PPDR as such is not explicitly defined in Czech law, but its principles and operations are covered by the following legislative documents:

Act No. 240/2000 Coll. on Crisis Management and on Amendments to Certain Acts (Crisis Act)

Act No. 239/2000 Coll. on the Integrated Rescue System and on Amendments to Certain Acts

Act No. 127/2005 Coll. on Electronic Communications and on Amendments to Certain Related Acts (the Electronic Communications Act)

2.2.1 Act No. 240/2000 Coll. on Crisis Management and on Amendments to Certain Acts (Crisis Act)

Act No. 240/2000 Coll. on Crisis Management and on Amendments to Certain Acts defines:

Security of crisis management information systems: Information systems must be technically and programmatically adapted for operation in difficult conditions, which includes resilience to outages, security measures against cyber threats, and the ability to quickly restore operations following a disruption.

Levels of crisis management: The Act defines various levels of crisis situations (state of emergency, state of national threat, state of war) and specifies the powers and duties of individual authorities in declaring and managing them.

Duties of state and local government bodies: It sets out the duties and responsibilities of state and local government bodies in preparing for and managing crisis situations.

2.2.2 Act No. 239/2000 Coll. on the Integrated Rescue System and amending certain acts

Act No. 239/2000 Coll. on the Integrated Rescue System and amending certain acts:

Defines the core and other components of the Integrated Rescue System (IRS): It defines the main components of the IRS, which are the Fire and Rescue Service of the Czech Republic, the Police of the Czech Republic, the Emergency Medical Service, and other components that may be involved in rescue and recovery operations, such as the Army, public health authorities, emergency services and specialist units.

It sets out the responsibilities of the individual components of the IZS: Each component has clearly defined responsibilities regarding preparedness for emergencies and crisis situations, their management and subsequent recovery.

Coordination and management of the Integrated Rescue System: The Act sets out the method of coordination and management between the individual components of the Integrated Rescue System, including the establishment and operation of operational and information centres.

2.2.3 Act No. 127/2005 Coll. on Electronic Communications and on Amendments to Certain Related Acts (the Electronic Communications Act)

Act No. 127/2005 Coll. on Electronic Communications regulates the conditions for the provision of electronic communications services, which has a direct impact on the activities and coordination of PPDR components in the Czech Republic. This Act ensures that the communications infrastructure is resilient, reliable and prepared for crisis situations.

Aspects relevant to the PPDR:

Infrastructure security: The Act requires communications service providers to ensure the continuous availability of services, which is crucial for the effective functioning of the Integrated Rescue System (IRS) units during crises.

Communication prioritisation: Obligations include enabling priority calls and data transmissions for the needs of emergency services, thereby ensuring that critical communications are not interrupted even when networks are overloaded.

Radio spectrum allocation: The law regulates the allocation of specific frequencies for public protection and emergency services, thereby ensuring reliable and continuous communication.

Although PPDR as a separate concept is not explicitly defined in Czech law, the legislative framework provided by the above-mentioned laws ensures that the principles and operations associated with PPDR are effectively integrated into the functioning of the Integrated Rescue System (IRS). These laws provide the necessary structure and powers for crisis management, public protection and coordination between the various emergency services.

2.2.4 Examples of regulations that must be taken into account when addressing IZS communication

Standards and agreements play an important role within the broader spectrum of events at the international level where the assistance of the Integrated Rescue System will be required, for example in the event of a state of war, natural disasters or terrorist attacks.

Examples of regulations that must be taken into account when addressing communication within the Integrated Rescue System include:

2.2.4.1 International relations and ties. Constitutional laws.

International relations and ties:

North Atlantic Treaty (Washington, D.C., 4 April 1949)

No. 168/1991 Coll., Communication from the Federal Ministry of Foreign Affairs on the Czech and Slovak Federal Republic's accession to Additional Protocols I and II to the Geneva Conventions of 12 August 1949 and on the protection of victims of international armed conflicts and conflicts not of an international character, adopted in Geneva on 8 June 1977

Constitutional Acts:

No. 1/1993 Coll., Constitution of the Czech Republic

No. 347/1997 Coll., Constitutional Act on the Establishment of Higher Territorial Self-Governing Units and on the Amendment of Constitutional Act of the Czech National Council No. 1/1993 Coll., Constitution of the Czech Republic

No. 110/1998 Coll., Constitutional Act on the Security of the Czech Republic

2.2.4.2 Public administration:

No. 36/1960 Coll., Act on the Territorial Division of the State

No. 2/1969 Coll., Act on the Establishment of Ministries and Other Central State Administration Bodies of

the Czech Republic No. 128/2000 Coll., Act on Municipalities (Municipal Organisation)

No. 129/2000 Coll., Act on Regions (Regional Organisation)

No. 131/2000 Coll., Act on the Capital City of Prague

No. 320/2002 Coll., Act on the Amendment and Repeal of Certain Acts in Connection with the Termination of the

Activities of District Offices No. 314/2002 Coll., Act on the Designation of Municipalities with an Authorised Municipal

Authority and the Designation of Municipalities with Extended Powers

No. 388/2002 Coll., Decree of the Ministry of the Interior on the determination of administrative districts of municipalities with delegated municipal authorities and administrative districts of municipalities with extended powers

No. 564/2002 Coll., Decree of the Ministry of the Interior on the determination of the territories of districts of the Czech Republic and the territories of districts of the capital city of Prague

2.2.4.3 The field of crisis management. The field of emergency planning and civil protection.

No. 240/2000 Coll., Act on Crisis Management and on Amendments to Certain Acts (Crisis

Act) No. 181/2014 Coll., Act on Cyber Security

No. 82/2018 Coll. Decree on security measures, cyber security incidents, reactive measures, requirements for submissions in the field of cyber security and data destruction (Cyber Security Decree)

No. 462/2000 Coll., Government Regulation implementing Section 27(8) and Section 28(5) of Act No. 240/2000 Coll., on crisis management and amending certain acts (Crisis Act)

No. 432/2010 Coll., Government Regulation on criteria for determining elements of critical infrastructure

No. 75/2001 Coll., Decree of the Czech Mining Authority laying down mining and technical conditions for the establishment, use and protection of mine workings selected for use in crisis situations for the application of preventive, technical and safety measures and the performance of inspections

No. 281/2001 Coll., Decree of the Ministry of Education, Youth and Sport implementing Section 9(3)(a) of Act No. 240/2000 Coll., on crisis management and amending certain acts (the Crisis Act)

No. 239/2000 Coll., Act on the Integrated Rescue System and amending certain acts

No. 463/2000 Coll., Government Regulation laying down rules for participation in international rescue operations, the provision and receipt of humanitarian aid, and the reimbursement of expenses incurred by legal entities and self-employed natural persons for the protection of the population

No. 328/2001 Coll., Decree of the Ministry of the Interior on certain details concerning the security of the integrated rescue system

No. 380/2002 Coll., Decree of the Ministry of the Interior on the preparation and implementation of civil protection tasks

2.2.4.4 Other areas

Fire protection

Major accident prevention

Economic measures for crisis situations Oil safety

Healthcare. Public health protection

Flood protection and emergency water supply Nuclear safety

Security and public order Defence

Chemical substances and the prohibition of chemical

weapons Waste management

Environment (air protection) Plant health

Veterinary care Energy

Transport

Communications and information systems Cyber

security

Recovery of affected areas Banking and

finance

Classified Information and Personal Data Protection Other Related

Legislation

Government resolutions, directives and methodological guidelines of ministries and other central administrative authorities

2.3 Emergency, crisis situation, states of emergency

2.3.1 Emergency

An emergency is an event that threatens lives, health, property or the environment and requires rescue and clean-up operations. Emergencies include, for example, natural disasters, industrial accidents or mass accidents. The aim is to minimise the consequences of such events through an effective and rapid response by the emergency services.

2.3.1.1 Overview of emergencies involving unacceptable risk

Based on the Threat Analysis for the Czech Republic, 22 types of emergencies have been identified for which the declaration of a state of emergency can reasonably be anticipated. For these emergencies, the responsible central administrative authorities have drawn up standard plans, which have become a fundamental part of all contingency plans. It is assumed that these plans cannot be managed using standard resources and procedures. An overview is provided in the table below.

No.	Emergency	Responsibility
1	Prolonged drought	Ministry of the Environment
2	Extremely high temperatures	Ministry of the Environment
3	Flash floods	Ministry of the Environment
4	Heavy rainfall	Ministry of the Environment
5	Extreme wind	Ministry of the Environment
6	Flood	Ministry of the Environment
7	Epidemic – mass infection of people	Ministry of Health
8	Epiphytotics – mass outbreaks in field crops	Ministry of Agriculture
9	Epizootics – mass outbreaks in livestock	Ministry of Agriculture
10	Large-scale disruption of food supplies	Ministry of Agriculture
11	Disruption to the functioning of critical electronic communications systems	Czech Telecommunications Office
12	Breach of the security of critical information infrastructure	National Security Authority
13	Exceptional flooding	Ministry of Agriculture
14	Leak of a hazardous chemical substance from a stationary installation	Ministry of the Environment
15	Large-scale disruption to drinking water supply	Ministry of Agriculture
16	Large-scale disruption to gas supplies	Ministry of Industry and Trade
17	Large-scale disruption to the supply of oil and petroleum products	Administration of State Material Reserves
18	Radiation accident	State Office for Nuclear Safety
19	Large-scale disruption to electricity supply	Ministry of Industry and Trade
20	Large-scale migration waves	Ministry of the Interior
21	Large-scale breaches of the law (including terrorism)	Ministry of the Interior

22	Large-scale disruption of the state's financial and foreign exchange economy	Ministry of Finance

2.3.2 Crisis situation

A crisis situation arises when an extraordinary event escalates to a state requiring the declaration of a state of emergency. A crisis situation threatens national security, public order, and the lives and health of the population on a large scale and with great intensity. Resolving a crisis situation involves coordinated cooperation between the various components of the integrated rescue system and often also cooperation with international partners.

2.3.3 States of emergency

States of emergency are legally defined states that enable the adoption of extraordinary measures to manage crisis situations.

States of emergency are declared so that the powers and competences under Act No. 240/2000 Coll., on crisis management, and Constitutional Act No. 110/1998 Coll., on the security of the Czech Republic, are transferred to the crisis management authorities. The table below provides an overview of states of emergency, including their legal basis, the declaring authority, definition, territorial scope and duration.

Four types of crisis states are declared in the Czech Republic: State

of War

State of National Threat

State of Emergency

State of danger

NAME	DEFINING ACT	DECLARED BY	DEFINITION	AREA	DURATION
STATE OF WAR	Constitutional Act No. 1/1993 Coll., Constitution of the Czech Republic, Constitutional Act No. 110/1998 Coll., on the security of the Czech Republic	Parliament of the Czech Republic	If the Czech Republic is attacked or if it is necessary to fulfil international treaty obligations regarding collective defence against attack	The whole state	No restrictions
STATE OF EMERGENCY	Constitutional Act No. 110/1998 Coll., on the security of the Czech Republic	The Parliament of the Czech Republic, on the proposal of the Government	If the sovereignty of the state, the territorial integrity of the state or its democratic foundations are under immediate threat	The whole country, a limited territory	Not restricted
STATE OF EMERGENCY	Constitutional Act No. 110/1998 Coll., on the security of the Czech Republic	Government (Prime Minister)	In the event of natural disasters, environmental or industrial accidents, incidents or other dangers which, to a significant extent, threaten lives, health or property, or internal order and security	The whole country, a limited area	Up to 30 days (extension subject to the consent of the Chamber of Deputies)
STATE OF EMERGENCY	Act No. 240/2000 Coll., on crisis management	Regional Governor	Where lives, health, property or the environment are at risk, provided that the scale of the threat is not significant and it is not possible to avert the threat through the normal activities of administrative authorities, regional and municipal bodies, units of the integrated rescue system or critical infrastructure entities	The whole region, part of the region	Up to 30 days (extension subject to government approval)

2.3.3.1 State of war

Declared by the Parliament of the Czech Republic in the event of an attack on the state or in fulfilment of international treaty obligations regarding collective defence against attack.

The role of the armed forces during a state of war

During a state of war, the Czech Armed Forces play a vital role in defending the sovereignty and territorial integrity of the state. Their main task is to move to full combat readiness, which means that all units are prepared for immediate deployment in military operations. The Army is responsible for the mobilisation of forces, which includes calling up reservists and ensuring sufficient quantities of military equipment. In addition, the Army must address the replenishment of losses and form new military units to ensure continuous combat readiness.

Cooperation with international partners, particularly NATO, is also a significant part of the army's activities, which includes the coordination of military operations and logistical support for allied forces on Czech territory. The army carries out tasks related to the defence of the state and the fulfilment of international commitments in the field of collective defence. Economic mobilisation is also an important part of these preparations, involving the provision of the materials and logistical resources required for military operations. This ensures the army's long-term ability to respond to military challenges and threats.

2.3.3.2 State of Emergency

It is declared by the Parliament of the Czech Republic in the event of an immediate threat to the independence, territorial integrity or democratic foundations of the state.

2.3.3.3 State of emergency

Declared by the government in the event of large-scale natural disasters, environmental or industrial accidents that threaten large areas or a large number of people.

2.3.3.4 State of danger

Declared by the regional governor in the event of an immediate threat to life, health, property or the environment, where the situation cannot be managed by ordinary means.

Since the establishment of the Czech Republic, regional governors have declared states of danger for various reasons; examples

of the number of states declared:[6] 28 cases of flooding

4 cases of landslides

2 cases of hazardous substances being found 2 cases of extreme wind (tornadoes) 1 case of a waterworks failure

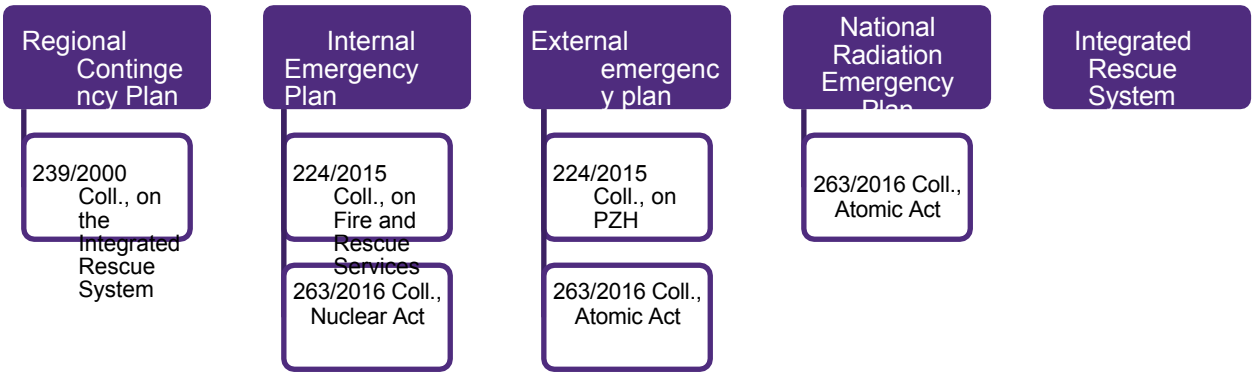
1 case of African swine fever 1 case of a pandemic

2.3.4 Contingency planning

Contingency planning is a key element of crisis management, the aim of which is to prepare for emergencies that may seriously endanger human life, health, property or the environment. This process involves drawing up and updating various planning documents that set out procedures for managing and resolving crisis situations.
The activities of both the core and other components of the Integrated Rescue System (IRS) are also linked to these contingency plans. These components must therefore always be prepared to deal with incidents that arise, in terms of capacity, communication and technical resources (equipment).

[6]https://www.priruckazastupitele.cz/10-krizove-rizeni-v-ceske-republice/

2.3.4.1 Types of Contingency Plans



Types of

of Emergency Plans

There are several types of emergency plans, which differ in their scope and specific requirements. The most significant include:

Regional Contingency Plan

The Regional Emergency Plan is a fundamental document used to manage emergencies within the region. These emergencies may include natural disasters, industrial accidents or other hazards threatening the population and property.

The regional emergency plan is drawn up by the regional Fire and Rescue Service in cooperation with the relevant bodies (Regional Authority, Municipal Authority, Police of the Czech Republic, Emergency Medical Service, Regional Veterinary Administration, Regional Public Health Authority, Regional Environmental Protection Authority). The plan is based on an analysis of the causes of emergencies and threats to the region. Two copies are produced: one forms part of the Regional Crisis Plan (RCP), the other is for the Operations and Information Centre (OIC). The plan is discussed and assessed by the Regional Security Council (BRK) and approved by the Regional Governor. It comprises three parts: information (characteristics of the region, risk analysis), operational (procedures and responsibilities), and specific activities.

External emergency plan

The external emergency plan is drawn up for facilities that handle hazardous substances and for nuclear installations. These plans serve to identify potential risks and set out measures to protect the public and mitigate the impact of accidents. In the event of a major accident, it is crucial to inform the public and coordinate the response of the integrated rescue system. The plan includes procedures for evacuation, warning and other necessary measures to minimise risks to the health and safety of citizens.

Internal emergency plan

Internal emergency plans are a key tool for ensuring emergency preparedness on operators' premises. They are drawn up for facilities where there is a risk of incidents with serious implications for safety and health. The plans focus on specific facilities, such as nuclear installations or workplaces with significant sources of ionising radiation, as well as operations handling hazardous substances classified in higher risk categories. Operators of these facilities are required to draw up and regularly update internal emergency plans so that they are prepared to manage potential crisis situations effectively.

National Radiation Emergency Plan

The National Radiation Emergency Plan is a key document for crisis preparedness in the event of incidents involving a radiation threat. This plan includes comprehensive measures to protect the public, such as iodine prophylaxis, evacuation and sheltering. It emphasises the timely warning and informing of the public to minimise health and safety risks. The plan also specifies procedures for coordinating responses to radiation accidents, including cooperation between the various components of the integrated rescue system and other relevant institutions. The aim is to ensure a rapid and effective response to radiation threats and to protect public health as much as possible.

Integrated Rescue System (IRS) emergency plans

Integrated Rescue System (IRS) emergency plans are a fundamental element of crisis management and are stored at the relevant regional Fire and Rescue Service (HZS) operational and information centres. These plans, which include the central IZS emergency plan as well as the emergency plans of individual regions, specify the procedures for activating the IZS in the event of an emergency. They contain important contact details for the core and other components of the IZS, an overview of available personnel and resources, and the method for summoning and informing the heads of IZS components and other responsible persons. The plans ensure effective coordination between the fire service, the police and the emergency medical service, and enable a rapid and effective response to crisis situations.

2.3.5 The crisis management system in the Czech Republic

Crisis management in the Czech Republic is comprehensive and involves not only the IZS units but also a wider range of public administration bodies, such as regional governors, mayors and other relevant institutions. This system is designed to ensure a coordinated and effective response to various types of crisis situations, including natural disasters, technological accidents, terrorist attacks and other emergencies.

Regional crisis management bodies ensure preparedness for crisis situations at the regional and municipal levels. Regions have security councils that coordinate preparations for crisis situations. Similar councils operate at the level of municipalities with extended powers, which establish crisis management teams in crisis situations. Regional governors and mayors lead these crisis management teams and inform the government of any crises that arise. Members of the security councils automatically become members of the crisis management teams.

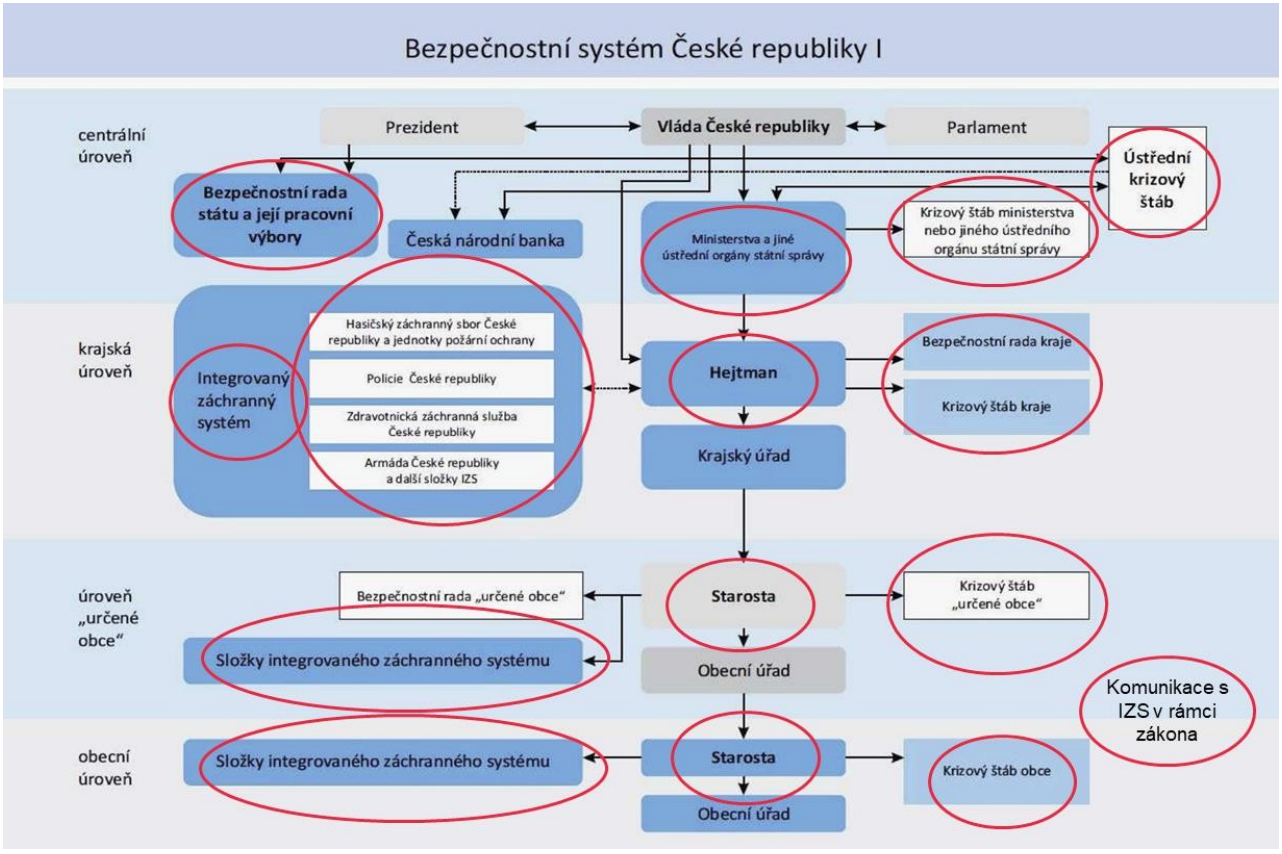
Regional fire and rescue services carry out tasks in the field of fire protection and crisis planning, as well as protecting the lives and health of the population, the environment, animals and property from fires and other emergencies and crisis situations (natural disasters, etc.). Regional headquarters of the Police of the Czech Republic ensure public order, whilst regional military commands play an important role in the field of defence.

2.3.5.1 The role of regional governors and mayors

Regional governors and mayors play a key role in the crisis management system at the level of regions and municipalities with extended powers. The regional governor is responsible for informing the government about a crisis situation and for coordinating the activities of crisis management teams. Mayors of municipalities with extended powers have similar responsibilities within their administrative territories. Both of these bodies are key players in the activation and leadership of crisis management teams, which are essential for the effective management of crisis situations.

2.3.5.2 Coordination and management bodies

Security councils operate at regional level to coordinate preparations for crisis situations. These councils are composed of representatives from key components of the Integrated Rescue System, public administration and other relevant organisations. The working body of the regional governor and the mayor of a municipality with extended powers is the crisis management team, which includes members of the security council and other experts as required. A crisis management team may also be established by the mayor of a municipal authority, and members of the security council automatically become members of this team.



Source: AMBIS University Crisis Management

2.3.5.3 Functions of crisis management teams

Crisis management teams fulfil several key functions:

Coordination of rescue and recovery operations: Crisis management teams organise and direct the activities of individual emergency services during emergencies.

Crisis communication: They ensure the reliable and effective exchange of information between all participating units and public administration bodies.

Strategic planning: They draw up plans for dealing with crisis situations and ensure they are kept up to date.

Situation assessment: They regularly assess the status of the crisis situation and decide on the necessary measures.

2.3.6 The state of IZS communication in the Czech Republic

2.3.6.1 Original state

The original state of the communication infrastructure of the Integrated Rescue System of the Czech Republic was characterised by the use of several unconnected communication solutions. A key element was a system based on TETRAPOL technology (known in the Czech Republic as the PEGAS network), which provided secure voice communication between individual IZS components, such as the Fire and Rescue Service, the Police of the Czech Republic and the Emergency Medical Service, with the exception of the Liberec Region Emergency Medical Service, which uses TETRA.

Alongside this system, other proprietary analogue and digital radio networks were used, such as DMR, TETRA, and also mobile operators' services.

2.3.6.2 Current status

At present, mobile communications for the IZS units are still provided by the aforementioned systems, with the PEGAS/TETRAPOL IP network continuing to play a key role. This network provides secure voice communication thanks to hardware-level encryption and is

used by all core emergency services units, with the exception of some ambulance services. A technological upgrade of the network has now been completed, involving a transition to IP technology between the radio and network layers. In addition, analogue and DMR networks are used as secondary communication systems with a lower level of security. The Czech Police and the Ministry of the Interior have access to the so-called Mobile Secure Platform, which utilises public mobile networks for secure access to internal systems.

2.3.6.3 Planned development

Planned development of the IZS communication infrastructure includes the implementation of a dedicated, unified CORE communication platform, which will interconnect the existing communication systems of all IZS components with the newly developed high-speed communication solution on commercial mobile operators' networks. The aim is to ensure high-speed data services and to increase the security and efficiency of communications. By 2025, the launch of a fully-fledged standalone (SA) 5G network is planned, which will offer sophisticated services such as network slicing and ultra-low latency. This development should also lead to a reduction in operating costs and increased flexibility of communication tools.

2.4 Classification of IZS/PPDR operations

PPDR interventions can be divided into several categories according to their scope and complexity. This classification helps to better understand the various levels of crisis situations and the corresponding communication needs. This section does not describe the current state of resources, but rather the needs of the IZS[7] .

Harmful effects of forces and phenomena caused by human activity, natural influences and accidents that threaten life, health, property or the environment and require rescue and clean-up operations. It is an emergency situation resulting in a state of emergency being declared.

Type of intervention	Description	Integrated Rescue System units	Communication requirements	Examples
Minor incidents	Standard routine operations requiring the intervention of a single emergency service	One unit	Voice communication, basic text communication	Ambulance call-outs to patients, small fires
Medium-scale incidents	Require coordination of two to three emergency services	Two to three units	Coordination of voice and data communications	Traffic accidents, major fires
Major incidents	Complex situations requiring the intervention of several emergency services	Multiple units	Highly demanding communications (voice, data, video)	Floods, mass casualty incidents
National incidents	Events with nationwide impact requiring coordination at national level	All agencies	Intensive use of all means of communication	Pandemics, national crises
International incidents	Require international cooperation and coordination	International cooperation	Interoperability between national systems	Cross-border floods, international crisis exercises

It is always important to remember that risks cannot be eliminated entirely; we can only reduce their likelihood of occurring and minimise their impact.

Individual events are interlinked. Every major event encompasses the requirements for addressing the needs of lower-level events as well.

The classification of events sets out requirements for response and communication in line with the fulfilment of needs, so as to optimise the costs of ensuring the minimisation of the impacts of individual events and the swiftest possible resolution of their consequences.

[7] https://www.youtube.com/watch?v=jqQIqfE6iCM&ab_channel=BCONetwork

2.4.1 Minor incidents

Minor incidents include standard routine operations that usually require the intervention of a single component of the Integrated Rescue System. These operations are the most common and include emergency medical service call-outs to individual patients, minor road traffic accidents and small-scale fires.

Communication requirements: Primarily voice communication and basic text communication (at SMS level). No complex coordination between multiple units is required.

2.4.2 Medium-scale incidents

Medium-scale incidents require the coordination of two to three components of the Integrated Rescue System. These incidents are more complex and require a higher level of coordination and communication. Examples include more serious traffic accidents, larger fires, or incidents requiring the simultaneous assistance of the Police of the Czech Republic and the Fire and Rescue Service of the Czech Republic.

Communication requirements: Increased demands on the coordination of voice and data communication between the units involved. The need to transfer information between various control centres and units at the scene of the incident.

2.4.3 Major incidents

Major incidents involve complex situations requiring the intervention of several IZS units and may affect an entire region. These incidents include mass casualty accidents, large-scale natural disasters or terrorist attacks.

Communication requirements: Highly demanding communication involving the transmission of voice, data and video. Effective incident management requires fast and reliable communication between all participating units and control centres.

2.4.4 National incidents

National incidents have a nationwide impact and require coordination at the national level. These incidents may include pandemics or other national emergencies affecting a large proportion of the population and infrastructure.

Communication requirements: Intensive use of all available means of communication, including crisis management centres and backup communication systems. Coordination between different levels of government is essential.

2.4.5 International incidents

International incidents require international cooperation and coordination. These incidents may include natural disasters with cross-border impact or international terrorist attacks.

Communication needs: A comprehensive communications infrastructure enabling interoperability between different national PPDR systems. The need for rapid and effective communication between international teams.

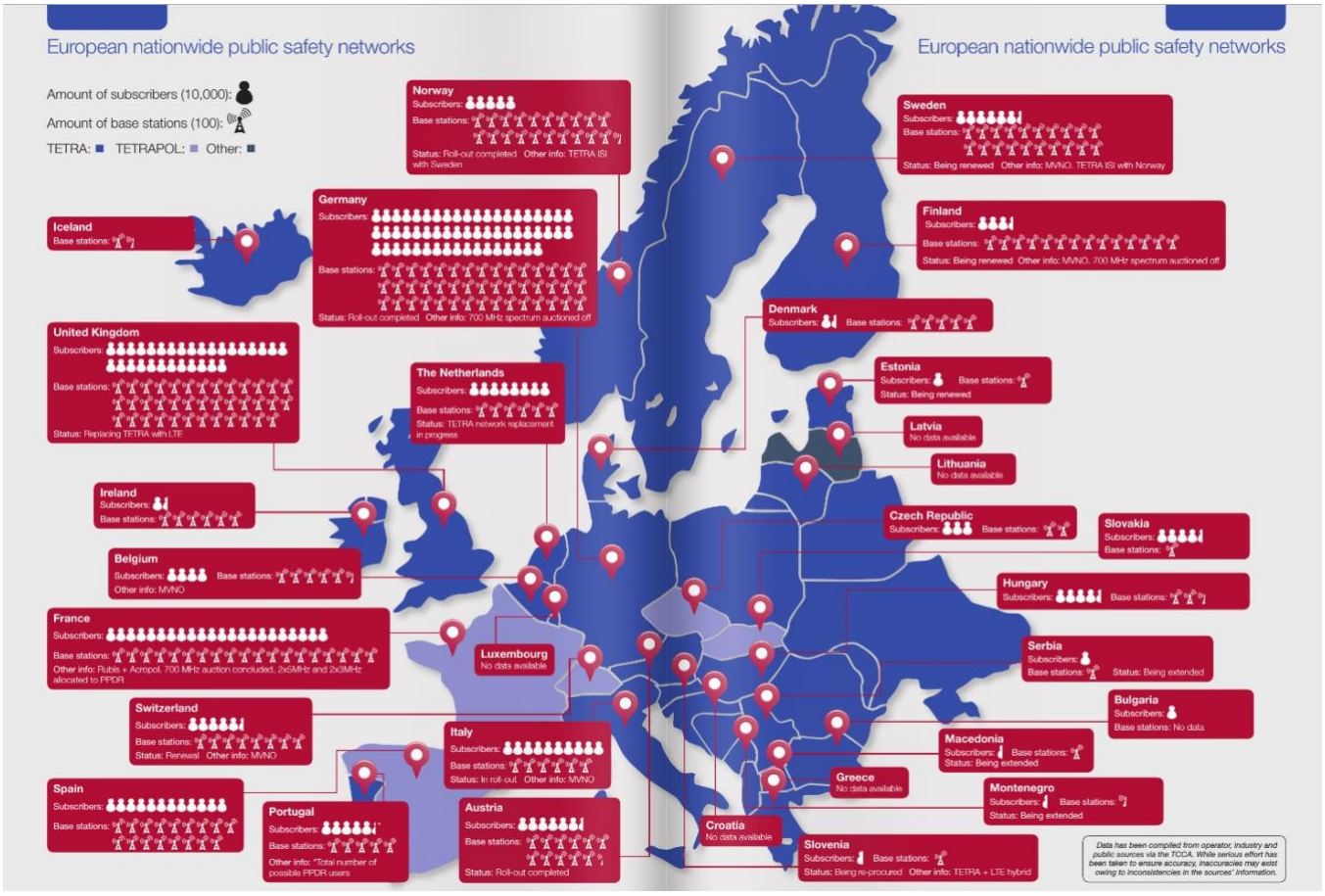
3 Definition of PPDR abroad

The integrated rescue system is a key element of crisis management, ensuring a coordinated response to emergencies, disasters and other crisis situations. Each country has its own emergency response system, tailored to its legislative, geographical and organisational conditions. These systems vary depending on local needs and available resources, with some placing greater emphasis on centralisation and unified management, whilst others prioritise regional cooperation and volunteering.

