Grant Thornton

MINISTERSTVO PRŮMYSLU A OBCHODU

Financováno Evropskou unií
NextGenerationEU

Rešerše řešení zajištění bezpečné komunikace státu pro složky IZS v rámci zemí Evropské unie s ohledem na technologická řešení 5G a PPDR

Připraveno pro Ministerstvo průmyslu a obchodu

[Září 2024]

Národní plán obnovy

Obsah

Obsah

Obsah

Obsah

Obsah

Obsah

Seznam zkratek a vysvětlivek

Zkratka	Celé znění	Vysvětlení
3D	Three-Dimensional	Trojrozměrný
3GPP	3rd Generation Partnership Project	Organizace vytvářející technické specifikace pro mobilní telekomunikace, včetně 3G, 4G a 5G standardů
4G	Fourth Generation	Čtvrtá generace mobilních sítí
4K	4K	Ultra vysoké rozlišení
5G	Pátá generace mobilních sítí	Technologie pro bezdrátovou komunikaci
AES	Advanced Encryption Standard	Pokročilý šifrovací standard
AES-128	Advanced Encryption Standard 128-bit	Pokročilý šifrovací standard s délkou klíče 128 bitů
API	Application Programming Interface	Rozhraní pro programování aplikací
AR	Augmented Reality	Rozšířená realita
ARC4	Alleged RC4	Šifrovací algoritmus pro zajištění ochrany dat
BB-PPDR	Broadband PPDR	Širokopásmové služby pro PPDR
BC	Business Critical	
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben	Německo – Federální agentura pro digitální rádiovou komunikaci pro bezpečnostní orgány a organizace
BDBOSG	Gesetz zur Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben	Německo – Zákon o zřízení Spolkového úřadu pro digitální komunikaci bezpečnostních složek a organizací
BRK	Bezpečnostní rada kraje	
BS	Base Station	Základní stanice
BTS	Base Transceiver Station	Základní vysílací stanice
CBS	Cell Broadcast Service	Služba pro hromadné vysílání zpráv na mobilní zařízení v dané oblasti
CE	Conformité Européenne	Evropská shoda, značka pro výrobky splňující evropské standardy
CEF	Connecting Europe Facility	Nástroj pro propojení Evropy
CEPT	European Conference of Postal and Telecommunications Administrations	Evropská konference poštovních a telekomunikačních správ
CO2	Carbon Dioxide	Oxid uhličitý
CORE	CORE	Komunikační platforma
CT	Computer Telephony	Počítačová telefonie
ČČK	Český červený kříž	
ČR	Česká republika	
ČTÚ	Český telekomunikační úřad	
D2D	Device-to-Device	Komunikace mezi zařízeními
DBK	Dansk Beredskabskommunikation	Dánsko – Dánská komunikace pro pohotovostní služby
dBm	Decibel-milliwatts	Decibel-miliwatty
DDoS	Distributed Denial of Service	Distribuované odepření služby
DMO	Direct Mode Operation	Režim přímého provozu

DMR	Digital Mobile Radio	Standard pro digitální mobilní komunikaci
DoS	Denial of Service	Odepření služby
DSMD	Disaster & Safety Management	Jižní Korea – Oddělení pro řízení katastrof a bezpečnost
DXT	Digital Exchange for TETRA	Digitální ústředna pro TETRA
DXTT	Digital Exchange for TETRA Transit Type	Tranzitní digitální ústředna pro TETRA
E2EE	End-to-End Encryption	Koncové šifrování
EADRCC	Euro-Atlantic Disaster Response Coordination Centre	Euroatlantické centrum pro koordinaci odezvy na katastrofy
EDR	Egységes Digitális Rádiórendszer	Maďarsko – Jednotný digitální rádiový systém
EK	Elektronická komunikace	
eMBMS	Evolved Multimedia Broadcast Multicast Service	Rozšířená služba pro vysílání a skupinové vysílání
EMM	Enterprise Mobility Management	Řízení podnikové mobility
eMPS	Enhanced Multimedia Priority Service	Rozšířená multimediální prioritní služba
ENISA	European Union Agency for Cybersecurity	Agentura Evropské unie pro kybernetickou bezpečnost
ETSI	European Telecommunications Standards Institute	Evropský institut pro telekomunikační standardy
EU	Evropská unie	
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	Vyspělá univerzální pozemní rádiová přístupová síť
GCF	Global Certification Forum	Globální certifikační fórum
GCSE	Group Communication System Enablers	Systém umožňující skupinovou komunikaci
GHz	Gigahertz	Jednotka frekvence
gNB	Next Generation NodeB	Stanice nové generace (v 5G sítích)
GNSS	Global Navigation Satellite System	Globální navigační satelitní systém
GPS	Global Positioning System	Globální polohový systém
HD	High Definition	Vysoké rozlišení
HDR	High Dynamic Range	Vysoký dynamický rozsah
HEVC	High Efficiency Video Coding	Vysoká účinnost kódování videa
HPUE	High Power User Equipment	Vysoce výkonné uživatelské vybavení
HW	Hardware	
HZS ČR	Hasičský záchranný sbor České republiky	Základní složka IZS
iDEN	Integrated Digital Enhanced Network	Integrovaná digitální vylepšená síť
IDS	Intrusion Detection System	Systém detekce vniknutí
IDSIS	Integrated Disaster and Safety Information System	Jižní Korea – Integrovaný systém informací o katastrofách a bezpečnosti
IMEI	International Mobile Equipment Identity	Mezinárodní identifikace mobilního zařízení
IOPS	Isolated Operations for Public Safety	Izolované operace pro veřejnou bezpečnost
IoT	Internet of Things	Internet věcí
IP	Internet Protocol	
IPS	Intrusion Prevention System	Systém prevence vniknutí
ISLP	Integrated Services Local Point	Mobilní přístup k datům
ITU	International Telecommunication Union	Mezinárodní telekomunikační unie
ITU-R 646 (REV.WRC 15)	ITU-R Recommendation 646 (REV.WRC 15)	Doporučení ITU-R 646 (revize Světové radiokomunikační konference 2015)
IZS	Integrovaný záchranný systém	
JRCC	Joint Rescue Coordination Centres	Norsko – Společná záchranná koordinační centra

JSVV	Jednotný systém varování a vyrozumění	
KHS	Krajská hygienická stanice	
KKB	Katasztrófavédelmi Koordinációs Kormánybizottság	Maďarsko – Vládní výbor pro koordinaci krizového řízení
KPI	Key Performance Indicator	Klíčový ukazatel výkonu
KPK	Krizový plán kraje	
KT	Korea Telecom	Jižní Korea – Korea Telecom
KTS	Key Telephone Systems	Klíčové telefonní systémy
KU	Krajský úřad	
KVS	Krajská veterinární správa	
KVV	Krajské vojenské velitelství	
LAN	Local Area Network	Lokální síť
LCS	Location Based Services	Lokalizační služby
LFFZ	Luftfunkzellen	Německo – Letecké rádiové buňky
LRT	LiveU Reliable Transport	Vlastní patentovaný protokol LiveU pro spolehlivý přenos dat
LTE	Long Term Evolution	Standard pro bezdrátovou komunikaci
LTE-M	Long Term Evolution for Machines	LTE pro stroje
LTE-R	Long Term Evolution for Railways	LTE pro železnice
Mbit/s	Megabit per second	Megabit za sekundu
MBP	Mobilní bezpečná platforma	
Mbps	Megabits per second	Megabity za sekundu
MBS	Multimedia Broadcast Multicast Service	Multimediální vysílání a skupinové vysílání
MC	Mission Critical	
MCC-ECO	Mission Critical Communication Ecosystem	Ekosystém kritické komunikace
MCD/MCData	Mission Critical Data	Kritická datová komunikace
MCON	Multi-Operator Core Network	Síťová infrastruktura sdílená více operátory v hybridním modelu
MCPTT	Mission Critical Push to Talk	Kritická komunikace stiskem tlačítka
MCS	Mission Critical Communication Systems	Systémy kritické komunikace
MCV/MCVideo	Mission Critical Video	Kritická video komunikace
MCX	Mission Critical Common Functionalities	Kritické společné funkce
MDT	Mobile Data Terminal	Mobilní datový terminál
MHz	Megahertz	Jednotka frekvence
Mm	Millimeters	Milimetry
MMR	Ministerstvo pro místní rozvoj	
MNO	Mobile Network Operator	Mobilní operátor
MOIS	Ministry of the Interior and Safety	Jižní Korea – Ministerstvo vnitra a bezpečnosti
Ms	Milliseconds	Milisekundy
MU	Mimořádná událost	
MV	Ministerstvo vnitra	
MVČR	Ministerstvo vnitra České republiky	
MVNO	Mobile Virtual Network Operator	Virtuální mobilní operátor
MŽP	Ministerstvo životního prostředí	

NATO	North Atlantic Treaty Organization	Severoatlantická aliance
NB-IoT	Narrowband Internet of Things	Úzkopásmový internet věcí
NEA	Notfall-Energieversorgungssysteme	Německo – Nouzové napájecí systémy
NFA	National Fire Agency	Jižní Korea – Národní hasičská agentura
NFC	Near Field Communication	Komunikace na krátkou vzdálenost
NFV	Network Functions Virtualization	Virtualizace síťových funkcí
NMHH	Nemzeti Média – és Hírközlési Hatóság	Maďarsko – Národní úřad pro média a komunikace
NTN	Non-Terrestrial Networks	Nepozemní sítě
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost	
NVKR	Nemzeti Veszélyhelyzet-kezelési Rendszer	Maďarsko – Národní systém řízení mimořádných událostí
OEM	Original Equipment Manufacturer	Výrobce originálního vybavení
OOP	Obecné oprávnění	Právní předpis vydávaný ČTÚ pro regulaci telekomunikací
OPIS	Operační a informační středisko	
ORP	Obec s rozšířenou působností	
OS	Operating System	Operační systém
OSN	Organizace spojených národů	
P25	Project 25	Standard pro digitální rádiovou komunikaci
PBX	Private Branch Exchange	Soukromá pobočková ústředna
PČR	Policie České republiky	
PEGAS	PEGAS	Komunikační systém v ČR
PIN	Personal Identification Number	Osobní identifikační číslo
PO	Požární ochrana	
PPDR	Public Protection and Disaster Relief	Ochrana veřejnosti a pomoc při katastrofách
ProSe	Proximity Services	Služby v blízkosti
PRS	Public Regulated Service	Veřejná regulovaná služba
PS-LTE	Public Safety Long Term Evolution	LTE pro veřejnou bezpečnost
PSTN	Public Switched Telephone Network	Veřejná komutovaná telefonní síť
PTT	Push-To-Talk	Komunikace stiskem tlačítka
PTZ	Pan-Tilt-Zoom	Funkce otáčení, naklánění a přibližování kamer
PWS	Public Warning System	Systém veřejného varování
PZH	Prevence závažných havárií	
QoS	Quality of Service	Kvalita služeb
RAKEL	Radiokommunikation för Effektiv Ledning	Švédsko – Radiokomunikační systém pro efektivní řízení
RAN	Radio Access Network	Radiový přístupový systém
RDP	Remote Desktop Protocol	Protokol vzdálené plochy
RF OTA	Radio Frequency Over-The-Air	Vysílání rádiové frekvence přes vzduch
RFP	Request for Proposal	Výzva k podání návrhu
RSPP	Radio Spectrum Policy Programme	Politika rádiového spektra
RSRP	Reference Signal Received Power	Příjem výkonu referenčního signálu
Ř SKIS MO	Ředitelství služeb informačních a komunikačních systémů Ministerstva obrany	

SA	Standalone	Samostatný režim nebo systém
SAR	Norwegian Search and Rescue Service	Norsko – Služba pro vyhledávání a záchranu
SCO	Systém centralizované ochrany	
SDN	Software Defined Network	Softwarově definovaná síť
SDS	Short Data Service	Krátká datová služba
SIEM	Security Information and Event Management	Správa bezpečnostních informací a událostí
SKT	SK Telecom	Jižní Korea – Bezdrátový telekomunikační operátor
SLA	Service Level Agreement	Smlouva o úrovni poskytovaných služeb
SMUR	Service Mobile d'Urgence et de Réanimation	Belgie – Mobilní jednotka pro urgentní lékařskou pomoc a resuscitaci
SOP	Standard Operating Procedure	Standardní operační postup
SSHR	Správa státních hmotných rezerv	Zajišťuje zásoby strategických materiálů
TCCA	TETRA and Critical Communications Association	Asociace pro TETRA a kritickou komunikaci
TDMA DMR	Time Division Multiple Access Digital Mobile Radio	Digitální mobilní rádio s časovým dělením
TEDS	TETRA Enhanced Data Service	Vylepšená datová služba v rámci sítě TETRA
TETRA	Terrestrial Trunked Radio	Standard pro digitální rádiovou komunikaci
TETRAPOL	TETRAPOL	Komunikační systém
THW	Technisches Hilfswerk	Německo – Federální agentura pro technickou pomoc při katastrofách a nouzových situacích
TMO	Trunked Mode Operation	Režim provozu s trunkováním
TMO-DMO Gateway	Trunked Mode Operation – Direct Mode Operation Gateway	Brána mezi trunkovaným a přímým režimem provozu
TVFZ	Terrestrische Versorgungszellen	Nemecko – Pozemní rádiové pokrytí
UAT	User Acceptance Testing	Akceptační testování uživatelů
UHD	Ultra High Definition	Ultra vysoké rozlišení
UHF	Ultra High Frequency	Velmi vysoká frekvence
UPS	Uninterruptible Power Supply	Nepřerušitelný zdroj energie
ÚR	Územní rozhodnutí	
USA	United States of America	Spojené státy americké
USB-C	Universal Serial Bus Type-C	Univerzální sériová sběrnice typu C, nový standard konektoru
VHCN	Very High Capacity Network	Síť s velmi vysokou kapacitou
VMS	Veřejná mobilní síť	
VoLTE	Voice over LTE	Hlas přes LTE
VPN	Virtual Private Network	Virtuální privátní síť
VPS	Veřejná pevná síť	
Wifi	Wireless Fidelity	Bezdrátová technologie
z.s.	Zapsaný spolek	Právní forma organizace
ZoEK	Zákon o elektronických komunikacích	
ZÚŘ	Zjednodušené územní řízení	
ZZS	Zdravotnická záchranná služba	

Zdroje

Informace nacházející se v tomto dokumentu byly čerpány z následujících zdrojů:

1 Definice PPDR/IZS

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

2 Definice v rámci České republiky

Zdroj	URL
Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů	https://www.zakonyprolidi.cz/cs/2000-240
Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů	https://www.zakonyprolidi.cz/cs/2000-239
Radiokomunikační síť integrovaného záchranného systému Pegas a její technické a kryptografické zabezpečení	https://digilib.k.utb.cz/handle/10563/38879
Příloha 2B k Vyhlášení výběrového řízení za účelem udělení práv k využívání rádiových kmitočtů pro zajištění sítí elektronických komunikací v kmitočtových pásmech 700 MHz a 3400–3600 MHz	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
Analýza a vize bezpečnosti radiové komunikace pro složky IZS	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
Vyhláška č. 328/2001 Sb.	https://www.zakonyprolidi.cz/cs/2001-328
BEZPEČNOSTNÍ STRATEGIE ČESKÉ REPUBLIKY 2023	https://mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf
Krizové stavy	https://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-krizove-stavy-krizove-stavy.aspx?q=Y2hudW09Mg%3D%3D
Krizové řízení v České republice	https://www.priruckazastupitele.cz/10-krizove-rizeni-v-ceske-republice/
Ambis – Krizový management	
Vnější havarijní plány a jejich vztah k ochraně obyvatelstva	http://www.hzsmsk.cz/sklad/kraoo/publikace/PO_VHP_vztah_k_OO.doc
Pojmy a definice krizového řízení	https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-ke-stazeni-ff.aspx?q=Y2hudW09NQ%3D%3D
Národní radiační havarijní plán	https://sujb.gov.cz/fileadmin/sujb/docs/dokumenty/NRHP/NRHP.pdf
Dokumentace IZS	https://www.hzscr.cz/clanek/dokumentace-izs-587832.aspx?q=Y2hudW09Ng%3D%3D
Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)	https://www.zakonyprolidi.cz/cs/2005-127#f7009936
Koncepce mobilizace ozbrojených sil České republiky	https://mocr.army.cz/images/id_40001_50000/46088/koncepce-mobilizace.pdf
Statistické ročenky Hasičského záchranného sboru ČR – Statistická ročenka 2023	https://www.hzscr.cz/clanek/statisticke-rocenky-hasicskeho-zachranneho-sboru-cr.aspx

3 Definice v zahraničí

Zdroj	URL
Behörden und Organisationen mit Sicherheitsaufgaben	https://abes-online.com/publikationen/fachbeitraege/behoerden-und-organisationen-mit-sicherheitsaufgaben/
Das Technische Hilfswerk	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 LORS D'UNE SITUATION D'URGENCE SUR LE TERRAIN	https://centredecrise.be/fr/que-font-les-autorites/gestion-de-crise/organisation-lors-dune-situation-durgence-sur-le-terrain
PUBLIC SAFETY FROM FINLAND	https://www.businessfinland.fi/4a845c/globalassets/ict-digi-maritime/bf_publicsafetyfromfinland_jointoffering_web.pdf
Pelastuslaki - 29.4.2011/379	https://www.finlex.fi/fi/laki/ajantasa/2011/20110379#P112
Pelastustoimi – luotettu turvallisuusviranomainen	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/institution/structures subordinated to /in coordination/ within the Ministry of Internal Affairs	https://www.mai.gov.ro/en/organisation/units-institution-or-structures-subordinated/
CENTRUL JUDEŢEAN DE CONDUCERE ŞI COORDONARE A INTERVENŢIEI – 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 systém 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_13.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 MOIS Disaster and Safety Management Department (DSMD)	

4 Legislativa a regulace pro Evropskou unii a Českou republiku

Zdroj	URL

Příloha 2B k Vyhlášení výběrového řízení za účelem udělení práv k využívání rádiových kmitočtů pro zajištění sítí elektronických komunikací v kmitočtových pásmech 700 MHz a 3400–3600 MHz	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 Krizové stavy a komunikace dle krizových stavů

Zdroj	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
Využití mobilních aplikací ve VS se zaměřením na policejní složky v ČR	https://dspace5.zcu.cz/bitstream/11025/53405/1/DP.pdf
Mobilní bezpečná platforma	https://katalog.polac.cz/Record/POLAC.119184/Description
VPN	https://www.eset.com/cz/vpn-pojem/
10 důvodů proč přejít na digitální DMR radiostanice a radiové sítě	https://www.hyt.cz/10-duvodu-proc-prejit-digitalni-dmr-radiostanice/
Jednotný systém varování a vyrozumění, koncové prvky	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
Srovnani Tetra Tetrapol – Ministerstvo vnitra České republiky	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
Prostředky rádiové komunikace pro internet věcí (IoT)	https://www.technickytydenik.cz/rubriky/archiv/prostredky-radiove-komunikace-pro-internet-veci-iot_42579.html

6 Technologické možnosti řešení

Zdroj	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 Možnost dalšího rozvoje technologií

Zdroj	URL
Study to determine the broadband frequency spectrum demand of the 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 Příklady řešení PPDR sítí v zahraničí

Zdroj	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 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 serve while being renewed 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 - 346/2010. (XII. 28.) Government decree about 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
Pelastuslaki (379/2011)	https://www.finlex.fi/fi/laki/ajantasa/2011/20110379
Julkisista hankinnoista ja käyttöoikeussopimuksista annettu laki (1397/2016)	https://www.finlex.fi/fi/laki/ajantasa/2016/20161397
§ 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)
Laki julkisen hallinnon turvallisuusverkkotoiminnasta	https://finlex.fi/fi/laki/alkup/2015/20150010
ATRID – Belgium	https://www.astrid.be
Loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité	https://etaamb.openjustice.be/fr/loi-du-08-juin-1998_n1998000389.html
BDBOS	https://www.bdbos.bund.de/DE/Home/home_node.html
FAQ Digitalfunk BOS	https://www.bdbos.bund.de/SharedDocs/Downloads/DE/Publikationen/faq-broschuere.html
Jižní 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)
Jižní Korea – Regulations on the operation and use of disaster safety communication networks	https://law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000189691
Jižní 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 organizations belonging to the scope of frequency management for non-civilian purposes	https://net.jogtar.hu/jogszabaly?docid=a1100012.nmh
Hungary - 7/2012. (I. 26.) NMHH decree on certain official procedures of civil frequency management	https://net.jogtar.hu/jogszabaly?docid=a1200007.nmh
Hungary - 346/2010. (XII. 28.) Government decree about networks for government purposes	https://net.jogtar.hu/jogszabaly?docid=a1000346.kor

9 Bezpečnostní hrozby

Zdroj	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
ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 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
Akční plán boje proti terorismu 2022	https://www.czdefence.cz/clanek/akcni-plan-boje-proti-terorismu-2022
AMBIS – KRIZOVÝ MANAGEMENT	
Výroční zpráva Vojenského zpravodajství za rok 2023	https://vzcr.cz/uploads/41-Vyrocni-zprava-2023.pdf

10 Aplikační možnosti

Zdroj	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

Manažerské shrnutí

Tato rešerše se zabývá aspekty bezpečné a spolehlivé komunikace pro složky Integrovaného záchranného systému (IZS) v zemích Evropské unie, přičemž klade důraz na využití moderních technologií, jako jsou 5G sítě a systémy PPDR (Public Protection and Disaster Relief). Bezpečnostní krizová komunikace je klíčovým prvkem pro efektivní reakci státu na mimořádné události a krizové situace. Zajišťuje plynulou a spolehlivou výměnu informací mezi složkami záchranných a bezpečnostních služeb, jako jsou Policie ČR, Hasičský záchranný sbor a Zdravotnická záchranná služba.

Vzhledem k rostoucím výzvám, jako jsou častější přírodní katastrofy, teroristické hrozby a technologické havárie, je nezbytné, aby komunikační systémy byly nejen bezpečné a odolné, ale také flexibilní a schopné rychle reagovat na nové hrozby a potřeby. Rešerše se proto zaměřuje na analýzu současného stavu technologií, konkrétní zahraniční implementace a identifikaci technologií a přístupů, které by mohly být efektivně využity v České republice.

Příklady implementace komunikačních systémů ve Finsku a Německu ukazují, jak moderní technologie zvyšují bezpečnost a spolehlivost krizové komunikace. Tyto poznatky mohou inspirovat a vést k zavedení obdobných systémů v českém kontextu.

Cílem je zhodnotit možnosti integrace těchto technologií do stávajících struktur IZS v ČR, přičemž při zhodnocení je kladen důraz na interoperabilitu, bezpečnost a celkovou efektivitu systémů. Tento dokument poskytuje přehled o možnostech modernizace krizové komunikace v České republice, s ohledem na globální trendy a nové bezpečnostní výzvy.

Závěr ke kapitole 1:

- PPDR představuje soubor činností zaměřených na ochranu veřejnosti a zvládání krizových situací. V České republice se tyto aktivity uskutečňují prostřednictvím IZS, který zajišťuje koordinaci záchranných a bezpečnostních složek, jako jsou Policie ČR, Hasičský záchranný sbor a Zdravotnická záchranná služba.
- V rámci legislativy se v České republice používá pojem IZS, zatímco pojem PPDR není v českém právním řádu explicitně definován. PPDR se v mezinárodním kontextu více soustředí na technologické a komunikační aspekty ochrany veřejnosti, zatímco IZS v České republice představuje komplexní systém koordinace záchranných a bezpečnostních složek.
- Pro zajištění spolehlivé a bezpečné komunikace mezi složkami IZS je nezbytné využití specifických frekvenčních pásem, včetně implementace moderních technologií, jako je 5G. Tyto technologie poskytují vyšší kapacitu a rychlost přenosu dat, což je klíčové pro efektivní řízení krizových situací a zajištění bezpečnosti obyvatelstva.

Závěr ke kapitole 2:

- Vzhledem k rostoucím bezpečnostním hrozbám a technologickým výzvám je modernizace PPDR systémů a komunikační infrastruktury potřebná. Přechod na širokopásmové a 5G technologie přinese vyšší rychlost, kapacitu a spolehlivost komunikace a zlepší se schopnost IZS reagovat na krizové situace a zajišťovat bezpečnost obyvatelstva.
- IZS v České republice se zaměřuje na ochranu veřejnosti a řešení krizových situací, čímž umožňují koordinovanou reakci na hrozby, jako jsou terorismus, kybernetické útoky, přírodní katastrofy a pandemie. Tento systém zahrnuje spolupráci klíčových složek, jako je Hasičský záchranný sbor, Policie ČR a Zdravotnická záchranná služba.
- Vzhledem k rostoucím bezpečnostním hrozbám a technologickým výzvám je modernizace komunikační infrastruktury pro IZS nezbytná. Přechod na širokopásmové a 5G technologie přinese vyšší rychlost, kapacitu a spolehlivost komunikace, což zlepší schopnost složek IZS efektivně reagovat na krizové situace a zajišťovat bezpečnost obyvatelstva.

Závěr ke kapitole 3:

- Organizace složek IZS se v jednotlivých zemích značně liší v závislosti na jejich legislativních, geografických a organizačních podmínkách. Základní principy – ochrana veřejnosti a zvládání krizových situací – zůstávají podobné, avšak jednotlivé země přizpůsobují své systémy specifickým potřebám a dostupným zdrojům.
- V porovnání se zahraničními systémy, jako je IZS v Německu nebo Finsku, je český IZS více centralizovaný a klade důraz na jednotnou koordinaci napříč celou zemí. I přes regionalizaci v zahraničí, kde je větší autonomie na regionální úrovni, je v České republice klíčová centralizace a jednotné řízení na národní úrovni.

- Různé země mají odlišné přístupy k implementaci pro 5G a PPDR, přičemž některé státy, například Německo a Francie, kladou důraz na pokročilé šifrovací standardy a bezpečnostní opatření, zatímco jiné se zaměřují na zajištění interoperability mezi systémy.

Závěr ke kapitole 4:

- Aukce kmitočtů v pásmu 700 MHz, vyhlášená ČTÚ, byla krokem pro rozvoj 5G sítí a zajištění prioritních služeb pro veřejnou bezpečnost a krizovou komunikaci v ČR a také stanovila podmínky pro národní roaming a poskytování prioritních širokopásmových služeb PPDR.
- Aukce kmitočtů v pásmu 700 MHz, vyhlášená ČTÚ, představuje významný krok směrem k rozvoji 5G sítí v České republice. Tento krok nejen podporuje rozvoj moderních telekomunikačních technologií, ale také zajišťuje prioritní služby pro veřejnou bezpečnost a krizovou komunikaci. Součástí této aukce bylo stanovení podmínek pro národní roaming a poskytování prioritních širokopásmových služeb pro složky IZS.
- Tento právní rámec a jeho technické normy jsou podstatným faktorem pro zajištění bezpečné a spolehlivé komunikace mezi složkami IZS. Díky těmto legislativním opatřením, která stanovují pravidla pro provoz a údržbu komunikačních systémů, je možné zajistit interoperabilitu a efektivní spolupráci mezi různými složkami záchranných a bezpečnostních služeb. Legislativa také podporuje implementaci moderních technologií, jako je 5G.

Závěr ke kapitole 5:

- Komunikaci složek IZS zajišťují různé typy komunikačních prostředků, jako jsou pevné sítě, mobilní sítě, TETRAPOL IP, DMR a další technologie. Každý z těchto prostředků má specifické vlastnosti a omezení, které ovlivňují jejich použití v krizových situacích.
- Sítě jako TETRAPOL a TETRA nabízejí bezpečnou a spolehlivou komunikaci díky své uzavřené infrastruktuře a hardwarovému šifrování, což zajišťuje ochranu citlivých informací a umožňuje efektivní koordinaci při krizových událostech. Veřejné sítě a satelitní komunikace poskytují širší pokrytí a flexibilitu, avšak přinášejí větší rizika v oblasti kvality služby a bezpečnosti, zejména během krizových situací s vysokým provozem. Celkově je pro efektivní krizovou komunikaci nutno kombinovat různé typy komunikačních systémů, které se vzájemně doplňují a zajišťují robustní a spolehlivé spojení v různých scénářích a podmínkách.
- Různé krizové stavy, jako jsou přírodní katastrofy, teroristické útoky nebo technologické havárie, vyžadují specifické komunikační strategie. Při přírodních katastrofách je podstatné rychle informovat veřejnost o evakuačních plánech a bezpečnostních opatřeních, zatímco v případě teroristických hrozeb je prioritou zajištění bezpečné a šifrované komunikace mezi složkami IZS.

Závěr ke kapitole 6:

- Z analýzy vyplývá, že modernizace komunikační platformy pro PPDR je nezbytná. Navržené postupy, včetně implementace širokopásmové PPDR sítě, kombinace stávajících sítí s komerčními sítěmi a rozvoj vlastní infrastruktury ve spolupráci s armádou, představují krok k zajištění robustnější a flexibilnější krizové komunikace. Využití moderních technologií jako 5G, digitálních rádiových sítí a pokročilých šifrovacích standardů nabízí možnost zvýšení kapacity, bezpečnosti a spolehlivosti komunikace.
- Budoucí technologické inovace, jako umělá inteligence, internet věcí nebo rozšířená realita, mohou dále zlepšit schopnosti složek IZS reagovat na krizové situace. Například AI může analyzovat velké objemy dat pro predikci krizových situací, zatímco AR může záchranářům pomoci efektivněji se orientovat v terénu pomocí vizualizace důležitých informací.
- Síť propojující více technologií, která zahrnuje jak vládní, tak komerční infrastrukturu, představuje optimální řešení pro zajištění spolehlivé a efektivní krizové komunikace. Tento přístup zajišťuje, že komunikace zůstane funkční i při výpadcích nebo zvýšené poptávce po kapacitě. Zároveň umožňuje integraci pokročilých funkcí, jako je přesné určování polohy nebo přenos videa v reálném čase.

Závěr ke kapitole 7:

- Rozvoj širokopásmových sítí, jako jsou LTE a 5G, přináší nové možnosti pro rychlou a spolehlivou krizovou komunikaci, včetně integrace pokročilých aplikací a datových služeb. Přechod na 5G technologie umožňuje nasazení inovativních aplikací.
- V oblasti zabezpečení se nabízí i technologie blockchain, která může zajistit transparentnost a integritu dat během krizových situací, čímž přispívá k ochraně citlivých informací.
- Zavedení těchto inovativních technologií může výrazně zlepšit schopnosti složek IZS reagovat na krizové situace a zvyšuje jejich připravenost a efektivita při ochraně obyvatelstva.