For each country, we focus on the organisational structure and a comparison with the Czech Republic. These aspects will enable us to better understand the differences and similarities between individual national emergency response systems and their capabilities to manage emergencies.

3.1 General

The map below illustrates the status of European nationwide public safety networks using TETRA technology as of 2017. TETRA networks are widely deployed across various European countries and support critical communications for emergency services. For example, in Norway and Sweden, these networks are fully implemented and include cooperation between these countries. Germany and the United Kingdom have some of the largest networks, with thousands of base stations and hundreds of thousands of users. The United Kingdom is transitioning to LTE technology. The Netherlands and France are also actively upgrading their TETRA networks to meet growing demands for critical communications. The map illustrates the widespread use of TETRA networks across Europe, highlights their importance for public safety, and shows plans for further improvements and integration with new technologies such as LTE.



The source of this map is TETRA Today magazine, issue 36, 2017.

The following table provides an overview of the spectrum allocated for public safety, the central agency responsible, and the broadband network operating model in each of the countries listed. The data in the table is from 2021 and was obtained from a study conducted by Capgemini. This table summarises the various approaches and operational models for national public safety broadband networks in different countries.

COUNTRY	DESCRIPTION	SPECTRUM ALLOCATED FOR PPDR	DEDICATED CENTRAL AGENCY	BROADBAND NETWORK OPERATING MODEL
AUSTRALIA	In 2019, the Australian government recognised the need for a mobile public safety broadband network for its emergency services. Pilot projects have been underway since 2018.	✓	✓ National administration to set guidelines	**Commercial model** It appears that the Australian government will opt for a commercial network with supplementary use of allocated spectrum for public safety
BELGIUM	Belgium has revised its public safety communications network strategy and plans to roll out a new nationwide mobile broadband network. Implementation is expected between 2023 and 2025.	✓	✓ ASTRID – operator	**Hybrid model (MCON)** Dedicated core network interconnected with the operator and a dedicated RAN. The network is operated and maintained by ASTRID
DUBAI	Dubai has established 'Nedaa', a government-owned network service provider dedicated to professional communications. Broadband services provided over LTE.	✓	✓ Neda – operator	**Dedicated model** Dedicated network (core and RAN) for public safety disciplines and other security and safety entities
FINLAND	Finland is developing VIRVE 2.0, the second generation of a public safety network based on LTE/5G technologies. Implementation is expected between 2023 and 2025.	✗ Subject to change in the future	✓ VIRVE – operator	**Hybrid model (MCON)** Dedicated core network interconnected with the operator and a dedicated RAN. The network is operated and maintained by VIRVE
FRANCE	France is modernising its public safety communications system with a centralised approach supporting broadband applications. Implementation expected between 2022 and 2025.	✓	✓ ACMOSS – operator	**Hybrid model (FMVNO)** Dedicated core network interconnected with the operator and the dedicated RANs of two operators, managed by a dedicated organisation
GERMANY	Germany currently operates a nationwide TETRA network for public safety communications. Pilot projects are being tested, but an official programme for a broadband network has not yet been announced.	✓	To be specified	To be confirmed
NETHERLANDS	The Netherlands operates a nationwide TETRA (C2000) network and plans to maintain it for some time. Mobile broadband services will be provided by commercial operators.	✓	✗	**Commercial model** Broadband services will be provided by commercial operators alongside the TETRA network
SINGAPORE	Singapore's emergency services use a dedicated but private network for their critical communications. The provider has gradually developed the provision of data services for public safety.	✓	✗	**Commercial model** Broadband services provided by a commercial operator specialising in professional communications
SOUTH KOREA	South Korea has launched the world's first mobile broadband network for its public safety, rail and maritime services. The PS-LTE network has been fully operational since 2018.	✓	✓ Safe-Net – operator	**Hybrid model (MCON)** Dedicated core network operated by Safe-Net, interconnected with the RANs of several operators

SWITZERLAND	Switzerland has a nationwide TETRA network for public safety (Polycom), but has begun testing for the development of a mobile broadband network for public safety. Current broadband services are provided only for non-critical applications.	To be confirmed, but likely yes	To be confirmed	To be confirmed
UNITED KINGDOM	The United Kingdom has begun developing a network for public safety agencies to replace the older TETRA network. Several issues have delayed implementation until 2024–2025.	✗	✗	**Commercial model** Broadband services will be provided by commercial operators
USA	The US has established a dedicated agency (FirstNet) which works with a national operator to roll out a public safety broadband network. The network has been operational since 2018 and is constantly being improved to meet public safety requirements.	✓	✓ FirstNet – oversight	**Hybrid model (MCON)** Dedicated network core connected to the operator's RAN, operator-controlled network

3.2 Definition of emergency services within the European Union

3.2.1 Germany

Germany has a federal emergency services system organised at the level of the individual federal states (Bundesländer). This system comprises professional and voluntary fire brigades, medical emergency services, the police and other organisations that cooperate in the provision of rescue and emergency services.

3.2.1.1 Organisational structure

Feuerwehr (Fire Service)

Professional and voluntary fire brigades, which are responsible for firefighting, rescue operations in the event of road traffic accidents, industrial accidents, natural disasters and other emergency situations.

Polizei (Police)

Provides public order and safety, and cooperates with fire and rescue services during evacuations and other operations.

Rettungsdienst (Ambulance Service)

Provides pre-hospital emergency medical care and the transport of patients to hospitals. Ambulance services are usually organised at a regional level and may be operated by various organisations, including the Red Cross, Johanniter-Unfall-Hilfe, Malteser Hilfsdienst and others.

Technisches Hilfswerk (THW)

The Federal Agency for Technical Relief, which provides technical support during disasters and emergencies.

Voluntary and humanitarian organisations

The German Red Cross, Johanniter-Unfall-Hilfe, Malteser Hilfsdienst, Arbeiter-Samariter-Bund and other organisations providing medical and humanitarian aid.

3.2.1.2 A comparison with the Czech Republic

Germany differs from the Czech Republic in several key respects regarding its emergency services system. The main difference lies in the organisational structure – whilst Germany has a federal system, where each federal state has its own legislation and

organisation of emergency services, the Czech Republic uses a centralised model. In Germany, each region can therefore tailor its emergency services to the specific needs of the local population, providing greater flexibility and faster responses at the local level. This approach is important given the size of Germany, which is several times larger than the Czech Republic.

Legislation in Germany varies by federal state, allowing for adaptation to local conditions and needs. This regional autonomy supports the effective management of emergency services. In contrast, the Czech Republic has uniform legislation across the whole country, ensuring consistent and unified management of emergency services at the national level.

The organisation of emergency services in Germany involves a significant proportion of volunteers and is managed at regional level. The federal agency Technisches Hilfswerk (THW) provides technical support during disasters. In the Czech Republic, the organisation is centralised, with regional branches of the Fire and Rescue Service of the Czech Republic responsible for coordinating and managing rescue operations at regional level.

Cooperation between the various units is important in both countries. In Germany, cooperation between fire brigades, the police, emergency services, the THW and voluntary organisations is organised at regional level, enabling a rapid and effective response to crisis situations. In the Czech Republic, strong cooperation between the Fire and Rescue Service, the police, the emergency medical service and other support agencies ensures an effective response to crisis situations. The centralised system in the Czech Republic promotes uniformity and consistency in nationwide coordination and ensures that all agencies can cooperate quickly and effectively in dealing with emergencies.

3.2.2 Belgium

The Belgian emergency response system is coordinated and operates at three levels: local, provincial and federal. This system includes the federal and local police, emergency medical services, professional fire brigades and civil protection. At the local level, emergency services are managed by local crisis centres, which provide the initial response to emergencies. The provincial level is activated during major crises that exceed the capacity of local centres and is managed by provincial crisis centres. The federal level is responsible for coordination during large-scale crises involving multiple provinces or requiring national intervention, and is managed by the National Crisis Centre

3.2.2.1 Organisational structure

The Belgian integrated emergency response system is divided into five main disciplines, each of which has a specific role in ensuring safety and responding to crisis situations. This system ensures coordinated and effective assistance to the population in various types of emergency situations.

Discipline 1: Pompiers (Fire Service)

The fire service in Belgium comprises both professional and volunteer firefighters. This branch is responsible for firefighting, technical interventions in road traffic accidents, industrial accidents, natural disasters and other emergency situations. Fire services have been reorganised into 34 safety zones to improve coordination and the effectiveness of operations. There are approximately 5,000 professional and 12,000 volunteer firefighters in Belgium.

Discipline 2: Aide médicale urgente (Emergency Medical Services)

Emergency medical services provide pre-hospital emergency care and transport patients to hospitals. These services include the 112 emergency call centre, ambulance services in Belgium, the SMUR system (mobile intensive care units) and air ambulance services.

Discipline 3: Police

The police in Belgium are divided into federal and local levels. The federal police focus on national and international security issues, whilst the local police ensure safety and public order at the local level. This also includes the traffic police and air support.

Discipline 4: Logistics

Logistics encompasses a wide range of support services that provide the necessary materials and technical support during various operations. This includes transport, supply, and technical maintenance essential for the effective functioning of other emergency services. Partner organisations include Elia, Electrabel, the Belgian Armed Forces and others.

Discipline 5: Information

This discipline covers communication and the dissemination of information during crisis situations. Authorities work with the media and other institutions to ensure the public is kept informed. Specialised communication centres are on standby to provide up-to-date and accurate information on crisis situations.

3.2.2.2 Comparison with the Czech Republic

The Belgian integrated rescue system and the Czech system differ in several key respects, primarily in their organisational structure and management approach.

The Belgian integrated rescue system is divided into five disciplines: fire service, emergency medical services, police, logistics and information. This multi-level system (local, provincial and federal levels) enables flexible and effective responses to crisis situations, with an emphasis on specific needs at the local level. The federal level, in turn, coordinates large-scale crises through the National Crisis Centre.

In the Czech Republic, the Integrated Rescue System is centralised, with regional units of the Fire and Rescue Service of the Czech Republic coordinating rescue operations at the regional level. This model ensures uniform management of rescue services across the whole country, with the General Directorate of the Fire and Rescue Service leading nationwide operations.

3.2.3 Finland

Finland, known for its high standards of safety and organisation, has a well-developed integrated rescue service system, which is an essential element in protecting people and property from various hazards. The Finnish rescue service is the cornerstone of ensuring the safety and protection of the population.

The Finnish integrated rescue service is decentralised and managed at regional level. Each region has its own rescue service, which is responsible for carrying out rescue operations and disaster prevention within its territory.

At national level, the activities of the emergency services are coordinated by the Finnish Safety Committee (Turvallisuuskomitea), which ensures that the activities of the emergency services are in line with national strategies and that optimal cooperation is achieved between different regions and services.

3.2.3.1 Organisational structure

Firefighters and rescue workers

Finnish fire brigades comprise both professional and volunteer firefighters, who are divided into 21 rescue regions. These brigades are responsible for firefighting, rescue operations in the event of traffic accidents, natural disasters, industrial accidents and other emergency situations. Regional fire services operate with a high degree of autonomy, which enables an effective response to local needs. In addition to operational interventions, firefighters also engage in preventive activities, such as safety inspections and public education.

Police

The Finnish police ensure the maintenance of public order and safety, working closely with the fire service and emergency medical services during evacuations and other operations. The police are divided into regional units, which are responsible for responding to local incidents, managing traffic during emergencies and ensuring safety at incident sites.

Emergency medical services

Emergency medical services provide pre-hospital emergency care and transport patients to hospitals. These services are integrated into regional emergency response areas and are crucial in responding to medical emergencies, such as road traffic accidents or sudden medical complications. Rescue teams are equipped with modern medical technology and provide a high standard of care.

Maritime rescue services

Maritime rescue services are a specialised component of the Finnish emergency services, ensuring safety at sea and providing assistance in the event of maritime accidents and disasters. Given Finland’s extensive coastline and numerous waterways, this component is essential for ensuring a rapid and effective response to incidents at sea and in coastal areas. The Maritime Rescue Services are equipped with modern vessels and technology for various types of rescue operations at sea.

Volunteer and humanitarian organisations

Volunteer and humanitarian organisations, such as the Finnish Red Cross, play a supporting role within the Finnish emergency services. These organisations provide assistance in rescue operations, first aid and the distribution of humanitarian aid, and are also actively involved in preventive activities and public education. Volunteer teams often cooperate with professional emergency services in managing large-scale emergencies and disasters.

3.2.3.2 Comparison with the Czech Republic

The Finnish rescue system is characterised by its decentralised structure, which places great emphasis on regional autonomy and prevention. Each of Finland's 21 rescue regions enjoys a high degree of autonomy in the management and execution of rescue operations, enabling an effective and rapid response to local needs and risks. This approach supports preventive measures such as regular inspections, educational campaigns and active public involvement in prevention and emergency preparedness.

In contrast, the Czech Integrated Rescue System (IZS) is more centralised, with significant coordination at national level through the Fire and Rescue Service of the Czech Republic (HZS ČR). The Czech system emphasises centralised planning and coordination, which enables a uniform and consistent approach to rescue operations across the country.

One of the differences between these two systems is the presence of maritime rescue services in Finland. Finland, with its extensive coastline and numerous waterways, must have effective and well-equipped maritime rescue services to ensure safety at sea and provide assistance in the event of maritime accidents and disasters. These services are essential for ensuring the protection of both inland waterways and the Baltic Sea.

3.2.4 Norway

Norway's integrated rescue system, known as the Norwegian Search and Rescue Service (SAR), comprises a range of rescue services for sea, land and air. This system is coordinated through two main centres – Joint Rescue Coordination Centres (JRCCs) – located in Bodø and Stavanger. These coordination centres are under the authority of the Ministry of Justice and Public Security.

The Norwegian SAR Service is organised to involve cooperation between government agencies, voluntary organisations and private companies. Together, these components provide rescue services throughout the country. In addition to the two main coordination centres, there are also 28 regional rescue centres that handle responses to local incidents.

3.2.4.1 Organisational structure

Police

The Norwegian Police play a key role in the rescue system, particularly in coordinating rescue operations on land and in cases involving missing persons. The police are divided into 12 districts, each with its own operations centre that manages and coordinates operations.

Fire Service

Fire services in Norway are provided through more than 300 fire stations, most of which are staffed by volunteer firefighters. In total, there are around 12,500 firefighters, of whom only approximately 3,500 are full-time professional firefighters. The fire service is responsible for fire protection and emergency response, including chemical and biological threats.

Emergency medical services

Emergency medical services include both ground and air ambulances. Norway has an extensive network of ambulances and air rescue crews capable of responding rapidly to medical emergencies. The air rescue service treats up to 20,000 patients annually and comprises 14 helicopters stationed across the country.

Air and sea rescue

Air and sea rescue is a key component of the Norwegian SAR system. This also includes the use of specially equipped helicopters, such as the Sea King, which are deployed for rescue operations at sea and in the mountains. Norway also has an extensive coastguard service, which is on standby 24/7.

3.2.4.2 Comparison with the Czech Republic

Both systems are tasked with coordinating the various components of the rescue and security forces to provide effective and rapid assistance in emergency situations. The main components in both countries include the ambulance service, the fire and rescue service, the police and civil defence.

In Norway, the Norwegian Search and Rescue Service (SAR) is coordinated through two main centres, the Joint Rescue Coordination Centres (JRCC), located in Bodø and Stavanger. These coordination centres are under the authority of the Ministry of Justice and Public Security. In the Czech Republic, the Integrated Rescue System is coordinated by the Ministry of the Interior and comprises a central coordination centre and regional coordination centres.

In Norway, coordination takes place at national, regional and local levels. Domestic SAR operations are delegated to one of 28 regional rescue sub-centres, which handle local responses. In the Czech Republic, coordination also takes place at national and regional levels, where regional coordination centres play a key role in regional coordination, whilst the local level is managed directly through local IZS units.

The Norwegian SAR system is governed by various legal provisions and royal decrees, which set out the responsibilities and tasks of the individual units. In the Czech Republic, the legal framework is established by Act No. 239/2000 Coll., on the Integrated Rescue System, which defines the functioning and structure of the IZS.

In Norway, military units may be called upon to support civilian rescue operations during major disasters or emergencies. In the Czech Republic, military units are involved in a similar manner, but their deployment is usually limited to specific situations where specialised capabilities or resources are required.

All government agencies involved in SAR operations in Norway cover their costs from their regular budgets. Commercial enterprises are paid at standard market rates and voluntary organisations are reimbursed for direct expenses. In the Czech Republic, the costs of IZS operations are covered by the state budget and other sources of funding in accordance with the Act on the Integrated Rescue System.

3.2.5 Hungary

In Hungary, the equivalent of the Czech Integrated Rescue System is called the Nemzeti Veszélyhelyzet-kezelési Rendszer (NVKR), which means the National Emergency Management System. This system comprises various rescue and security services that cooperate in dealing with emergencies and disasters. The NVKR is coordinated primarily through the Katasztrófavédelmi Koordinációs Kormánybizottság (KKB), i.e. the Coordination Committee for Disaster Protection, which is headed by the Minister of the Interior.

3.2.5.1 Organisational structure

Hungarian Medical Emergency Service

The Hungarian Medical Rescue Service provides rapid medical assistance and the transport of patients to healthcare facilities. This organisation operates ambulances equipped with modern medical devices, enabling first aid to be administered directly at the scene of an incident. In addition to the ground ambulance service, it also operates an air ambulance service capable of rapidly transporting patients over longer distances, particularly in hard-to-reach areas or in critical situations requiring urgent medical intervention.

Fire and Rescue Service

The Fire and Rescue Service is responsible for fighting fires and carrying out rescue operations during road traffic accidents, natural disasters and other emergency situations. This service is equipped with state-of-the-art technology and trained personnel who are ready to respond to any emergency. In addition to firefighting, it provides technical assistance during accidents and disasters, such as hazardous substance leaks or building collapses. The Fire and Rescue Service also cooperates with other branches of the NVKR and ensures the protection of property and the environment.

Police

The police maintain public order and safety. Their main tasks include preventing and combating crime, traffic control and ensuring security measures at public events. The police are equipped with modern technology and have specialised units at their disposal, such as criminal investigators, riot police and traffic police. They cooperate with other branches of the NVKR and ensure a rapid response to crisis situations.

Civil Protection

Civil Protection coordinates rescue operations during natural disasters and chemical, biological, radiological and nuclear threats. Its role also includes providing information and support to the public during emergencies. Civil Protection focuses on the preparation and implementation of evacuation plans, training the public in first aid and safety measures, and cooperates with the media to disseminate important information during crisis situations. The organisation also maintains emergency stocks and ensures the rapid distribution of necessary supplies in the event of an emergency.

Military units

Military units may be called upon to support civil rescue operations during major disasters or emergencies. The army provides logistical support, specialists and equipment necessary for managing large-scale crisis situations. Military units are ready to intervene if necessary, and their deployment is coordinated with other components of the NVKR. Military units also ensure the protection of critical infrastructure and can provide humanitarian aid at both national and international levels.

3.2.5.2 Comparison with the Czech Republic

A comparison of the integrated rescue systems in Hungary and the Czech Republic reveals several common features, but also significant differences in their organisation and operation.

Both systems are designed to coordinate the various components of the emergency and security services in order to provide effective and rapid assistance in emergency situations. The main components in both countries include the ambulance service, the fire and rescue service, the police and civil protection. In both countries, emphasis is placed on cooperation between these units, which are coordinated through a central governing body. In Hungary, this is the Katasztrófavédelmi Koordinációs Kormánybizottság (KKB), whilst in the Czech Republic it is the Integrated Rescue System under the Ministry of the Interior.

In Hungary, the NVKR is coordinated through the KKB, which is headed by the Minister of the Interior and comprises senior representatives from various ministries and national organisations. In contrast, in the Czech Republic, the IZS is coordinated by the Ministry of the Interior and comprises a central coordination centre and regional coordination centres.

Coordination in Hungary takes place at national, regional and local levels. The KKB ensures nationwide coordination, whilst regional operational bodies operate at the regional level and local defence committees at the local level. In the Czech Republic, coordination also takes place at national and regional levels.

The Hungarian civil protection system is governed by the Act on Disaster Prevention, which sets out the tasks and responsibilities of the individual components and the coordinating body. In the Czech Republic, the legal framework is established by Act No. 239/2000 Coll., on the Integrated Rescue System, which defines the functioning and structure of the IZS.

In Hungary, military units may be called upon to support civilian rescue operations during major disasters or emergencies. In the Czech Republic, military units are involved in a similar manner, but their deployment is usually limited to specific situations where specialised capabilities or resources are required.

3.3 Definitions outside the EU

3.3.1 South Korea

The South Korean integrated rescue system, known as the Korean Disaster and Safety Management System, is administered by the Ministry of the Interior and Safety (MOIS). This system encompasses various rescue and safety units that cooperate in addressing emergencies and disasters, and is designed to ensure a rapid and effective response to various types of threats.

3.3.1.1 Organisational structure

Ministry of the Interior and Safety (MOIS)

The Ministry of the Interior and Safety (MOIS), through its Disaster and Safety Management Department (DSMD), oversees the coordination of disaster and safety tasks carried out by central and local governments. Every five years, the DSMD compiles the National Basic Safety Plan, which sets the overall direction of government safety policies. Based on this plan, the relevant ministries prepare annual action plans.

The MOIS also provides ongoing education and training for members of the emergency services, regularly evaluates operational plans and, based on these evaluations, adjusts strategies to enhance their effectiveness. Other tasks include analysing and reviewing budgets for disaster and security-related projects, ensuring safety standards are met, and organising public safety campaigns.

National Fire Agency (NFA)

The NFA is the main body responsible for fire prevention, firefighting, rescue and the provision of first aid. The NFA also oversees the National 119 Emergency Services Headquarters, which specialises in large-scale rescue operations. Under the supervision of the NFA, municipal and provincial fire headquarters operate, coordinating local fire stations and academies. This structure ensures that fire services are accessible and effectively managed at all levels.

Emergency Medical Service

The emergency medical service comprises an extensive network of ambulances and paramedics capable of responding rapidly to medical emergencies. This service is closely integrated with other components of the emergency response system to ensure a coordinated and effective response to various incidents. Medical teams are equipped with modern technology and trained staff, enabling them to provide a high standard of care at the scene.

Coastguard and Maritime Rescue Service

The Coast Guard is a key component of rescue operations at sea. It is responsible for search and rescue, responding to maritime accidents and protecting coastal areas. The Coast Guard utilises specialised equipment and technology to carry out rescue operations effectively in a maritime environment.

Central Disaster and Safety Countermeasures Headquarters

In the event of a major disaster, the Central Disaster and Safety Countermeasures Headquarters is convened to oversee the coordination of the response and recovery. This headquarters comprises representatives from various organisations and serves as the main command centre for coordinating all rescue and recovery activities. The Headquarters works with local authorities and other relevant agencies to ensure a swift and effective response to emergency situations.

3.3.1.2 Comparison with the Czech Republic

In South Korea, the system is known as the Korean Disaster and Safety Management System and is managed by the Ministry of the Interior and Safety (MOIS). This system comprises various components that collaborate via the Integrated Disaster and Safety Information System (IDSIS), which supports communication and cooperation between government agencies at all levels. In the Czech Republic, the system is known as the IZS and is coordinated by the Ministry of the Interior. This system comprises a central coordination centre and regional coordination centres, which play a key role in regional coordination.

In South Korea, coordination takes place at national, regional and local levels, with the Central Disaster and Safety Countermeasures Headquarters playing a key role. This headquarters is convened during major disasters and comprises representatives from various organisations who oversee the response and recovery. In the Czech Republic, coordination also takes place at national and regional levels.

The South Korean system is characterised by the extensive use of modern technologies, such as big data and artificial intelligence, to improve risk management and disaster response.

The Czech system focuses on broad international cooperation within the EU and the Visegrad Group, particularly in the areas of joint exercises and information exchange.

Funding and training are provided from state budgets in both countries, although in South Korea, commercial enterprises and voluntary organisations are reimbursed for direct expenses related to rescue operations. In the Czech Republic, the costs of IZS operations are covered by the state budget and other sources of funding.

4 Legislation and regulation in the field of civil protection

4.1 Legislation and regulation for the Czech Republic

4.1.1 Auction commitment

In March 2020, the Czech Telecommunications Office (ČTÚ) announced an auction of frequencies in the 700 MHz and 3400–3600 MHz bands. The aim of this auction was to support the development of 5G networks in the Czech Republic and to ensure the provision of specific services for public safety and emergency communications.

The auction set out obligations for commercial mobile operators to provide access to national roaming services and priority broadband services for PPDR. Auction participants had to meet coverage and service quality requirements, which are crucial for the effective operation of the Integrated Rescue System (IRS).

The aim of the auction was to create conditions for the efficient use of radio frequencies and to support several key areas. The main objectives included:

Promoting competition in the field of electronic communications services. Ensuring

the efficient use of radio frequencies for the benefit of end-users.

Developing new electronic communications services via wireless high-speed networks.

Creating conditions for technological innovation in electronic communications networks and services, particularly with regard to the future development of 5G networks and the services provided over them.

Another important objective was to support future solutions for public safety and emergency communications in accordance with Government Resolution No. 293 of 16 May 2018.

4.1.1.1 Conditions

Purpose of the PPDR commitments:

To ensure mobile emergency communications for PPDR units.

Communication via a non-public mobile electronic communications network for the purposes of emergency communications.

Priority BB-PPDR commitment:

Scope of the Priority BB-PPDR commitment:

– The allocation holder must provide an authorised PPDR applicant with access to the network operated using radio frequencies in the 700 MHz band.

– Access must include interoperability with the core of the eligible PPDR applicant's BB-PPDR network and support for traffic management by the eligible PPDR applicant.

– Access may be extended to networks in the 800 MHz band, provided that the compatibility of the eligible PPDR applicant's terminal equipment is not restricted.

Scope of Priority BB-PPDR services:

– Broadband data services for mobile emergency communications and voice services provided via a broadband connection.

– Specific services include:

– “Push to Talk” services for emergency response (Mission Critical Push to Talk – MCPTT)

- Video transmission for emergency response (Mission Critical Video – MCV)
- Data transmission for emergency response (Mission Critical Data – MCD)
- MCX (Mission Critical Common Functionalities), including provision of eMBMS (evolved Multimedia Broadcast Multicast Services)
- IOPS (Isolated E-UTRAN Operation for Public Safety)
- QPP (QoS, priority, pre-emption, access-class barring) and eMPS (enhanced Multimedia Priority Service)
- LCS (Location-Based Services)
- PWS (Public Warning System) utilising CBS (Cell Broadcast Service)
- Higher transmission power HPUE (High Power User Equipment)
- Direct mode communication ProSe (Proximity Services)

Priority traffic:

- Services for users specified by an authorised PPDR applicant must always take precedence over commercial services provided by other users.
- In the event of different priority levels, the priority level of services must be determined in accordance with the authorised applicant's specifications.

National Roaming Obligation for PPDR:

- Content of the National Roaming Obligation for PPDR:
  - The allocation holder must provide the authorised PPDR applicant with access to public communications networks in the 700 MHz and 800 MHz bands.
  - Access must be of the 'Full-MVNO' type with an architectural roaming model featuring an S8 interface and Home Routed Roaming as defined in the 3GPP/ETSI technical specification.
- Scope and quality of services:
  - Access to the networks must be without territorial or quality restrictions.
  - The scope, quality and composition of services provided to an authorised PPDR applicant must not be inferior to those provided to commercial users based on 4G and 5G technologies.
- Conditions of validity:
  - The national roaming obligation for PPDR does not apply for the period during which the allocation holder provides Priority BB-PPDR.

4.1.1.2 Auction results

The results of the auction in the 700 MHz frequency band are as follows:

Frequency band	Size	Holder	Valid until
703–713 / 758–768 MHz	2×10 MHz	O2 Czech Republic a.s.	1.190 billion
713–723 / 768–778 MHz	2×10 MHz	T-Mobile Czech Republic a.s.	1.400 billion
723–733 / 778–788 MHz	2×10 MHz	Vodafone Czech Republic a.s.	1.400 billion

4.1.2 Spectrum allocation

The Czech Telecommunications Office (ČTÚ) has allocated specific frequencies in several bands for PPDR (Public Protection and Disaster Relief) purposes. These frequencies are intended to ensure high-quality and reliable communication for the components of the integrated rescue system, which are key to public safety and emergency communications.

The reserved spectrum has the following characteristics:

700 MHz band: Reserved primarily for PPDR broadband services, which include data and voice communications, video transmissions and other specific services such as Mission Critical Push to Talk (MCPTT), Mission Critical Video (MCV) and Mission Critical Data (MCD). This band is key to the roll-out of modern 5G technologies, which enable high-speed data transmission and reliable communication even in emergency situations.

800 MHz band: Serves as a supplement to provide PPDR broadband services and supports interoperability and coverage expansion where required. The use of this band ensures robust coverage and support for both voice and data communications across the country.

400 MHz band: Provides narrowband services for voice communication and certain data transmissions, used primarily in the PEGAS network, based on Tetrapol technology. This band is crucial for existing technologies and infrastructure solutions for emergency communications. It enables stable and reliable voice communication between emergency services.

450 MHz band: This can be used for broadband PPDR services, providing high-speed data and voice services. It offers sufficient coverage and is suitable for long-distance communication, making it ideal for use in less densely populated areas. This band is also being considered for the future expansion of PPDR services, which require higher data transmission capacity.

The data rate will depend on the number of users and the minimum capacity required to manage the connection. Assuming a full 5 MHz block, LTE can achieve speeds of up to 150/75 (upstream) Mbps per sector, according to ETSI peak performance 8.1.1. This corresponds to 30 bps/Hz for the downlink and 15 bps/Hz for the uplink. From this, we deduce that there will be approximately 10 communication channels with a capacity of approximately 6.5 MHz[8] .

160 MHz band: Traditionally used for analogue communications by emergency services, it primarily covers communications by the Fire and Rescue Service and the Police of the Czech Republic. This band is vital for basic voice communications in emergency situations and provides a reliable platform for immediate communication.

Other bands: Other frequency bands may also be used for PPDR services, for example in the 3.5 GHz range for specific high-speed data transmissions, which can support advanced services and applications within the emergency services.

The obligations set out in the auction primarily relate to frequencies in the 700 MHz band. Other services and frequencies, such as the 400 MHz, 450 MHz and 160 MHz bands, are frequently used within existing technologies and infrastructure solutions. For example, the PEGAS network, based on Tetrapol technology, utilises the 400 MHz band for its operations and provides narrowband voice and data services for emergency services.

4.1.2.1 Justification for the request to use the radio spectrum

Ideal radio spectrum range for use in the 700 MHz band – 2x13 MHz and 2x5 MHz reserve

Option A – 703–733 MHz (uplink) / 758–788 MHz (downlink) – 2x10 MHz

- Purpose – a nationwide radio access network for emergency communications.
- It addresses current and future capacity requirements for emergency communications, covering both broadband data services and narrowband voice services.
- Globally standardised band (3GPP Band 28).
- Large market for infrastructure and end devices = economies of scale, avoidance of vendor lock-in, international harmonisation and interoperability, standardised solutions, long-term prospects for operation and development.
- The only available section of suitable radio spectrum that can be utilised for the needs of security and emergency services by 2030 – the state (CTU) has no alternative.

Option D – 733–736 MHz (uplink) / 788–791 MHz (downlink) – 2.3 MHz

- Purpose – specific services, scenarios and means of communication – services for close-range communication (i.e. line-of-sight communication), autonomous systems (e.g. IoT), isolated tactical deployment systems, communication with airborne assets, etc.
- Enables the operation of the above-mentioned specific services and scenarios without capacity impacts on the wide-area radio access network (Option A, 2x10 MHz) and eliminates mutual interference.
- A globally standardised band (3GPP Band 28) but with restrictions arising from its location within a protected band.

Option C – 698–703 MHz (uplink) / 753–758 MHz (downlink) – 2x5 MHz

- Purpose – reserve until 2028 – usable only once technical limitations have been resolved (minority standardised band, 3GPP Band 68).

Option B – combination of Option C and Option D – 2x8 MHz

Justification for the use of radio spectrum in a range of at least 2x10 MHz

[8] https://www.etsi.org/deliver/etsi_tr/136900_136999/136913/12.00.00_60/tr_136913v120000p.pdf)

Today's operational and tactical procedures used by emergency services are primarily dependent on voice services. The effectiveness and safety of emergency services can be enhanced by providing them with a new information dimension to support their decision-making. This can only be achieved provided that secure high-speed data services are available. The benefits of having these services available are clear – they will create the conditions for the deployment and development of a wide range of applications to support the operations of emergency services, just as they have become an indispensable part of everyday civilian life. This primarily involves providing detailed information to emergency services on the ground (e.g. visual information from the incident scene prior to arrival; advanced navigation; the use of biometric elements for checking, identifying and registering individuals) or the transmission of detailed information from the scene of an incident to remote control centres (e.g. real-time video transmission), which are key to enhancing the efficiency and safety of the operations carried out by the services during an incident.