Závěr ke kapitole 8:

- Přehled implementace PPDR sítí v různých zemích ukazuje, že přístupy k těmto technologiím se výrazně liší v závislosti na místních legislativních rámcích, technologických možnostech a operačních potřebách záchranných složek. Příklady z Německa, Francie, Velké Británie a Švédska poskytují cenné poznatky o tom, jak různé země přizpůsobily své komunikační systémy specifickým národním podmínkám.
- Například v Německu byla implementována širokopásmová síť BDBOS, která zajišťuje digitální rádiovou komunikaci pro všechny složky IZS s vysokou úrovní šifrování a bezpečnosti. Ve Francii zavedli širokopásmovou PPDR síť založenou na technologii LTE, která umožňuje přenos hlasu a dat v reálném čase. Velká Británie implementovala síť ESN, využívající technologie 4G a 5G, která je interoperabilní s dalšími systémy a umožňuje širokou škálu pokročilých funkcí, jako je sledování polohy a videokonference. Švédsko využívá síť TETRA, která nabízí vysokou úroveň bezpečnosti a odolnost proti rušení.
- Tyto příklady zdůrazňují, že úspěšná implementace PPDR sítí závisí na přizpůsobení místním podmínkám, ale zároveň umožňuje inspiraci pro budoucí rozvoj krizové komunikace v České republice.

Závěr ke kapitole 9:

- Kybernetické hrozby a teroristické útoky představují významná rizika pro komunikační prostředky složek IZS. S narůstající složitostí a propojeností systémů, zejména při přechodu na 5G technologie, tyto hrozby nabývají na četnosti i sofistikovanosti. Kybernetické útoky, jako je ransomware, phishing nebo DDoS, mohou vážně narušit dostupnost a bezpečnost krizové komunikace, zatímco teroristické útoky mohou cílit na fyzickou infrastrukturu, což vede k rozsáhlým výpadkům.
- Pro minimalizaci těchto hrozeb je klíčové zavedení komplexních bezpečnostních opatření. To zahrnuje zabezpečení síťové infrastruktury prostřednictvím pokročilých šifrovacích standardů, pravidelného monitoringu hrozeb a ochrany kritických systémů. Fyzická ochrana infrastruktury, včetně zabezpečení základnových stanic a datových center, je stejně důležitá jako prevence technických poruch pravidelnou údržbou a modernizací.
- Plánování krizových situací a příprava na přírodní katastrofy zajišťuje, že komunikace zůstane funkční i v těch nejnáročnějších podmínkách. Zároveň je potřebné průběžné školení personálu a osvěta v oblasti kybernetické bezpečnosti, aby se minimalizovaly lidské chyby a zvýšila celková připravenost složek IZS na potenciální bezpečnostní hrozby.

Závěr ke kapitole 10:

- Aplikační možnosti komunikačních systémů jsou prvkem pro efektivní fungování složek IZS. Rozdíl mezi komerčními a kritickými systémy je zásadní – zatímco komerční systémy se zaměřují na široké spektrum uživatelů a prioritizují ziskovost, kritické systémy určené pro PPDR kladou důraz na spolehlivost, bezpečnost a odolnost. Komunikační systémy pro složky IZS, jako jsou MC systémy, vyžadují speciální infrastrukturu podporující nepřetržitou dostupnost a bezpečnost dat.
- Současné technologické možnosti zahrnují digitální rádiové sítě, mobilní komunikační systémy a pokročilé šifrovací technologie. Budoucí inovace, jako je umělá inteligence, internet věcí a rozšířená realita, mají potenciál dále zlepšit efektivitu a reakční schopnosti složek IZS v krizových situacích.
- Pro zajištění bezpečné a efektivní komunikace je zásadní nejen integrace těchto technologií, ale i jejich propojení do robustního a flexibilního systému, který dokáže splnit specifické požadavky kritických operací. Implementace takových technologií bude hrát zásadní roli v budoucnosti krizové komunikace.

Na základě zahraničních zkušeností lze pro komunikační sítě složek IZS v ČR stanovit následující cíle:

- **Rozvoj vlastních komunikačních sítí:** Modernizace komunikačních technologií prostřednictvím implementace 5G a PPDR technologií zajistí rychlou a spolehlivou komunikaci, včetně záložních řešení pomocí bezpečné neveřejné komunikační sítě.
- **Interoperabilita:** Je nutné zajistit kompatibilitu s mezinárodními systémy a standardy pro efektivní spolupráci v krizových situacích na globální úrovni.
- **Bezpečnost a šifrování:** Zavedení pokročilých šifrovacích standardů a dalších bezpečnostních opatření je nezbytné pro ochranu citlivých dat a zajištění bezpečnosti komunikačních systémů.
- **Výzkum a vývoj:** Zvýšení investic do výzkumu a vývoje v oblasti bezpečné komunikace je klíčové pro podporu inovací a dlouhodobého zlepšování komunikační infrastruktury složek IZS.

Tato opatření by měla zvýšit efektivitu, bezpečnost a připravenost složek IZS na krizové situace v České republice.

Management summary

This research focuses on the aspects of secure and reliable communication for the Integrated Rescue System units in European Union countries, emphasizing 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 analyzing the current state of technology, specific foreign implementations, and identifying technologies and approaches that could be effectively utilized in the Czech Republic.

Examples of communication system implementations in Finland and Germany show 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 goal 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 modernizing crisis communication in the Czech Republic, considering 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, while 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 modernization 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 includes cooperation among 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 modernization 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 organization of IZS units varies significantly across countries, depending on their legislative, geographical, and organizational 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 centralized and emphasizes unified coordination across the entire country. Despite regionalization abroad, where there is greater

autonomy at the regional level, centralization 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, while others prioritize 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 ČTÚ represents a significant move 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 included setting conditions for national roaming and the provision of priority broadband services for 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:

- The communication of IZS units is ensured 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 like 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, while in the case of terrorist threats, the priority is to ensure secure and encrypted communication between IZS units.

Conclusion to Chapter 6:

- The analysis shows that modernizing 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 analyze large volumes of data to predict crisis scenarios, while AR can help rescuers navigate the terrain more effectively by visualizing 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 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, introduces 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 IZS 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 IZS 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, utilizing 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 successful implementation of PPDR networks depends on adapting to local conditions, while also providing inspiration for the future development of crisis communication in the Czech Republic.

Conclusion to Chapter 9:

- Cyber threats and terrorist attacks represent 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, while terrorist attacks can target physical infrastructure, leading to widespread outages.
- To minimize 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 centers, is just as important as preventing technical malfunctions through regular maintenance and modernization.
- 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 minimize 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—while commercial systems target a broad spectrum of users and prioritize profitability, critical systems intended for PPDR emphasize reliability, security, and resilience. Communication systems for IZS units, such as MC systems, require specialized 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 connection into a robust and flexible system that can meet 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 experiences, the following goals can be set for the communication networks of IZS units in the Czech Republic:

– **Development of independent communication networks:** Modernizing 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 innovations 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.

Úvod

Bezpečnostní krizová komunikace, označovaná jako PPDR, představuje nástroj v reakčních schopnostech státu na různé mimořádné události, včetně přírodních katastrof, teroristických útoků a technologických havárií. Zajištění spolehlivé a odolné komunikace mezi různými složkami záchranných a bezpečnostních orgánů, jako jsou policie, hasiči, zdravotnické služby a další, je nutná pro efektivní zvládání těchto krizových situací. V dnešní době se rostoucí počet a komplexita těchto událostí stávají výzvou, kterou je třeba řešit prostřednictvím moderních technologických řešení.

Tato studie se zaměřuje na analýzu současných technologií používaných v oblasti bezpečnostní krizové komunikace v rámci Evropské unie, se zvláštním důrazem na využití 5G sítí. Technologie 5G nabízí významné výhody v oblasti rychlosti, kapacity a bezpečnosti přenosu dat, což jsou faktory pro úspěšnou implementaci systémů PPDR. Kombinace 5G sítí s již existujícími systémy pro krizovou komunikaci může významně zvýšit schopnost efektivně reagovat na mimořádné události a zajistit vysokou úroveň ochrany veřejnosti.

V rámci této studie jsou zkoumány různé přístupy a technologická řešení implementovaná v zahraničních systémech krizové komunikace, jako jsou například systémy ve Finsku, Německu, Koreji a dalších zemích. Analýza zahraničních use-case poskytuje osvědčené postupy, které mohou být aplikovány i v kontextu České republiky. Studie se zaměřuje na identifikaci faktorů, které přispívají k účinnosti a odolnosti těchto systémů, a zároveň se snaží identifikovat potenciální rizika a výzvy, které mohou nastat při jejich implementaci v lokálním prostředí.

1 Definice PPDR/IZS

1.1 Definice PPDR

Public Protection and Disaster Relief (PPDR) je zkratka označující aktivity a služby zaměřené na ochranu veřejnosti a zvládání mimořádných událostí. V překladu PPDR znamená "Ochrana veřejnosti a pomoc při katastrofách". Tento pojem zahrnuje široké spektrum činností, které mají za cíl zajištění bezpečnosti obyvatel a efektivní reakci na krizové situace, jako jsou přírodní katastrofy, technologické havárie a teroristické útoky.

V České republice není tato zkratka legislativně definována. Český právní rámec neobsahuje přímou definici PPDR, ale související aktivity jsou upraveny v několika zákonech, například v zákoně č. 239/2000 Sb. o integrovaném záchranném systému a zákoně č. 240/2000 Sb. o krizovém řízení.

Termín PPDR jako takový je definován v evropských dokumentech a standardech, které poskytují rámec pro harmonizaci a interoperabilitu systémů krizové komunikace mezi členskými státy EU[1].

Evropská unie má strategii pro komunikaci PPDR[2] zaměřenou na modernizaci a harmonizaci frekvenčního spektra a technologií napříč členskými státy. Klíčovým cílem je přechod na širokopásmové sítě, které umožní lepší sdílení informací a zvýšení efektivity zásahů při krizových situacích. Strategie zahrnuje využití 700 MHz pásma pro širokopásmové služby PPDR, což má zajistit dostatečnou kapacitu pro přenos dat, včetně videa a hlasových služeb.

Implementace 5G technologií do komunikace složek PPDR je dalším krokem v této strategii[3], neboť 5G nabízí vyšší přenosové rychlosti, nižší latenci a vyšší spolehlivost, což je klíčové pro krizovou komunikaci. Tyto strategie jsou např. v ČR zhmotněné v Aukci kmitočtů pro sítě 5G.

1.2 Definice IZS

V České republice je PPDR realizováno prostřednictvím IZS. Tento systém je komplexní a zahrnuje koordinaci základních i rozšířených složek, které spolupracují při zvládání mimořádných událostí. Základní složky IZS zahrnují Hasičský záchranný sbor ČR, Policii ČR, Zdravotnickou záchrannou službu a Jednotky požární ochrany. Rozšířené složky pak zahrnují ozbrojené síly, ostatní ozbrojené bezpečnostní sbory, orgány ochrany veřejného zdraví, havarijní pohotovostní služby, zařízení civilní ochrany a neziskové organizace.

Většina evropských zemí má své vlastní verze integrovaných záchranných systémů, které zahrnují koordinaci různých složek záchranných služeb, ozbrojených sil a dalších specializovaných jednotek. Tyto systémy se mohou lišit v názvu, organizaci a rozsahu, ale všechny sdílejí podobné cíle a funkce.

1.3 Prostředky pro realizaci služeb PPDR

1.3.1 Frekvenční spektrum

Frekvenční spektrum je klíčovým prvkem pro zajištění služeb PPDR, protože umožňuje přenos signálů mezi různými složkami záchranného systému. V České republice jsou pro složky IZS vyhrazena specifická frekvenční pásma. Tato pásma zajišťují spolehlivou a bezpečnou komunikaci mezi složkami IZS během krizových situací. Harmonizace těchto pásem na evropské úrovni

[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

umožňuje efektivní přeshraniční spolupráci a interoperabilitu, což je nezbytné pro zvládání přeshraničních krizových situací. Vyhrazená frekvenční pásma pro IZS jsou tak důležitá pro zajištění efektivní krizové reakce a koordinace mezi záchrannými složkami.

1.3.2 Použití frekvenčních pásem – vlastní a sdílená

Použití frekvenčních pásem pro složky IZS zahrnuje, jak vlastní, tak sdílená pásma, což umožňuje efektivní a flexibilní krizovou komunikaci. Vlastní frekvenční pásma, jako například pásmo 380-385 MHz pro síť PEGAS/TETRAPOL IP, jsou vyhrazena specificky pro potřeby IZS a poskytují vysokou úroveň spolehlivosti a bezpečnosti díky absenci komerčního provozu. Sdílená frekvenční pásma, například 700 MHz a 3400-3600 MHz, využívaná také pro komerční mobilní služby, nabízejí dodatečnou kapacitu a flexibilitu. Sdílená pásma mohou být dynamicky přidělována podle aktuální potřeby a využívají technologii QoS pro zajištění prioritního přístupu ke službám PPDR v krizových situacích, čímž umožňují efektivní komunikaci mezi záchrannými složkami. Tento kombinovaný přístup zajišťuje, že záchranné složky mají vždy dostupné spolehlivé komunikační prostředky pro efektivní zvládání mimořádných událostí.

1.3.3 Typy sítí využívané složkami IZS/PPDR– veřejné a neveřejné sítě

Pro zajištění služeb PPDR se využívají veřejné a neveřejné sítě.
Veřejné sítě jsou provozovány komerčními operátory, nabízejí široké pokrytí a vysokou kapacitu díky moderním technologiím jako 2G, LTE a 5G, avšak mohou mít problémy s prioritizací a bezpečností během krizových situací díky povinnosti zajistit veřejně dostupnou službu elektronických komunikací.
Neveřejné sítě jsou specificky vyhrazené pro interní potřeby státní správy a samosprávy, potřeby záchranných a bezpečnostních složek. Tyto sítě poskytují dle konfigurace i vyšší spolehlivost, bezpečnost a možnost prioritizace provozu. Na tyto sítě se mnohdy uplatňují i povinnosti kritické infrastruktury.

2 Definice v rámci České republiky

PPDR v České republice se zaměřuje na ochranu veřejnosti a zvládání mimořádných událostí a krizových situací prostřednictvím koordinovaných činností složek Integrovaného záchranného systému (IZS). Tento systém je nosný pro efektivní reakci na různé typy krizí.

Bezpečnostní strategie České republiky identifikuje řadu bezpečnostních hrozeb a zdrojů nestability, které mají přímý dopad na potřebu efektivních systémů veřejné ochrany a reakce na katastrofy. Mezi hlavní hrozby patří terorismus, kybernetické útoky, hybridní hrozby, přírodní katastrofy, technologické havárie a pandemie. Tyto hrozby vyžadují robustní a interoperabilní komunikační infrastrukturu, která umožní rychlou a koordinovanou reakci složek IZS.

Vzhledem k těmto hrozbám je klíčové, aby PPDR systémy byly modernizovány a integrované, čímž se zvýší schopnost České republiky efektivně řešit krizové situace. Například kybernetické útoky a hybridní hrozby vyžadují pokročilou ochranu komunikačních sítí, zatímco přírodní katastrofy a technologické havárie kladou důraz na rychlou a spolehlivou komunikaci mezi záchrannými složkami.

Změny v bezpečnostním prostředí kladou nové nároky na komunikační infrastrukturu. Česká republika se připravuje na ukončení podpory systému TETRAPOL, protože pro ČR je podpora TETRAPOL zaplacena do roku 2035. Modernizace PPDR systémů zahrnuje přechod na širokopásmové komunikační technologie, které nabídnou vyšší kapacitu, rychlost a spolehlivost komunikace.

Investice do modernizace PPDR systémů proto reflektují potřebu adaptace na měnící se bezpečnostní prostředí. Moderní a interoperabilní komunikační infrastruktura umožní lepší koordinaci záchranných složek, rychlejší reakci na krizové situace a zvýšení celkové bezpečnosti obyvatelstva.

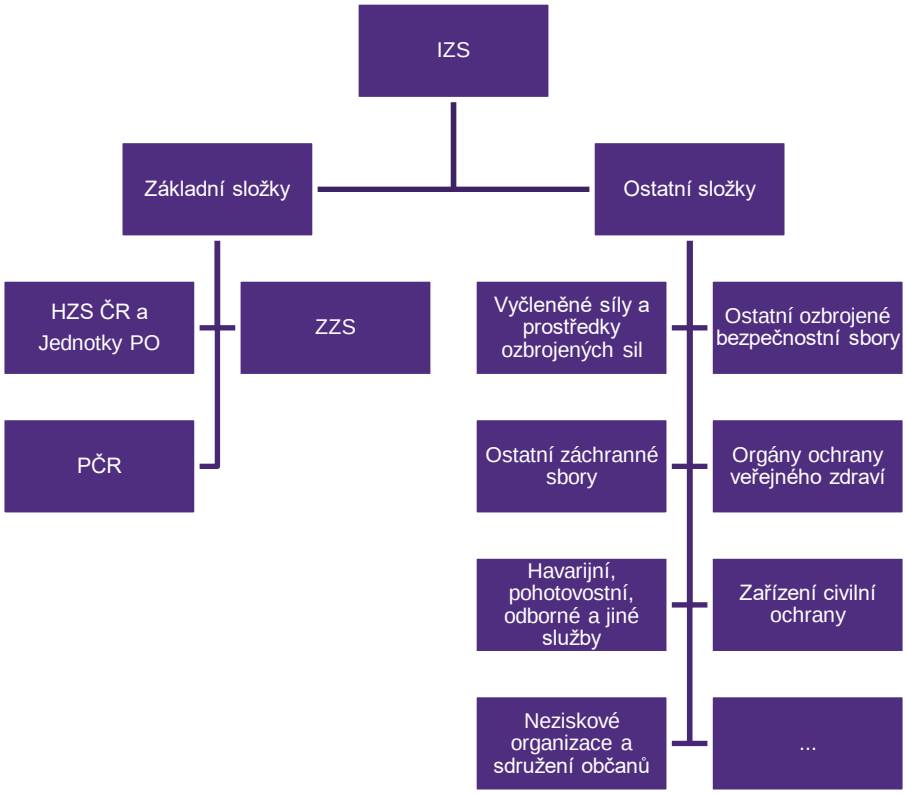
2.1 Složky Integrovaného záchranného systému (IZS)

Integrovaný záchranný systém České republiky je komplexní struktura zahrnující více složek, které společně pracují na zajištění ochrany veřejnosti a efektivnímu zvládání mimořádných událostí. Systém IZS je navržen tak, aby umožňoval rychlou a koordinovanou reakci na různé typy krizových situací, včetně přírodních katastrof, technických havárií, teroristických útoků a dalších mimořádných událostí, které mohou ohrozit životy, zdraví nebo majetek občanů.

Jednou z hlavních výhod IZS je schopnost propojit různé organizace a instituce do jednoho funkčního celku, který může efektivně reagovat na krizové situace. Tento systém zahrnuje jak základní složky, které jsou klíčové pro každodenní záchranné operace, tak i další specializované složky, které se zapojují při rozsáhlejších nebo specifických krizích.

Podle zákona č. 239/2000 Sb., o integrovaném záchranném systému, se složky IZS dělí na základní a ostatní. Základní složky IZS zajišťují nepřetržitou pohotovost pro ohlášení vzniku mimořádné události, její vyhodnocení a neodkladný zásah v místě mimořádné události. Vzájemnou komunikací se rozumí koordinovaný postup těchto složek při přípravě na mimořádné události a při provádění záchranných a likvidačních prací. Složky IZS současně zajišťují i klíčové úkoly podle krizového zákona.

Podrobnosti o organizaci a činnosti integrovaného záchranného systému dále specifikuje vyhláška č. 328/2001 Sb., o některých podrobnostech zabezpečení integrovaného záchranného systému. Tato vyhláška stanovuje konkrétní pravidla a postupy, které musí složky IZS dodržovat.



Struktura IZS

2.1.1 Základní složky IZS

Mezi základní složky IZS patří:

Hasičský záchranný sbor České republiky (HZS ČR) včetně jednotek požární ochrany – zařazené do plošného pokrytí kraje jednotkami požární ochrany

Policie České republiky (PČR)

Poskytovatelé zdravotnické záchranné služby

2.1.1.1 Hasičský záchranný sbor České republiky (HZS ČR)

Hasičský záchranný sbor České republiky je základní složkou IZS a koordinátorem záchranných prací a ochrany obyvatelstva. HZS ČR je zodpovědný za zásahy při požárech, chemických a radiologických haváriích, dopravních nehodách a dalších mimořádných událostech. Kromě toho provádí preventivní činnosti a školení zaměřená na zvýšení bezpečnosti obyvatelstva.

HZS ČR je jednotný bezpečnostní sbor, jehož základním úkolem je chránit životy, zdraví, životní prostředí, zvířata a majetek před požáry a jinými mimořádnými událostmi. Podílí se na zajišťování bezpečnosti České republiky plněním úkolů požární ochrany, ochrany obyvatelstva, civilního nouzového plánování, krizového řízení a dalších úkolů podle právních předpisů. Tyto činnosti jsou vymezeny zejména zákonem č. 320/2015 Sb. o hasičském záchranném sboru, zákonem č. 133/1985 Sb. o požární ochraně a zákonem č. 239/2000 Sb. o integrovaném záchranném systému. HZS ČR spadá do působnosti Ministerstva vnitra.

Historie HZS ČR sahá až k systému civilní obrany, konkrétně k 75. záchranné a výcvikové základně Olomouc Armády ČR, která vznikla v roce 1991. V průběhu roku 2000 zde vznikl odloučený záchranný prapor dislokovaný v posádce Hlučín. Tento prapor se v roce 2004 stal základem nově vznikajícího 157. záchranného praporu. Usnesením Vlády ČR ze dne 22. října 2007 a schválením transformace resortu Ministerstva obrany ČR byl 157. záchranný prapor předán HZS ČR a 1. ledna 2009 vznikl Záchranný útvar HZS ČR.

Velitelství Záchranného útvaru HZS ČR se nachází v Hlučíně, přičemž útvar má dvě záchranné roty – jednu v Jihlavě a druhou ve Zbirohu. Záchranné roty jsou vybaveny pro širokou škálu záchranných operací, od odstraňování následků přírodních katastrof až po pomoc při průmyslových haváriích.

V některých dokumentech se HZS nazývá „Jednotkou požární ochrany“ (JPO) tou se rozumí organizovaný soubor odborně vyškolených osob, hasičské techniky a věcných pro odborně vyškolených osob, hasičské techniky a věcných prostředků PO. Vzhledem k tomu, že nelze vyloučit vznik požáru či jiné mimořádné události kdekoli na území ČR, je vytvořen systém JPO, který plošně v celé ČR zabezpečuje účinnou pomoc do určitého časového limitu s určitým množstvím sil a prostředků (hasičů, hasičské techniky a dalších prostředků PO). V současné době zajišťuje tuto pomoc 247 jednotek HZS ČR, 93 jednotek HZS podniků, 6 063 JSDH obcí a 89 JSDH podniků. JPO jsou z důvodu rychlého vývoje nových technologií, rozvoje průmyslu a v důsledku urbanistických změn vystaveny novým výzvám, na které je nutné reagovat. V této souvislosti je dlouhodobou prioritou HZS ČR obměna stávající techniky zajišťující výjezd JPO.

V roce 2023 bylo v České republice evidováno 7 826 hasičů v Hasičském záchranném sboru ČR, 3 148 hasičů v Hasičském záchranném sboru podniků a 1 150 hasičů v jednotkách sboru dobrovolných hasičů podniků, 79 468 hasičů v jednotkách sboru dobrovolných hasičů obcí.

Pod HZS ČR spadají následující složky:

- Generální ředitel
- MV-generální ředitelství HZS České republiky
- HZS hlavního města Prahy
- HZS Středočeského kraje
- HZS Jihočeského kraje
- HZS Plzeňského kraje
- HZS Karlovarského kraje
- HZS Ústeckého kraje
- HZS Libereckého kraje
- HZS Královéhradeckého kraje
- HZS Pardubického kraje
- HZS Kraje Vysočina
- HZS Jihomoravského kraje
- HZS Olomouckého kraje
- HZS Moravskoslezského kraje
- HZS Zlínského kraje
- Záchranný útvar HZS ČR
- SOŠ PO a VOŠ PO
- Technický ústav požární ochrany
- Školy požární ochrany ve Frýdku Místku
- Školní a výcvikové zařízení HZS ČR
- Institut ochrany obyvatelstva
- Servisní a opravárenské zařízení HZS ČR
- Český národní výbor CTIF
- Nadace policistů a hasičů
- Expozice požární ochrany ve Zbirohu
- Hasičský útvar ochrany Pražského hradu

2.1.1.2 Jednotky požární ochrany zařazené do plošného pokrytí kraje jednotkami požární ochrany

Jednotky požární ochrany zahrnují profesionální i dobrovolné hasičské jednotky. Profesionální jednotky jsou součástí Hasičského záchranného sboru České republiky a působí na celostátní úrovni, zatímco dobrovolné hasičské sbory, organizované na místní úrovni, poskytují podporu při zásazích a často fungují jako první reakce na menší požáry a jiné události.

Systém jednotek požární ochrany je navržen tak, aby zajišťoval účinnou pomoc po celém území České republiky v určitém časovém limitu s dostatečným množstvím sil a prostředků. Tento systém zajišťuje, že ochrana majetku a životů není limitována pouze možnostmi jednotlivých obcí, ale je zabezpečena na celostátní úrovni. Jednotky požární ochrany zasahují nejen při požárech, ale i při dopravních nehodách, úniku nebezpečných látek, živelních pohromách a dalších mimořádných událostech.

Organizace a činnost jednotek požární ochrany je upravena zákonem č. 133/1985 Sb., o požární ochraně, a vyhláškou Ministerstva vnitra č. 247/2001 Sb., která stanoví podmínky pro plošné pokrytí území ČR jednotkami požární ochrany. Nařízení vlády č. 172/2001 Sb., k provedení zákona o požární ochraně, definuje zásahové obvody a opěrné body jednotek požární ochrany. Každé katastrální území obce je předurčeno odpovídajícím zajištěním jednotkami požární ochrany podle stupně nebezpečí, což zajišťuje rychlou a efektivní pomoc při mimořádných událostech na celém území České republiky.

Profesionální jednotky požární ochrany, konkrétně Hasičský záchranný sbor České republiky, jsou podřízeny Ministerstvu vnitra. Toto ministerstvo zajišťuje legislativní rámec, finanční prostředky a celkovou koordinaci činností HZS ČR. Dobrovolné hasičské jednotky jsou organizovány na úrovni obcí, které odpovídají za jejich financování a vybavení, a spolupracují s HZS ČR.

Základní princip organizace systému jednotek PO[4] spočívá v tom, že každému katastrálnímu území obce je, dle stupně jeho nebezpečí, předurčeno odpovídající zajištění jednotkami PO které garantuje:

dobu dojezdu jednotek PO, danou operační hodnotou jednotek PO dle jejich druhu,

množství sil a prostředků jednotek PO (počet jednotek PO a jejich vybavení, počet hasičů), které se do určeného časového okamžiku dostaví na místo zásahu.

Stupeň nebezpečí území obce	Počet jednotek PO a doba jejich dojezdu na místo zásahu
I	A: 2 JPO do 7 min a další 1 JPO do 10 min B: 1 JPO do 7 min a další 2 JPO do 10 min
II	A: 2 JPO do 10 min a další 1 JPO do 15 min B: 1 JPO do 10 min a další 2 JPO do 15 min
III	A: 2 JPO do 15 min a další 1 JPO do 20 min B: 1 JPO do 15 min a další 2 JPO do 20 min
IV	A: 1 JPO do 20 min a další 1 JPO do 25 min

Základní tabulka plošného pokrytí území ČR jednotkami PO

1 JPO – jedna jednotka PO

2 JPO – dvě jednotky PO

min – minut

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

Systém jednotek PO vybudovaný dle tohoto principu garantuje základní úroveň pomoci poskytovanou jednotkami PO a je označován jako plošné pokrytí území ČR jednotkami PO (dále jen „plošné pokrytí“). Plošné pokrytí vychází z § 65 odst. 6 a přílohy č. 1 zákona č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů; dále je upraveno § 1 a přílohou č. 1 vyhlášky Ministerstva vnitra č. 247/2001 Sb., o organizaci a činnosti jednotek požární ochrany, ve znění vyhlášky č. 226/2005 Sb., § 5 nařízení vlády č. 172/2001 k provedení zákona o požární ochraně ve znění nařízení vlády č. 498/2002 Sb.

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

Rostoucí počet událostí zajišťovaných HZS (https://www.hzscr.cz/soubor/informacni-servis-statistiky-rocenka-2023-pdf.aspx)

Druhy řešených událostí v roce 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

Závěrem jedna ze Statistické ročenky HZS ČR 2023 ((https://www.hzscr.cz/soubor/informacni-servis-statistiky-rocenka-2023-pdf.aspx)) týkající se negativních vlivů na zásah.

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

2.1.1.3 Policie České republiky (PČR)

Policie České republiky hraje klíčovou roli v zajištění veřejného pořádku a bezpečnosti. PČR je zodpovědná za prevenci a potírání trestné činnosti, ochranu majetku a zdraví občanů, a asistenci při záchranných a likvidačních pracích. Policie také poskytuje podporu ostatním složkám IZS při koordinaci a řízení zásahů.

Policie České republiky je jednotný ozbrojený bezpečnostní sbor zřízený na základě zákona č. 273/2008 Sb., o Policii České republiky ve znění pozdějších předpisů. Jejím úkolem je chránit bezpečnost osob a majetku, chránit veřejný pořádek a předcházet trestné činnosti. Plní rovněž úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, předpisy Evropských společenství a mezinárodními smlouvami, které jsou součástí právního řádu České republiky.

Policie České republiky je podřízena Ministerstvu vnitra. Tvoří ji policejní prezidium, útvary s celostátní působností, krajská ředitelství policie a útvary zřízené v rámci krajských ředitelství. Zákon zřizuje 14 krajských ředitelství policie, jejichž územní obvody se shodují s územními obvody 14 krajů České republiky.

2.1.1.4 Zdravotnická záchranná služba (ZZS)

Zdravotnická záchranná služba je odpovědná za poskytování neodkladné lékařské pomoci při mimořádných událostech. ZZS zajišťuje přednemocniční péči, transport pacientů do zdravotnických zařízení a podporu při hromadných neštěstích. Její činnost je klíčová pro záchranu životů a minimalizaci zdravotních následků krizových situací.

ZZS je zdravotní službou, v jejímž rámci je na základě tísňové výzvy poskytována přednemocniční neodkladná péče osobám se závažným postižením zdraví nebo v přímém ohrožení života. Dostupnost zdravotnické záchranné služby je zajištěna plánem pokrytí území kraje výjezdovými základnami. Tento plán stanoví počet a rozmístění výjezdových základen podle demografických, topografických a rizikových parametrů jednotlivých obcí a městských částí, tak aby místo události bylo dosažitelné z nejbližší výjezdové základny v dojezdové době do 20 minut[5].

Hlavní podmínky činnosti zdravotnické záchranné služby jsou definovány v zákoně č. 374/2011 Sb., o zdravotnické záchranné službě, a souvisejících prováděcích vyhláškách. ZZS spadá do působnosti krajů, přičemž poskytovateli jsou příspěvkové organizace zřízené jednotlivými kraji, metodicky řízené Ministerstvem zdravotnictví.