The communication needs of security and emergency services are virtually constant over time. They need to transmit or receive the information necessary for decision-making at any given moment. Whilst this information is currently verbal in nature, there is a growing demand for additional information sources, particularly relating to the exchange of situational information, both before and during
and after an operation, as well as during the routine daily activities of the relevant services. This primarily involves the rapid availability of accurate information without distortion (particularly in the form of video and photographs). Already today, for example, the Czech Police make extensive use of high-speed data services enabling rapid background checks (the Czech Police's secure mobile platform). Another method of gathering information involves the widespread use of smart devices, sensors and, above all, applications that collect the necessary data and transmit processed information inputs to the relevant agencies. The outlook for the future therefore anticipates the significant integration of technologies for the collection, analysis and distribution of information to individual agencies.

This follows from the analysed needs of security and rescue services for mobile communications (in particular CEPT ECC Report 199 and others, see below), where the introduction of broadband data services is crucial.

- The minimum bandwidth of 2x10 MHz covers the introduction of broadband data services; it does not cover existing narrowband voice services and specific scenarios (AGA, DMO, mobile/autonomous/tactical systems, M2M, IoT, etc.)
  - Calculations for the migration of narrowband voice services to the BB-PDPR system result in a requirement for additional radio spectrum in the range of 2x3.2 MHz
  - For the other specific scenarios mentioned, there is currently no standardised solution and their implementation may vary significantly; the location and extent of the radio spectrum depend on specific user scenarios and requirements (DMO requires MHz-level allocations, AGA assumes tens of MHz, mobile/autonomous/tactical systems assume higher units up to tens of MHz, m2m and IoT assume MHz units) – the need for additional radio spectrum (hence the Strategy's requirement for 2x18 MHz and cooperation with operators, as well as other proposed mechanisms for the dynamic release of radio spectrum).
- Approximations of estimates according to the CEPT ECC Report 199 methodology for conditions in the Czech Republic form part of the reserved material of the Strategy for Mobile Communications of Security and Rescue Services:
  - new communication services – Chapter 2.2 (27),
  - current communication services – 2.3 (31),
  - state of technological standardisation – 2.4 (42),
  - radio spectrum suitable for PPDR – 2.5. (52),
  - required capacities for various PPDR activities and operations – 2.5.2.4 (57).
- Even now, therefore, the requirement of the Mobile Communications Strategy for Security and Rescue Services regarding the required radio spectrum is a compromise – it assumes the use of 2x10 MHz for both the introduction of broadband data services and existing narrowband voice services.

CEPT ECC Report 199 – key calculations for model scenarios:

- Further materials provide calculations of a similar, if not greater, scope of radio spectrum requirements according to national needs.
- Scenarios:
  - PP1: road accident or road check – routine operational event
    - Peak traffic 'generated' by a single event under the PP1 scenario (i.e. 1 incident) corresponds to 1300/1300 Kbps:
    - key information for calculating the required radio spectrum is therefore a description of the operational event, including the communication means used, cell size, number of concurrent operational events within the cell, location of the event within the cell, spectral efficiency, link budget and others,
  - PP2: the royal wedding (a planned large-scale event) or the 2011 London riots (an unplanned large-scale event),
  - DR: disaster scenario (e.g. flood).

– PP1 scenario

  - Uplink

Frequency band	Traffic assumption	Low estimate	Medium estimate
420 MHz	1 incident "cell edge" 3 incidents near cell centre and background communications	8.0 MHz	12.5 MHz
750 MHz	1 incident "cell edge" 2 incidents near centre and background communications	7.1 MHz	10.7 MHz

  - Downlink

Frequency band	Traffic assumptions	Low estimate	Medium estimate
420 MHz	1 incident "cell edge" 3 incidents near centre with background communications	7.6 MHz	10.5 MHz
750 MHz	1 incident "cell edge" 2 incidents near centre with background communications	6.9 MHz	9.0 MHz

– PP2 scenario

  - Royal wedding – uplink

Frequency band	Traffic assumption	Less stringent case	Worst case
Independent of frequency band	PP2 traffic scenario with background communications	10.3 MHz	14.3 MHz

  - London riots – uplink

Frequency band	Traffic assumption	Less stringent case	Worst case
Independent of frequency band	PP2 traffic scenario with background communications	5.8 MHz	7.8 MHz

– DR scenario – corresponds to the PP2 scenario, but occurs over a larger area (more cells).

The radio spectrum range must therefore cover a wide range of operational scenarios; it is clear from the above that even a radio spectrum range of 2x10 MHz is insufficient in certain situations, and additional transmission capacity must be provided for such situations.

– References to capacity requirements – CORE OF THE ARGUMENT:

– CEPT ECC Report 199

– LEWP-RCEG matrix and LEWP-RCEG matrix (xls)

– ETSI TR 102 628, in particular Chapters 8, A.5, F.4, F.5

– ITU-R Radiocommunication objectives and requirements for PPDR, in particular Annex 7

– WIK PPDR Spectrum Harmonisation in Germany, Europe and Globally

– NPSTC Public Safety Communications Assessment 2012–2022, Technology,

– Operations, and Spectrum Roadmap, in particular Chapters 1.3 and 3.8.3

– DRDC CSS 700 MHz Spectrum Requirements for Canadian Public Safety Interoperable Mobile Broadband Data Communications, in particular Chapters 5.1, 5.2.3 and the conclusion

– APT, Report 38 on technical requirements for mission-critical broadband PPDR communications, in particular Attachment 2 and Example 2

– Andrew Seybold, Public Safety Broadband Real World Testing Results

– Radio Spectrum Management Strategy (CTU), in particular Chapter 6.4.7

– Analysis Mason, 'Report for the TETRA Association: Public safety mobile broadband and spectrum needs', in particular Chapter C.2a

– Motorola, Barricaded suspect incident analysis

4.1.2.2 Why not just Option B (non-contiguous 2x8 MHz)?

The reasons are set out in the restricted material of the Strategy for Mobile Communications for Security and Emergency Services, specifically Chapter 2.5.2.3, and in the unrestricted summary of the Strategy, specifically Chapter 2.4.1.3. These include, in particular:

- **Unsuitability for the construction of a nationwide network** (functional, capacity, financial, operational), which is primarily due to the use of protection zones with significant regulatory restrictions, a niche market for equipment and technologies enabling economies of scale, and the use of off-the-shelf products (COTS):
  - insufficient bandwidth – failure to meet user requirements for capacity and transmission speeds,
  - risk of 'vendor lock-in' – in the area of terminals and LTE/5G technology,
  - negative economic impacts – higher prices for terminals and technologies, and higher operating costs associated with the operation of modified standard technology.

Frequency bands are currently not viable on their own (without allocation under Option A), primarily due to the negligible size of the commercial market for end-user devices – at present, no country has implemented such an allocation for the purposes of routine crisis and non-crisis communications (France is piloting and planning only isolated tactical systems):

- all end-user equipment would be made to order (analogous to the U:fon operator or TETRAPOL technology) – limited and insufficient portfolio, high prices (estimated +30% for technology, +30% for operating costs and +50–100% for terminals), risk of vendor lock-in, uncertainty regarding long-term sustainability,
- individual countries with this allocation are currently considering how to utilise this band, or rather how to ensure sufficient capacity – this will generally involve supplementary solutions for the implementation of tactical systems, see e.g. France, Germany.

Specific (stricter) European requirements for the 3GPP Band 68 (covering Option C) are set to prevent interference with digital terrestrial television (DTT) broadcasting. These stricter requirements mean that there is currently no confirmation from major chipset manufacturers that they will develop this variant at all.

- Option C is a stopgap solution artificially removed from the DTT guard band. This poses a significant risk of reverse interference, i.e. interference from DTT transmitters, and thus a reduction in the reliability or capacity of the communication network in the vicinity of DTT transmitters

4.1.2.3 Assessment of the suitability of individual frequency bands for the implementation of the BB-PPDR system

Theoretical data rates for the 400 and 700 MHz bands

Band	Frequency	Bandwidth	DL modulation	UL modulation	MIMO	DL data rate	UL data rate
B72	450 MHz	1.4 MHz	16QAM	QPSK	1x1 SISO	3 Mbps	1.5 Mbps
B72	450 MHz	1.4 MHz	16QAM	QPSK	2x2 MIMO	6 Mbps	1.5 Mbps
B72	450 MHz	1.4 MHz	16QAM	16QAM	1x1 SISO	3 Mbps	3 Mbps
B72	450 MHz	1.4 MHz	16QAM	16QAM	2x2 MIMO	6 Mbps	3 Mbps
B72	450 MHz	1.4 MHz	64QAM	64QAM	1x1 SISO	4.5 Mbps	4.5 Mbps
B72	450 MHz	1.4 MHz	64QAM	64QAM	2x2 MIMO	9 Mbps	4.5 Mbps
B72	450 MHz	3 MHz	16QAM	QPSK	1x1 SISO	7.5 Mbps	3.75 Mbps
B72	450 MHz	3 MHz	16QAM	QPSK	2x2 MIMO	15 Mbps	3.75 Mbps
B72	450 MHz	3 MHz	16QAM	16QAM	1x1 SISO	7.5 Mbps	7.5 Mbps
B72	450 MHz	3 MHz	16QAM	16QAM	2x2 MIMO	15 Mbps	7.5 Mbps
B72	450 MHz	3 MHz	64QAM	64QAM	1x1 SISO	11.25 Mbps	11.25 Mbps
B72	450 MHz	3 MHz	64QAM	64QAM	2x2 MIMO	22.5 Mbps	11.25 Mbps
B72	450 MHz	5 MHz	16QAM	QPSK	1x1 SISO	12.5 Mbps	6.25 Mbps
B72	450 MHz	5 MHz	16QAM	QPSK	2x2 MIMO	25 Mbps	6.25 Mbps
B72	450 MHz	5 MHz	16QAM	16QAM	1x1 SISO	12.5 Mbps	12.5 Mbps
B72	450 MHz	5 MHz	16QAM	16QAM	2x2 MIMO	25 Mbps	12.5 Mbps
B72	450 MHz	5 MHz	64QAM	64QAM	1x1 SISO	18.75 Mbps	18.75 Mbps

B72	450 MHz	5 MHz	64QAM	64QAM	2x2 MIMO	37.5 Mbps	18.75 Mbps
B28	700 MHz	3 MHz	16QAM	QPSK	1x1 SISO	7.5 Mbps	3.75 Mbps
B28	700 MHz	3 MHz	16QAM	QPSK	2x2 MIMO	15 Mbps	3.75 Mbps
B28	700 MHz	3 MHz	16QAM	QPSK	4x4 MIMO	30 Mbps	3.75 Mbps
B28	700 MHz	3 MHz	16QAM	16QAM	1x1 SISO	7.5 Mbps	7.5 Mbps
B28	700 MHz	3 MHz	16QAM	16QAM	2x2 MIMO	15 Mbps	7.5 Mbps
B28	700 MHz	3 MHz	16QAM	16QAM	4x4 MIMO	30 Mbps	7.5 Mbps
B28	700 MHz	3 MHz	64QAM	64QAM	1x1 SISO	11.25 Mbps	11.25 Mbps
B28	700 MHz	3 MHz	64QAM	64QAM	2x2 MIMO	22.5 Mbps	11.25 Mbps
B28	700 MHz	3 MHz	64QAM	64QAM	4x4 MIMO	45 Mbps	11.25 Mbps
B28	700 MHz	5 MHz	16QAM	QPSK	1x1 SISO	12.5 Mbps	6.25 Mbps
B28	700 MHz	5 MHz	16QAM	QPSK	2x2 MIMO	25 Mbps	6.25 Mbps
B28	700 MHz	5 MHz	16QAM	QPSK	4x4 MIMO	50 Mbps	6.25 Mbps
B28	700 MHz	5 MHz	16QAM	16QAM	1x1 SISO	12.5 Mbps	12.5 Mbps
B28	700 MHz	5 MHz	16QAM	16QAM	2x2 MIMO	25 Mbps	12.5 Mbps
B28	700 MHz	5 MHz	16QAM	16QAM	4x4 MIMO	50 Mbps	12.5 Mbps
B28	700 MHz	5 MHz	64QAM	64QAM	1x1 SISO	18.75 Mbps	18.75 Mbps
B28	700 MHz	5 MHz	64QAM	64QAM	2x2 MIMO	37.5 Mbps	18.75 Mbps
B28	700 MHz	5 MHz	64QAM	64QAM	4x4 MIMO	75 Mbps	18.75 Mbps
B28	700 MHz	10 MHz	16QAM	QPSK	1x1 SISO	25 Mbps	12.5 Mbps
B28	700 MHz	10 MHz	16QAM	QPSK	2x2 MIMO	50 Mbps	12.5 Mbps
B28	700 MHz	10 MHz	16QAM	QPSK	4x4 MIMO	100 Mbps	12.5 Mbps
B28	700 MHz	10 MHz	16QAM	16QAM	1x1 SISO	25 Mbps	25 Mbps
B28	700 MHz	10 MHz	16QAM	16QAM	2x2 MIMO	50 Mbps	25 Mbps
B28	700 MHz	10 MHz	16QAM	16QAM	4x4 MIMO	100 Mbps	25 Mbps
B28	700 MHz	10 MHz	64QAM	64QAM	1x1 SISO	37.5 Mbps	37.5 Mbps
B28	700 MHz	10 MHz	64QAM	64QAM	2x2 MIMO	75 Mbps	37.5 Mbps
B28	700 MHz	10 MHz	64QAM	64QAM	4x4 MIMO	150 Mbps	37.5 Mbps

BB-PPDR implementation options

Use of mobile operators' networks:

– 410–430 MHz band,

– 450–470 MHz band,

– commercial bands, including the 700 MHz band.

Use of spectrum in other 700 MHz bands outside its main portion (guard band, SDL).

4.1.2.4 Use of mobile operators' networks – 410–430 MHz band

Not under state control; the licence holder is Nordic Telecom.

– According to the CTO, a change in the licence is required to provide services

exclusively for PPDR. Possible as a service in several modes:

– Reservation of part of the spectrum on shared infrastructure.

– Reservation of the entire spectrum (not possible without a licence amendment).

– Sharing the entire spectrum and infrastructure with commercial

operations. Standardisation of this band for LTE/5G technology is

underway:

– Limited number of suppliers for parts of the network technology (core and radio access network requiring modifications) – partial vendor lock-in.

– Significantly limited portfolio of end devices – a handful of manufacturers, likely custom manufacturing, high prices and partial vendor lock-in.

– Challenges in ensuring cross-border interoperability until standardisation is complete and given the use of the band by neighbouring countries.

– Frequency coordination – bilateral agreements are required.

– Hungary and France are currently the main countries involved in standardisation.

Max 2x4.25 MHz, in reality 2x3 MHz (partial allocation), which is insufficient in terms of capacity on its own

– The use of 2x4.25 MHz is not fully compatible with 3GPP blocks (1.4, 3, 5, 10, 20)

– In the case of using 2x3 MHz, it theoretically allows speeds of approx. 15/7.5 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MIMO)

– If 2x4.25 MHz is used, this theoretically allows speeds of approx. 20/10 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MIMO)

It does not meet the requirements of users, the owner or the operator (insufficient capacity, non-standardisation, risk of vendor lock-in, infrastructure sharing, ownership, control, security, interoperability…).

4.1.2.5 Use of mobile operators' networks – 450–470 MHz band

It is not under state control; O2 holds the licence:

– according to the Czech Telecommunications Office (ČTÚ), a change in the licence is required to provide services exclusively for PPDR.

Likely only possible as a turnkey service including the network core without sharing with commercial traffic (not possible

without a licence amendment). The allocation partially overlaps with the standardised 'Band 31' and fully with the newly

standardised 'Band 72':

– standardisation of network technology for band 72 is still ongoing,

– a limited number of suppliers for parts of the network technology (core and radio access network requiring modifications) for both bands 31 and 72 – partial vendor lock-in,

– a significantly limited portfolio of end-user devices for both bands – single manufacturers, likely custom manufacturing and partial vendor lock-in,

– compared to the 410–430 MHz band, the situation regarding the number of suppliers is better, but it is still far from matching existing commercial bands or the future 700 MHz band.

– problems in ensuring cross-border interoperability given the use of the band by neighbouring countries,

– Frequency coordination – bilateral agreements are required.

Max. 2x 4.4 MHz (currently effectively 2x 3 MHz; utilisation of 4.4 MHz requires refarming of the band by O2), which is insufficient in terms of capacity on its own:

– The use of 2x 4.4 MHz is not fully compliant with 3GPP blocks (1.4, 3, 5, 10, 20).

– In the case of using 2x 3 MHz, this would theoretically allow speeds of approx. 15/7.5 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MIMO).

– In the case of using 2x 4.4 MHz, it would theoretically allow speeds of approx. 20/10 Mbps (DL – 16QAM, UL – 16QAM, 2x2

MIMO). With the exception of spectrum allocation from the 700 MHz baseband, this is the least problematic alternative:

  – The Strategy considered using this option for a transitional period to ensure broadband data services with a high level of security and availability as quickly as possible.

– During the drafting of the Strategy, this was one of the potential options for avoiding the modernisation of the PEGAS system, which the emergency services (particularly the Fire and Rescue Service of the Czech Republic) firmly rejected and demanded that the PEGAS system be retained until at least 2025; however, given the delay in the Strategy's approval and the availability of spectrum in the 700 MHz band as of 30 June 2020, this option has now lost its relevance, but it cannot be ruled out in connection with the open tender procedure.

– It partially meets the requirements of users, the owner and the operator (insufficient capacity, ongoing development, risk of vendor lock-in, ownership, control, security, interoperability…)

– O2 withdrew its interest in cooperating with the Ministry of the Interior following the finalisation of the Strategy at the end of 2017, but renewed it in 2018.

4.1.2.6 Use of mobile operators' networks – main commercial bands

Existing spectrum allocations owned by T-Mobile, Vodafone and O2 – 800/900/1800/2100/2600/3700 MHz, and 700 MHz in the future.

A wide range of technical approaches to deployment, operation and development – proposals from commercial entities are expected, detailing in particular the technical, operational, commercial and legal aspects as part of the tender process with proposed solutions.

Probably the best option in terms of capacity – transmission speeds of up to hundreds of Mbps can be expected.

However, the option preferred by the CTO and mobile operators lacks specific details regarding the technical solutions, of which there are many:

– Commitments regarding the future auction of the 700 MHz band are one possibility.

– Another option is to conduct an open tender without conditions in the 700 MHz band auction.

– The proposal itself is in direct conflict with the resolution of the steering committee for the preparation of the Strategy – it does not meet the requirement for full control over the operation and development of infrastructure, technologies and services – this involves the elimination of ever-increasing security risks (cyber security, physical security) and is in line with the state's strategy to reduce dependence on commercial entities.

  – Cooperation with and the use of mobile operators' networks is, however, an integral part of the Strategy for ensuring crisis communication services, but it is a supplementary (to increase availability and capacity) rather than a primary means of communication.

The use of commercial operators' networks raises a number of issues that must be reflected in legislation, regulation or auction commitments, e.g.:

– territorial coverage,

– specific functionalities,

– high availability,

– high security,

– control over communication resources

– etc.

Currently, only one country, the United Kingdom, is implementing this model; delays are being reported and there is a need for significant compromises, particularly regarding functional requirements (e.g. direct communication) and improving availability.

Other countries (e.g. Finland), following the sale of the 700 MHz band to operators, face similar challenges, where it is not possible (without legislative and/or regulatory changes, including extensive commitments prior to the 700 MHz band auction) to effectively and on a commercial basis ensure the required level of emergency communication services that meet the requirements of users, the operator and the owner.

It does not meet the requirements of users, the owner and the operator (infrastructure sharing, ownership, control, security, …).

The reservation and use of these frequencies are essential to ensure that communications between emergency services are reliable, secure and interoperable. This also includes the obligations set for the auction winner, which encompass the duty to provide national roaming and priority broadband services for PPDR.

4.1.2.7 Details of frequency bands

700 MHz band:

Primarily intended for PPDR broadband services.

Includes specific services such as MCPTT, MCV, MCD.

Key to the roll-out of 5G technologies.

800 MHz band:

Serves as a complement to the 700 MHz band.

Supports coverage expansion and interoperability.

400 MHz band:

Used for narrowband voice services.

Used in the PEGAS network based on Tetrapol technology.

450 MHz band:

Supports the allocation and use of 400/450 MHz frequencies by the 450 MHz

Alliance[9] . Suitable for broadband data and voice services.

Offers sufficient coverage for less densely populated areas.

160 MHz band:

Traditionally used for analogue emergency

services communications. Provides basic

voice communication.

Other bands:

The 3.5 GHz band for high-speed data transmission and enhanced emergency services.

4.2 Legislation

Legislation governing the use of frequencies for PPDR and, more generally, for emergency communications is a key element in ensuring secure and effective communications for emergency services. The following legislation and regulations set out the framework for the use of radio frequencies, technical requirements and conditions for the interoperability of services

4.2.1 Legislation in the Czech Republic

Decree No. 127/2005 Coll., on electronic communications and amending certain related acts (the Electronic Communications Act): This Decree regulates the conditions for the use of radio frequencies and lays down rules for the provision of electronic communications services. It is essential for determining the conditions under which mobile operators and other entities may provide PPDR services.

Act No. 240/2000 Coll., on crisis management and amending certain acts (the Crisis Management Act): This Act lays down rules for crisis management, including the use of crisis management information systems. It regulates the responsibilities of crisis management authorities and sets out how means of communication for crisis situations are to be ensured.

Act No. 239/2000 Coll., on the Integrated Rescue System and amending certain acts: This Act defines the components of the Integrated Rescue System and their responsibilities. It sets out how communication facilities are to be provided for the individual components of the Integrated Rescue System, such as the Fire and Rescue Service, the Police of the Czech Republic and providers of emergency medical services.

Government Regulation No. 432/2010 Coll., on criteria for determining elements of critical infrastructure: This Government Regulation defines the criteria for determining elements of critical infrastructure that are essential for ensuring the security of the state and its inhabitants. It also sets out requirements for the protection and security of these elements, including communication systems.

4.2.2 Technical specifications and standards

The implementation of PPDR services must meet specific technical requirements and standards that ensure the reliability, security and interoperability of communication systems.

3GPP/ETSI technical specifications: These specifications define requirements for mobile communication technologies, including broadband services and interoperability between different systems and operators. They are essential for ensuring high-quality and secure communication services for PPDR. Specific specifications include:

3GPP TS 23.501: Defines the architecture of 5G systems.

[9] https://450alliance.org/

3GPP TS 23.401: Specification for the LTE system architecture and its extension to support PPDR services.

Interoperability standards: Standards such as Mission Critical Push to Talk (MCPTT), Mission Critical Video (MCV) and Mission Critical Data (MCD) ensure that different communication systems can work together effectively when responding to emergency situations. These standards include:

MCPTT: Provides reliable and instant voice services for emergency situations.

MCV: Enables real-time video transmission for improved situational awareness.

MCD: Provides data services that support the various applications and services required in emergency situations.

4.2.3 Obligations set out in the spectrum auction

According to CTU documents, obligations for the provision of PPDR services have been set for operators who have acquired frequencies in the 700 MHz band. These obligations include:

National roaming: The obligation to provide national roaming for new auction participants who are not existing operators.

Priority BB-PPDR: Provision of priority broadband services for PPDR in the 700 MHz band. This includes interoperability with the PPDR network core and support for traffic management for emergency services.

4.2.4 European Union documents and international conventions

The implementation of PPDR services in the Czech Republic is also influenced by European Union documents and international conventions, which set out the framework for the use of radio frequencies and technical standards:

EU Radio Spectrum Policy Programme (RSPP): Sets out objectives and measures for the efficient use of radio spectrum in the EU.

ECC Decision (16)02: Recommendations for the harmonisation of frequency bands for PPDR services in Europe.

4.3 Information from abroad

The European Union has focused on harmonising spectrum for PPDR services, with the 700 MHz band being key. This step aims to ensure the availability of spectrum for all Member States and to promote interoperability between them. Harmonised spectrum not only facilitates cooperation during cross-border incidents but also ensures that the technologies and equipment used in different countries are compatible.

Mobile operators that are allocated spectrum in the 700 MHz band are obliged to provide PPDR services. These services include priority access for emergency communications, quality of service (QoS) and national roaming. This means that, in an emergency, emergency services will have priority access to the network, which is crucial for rapid and effective communication during crisis situations.

The transition to broadband technologies such as LTE and 5G is one of the main objectives of the strategy. These technologies offer higher speeds and greater capacity than existing TETRA systems. The 3GPP standards specify functions for critical communications, such as Mission Critical Push-to-Talk, Mission Critical Data and Mission Critical Video. These specifications ensure that new technologies will be capable of supporting all the necessary services for PPDR.

The key spectrum for PPDR in the EU is the 700 MHz band, where 2x10 MHz is allocated for PPDR broadband services. In addition, some countries utilise further spectrum blocks in the 700 MHz band, such as 2x5 MHz or 2x3 MHz (733–736 MHz (uplink) and 788–791 MHz (downlink)). In addition, UHF bands are also being considered, particularly the 400 MHz band (410–430 MHz and 450–470 MHz), which can provide supplementary PPDR services, especially in areas where the 700 MHz spectrum may not be sufficient.

Many EU countries are planning a gradual migration of existing TETRA networks to modern broadband networks based on LTE and 5G. This process involves drawing up a migration timetable, implementing pilot projects and testing new technologies. An important step is to ensure service continuity during the transition period so as not to disrupt emergency communications.

Pilot projects and testing of new technologies are essential to verify their ability to support PPDR. These projects focus on testing coverage, capacity and interoperability between different systems and devices. Ensuring that different systems can work together seamlessly is key to effective emergency communications.

One of the main challenges is ensuring sufficient geographical coverage, particularly in remote or hard-to-reach areas. Financing network modernisation and ensuring a return on investment represent further economic challenges faced by many Member States.

Overall, the 5G strategy for PPDR in the EU focuses on modernising technological platforms, ensuring interoperability and service quality. Although challenges such as funding and coverage remain, the commitments made by individual Member States demonstrate a strong commitment to modernising emergency communications and enhancing the safety and effectiveness of public protection and emergency response.

4.3.1 Austria

Regional TETRA networks have been rolled out since 2006, with completion in 2019.

The TETRA network is privately owned but is operated and managed by the Austrian Ministry of the Interior.

Dedicated spectrum: 2 x 8 MHz in the 700 MHz band for PPDR.

There are currently no plans to use the UHF band (410–430 MHz, 450–470 MHz).

4.3.2 Belgium

One of the first nationwide TETRA networks for public safety, established in 1998 (operator: ASTRID). The 700 MHz spectrum (2 x 30 MHz) will be auctioned subject to MCPTT support.

Harmonised: 2 x 8 MHz in the 700 MHz band for PPDR. Possibility of reserving band 68 (2 x 5 MHz) for ASTRID.

4.3.3 Bulgaria

One of the first TETRA networks, built in the late 1990s, with a major upgrade in 2017. Plan to release spectrum for 5G: 2x20 MHz in the 700 MHz and 800 MHz bands.

Spectrum reserved for PPDR: lower 2x5 MHz (Band 68 (698–703 MHz and 753–758 MHz)).

4.3.4 Denmark

DBK has built a nationwide TETRA network with 99.5% coverage.

Motorola Solutions has proposed allocating 2x10 MHz (713-723 / 768-778 MHz) for PPDR.

The government will auction 2x30 MHz and 20 MHz with coverage requirements.

4.3.5 Finland

The VIRVE TETRA network is in operation, with plans to migrate to a 3GPP broadband solution by 2025. A 700 MHz spectrum auction took place in 2016.

The 700 MHz band is unsuitable for PPDR due to its proximity to Russia.

4.3.6 France

The Tetrapol network will be switched off by 2024.

700 MHz spectrum auction in 2015, allocation of 2x8 MHz for PPDR. The 700 MHz band is insufficient for future PPDR needs.

4.3.7 Germany

The largest TETRA network (BDBOS), completed in 2016, covers more than 99% of the territory. The TETRA network will remain operational until at least 2030.

Exploring spectrum options in the 400 MHz and 450 MHz bands.

4.3.8 Hungary

National TETRA network managed by Pro-M.

NMHH proposes 2 x 8 MHz in the 400 MHz band for BB-PPDR.

Plans to use 410-430 MHz and 450-470 MHz for public safety.

4.3.9 Netherlands

Decision to replace the C2000 network with TETRA, new contract for 8–10 years. Auction of the 700 MHz spectrum for 5G in 2020.

Interest in the 700 MHz guard bands and the duplex gap.

4.3.10 Norway

Nationwide TETRA network completed in 2016, with TEDS added to one-third of sites.

Recommendation to make the 700 MHz spectrum available for commercial services.

PPDR requirements will be met by commercial operators.

4.3.11 Slovenia

Nationwide TETRA network, seeking a hybrid solution for PPDR.

700 MHz spectrum with an obligation to offer national roaming for secure public MVNOs.

Reserved: 2x3 MHz and 2x5 MHz in the 450-470 MHz band.

4.3.12 Sweden

Largest TETRA network (RAKEL), no plans for shutdown.

Proposal for LTE critical communications with 2 x 10 MHz FDD in the 700 MHz band. 700 MHz auction in 2018, two mobile operators acquired 2x20 MHz.

4.3.13 Switzerland

5G spectrum auction in 2019, 700 MHz band for commercial use. Interest in 700 MHz guard bands, 450–470 MHz band congested.

4.3.14 United Kingdom

TETRA network for emergency services established in 1996, migration to LTE. 700 MHz spectrum auction.

There is currently no possibility of using the 700 MHz or 450-470 MHz guard bands for PPDR.

5 Emergencies and communications in emergencies

5.1 Examples of communication equipment used by selected emergency services

MEANS	PUBLIC/NON-PUBLIC	SLA
FIXED NETWORK	Public / Non-public	Public: service quality determined by a contractually agreed scenario. No SLAs for voice services. Same as for residential customers. Non-public: voice and data services provided with individually configurable quality.
MOBILE NETWORK	Public	Not available; service quality is the same as for other users. Call priority is difficult to enforce and difficult to access.
TETRAPOL IP	Non-public	Voice and data services with individually configurable quality. Quality is managed by the Ministry of the Interior itself.
DMR (160 MHz)	Confidential	SLA addressed at the level of the spectrum's technical capabilities, where service immunity cannot be guaranteed.
UNIFIED WARNING AND ALERT SYSTEM	Non-public	Secure data service with individual SLAs and regular functionality checks.
SPECIAL PROPRIETARY SYSTEM	Non-public	SLAs are often negotiated here, due to the limited impact on the number of users.
SATELLITE	Public	Not available; service quality is the same as for other users. Call priority is difficult to enforce and difficult to access.
ANALOGUE RADIO (160 MHz)	Non-public, with the possibility of interception by unauthorised persons	SLA addressed at the level of the spectrum's technical capabilities, where service immunity cannot be guaranteed. There is a risk of eavesdropping/breach of confidentiality.
TETRA (400 MHz)	Non-public	Quality parameters are set out in the general terms and conditions for end-users of non-publicly available electronic communications networks and are not affected by other services for retail end-users.

5.1.1 Basic classification of types of electronic communications networks

The fundamental element of telecommunications networks is **the** so-called **passive infrastructure**, which is defined in the Electronic Communications Act No. 127/2005 Coll., as amended (ZoEK), as **the means assigned to** the assigned service under Section 2(2)(a) - (*this includes physical infrastructure and other equipment or elements related to an electronic communications network or electronic communications service which enable or support the provision of services via that network or service, or are capable of doing so, and includes buildings or building entrances, cable distribution systems within buildings, antennas, towers and other supporting structures, cable ducts, conduits, masts, manholes and distribution boxes.*)

Passive infrastructure and active elements are used to implement **electronic communications networks** ZoEK §2(2)(b) - (*electronic communications networks are transmission systems, regardless of whether they are based on fixed infrastructure or are centrally capacity-controlled or not, and, where applicable, also switching or routing equipment and other means, including inactive network*

elements, which enable the transmission of signals via wire, radio, optical or other electromagnetic

means, including satellite networks, fixed circuit-switched or packet-switched networks, including the internet, mobile networks, electricity distribution networks to the extent that they are used for the transmission of signals, radio and television broadcasting networks and cable television networks, regardless of the type of information transmitted)

Electronic communications networks are further divided into:

A public communications network is **an electronic communications network** (Section 2(2)(d)) which is used wholly or mainly for the provision of publicly available electronic communications services and which supports the transmission of information between network end-points, or an electronic communications network through which radio and television broadcasting services are provided,

Non-public communications networks (not described in the ZoEK) – these are described in the National VHCN Network Development Plan[10]

- **Non-public critical infrastructure networks:** Critical infrastructure is subject to Act No. 181/2014 Coll., on cyber security, which regulates the scope of competence and powers of public authorities in the field of cyber security and the safeguarding of the security of electronic communications networks and information systems.
- **Non-public public administration networks:** A non-public public administration network can be defined as a next-generation data network based wholly or partly on technology utilising optical communication elements and operated by a public authority (state authorities or local government bodies, or entities authorised by them) for the purposes of public administration and public services. The category of non-public public administration networks includes, in particular, regional and municipal networks. The network is not used by households or private-law entities, with the exception of organisations established or set up by municipalities, regions or the state. Furthermore, the network must not be commercially leased, and users are not charged any fees for its operation.
- **Other non-public networks:** Other non-public networks include, for example, networks within corporate premises that serve to support the operation of production and processing lines. These networks are generally not subject to regulation or data collection as part of geographical mapping.