2.1.2 Ostatní ozbrojené a záchranné složky

Ostatní složky IZS poskytují při záchranných a likvidačních pracích plánovanou pomoc na vyžádání. Mezi ostatní složky IZS například patří:

- Obecní/městská policie
- Vyčleněné síly a prostředky ozbrojených sil
- Ostatní ozbrojené bezpečnostní sbory
- Ostatní záchranné sbory
- Armáda České republiky
- Orgány ochrany veřejného zdraví
- Havarijní, pohotovostní, odborné a jiné služby
- Záchranný tým Českého červeného kříže
- Zařízení civilní ochrany
- Neziskové organizace a sdružení občanů, které lze využít k záchranným a likvidačním pracím, např. Asociace dobrovolných záchranářů ČR, z.s.
- Horská služba ČR
- Vodní záchranná služba ČČK
- Skalní záchranná služba ČČK
- Odborná zdravotnická zařízení na úrovni fakultních nemocnic pro poskytování specializované péče (stávají se ostatními složkami IZS v době krizových stavů).

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

2.1.2.1 Armáda České republiky

Armáda České republiky je jednou z klíčových ostatních složek IZS, která poskytuje podporu v rámci záchranných a likvidačních prací. AČR je zapojena do krizového řízení a civilní ochrany obyvatelstva, přičemž její role je definována zákonem č. 219/1999 Sb., o ozbrojených silách České republiky. Armáda ČR se do záchranných operací zapojuje zejména na vyžádání – je povolávána, kdy poskytuje své specifické schopnosti, prostředky a odborný personál k řešení mimořádných událostí a krizových situací.

Hlavní úlohou Armády ČR v rámci IZS je:

Poskytování odborné a technické pomoci při rozsáhlých přírodních katastrofách, jako jsou povodně, lesní požáry, zemětřesení a další živelní pohromy.

Pomoc při zajištění evakuace obyvatelstva z ohrožených oblastí a poskytování humanitární pomoci.

Pomoc při likvidaci následků chemických, biologických, radiologických a nukleárních incidentů.

Podpora při zajišťování logistiky, dopravy a komunikace v krizových situacích.

Spolupráce s ostatními složkami IZS při plnění úkolů ochrany obyvatelstva a majetku.

Pomoc při identifikaci a řešení hybridních kybernetických hrozeb/útoků.

Armáda ČR je vybavena specializovanými jednotkami a technikou, které jsou připraveny k rychlému nasazení v případě potřeby. Mezi tyto jednotky patří například ženijní jednotky, které jsou schopné provádět technické zásahy, stavět provizorní mosty a odstraňovat překážky, a chemické jednotky, které jsou vyškoleny k zásahům při úniku nebezpečných látek.

Spolupráce mezi Armádou ČR a ostatními složkami IZS je koordinována prostřednictvím krizových štábů na různých úrovních státní správy a samosprávy. Tato koordinace zajišťuje efektivní využití všech dostupných prostředků a odborností při řešení krizových situací a mimořádných událostí.

2.1.3 Koordinace a komunikace v rámci IZS

Efektivní koordinace mezi různými složkami IZS je zásadní pro úspěšné zvládání krizových situací. Klíčovým prvkem této koordinace je spolehlivá a bezpečná komunikační infrastruktura, která umožňuje rychlou a přesnou výměnu informací. V České republice se pro tento účel využívá radiokomunikační síť PEGAS/TETRAPOL IP, která poskytuje zabezpečenou komunikaci mezi složkami IZS.

Hlavním koordinátorem činnosti IZS ČR je HZS ČR. Tato role je stanovena zákonem č. 239/2000 Sb., o integrovaném záchranném systému, a podrobněji upravena vyhláškou č. 328/2001 Sb., o některých podrobnostech zabezpečení integrovaného záchranného systému. Ministerstvo vnitra koordinuje a rozvíjí tísňovou komunikaci (hlasovou i textovou), aby bylo zajištěno připojení k základním složkám IZS prostřednictvím čísel 112, 150, 155 a 158. Přijímá opatření pro přístup osob se zdravotním postižením, shromažďuje informace o kvalitě tísňové komunikace a spolupracuje s dalšími ministerstvy a orgány EU.

2.1.3.1 Komunikační potřeby složek IZS

Komunikační potřeby složek IZS souvisejí s výkonem jejich činností podle zákonů, definovaných podmínek a operačních postupů. Tyto potřeby se vyvíjejí s technologickým rozvojem komunikační infrastruktury a bezpečnostními standardy. Historicky byly tyto potřeby realizovány prostřednictvím oddělených hlasových a datových služeb, které se dnes stále více integrují díky pokročilým technologiím.

Řízení IZS je rozděleno do 14 krajů, což odpovídá i rozdělení krajských dispečinků a řízení komunikačních sítí. Privátní sítě (PEGAS/ TETRAPOL IP, DMR a TETRA) a zprostředkovaná komunikace jsou propojeny na úrovni dispečinku (dispečink má přístup ke všem dostupným sítím v rámci kraje, ale systémy propojeny nejsou) nebo na úrovni velitele zásahu, který je vybaven více komunikačními terminály. Dispečinky jsou propojeny do veřejné pevné sítě (VPS) i veřejná mobilní sítě (VMS) a vzájemně mezi sebou. Datové služby jsou dostupné pouze na úrovni dispečinku (pevná datová síť) nebo omezeně některým uživatelům (např. Policie ČR) v podobě tzv. Mobilní bezpečné platformy i mobilní datové služby. Datové služby mají nyní legislativně z hlediska krizové komunikace pouze omezenou podpůrnou roli, díky dlouho neaktualizované právní úpravě.

Mobilní komunikace složek IZS je v současné době zajišťována několika vzájemně nepropojenými komunikačními řešeními. Současný koncept komunikační infrastruktury bezpečnostních a záchranných služeb vychází z historického modelu, kdy klíčovým úkolem komunikační infrastruktury bylo zajištění zabezpečené hlasové komunikace jednotlivých složek IZS, kterou

primárně zajišťoval systém TETRAPOL (v ČR provozovaný jako síť PEGAS/ TETRAPOL IP). Vedle tohoto systému jsou parciálně využívány i jiné rádiové analogové i digitální sítě jako DMR, TETRA a služby mobilních operátorů.

2.1.3.2 Hmotné rezervy v České republice

Hmotné rezervy jsou klíčovou součástí krizového řízení České republiky. Jejich správa je v kompetenci Správy státních hmotných rezerv (SSHR), která zajišťuje zásoby strategických materiálů a surovin potřebných pro zvládání krizových situací, jakými jsou přírodní katastrofy, technické havárie či jiné mimořádné události. Hmotné rezervy zahrnují například potraviny, ropné produkty, zdravotnický materiál a další nezbytné suroviny, které mohou být rychle mobilizovány pro zajištění stability a bezpečnosti státu.

SSHR je řízena zákonem č. 97/1993 Sb., o působnosti Správy státních hmotných rezerv. Tento zákon definuje rozsah a způsob zajištění státních hmotných rezerv, jejich doplňování a obměny, a stanovuje, že SSHR je podřízena vládě České republiky a koordinuje své aktivity s ostatními složkami krizového řízení a IZS.

Hmotné rezervy jsou skladovány ve strategicky rozmístěných skladech po celé republice, což umožňuje jejich rychlé a efektivní využití při krizových situacích. SSHR je také odpovědná za aktualizaci a správu zásob, aby odpovídaly současným potřebám a byly vždy připraveny k použití.

Součástí hmotných rezerv jsou i prostředky nezbytné pro zvládání krizových situací od pohonných hmot až po nezbytné vybavení.

2.2 Legislativní rámec pro PPDR/IZS

Legislativní rámec pro služby PPDR/IZS v České republice je určen několika zákony a nařízeními, které společně zajišťují organizaci, koordinaci a technické zabezpečení IZS. PPDR jako takové není v českých zákonech explicitně definováno, avšak jeho principy a operace jsou zahrnuty v následujících legislativních dokumentech:

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (Krizový zákon)

Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů

Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

2.2.1 Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (Krizový zákon)

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů definuje:

Zabezpečení informačních systémů krizového řízení: Informační systémy musí být technicky a programově přizpůsobeny pro činnost v obtížných podmínkách, což zahrnuje odolnost proti výpadkům, bezpečnostní opatření proti kybernetickým hrozbám a schopnost rychle obnovit provoz po narušení.

Úrovně krizového řízení: Zákon určuje různé úrovně krizových stavů (nouzový stav, stav ohrožení státu, válečný stav) a specifikuje pravomoci a povinnosti jednotlivých orgánů při jejich vyhlašování a řízení.

Povinnosti orgánů státní správy a samosprávy: Stanovuje povinnosti a odpovědnosti orgánů státní správy a samosprávy při přípravě na krizové situace a jejich zvládání.

2.2.2 Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů

Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů:

Stanovuje základní a ostatní složky IZS: Definuje hlavní složky IZS, kterými jsou Hasičský záchranný sbor České republiky, Policie České republiky, Zdravotnická záchranná služba a také další složky, které mohou být zapojeny do záchranných a likvidačních prací, jako jsou Armáda, orgány ochrany veřejného zdraví, havarijní služby a specializované jednotky.

Určuje povinnosti jednotlivých složek IZS: Každá složka má jasně definované povinnosti při přípravě na mimořádné události a krizové situace, jejich zvládání a následné obnově.

Koordinace a řízení IZS: Zákon určuje způsob koordinace a řízení mezi jednotlivými složkami IZS, včetně zřízení a fungování operačních a informačních středisek.

2.2.3 Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Zákon č. 127/2005 Sb. o elektronických komunikacích upravuje podmínky poskytování elektronických komunikačních služeb, což má přímý vliv na činnost a koordinaci složek PPDR v České republice. Tento zákon zabezpečuje, aby komunikační infrastruktura byla odolná, spolehlivá a připravená na krizové situace.

Aspekty relevantní pro PPDR:

Zabezpečení infrastruktury: Zákon vyžaduje, aby poskytovatelé komunikačních služeb zajistili nepřetržitou dostupnost služeb, což je klíčové pro efektivní fungování složek IZS během krizí.

Prioritizace komunikací: Povinnosti zahrnují umožnění prioritních hovorů a datových přenosů pro potřeby záchranných služeb, čímž se zajistí, že kritická komunikace není přerušena ani při přetížení sítí.

Přidělení rádiového spektra: Zákon upravuje přidělení specifických frekvencí pro veřejnou ochranu a záchranné služby, čímž se zajistí spolehlivá a neustálá komunikace.

Ačkoli PPDR jako samostatný pojem není v českých zákonech explicitně definovaný, legislativní rámec daný výše uvedenými zákony zajišťuje, že principy a operace spojené s PPDR jsou efektivně integrovány do fungování IZS. Tyto zákony poskytují potřebnou strukturu a pravomoci pro zvládání krizových situací, ochranu veřejnosti a koordinaci mezi různými záchrannými složkami.

2.2.4 Příklady předpisů, které je nutné zohlednit při řešení komunikace IZS

Normy a smlouvy hrají důležitou roli v rámci širšího spektra událostí na mezinárodní úrovni, kde bude potřebná pomoc IZS, například v případě válečného stavu, přírodních katastrof nebo teroristických útoků.

Mezi příklady předpisů, které je nutné zohlednit při řešení komunikace Integrovaného záchranného systému, patří:

2.2.4.1 Mezinárodní vztahy a vazby. Ústavní zákony.

Mezinárodní vztahy a vazby:

Severoatlantická smlouva (Washington, D.C., 4.dubna 1949)

č. 168/1991 Sb., Sdělení federálního ministerstva zahraničních věcí o vázanosti České a Slovenské federativní republiky Dodatkovými protokoly I a II k Ženevským úmluvám z 12. srpna 1949 a o ochraně obětí mezinárodních ozbrojených konfliktů a konfliktů nemajících mezinárodní charakter, přijatých v Ženevě dne 8. června 1977

Ústavní zákony:

č. 1/1993 Sb., Ústava České republiky

č. 347/1997 Sb., Ústavní zákon o vytvoření vyšších územních samosprávných celků a o změně ústavního zákona České národní rady č. 1/1993 Sb., Ústava České republiky

č. 110/1998 Sb., Ústavní zákon o bezpečnosti České republiky

2.2.4.2 Oblast veřejné správy:

č. 36/1960 Sb., Zákon o územním členění státu

č. 2/1969 Sb., Zákon o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky

č. 128/2000 Sb., Zákon o obcích (obecní zřízení)

č. 129/2000 Sb., Zákon o krajích (krajské zřízení)

č. 131/2000 Sb., Zákon o hlavním městě Praze

č. 320/2002 Sb., Zákon o změně a zrušení některých zákonů v souvislosti s ukončením činnosti okresních úřadů

č. 314/2002 Sb., Zákon o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností

č. 388/2002 Sb., Vyhláška Ministerstva vnitra o stanovení správních obvodů obcí s pověřeným obecním úřadem a správních obvodů obcí s rozšířenou působností

č. 564/2002 Sb., Vyhláška Ministerstva vnitra o stanovení území okresů České republiky a území obvodů hlavního města Prahy

2.2.4.3 Oblast krizového řízení. Oblast havarijního plánování a ochrany obyvatelstva.

č. 240/2000 Sb., Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)

č. 181/2014 Sb., Zákon o kybernetické bezpečnosti

č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

č. 462/2000 Sb., Nařízení vlády k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvků kritické infrastruktury

č. 75/2001 Sb., Vyhláška Českého báňského úřadu, kterou se stanoví báňsko-technické podmínky pro zřizování, využití a ochranu důlních děl vybraných pro využití při krizových situacích pro uplatňování preventivních, technických a bezpečnostních opatření a provádění kontrol

č. 281/2001 Sb., Vyhláška Ministerstva školství, mládeže a tělovýchovy, kterou se provádí § 9 odst. 3 písm. a) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

č. 239/2000 Sb., Zákon o integrovaném záchranném systému a o změně některých zákonů

č. 463/2000 Sb., Nařízení vlády o stanovení pravidel zapojování do mezinárodních záchranných operací, poskytování a přijímání humanitární pomoci a náhrad výdajů vynakládaných právnickými osobami a podnikajícími fyzickými osobami na ochranu obyvatelstva

č. 328/2001 Sb., Vyhláška Ministerstva vnitra, o některých podrobnostech zabezpečení integrovaného záchranného systému

č. 380/2002 Sb., Vyhláška Ministerstva vnitra k přípravě a provádění úkolů ochrany obyvatelstva

2.2.4.4 Další oblasti

Oblast požární ochrany

Oblast prevence závažných havárií

Oblast hospodářských opatření pro krizové stavy

Oblast ropné bezpečnosti

Oblast zdravotnictví. Oblast ochrany veřejného zdraví

Oblast ochrany před povodněmi, nouzové zásobování vodou

Oblast jaderné bezpečnosti

Oblast bezpečnosti a veřejného pořádku

Oblast obrany

Oblast chemických látek a zákazu chemických zbraní

Oblast odpadového hospodářství

Oblast životního prostředí (ochrana ovzduší)

Oblast rostlinolékařské péče

Oblast veterinární péče

Oblast energetiky

Oblast dopravy

Oblast komunikačních a informačních systémů

Oblasti kybernetické ochrany

Oblast obnovy postiženého území

Oblast bankovnictví a financování

Oblast ochrany utajovaných informací a ochrany osobních údajů

Ostatní související legislativa

Usnesení vlády, směrnice a metodické pokyny ministerstev a ostatních ústředních správních úřadů

2.3 Mimořádná událost, krizová situace, krizové stavy

2.3.1 Mimořádná událost

Mimořádná událost je událost, která ohrožuje životy, zdraví, majetek nebo životní prostředí a vyžaduje provedení záchranných a likvidačních prací. Mezi mimořádné události patří například přírodní katastrofy, průmyslové havárie nebo hromadné nehody. Cílem je minimalizovat následky těchto událostí prostřednictvím efektivní a rychlé reakce záchranných složek.

2.3.1.1 Přehled mimořádných událostí s nepřijatelným rizikem

Na základě Analýzy hrozeb pro Českou republiku bylo stanoveno 22 typů mimořádných událostí, pro které lze odůvodněně předpokládat vyhlášení krizového stavu. Pro tyto mimořádné události zpracovaly odpovědné ústřední správní úřady typové plány, které se staly základní součástí všech krizových plánů. Pro tyto plány se předpokládá, že je nebude možno zvládnout za použití běžných prostředků a postupů. Přehled je uveden v tabulce níže.