From the perspective of quality parameters and conditions for the provision of services on the networks in question:

Publicly available electronic communications services (or non-public communications services), where operated on a public electronic communications network – minimum quality parameters are set out in the Electronic Communications Act (ZoEK) and relevant decrees and OOPs issued by the Czech Telecommunications Office (ČTÚ) – a description must be included in the general terms and conditions for end-users of publicly available electronic communications networks.

A non-public communications service is provided on a non-public communications network – it does not have pre-defined minimum parameters. Quality parameters are set out in the general terms and conditions for end-users of non-publicly available electronic communications networks.

Types of electronic communications services:

- **voice** – an interpersonal communications service,
- **data** – internet access service,
- **services consisting wholly or mainly of the transmission of signals**, such as transmission services used for the provision of machine-to-machine communication services and for radio and television broadcasting,
- **a radiocommunication service** is a communication activity consisting of the transmission, broadcasting or reception of signals via radio waves,
- **emergency communications means communications** via interpersonal communications services between an end-user and an emergency communications centre, the purpose of which is to request and obtain assistance from emergency services in the event of an emergency.

The impact of this electronic communications service on the construction and authorisation process.

Construction processes will also need to be taken into account during network implementation.

	Can be used for **public** electronic communications **networks**	Can be used for **non-public** electronic communications **networks**
Construction in accordance with the Building Act 183/2006 Coll.		
Section 79 (Decision on the location of a structure) • Antennas up to 8 m in height (BTS) • Replacement of technical infrastructure cables	**Yes**	**Yes**
Section 81 (Decision on changes to the impact of building use on the area)	**Yes**	**Yes**

[10]https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke-komunikace/koncepce-a-strategie/narodni-plan-rozvoje-siti-nga/narodni-plan-rozvoje-siti-s-velmi-vysokou-kapacitou--259858/

Section 103 (Buildings, landscaping, facilities and maintenance works not requiring a building permit or notification), • paragraph 1, point (e), **sub-point 4** (Planning permission for the location of a structure, planning consent, VPS replacing planning permission), ZÚŘ • para. 1, letter e), **point 10** (EK connections)	**Yes**	**Yes**
• **Sections 104 to 107 (Notification)** exceptionally, for example for central network elements	**Yes**	**Yes**
Section 108 (Planning permission) • Everything not covered by Sections 103 to 107 • in very exceptional cases, for example for data centres	**Yes**	**Yes**

Construction under Act No. 416/2009 Coll. (Linear Act) – Act on the Acceleration of Construction		
Section 2i, paragraph 1) (so-called connection up to 100 m)	**Yes**	**NO** *)
Section 2i, paragraphs 3) and 4) (so-called 'adjacent connection')	**Yes**	**NO** *)

**) Section 1(11) of Act No. 416/2009 Coll. (the Line Act) (For the purposes of this Act, 'electronic communications infrastructure' means the construction of communication lines of a public communications network as technical electronic communications infrastructure and related communications equipment, including their electrical connections.)*

5.1.2 Fixed network

A fixed network refers to infrastructure that provides telecommunications services via fixed cable routes (such as optical or copper cables). This network provides access to telephone and data services, such as the internet or television broadcasting, via fixed connections. Fixed networks are more stable and less prone to outages caused by environmental factors compared to wireless networks.

5.1.2.1 Public network

A fixed (public) network is referred to as the Public Switched Telephone Network (PSTN), which is a global network of public telephone networks that are interconnected and focused on voice services. The PSTN is a traditional circuit-switched telephone network that has been in operation since the late 19th century. This network encompasses all telephone networks worldwide operated by local, national or international operators. These networks provide the infrastructure and services for public telecommunications. Fixed lines, also known as PSTN, fixed telephone services or traditional telephone lines, use underground copper wires for reliable communication.

The PSTN is a combination of telephone networks used worldwide, comprising telephone lines, fibre-optic cables, switching centres, cellular networks, satellites and cable systems. It enables users to make landline calls to one another.

5.1.2.2 Private network

Private telephone systems are independent telephone systems owned or leased by a company or an individual. These systems include key telephone systems (KTS), private branch exchanges (PBX), computer telephony (CT), wireless PBX, local area network (LAN) telephony and multimedia communication, such as video conferencing. Private telephone systems consist primarily of telephones (known as stations or terminals), local cabling and switching systems. Telephone stations act as the interface between the user and the telephone network. Cables connect the telephone stations to the switching systems or distribution points. Local cabling in private systems can range from shared lines (key systems) to individual lines (digital stations). Switching systems interconnect stations or connect them to external telephone lines or internal company connections.

A private network is intended solely for a specific group of users and is not accessible to the general public. These networks often utilise specialised technologies and are operated for the internal needs of organisations, such as emergency communication networks, corporate networks and networks of state institutions. Emergency communication networks are used, for example, by the integrated rescue system to ensure secure and reliable communication in the event of an emergency. Corporate networks are used for internal communication and data transfer within companies and institutions, whilst government networks are designed for communication and administration between various government bodies. Non-public networks often have a higher level of security, restricted access and may be designed to meet specific requirements for availability and reliability.

5.1.3 Mobile network

5.1.3.1 Mobile Secure Platform

The Mobile Secure Platform (MBP) is an innovative system developed primarily for the Czech Police. This system enables secure access to internal databases and information systems directly from mobile devices such as smartphones and tablets. The main functionality of the MBP is to provide immediate access to information on individuals, vehicles and other relevant data, which streamlines the work of police officers in the field and reduces reliance on central operations centres.

The platform was designed to ensure a high level of security for transmitted data. This is achieved through encryption and the use of secure communication channels, which protect sensitive information from unauthorised access. MBP supports various types of mobile devices and is integrated with a wide range of applications, ensuring that police officers can quickly and efficiently carry out background checks, access registers and enter data directly from the scene of an incident. This flexibility and immediate access to data directly in the field are key factors contributing to a faster and more effective response in crisis situations.

The MBP is used primarily for background checks and to access the Czech Police's information systems, such as the population register, the vehicle register, and the system for tracing persons and vehicles. Thanks to this system, police officers can carry out immediate identity checks on persons and vehicles at the scene, thereby increasing the efficiency of their work. The system is also designed to enable fast and secure data sharing between individual patrols and operations centres, which contributes to better coordination and management of police operations in real time.

The SLA and security of these networks are tailored to the requirements of a publicly available electronic communications network. The operation and parameters of the networks are defined by the Electronic Communications Act No. 127/2005 Coll., as amended, and related regulations.

5.1.3.2 Virtual Private Network

A Virtual Private Network (VPN) is a technology that enables the creation of a secure connection over public or unsecured networks, such as the internet. A VPN encrypts data transmitted between the user's device and the destination server, thereby protecting communications from unauthorised access. This encryption is particularly important when using public Wi-Fi networks, where there is an increased risk of eavesdropping. In addition, a VPN hides the user's real IP address and replaces it with the IP address of the VPN server, thereby providing anonymity and privacy protection.

A VPN also allows access to geographically restricted content, meaning that censorship or regional blocks can be bypassed to access websites and services that would otherwise be unavailable in a given area. This technology is often used by companies to provide secure connections for employees to corporate networks, enabling secure access to internal resources and applications from anywhere, thereby increasing the flexibility of remote workers.

Using a VPN prevents internet service providers and other parties from monitoring a user's online activities, thereby ensuring that searches, websites visited and other internet activities remain private. A VPN creates an encrypted 'tunnel' between the device and the VPN server, which secures the data and prevents it from being easily intercepted or decrypted.

5.1.4 DMR (160 MHz)

Digital Mobile Radio (DMR) in the 160 MHz band is a modern communication technology used by some emergency services and other professional organisations in the Czech Republic. This system provides reliable and secure communication, which is ensured by hardware encryption at the terminal level. The use of encryption algorithms such as ARC4 or AES guarantees a high level of data protection against unauthorised access.

DMR technology is backwards compatible with traditional analogue systems, which facilitates the transition to newer technologies without the need to replace all equipment immediately. Thanks to TDMA time-division multiplexing technology, DMR makes efficient use of available frequency channels, allowing two independent calls or data transmissions to be conducted simultaneously. This offers greater efficiency compared to traditional analogue systems.

In addition to high call quality and a stable signal, DMR offers advanced features such as individual and group calls, emergency calls, GPS location tracking and text messaging. These features increase the system's flexibility and suitability for use in various situations, including emergencies. Furthermore, DMR systems are more energy-efficient, which extends battery life and reduces operating costs, making them cost-effective for professional use.

5.1.5 Unified Warning and Notification System

The unified warning and notification system is a key tool for protecting the population against emergencies in the Czech Republic. This system, which has been under development since 1991, comprises a network of alarm sirens and notification centres, whose main task is to provide timely and effective warnings to the public via acoustic signals and subsequent verbal information about the nature of the threat. Public warning is provided by local authorities, regional fire and rescue services and other agencies, which operate the unified warning and notification system for this purpose.

The system consists of warning terminals and a transmission network. The transmission network comprises separate radio transmitters, which are evenly distributed across the region. These transmitters ensure the transmission and dissemination of the radio signal used to control the warning terminals. The warning terminals consist of rotating sirens, electronic sirens and remotely controlled public address systems. Rotating sirens are installed in municipalities with more than 500 inhabitants or in areas at risk of flooding. Electronic sirens and public address systems provide not only acoustic signals but also subsequent verbal information regarding the nature of the threat.

The unified system allows the sirens to be controlled individually or in groups from the central operations centre of the regional fire and rescue service, or to trigger all sirens simultaneously. This centralised control is key to a rapid and coordinated response to emergency situations, which increases the chances of protecting the health and lives of residents. Information on the location and types of warning devices is available from local authorities, which can provide details to residents.

A unified warning and notification system is therefore an essential element in ensuring the timely warning and informing of residents in the event of a threat, enabling the effective implementation of measures to protect their health and safety.

5.1.6 Special proprietary system

Proprietary radio networks are closed communication systems designed and managed by a specific manufacturer. These networks provide a high level of security and control, making them ideal for applications where secure communication is crucial, such as in industry or security operations.

One of the main advantages of these networks is their ability to be optimised for the specific needs of a given application. This ensures they are capable of delivering high performance and reliability in demanding conditions where standardised systems may not always be suitable. However, their closed nature means they are not compatible with other technologies, which can lead to higher costs and limited flexibility when expansion or a change in technology is required.

In the field of the Internet of Things (IoT) and industrial applications, proprietary radio networks are often utilised for their specific characteristics, which include low latency and high reliability. These networks enable data transmission with the required level of security and speed, which is essential for monitoring and controlling industrial processes.

Proprietary radio networks therefore represent a specialised solution for applications requiring secure and efficient communication, albeit at the cost of limited interoperability and dependence on a specific manufacturer.

5.1.7 Satellite

Satellite communication uses satellites to transmit signals over long distances, thereby providing global coverage even in areas without access to traditional communication networks. This technology is key to ensuring reliable communication in remote and hard-to-reach areas where terrestrial infrastructure is unavailable or impractical.

One of the main advantages of satellite communication is its independence from terrestrial infrastructure, enabling reliable connectivity regardless of geographical or political boundaries. Satellite systems provide flexible and rapidly deployable communication solutions, which is essential in emergency situations, such as natural disasters, where connections must be established quickly.

Satellites support various types of services, including voice communication, data transmission and internet connectivity, making them a versatile tool for many applications. Thanks to their resilience and reliability, they ensure uninterrupted connectivity even in challenging conditions.

5.1.8 Analogue Radio (160 MHz)

The analogue communication system in the 160 MHz band, known as Analogue Radio (AR), is used by the Fire and Rescue Service as a secondary communication system. Volunteer fire brigade units are also connected to this system, enabling its

widespread use in rescue operations. Due to its versatility, this technology has a very low level of security, meaning that communications are not protected against unauthorised access or eavesdropping.

Analog Radio is used primarily for voice communication and the transmission of codes for typical activities, such as unit statuses. This technology does not support data transmission, which limits its functionality to basic communication needs. If necessary, the PEGAS and Analog Radio networks can be interconnected using a single-channel converter installed in the fire service vehicle at the scene of the incident. This converter enables coordinated communication between different systems.

Incident command via Analog Radio is managed by the incident commander, who is equipped with two separate terminals or a combination of a terminal and an analogue radio. The control centre has access to both networks, ensuring effective coordination and management of rescue operations. In selected rescue service units, hybrid terminals are also used, which enable communication via both DMR and Analog Radio, thereby expanding communication options in the field.

5.1.9 TETRA (400 MHz)

The TETRA (Terrestrial Trunked Radio) network in the 400 MHz band is a modern digital radio communication system used by emergency services in several regions of the Czech Republic. TETRA is a private network that uses hardware encryption at the terminal level, ensuring a high level of communication security. This system was developed to provide secure, reliable and efficient communication between the components of the integrated emergency response system and other security authorities.

TETRA technology supports both voice and limited data communication. Although this technology offers basic data services, compared to modern 5G networks it has limited capabilities and cannot fully meet the future needs of the integrated rescue system units, which will require higher transmission speeds and advanced data services. However, the TETRA system remains a key tool for emergency communications, thanks to its ability to ensure continuous and stable communication in challenging conditions.

The TETRA network consists of a series of base stations that provide coverage across large areas and allow mobile units to switch easily between individual stations depending on signal quality, much like mobile phones on commercial operators' networks. This system also supports group calls, which are essential for the effective coordination of rescue operations. The use of TETRA technology enables secure communication even beyond the reach of standard infrastructure, which is crucial for field operations.

There are currently 13 TETRA-based networks in operation in the Czech Republic. The first network, established in 2002 (NATO summit), is in the capital city of Prague, where more than 4,000 radio stations are registered (municipal police approx. 1,500, transport company approx. 2,500, crisis management team approx. 100, technical road administration approx. 80). Other networks are in operation at Prague-Ruzyně Airport, the military air bases at Kbely, Čáslav, Pardubice and Přerov, the military sites at Doupov and Libavá, municipal radio systems in Brno, Liberec and České Budějovice, and corporate radio systems at Hyundai Nošovice and Chemopetrol Litvínov.

5.1.10 PEGAS (TETRAPOL – 380 MHz)

PEGAS is a private nationwide communications network based on the TETRAPOL standard, operating in the 380 MHz band. The network comprises approximately 230 base stations and covers 68% of the territory of the Czech Republic, making it the primary means of communication for the Integrated Rescue System (IRS). PEGAS is used by all core emergency services, including the Fire and Rescue Service, the Police of the Czech Republic and the Emergency Medical Service. The network brings together regional control centres corresponding to the individual regions of the Czech Republic.

Thanks to the private nature of the network and hardware encryption at the terminal level (end-to-end), voice communication on the PEGAS network is highly secure. A technological upgrade of the network is currently underway, involving a transition to IP technology between the radio and network layers (exchanges). This upgrade will extend the technology's lifespan. PEGAS is a purely voice-based communication system and will not support high-speed data services even after the upgrade. Support for the existing upgraded solution is contracted until 2027. After this period, an increase in service costs can be expected due to the lifespan of IT components, as is common in the market.

5.1.10.1 Scope of Tetrapol technology

219 base stations

25 repeaters

43 radio exchanges

digital trunking and other technologies and

software 1,868 control room workstations

16,269 handheld radios

7,659 vehicle-mounted radios

1,191 vehicle adapters for handheld radios 390 GPS

applications

6 Technological capabilities

The technological capabilities of mobile communication solutions for security and emergency services in the Czech Republic are key to an effective and rapid response to crisis situations. With ever-increasing demands on the speed and reliability of communication, it is essential to modernise current technologies and systems so that they better meet present and future needs. The current state of the technologies in use encompasses various communication platforms, which are often limited in their functionality and interoperability.

As part of the analysis of the current state, key technologies and end-user devices currently used by the emergency services were identified. This analysis revealed a number of shortcomings and limitations that need to be addressed, such as limited support for data services, insufficient security of communications outside proprietary networks, and the limited territorial coverage of these networks.

Based on these findings, possible approaches for modernising and improving the communication capabilities of the IZS units were proposed. These approaches take into account technological, economic and security aspects in order to select the most suitable solution for the current and future needs of the IZS.

6.1 Current status of technologies in use

As part of the analysis of the current situation, the following technologies currently used by the core components of the IZS were identified:

PEGAS Tetrapol IP

AGNET voice communication Data

communication – low speed

Satellite data communication

Voice communication Data

communication

Unified Warning and Notification System (JSVV)

Pocsag technology, gradually transitioning to

digital radio Data – analogue communication

Services on public mobile networks – without QoS

MBP Police GINA

– Fire Service

POINTX – Fire

Service

Temporary wireless connection

Voice communication Data

communication

pTRACK

Data – Mash communication for search and rescue teams

IoT sensors

Data – crisis communication monitoring (water, air, radiation) – under development and testing

Radio network of passive receivers, video transmission from a helicopter, SOVA 2GHz system, flight altitude 300m above ground

Video transmission, single-wire

Upcoming project to expand monitoring stations and reduce flight altitude to 150m above ground

SCO – 400 MHz centralised protection system

Data connectivity for facility protection – need for police backup communications, interference from Tetrapol base stations

Fixed connection via a fixed network (wired/fibre/wireless)

Voice communication Data

communication

Communication for covert use

Voice communication

Traffic management – for analysis

Data management and control of traffic flow according to the needs of emergency

services Backup for an autonomously controlled vehicle

Control centres

The link to new services at control centres has not been analysed This

analysis will continue once the needs of the emergency services have

stabilised

160 MHz radio

Voice communication – analogue Voice

and data communication – DMR

TETRA

Voice and data communication

The current emergency communications system is primarily based on voice communication, whilst data services are supported only to a limited extent. This situation limits the effectiveness and flexibility of emergency communications. Furthermore, the various communication platforms are not interconnected, which means that the control centre must play a significant role in coordinating communications between the emergency services.

The technological capabilities and management of current platforms are often inflexible, and user terminals are inadequately equipped. Many of these technologies are outdated and do not meet modern requirements. Proprietary networks such as PEGAS and TETRA provide a high level of communication security, whilst other platforms only partially meet security requirements or are insufficient for the future needs of crisis communication.

Another problem is the limited territorial coverage of proprietary networks, which can be an obstacle in large-scale crisis situations. The current use of data services within the Integrated Rescue System (IRS) is merely supportive, yet their importance in crisis communication and management is undeniable. Modernisation and innovation in incident management are often limited by the inability to utilise high-speed data transmission, which represents a significant obstacle to increasing the efficiency and safety of these operations.

6.2 Possible solutions

There are four possible approaches to ensuring and developing mobile communications for security and rescue services:

6.2.1 Retain and develop Tetrapol IP

The transition to Tetrapol IP was completed at the end of the year. This approach would allow for the continued use and development of the existing infrastructure. Retaining this technology would ensure continuity and enable further optimisation of the system, which could lead to increased efficiency and reliability of communications.

6.2.2 Retain Tetrapol IT in its current configuration and enter into a long-term contract with mobile operators

This approach involves the parallel use of the current Tetrapol IT configuration and a long-term service agreement with mobile operators without an SLA for the Ministry of the Interior. This approach could offer flexibility and cost-effectiveness by utilising the existing infrastructure whilst also using commercial mobile networks for support.

6.2.3 Implement BB PPDR/NR PPDR

This approach involves the implementation of a broadband network for emergency communications, but carries significant risks, including high costs and inadequate SLA terms. Standard mobile technologies (3GPP) offer high capacity, robustness and security, which could be key to the successful implementation of broadband networks for public protection and emergency communications.

6.2.4 Build a proprietary network in agreement with the Army

This approach involves building a proprietary network based on existing TetraPol transmitters and contracting coverage overlaps with mobile operators. A symbiotic network combining commercial and government infrastructure can offer the necessary flexibility and ensure communications even in the event of outages or increased capacity demands. This approach would enable resource sharing between government and commercial networks, thereby improving overall resilience and service availability.

6.3 A network connecting multiple technologies to ensuring critical communications

One of the modern solutions for ensuring effective and secure emergency communications is the implementation of a network that combines multiple technologies. This approach utilises a combination of commercial mobile networks and dedicated government networks to create a flexible and robust communications system capable of meeting the demands of emergency communications even under the most challenging conditions.

6.3.1 Network configuration

This network enables the government's critical network to interact with commercial networks, thereby providing significant benefits to both parties. This approach allows commercial networks to act as a capacity booster, whilst the government network can serve as a backup communication channel. The network architecture ensures that communications are reliably maintained in the event of outages or increased demand for capacity.

The main components of the network include static and dynamic infrastructure. The static infrastructure comprises dedicated geo-redundant core networks that provide overall control over equipment and data traffic, including functions such as subscriber management, billing and policy management.

The dynamic infrastructure comprises mobile units and temporary base stations, known as Cell-on-Wheels, which can be deployed to increase coverage and capacity as required. These units can be rapidly deployed in areas where they are needed, for example during natural disasters or major emergencies.

6.3.2 Key capabilities

A multi-technology network provides several key capabilities that are essential for effective crisis communication. One of these is support for national roaming between government and commercial networks, which enables the expansion of coverage and capacity, which is crucial for ensuring emergency communication in crisis situations. Another is the concept of Network Slicing, which allows the logical division of the network into multiple virtual segments that can be utilised by different service providers. Each network 'slice' can be configured to meet specific requirements for bandwidth, latency and security.

Another capability of this network is data security and protection. It ensures the separation and encryption of sensitive information, as well as the prioritisation of emergency communications.

6.3.3 Network support techniques

Certain techniques and standards are necessary to support both dedicated government networks and networks combining multiple technologies. 3GPP standards describe various roaming scenarios that enable the interconnection of government and commercial networks. These standards ensure that users can switch seamlessly between networks without any disruption to services.

Virtual and software-defined networks enable flexible resource allocation and dynamic user management. This includes the ability to dynamically change policies for routing and authorising user sessions, ensuring a high degree of flexibility and scalability. Today's LTE and future 5G networks offer a wide range of capacity options and reliable geographical coverage. This technology supports a massive number of connected devices and meets the high bandwidth and reliability requirements for emergency applications.

Proximity Services enables devices in emergency vehicles to extend network connectivity into buildings or areas with poor coverage, effectively extending the reach of the public safety network. Precise positioning can be used to locate mobile callers in distress, emergency responders' communication devices, and specific resources or equipment connected to the network. Modern technologies enable high-precision positioning.

6.3.4 Network implementation and benefits

Network implementation involves several steps. The first is an analysis of the specific communication requirements and demands of the Integrated Rescue System (IRS). This is followed by planning and design, which involves creating an architectural design encompassing both static and dynamic infrastructure. The next step is the deployment of the necessary hardware and software, including base stations and mobile units. The process concludes with testing and optimisation to verify functionality and optimise network performance.

The benefits of this network include increased capacity and coverage, enabling better coverage in geographically challenging areas and higher capacity during crisis situations. Flexibility and scalability allow for easy adaptation to changing needs and rapid expansion of capacity. Cost-effectiveness is another significant benefit, as the use of existing commercial technologies and infrastructure reduces development and maintenance costs.

The implementation of this network for the Integrated Rescue System (IRS) in the Czech Republic represents a step forward towards modern, robust and effective crisis communication capable of responding to the challenges of today's world. This approach not only increases the efficiency and reliability of communication but also brings significant savings and opportunities for future development and innovation in the field of crisis management.

Examples of the implementation of these services at the level of the Fire and Rescue Service Headquarters include projects that form part of grant applications submitted to the Ministry of Regional Development (MMR). These projects involve the implementation of a network that integrates multiple technologies to ensure effective crisis communication.

6.3.5 Project to implement video transmission via 5G networks for the Integrated Rescue System

The project to implement video transmission via 5G networks for the Integrated Rescue System (IRS) has several key objectives that are essential for improving crisis communication and increasing the effectiveness of emergency response operations. The main objective of the project is to enable IZS units to respond more quickly and effectively to crisis situations. Thanks to live video transmission from the scene of the incident to control rooms and other coordination centres, emergency responders can obtain up-to-date and accurate information in real time. This enhances the ability to make rapid and informed decisions.

Effective coordination between the various emergency services (fire brigade, police, ambulance service) is essential for the successful management of crisis situations. The project aims to improve communication and cooperation between these services through the integration of advanced technologies. Real-time video transmission ensures that all units have access to the same information, which

facilitates coordination and reduces the risk of misunderstandings. Another objective of the project is to ensure high-quality and stable video transmission from the scene of the incident

to control centres. LiveU technology and 5G networks provide high-speed, low-latency data transmission. The use of multiple transmission paths (WiFi, 4G, 5G) ensures transmission stability even in challenging conditions.

Data security and protection are crucial aspects of emergency communications. The project aims to ensure that all video transmissions are encrypted and secured against unauthorised access. LiveU technology utilises its own patented LRT (LiveU Reliable Transport) protocol, which provides a high level of security and transmission reliability. Another objective of the project is the flexibility and scalability of the system. The system is designed so that it can be easily adapted to changing needs and expanded according to current requirements. The modular solution and the ability to quickly change the configuration allow for easy deployment of the technology in various situations and environments.

The project supports various use cases, such as telemedicine, remote support for surgical procedures, and hospital emergency departments. Real-time video transmission not only improves emergency communications but also enables rapid and effective decision-making across a range of areas. Another objective is to ensure the project's full integration with existing emergency services systems. This includes compatibility with various types of devices and transmission channels, ensuring a smooth transition to new technologies without the need for extensive modifications to the existing infrastructure. The project also includes demonstrations and practical tests of the technology in real-world conditions. These tests will help to verify the system's functionality and performance, identify any potential issues, and optimise the technology for maximum efficiency and reliability.

6.3.6 Key components of the project

The project to implement video transmission over 5G networks for the integrated emergency response system comprises several components to ensure effective and reliable emergency communications. These components include LiveU technology, 5G networks and LiveU mobile encoders, which together enable real-time video transmission from the scene of an incident to control rooms and other coordination centres.

6.3.6.1 LiveU technology

LiveU is a world leader in live video transmission over mobile networks. This technology provides secure, professional-quality video transmission. LiveU uses the H.265 HEVC codec, which enables transmission in HD or 4K quality with an adjustable bitrate of up to 70 Mbit/s. This system is modular, allowing for quick and easy reconfiguration of components as required. LiveU technology has been proven in practice, including deployment in war zones and during natural disasters, demonstrating its reliability and robustness.

The accompanying image illustrates a system for transmitting video from the scene of an incident to emergency services control centres using LiveU technology. This system ensures effective emergency communication between emergency services units, such as the fire brigade, police, ambulance service and hospitals.

Drones and PTZ cameras at strategic locations capture video and transmit it in real time. Cameras mounted on emergency vehicles and body-worn cameras (BodyCams) on emergency personnel's uniforms provide vital footage directly from the field. The LiveU mobile encoder transmits the video signal from various sources to a secure network via WiFi, 4G and 5G. The patented LRT protocol ensures reliable and secure video transmission.

The LiveU Decoder decodes the video signal and enables it to be displayed on monitoring devices in the control room.

LiveU Ingest automatically records and stores the received video, whilst Video Return enables video to be broadcast back to the scene of the incident for better coordination.

Video transmission enables hospitals' A&E departments to prepare for the arrival of injured patients. The control centre monitors and coordinates the response of emergency services. A mobile control centre equipped with LiveU technology transmits video directly from the field. The Video Management System manages and analyses received video and enables it to be shared. Monitoring on a tablet or mobile phone increases mobility and the availability of information for emergency responders.

6.3.6.2 5G networks

The use of 5G technology is a key element of the project, as it enables high-speed data transmission with low latency. 5G networks provide extensive geographical coverage and support a massive number of connected devices. Network Slicing technology, which is part of 5G, allows the network to be logically divided into multiple virtual segments that can be utilised by different service providers. Each "slice" can be configured to meet specific requirements for bandwidth, latency and security.

6.3.6.3 LiveU mobile encoders

LiveU mobile encoders, also known as "backpacks", enable the transmission of video signals from the field. These encoders support various connection types, including LTE, 5G, Wi-Fi and satellite links. They are equipped with touchscreens and allow for

transmissions in various quality

and bitrates, ensuring high flexibility and reliability. For example, the LU600 is a compact, native 5G 4K HDR HEVC field unit for live streaming with top performance in HEVC bonding. It offers a maximum bitrate of up to 70 Mbps and the transmission of 1–4 video channels.

6.3.6.4 Real-time video transmission

By utilising LiveU technology and 5G networks, it is possible to transmit video from incident locations in real time to control rooms and other coordination centres, which improves the situation on the ground and enables faster and more effective decision-making.

6.3.6.5 Improved coordination

Real-time video and audio enable better coordination between different emergency services, leading to faster and more effective response. Real-time video transmission ensures that all units have up-to-date and accurate information.

6.3.6.6 Safety and security

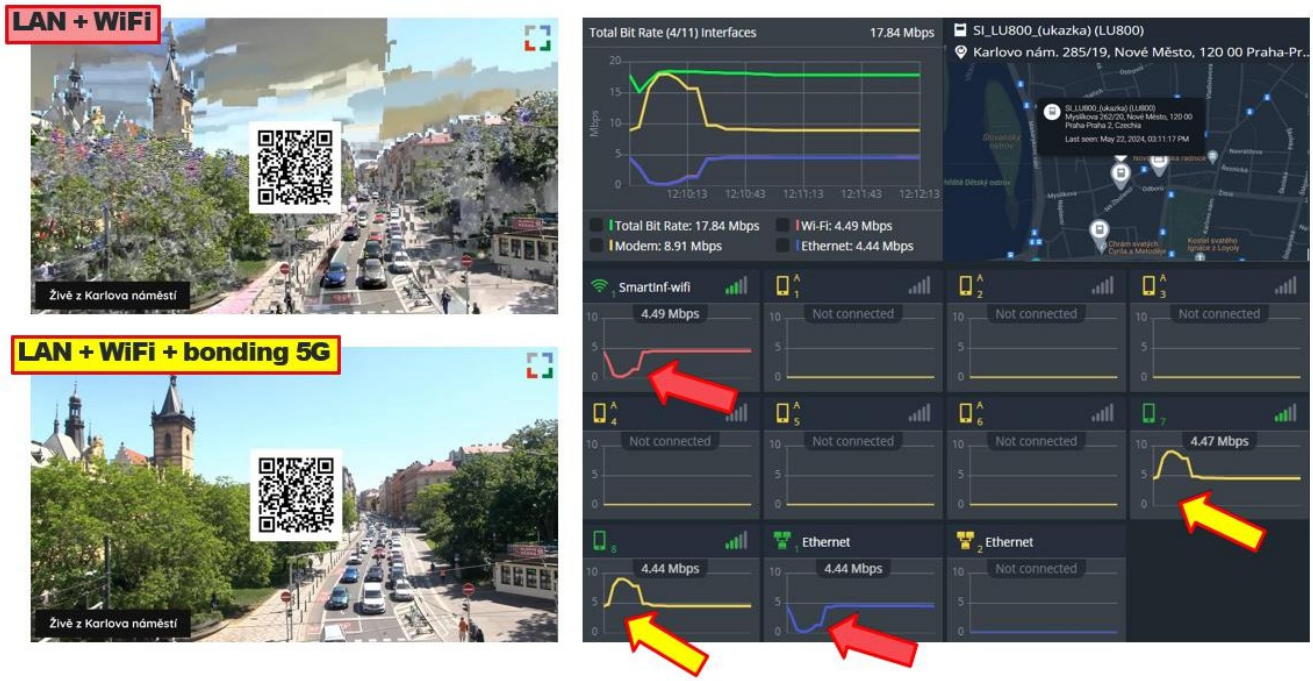
Transmissions are encrypted and secured, ensuring the protection of sensitive information. LiveU technology utilises its own patented LRT protocol for transmission over unguaranteed connections with a high level of security, AES-128 encryption, stability even in challenging conditions, and dynamic error correction.

6.3.6.7 Flexibility and scalability

Modular solutions and the ability to quickly change configurations allow for easy adaptation to changing needs and rapid capacity expansion. The system is designed to be easily scalable and adaptable to the specific needs of various situations.

6.3.6.8 Wide range of applications

The project supports various use cases, including telemedicine, remote surgical support and hospital A&E departments. Real-time video transmission not only improves emergency communication but also enables rapid and effective decision-making across various sectors.



The image demonstrates the benefits of combining transmission technologies to ensure high-quality video transmission.

The top part of the image shows data transmission using only LAN and WiFi. The video quality is clearly impaired and the image is pixelated, indicating problems with transmission capacity and connection stability.

In contrast, the lower part of the image shows data transmission using a combination of LAN, WiFi and 5G with bonding technology. The video quality is significantly better here; the image is clear and stable.

The use of multiple technologies ensures higher overall transmission capacity and connection stability, which is key to reliable video transmission even if one of the technologies fails.

7 Potential for further technological development

With growing demands on bandwidth, data transfer speeds and communication security, it is essential that the technologies used by these agencies are constantly developed and modernised. Advances in communication technologies enable not only faster and more reliable communication, but also the integration of advanced applications and data services that can significantly improve the coordination and efficiency of rescue operations.