č.	Mimořádná událost	Odpovědnost
1	Dlouhodobé sucho	Ministerstvo životního prostředí
2	Extrémně vysoké teploty	Ministerstvo životního prostředí
3	Přívalová povodeň	Ministerstvo životního prostředí
4	Vydatné srážky	Ministerstvo životního prostředí
5	Extrémní vítr	Ministerstvo životního prostředí
6	Povodeň	Ministerstvo životního prostředí
7	Epidemie – hromadné nákazy osob	Ministerstvo zdravotnictví
8	Epifytie – hromadné nákazy polních kultur	Ministerstvo zemědělství
9	Epizootie – hromadné nákazy zvířat	Ministerstvo zemědělství
10	Narušení dodávek potravin velkého rozsahu	Ministerstvo zemědělství
11	Narušení funkčnosti významných systémů elektronických komunikací	Český telekomunikační úřad
12	Narušení bezpečnosti informací kritické informační infrastruktury	Národní bezpečnostní úřad
13	Zvláštní povodeň	Ministerstvo zemědělství
14	Únik nebezpečné chemické látky ze stacionárního zařízení	Ministerstvo životního prostředí
15	Narušení dodávek pitné vody velkého rozsahu	Ministerstvo zemědělství
16	Narušení dodávek plynu velkého rozsahu	Ministerstvo průmyslu a obchodu
17	Narušení dodávek ropy a ropných produktů velkého rozsahu	Správa státních hmotných rezerv
18	Radiační havárie	Státní úřad pro jadernou bezpečnost
19	Narušení dodávek elektrické energie velkého rozsahu	Ministerstvo průmyslu a obchodu
20	Migrační vlny velkého rozsahu	Ministerstvo vnitra

21	Narušování zákonnosti velkého rozsahu (včetně terorismu)	Ministerstvo vnitra
22	Narušení finančního a devizového hospodářství státu velkého rozsahu	Ministerstvo financí

2.3.2 Krizová situace

Krizová situace nastává, když mimořádná událost přeroste do stavu, který vyžaduje vyhlášení krizového stavu. Krizová situace ohrožuje bezpečnost státu, veřejný pořádek, životy a zdraví obyvatel ve větším rozsahu a intenzitě. Řešení krizové situace zahrnuje koordinovanou spolupráci mezi různými složkami integrovaného záchranného systému a často také spolupráci s mezinárodními partnery.

2.3.3 Krizové stavy

Krizové stavy jsou legislativně definované stavy, které umožňují přijmout mimořádná opatření ke zvládnutí krizových situací.

Krizové stavy se vyhlašují proto, aby se pravomoci a kompetence podle zákona č. 240/2000 Sb., o krizovém řízení a ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky dostaly do rukou orgánů krizového řízení. Tabulka níže poskytuje přehled krizových stavů, včetně jejich zákonného základu, vyhlašujícího orgánu, definice, územního rozsahu a doby trvání.

V České republice jsou vyhlášeny čtyři typy krizových stavů:

- Válečný stav
- Stav ohrožení státu
- Nouzový stav
- Stav nebezpečí

NÁZEV	DEFINUJÍCÍ ZÁKON	VYHLAŠUJE	DEFINICE	ÚZEMÍ	DOBA TRVÁNÍ
VÁLEČNÝ STAV	Ústavní zákon č. 1/1993 Sb., Ústava České republiky, Ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR	Parlament České republiky	Je-li Česká republika napadena nebo je-li třeba plnit mezinárodní smluvní závazky o společné obraně proti napadení	Celý stát	Není omezeno
STAV OHROŽENÍ STÁTU	Ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR	Parlament České republiky na návrh vlády	Je-li bezprostředně ohrožena svrchovanost státu, územní celistvost státu nebo jeho demokratické základy	Celý stát, omezené území	Není omezeno
NOUZOVÝ STAV	Ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR	Vláda (předseda vlády)	V případě živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo jiného nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty, anebo vnitřní pořádek a bezpečnost	Celý stát, omezené území	Nejdéle 30 dnů (prodloužení se souhlasem Poslanecké sněmovny)
STAV NEBEZPEČÍ	Zákon č. 240/2000 Sb., o krizovém řízení	Hejtman kraje	Jsou-li ohroženy životy, zdraví, majetek, životní prostředí, pokud nedosahuje intenzita ohrožení značného rozsahu a není možné odvrátit ohrožení běžnou činností správních úřadů, orgánů krajů a obcí, složek integrovaného záchranného systému nebo subjektů kritické infrastruktury	Celý kraj, část kraje	Nejdéle 30 dnů (prodloužení se souhlasem vlády)

2.3.3.1 Válečný stav

Vyhlašuje Parlament ČR v případě napadení státu nebo při plnění mezinárodních smluvních závazků o společné obraně proti napadení.

Role armády během válečného stavu

Během válečného stavu má Armáda České republiky zásadní úlohu v obraně suverenity a územní celistvosti státu. Jejím hlavním úkolem je přejít do plné bojové pohotovosti, což znamená, že všechny jednotky jsou připraveny k okamžitému nasazení do vojenských operací. Armáda je zodpovědná za mobilizaci sil, která zahrnuje povolávání vojáků v záloze a zajištění dostatečného množství vojenského materiálu. Kromě toho musí armáda řešit úhradu ztrát a vytvářet nové vojenské útvary, aby byla zajištěna nepřetržitá bojeschopnost.

Významnou součástí činnosti armády je také spolupráce s mezinárodními partnery, zejména s NATO, což zahrnuje koordinaci vojenských operací a logistickou podporu spojeneckých vojsk na českém území. Armáda plní úkoly spojené s obranou státu a dodržováním mezinárodních závazků v oblasti kolektivní obrany. Důležitou částí příprav je i hospodářská mobilizace, která zahrnuje zajištění materiálu a logistických prostředků potřebných pro vojenské operace. Tím se zajišťuje dlouhodobá schopnost armády reagovat na vojenské výzvy a hrozby.

2.3.3.2 Stav ohrožení státu

Vyhlašuje Parlament ČR při bezprostředním ohrožení samostatnosti, územní celistvosti nebo demokratických základů státu.

2.3.3.3 Nouzový stav

Vyhlašuje vláda při rozsáhlých živelních pohromách, ekologických nebo průmyslových haváriích, které ohrožují velké oblasti nebo velké množství obyvatel.

2.3.3.4 Stav nebezpečí

Vyhlašuje hejtman kraje při bezprostředním ohrožení životů, zdraví, majetku nebo životního prostředí, kdy nelze situaci zvládnout běžnými prostředky.

Od vzniku České republiky byly hejtmany vyhlášeny stavy nebezpečí z různých důvodů, příklady počtu vyhlášených stavů:[6]

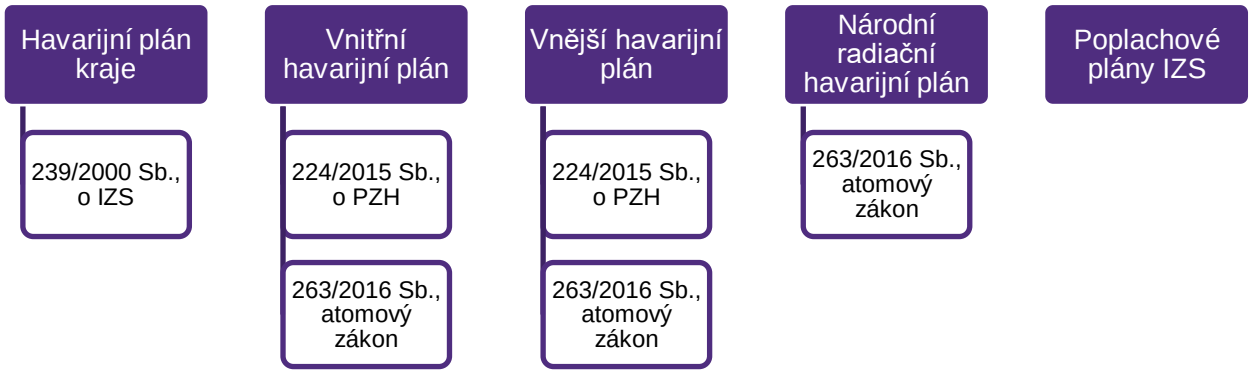
- 28 případů povodní
- 4 případy sesuvu půdy
- 2 případy nálezu nebezpečných látek
- 2 případy extrémního větru (tornáda)
- 1 případ poruchy vodního díla
- 1 případ afrického moru prasat
- 1 případ pandemie

2.3.4 Havarijní plánování

Havarijní plánování je klíčovým prvkem krizového řízení, jehož cílem je připravit se na mimořádné události, které mohou vážně ohrozit lidské životy, zdraví, majetek nebo životní prostředí. Tento proces zahrnuje vytváření a aktualizaci různých plánovacích dokumentů, které stanovují postupy pro zvládání a řešení krizových situací.
Na tyto havarijní plány navazuje i činnost jak základních i ostatních složek IZS. Tyto složky tedy musí být vždy připraveny na řešení vzniklých událostí, a to jak kapacitně, komunikačně, tak i technicky(vybavením).

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

2.3.4.1 Typy Havarijních Plánů



Typy Havarijních plánů

Existuje několik typů havarijních plánů, které se liší svou působností a specifickými požadavky. Mezi nejvýznamnější patří:

Havarijní Plán Kraje

Havarijní plán kraje je základním dokumentem, který slouží k řešení mimořádných událostí (MU) na území kraje. Tyto události mohou zahrnovat živelní pohromy, technologické havárie nebo jiná nebezpečí ohrožující obyvatelstvo a majetek.

Havarijní plán kraje zpracovává HZS kraje ve spolupráci s dotčenými subjekty (KU, ORP, PČR, ZZS, KVS, KHS, KVV). Plán vychází z analýzy vzniku mimořádných událostí a ohrožení území kraje. Jsou vyhotoveny dvě kopie: jedna součástí krizového plánu kraje (KPK), druhá pro operační a informační středisko (OPIS). Plán projednává a posuzuje bezpečnostní rada kraje (BRK) a schvaluje hejtman. Obsahuje tři části: informační (charakteristika kraje, analýza rizik), operativní (postupy a odpovědnosti), a konkrétní činnosti.

Vnější havarijní plán

Vnější havarijní plán je vytvořen pro objekty, které manipulují s nebezpečnými látkami a pro jaderná zařízení. Tyto plány slouží k identifikaci možných rizik a stanovují opatření k ochraně obyvatelstva a zmírnění dopadů havárií. V případě vzniku závažné havárie je klíčové informovat obyvatelstvo a koordinovat zásah složek integrovaného záchranného systému. Plán zahrnuje postupy pro evakuaci, varování a další nezbytná opatření, která minimalizují rizika pro zdraví a bezpečnost občanů.

Vnitřní havarijní plán

Vnitřní havarijní plány jsou klíčovým nástrojem pro zajištění havarijní připravenosti v areálech provozovatelů. Jsou vytvářeny pro objekty, kde je riziko vzniku mimořádných událostí s vážnými dopady na bezpečnost a zdraví. Plány jsou zaměřeny na specifické objekty, jako jsou jaderná zařízení nebo pracoviště s významným zdrojem ionizujícího záření, a také na provozy manipulující s nebezpečnými látkami, které jsou zařazeny do vyšších rizikových kategorií. Provozovatelé těchto zařízení jsou povinni zpracovat a pravidelně aktualizovat vnitřní havarijní plány, aby byli připraveni na efektivní zvládání potenciálních krizových situací.

Národní radiační havarijní plán

Národní radiační havarijní plán je zásadním dokumentem pro krizovou připravenost na události související s radiačním ohrožením. Tento plán zahrnuje komplexní opatření k ochraně obyvatelstva, jako je jodová profylaxe, evakuace a ukrytí. Klade důraz na včasné varování a informování veřejnosti, aby se minimalizovaly zdravotní a bezpečnostní rizika. Plán také specifikuje postupy pro koordinaci zásahů při radiačních haváriích, zahrnující spolupráci mezi různými složkami integrovaného záchranného systému a dalšími relevantními institucemi. Cílem je zajistit rychlou a efektivní reakci na radiační hrozby a maximálně chránit zdraví obyvatelstva.

Poplachové plány IZS

Poplachové plány IZS jsou zásadním prvkem krizového řízení a jsou uloženy na územně příslušných operačních a informačních střediscích HZS kraje. Tyto plány, které zahrnují ústřední poplachový plán IZS i poplachové plány jednotlivých krajů, specifikují postupy pro aktivaci IZS v případě mimořádné události. Obsahují důležité kontaktní údaje na základní a ostatní složky IZS, přehled dostupných sil a prostředků a způsob povolávání a informování vedoucích složek IZS a dalších zodpovědných osob. Plány zajišťují efektivní koordinaci mezi hasiči, policií a zdravotnickou záchrannou službou a umožňují rychlou a účinnou reakci na krizové situace.

2.3.5 Systém krizového řízení v České republice

Krizové řízení v České republice je komplexní a zahrnuje nejen složky IZS, ale také širší okruh orgánů veřejné správy, jako jsou hejtmani, starostové a další relevantní instituce. Tento systém je navržen tak, aby zajistil koordinovanou a efektivní reakci na různé typy krizových situací, včetně přírodních katastrof, technologických havárií, teroristických útoků a dalších mimořádných událostí.

Územní prvky krizového řízení zajišťují připravenost na krizové situace na úrovni krajů a obcí. Kraje mají bezpečnostní rady, které koordinují přípravy na krizové situace. Na úrovni obcí s rozšířenou působností fungují podobné rady, které v krizových situacích zřizují krizové štáby. Hejtmani a starostové vedou tyto krizové štáby a informují vládu o vzniklých krizích. Členy krizových štábů se automaticky stávají členové bezpečnostních rad.