Modern emergency scenarios require communication that goes beyond traditional voice services and involves the transmission of large volumes of data, such as video footage, sensor data and real-time information from the field. Technological advances, particularly in the field of mobile broadband networks such as LTE and the upcoming 5G, offer enormous potential for improving these capabilities. Broadband technologies provide higher capacity and data transfer speeds, enabling emergency responders to access critical information in real time and improving their ability to make decisions based on up-to-date data.

One aspect of further development is the transition to 5G technologies, which promise significant improvements not only in network speed and capacity, but also in their reliability and latency. 5G technology will enable the deployment of new applications, which may include, for example, remote medical diagnostics, autonomous drones for surveying hazardous areas, or augmented reality for better orientation in the field.

The security of communication networks is another area that must be addressed in the context of technological development. With the growing volume of data transmitted and its sensitivity, it is essential to ensure a high level of protection against cyber threats and data loss. Modern encryption technologies and security protocols play a key role in protecting communications and maintaining the integrity of information.

Another key area is the modernisation of the end-user devices used by members of the security and emergency services. New devices must not only be capable of utilising advanced communication technologies, but also be resilient to the demanding conditions in which these professionals often work. Key factors include ergonomics, robustness and long battery life, which influence the effectiveness and reliability of these devices.

Overall, it can be said that technological developments in mobile communications for the emergency services present many challenges, but at the same time open up new opportunities for improving crisis management and rescue operations. The integration of modern technologies, such as 5G networks, advanced applications and security protocols.

7.1 The transition to 5G

7.1.1 Technological Aspects of the Transition to 5G

Higher speed and data capacity: 5G networks provide much higher data transfer speeds than 4G networks, enabling faster transmission of large volumes of data, such as video recordings and sensor data. This improved capacity is useful for applications requiring immediate response and high data throughput, such as drones, wearable devices and advanced sensor systems.

Low latency: Latency is the time it takes for data to travel from one point to another. 5G technology reduces latency to a few milliseconds, which is essential for applications requiring immediate response, such as remote control of robots and drones or real-time video communication between emergency responders in the field.

Reliability and availability: 5G networks are designed to provide a high level of reliability and availability. This includes robust infrastructure capable of withstanding various types of outages and crisis situations, such as natural disasters or terrorist attacks. This is made possible, for example, through the use of backup systems and temporary coverage sites.

Support for advanced applications: With the transition to 5G technology, it is possible to deploy new types of applications that

would not be feasible on older networks. These applications include remote medical diagnostics, autonomous exploration of hazardous areas using drones, augmented reality for better navigation in the field, and many others.

Energy efficiency: 5G technology is designed with a focus on energy efficiency, meaning lower energy consumption for data transmission compared to previous generations of mobile networks. This is particularly important for deployment in remote areas and for devices with limited battery capacity.

Flexible network architecture: 5G networks are based on a flexible architecture that allows for the dynamic allocation of resources according to current needs. This means the network can be optimised for various types of services, such as voice calls, video streaming and data from IoT devices.

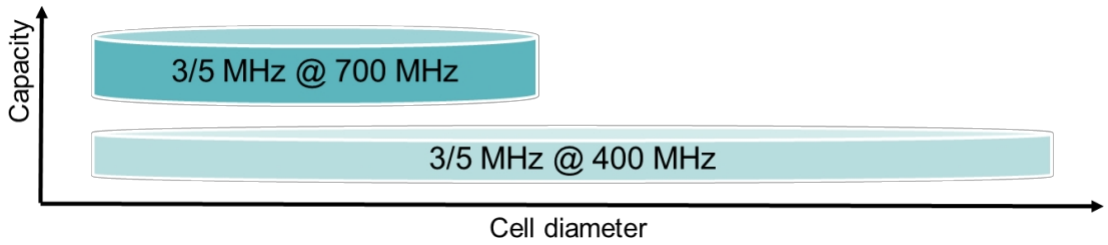
Edge computing: The integration of edge computing with 5G networks enables data to be processed closer to where it is generated, significantly reducing latency and increasing the speed of response to emergencies.

Advanced mobile high-speed networks*: Mobile broadband focuses on human-centric use cases for accessing multimedia content, services and data. Demand for mobile broadband will continue to grow, leading to advanced mobile high-speed networks. This use case will bring new application areas and requirements alongside existing mobile broadband applications to improve performance and deliver an increasingly seamless user experience. This use case encompasses a range of scenarios, including broadband coverage and hotspots, which have different requirements. In areas with high user density, very high transmission capacity is required, whilst the demand for mobility is low and user data rates are higher than for broadband coverage. For broadband coverage, seamless coverage and medium to high mobility are desirable, with significantly improved user data rates compared to existing data rates. However, the requirement for data rate may be relaxed compared to user density.*

Highly reliable, low-latency communication*: This use case has strict requirements for capabilities such as throughput, latency and availability. Some examples include wireless control of industrial production or manufacturing processes, remote medical operations, smart grid distribution automation, transport safety, etc.*

Massive machine-to-machine/device communication*: This use case is characterised by a very large number of connected devices, which typically transmit relatively low volumes of data that are not sensitive to delay. The devices must be low-cost and have a very long battery life.*

7.1.2 The impact of the radio spectrum on the number of base stations required for the same area coverage



Dedicated network in the 700 MHz guard bands

Cell diameter of around 15 km

Bandwidth of 3 or 5 MHz (B28 or B68) Guaranteed

maximum internet speed of up to 35 Mbit/s 1,300–1,700

eNBs to cover 95% of the territory

Seamless cross-border cooperation

Standard terminals compatible with Tetrapol

BBPPDR 400 MHz – dedicated network

Cell diameter up to 35 km

Bandwidth currently 3 MHz, with a future target of 5 MHz

Guaranteed maximum internet speed of up to 35 Mbit/s

850–1,100 eNBs to cover 95% of the territory

No interworking at borders – must be addressed with special coverage and routing Standard

terminals compatible with Tetrapol

7.1.2.1 Maximum radiated power

Comparison made in the context of experience with existing technology in the 380 MHz band versus services in the 410 MHz and 450 MHz bands.

Článek 6
Konkrétní podmínky pro terminály v sítích zvláštního určení

(1) Pomocí terminálů je možno využívat rádiové kmitočty v těchto úsecích rádiového spektra:

Ozn. úseku	Kmitočtový úsek – vysílání[24])	Kmitočtový úsek – příjem[24])	Max. vyzářený výkon terminálu	Určení	Pozn.
a	148,200–149,050 MHz	152,800–153,650 MHz	10 W e.r.p.	železniční doprava	
a1	148,200–149,050 MHz				
c1	152,800–153,650 MHz				
e	380,000– 384,9875 MHz	390,000– 394,9875 MHz	10 W e.r.p.	integrovaný záchranný systém	technologie TETRAPOL [25])
f	457,400–458,450 MHz	467,400–468,450 MHz	6 W e.r.p.	železniční doprava	
g1	876,0125 MHz, 876,025 MHz, 876,0375 MHz, 876,05 MHz, 876,0625 MHz			železniční doprava	technologie GSM-R – DMO
g2	876,1–880,1 MHz	921,1–925,1 MHz			technologie GSM-R

For the 380 MHz band, where the TETRAPOL system is operated, the maximum radiated power of terminal equipment is 10 W.

Source: ČTÚ – VO-R/1/12.2018-8 valid as of 18 December 2018

For the TETRA system and narrowband technology in the 410 MHz band, similar parameters apply to those for TETRAPOL technology shown in the figure below.

Článek 4
Konkrétní podmínky pro terminály pozemních mobilních sítí využívajících úzkopásmovou technologii

(1) Pomocí terminálů je možno využívat rádiové kmitočty v těchto úsecích rádiového spektra:

Ozn. úseku	Kmitočtový úsek – vysílání	Kmitočtový úsek – příjem	Typ sítě
a	410,0–419,8 MHz	420,0–429,8 MHz	TETRA[8])
b	455,74–457,38 MHz	465,74–467,38 MHz	PMR/PAMR[9])

(2) Terminály lze provozovat s vyzářeným výkonem maximálně 10 W e.r.p.

(3) Efektivní výška antény nepohyblivých terminálů v úseku *b,* vypočtená metodou podle Doporučení ITU-R P.1546, může být nejvýše 30 m.

[8]) Terrestrial Trunked Radio – pozemní svazková rádiová síť.
[9]) PMR – Private Mobile Radio, soukromé nebo firemní pohyblivé rádiové sítě a spoje; PAMR – Public Access Mobile Radio, sítě PMR s přístupovým bodem do veřejných sítí.

Source: ČTÚ - VO-R/1/12.2018-8 valid as of 18 December 2018

For bands based on the LTE standard at 410 MHz and 450 MHz, the maximum permissible radiated power of terminal equipment is 2 W (for channels narrower than 200 kHz; otherwise, only 1 W).

Článek 3

Konkrétní podmínky pro terminály širokopásmových mobilních a přístupových sítí

(1) Pomocí terminálů je možno využívat rádiové kmitočty v těchto úsecích rádiového spektra:

Ozn. úseku	Kmitočtový úsek – vysílání	Kmitočtový úsek – příjem	Další upřesnění v odstavci:
a	410–419,8 MHz	420–429,8 MHz	2
b	450–460 MHz	460–470 MHz	2
c1	703–733 MHz	758–788 MHz	2

(2) Terminály v úsecích *a* až *g2* využívající šířku rádiového kanálu > 200 kHz lze provozovat s vyzářeným výkonem maximálně 1 W e.r.p. Tato hodnota musí být dodržena při jakékoliv kombinaci výstupního výkonu terminálu a použité antény. Terminály v úsecích *a, b, d, e* využívající šířku rádiového kanálu ≤ 200 kHz lze provozovat s vyzářeným výkonem maximálně 2 W e.r.p.

Source: ČTÚ - VO-R/1/12.2018-8 valid as of 18 December 2018

7.1.3 Standards

Standardisation is a key element in ensuring compatibility and interoperability between different devices and systems. Standardisation enables different organisations and countries to cooperate effectively and share resources in emergency situations. Organisations such as 3GPP (Third Generation Partnership Project) play a vital role in the development and implementation of these standards.

7.1.3.1 3GPP standards for PPDR

3GPP develops standards for mobile communications, which include specifications for public safety and critical communications. Release 13 and later include features specifically designed for PPDR. 3GPP Release 13 also introduces new features for 5G RAN, such as new types of antennas, a new mmWave band and new methods of accessing the radio spectrum.

The most commonly applied MC (Mission Critical) services relate to[11] :

Mission Critical related items

General aspects of Mission Critical improvements

- Re-organising the MCPTT Stage 1 documents
- Re-organising the MCPTT Stage 2 documents
- MCPTT document structure

Mission-Critical Push-to-Talk over LTE Realignment

[11] https://portal.3gpp.org/desktopmodules/Specifications

Mission Critical Services Common Requirements Mission

Critical Video over LTE

Mission Critical Data over LTE

Common functional architecture to support mission-critical services Enhancements

for Mission-Critical Push-to-Talk

Enhancements to MCPTT

Enhancements to MC Data

Enhancements to MC Video

Other Mission Critical Enhancements

– MC Security Enhancements
– MBMS usage for MC communication services

7.1.3.2 Support for standards in 5G networks

5G technologies include advanced features and standards that support PPDR requirements. These include:

QoS (Quality of Service): Ensuring that voice, data and video services are prioritised and delivered with a high level of reliability and low latency.

Proximity Services (ProSe): Enables direct communication between devices without the need for network infrastructure, which is useful in situations where the network is unavailable or overloaded.

Isolated Operation for Public Safety (IOPS): Enables network nodes to operate independently in the event of disconnection from the main network, thereby ensuring service continuity even in crisis conditions.

Standardisation also facilitates international cooperation and interoperability between different countries. Projects such as the European Broadway initiative, which focuses on creating 'borderless' broadband critical communications, are an example of how standardisation supports coordination and resource sharing at an international level.

When introducing new standards, it is important to ensure backward compatibility with existing systems so that the transition to new technologies is smooth and service continuity is maintained. This includes interoperability with already established systems such as TETRA and P25, which are widely used in current PPDR systems.

7.1.4 Applications

Augmented reality (AR) enables emergency responders and security personnel to better navigate the terrain by providing vital information in real time directly into their field of view. AR applications can display navigation instructions, identify hazards, show building plans and provide first aid instructions, thereby increasing situational awareness and the effectiveness of rescue operations. Autonomous drones play a key role in surveying hazardous areas where deploying human personnel would be too risky. Drones equipped with cameras and sensors can provide live video footage and sensor data to aid decision-making and the coordination of rescue operations. Furthermore, drones can deliver medicines, medical equipment or other essential supplies to hard-to-reach areas.

5G technology enables real-time remote medical diagnosis, which can be utilised to provide rapid and effective medical care in emergency situations. Healthcare professionals can consult with specialists remotely via video conferencing and real-time data transmission, diagnose patients and provide first aid guidance. This technology can significantly improve treatment outcomes and save lives. Wearable technologies, such as smartwatches and medical sensors, can monitor the health of emergency responders and provide real-time data on their physiological parameters. This data can be analysed to detect fatigue, stress or other health risks.

Smart sensors and IoT devices can monitor the environment and provide important data such as temperature, humidity, the presence of hazardous substances and more. This data can be transmitted in real time to control centres, where it is analysed to improve decision-making and the coordination of rescue operations. IoT technologies also enable the tracking and management of resources such as vehicles and equipment, which improves logistics and the efficiency of operations. Advanced communication platforms based on 5G technologies provide integrated voice, data and video services that enable effective communication between all participants in rescue operations. These platforms support features such as group communication, call prioritisation and secure data transmission.

7.1.5 Data services

5G technology is revolutionising data services. Thanks to the high speed and capacity of 5G networks, emergency responders and security services can transmit and receive vast amounts of data in real time. This includes live video footage, photographs, maps, documents and other vital information.

One of the main benefits of 5G data services is the ability to analyse data in real time. This enables security and emergency services to assess situations immediately and respond to them with accurate information. Sensors and IoT devices deployed in the field can collect environmental data such as temperature, humidity, air quality and the presence of hazardous substances. This data is then transmitted to control centres, where it is analysed and used to optimise emergency operations.

Another significant aspect of 5G data services is the support for a large number of devices connected to the network simultaneously. This is practical for deploying extensive networks of sensors and other IoT devices that monitor and report on the situation in real time. This capability enables the creation of a comprehensive and detailed picture of the situation.

5G technology also ensures a high level of data security. Modern encryption methods and security protocols protect sensitive information from cyber-attacks and unauthorised access, and also serve to protect personal data and sensitive information, which are often part of communications between security and emergency services.

Another key feature of 5G data services is the ability to prioritise traffic. This means that during emergency situations, data from emergency services and security agencies can be transmitted with priority, ensuring that critical information is delivered without delay.

7.1.6 End-user devices

The new generation of PPDR end devices incorporates advanced communication technologies that support voice, data and video services on 5G networks. These devices must be capable of handling the high data transfer speeds and low latency offered by 5G.

These include, for example, smartphones, tablets and wearable technologies that are optimised for the demanding conditions of emergency management.

7.1.6.1 Robustness and durability

End-user devices used in PPDR must be designed to withstand the extreme conditions in which emergency responders often work. This includes resistance to water, dust, impacts and extreme temperatures. The devices must also be ergonomic so that they can be used comfortably for long hours, and must have a long battery life to remain operational during lengthy operations without the need for frequent recharging.

7.1.6.2 Security features

Security is also a key consideration for end-user devices. They must be equipped with advanced encryption technologies and security protocols that protect communications from cyber threats. In addition, devices should have multi-level authentication mechanisms, such as biometric verification and multi-factor authentication, to ensure that only authorised persons have access to the device and the data being transmitted.

7.1.6.3 Interoperability and compatibility

End devices must be interoperable with the various systems and technologies used in PPDR. This includes compatibility with various communication protocols, such as MCPTT, MCData and MCVideo, which are standardised within 3GPP. Interoperability ensures that devices can communicate effectively with different systems and devices.

7.1.6.4 Integration with IoT and sensors

Modern end devices should be capable of integrating with various IoT devices and sensors that provide real-time data. This includes environmental monitoring sensors, medical sensors and other IoT devices that can improve situational awareness and operational efficiency. Devices should be capable of collecting, analysing and visualising data from these sensors.

7.2 Integration and interoperability

7.2.1 Options for integrating existing and new systems

Integrating existing systems with new 5G technologies presents one of the greatest challenges in modernising communication systems for security and emergency services. The aim is to ensure a smooth transition that minimises service disruptions whilst maximising the benefits of new technologies. This process requires thorough planning and careful execution to ensure operational continuity and the utilisation of new functionalities.

To ensure seamless integration, new 5G devices must be compatible with existing communication systems. This encompasses both hardware and software, enabling the coexistence of older and newer technologies during the transition period. Modern communication devices must be capable of operating in hybrid mode, where they can communicate via both existing networks and new 5G networks. This approach ensures that security and emergency services can gradually transition to new technologies without disrupting their operational activities.

The use of middleware and software gateways can facilitate the integration of different systems. These technologies enable data transfer between incompatible systems and ensure that information can be shared and utilised across different platforms. Middleware can be designed to support various communication protocols and data formats, which facilitates integration and increases the flexibility of the entire system. This not only improves efficiency but also reduces the costs of transition, as it is not necessary to replace all existing systems at once.

Standardised application programming interfaces (APIs) enable the easy integration of various applications and systems. APIs provide defined methods of communication between different software components, allowing developers to easily integrate new features and applications into existing systems. The use of open standards for APIs ensures interoperability and enables collaboration between different manufacturers and developers.

One aspect of integration is the ability to effectively manage and integrate data from various sources. This involves not only technical solutions for data transfer and processing, but also ensuring data integrity, quality and security.

7.3 Building a resilient ecosystem for emergency communications

The development of broadband systems for emergency communications is not merely a choice of technology, but also involves important organisational, operational and technical considerations. Historically, public safety networks and organisations were often decentralised, sometimes by geographical area or discipline. However, collaboration between different disciplines and the need for interoperability have gradually become essential, leading most governments to establish dedicated organisations and systems. The transition to the 3GPP ecosystem opens up new opportunities for telecommunications providers and calls into question the relevance of these dedicated organisations and systems.

Challenges and opportunities for public safety authorities: Public safety authorities will face many challenges and opportunities during the transition to broadband systems. A key factor for success is user involvement before, during and after the system deployment and operation process, as well as their active participation in shaping network reinvestments and evolutions. For organisations driven by the needs of a large number of commercial users rather than a small number of public safety users, there will always be a tendency to prioritise the needs of commercial users, which may conflict with public safety requirements.

Market fragmentation: Business-critical and emergency applications are converging towards the same 3GPP-based technologies. This opens up new opportunities for players such as mobile network operators (MNOs), private network providers, equipment manufacturers and others. However, how can governments ensure the highest levels of confidentiality, security and interoperability of services for their users if more third parties are involved, particularly if solutions may prioritise profitability over the public interest?

Budget: Public safety authorities must secure sufficient budgets to build and operate the components of the emergency network whilst ensuring the cost-effectiveness and financial viability of the new network. Investment in existing systems has often focused on the development and deployment phases, leading to high operational costs due to a limited supplier ecosystem. In contrast, the broadband emergency communications environment involves a greater diversity of stakeholders, which should lead to lower costs.

Ecosystem orchestration: Building and operating emergency communication systems requires the orchestration of a large ecosystem of partners. An end-to-end vision of the network and services is essential to ensure performance and flexibility and to avoid vendor lock-in. Creating a robust ecosystem that includes a wide range of stakeholders can help public safety authorities avoid long-term vendor lock-in, as has been the case in some countries.

Technology: Public safety authorities will need to ensure that networks are resilient and designed for maximum performance, resilience, reliability, security, interoperability and the ability to evolve. The standardisation of broadband services is still evolving, meaning that technologies are not yet mature enough to support all the requirements and applications of emergency communications. Public safety authorities must ensure that the networks used are robust and resilient to future technological changes, new solutions and interconnection possibilities within broader ecosystems, including international cooperation.

User adoption and adaptation: End users – from command centres to first responders across all disciplines – must be at the heart of the transformation journey, from the design of systems and services through to appropriate training and change management. Public safety agencies are generally attached to their existing communication tools and solutions, and it will therefore be a challenge for authorities to convince users of the need for evolution or the approach to evolution. A change management campaign will be essential to secure consensus and support from all users across different geographical areas to ensure a smooth transition period.

Migration and timing: The design, deployment and testing of a new end-to-end crisis communication system takes several years. Furthermore, the migration of all disciplines to new equipment, services and processes requires careful planning. Timing is crucial for a smooth transition to new technologies. The challenge is to ensure that authorities act without delay to embark on the transformation journey, plan the migration of systems and equipment, and manage technological evolution, whilst securing user trust and international integration within the wider ecosystem.

7.4 Examples of 5G applications for various crisis management units

7.4.1 Police forces

Live streaming from in-car and body-worn cameras: 5G technology enables police units to transmit live video feeds from in-car and body-worn cameras in real time to central control centres. This allows for better situational awareness, immediate response and coordination based on up-to-date visual information from the field.

Biometric sensors and location tracking: The use of biometric sensors combined with location tracking technologies enables real-time monitoring of individual officers' health and location. This data can be used to ensure the safety and efficiency of operations.

Predictive threats and risk assessment: Using advanced analytical tools and artificial intelligence, police forces can predict potential threats and assess risks based on various data inputs. This enables preventive measures and a rapid response to potential dangers.

Smart city monitoring: The integration of sensor networks and cameras within the smart city concept enables the police to monitor various areas of the urban environment in real time. This enhances the safety and efficiency of police operations.

Real-time tracking of field officers: 5G technology enables the precise and real-time tracking of field officers, improving the coordination and effectiveness of operations. Command centres can better manage the deployment of personnel and resources according to current needs.

7.4.2 Fire brigades

Connected helmets: Firefighters can use connected helmets equipped with cameras and sensors that transmit data in real time to control centres. This enables better situational awareness in the field and more efficient management of operations.

Rugged tablets and smartphones: The use of rugged mobile devices, designed for demanding conditions, allows firefighters to access digital tools and information directly at the scene of the incident.

Autonomous drones: Drones can be used to survey hazardous areas, detect fires and provide live video footage from locations that are difficult for firefighters to access. This enhances the safety and efficiency of operations.

3D mapping and indoor positioning: Using 3D mapping and indoor positioning technologies, firefighters can gain an accurate overview of the situation inside buildings. This facilitates navigation and the planning of operations.

Live streaming of operations: 5G technology enables the transmission of live video footage from operations, which improves coordination between different units and control centres.

7.4.3 Health and emergency services

Connected ambulances with video calls to hospitals: Ambulances equipped with 5G technology can transmit data and video footage in real time directly to the hospital. This allows doctors to prepare for the patient's arrival and provide guidance during transport.

Sensors on patients: Sensors on patients can monitor vital signs and health status in real time. This data can be transmitted to the hospital, allowing doctors to monitor the patient's condition even before their arrival.

Protection against violence: Healthcare staff can be equipped with devices that provide protection against violent attacks during interventions. This includes emergency buttons and monitoring systems.

Support during remote operations: Remote support from medical specialists during operations can be provided via video links and real-time consultations. This improves the quality of medical care in the field.

Mobile access to patient data: Healthcare professionals can access patients' electronic health records directly in the field, enabling better and faster decision-making.

7.5 Other sectors (defence, customs, etc.)

Officers equipped with **connected devices:** The use of connected devices allows officers to access data and communicate in real time, improving the efficiency and coordination of operations.

Tactical information sharing: Real-time sharing of tactical information between different agencies ensures better coordination and effectiveness of operations.

Automated reporting: Automating reporting processes reduces the administrative burden and allows for greater focus on operational activities.

Maintenance and predictive logistics: Predictive maintenance and logistics enable better planning and problem prevention, ensuring smooth operations and the availability of necessary equipment.

Mobile office: Mobile devices enable officers to work effectively from various locations, increasing their flexibility and availability.

8 Examples of PPDR network solutions abroad

This chapter provides an overview of PPDR systems abroad. It describes the legislative and technological aspects of solutions implemented in various countries. It is important to note that there is no standard procedure for deploying PPDR networks, as each solution is specific to a particular country and its needs. This ensures that the systems are tailored to local legislative requirements, technological capabilities and the operational needs of emergency services and other security agencies.

8.1 Germany – Digitalfunk BOS

Germany has decided to modernise its public safety communication system through the implementation of the Digitalfunk BOS system. This system was developed to ensure reliable and effective communication for all emergency and security services at federal, state and local levels. Digitalfunk BOS is managed by the Federal Office for Digital Radio of Security Services (BDBOS), which was established in 2007 with the aim of building, operating and developing this system on a long-term basis.

BOS digital radio is based on TETRA (Terrestrial Trunked Radio) technology, which is the international standard for digital radio communication. This system enables effective and secure communication, which is essential for emergency services such as the police, fire brigades, rescue services and disaster management authorities. The system provides both voice communication and data transmission, enabling a flexible and rapid response in crisis situations.

The main objective of Digitalfunk BOS is to ensure reliable communication even under the most demanding conditions. The system comprises more than 5,000 base stations covering the whole of Germany and includes several regional and transit switching centres that facilitate data and voice transmission between different regions. Users of the system utilise various types of end devices, such as portable and vehicle-mounted radios, which enable direct communication within the system.

The main users of BDBOS include: State

police forces; the Federal Police;

the Federal Agency for Technical Relief (THW); the

Federal Customs Administration;

Public fire brigades and company fire brigades established or recognised under state law;

Federal and state disaster control and civil protection authorities, and federal and state constitutional protection authorities.

Digitalfunk BOS represents a major advance in the field of communications for emergency and security services in Germany. Thanks to advanced technology and a robust infrastructure, the system offers several key advantages. A high level of security is ensured by advanced encryption methods that protect communications between users from unauthorised access. The reliability and availability of the system are ensured by emergency power supply systems, which guarantee uninterrupted service even in crisis situations, including power cuts.

The system is also designed to be compatible with similar systems in other countries, enabling international cooperation and the management of cross-border crisis situations. Digitalfunk BOS is flexible and scalable, allowing for easy expansion and adaptation to the changing needs and requirements of security forces and other users.

This modern communication system is designed to meet the demanding requirements of public safety communications and to ensure effective and rapid communication even in crisis situations, which is key to safeguarding the safety of citizens. Digitalfunk BOS represents a strategic step towards strengthening the efficiency and reliability of Germany's communication infrastructure.

8.1.1 Development and transition to the dedicated Digitalfunk BOS broadband network

Mobile broadband communication offers emergency services many new ways to effectively help people, save lives and ensure safety. To achieve this, a dedicated broadband network infrastructure is essential.

The use of messenger services, sending and receiving situation and search information, querying databases, transmitting vital data and live video streams – these new applications can support the police, fire services and rescue services in various ways to successfully complete their missions. The technical capabilities include highly integrated systems that can provide relevant information to a large number of users simultaneously and in real time. Modern mobile data communication enables people to quickly obtain the help they need.

The current TETRA standard, on which BOS digital radio is based, utilises the available technical potential for voice and short data transmission, but broadband data transmission is not technically feasible. Some federal states are therefore temporarily relying on commercial mobile networks as an interim solution. However, these networks are neither secure nor reliable enough for critical communications. Germany, together with the federal and state governments, is therefore planning to build its own BOS broadband digital radio network.

8.1.1.1 Building its own BOS broadband network:

Phase 0: Preparation and use of commercial networks:

In Phase 0, emergency services will be able to roam and use additional functions via commercial mobile networks. The individual contracts that the federal government and many federal states have concluded with commercial mobile operators will be consolidated.

Phase 1: Construction of the core broadband network

Phase 1 involves the start of construction of the planned broadband network. A dedicated broadband backbone network will be developed and built. During this phase, the radio and access networks of commercial mobile operators will continue to be used.

Phase 2: Expansion of the company's own network

In Phase 2, the company's own radio and access network will be gradually built across Germany in cooperation with federal and state governments.

Phase 3: Transition and migration of services

In Phase 3, the use of commercial networks will be gradually reduced and voice services will be migrated. All voice and data communication in the BOS digital radio system will take place via the BOS's own broadband network. The TETRA system technology will be phased out. The start of this phase is planned for the early 2030s.

8.1.2 Digitalfunk BOS technical infrastructure

8.1.2.1 Operational and access network

The Digitalfunk BOS core and access network comprises more than 5,000 base stations (TETRA Base Stations – TBS) covering the whole of Germany. These base stations are deployed in individual network cells and ensure the transmission of voice and data between users and the network's central nodes. Each base station processes incoming and outgoing communications within its cell, enabling effective coordination and rapid response by security forces in the field.

8.1.2.2 Core network

The core network is the central part of the Digitalfunk BOS system and ensures the transmission of data and voice between different regions. The system comprises 64 regional switching centres (Digital Exchange for TETRA – DXT) and 4 transit switching centres (Digital Exchange for TETRA Transit Type – DXTT), which provide interconnection between regional centres and enable inter-regional communication. The core network also contains systems for managing all devices and user groups, as well as central control centres that oversee the entire system.

8.1.2.3 End-user devices

Users of the Digitalfunk BOS system utilise various types of end devices, including portable and vehicle-mounted radios, as well as fixed radios in control centres. These devices enable direct communication within the system, both in Trunked Mode Operation (TMO) and Direct Mode Operation (DMO), which allows communication between devices without using the network infrastructure. In Trunked Mode Operation, the device communicates with the nearest base station, which relays voice and data information further into the network.

8.1.2.4 Frequency

The Digitalfunk BOS system uses a specific frequency band to ensure secure and reliable communication. Base stations transmit in the downlink band in the 390–395 MHz range, whilst end devices transmit in the uplink band in the 380–385 MHz range. The 406.1–410 MHz frequency band is used for direct communication between devices (Direct Mode Operation – DMO).

8.1.2.5 Power supply

To ensure uninterrupted operation even in the event of power failures, the Digitalfunk BOS infrastructure is equipped with emergency power supply systems. These include uninterruptible power supplies (UPS) and emergency power supply systems (NEA), which provide long-term power via diesel generators. These measures ensure that the system remains operational even in crisis situations.

8.1.3 Key Digitalfunk BOS services

The Digitalfunk BOS system provides a wide range of key services that support the effective operation of security forces and ensure public safety. These services include basic voice communication, advanced data services, and various other functions that enable rapid information transfer and coordination.

8.1.3.1 Group communication

Group communication involves point-to-multipoint connections for voice communication between multiple communication partners. Group calls are conducted using a round-robin speaking order, meaning there is one speaking participant and several listening participants. The role of the speaker may change, but simultaneous speaking and listening is not possible.

Group communication can be used for any group nationwide across the entire network or within a geographically limited call area. Participants may be members of several groups at the same time, but can only be active in one group at a time, i.e. they are either speaking or listening. Group communication management is supported by tools for administering group membership and call areas.

8.1.3.2 Individual communication

Individual communication is a point-to-point connection for voice communication between two participants, similar to a telephone call. Individual calls can be made using alternate speaking (i.e. only one person can speak at a time) or two-way speaking (i.e. both can speak simultaneously). The communication partners may both be on the BOS digital network, or one may be outside it, for example on a fixed telephone network. Management of individual communication usage is supported by tools for managing permissions.

8.1.3.3 Emergency services

In addition to standard emergency calls, emergency services also include two other types of emergency service: priority reporting and local calls for assistance.

When an emergency call is initiated by pressing the emergency button on a radio device, existing calls may be interrupted and the emergency call is given priority. Furthermore, when an emergency call is sent, the sender’s current GPS position is automatically transmitted, enabling their location to be determined. The tactical status ‘Emergency’ is also automatically sent. The voice portion of the emergency call, the location and the tactical status are automatically routed to the relevant local emergency response centre.

The priority message is broadcast by the control centre with emergency call priority. Thanks to this priority, it interrupts all other calls except emergency calls. It is used to convey urgent information to the responding units

Local calls for assistance are also included in emergency services, but do not have emergency call priority. Local calls for assistance are automatically routed to the relevant local centre. They are used to obtain information, for example regarding an operation, or for orientation in unfamiliar operational areas.

8.1.3.4 Alarming

The term ‘alarming’ refers to the sending of an alarm message to individual alarm recipients or an alarm group within the BOS digital network. The alarm message is sent as a short data message. It is used to summon emergency response units by the control centre and for remote control, for example, to activate sirens. The notification can be sent to both individual alarm recipients and an entire group of recipients. The decision on the use of the alarming service in the BOS digital network is made by the relevant state and the federal government for subordinate BOS units. BDBOS ensures that the system technology on the network side supports alarming.

8.1.3.5 Short data message service

The short data message service includes the transmission of tactical status reports and short data messages.

Tactical status reports can be used to convey information on the status of an operation or, for example, to request permission to speak. Short data messages can be used to transmit the following information, amongst other things:

Text messages, similar to SMS on a mobile phone

Location messages that transmit the position of the responding unit to the control

centre Alarm messages

Both tactical status messages and short data messages can, in principle, be sent to individual recipients or groups.

8.1.3.6 GPS-based tracking of vehicles and personnel

This service enables radio devices to automatically transmit their location. Messages containing precise GPS coordinates are sent. Messages can be sent at regular intervals or after a certain distance has been travelled, for example every 10 minutes or every 100 metres. In the event of an emergency call, a message containing the location is sent automatically.

8.1.3.7 Prioritisation

This service determines which services and devices take precedence over others when communicating on the BOS digital network. For example, it ensures that emergency calls have higher priority than normal radio traffic. Priority management is supported by tools that enable the management of service and subscriber priorities.

8.1.3.8 Communication via aviation radio cells

Radio equipment installed in aircraft uses not only ground-based radio coverage (TVFZ) but also specially created air traffic radio cells (LFFZ) for airspace. Upon reaching a certain flight altitude, this radio equipment automatically switches from ground coverage to the available air traffic cell and uses it until landing.

8.1.3.9 Operation of gateways between network and direct modes (TMO-DMO Gateway)

To support operations in areas with insufficient network coverage (TMO), it may be useful to use the TMO-DMO Gateway. For example, units operating in buildings that lack sufficient outdoor coverage or are not covered by base stations can communicate with the control centre in TMO via the gateway in direct mode (DMO). The gateway enables communication between a group in TMO and a group in DMO.

8.1.3.10 Transition to external networks

External networks refer to TETRA networks of other organisations, for example from neighbouring German states, or private network operators such as transport companies or airports. The basic service ‘Transition to external networks’ regulates the use of services in these external networks and communication between units of the digital network’s BOS and units in these external networks.

8.1.3.11 Encryption

Radio communication in the BOS digital network meets the requirements for secure voice and data communication. To this end, radio links are first encrypted, followed by voice and short data. The radio link is secured using encryption at the

radio interface. Voice and all short data are further protected by end-to-end encryption. This ensures that all communication is fully encrypted using the BOS cryptosystem.

The basic configuration of all services is uniformly available to all responding units across the country. In collaboration with users, guidelines for the uniform use and customisation of services according to needs are continuously developed and refined.

8.1.4 Legislative framework for Digitalfunk BOS

The legislative framework for the Digitalfunk BOS system is defined by the Act on the Establishment of the Federal Office for Digital Communications of Security Forces and Organisations (BDBOS-Gesetz – BDBOSG). This Act, which was adopted on 28 August 2006 and last amended on 19 December 2022, regulates the establishment, purpose, tasks and administration of the Digitalfunk BOS system.

Under the BDBOSG, the Federal Agency for Digital Radio Communications of Authorities and Organisations with Security Tasks (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben – BDBOS) was established. This agency is a legal entity under public law within the Federal Ministry of the Interior, Building and Community. Its main purpose is the construction, operation and development of a unified digital voice and data communication system for security agencies and organisations in Germany.

The BDBOS is tasked with ensuring the functionality and security of the Digitalfunk BOS system, which encompasses not only technical aspects but also organisational and administrative support. Cooperation between the federal government and the federal states regarding the operation of the Digitalfunk BOS system is governed by an administrative agreement. This agreement contains provisions concerning cooperation, financing and the states' participation in the operation and development of the system.

The governing bodies of the BDBOS are the President and the Administrative Board. The President is responsible for managing the office and implementing the decisions of the Administrative Board, which supervises the President's activities and supports him in fulfilling his tasks. The Administrative Board is composed of representatives of the Federal Government and each federal state, and decides on fundamental issues concerning the BDBOS.

The financing of the BDBOS is provided through a joint budget of the Federal Government and the federal states. Detailed provisions on financing are set out in an administrative agreement between the Federal Government and the federal states. This joint budget ensures that the BDBOS has sufficient resources to fulfil its tasks.

The BDBOSG Act contains key provisions for ensuring secure and reliable communications for security agencies throughout Germany, which is essential for coordination in crisis situations and for ensuring public safety.

8.2 Finland – Virve 2

Finland decided to upgrade its original Virve communication system to the new generation, Virve 2, to meet the growing demands for public safety communications. The original system, launched in 2002, comprised 1,400 base stations and provided services for 41,000 user connections. Each week, approximately 1.1 million group calls were made and 50 million short data messages (SDS) were sent over the network. This system, managed by State Security Networks Group Finland (Erillisverkot), provided reliable communications for a wide range of public safety agencies and other key organisations.

In 2016, the Finnish Ministry of Transport and Communications auctioned off the 700 MHz frequencies, previously used by television broadcasters, to commercial telecoms operators. This decision enabled the creation of a robust infrastructure for a new generation of communication technologies, which form the basis for Virve 2.

According to a 2018 survey by Erillisverkot, 80% of users expressed a need for services comparable to commercial mobile networks. Virve 2 therefore provides advanced broadband services that enable the transmission of high-quality video and data in real time for the effective fulfilment of public safety tasks. This transition to Virve 2 is not merely a technological upgrade, but represents a strategic step towards enhancing the efficiency and reliability of the communications infrastructure.

Virve 2 is designed to prioritise communications by security services over commercial users when using mobile broadband services. This means that access to and availability of services for these services will be ensured even under high network load. The system also provides fast and seamless group calls and short data messages (SDS).

The new Virve 2 system utilises the capacity of commercial mobile networks, enabling wide coverage and high reliability. This approach ensures that security services have access to the latest technologies and can utilise the capacity and coverage of commercial mobile networks, guaranteeing a reliable and secure connection for all key services. The transition to Virve 2 is

being implemented in collaboration between government agencies and commercial partners. In 2019, Erillisverkot launched a tender for commercial operators to ensure that services would meet public safety needs using the winning 4G network

Virve 2 utilises a hybrid model (MOCN – Multi-Operator Core Network), which combines dedicated network infrastructure with commercial mobile operators, ensuring a robust and secure network architecture. The deployment of the new generation of communication network, based on LTE/5G technologies, is planned for the period 2023–2025.

The main users of the Virve 2 system are:

- Emergency services
- Police
- Social and healthcare services
- Armed forces
- Border Guard
- Railway operators
- Customs authorities
- Emergency services
- Finnish Transport and Communications
- Agency National public service broadcaster
- YLE

Virve 2 covers the whole of Finland and is designed to meet the demanding communication requirements of the public safety sector. The system enables efficient and rapid communication even in crisis situations, which is crucial for ensuring the safety of citizens.

8.2.1 Transition to Virve 2

The transition from the original Virve system to its modernised version, Virve 2, is a complex process involving the gradual migration of all users to the new platform to ensure the smooth operation and continuity of services.

The transition to Virve 2 is divided into several phases:

Planning and preparation: This step involves detailed planning of the transition, legislative changes and the selection of suppliers. The process began in 2018 and included a thorough analysis of user needs and the design of the new infrastructure.

Testing and pilot operation: Between 2022 and 2024, testing of new broadband services and equipment took place, including the activation of key features such as group calls and data services, to ensure that the new infrastructure meets all security and reliability requirements.

User migration: From 2024 to 2028, the old Virve system and the new Virve 2 system will operate in parallel. This approach allows users to transition to the new platform gradually without disrupting their day-to-day activities and ensures the smooth integration of new features.

Full implementation and decommissioning of the old system: From 2029, Virve 2 is expected to be fully implemented and the original Virve system gradually phased out. During this phase, new tenders will be launched for the further development of services and to ensure that the system meets future communication and security requirements.

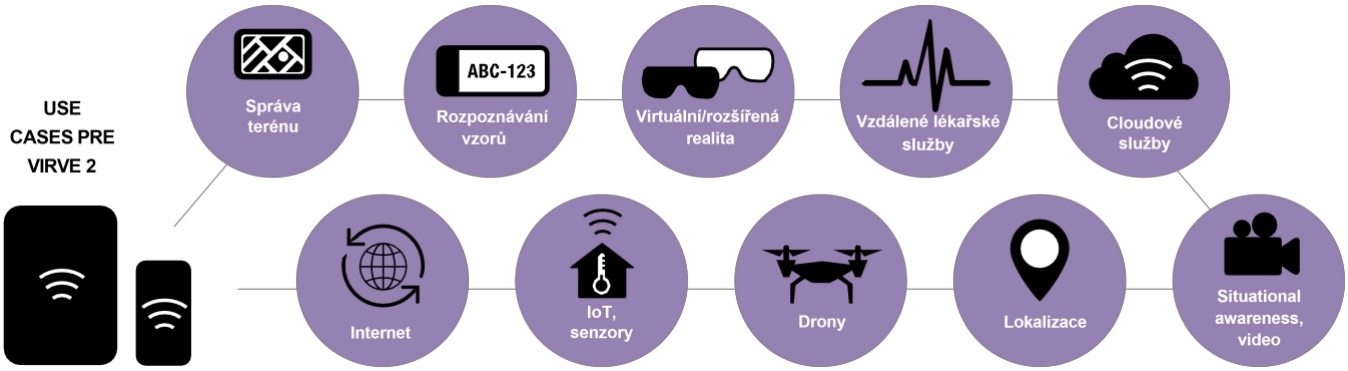
Virve 2 brings significant improvements over the original system, including higher data transmission capacity, better coverage and an enhanced level of security.

The transition to Virve 2 also enables integration with similar systems in other countries, thereby improving international cooperation and the ability to effectively manage cross-border crisis situations. This step therefore not only improves national security but also strengthens Finland’s position as a leader in public safety communications at the international level.

Virve 2 is a modern communications platform that provides advanced services and applications for public safety agencies and other critical infrastructure organisations. This new generation of the communications system brings significant improvements over the original

Virve system, including broadband connectivity, higher data transmission capacity and expanded features that support more efficient and secure operations.

8.2.2 Key Virve 2 services



8.2.2.1 Mission Critical Push-to-talk (MCPTT)

Virve 2 provides advanced MCPTT services that ensure reliable and instant voice communication between public safety teams in the field. The system supports both group calls and individual calls, enabling effective coordination during emergency situations. These services are designed to function even in challenging conditions and prioritise voice communication over data transmission.

8.2.2.2 Real-time video and multimedia transmission

The new system enables the transmission of high-quality video and visual material in real time. This includes, for example, video transmission from drones or cameras mounted on uniforms.

8.2.2.3 Internet of Things (IoT) integration

There is already a wide range of standalone IoT devices on the market for various types of alarms and monitoring, which security forces can integrate into their systems. With the development of NB-IoT and LTE-M technologies, these functions are expected to become available with greater reliability and efficiency. In the future, security forces will be able to collect data from their own, open and commercial sources, enabling effective environmental monitoring, threat detection and rapid response to incidents.

8.2.2.4 Augmented and virtual reality

The system supports applications based on augmented and virtual reality, which can be used for training purposes or to provide additional real-time information during operations.

8.2.2.5 Automation and robotics

Virve 2 supports innovation in the field of automation and robotics, including the use of autonomous devices such as drones and robots, which can improve the efficiency of operations and the safety of personnel in the field. These technologies enable, for example, the reconnaissance of hazardous areas without the need to deploy human personnel.

8.2.3 Legislation and its impact on the implementation of Virve 2

The current Virve radio network will be gradually replaced by the Virve 2.0 broadband network, which has been approved by legislation. This change aims to improve the safety and efficiency of emergency services operations. The legislation required for this modernisation comprises three acts: the Electronic Communications Services Act, the Emergency Services Act and the Act on the Operation of the Government Security Network. The Electronic Communications Services Act and the Emergency Services Act were updated in 2019.

The main legislative framework comprises the following acts:

Act on Electronic Communications Services (917/2014) / Laki sähköisen viestinnän palveluista (917/2014) Act on

Rescue Services (379/2011) / Pelastuslaki (379/2011)

Act on the Operation of the Government Security Network (10/2015)

8.2.3.1 Act on Electronic Communications Services (917/2014) / Laki sähköisen viestinnän palveluista (917/2014)

The Act on Electronic Communications Services focuses on the regulation and management of electronic communications networks and services in Finland. The aim of this Act is to ensure that communications services are reliable, secure and accessible to all citizens, whilst emphasising the protection of user data, the security of communications and the promotion of competitiveness in the field of electronic communications.

This Act regulates the obligations of electronic communications service providers, sets out technical and organisational requirements for the security of networks and services, and defines the rights and obligations of users of these services. An important part of the Act is also the regulation of broadband services and specific requirements for services provided for public safety networks.

The Act emphasises the importance of the quality and security of communications networks and services. Service providers must ensure that their networks are resilient to external influences and threats to information security. This Act also entrusts the Finnish Transport and Communications Agency (Traficom) with the supervision of the quality, security and interoperability of communications networks and services.

The Act also establishes a framework for ensuring the continuous availability and reliability of data transmission for public security purposes. Service providers must implement technical and organisational measures to protect against unauthorised access and ensure the confidentiality and integrity of transmitted data. This also includes access control and the allocation of network resources for priority communications by public authorities.

The following Chapters 29 and 29a focus on specific requirements for broadband services for public safety networks and on ensuring the security of electronic communications networks and services. These chapters set out in detail how networks and services should be designed, built and maintained to meet high standards of technical quality and security.

Chapter 29 – Broadband services for public safety networks

This chapter focuses on the regulation of broadband services provided for public safety networks. It specifies requirements for data transmission, communication protection and security. For example, service providers must ensure the continuous availability and reliability of data transmission for public safety purposes.

The more detailed requirements and regulations set out in this chapter are:

Public communications networks and services must be designed, built and maintained in such a way as to ensure high technical quality and information security. They must be resilient to various external influences and threats to information security. Ensuring reliable access to emergency services even during network outages is crucial.

Traficom (the Finnish Transport and Communications Agency) may issue regulations concerning the quality, information security and interoperability of communications networks and services. These regulations cover, for example, prioritisation, power supply, integrity, redundant routes and network protection (Section 244).

Network equipment must not jeopardise national security, and Traficom may order the removal of such equipment from critical parts of the network to protect infrastructure such as nuclear power stations, ports and airports (Section 244a).

The Advisory Committee on Network Security, established by the government, assesses national security in communications networks, monitors developments and submits proposals for improving network security (Section 244b).

Authorities must submit proposals for operational requirements for interception and monitoring, and operators must inform the authorities of changes relevant to these activities (Section 245).

Providers must maintain the security of information relating to services, communications, traffic data and location data, with measures being proportionate to the threats and technological developments (Section 247). Providers of online marketplaces, search engines and cloud services must manage risks to networks and systems, including system security, threat response, business continuity and compliance with international standards (Section 247a).

Operators must minimise disruption to others during construction, maintenance or security measures, and temporary outages must be notified to the operators concerned (Section 248).

Chapter 29a – Ensuring the security of electronic communications networks and services

This chapter expands on the requirements for network and service security. It sets out the obligation for providers to implement technical and organisational measures to ensure the security and integrity of networks, which includes protection against unauthorised access and ensuring the confidentiality and integrity of transmitted data.

The more detailed requirements and regulations set out in this chapter are:

Subscriptions for the use of the public administration network and related communication services may be offered to authorities and other important groups that perform tasks related to national security, public order, rescue operations and other key state functions. The Ministry of Transport and Communications decides on these groups and the number of subscriptions.

The public administration service provider must ensure that these services have priority access and sufficient quality even in the event of network congestion. This includes access control and the allocation of network resources for priority communications by public administration bodies (Section 250b).

Where necessary, telecommunications operators must provide national roaming for public administration communications if the primary service provider's network is unavailable. Traficom may determine the conditions for the provision of these services if the parties fail to reach an agreement (Section 250d).

Telecommunications operators must connect the public administration network to the public communications network free of charge upon request, in order to ensure the necessary interoperability and functionality (Section 250e).

8.2.3.2 Emergency Services Act (379/2011) / Pelastuslaki (379/2011)

The Rescue Services Act (379/2011) stipulates the following in Section 109(1):

If a building poses a higher risk to personal safety and the existing Virve network or the future Virve 2 network does not provide sufficient signal coverage to meet the needs of the emergency services, the building owner is obliged to ensure sufficient Virve signal coverage inside the building.

A higher risk to personal safety applies to buildings where dangerous situations are more likely to occur. This includes buildings with large numbers of people (e.g. shopping centres, hospitals, schools) or buildings where hazardous substances are stored.

The building owner is responsible for ensuring that, in the event of insufficient signal coverage, a technical solution is provided to improve it. This may involve, for example, the installation of repeaters (signal boosters) or other technologies that ensure the necessary signal quality inside the building.

The aim of this obligation is to ensure that emergency and security services can communicate effectively even inside buildings that pose an increased risk. This enhances safety for both the emergency services and the people inside these buildings.

This obligation forms part of a broader framework for ensuring the safety and effective operation of emergency services, which is in accordance with the Electronic Communications Services Act (917/2014) and other relevant legislation.

8.2.3.3 The Act on security public public administration (10/2015) / Laki public public administration security network operations (10/2015)

The Act on the Public Administration Security Network, adopted on 13 January 2015, aims to ensure the smooth flow and continuity of communication necessary for cooperation between the state's senior leadership and other authorities important to the security of society. This Act focuses on the public administration security network, its services and infrastructure, whilst seeking to ensure the availability, integrity and confidentiality of information necessary for state decision-making and governance

Under the Act, the obligation to use the security network is imposed on state administration bodies, the defence forces, the police, the border guard, emergency services and other critical entities. The security network comprises a communications network, equipment and other infrastructure necessary to ensure a high level of preparedness and security. This Act also permits the use of the security network by other entities, provided their activities relate to national security and they are approved by the Ministry of Finance.

The provider of network and infrastructure services for the security network is Suomen Erillisverkot Oy, a state-owned company that is not intended to generate commercial profit. The company's tasks include the production, maintenance and development of network services, the management of equipment, and ensuring the security and continuity of services under normal, disrupted and exceptional conditions. The provider of technical and integration services is a state service centre, which must separate activities related to the security network from other activities.

The Ministry of Finance is responsible for the overall control and supervision of the operation of the security network, including strategic and financial management and the assurance of information and communication security. An advisory committee has been established to support the Ministry of Finance in the management and supervision of the security network.

The Act also contains transitional provisions governing the organisation of tasks, the introduction of the obligation to use the security network, and the transfer of assets to the new service provider. This Act comes into force on 15 January 2015 and stipulates that the relevant authorities must begin using the security network's services no later than upon the expiry of existing contracts for similar services. The transitional provisions also apply to the deployment of information systems within the security network's facilities and to the organisation of staff employment relationships.

Act No. 10/2015 is a key piece of legislation aimed at enhancing the preparedness and security of public administration in Finland. This Act ensures secure and uninterrupted communication for state authorities and other key entities.

8.3 Belgium – ASTRID

Belgium has decided to modernise its public safety communications infrastructure through the introduction and continuous development of the ASTRID (Agency for Safety and Emergency Response) system. Launched in 1998, this system is specifically designed to support the communications needs of the police, fire services, medical services and other emergency and security services.

ASTRID is a specialised telecommunications operator providing technological services to all emergency and security services in Belgium. Effective, fast and secure communication via the ASTRID network enhances the safety of all citizens. The ASTRID system uses the TETRA (TErrestrial Trunked Radio) standard, which is the European standard for digital radio communication, used in almost all European countries.

ASTRID was established as a public limited company under public law and is wholly owned by the Belgian state. This system provides a unified platform for communication among all emergency and security services, thereby eliminating the technical barriers of the past and enabling better coordination and efficiency during operations.

ASTRID comprises several key services that are essential for the effective functioning of public safety services: **Radio communications:** Provides high-quality voice communication with rapid connection for teams in the field. **Paging:** Sending alert messages to the fire service and medical services.

Emergency control centres: Technical equipment and software for regional centres handling emergency calls (100, 101, 112).

Mobile broadband data: Blue Light Mobile SIM cards provide priority on the Proximus network, which is important during network congestion.

Consultancy and support: Ongoing contact with users to ensure they are familiar with the technology, providing training and advice as required.

8.3.1 Modernisation and future plans

The ASTRID system is being upgraded to meet the ever-increasing demands for communication in the public safety sector. The planned modernisation includes a transition to 5G technology, which will significantly increase data transmission capacity and improve the reliability and security of communications between emergency and security services.

In 2023, the Belgian government approved the fourth administrative contract between the state and ASTRID, which sets out the framework for this modernisation. Development of the new 5G radio network will begin in 2024, with the aim of completing the implementation of core functions by 2026. The new broadband network will enable the secure and reliable transmission of large volumes of data. This includes video transmission, the use of sensors and improved situational awareness.

The modernisation involves a hybrid model that combines the infrastructure of commercial telecommunications operators with ASTRID's own infrastructure. This approach ensures a high degree of flexibility and reduces the costs of building new infrastructure. The brain of the network, i.e. its core, will remain fully under ASTRID's control.

ASTRID also plans to introduce a new generation of emergency centres that will be able to utilise modern technologies such as artificial intelligence, sensors and video transmission, which will improve their proactive capabilities and their ability to respond to incidents more quickly and effectively. Pilot projects for these new centres are expected to begin in 2025, with full deployment planned for 2027.

8.3.2 Key ASTRID services

ASTRID provides key services that are essential for the effective functioning of public safety services in Belgium.

8.3.2.1 Radio communications

The ASTRID radio communication system is designed to meet the needs of the police, fire brigades and emergency services, utilising TETRA (Terrestrial Trunked Radio) technology. This European standard for digital radio communication provides high-quality voice communication, rapid connection establishment and enables group calls, which is key to effective coordination during operations.

TETRA offers:

High-quality, noise-free voice communication. Rapid

connection establishment, essential for emergency

situations.

Group calls for coordination between different units.

The ASTRID network covers the whole of Belgium with more than 520 base stations, ensuring reliable communication even in remote areas. The network offers more than 99.98% service availability, which significantly exceeds industry standards. Backup systems and generators ensure uninterrupted communication during power cuts. Communication encryption protects against unauthorised access and ensures the confidentiality of information. ASTRID enables direct communication between various security and emergency services, ensuring effective coordination during operations and a faster response to crisis situations.

The ASTRID radio communication system also offers:

Data services for the transmission of short data messages (SDS).

GPS tracking for monitoring the location of units.

Call prioritisation during periods of high network load, giving priority to calls from emergency services.

The ASTRID radio communication system thus provides a robust, reliable and secure platform for all services involved in public safety in Belgium.

8.3.2.2 Paging

The ASTRID paging system is a critical tool for rapid and effective communication in emergency situations. This system is designed to enable the sending of alert messages to the fire service, medical services and other civil protection agencies. Thanks to the paging system, alert messages can be sent immediately, which is crucial for a rapid response to emergencies. The paging network covers the whole of Belgium, ensuring that messages can be delivered even in remote areas. More than 6,400 paging messages are sent via the system every day, demonstrating its reliability and capacity.

The ASTRID paging system allows messages to be sent to a large number of users simultaneously, which is important for coordination during large-scale operations. In crisis situations, alert messages are prioritised, ensuring that critical information is delivered in a timely manner. The system is also integrated with other ASTRID communication systems.

Security and reliability are key aspects of the paging system. Like other ASTRID systems, the paging system is equipped with backup batteries and generators, ensuring its uninterrupted operation even during power cuts. Alert messages are encrypted to ensure their security and protection against unauthorised access. This robust and reliable system is therefore an essential element of the public safety infrastructure, contributing significantly to the efficiency and success of emergency operations.

8.3.2.3 Emergency centres (Noodcentrales)

Emergency centres (Noodcentrales) form part of the ASTRID system and play a role in receiving and processing emergency calls. These regional centres, which handle emergency calls to the numbers 100, 101 and 112, are technically equipped and supported by software to ensure an effective and rapid response to emergencies. The centres are responsible for receiving emergency calls and dispatching emergency services to the scene of the incident.

The technical equipment of the emergency centres includes modern communication technologies that enable fast and reliable contact with units in the field. This includes not only voice communication but also data transmission and location services, which help operators pinpoint the caller's location and direct assistance to the correct place. The modernisation of these centres is an ongoing process involving the integration of new technologies and systems.

The planned new generation of emergency call centres will be capable of utilising advanced technologies such as artificial intelligence and video transmission. These technologies will enable operators not only to receive and process calls, but also to analyse situations in real time and provide more accurate and rapid instructions to units in the field. Pilot projects for these new centres are expected to begin in 2025, with full deployment planned by 2027.

8.3.2.4 Mobile broadband data

This service is provided via Blue Light Mobile, a dedicated mobile operator focused on public safety needs. Blue Light Mobile utilises the infrastructure of the commercial operator Proximus and offers prioritised connectivity for emergency and security services. This means that in the event of network congestion, Blue Light Mobile users have priority access to network resources, which is essential for ensuring uninterrupted and reliable data transmission during crisis situations.

Mobile broadband data enables emergency services to access the internet, data services and applications. These include, for example:

Real-time video transmission: Enables the sharing of live footage from the scene of an incident, which is vital for situational awareness and decision-making.

Access to databases and information systems: Emergency services can obtain necessary information in real time, such as medical records, building plans or vehicle registers.

GPS and location services: These help track the position of units in the field and coordinate their movements.

Blue Light Mobile is also designed to be resilient to outages and provide uninterrupted service even under adverse conditions. The network is supported by backup systems, and its infrastructure is regularly maintained and updated to meet the highest standards of security and reliability.

8.3.2.5 Mobile data access (ISLP)

Mobile data access via the Integrated Location and Access System (ISLP) is a key component of the ASTRID system and enables emergency and security services to access vital information directly in the field, thereby enhancing the efficiency of operations.

ISLP provides mobile units, such as the police, fire service and medical teams, with access to central databases and information systems via mobile data terminals (MDTs). These terminals are equipped with technology enabling fast and secure data transmission.

One of the main benefits of ISLP is the ability to access important information such as medical records, building plans, vehicle registers or criminal records. This access enables units in the field to quickly obtain the data needed for decision-making and the coordination of interventions. For example, medical teams can access patients' medical records, enabling them to provide targeted and effective care on the spot.

ISLP also supports GPS tracking, which enables the monitoring of the location of individual units in the field. This feature is crucial for operations centres, which can monitor the deployment and movement of units and effectively manage their deployment. GPS tracking also contributes to the safety of response units by providing an overview of their current location and enabling a rapid response in the event of an emergency.

Another significant benefit of ISLP is its integration with desktop applications via RDP (Remote Desktop Protocol). This approach allows mobile units to use the same applications and systems available on their stationary workstations. This ensures consistency and availability of information regardless of the unit's location.

ISLP is designed with a focus on security and reliability. All communication and data transmission are encrypted to ensure that sensitive information is protected against unauthorised access. At the same time, the system is equipped with backup mechanisms that ensure uninterrupted operation even during technical issues or power cuts.

8.3.3 Legislation

The legislative framework governing the deployment and operation of the ASTRID system is key to ensuring its reliability, security and efficiency. The following documents form the basis of this framework:

The Act of 8 June 1998 on radio communications for emergency and security services (Loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité)

This Act is the fundamental legal document establishing the general framework for the creation and operation of the ASTRID system. It defines ASTRID's social objective, allocates a specific frequency band, and provides for the supervision and monitoring of the system's financial situation. It ensures that ASTRID fulfils its public service obligation and supports the operation of emergency and security services in Belgium.

Royal Decree establishing the fourth ASTRID management contract (2023–2027) (Arrêté royal fixant le quatrième contrat de gestion d'ASTRID (2023–2027))

The Royal Decree is a legislative act that formally approves the management contract between ASTRID and the Belgian government for the period 2023–2027. This decree provides the contract with a legal basis and binding force. It sets out ASTRID's specific obligations, such as the maintenance and modernisation of infrastructure, ensuring the security and reliability of services, and supporting interoperability with other systems.

Management Agreement 2023–2027 (Contrat de gestion 2023–2027)

The 2023–2027 Management Contract is a detailed operational document that specifies the obligations, rights and commitments between ASTRID and the Belgian government for the period in question. This contract provides a clear and transparent framework for the operation, financing and development of the ASTRID system. It is a key tool for ensuring effective and secure communication between the various public security services.

Royal Decree on the financing and investment framework for ASTRID (Arrêté royal concernant le financement et le cadre d'investissement pour ASTRID)

The Royal Decree on the financing and investment framework for ASTRID is a fundamental document that specifies the financial and investment mechanisms to ensure the long-term sustainability and development of the ASTRID system. This decree provides a stable and predictable financial framework that enables ASTRID to plan and implement long-term investment projects effectively, thereby contributing to the provision of secure and reliable communications for public security services in Belgium.

8.3.3.1 The Act of 8 June 1998 on radio communications for emergency and security services

The Act of 8 June 1998 on radio communications for emergency and security services (Loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité) is a key piece of legislation that established the legal basis for the creation and operation of the ASTRID system (All-round Semi-cellular Trunking Radio communication system with Integrated Dispatchings).

This Act has several main functions and provisions:

Establishment of ASTRID

The Act provides for the establishment of ASTRID as the national operator for emergency and security services communications in Belgium. The Federal Investment Company (Federale Investeringsmaatschappij/Société Fédérale d'Investissement) was tasked with establishing ASTRID. This created the institutional framework for the centralisation and management of communications between the various public security services and other key organisations.

ASTRID's social objective

The law defines ASTRID's social objective, which includes the provision of reliable and secure communication services for emergency and security services in Belgium. ASTRID is tasked with ensuring that these services have access to the high-quality communication tools necessary for effective coordination and response in the event of crisis situations. The composition of ASTRID's board of directors is also laid down by law, comprising representatives from various public and private institutions to ensure a broad range of expertise and experience. The Act also addresses issues relating to capital and financing.

Allocation of the frequency band

One of the key elements of the Act is the allocation of a specific frequency band, 380–385/390–395 MHz, for use by the ASTRID system. This frequency range is reserved exclusively for security communications, ensuring the independence and quality of data and voice transmission.

Supervision of ASTRID

The Act stipulates that supervision of ASTRID is carried out by the Minister of the Interior and the Minister of Finance. This supervision includes monitoring the operational efficiency and financial stability of the ASTRID system. The ministers are responsible for ensuring that ASTRID fulfils its objectives and provides a high level of service to public security agencies.

Monitoring of the financial situation

ASTRID's financial situation, annual financial statements and the company's compliance with the law are monitored by a group of commissioners. These commissioners are tasked with ensuring transparency and accountability in the management of ASTRID's funds. This control mechanism is important for maintaining public confidence and ensuring that funds are used effectively and in accordance with the law. The group of commissioners regularly assesses ASTRID's financial health and provides reports to the Ministers of the Interior and Finance. The reports include analyses of financial results, identification of potential risks and recommendations for improving financial management.

Other provisions of the Act

In addition to the key points mentioned above, the Act also contains provisions concerning cooperation between ASTRID and other public and private entities. For example, integration with other communication systems and ensuring interoperability at both national and international levels. The Act also establishes a framework for the protection of personal data and the security of communications. ASTRID must comply with strict data protection standards and ensure that all communications are secure and protected against unauthorised access.

Overall, the Radio Communications Act for Emergency and Security Services provides a comprehensive legal framework for the establishment, management and development of the ASTRID system. This Act contributes to effective and secure communication between emergency and security services in Belgium, thereby ensuring better coordination and a faster response to crisis situations, which is key to the protection and safety of citizens.

8.3.3.2 Royal Decree establishing the fourth ASTRID management contract (2023–2027)

The Royal Decree establishing the fourth ASTRID management contract (Arrêté royal fixant le quatrième contrat de gestion d'ASTRID) for the period 2023–2027 is a key legislative document that officially approves and brings into force the management contract between ASTRID and the Belgian government. This decree provides the legal basis and binding framework for the operational and financial framework within which ASTRID operates.

Main objectives and obligations

Provision of services: The Royal Decree stipulates that ASTRID must provide a range of specific services aimed at supporting public safety. These services include the maintenance and modernisation of the communications infrastructure, ensuring the reliability and security of services, and supporting interoperability with other national and international systems. ASTRID is obliged to ensure that all its systems are constantly updated and prepared to meet new technological and security challenges.

Infrastructure modernisation: The decree emphasises the modernisation and expansion of the communications infrastructure. Particular attention is paid to the transition to broadband technologies, such as 4G and 5G, which enable higher capacity and data transfer speeds. Investment in these technologies is essential to ensure that ASTRID can provide high-quality services that meet current public safety requirements.

Security and reliability: Ensuring the security and reliability of services is another aspect of the decree. ASTRID must implement advanced security measures to protect against cyber threats and ensure the continuous availability of services, particularly during crisis situations. This includes regular testing and updating of security protocols, staff training and cooperation with other security organisations.

Funding

Annual funding: The decree sets out mechanisms for the annual funding of operating costs. The Belgian government has allocated an annual subsidy of €46.5 million for 2023 and for each subsequent year up to 2027. The funds are earmarked for system maintenance, operating costs and other necessary expenditure to ensure the smooth functioning of the ASTRID system.

Investment projects: Investment projects are financed through pre-funding from ASTRID's own resources, with the total amount subsequently covered by users' annual subscriptions. The value of ASTRID's investment activities covered by subscription revenue amounts to €117 million. This funding model enables flexible and long-term sustainable investment in infrastructure and technology.

Performance monitoring and evaluation

The Decree sets out clear mechanisms for monitoring and evaluating ASTRID's performance. This includes regular reports on the operational and financial situation, which must be submitted to the supervisory authority and government bodies. The monitoring system ensures that ASTRID meets its objectives effectively and transparently.

Transparency and accountability

ASTRID is required to regularly inform the public and users about its activities and performance, which includes public consultations and engagement with key stakeholders.

Flexibility and adaptability

The Royal Decree also ensures that ASTRID has sufficient flexibility and the ability to adapt to changing conditions and requirements. It includes the possibility of updating the contract during its term in line with new technical or operational needs.