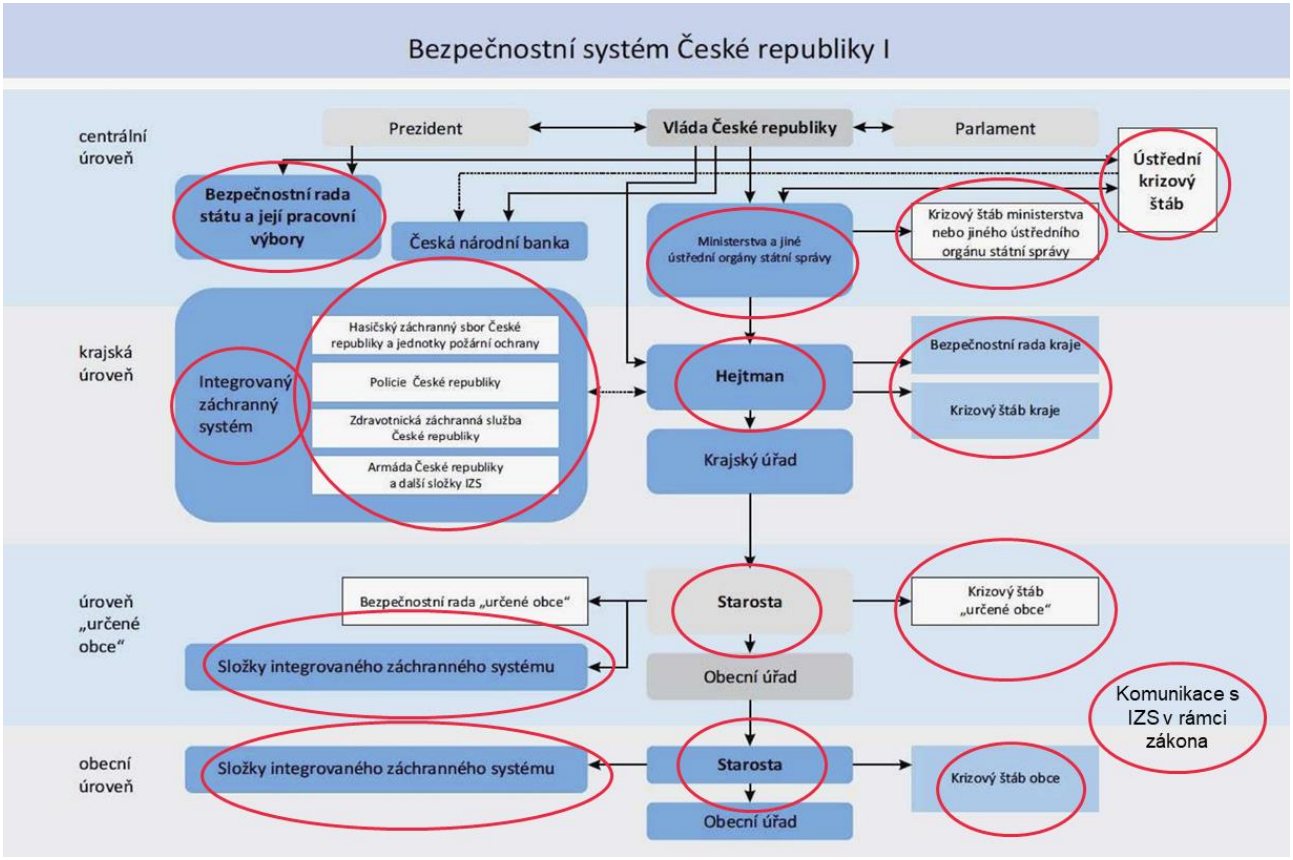
Hasičské záchranné sbory krajů plní úkoly v oblasti požární ochrany a krizového plánování, no také chrání životy a zdraví obyvatel, životní prostředí, zvířata a majetek před požáry a jinými mimořádnými událostmi a krizovými situacemi (živelní pohromy apod.). Krajská ředitelství Policie ČR zajišťují veřejný pořádek, zatímco krajská vojenská velitelství hrají důležitou roli v oblasti obrany.

2.3.5.1 Role hejtmanů a starostů

Hejtmani a starostové hrají klíčovou roli v systému krizového řízení na úrovni krajů a obcí s rozšířenou působností. Hejtman je odpovědný za informování vlády o krizové situaci a za koordinaci činností krizových štábů. Starostové obcí s rozšířenou působností mají podobné povinnosti v rámci svého správního území. Oba tyto subjekty jsou klíčovými hráči při aktivaci a vedení krizových štábů, které jsou nezbytné pro efektivní zvládání krizových situací.

2.3.5.2 Koordinační a řídící orgány

Na úrovni krajů působí bezpečnostní rady, které koordinují přípravu na krizové situace. Tyto rady jsou tvořeny zástupci klíčových složek IZS, veřejné správy a dalších relevantních organizací. Pracovním orgánem hejtmana a starosty obce s rozšířenou působností je krizový štáb, který zahrnuje členy bezpečnostní rady a další odborníky dle potřeby. Krizový štáb může být zřízen i starostou obecního úřadu a jeho členy se automaticky stávají členové bezpečnostní rady.



Zdroj: VŠ AMBIS Krizový management

2.3.5.3 Funkce krizových štábů

Krizové štáby plní několik klíčových funkcí:

Koordinace záchranných a likvidačních prací: Krizové štáby organizují a řídí činnosti jednotlivých složek IZS během mimořádných událostí.

Krizová komunikace: Zajišťují spolehlivou a efektivní výměnu informací mezi všemi zúčastněnými složkami a orgány veřejné správy.

Strategické plánování: Vypracovávají plány pro řešení krizových situací a zabezpečují jejich aktualizaci.

Vyhodnocení situace: Pravidelně vyhodnocují stav krizové situace a přijímají rozhodnutí o potřebných opatřeních.

2.3.6 Stav IZS komunikace v ČR

2.3.6.1 Původní stav

Původní stav komunikační infrastruktury Integrovaného záchranného systému České republiky byl charakterizován použitím několika vzájemně nepropojených komunikačních řešení. Klíčovým prvkem byl systém založený na technologii TETRAPOL (v ČR známý jako síť PEGAS), který zajišťoval zabezpečenou hlasovou komunikaci mezi jednotlivými složkami IZS, jako jsou Hasičský záchranný sbor, Policie ČR a Zdravotnická záchranná služba kromě ZZS Libereckého kraje, kde používají TETRA.

Vedle tohoto systému byly využívány ostatní proprietární analogové i digitální rádiové sítě jako například DMR, TETRA a také služby mobilních operátorů.

2.3.6.2 Aktuální stav

V současnosti je mobilní komunikace složek IZS stále zajišťována výše zmíněnými systémy, přičemž hlavní roli stále hraje síť PEGAS/ TETRAPOL IP. Tato síť poskytuje bezpečnou hlasovou komunikaci díky šifrování na úrovni hardware zařízení a je

využívána všemi základními složkami IZS, kromě některých ZZS. V současnosti je dokončen technologický upgrade sítě, který zahrnuje přechod na IP technologii mezi radiovou a síťovou vrstvou. Vedle toho jsou analogové a DMR sítě využívány jako sekundární komunikační systémy s nižší úrovní zabezpečení. Policie ČR a MV mají přístup k tzv. Mobilní bezpečné platformě, která využívá veřejné mobilní sítě pro zabezpečený přístup do interních systémů.

2.3.6.3 Plánovaný vývoj

Plánovaný vývoj komunikační infrastruktury IZS zahrnuje implementaci vyhrazené jednotné technologické CORE komunikační platformy, která propojí stávající komunikační systémy všech složek IZS a nově připravované vysokorychlostní komunikační řešení v komerčních sítích mobilních operátorů. Cílem je zajistit vysokorychlostní datové služby a zvýšit bezpečnost a efektivitu komunikace. Do roku 2025 je plánováno spuštění plnohodnotné SA (Standalone) sítě 5G, která nabídne sofistikované služby, jako je slicing sítě a ultra nízké latence. Tento vývoj by měl také přinést snížení provozních nákladů a zvýšení flexibility komunikačních nástrojů.

2.4 Rozdělení zásahů IZS/PPDR

Zásahy v PPDR lze rozdělit do několika kategorií podle jejich rozsahu a složitosti. Toto rozdělení pomáhá lépe pochopit různé úrovně krizových situací a odpovídající komunikační potřeby. V této části se nepopisuje současný stav prostředků, ale potřeby IZS[7].

Škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací. Je mimořádná událost, v jejímž důsledku se vyhlašuje krizový stav.

Typ zásahu	Popis	Složky IZS	Komunikační potřeby	Příklady
Malé události	Standardní rutinní operace, vyžadující zásah jedné složky IZS	Jedna složka	Hlasová komunikace, základní textová komunikace	Výjezdy ZZS k pacientům, malé požáry
Střední události	Vyžadují koordinaci dvou až tří složek IZS	Dvě až tři složky	Koordinace hlasové a datové komunikace	Dopravní nehody, větší požáry
Velké události	Komplexní situace, vyžadující zásah několika složek IZS	Více složek	Vysoce náročná komunikace (hlas, data, video)	Povodně, hromadné nehody
Národní události	Události s celostátním dopadem, vyžadující koordinaci na národní úrovni	Všechny složky	Intenzivní využití všech komunikačních prostředků	Pandemie, státní krize
Mezinárodní události	Vyžadují mezinárodní spolupráci a koordinaci	Mezinárodní spolupráce	Interoperabilita mezi národními systémy	Přeshraniční povodně, mezinárodní krizová cvičení

Vždy je třeba si uvědomit, že rizika nejde 100 % eliminovat, jen snížit jejích pravděpodobnost vzniku a minimalizovat dopady.

Jednotlivé události na sebe navazují. Každá vyšší událost zahrnuje potřeby plnění i nižších potřeb událostí.

Členění událostí nastavuje požadavky na zásah a komunikaci v souladu s plněním potřeb tak, aby se maximálně optimalizovaly náklady na potřeby zajištění minimalizace dopadů jednotlivých událostí a jejich co nejrychlejší odstranění následků těchto události.

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

2.4.1 Malé události

Malé události zahrnují standardní rutinní operace, které obvykle vyžadují zásah jedné složky Integrovaného záchranného systému. Tyto operace jsou nejčastější a zahrnují výjezdy zdravotnické záchranné služby k jednotlivým pacientům, menší dopravní nehody a požáry malého rozsahu.

Komunikační potřeby: Primárně hlasová komunikace a základní textová komunikace (na úrovni SMS). Není nutná komplexní koordinace mezi více složkami.

2.4.2 Střední události

Střední události vyžadují koordinaci dvou až tří složek IZS. Tyto události jsou složitější a vyžadují vyšší úroveň koordinace a komunikace. Příklady zahrnují vážnější dopravní nehody, větší požáry nebo incidenty vyžadující asistenci Policie ČR a HZS ČR současně.

Komunikační potřeby: Zvýšené nároky na koordinaci hlasové a datové komunikace mezi zapojenými složkami. Potřeba přenosu informací mezi různými dispečerskými centry a jednotkami na místě události.

2.4.3 Velké události

Velké události zahrnují komplexní situace, které vyžadují zásah několika složek IZS a mohou mít dopad na celý kraj. Tyto události zahrnují hromadné nehody, rozsáhlé přírodní katastrofy nebo teroristické útoky.

Komunikační potřeby: Vysoce náročná komunikace zahrnující přenos hlasu, dat a videa. Efektivní řízení zásahu vyžaduje rychlou a spolehlivou komunikaci mezi všemi zúčastněnými složkami a dispečerskými centry.

2.4.4 Národní události

Národní události mají celostátní dopad a vyžadují koordinaci na národní úrovni. Tyto události mohou zahrnovat pandemie nebo jiné národní krizové stavy, které ovlivňují velkou část populace a infrastruktury.

Komunikační potřeby: Intenzivní využití všech dostupných komunikačních prostředků, včetně krizových řídicích center a záložních komunikačních systémů. Důležitá je koordinace mezi různými úrovněmi vlády.

2.4.5 Mezinárodní události

Mezinárodní události vyžadují mezinárodní spolupráci a koordinaci. Tyto události mohou zahrnovat přírodní katastrofy s přeshraničním dopadem nebo mezinárodní teroristické útoky.

Komunikační potřeby: Komplexní komunikační infrastruktura umožňující interoperabilitu mezi různými národními systémy PPDR. Potřeba rychlé a efektivní komunikace mezi mezinárodními týmy.

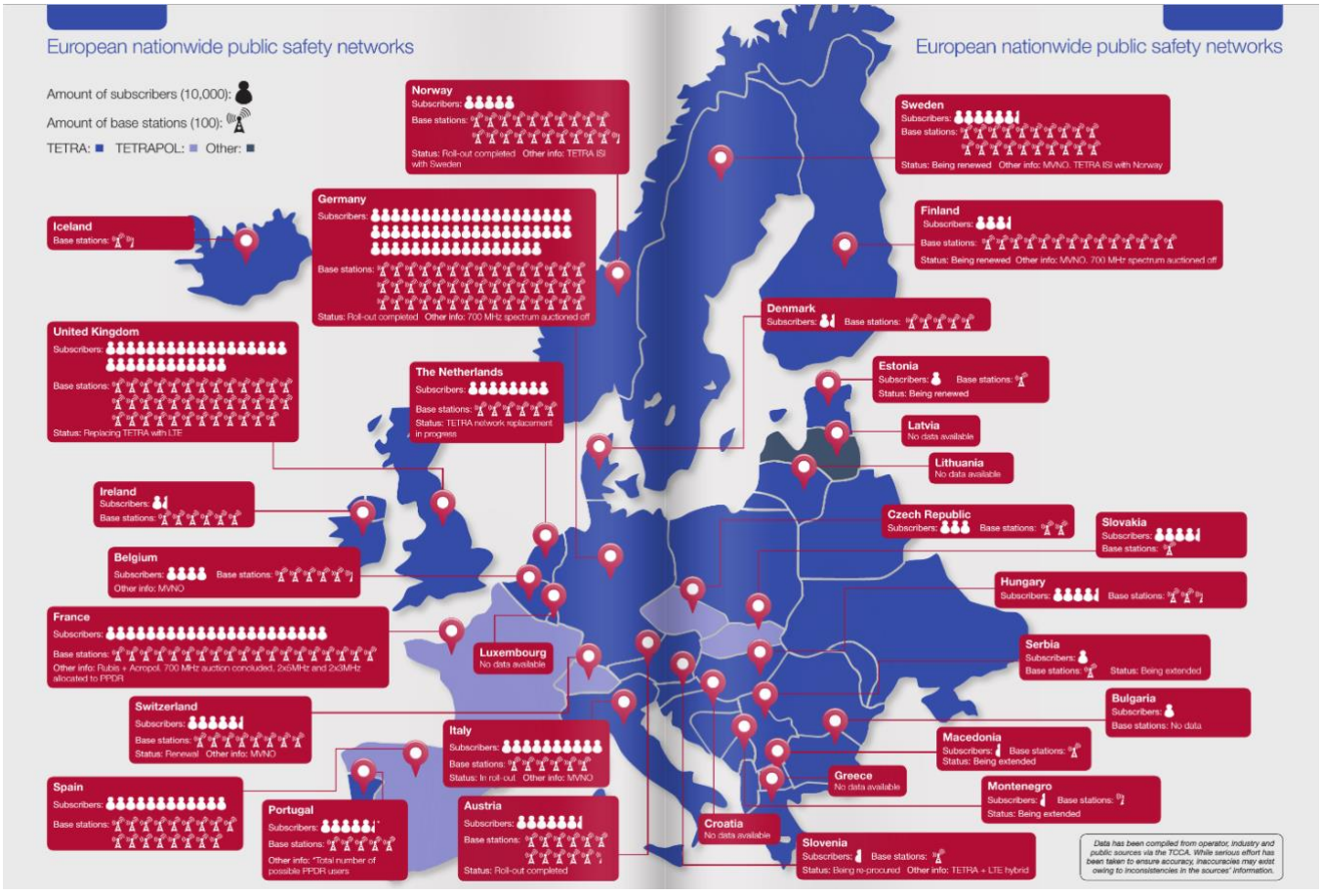
3 Definice PPDR v zahraničí

Integrovaný záchranný systém je klíčovým prvkem krizového managementu, který zajišťuje koordinovanou reakci na mimořádné události, katastrofy a jiné nouzové situace. Každá země má svůj vlastní systém IZS, který je přizpůsoben jejím legislativním, geografickým a organizačním podmínkám. Tyto systémy se liší v závislosti na místních potřebách a dostupných zdrojích, přičemž některé kladou větší důraz na centralizaci a jednotné řízení, zatímco jiné upřednostňují regionální spolupráci a dobrovolnictví.

U každého státu se soustředíme na organizační strukturu a porovnání s Českou republikou. Tyto aspekty nám umožní lépe porozumět rozdílům a podobnostem mezi jednotlivými národními systémy IZS a jejich schopnostem zvládat mimořádné události.

3.1 Obecné

Mapa uvedená níže ilustruje stav evropských celonárodních sítí veřejné bezpečnosti, které využívají technologii TETRA k roku 2017. V různých zemích Evropy jsou TETRA sítě široce nasazeny a podporují klíčové komunikace pro záchranné složky. Například v Norsku a Švédsku jsou tyto sítě plně implementovány a zahrnují spolupráci mezi těmito zeměmi. Německo a Spojené království mají jedny z největších sítí s tisíci základnovými stanicemi a stovkami tisíc uživatelů. Spojené království přechází na LTE technologii. Nizozemsko a Francie také aktivně obnovují své TETRA sítě, aby vyhověly rostoucím požadavkům na kritickou komunikaci. Mapa ilustruje rozsáhlé využití TETRA sítí napříč Evropou, zdůrazňuje jejich význam pro veřejnou bezpečnost a ukazuje plány na další vylepšení a integraci s novými technologiemi, jako je LTE.