8.3.3.3 Management Contract 2023–2027 (Contrat de gestion 2023–2027)

The Management Contract 2023–2027 (Contrat de gestion 2023–2027) is a detailed operational document governing the relationship between ASTRID, the Belgian government and end users. This contract provides a clear and transparent framework for the operation, financing and development of the ASTRID system during the specified period. It is a key tool for ensuring effective and secure communication between the various public security services.

The contract defines the specific services that ASTRID must provide. These services include:

Maintenance and modernisation of infrastructure: ASTRID must ensure the regular maintenance and modernisation of its communications infrastructure to guarantee its reliability and performance. This includes both physical infrastructure, such as base stations, and software systems.

Ensuring the security and reliability of services: Security and reliability are key aspects of ASTRID's operations. The contract stipulates that ASTRID must implement measures to protect against cyber threats and ensure the continuous availability of services, particularly during crisis situations.

Supporting interoperability: ASTRID is obliged to ensure the interoperability of its system with other national and international communication systems. This includes technical compatibility and cooperation with other operators and organisations involved in public safety.

The contract describes in detail the financing mechanisms, which include:

Annual funding of operating costs: Annual funding of operating costs (system maintenance and operational costs) is provided through a grant from the Ministry of the Interior's budget as part of the overall budget. The Belgian government has allocated an annual grant of EUR 46.5 million for 2023 and each of the following four years.

Investment projects: Investment projects are financed through pre-financing from ASTRID's own resources, with the total amount covered by users' annual subscriptions. The value of ASTRID's investment activities covered by subscription revenue amounts to €117 million.

Technical requirements:

The contract sets out technical standards and requirements for infrastructure, security and interoperability. ASTRID must ensure that its systems meet high standards of quality and security so that they are able to effectively support emergency and security services.

Performance monitoring and evaluation:

The contract includes mechanisms for monitoring and evaluating ASTRID's performance – regular reports on the operational and financial situation, which must be submitted to the supervisory authority and government bodies.

Transparency and accountability:

Transparency and accountability are key principles underpinning ASTRID's operations. The contract requires ASTRID to regularly inform the public and users about its activities and performance. This includes public reports and consultations with stakeholders.

Flexibility and adaptability:

The contract ensures that ASTRID has sufficient flexibility and the ability to adapt to changing conditions and requirements. This includes the possibility of updating the contract during its term in response to new technical or operational needs.

8.3.3.4 Royal Decree on the financing and investment framework for ASTRID

The Royal Decree on the financing and investment framework for ASTRID (Arrêté royal concernant le financement et le cadre d'investissement pour ASTRID) is a legal act that specifies the financial and investment mechanisms necessary for the long-term sustainability and development of the ASTRID system. This decree is key to ensuring that ASTRID has sufficient resources to provide its services and to modernise its infrastructure.

The Decree establishes mechanisms for the annual financing of ASTRID's operating costs.

The decree sets out a financial framework that covers the allocation of funds, sources of funding and how they are to be used. The financial framework is designed to ensure stable and predictable funding for ASTRID.

8.4 South Korea – Safe-Net

South Korea has developed a comprehensive public safety and disaster response system known as Korea Safe-Net. This system was established following a decision in 2014, when South Korea decided to build a dedicated mobile broadband network for public safety. The main reason for this decision was the need to replace various public safety networks based on different technologies, such as analogue networks, TETRA and iDEN, which were not interoperable. The aim was to ensure interoperability between all public safety agencies.

Korea Safe-Net combines three LTE networks: PS-LTE for public safety, LTE-R for railways and LTE-M for maritime users. These networks share the same frequency band (B28 in the 700 MHz band). PS-LTE is planned for use by 333 agencies, including the fire service, power companies, the coastguard, the military, the police, medical services, gas companies and government departments. The estimated number of user devices is 240,000 for PS-LTE, 10,000 for LTE-R and 35,000 for LTE-M.

Safe-Net technology was validated in two pilot projects between 2015 and 2018. The second phase of the pilot project provided support for the 2018 Winter Olympic and Paralympic Games in PyeongChang. The deployment of PS-LTE took place in three phases between 2018 and 2021. Three geographically redundant operations centres have been established in different regions of the country to operate the network: in Seoul, Daegu and Jeju. These centres provide core LTE services, MCPTT services and network management.

PS-LTE network coverage was built using dedicated LTE radio stations (more than 17,000 base stations). The coverage and capacity of other networks can also be utilised through network sharing, including commercial mobile networks and LTE-R and LTE-M. The fourth element consists of deployable networks, based either on vehicles or portable solutions. LTE-M provides coverage up to 100 km from the coast, and LTE-R provides coverage of over 4,800 kilometres.

Korea Safe-Net follows a business model based on a multi-stakeholder dedicated network model. The construction of the PS-LTE network was commissioned to Korea Telecom (KT) and SK Telecom (SKT). KT is responsible for two areas, whilst SKT is responsible for one. KT was also tasked with building the operations centres. Government ministries oversee the operation of the network and MCPTT services. The administration of Safe-Net is shared among several ministries: the Ministry of the Interior and Safety oversees PS-LTE, the Ministry of Oceans and Fisheries oversees LTE-M, and the Ministry of Land, Infrastructure and Transport oversees LTE-R. The Safe-Net Forum coordinates research, standardisation and government policies within Safe-Net.

PS-LTE services were launched in 2020 and nationwide coverage was achieved in 2021. The migration of all public safety users is planned for the period 2020–2027. Future developments include device-to-device and air-to-ground communications, IoT sensors in public safety, and the gradual roll-out of 5G technology.

8.4.1 Technical infrastructure

The technical infrastructure of Korea Safe-Net is designed to provide reliable communication between emergency and security services across the country. It incorporates modern technologies, extensive coverage and interoperability between different systems and devices.

8.4.1.1 PS-LTE technology

Korea Safe-Net utilises Public-Safety Long Term Evolution (PS-LTE) technology, which ensures high-speed data and voice communication. PS-LTE is specifically designed for public safety needs, providing priority and preferential access to key users during emergencies.

8.4.1.2 Base stations and mobile stations

The network infrastructure comprises approximately 17,000 base stations covering the entire territory of South Korea. In addition, there are around 200,000 mobile stations, including fixed mobile stations, vehicle radios, smartphones and two-way radios. Base stations are strategically located to ensure full coverage even in remote and hard-to-reach areas. Mobile stations are equipped to provide reliable communication in the field, both during routine operations and in crisis situations.

8.4.1.3 Facilities and equipment

The Korea Safe-Net network utilises a wide range of devices and equipment from various manufacturers to ensure the system's robustness and reliability. These include specialised terminals, radio equipment, smartphones, in-vehicle communication systems and portable communication units. These devices are designed to meet the specific needs of individual emergency and security services, and are regularly tested and certified to ensure their functionality and compatibility with the system.

8.4.1.4 Interoperability and integration

One of the key objectives of Korea Safe-Net is to ensure interoperability between the various technologies and devices used by different agencies and organisations. The network is designed to allow integration with existing systems such as TETRA, iDEN, VHF, UHF and others. This ensures seamless communication between the various components of the emergency services, whether they be the police, fire service, ambulance service or other agencies. Interoperability is ensured through standardised protocols and technologies that facilitate interconnection and collaboration between different systems.

8.4.2 Key services

8.4.2.1 Mission-Critical Push-to-Talk (MCPTT)

One of the most important services is Mission-Critical Push-to-Talk (MCPTT), which enables fast and reliable voice communication between emergency response teams. MCPTT has a faster response time than standard LTE and is designed to prioritise communication for key personnel, such as incident commanders and the president.

8.4.2.2 Group Calling and Broadcasting (GCSE and eMBMS)

Group Calling and Broadcasting (GCSE and eMBMS) enables mass communication between multiple users simultaneously.

8.4.2.3 Voice over LTE (VoLTE)

Voice over LTE (VoLTE) ensures high-quality voice communication.

8.4.2.4 Device-to-Device (D2D)

Device-to-Device (D2D) communication enables direct communication between devices, which is used in the event of infrastructure failures or in areas without coverage. The service ensures that emergency services can communicate directly with one another without the need for base stations.

8.4.2.5 Real-time video and data transmission

Korea Safe-Net enables real-time video and data transmission, allowing rescue teams to share live feeds from the scene, map data and other vital information.

8.4.3 Application service guidelines

The Application Service Guidelines within Korea Safe-Net provide a detailed framework for the development, deployment and updating of application services that can be used for disaster management and public safety.

The development of application services focuses on creating applications that can be used by various organisations involved in disaster management and security. Application services are developed based on core services and are progressively expanded and updated in line with technological advancements and subsequent 3GPP releases. These services include those focused on prevention, rapid response and recovery, such as live streaming during crisis situations, mapping software for the localisation and management of critical assets, and other applications for data monitoring and analysis.

The process for implementing new application services is described in detail to ensure that the services are fully functional and safe for use within Korea Safe-Net. Organisations planning to introduce new equipment or services must submit a plan and request consultation with the Ministry of Public Safety and Security. Prior to deployment, the equipment must undergo a technical verification process, which includes security reviews and testing. Testing takes place on a test network and the main network, followed by the issuance of test reports and a verification certificate. Services are regularly updated in line with technological innovations and user feedback.

All users have access to training focused on standard operating procedures (SOPs) and the use of the communications network and its applications in emergency situations. Technical support is provided throughout the entire process of implementing and using new equipment and services, including consultation and assistance with registration and device connection.

The Ministry of Public Safety and Security reviews implementation plans and approves the interconnection of equipment with the main network. User organisations submit applications for the registration and interconnection of equipment that has been verified and approved. Verification agencies establish technical specifications and carry out technical verification of equipment and services. These guidelines and procedures ensure that Korea Safe-Net is prepared to respond to all types of crisis situations and to provide a reliable and secure communications infrastructure.

8.4.4 Legislation

The legislative framework of Korea Safe-Net is essential for ensuring the effective operation and security of this public safety communications network. It comprises various laws, regulations and institutions which together form the structure for the management, operation and protection of the system.

8.4.4.1 Legal framework

The legal basis for Korea Safe-Net was established in 2014, when South Korea decided to create a dedicated mobile broadband network for public safety. This step involved the allocation of radio spectrum for public safety purposes. The main reason was to unify the various existing security networks, which used different technologies such as analogue systems, TETRA and iDEN, and which were not interoperable.

8.4.4.2 Laws and Regulations

Korea Safe-Net is supported by several key pieces of legislation that provide a solid legal basis for the establishment, operation and maintenance of this critical public safety communications network. The main legislation includes:

The Disaster and Safety Communications Network Act (재난안전통신망법)

Passed in 2021, this Act provides the main legal framework for the establishment and operation of a communications network for disaster and public safety. It sets out the obligations of the various governmental and non-governmental agencies involved in the operation of the network, infrastructure requirements and necessary security measures. The Act also defines the technical and operational standards that must be adhered to.

Regulations on the Operation and Use of the Disaster and Safety Communications Network (재난안전통신망 운영 및 사용 규정)

The Regulations provide detailed guidelines for the day-to-day operation and use of Korea Safe-Net. They contain rules for the registration and verification of new equipment and services to be connected to the network. The Regulations also set out procedures for the testing and certification of equipment. Furthermore, they address the operational procedures that must be followed during normal operations and in crisis situations.

Act on the Prevention of Terrorism and the Protection of Public Safety (Act on the Prevention of Terrorism for the Protection of

Citizens and Public Safety)

The Act provides a broader framework for all activities related to public safety, including the prevention of terrorism and the protection of critical infrastructure. It defines the roles and responsibilities of various government bodies and institutions in ensuring public safety. The Act includes measures to protect information and communication systems from cyber threats and other security risks.

8.4.4.3 Institutional Roles

The administration of Korea Safe-Net is shared among several key ministries and institutions, each with specific responsibilities for different aspects of this public safety network. This multi-institutional approach ensures that all aspects of the network's operation, maintenance and development are thoroughly covered and coordinated.

The Ministry of the Interior and Safety (MOIS) oversees Public-Safety LTE (PS-LTE), which is the main component of the network designed for public safety needs. The Ministry is responsible for the overall management and coordination of PS-LTE operations, ensuring that the network meets all technical and security standards, and overseeing integration with other public safety agencies. The MOIS also provides user training and support for the deployment of new equipment and services on the network.

The Ministry of Oceans and Fisheries is responsible for LTE-M, a network component specifically designed for maritime communications. The Ministry manages the LTE-M infrastructure and services, ensuring coverage of maritime areas and integration with maritime rescue and safety services. The Ministry of Oceans and Fisheries also coordinates safety measures and contingency plans for maritime areas.

The Ministry of Land, Infrastructure and Transport manages LTE-R, a network component designed for railway communications. This ministry oversees the construction and maintenance of railway communications infrastructure, ensures the integration of LTE-R with other parts of Korea Safe-Net, and coordinates the communications needs of the railway sector during emergency situations.

The Safe-Net Forum is another key institution that coordinates research, standardisation and government policies relating to Safe-Net. The Forum brings together representatives from various ministries, technical agencies and other relevant organisations to ensure that all aspects of the network's development and operation are managed consistently. The Forum also ensures that new technologies and procedures comply with international standards and best practices, and promotes cooperation between the public and private sectors in the development and implementation of new technologies.

8.4.4.4 Security measures

Security measures are a key component of the Korea Safe-Net legislative framework and ensure that all parts of the network are protected against various threats and risks. Before any new equipment or service is introduced into the network, a thorough technical and security verification must take place.

The verification process begins with security reviews conducted by the National Intelligence Service in collaboration with other technical agencies. This review involves an assessment of potential security threats, vulnerabilities and risks associated with the new device or service. This is followed by technical verification, which involves detailed testing of the equipment or service to ensure that it meets all required technical and security standards. Testing is carried out on a test network and includes the simulation of various crisis situations to verify the reliability and effectiveness of the equipment or service under real-world conditions.

Upon successful completion of the security reviews and technical verification, a verification certificate is issued. This certificate confirms that the equipment or service meets all required standards and may be integrated into the Korea Safe-Net network. The verification certificate is essential for the formal approval and interconnection of the new equipment or service with the main network.

The Ministry of Public Safety and Security reviews plans for the introduction of new equipment and services and approves their interconnection with the main network. This process ensures that all equipment and services meet strict security and technical standards, thereby minimising the risk of system failure or misuse. The Ministry also monitors the operation of equipment and services within the network to ensure their security and reliability.

8.5 Hungary – Unified Digital Radio Communications System (EDR)

EDR (Egységes Digitális Rádiórendszer) is a national public safety system in Hungary that uses TETRA (Terrestrial Trunked Radio) technology. This system provides reliable communications for a wide range of public safety agencies, including the Hungarian Armed Forces, the National Police, the National Border Guard, the National Directorate for Disaster Prevention,

the Tax and Customs Administration, the National Law Enforcement Agency, the National Ambulance Service and the National Directorate for Environmental Protection and Water Management.

The EDR project was launched in 2006 and completed in 2007, involving the rapid installation of a nationwide network within one year and one day. Modernisation of this network began in 2013, with further upgrades taking place in 2016. The main components of this network include 4 switches and 300 TETRA base stations, which provide communication for more than 42,000 radios and protect approximately 10 million inhabitants.

8.5.1 Pro-M Zrt. and the future PPDR network

Pro-M Zrt., a leading innovator in telecommunications technology and a provider of communication services for emergency services in Hungary, has announced significant developments in the field of public protection and disaster relief networks. Since 2020, Pro-M Zrt. has been focusing on planning future broadband systems tailored to the needs of emergency situations.

Pro-M Zrt.'s main objective is to establish broadband data and video communication, which involves transitioning from the current TETRA-based EDR network to new broadband solutions. The aim is to achieve 99.99% infrastructure availability, with full population coverage planned for the end of 2024 and nationwide coverage by 2026.

Pro-M Zrt. also plans to introduce applications and services that will enhance the efficiency of communication and management in emergency situations, including tools for localisation and deployment management. Among the key ones is MCX, an application for critical voice and video communication that enables secure and highly available group communication. The company is also preparing for the transition to 5G technology as part of an EU project, which involves testing 5G applications in a closed experimental network along the Ukrainian border.

8.5.2 Legislation

8.5.2.1 Electronic Communications Act (Elektronikus Hírközlési Törvény)

The Electronic Communications Act in Hungary provides a comprehensive framework for radio spectrum management. This Act plays a role in ensuring the efficient and equitable use of radio frequencies. The main objective is to enable the widest and most flexible use of this spectrum with minimal restrictions.

One of the key principles of this Act is technological neutrality. This means that radio frequencies may be used by various technologies without prior restrictions on specific technologies. This approach allows for the introduction of new and innovative technologies without the need for changes to the legal framework, thereby promoting technological progress and innovation in the field of electronic communications.

Another important principle is service neutrality, which allows radio frequencies to be used for various types of services without specific restrictions. This provides operators with the flexibility to respond to changes in demand for different types of services.

The Act also emphasises the efficient and economical use of the radio spectrum. This includes rules for the allocation of frequencies through auctions and tenders, which aim to maximise the value of the spectrum for society as a whole. A transparent and competitive frequency allocation process ensures that the spectrum is used in the most efficient manner, which benefits both service providers and end-users.

The National Media and Infocommunications Authority (NMHH) is responsible for radio spectrum management in Hungary. The NMHH oversees frequency allocation, monitors their use and ensures compliance with both national and international rules. In addition, the NMHH issues decrees and regulations that set out specific aspects of spectrum management in detail, thereby ensuring that the principles laid down in the Electronic Communications Act are observed.

8.5.2.2 NMHH Decrees (National Media and Infocommunications Authority)

NMHH Decree No. 12/2011 (16 December)

NMHH Decree No. 12/2011, issued on 16 December 2011, focuses on the management and allocation of radio frequencies for non-civilian users. This decree is important for organisations involved in public safety and crisis management, such as police and fire services, emergency services and others.

The Decree sets out specific rules for the allocation of frequencies to non-civilian users, ensuring that these frequencies are used for public safety and crisis management purposes. The NMHH is responsible for managing these frequencies and ensuring compliance with established standards and regulations – monitoring frequency usage and ensuring that they are not interfered with by other users.

Furthermore, this decree allows for the allocation of frequencies for specific purposes, such as operations during natural disasters, terrorist attacks or other crisis situations. The allocation process is designed to be swift and efficient.

NMHH Decree No. 7/2012 (26 January)

NMHH Decree No. 7/2012, issued on 26 January 2012, deals with frequency management and the conditions for issuing licences to civilian users, with an emphasis on public safety and disaster relief applications. It sets out detailed procedures for the allocation of frequencies to civilian users, including the conditions and requirements that must be met to obtain licences. This administrative process ensures transparency and fairness in spectrum allocation. Specific conditions for the issuance of licences include technical requirements, operational restrictions and other criteria that must be met.

8.5.2.3 Government Decree No. 346/2010 (28 December)

Government Decree No. 346/2010, issued on 28 December 2010, is a key piece of legislation specifying the obligations and requirements for the use of the EDR (Egységes Digitális Rádiórendszer) system for certain critical infrastructure sectors and high-risk facilities in Hungary.

The Decree requires certain critical infrastructure sectors, such as energy, water management, transport and communications, to use the EDR system for their internal and external communications. The use of EDR is mandatory for these sectors to ensure a high level of security and reliability of communications in the event of emergencies or crisis situations.

The Regulation stipulates that high-risk facilities posing a significant risk to public safety and the environment must use the EDR system for their communications. This includes chemical plants, refineries, nuclear power stations and other facilities requiring a heightened level of security and a rapid response in the event of an accident.

The regulation also defines the authorisation for major national public service providers, such as energy companies, telecommunications operators and others, to use the EDR system. These companies may use the EDR on the basis of an individual ministerial authorisation, which is granted according to the specific needs and requirements of the company in question, ensuring that large enterprises playing a key role in the national economy and infrastructure have access to a secure and reliable communications network.

8.5.2.4 Organisation and Management

Pro-M Zrt. is a key provider of government communication services in Hungary, responsible for the operation of the EDR (Egységes Digitális Rádiórendszer) system. This company, a subsidiary of NISZ Zrt., manages and operates the EDR system under the supervision of the Ministry of the Interior.

Pro-M Zrt. is responsible for ensuring that the EDR system operates reliably and efficiently so that it can support a wide range of organisations involved in public safety and crisis management. This includes coordination and cooperation with various agencies, such as the police, fire service, emergency services and other critical infrastructure.

The EDR system is planned to be supported until 2035, with the aim of ensuring its long-term sustainability and adaptation to new technological challenges. Key future plans include a transition to broadband data services, which will enable faster and more efficient data transmission.

Another significant aspect of future development is the potential use of commercial mobile infrastructure in a hybrid model. This approach would allow for a combination of public and private infrastructure, thereby increasing the capacity and flexibility of the EDR system. A hybrid model could also deliver cost savings and improve service availability in remote areas.

8.5.2.5 International and European cooperation

Hungary adheres to European and international standards in radio spectrum management, thereby ensuring harmonisation and efficient spectrum management for PPDR applications. This approach involves compliance with the recommendations of the European Conference of Postal and Telecommunications Administrations (CEPT) and the International Telecommunication Union (ITU).

European directives and decisions concerning radio spectrum management are implemented into Hungary's national legal framework. This process involves the adoption and application of legislative acts that ensure national regulations are in line with European requirements. The implementation of European directives ensures that Hungary adheres to uniform standards and procedures.

By adhering to European and international standards, Hungary ensures that its national radio spectrum management policy is harmonised with that of other countries.

CEPT and ITU Recommendations

CEPT (European Conference of Postal and Telecommunications Administrations) issues recommendations and decisions that establish harmonised conditions for the use of the radio spectrum.

The ITU (International Telecommunication Union) is a specialised agency of the United Nations that coordinates global radio spectrum management and develops international standards.

8.5.3 5G PPDR project on the Hungarian-Ukrainian border

The 5G-PPDR (Public Protection and Disaster Relief) project aims to provide high-quality, secure and resilient communications for the police, border guards and emergency services on the Hungarian-Ukrainian border. This project, funded by the European Union, involves the development and implementation of a 5G-based mobile broadband network. The main objectives of the project include ensuring secure communications, enhancing border security, delivering environmental and climate benefits, and supporting digitalisation in the EU.

The aim of the project is to build a 5G infrastructure based on PPDR-BB at the EU's external border between Hungary and Ukraine. This network is designed to be disaster-resilient and to ensure secure and reliable real-time communication for national ambulance, police and border units. The project focuses on enhancing security through the protection of the Schengen border. Given the current situation in Ukraine and the risks associated with migration and terrorism, this aspect of the project is particularly relevant. The project contributes to environmental protection and the reduction of CO2 emissions through the transmission of real-time imagery via drones. It also improves the flow of information in the event of local natural disasters and ensures safer monitoring and tracking of the transport of hazardous materials. The PPDR 5G project supports the European Union's digitalisation efforts and introduces best practices that can be utilised at EU level. It provides broadband access to users and enhances the quality of public services.

The network roll-out involves the deployment of 17 next-generation (gNB) 5G base stations and a separate 5G core network for service operation. These base stations and the core network will provide minimum download and upload speeds of 3 Mbps and 2 Mbps, with latency below 5 ms. The 5G network core will be private and based on cloud solutions, ensuring a high level of security. Applications developed as part of the project will also utilise private cloud solutions.

The total project budget is €5.3 million, of which €4 million comes from the Connecting Europe Facility (CEF) Digital programme. In the long term, emergency services will contribute to the funding, as they will be exempt from charges due to their public service status.

The project is led by Pro-M Zrt., a mobile network operator and provider of PPDR telecommunications services. Key partners include IdomSoft Ltd, the National Rescue Service, the National Police Headquarters and the Hungarian Defence Forces Headquarters. These partners will utilise the infrastructure and applications developed to respond more effectively to emergencies and ensure safety.

The project will provide 5G radio coverage in areas not previously covered, as well as a 5G core network. Seventeen base stations will be deployed and 500 5G-capable smart devices distributed. Several applications will also be developed to support emergency services. The project is scheduled to run from 1 January 2023 to 31 December 2025.

9 Security threats

9.1 Cyber threats

Cyber threats include various types of attacks that may target information systems and infrastructure. The most common include malware, ransomware, phishing, spear-phishing and supply chain attacks. Specific threats to 5G networks include attacks on network architecture, exploitation of vulnerabilities in network protocols, and Denial of Service (DoS) attacks.

Due to their more complex architecture and higher throughput, 5G networks present new challenges in the field of cybersecurity. The higher number of devices connected to the network, the widespread use of software-defined networking (SDN) and network function virtualisation (NFV) can lead to new vulnerabilities. The expansion of IoT device usage also increases the risk of massive botnets, which can be exploited for DDoS attacks.

9.1.1 Examples of cyber attacks and their impact on PPDR

Ransomware attacks: These attacks are particularly dangerous for PPDR as they can encrypt critical data and block access to vital systems. For example, ransomware attacks such as WannaCry or NotPetya can paralyse infrastructure and demand high ransoms to restore access.

Phishing and spear-phishing: These social engineering techniques often target staff with the aim of obtaining login credentials or infecting systems with malware. Phishing campaigns, which are becoming increasingly sophisticated, can lead to leaks of sensitive data or the compromise of internal networks.

DDoS attacks: Distributed Denial of Service (DDoS) attacks can overload servers and networks, leading to service unavailability. In the context of PPDR, DDoS attacks can prevent communication and coordination between emergency services during crisis situations
.

9.1.2 Measures and technologies to protect against cyber threats

To protect against cyber threats, it is necessary to implement a comprehensive set of measures and technologies, including:

Network infrastructure security: The use of advanced firewalls, intrusion detection/prevention systems (IDS/IPS) and communication encryption are fundamental security elements. Implementing network segmentation and using VPNs to secure communication between individual network components can significantly reduce the risk of attacks.

Threat monitoring and detection: Proactive monitoring using SIEM (Security Information and Event Management) systems enables the early detection of and response to suspicious activity. Network traffic analysis can help identify anomalies indicating an ongoing attack.

Endpoint protection: Deploying antivirus and anti-malware software on endpoints and servers, along with regular system updates and patching, is key to minimising vulnerabilities. The use of EDR (Endpoint Detection and Response) solutions provides better control and protection against advanced threats.

Education and training: Regular staff training focused on recognising phishing attacks and safe behaviour when using IT technologies is essential for reducing risk.

Redundancy and backup: The implementation of redundant systems and regular data backups ensure business continuity and rapid recovery following a cyber incident. Backups should be stored offline to protect against ransomware attacks.

Cooperation and information sharing: Cooperation between the public and private sectors, and the sharing of information on current threats and incidents, is key to an effective response to cyber attacks. Within the Czech Republic, this cooperation is facilitated by NÚKIB in conjunction with other authorities and organisations.

9.2 Terrorist attacks

Terrorist attacks may take the form of physical attacks on infrastructure, cyber attacks on critical systems, or a combination of both. In the context of PPDR, the targets of terrorist threats are primarily communication networks, energy sources, healthcare facilities and other elements of infrastructure that are essential for an effective response to crisis situations.

9.2.1 Examples of terrorist attacks on communications infrastructure

Cyber attacks: Attacks on communication networks and infrastructure include, for example, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which can take key communication channels offline.

Physical attacks: Examples of physical attacks include bomb attacks on telecommunications centres or acts of sabotage against infrastructure such as transmitters and data centres. These attacks can cause widespread disruption to communication services and threaten public safety.

9.2.2 Prevention and response to terrorist threats

Prevention and response to terrorist threats require a comprehensive and coordinated approach involving several measures:

Monitoring and analysis: The first step is the continuous monitoring and analysis of potential threats. This includes monitoring online activity, identifying radicalised individuals and groups, and analysing information from various sources. It is also important to train security personnel in methods for identifying and reporting suspicious activity.

Infrastructure security: The implementation of both physical and cyber security measures is crucial. This includes, for example, fortifying and protecting critical facilities, installing advanced security systems, and regularly updating software and hardware.

Cooperation and communication: Effective communication and cooperation between security agencies, the public and relevant bodies is essential.

Legislation and regulation: The introduction of legislative measures to enable a swift and effective response to terrorist threats. This includes, for example, the Regulation of the European Parliament and of the Council on combating the dissemination of terrorist content online, which focuses on the rapid removal of terrorist content from the internet and the harmonisation of obligations for internet service providers across the EU.

Education and awareness-raising: Regular training and education for all relevant stakeholders, including the public, is key to raising awareness of terrorist threats and the ability to respond to them effectively.

9.3 Natural disasters

Natural disasters such as floods, earthquakes, hurricanes, tornadoes and wildfires – these disasters can cause physical damage.

9.3.1 Examples of natural disasters and the subsequent crisis management response

Floods: The 2002 floods in the Czech Republic caused widespread disruption to telecommunications services, which significantly hampered crisis communication and the coordination of rescue efforts. Crisis management had to rely on backup communication methods and improvised systems to ensure the coordination of rescue operations.

Earthquakes: The 2016 earthquake in Italy led to extensive damage to infrastructure, including communication networks. The crisis management response involved the rapid mobilisation of backup systems and temporary communication means, such as satellite phones and mobile base stations.

Forest fires: The 2020 California wildfires caused widespread power and communications network outages. Crisis management utilised drones and mobile communications units to restore communications and coordinate evacuations and firefighting operations.

9.3.2 Environmental security in the Czech Republic

Environmental security is a state in which the probability of a crisis situation arising from environmental disruption is still acceptable. In relation to ecosystem services, it can be defined as the long-term maintenance of ecosystem services that determine the quality of human life. The purpose of all activities in environmental security is to link environmental protection with the security interests of the Czech Republic. Individual components of the environment as well as entire ecosystems may be at risk, with both long-term and short-term impacts. It is necessary to take into account the interdependence of these risks and to create an integrated system of preventive, mitigation and adaptation measures. In the Czech Republic, the Ministry of the Environment (MoE) is the lead agency in this area, managing the climate change adaptation strategy and the Czech Republic 2030 strategic framework.

9.3.3 Measures to minimise the risks and consequences of natural disasters

Backup and redundant systems: Implementation of backup systems and redundant infrastructure to ensure service continuity – backup power supplies, backup servers and mobile base stations that can be rapidly deployed in the event of a failure.

Resilient infrastructure: Construction of more resilient infrastructure capable of better withstanding natural disasters – use of water- and earthquake-resistant materials and siting of critical facilities in safer locations.

Monitoring and early warning: Implementation of advanced monitoring and early warning systems capable of detecting natural disasters and enabling a rapid response – sensors, drones and satellites that provide up-to-date data on the condition of infrastructure and natural conditions.

Training and exercises: Regular crisis management training and exercises for emergency services and other relevant bodies. This ensures preparedness for crisis situations and improves the ability to respond quickly and effectively to natural disasters.

To manage natural disasters effectively, it is essential to integrate environmental security into crisis management, linking environmental protection with the security interests of the Czech Republic.

9.4 Pandemics

Pandemics, such as COVID-19, have a significant impact on communications infrastructure and crisis management. Increased communication volumes, network congestion and the need for rapid information sharing between emergency services and the public require robust and reliable communications systems. Remote working and education also became critical during the pandemic, placing further demands on the capacity and stability of communication networks.

The COVID-19 pandemic has highlighted the importance of fast and reliable data transmission. Thanks to their high speed and low latency, 5G networks can make a significant contribution to effective crisis communication. They enable faster transmission of large volumes of data, support for telemedicine, contact tracing and other key applications. In South Korea, for example, 5G technology was used to track the spread of the virus and keep the public informed.

9.4.1 Prevention and preparedness for future pandemics

To prevent and prepare for future pandemics, the following measures should be implemented:

Strengthening infrastructure: Ensuring a robust and resilient communications infrastructure capable of handling increased traffic and enabling rapid switching between primary and backup systems.

Integration of 5G technologies: Utilising 5G networks for rapid data transmission, supporting telemedicine and remote working, which is essential for effective crisis management and pandemic response.

Development of monitoring and information applications: Implementation of applications and systems to track the spread of infections, conduct contact tracing, and rapidly inform the public about current measures and recommendations.

International cooperation: Sharing of information, resources and technologies between states and international organisations for a coordinated response to global health threats.

9.5 Geopolitical conflicts

In recent years, the international security environment has deteriorated significantly. A key factor in this destabilisation is Russia's military aggression against Ukraine. This conflict is not merely a struggle for Ukraine's sovereignty and territorial integrity, but represents a broader threat to the international order.

Conflicts such as the war in Ukraine, the crisis in the Middle East or instability in Africa have a fundamental impact on global security. These conflicts not only affect the security situation in the regions concerned, but also have wider implications for economic and political stability worldwide.

The Czech Republic's military intelligence highlights growing cyber threats and information operations by foreign powers. These activities include targeted phishing campaigns, the creation of polymorphic malware, and the use of large language models to spread propaganda and disinformation. Deepfake videos are particularly dangerous, as they can be used to discredit public figures or to manipulate public opinion.

9.5.1 Prevention and preparedness

Prevention and preparedness are crucial for minimising the risks and consequences of geopolitical conflicts. The Czech Republic focuses on regularly updating its security strategies and contingency plans, which include identifying potential threats and assessing their impacts. As part of prevention efforts, crisis management training and exercises are conducted to ensure that all parts of the public administration and the private sector are prepared for various crisis scenarios.

Enhancing cyber security: Cyber threats pose a significant risk to national security. The Czech Republic is therefore investing in enhancing cyber security, protecting critical infrastructure, strengthening cyber defence capabilities and training experts in the field of cyber security. In addition, new technologies and procedures are being developed for the detection and prevention of cyber attacks.

International cooperation: The Czech Republic actively cooperates with NATO, the EU and other international organisations on information sharing, the coordination of defence strategies and joint training.

Strengthening economic resilience: Geopolitical conflicts can have significant economic repercussions. To minimise these consequences, the Czech Republic is focusing on diversifying its economic resources and strengthening strategic reserves. Investment in innovation and technological development helps to maintain economic stability even in times of crisis. Support for the domestic defence industry is also part of economic resilience.

Public education and information: To strengthen societal resilience, campaigns are being carried out to raise awareness of security issues, alongside educational programmes and transparent communication between the government and citizens.

Crisis management and response to crisis situations: Effective crisis management is fundamental to minimising the impact of geopolitical conflicts. The Czech Republic has a well-developed crisis management system, which includes security councils, crisis management teams and standing working groups responsible for coordinating the response to crisis situations, mobilising resources and providing support to affected areas.

9.6 The Czech Republic's Perspective

The Czech Republic's security strategy reflects the dynamic and complex threats facing our country in the current global environment. A key role in this strategy is played not only by safeguarding sovereignty and territorial integrity, but also by protecting citizens' fundamental rights and freedoms, ensuring economic stability, and building society's resilience to various types of crises and conflicts.

The Czech Republic is situated in the heart of Europe, and its geopolitical position requires active participation in international organisations such as NATO and the European Union, which provide a platform for collective defence and security. In the context of current security challenges, the Czech Republic recognises the importance of international cooperation and solidarity.

9.6.1 Security priorities

Defence of sovereignty and territorial integrity: The Czech Republic places emphasis on the defence of its territory through the modernisation of its armed forces and participation in NATO's collective defence.

Cyber and information security: With the growing number of cyber attacks and disinformation campaigns, the Czech Republic is focusing on strengthening cyber security and protecting critical information systems.

Economic resilience: The Czech Republic is seeking to diversify its supply chains and ensure energy security through investment in renewable energy sources and strategic reserves.

Civil protection and crisis management: The Czech Republic is investing in the modernisation of its emergency services and improving coordination between the various actors involved in crisis management.

One of the key aspects of the security strategy is the integration of the services of the armed forces and the Ministry of the Interior. In this regard, the Directorate of Information and Communication Systems Services of the Ministry of Defence (Ř SKIS MO) plays a significant role, acting as the Ministry of Defence's digital representative. This integration enables the effective sharing of information and resources between the armed forces and civilian crisis management units.

9.7 The EU's perspective

The European Union regards geopolitical conflicts as a significant threat to security and stability in the region and emphasises collective defence and cooperation between Member States to address these challenges; it supports the development of Member States' defence capabilities through investment in modern technologies and research.

Particular attention is paid to cybersecurity, an area in which the EU has established a number of initiatives and standards. The European Union Agency for Cybersecurity (ENISA) supports Member States in improving their cyber defences and in establishing common security standards for technologies such as 5G. Through cooperation with international partners such as NATO and the UN, the EU also seeks to strengthen the global security architecture.

9.7.1.1 NATO

In relation to civil protection and disaster relief, the European Union and NATO play a key role in ensuring security and coordinating an effective response to crisis situations

The European Union utilises its cooperation with NATO to strengthen its capacity to respond to security threats and emergencies. This cooperation facilitates information sharing, joint planning and training, leading to the effective mobilisation of resources and the provision of necessary assistance during crisis situations.

NATO also contributes to ensuring regional stability and security in the Euro-Atlantic area, including support for crisis management and disaster response. Organisations such as the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) provide a platform for coordinating international assistance and support in the event of disasters, including activities related to PPDR.

One aspect of cooperation between the EU and NATO is the harmonisation of frequency bands and the standardisation of communication technologies for PPDR. ITU-R Resolution 646 (REV.WRC 15) encourages administrations to identify and harmonise frequency bands for advanced PPDR solutions. It recommends the use of the 380–470 MHz and 694–894 MHz frequency bands, with the 380–385/390–395 MHz band being preferred for permanent civil protection activities.

The Treaty of Lisbon, specifically Article 196, strongly supports cooperation in the field of civil protection and PPDR. This article facilitates cooperation between EU Member States and partners such as NATO, with the aim of improving disaster response capabilities and ensuring the safety of the population. Thanks to the Treaty of Lisbon, resources are being effectively coordinated and shared between the EU and NATO.

10 Application possibilities

In the world of mobile communication systems, there are three main categories of use, which differ according to user objectives and corresponding configuration requirements (in terms of end-user devices, technology, network functions, characteristics, standardisation, etc.). The commercial segment targets commercial users for their everyday communication needs. At the other end of the spectrum are critical systems, comprising primarily Business Critical and Mission Critical systems, which require mobile radio systems capable of providing secure and reliable communication in the most extreme or specific conditions.

Business Critical systems generally serve organisations operating in environments with high economic value and/or sensitive information.

Mission-critical systems are designed for operations where failure could result in serious safety or security breaches, injury, loss of life, or cause significant harm to society or the environment. Their users are predominantly PPDR (Police, Fire and Rescue) personnel.

The main objective of critical systems in general is to ensure the efficiency and effectiveness of systems in critical situations. Mission-critical systems are centred on the safety and security of society, which means that profitability is secondary and the public interest is the priority.

10.1 Classification of communication systems

10.1.1 Commercial segment

The commercial segment focuses on ordinary users who utilise mobile communication systems for their everyday personal and work needs. These systems are designed to be profitable, competitive and reliable in most situations, but do not require the same level of resilience and security as critical systems.

10.1.2 Critical systems

Critical systems are designed to provide secure and reliable communication in demanding conditions. These systems are divided into two main categories: Business Critical and Mission Critical systems.

10.1.2.1 Business Critical systems

Business Critical systems serve organisations operating in environments where significant economic value or sensitive information is at risk.

10.1.2.2 Mission-Critical Systems

Mission Critical systems are intended for operations where failure could result in serious safety or security breaches, injury, loss of life, or significant damage to society or the environment. Typical users of these systems are PPDR services. These systems are designed to be as reliable and available as possible under all circumstances, including crises and outages.

10.2 Classification of critical systems

Abroad, these systems are divided into Business Critical (BC) and Mission Critical (MC). The table below compares these categories. In this document, in Chapter 2, we divide incidents into five categories, with Category 1 (Minor Incidents) and Category 2 (Medium Incidents) classified as BC, and Category 3 (Major Incidents) through to Category 5 (International Incidents) as MC. The entire system defines the requirements for the communication system. Abroad, it is reported that commercial networks are used for certain types of communication, but dedicated and reinforced networks should be provided for MC.

The entire IZS operational system needs to be integrated into a single platform or system that would allow for mutual substitutability and could also be complementary. This can be addressed at both the central and end-user levels. For the end-user, it is advisable to use LiveU, whilst the central part should be managed via the CORE communication platform.

The dimensions of critical systems encompass several key aspects that determine their design, use and performance. The following table provides an overview of these dimensions and compares Business Critical (BC) and Mission Critical (MC) systems. The dimensions of critical systems encompass several key aspects that determine their design, use and performance:

DIMENSIONS	BUSINESS CRITICAL (BC)	MISSION CRITICAL (MC)
DESIGN PRINCIPLES	Profitability, competitiveness and reliability in most situations	Full redundancy, reinforcement, maximum reliability, priority and precedence
TARGET AUDIENCE	Commercial and industrial organisations, private users	Public safety and associated organisations
NETWORK TYPE	Commercial networks	Dedicated and hardened networks
APPLICATION SCALABILITY AND FUNCTIONALITY	Development and innovation in line with market pace	Need for standardisation before reaching mission-critical levels
COMMUNICATION AVAILABILITY	Under normal or moderately critical conditions	Under all circumstances, including crises and outages
IMPACT IN THE EVENT OF FAILURE	Economic losses or compromise of sensitive information	Risk of loss of life and significant material damage
COVERAGE	≤ 99.5% of the population	≥ 99.5% of the territory
BACKUP TIME IN THE EVENT OF A POWER FAILURE	≤ 2 hours	≥ 8 hours

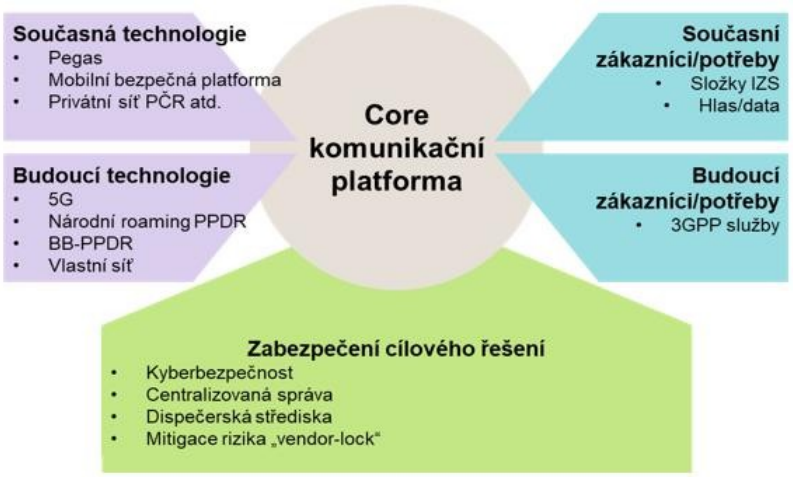
Overall, this table illustrates how the requirements for Business Critical and Mission Critical systems differ depending on their specific use and needs, with an emphasis on a higher level of reliability, resilience and availability for MC systems.

10.2.1 CORE Communication Platform

The CORE platform is a key element in the modernisation and provision of a robust and secure communications infrastructure for the Integrated Rescue System (IRS) units in the Czech Republic. Given the constantly changing environment, technological advances and growing demands for efficiency and speed of response, it is essential to provide the IRS units with a modern, reliable and broadband communications system.

The CORE platform is the result of a comprehensive analysis of the needs and requirements of individual emergency services, including the Czech Police, the Fire and Rescue Service and the Emergency Medical Service. The platform aims to replace existing, often unconnected and outdated systems, and to create a unified and integrated communications infrastructure. The emphasis is on enhancing cyber security, improving interoperability between individual units, and ensuring high availability and resilience of communication resources even in crisis situations.

The creation of the platform also reflects the need to transition from traditional voice communication systems to modern data services that enable the rapid and accurate exchange of multimedia information flows. The implementation of CORE is also closely linked to the results of 5G spectrum auctions, which provide the technical and legislative foundations for the development of high-speed data services.



In addition to ensuring secure and effective communication between emergency services, economic efficiency is also a key aspect, both in terms of investment and operational costs. The CORE communication platform is designed to enable the optimisation of existing resources, the use of modern technologies, and to minimise dependence on external suppliers. It also ensures interoperability and compatibility with European standards and legislative requirements. The CORE platform thus represents not only a technological but also a strategic tool that significantly strengthens the capabilities and preparedness of emergency services to respond to a wide range of crisis situations.

10.3 Minimum requirements for PPDR devices

The minimum requirements for public safety and emergency response equipment are based on the document "PPDR Rugged Handheld Device for Heavy Use" from NCCOM (Nordic Critical Communication Operators Meeting). This document provides detailed guidance for device manufacturers to understand the common requirements of PPDR users in the Nordic countries, and sets out minimum, supplementary and future requirements for rugged handheld devices designed for heavy use in demanding conditions. The document was developed in collaboration with PPDR operators in Denmark, Finland, Norway, Sweden and Iceland and ensures that devices meet high standards for safety and reliability.

Given the detailed specifications and high standards in the Nordic countries, this document can serve as inspiration and a reference point for the mapping and implementation of similar systems in the Czech Republic. The aim is to ensure that PPDR systems achieve a high level of reliability and safety.

10.3.1 Environmental requirements

Equipment intended for heavy-duty use in PPDR environments must be capable of functioning effectively in demanding conditions and withstanding physical threats such as humidity, water, dust, heat and cold. The equipment must be designed to withstand repeated drops from typical operating heights onto hard surfaces without damage. Touchscreens and other displays must be easily readable in all lighting conditions.

10.3.2 Hardware specifications

PTT button: The device must be equipped with a dedicated push-to-talk (PTT) button that is tactile, easily identifiable and easy to operate, including the ability to operate it whilst wearing protective gloves.

Emergency button: The device must have a dedicated emergency button that is tactile, colour-coded (e.g. red) and located on the top of the device. The button must be easily accessible and operable even when wearing protective gloves.

Talk group selection switch: The device must be equipped with easy-to-operate buttons that allow for easy and seamless switching between talk groups. The buttons must be protected against accidental use and operable even when wearing protective gloves, without the need for visual assistance.

Display: The display must have sufficient resolution and size to support effective interaction with MCX applications. It must be scratch-resistant and legible in bright sunlight as well as in complete darkness. The display must automatically adjust its brightness

to changing light conditions and allow it to be switched off during PTT operations. Users must be able to operate the touchscreen even when wet and whilst wearing gloves.

Speaker and microphone: The device must include speakers and microphones that enable clear communication under all normal conditions, including noisy environments. The speaker/microphone must be designed to account for factors such as wind or loud sirens and ensure clear audio for call participants, even in situations where sirens are sounding. Furthermore, the device and its accessories must protect the user from sudden loud bursts of sound and warn of potential danger.

Camera: The device must be equipped with a front camera with a minimum resolution of 2 megapixels and a rear camera with a minimum resolution of 8 megapixels and a flash. The cameras must be capable of capturing high-quality photos and videos with sufficient detail to identify people and objects, such as number plates. The cameras must function in both daylight and low-light conditions.

Battery: The device and its battery must be optimised so that:

– A duty cycle of 80% standby / 20% active use at +20 °C and –110 dBm RSRP signal lasts for at least 12 hours when using the MCX application.

– A duty cycle of 80% standby / 20% active use at -20 °C and –110 dBm RSRP signal lasted for at least 6 hours when using the MCX application.

– After 1,000 charge cycles (20% to 100% charge), the battery retains at least 85% of its original capacity.

The device must be capable of charging from 0 to 50% in half an hour when using a high-power fast charger. The battery must be easily replaceable by the user without specialised tools or technical expertise, without compromising the device's protection rating.

Connectors for peripheral devices: All physical connectors for peripheral devices must be waterproof, robust and designed for heavy-duty use. Connectors must provide robust, easy-to-use and secure locking mechanisms to prevent accidental disconnection. In addition to the standard USB-C connector, the following connectors are required as a minimum:

– Audio jack (2.5 or 3.5 mm) with PTT support

– Side or bottom connector with support for PTT, emergency button and audio

– Exposed charging pins enabling robust charging, e.g. pogo pins for charging in single and multi-docking stations

– Bluetooth version 5.0 or higher and NFC for pairing. Ability to block Bluetooth usage via EMM. Bluetooth must support Secure Connections security mode 4, level 4.

All connectors must be usable simultaneously to allow connection of multiple accessories, e.g. body-worn cameras, external screens and RSMs.

10.3.3 Accessories

The device manufacturer must be able to provide or support several accessories for the device: Single and multi-

docking stations and chargers

Headphones with a PTT button connected to the device via a side connector with a robust locking mechanism, e.g. USB-C or audio jack.

All accessories must be waterproof, robust and designed for heavy-duty use, capable of utilising a robust, easy-to-use and secure locking mechanism to prevent accidental disconnection.

10.3.4 Wi-Fi hotspot capability

The device must be capable of functioning as a Wi-Fi hotspot. The ability to block this feature via EMM.

10.3.5 Device-to-device communication

TETRA DMO (direct-mode operation) will be used until 3GPP technology provides a proven solution for device-to-device (D2D) communication, and interoperability with PPDR TETRA DMO is no longer required. This capability must be supported either by the device itself or in conjunction with accessories.

10.3.6 RF OTA antenna performance

RF antenna performance must be as good as possible, in accordance with the RF OTA performance criteria measured in accordance with 3GPP TR 37.977 V17.0.0 and 3GPP TR 25.914 V17.0.0. The device must support at least the ITU Region 1 Band 8 (900 MHz) and Band 20 (800
MHz), Band 28 (700 MHz), Band 3 (1800 MHz) and Band 1 (2100 MHz).

10.3.7 Security and firmware

The device must meet the baseline level of security requirements for each country, which is the minimum level required for PPDR users. These requirements are typically equivalent to the RESTRICTED classification.

Lifecycle support: A long device lifecycle and the ability to provide continuous support are important for PPDR users. This includes chipset maintenance, firmware updates and security updates. Updates to the latest operating system (OS) must be available throughout the lifecycle, along with the latest security and firmware updates, including bug fixes. Updates containing new features and bug fixes must be available at regular intervals. Security and emergency updates must be available immediately. The device manufacturer must provide support for the device for a minimum of five (5) years from its launch.

Internet access: The device must be capable of functioning fully without relying on internet access during registration or operation.

Third-party management: The device must be capable of being managed by a third-party EMM solution installed on-premises and may be restricted to a closed network, i.e. completely isolated from public internet connections, for example using AOSP (Android Open Source Project). It must be possible to manage all software updates via the EMM.

Control of external IP connections: To ensure device security, manufacturers should provide detailed information on outbound connection points during device boot-up, activation and operation, etc. This information includes IP addresses, domain names and communication protocols. PPDR operators must have control over these connections so that they can monitor, block and allow connections as required. Device security requires collaboration between the manufacturer and the PPDR operator to protect sensitive data and prevent security breaches.

Permitted applications: Only critical system applications and those necessary for the proper functioning of the device and required for the MCX application should be included in the firmware and operating system. The manufacturer must provide the PPDR operator with a list of applications and detailed information on their purpose and the reasons why they are required on the device.

Device access: The device must support various access security methods, e.g. PIN, password, fingerprint and facial recognition. To enhance security, the device must support a configurable function for failed password attempts, which initiates a factory reset after a specified number of failed password attempts has been exceeded. The number of failed attempts must be configurable. The manufacturer should provide instructions for managing this function to ensure optimal device security.

Standardisation and certification: Devices used in LTE- and 5G-based PPDR networks must:

- Bear a valid CE mark
- Have a unique IMEI code that has not been and will not be used in other devices
- Be certified by the Global Certification Forum (GCF) for compliance with 3GPP
- Support 3GPP Mission Critical Services, including MCX client functionality, which complies with the 3GPP specifications for critical communications (Release 16 or later). This verification is established by the provision of a certificate of conformity based on the GCF Mission Critical Services certification procedures.
- Be accompanied by an RF OTA test report.

Location services: The device must be compatible with Global Navigation Satellite System (GNSS) receivers and function with at least the Galileo and GPS systems, alongside location services provided by the mobile network. Indoor location services must be available using existing technologies, i.e. Bluetooth or Wi-Fi.

10.4 Complementary requirements

Complementary requirements for PPDR devices provide further specifications and may be more stringent than the minimum requirements. These requirements are designed to meet specific needs in more demanding situations or environments.

10.4.1 Additional environmental requirements

In some cases, it is necessary to tighten the environmental requirements for devices intended for heavy-duty use. These devices should support:

Operating temperature range: -30 to +55 degrees Celsius

Resistance to drops from a height of 3 metres onto hard, rough surfaces without damage

Protective mechanisms for contacts, seals and casings to prevent corrosion following contact with salt water

10.4.2 Additional hardware requirements

Programmable buttons: Devices should have programmable buttons that can be configured via EMM (Enterprise Mobility Management). Each button should be programmable with specific functions within applications, such as a second PTT button, sending predefined messages, or system functions such as selecting a talk group and opening applications.

Battery: Additional battery requirements include:

– A duty cycle of 80% standby / 20% active use at +20 °C and -110 dBm RSRP should last for at least 16 hours when using the MCX application.

– After 2000 charge cycles (20% to 100% charge), the battery should retain 90% of its original capacity.

– Support for wireless charging compatible with Qi 1 and Qi 2.

– The battery should be replaceable without interrupting MCX communication, enabling hot swapping.

Connectors for peripheral devices: The device should be equipped with an external antenna connector, which improves usability and expands application possibilities.

10.4.3 Additional accessories

The device manufacturer should be able to provide or support the following accessories:

– Single and multi-charger banks for replaceable batteries

– Vehicle mounts that enable charging and facilitate connection to external antennas, audio accessories and in-vehicle displays

10.4.4 Additional security and firmware requirements

Lifecycle support: Continuous lifecycle extension is important, and the device manufacturer should provide full support for the device for a period of six (6) years from its launch.

Support for MC services: Large-scale operations require solutions that enable capacity sharing among many users. The device should support broadcast/multicast services (eMBMS, MBS).

End-to-End Encryption (E2EE): PPDR organisations need to communicate and share information without the risk of interception or leakage of sensitive information. The device should be capable of supporting end-to-end encryption solutions that are interoperable with existing end-to-end encryption solutions in TETRA devices. This functionality is provided by third parties via smart cards that are inserted into the device.

10.5 Future requirements

Future requirements for PPDR devices take into account the rapid development of mobile technologies and standardisation. Suppliers should collaborate with the PPDR community to ensure that new features and improvements are continually added and that devices are capable of supporting the latest technologies and standards.

10.5.1 Hardware

Call group selection via a rotary switch: To facilitate smooth switching between call groups, even when wearing protective gloves and without the need for visual assistance, the device should feature a button that is easily operable by touch, such as a rotary switch.

Device-to-device communication: Users need access to reliable and predictable communication services even in the absence of a network connection. Device manufacturers should monitor and contribute to the development of a standardised 3GPP solution to replace the current DMO (direct-mode operation) and implement it in devices.

RF OTA antenna performance: In addition to minimum and complementary frequency requirements, the device should support ITU Region 1 B68 (698–703 MHz) and, to enhance indoor coverage, n40 (2300 MHz), n22 (3500 MHz), n74 (1500 MHz), n258 26 GHz (24.25–27.5 GHz). To ensure wide geographical coverage and achieve the required RF OTA performance, an external antenna solution compatible with frequencies below 1 GHz may be used.

– Carrier aggregation should support the following band aggregation combinations:
  – CA combo LTE B20 + NR28
  – CA combo LTE B1 + LTE B3 + LTE B20

Lifecycle support: In future, device manufacturers are expected to provide full support for devices for a period of six (6) years from their launch.

Location services: The PPDR community's access to reliable position and time information is essential for all critical service operations. PPDR users rely on accurate, high-quality positions that are protected from external interference. Devices should support the Galileo Public Regulated Service (PRS) as soon as it becomes available for implementation. Among other things, this means that the receiver must be capable of receiving the PRS signal on the E1 and E6 frequency bands. The GNSS receiver should have protective mechanisms to prevent jamming and spoofing.

Device-to-satellite communication: PPDR users operating in remote areas without mobile network coverage are dependent on other means of communication. Device manufacturers should monitor and ideally contribute to standardisation initiatives within 3GPP and TCCA to find a solution for device-to-satellite (NTN) communication to be implemented in the device.

10.6 Key phases of broadband MCS implementation

The implementation of broadband communication systems for Mission Critical Communication Systems (MCS) involves several key phases. Each of these phases has its own activities and objectives, which are essential to the success of the entire programme.

1. **Strategy:** Conducting a comprehensive study of network requirements for critical operations, overall objectives, needs and intentions. This phase is crucial for determining the project's viability, including funding, spectrum allocation, coverage identification and stakeholder engagement. The strategy also defines the project's business model and implementation plan.
2. **Concept:** A detailed description of the MCS programme's use cases, which helps to refine its overall objectives. Based on these use cases, proof-of-concept studies are carried out to obtain feedback and user acceptance of these defined use cases.
3. **Planning and Design:** Defines the detailed technical architecture of the MCS system, covering network architecture (construction of new masts, modernisation of existing infrastructure) and technical and functional specifications for the core, RAN, user equipment and active network components. Planning and design also establishes standardised equipment, protocols and procedures to ensure interoperability.
4. **Procurement:** Various procurement models are defined based on requests for proposals (RFPs) issued to solicit bids for the construction of network infrastructure, the purchase of equipment and the necessary services. These bids are evaluated technically and commercially, ensuring that procurement processes are transparent and efficient when placing orders and negotiating contracts.
5. **Implementation:** Once the contract has been awarded to the implementing agencies, the implementation phase begins the roll-out of the MCS system based on its detailed design and technical architecture. This is followed by the deployment of the physical network infrastructure, delivery, installation, commissioning, testing of user devices and applications, and training and capacity-building programmes for end-users. During this phase, end-users conduct user acceptance testing (UAT) to verify the project implementation and set up a sandbox environment to ensure network security and stability.
6. **Optimisation:** During optimisation, the MCS network is tested and monitored for performance, reliability and security. Based on these observations, improvements are made to enhance performance and services. Key performance indicators (KPIs) and SLAs are monitored to ensure service quality and a better user experience.

10.7 Factors for successful MCS implementation

Successful implementation of a Mission Critical System (MCS) requires careful consideration of several key factors.

Allocation of required funding: Securing sufficient funding for the implementation of a mission-critical broadband communications network often influences the implementation timeline.

Spectrum allocation: Securing the required spectrum and bandwidth is essential for the success of a critical communications programme.

Stakeholder support: It is essential that all relevant parties are supportive, committed to the programme's success, and fulfil their roles at each stage.

Interoperability issues between different public safety agencies: Enabling seamless information exchange between multiple public safety agencies is essential, as each agency may be at a different level of maturity regarding critical mission communication systems.

Standardisation of equipment and protocols: Compatibility and standardisation of all equipment and protocols are essential to prevent potential operational disruptions and to enable various use cases.

End-to-end security: End-to-end security of mission-critical communication networks is essential, including data encryption and protection against cyber attacks.

Coverage: Providing comprehensive network availability and coverage across the entire service area is important for the ability to respond to crises in remote areas.

Procurement process: Effective management of the procurement process is important for obtaining the best value for money and preventing unexpected costs and budget-related delays.

User adoption: Supporting and facilitating the testing and use of the network for critical communications by all public safety agencies is vital to maximising their efficiency and effectiveness.

Scalability: Ensuring the network's scalability to meet the needs of a growing number of public safety agency users is necessary to prevent service disruption due to insufficient capacity and high load.

Regulation: Compliance with relevant national regulations and policies governing the implementation and use of the critical communications network is essential for the lawful and secure operation of the system.

Public acceptance: Informing the public and gaining their consent regarding the critical communications network is important to prevent potential delays or the halting of the project due to protests or opposition, which should be achieved in the early stages of implementation.

10.8 Key aspects of critical communication systems

Effective and reliable critical communication systems must meet several essential criteria that ensure their functionality and availability under any conditions. The following diagram illustrates the main factors that must be ensured and optimised during the planning, implementation and operation of critical communication systems.

Voice services and management: Critical communication systems must ensure reliable, high-quality voice communication, which is key to effective coordination in crisis situations.

Quality and security: Data security and communication quality are fundamental requirements. Systems must provide a high level of encryption and protection against cyber threats.

Network resilience: Networks must be designed to withstand various physical and environmental influences, including extreme temperatures, humidity and mechanical damage.

Network coverage: Ensuring wide geographical coverage is essential for achieving reliable communication even in remote and hard-to-reach areas.

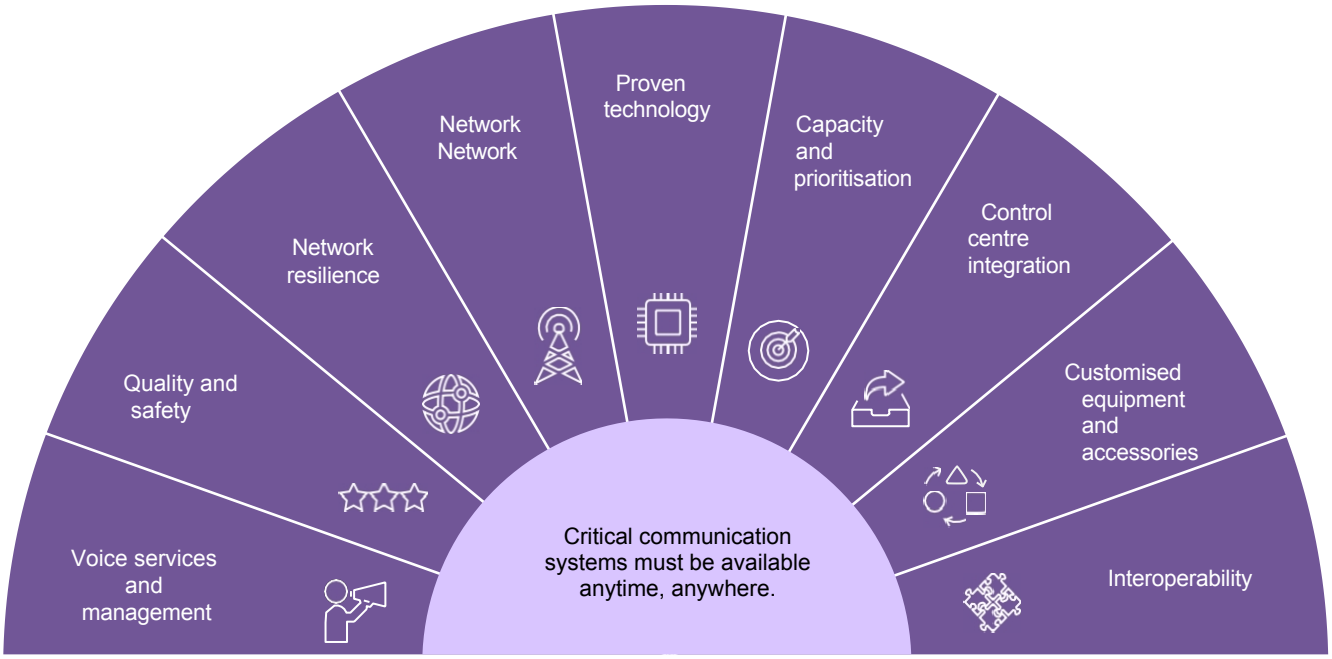
Proven technology: The use of proven and standardised technologies ensures system compatibility and reliability under various conditions.

Capacity and prioritisation: Systems must be capable of handling large volumes of communication and effectively prioritising messages and calls according to their importance.

Control room integration: Integration with control room systems is key to ensuring coordination and effective resource management during crisis situations.

Customised equipment and accessories: Equipment must be tailored to the specific needs of users in crisis situations, including robustness and the ability to operate in demanding conditions.

Interoperability: Ensuring interoperability between different systems and devices is essential for effective collaboration between various agencies and public safety organisations.



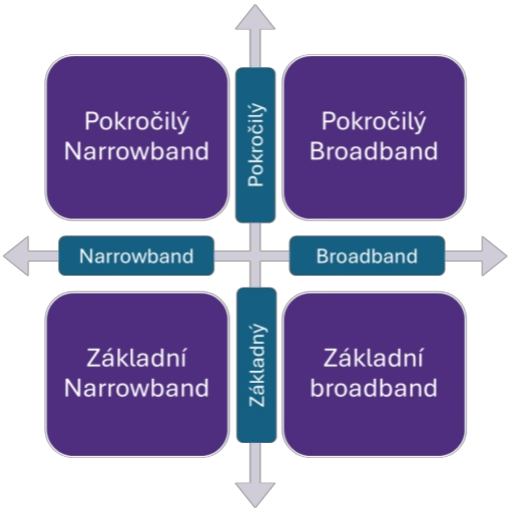
This diagram provides a comprehensive overview of the key aspects that must be addressed to achieve an effective and reliable critical communication system capable of operating anytime, anywhere.

10.9 Practical implementations and examples of MCC-ECO

Real-world implementations of the Mission Critical Communication Ecosystem (MCC-ECO) demonstrate how different countries approach the development and deployment of these systems. Below are various aspects of practical implementation and specific real-world examples.

10.9.1 Categorisation by technology

Countries can be categorised according to their technological implementations in the field of MC communication systems. These categories include:



Critical communication technologies vs. maturity categories

Advanced Narrowband Early adopters of narrowband technologies anticipate user requirements, with continuous investment and progressively improved implementations. Nationwide implementation with dedicated governance mechanisms to optimise investment and ensure universal support for public safety agencies (PSAs).

Advanced Broadband Nationwide public safety over LTE implemented, with a well-functioning MCC-ECO featuring clarity in roles and responsibilities, a robust governance structure, business models, and an appropriate financial strategy, and beginning to utilise new technologies.

Basic narrowband Reactive adoption of narrowband technologies, based on specific user needs. Individual public safety agencies (PSAs) tasked with implementation.

Basic broadband: Discussions have begun on preparations for broadband implementation. This includes discussions with OEMs (Original Equipment Manufacturers) regarding technology selection, pilot implementations, the programme management structure, spectrum allocation, defining a business model to support stakeholders, and appropriate financial mechanisms.

10.9.2 Implementation programmes by country

Each country has embarked on its own path towards the implementation of mission-critical communication systems, influenced by various factors such as the potential impacts of external factors (including accidents, emergencies and potential threats), funding strategies, governance structures, dependence on suppliers and the availability of spectrum bandwidth. Although each country begins this journey from different starting points and with different resource allocations, much can be learnt from the best practices of pioneering nations.

The figure below shows implementation by country according to the 2022 PwC study "The shortest critical path to Next-Generation Public Safety Networks"[12] .

[12] https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/documents/critical-communications-world.pdf

Implementation programmes by country