Zdroj této mapy je časopis TETRA Today, číslo 36, 2017.

Následující tabulka poskytuje přehled o přiřazeném spektru pro veřejnou bezpečnost, vyhrazené centrální agentuře a modelu provozu širokopásmové sítě v každé z uvedených zemí. Data v tabulce pocházejí z roku 2021 a byla získána ze studie, kterou realizovala společnost Capgemini. Tato tabulka shrnuje různé přístupy a modely provozu národních širokopásmových sítí pro veřejnou bezpečnost v různých zemích.

ZEMĚ	POPIS	PŘIŘAZENÉ SPEKTRUM PRO PPDR	VYHRAZENÁ CENTRÁLNÍ AGENTURA	MODEL PROVOZU ŠIROKOPÁSMOVÉ SÍTĚ
AUSTRÁLIE	V roce 2019 australská vláda uznala potřebu mobilní širokopásmové sítě pro veřejnou bezpečnost pro své nouzové služby. Pilotní projekty se vyvíjí od roku 2018.	✓	✓ Vnitrostátní správa pro stanovení pokynů	**Komerční model** Zdá se, že australská vláda se rozhodne pro komerční síť s doplňkovým využitím přiděleného spektra pro veřejnou bezpečnost
BELGIE	Belgie zrevidovala svou strategii komunikační sítě pro veřejnou bezpečnost a plánuje zavést celostátně novou mobilní širokopásmovou síť. Implementace očekávána v letech 2023-2025.	✓	✓ ASTRID – operátor	**Hybridní model (MCON)** Vyhrazená jádrová síť propojená s operátorem a vyhrazeným RAN. Síť provozuje a udržuje ASTRID
DUBAJ	Dubaj vytvořila organizaci „Nedaa“, vládního poskytovatele síťových služeb, věnovaného profesionální komunikaci. Širokopásmové služby poskytovány na LTE.	✓	✓ Neda – operátor	**Vyhrazený model** Vyhrazená síť (jádro a RAN) pro disciplíny veřejné bezpečnosti a další bezpečnostní a zabezpečovací subjekty
FINSKO	Finsko vyvíjí VIRVE 2.0, druhou generaci sítě pro veřejnou bezpečnost založené na LTE/5G technologiích. Implementace očekávána v letech 2023-2025.	✗ Může se v budoucnu změnit	✓ VIRVE – operátor	**Hybridní model (MCON)** Vyhrazená jádrová síť propojená s operátorem a vyhrazeným RAN. Síť provozuje a udržuje VIRVE
FRANCIE	Francie modernizuje svůj komunikační systém pro veřejnou bezpečnost s centralizovaným přístupem podporujícím širokopásmové aplikace. Implementace očekávána v letech 2022-2025.	✓	✓ ACMOSS – operátor	**Hybridní model (FMVNO)** Vyhrazená jádrová síť propojená s operátorem a vyhrazeným RAN dvou operátorů, řízená dedikovanou organizací
NĚMECKO	Německo aktuálně provozuje celostátní síť TETRA pro potřeby komunikace veřejné bezpečnosti. Pilotní projekty jsou testovány, ale oficiální program pro širokopásmovou síť zatím nebyl vyhlášen.	✓	Bude upřesněno	Bude upřesněno
NIZOZEMSKO	Nizozemsko provozuje celostátní síť TETRA (C2000) a plánuje ji udržovat po nějakou dobu. Mobilní širokopásmové řešení bude poskytováno komerčními operátory.	✓	✗	**Komerční model** Širokopásmové služby budou poskytovány komerčními operátory vedle sítě TETRA
SINGAPUR	Singapurské IZS používají vyhrazenou, ale soukromou síť pro svou kritickou komunikaci. Poskytovatel postupně vyvinul poskytování datových služeb pro veřejnou bezpečnost.	✓	✗	**Komerční model** Širokopásmové služby poskytovány komerčním operátorem specializovaným na profesionální komunikaci
JIŽNÍ KOREA	Jižní Korea zavedla první mobilní širokopásmovou síť na světě pro svou veřejnou bezpečnost, železniční a námořní služby. Síť PS-LTE je v plném provozu od roku 2018.	✓	✓ Safe-Net – operátor	**Hybridní model (MCON)** Vyhrazená jádrová síť provozovaná Safe-Net propojená s RAN několika operátorů

ŠVÝCARSKO	Švýcarsko má celostátní síť TETRA pro veřejnou bezpečnost (Polycom), ale začalo testování pro vývoj mobilní širokopásmové sítě pro veřejnou bezpečnost. Současné širokopásmové služby jsou poskytovány pouze pro nekritická řešení.	Bude upřesněno, ale pravděpodobně ano	Bude upřesněno	Bude upřesněno
SPOJENÉ KRÁLOVSTVÍ	Spojené království začalo vyvíjet síť pro agentury veřejné bezpečnosti, která nahradí starší síť TETRA. Několik problémů zpozdilo implementaci do let 2024-2025.	✗	✗	**Komerční model** Širokopásmové služby budou poskytovány komerčními operátory
USA	USA vytvořily dedikovanou agenturu (FirstNet), která spolupracuje s národním operátorem na zavedení širokopásmové sítě pro veřejnou bezpečnost. Síť funguje od roku 2018 a neustále se zlepšuje, aby splňovala požadavky veřejné bezpečnosti.	✓	✓ FirstNet – dozor	**Hybridní model (MCON)** Vyhrazené jádro sítě propojené s operátorovým RAN, síť řízená operátorem

3.2 Definice IZS v rámci Evropské Unie

3.2.1 Německo

Německo má federální systém záchranných služeb, který je organizován na úrovni jednotlivých spolkových zemí (Bundesländer). Tento systém zahrnuje profesionální a dobrovolné hasičské sbory, zdravotnické záchranné služby, policii a další organizace, které spolupracují na poskytování záchranných a nouzových služeb.

3.2.1.1 Organizační struktura

Feuerwehr (Požární sbor)

Profesionální a dobrovolné hasičské sbory, které jsou odpovědné za hašení požárů, záchranné operace při dopravních nehodách, průmyslových haváriích, přírodních katastrofách a dalších nouzových situacích.

Polizei (Policie)

Poskytuje ochranu veřejného pořádku a bezpečnosti, spolupracuje s hasičskými a záchrannými službami při evakuacích a dalších zásazích.

Rettungsdienst (Záchranná služba)

Poskytuje přednemocniční neodkladnou zdravotní péči a převoz pacientů do nemocnic. Záchranné služby jsou obvykle organizovány na regionální úrovni a mohou být provozovány různými organizacemi včetně Červeného kříže, Johanniter-Unfall-Hilfe, Malteser Hilfsdienst a dalších.

Technisches Hilfswerk (THW)

Federální agentura pro technickou pomoc, která poskytuje technickou podporu při katastrofách a nouzových situacích.

Dobrovolné a humanitární organizace

Německý Červený kříž, Johanniter-Unfall-Hilfe, Malteser Hilfsdienst, Arbeiter-Samariter-Bund a další organizace poskytující zdravotní a humanitární pomoc.

3.2.1.2 Porovnání s Českou republikou

Německo se od České republiky v systému záchranných složek liší v několika klíčových ohledech. Hlavní rozdíl spočívá v organizační struktuře – zatímco Německo má federální systém, kde každá spolková země má svou vlastní legislativu a

organizaci záchranných služeb, Česká republika používá centralizovaný model. V Německu tak každý region může přizpůsobit své záchranné služby specifickým potřebám místní populace, což poskytuje větší flexibilitu a rychlejší reakce na místní úrovni. Tento přístup je důležitý vzhledem k velikosti Německa, které je několikanásobně větší než Česká republika.

Legislativa se v Německu liší podle jednotlivých spolkových zemí, což umožňuje přizpůsobení místním podmínkám a potřebám. Tato regionální autonomie podporuje efektivní řízení záchranných služeb. Naproti tomu má Česká republika jednotnou legislativu pro celou zemi, což zajišťuje konzistentní a jednotné řízení záchranných služeb na celostátní úrovni.

Organizace záchranných služeb v Německu zahrnuje významný podíl dobrovolníků a je řízena na regionální úrovni. Federální agentura Technisches Hilfswerk (THW) poskytuje technickou podporu při katastrofách. V České republice je organizace centralizovaná s krajskými složkami Hasičského záchranného sboru ČR, které jsou odpovědné za koordinaci a řízení záchranných operací na regionální úrovni.

Spolupráce mezi složkami je důležitá v obou zemích. V Německu je spolupráce mezi požárními sbory, policií, záchrannými službami, THW a dobrovolnickými organizacemi organizována na regionální úrovni, což umožňuje rychlé a efektivní reakce na krizové situace. V České republice zajišťuje silná spolupráce mezi HZS, policií, zdravotnickou záchrannou službou a dalšími podpůrnými složkami efektivní reakci na krizové situace. Centralizovaný systém v ČR podporuje jednotnost a konzistenci v celostátní koordinaci a zajišťuje, že všechny složky mohou rychle a efektivně spolupracovat při řešení mimořádných událostí.

3.2.2 Belgie

Belgický záchranný systém je koordinovaný a funguje na třech úrovních: místní, provinční a federální. Tento systém zahrnuje federální a místní policii, zdravotnické záchranné služby, profesionální hasičské sbory a civilní ochranu. Na místní úrovni jsou záchranné služby řízeny místními krizovými centry, která zajišťují první reakci na nouzové situace. Provinční úroveň se aktivuje při větších krizích, které přesahují kapacity místních center, a je řízena provinčními krizovými centry. Federální úroveň je zodpovědná za koordinaci při rozsáhlých krizích, které zahrnují více provincií nebo vyžadují národní zásah, a je řízena Národním krizovým centrem

3.2.2.1 Organizační struktura

Belgický integrovaný záchranný systém je rozdělen do pěti hlavních disciplín, z nichž každá má specifickou úlohu v zajištění bezpečnosti a reakci na krizové situace. Tento systém zajišťuje koordinovanou a efektivní pomoc obyvatelstvu při různých typech nouzových situací.

Discipline 1: Pompiers (Hasičský sbor)

Hasičský sbor v Belgii zahrnuje jak profesionální, tak dobrovolné hasiče. Tato složka je odpovědná za hašení požárů, technické zásahy při dopravních nehodách, průmyslových haváriích, přírodních katastrofách a dalších nouzových situacích. Hasičské jednotky byly reorganizovány do 34 zón bezpečnosti, aby se zlepšila koordinace a efektivita zásahů. V Belgii je přibližně 5 000 profesionálních a 12 000 dobrovolných hasičů.

Discipline 2: Aide médicale urgente (Zdravotní záchranná služba)

Zdravotní záchranné služby poskytují přednemocniční neodkladnou zdravotní péči a převoz pacientů do nemocnic. Tyto služby zahrnují centrálu 112, služby ambulancí v Belgii, systém SMUR (mobilní jednotky intenzivní péče) a leteckou zdravotní pomoc z centra.

Discipline 3: Police (Policie)

Policie v Belgii je rozdělena na federální a místní úroveň. Federální policie se zaměřuje na národní a mezinárodní bezpečnostní otázky, zatímco místní policie zajišťuje bezpečnost a veřejný pořádek na lokální úrovni. Zahrnuje také silniční policii a leteckou podporu.

Discipline 4: Logistique (Logistika)

Logistika zahrnuje širokou škálu podpůrných služeb, které poskytují potřebné materiály a technickou podporu při různých zásazích. To zahrnuje dopravu, zásobování, a technickou údržbu nezbytnou pro efektivní fungování ostatních záchranných složek. Mezi spolupracující organizace patří Elia, Electrabel, belgické ozbrojené síly a další.

Discipline 5: Information (Informace)

Tato disciplína zahrnuje komunikaci a šíření informací během krizových situací. Úřady spolupracují s médii a dalšími institucemi na zajištění informovanosti veřejnosti. Speciální komunikační centra jsou připravena poskytovat aktuální a přesné informace o krizových situacích.

3.2.2.2 Porovnání s Českou republikou

Belgický integrovaný záchranný systém a český systém se liší v několika klíčových ohledech, především v organizační struktuře a způsobu řízení.

Belgický IZS je rozdělen do pěti disciplín: hasiči, zdravotní záchranná služba, policie, logistika a informace. Tento víceúrovňový systém (místní, provinční a federální úroveň) umožňuje flexibilní a efektivní reakce na krizové situace, s důrazem na specifické potřeby na místní úrovni. Federální úroveň zase koordinuje rozsáhlé krize prostřednictvím Národního krizového centra.

V České republice je IZS centralizovaný s krajskými složkami Hasičského záchranného sboru ČR, které koordinují záchranné operace na regionální úrovni. Tento model zajišťuje jednotné řízení záchranných služeb napříč celou zemí, s Generálním ředitelstvím HZS na čele celostátních operací.

3.2.3 Finsko

Finsko, známé svou vysokou úrovní bezpečnosti a organizovanosti, má dobře vyvinutý systém integrované záchranné služby, který je podstatným prvkem při ochraně obyvatel a majetku před různými nebezpečími. Finská záchranná služba, je základním stavebním kamenem pro zajištění bezpečnosti a ochrany obyvatelstva.

Finský IZS je decentralizovaný a spravovaný na regionální úrovni. Každý region má svůj vlastní záchranný sbor, který odpovídá za provádění záchranných operací a prevenci katastrof v rámci svého území.

Na národní úrovni koordinuje činnost IZS Finská rada pro bezpečnost (Turvallisuuskomitea), která zajišťuje, aby byly činnosti záchranných složek v souladu s národními strategiemi a aby bylo dosaženo optimální spolupráce mezi různými regiony a složkami.

3.2.3.1 Organizační struktura

Hasiči a záchranáři

Finské hasičské sbory zahrnují profesionální i dobrovolné hasiče, kteří jsou rozděleni do 21 záchranných oblastí. Tyto sbory mají na starost hašení požárů, záchranné operace při dopravních nehodách, přírodních katastrofách, průmyslových haváriích a dalších nouzových situacích. Regionální hasičské sbory fungují s vysokou mírou autonomie, což umožňuje efektivní reakci na místní potřeby. Kromě operativních zásahů se hasiči věnují i preventivním aktivitám, jako jsou inspekce bezpečnosti a vzdělávání veřejnosti.

Policie

Finská policie zajišťuje ochranu veřejného pořádku a bezpečnosti, přičemž úzce spolupracuje s hasiči a zdravotnickými záchrannými službami při evakuacích a jiných zásazích. Policie je rozdělena do regionálních jednotek, které jsou odpovědné za reakci na místní incidenty, řízení dopravy během mimořádných událostí a zajištění bezpečnosti na místech zásahu.

Zdravotnické záchranné služby

Zdravotnické záchranné služby poskytují přednemocniční neodkladnou zdravotní péči a přepravu pacientů do nemocnic. Tyto služby jsou integrovány do regionálních záchranných oblastí a jsou klíčové při reakci na mimořádné zdravotní situace, jako jsou dopravní nehody nebo náhlé zdravotní komplikace. Záchranné týmy jsou vybaveny moderními zdravotnickými technologiemi a poskytují vysokou úroveň péče.

Námořní záchranné služby

Námořní záchranné služby jsou specializovanou složkou finského IZS, která zajišťuje bezpečnost na moři a poskytuje pomoc při námořních nehodách a katastrofách. S ohledem na rozsáhlé pobřeží a množství vodních ploch ve Finsku je tato složka nezbytná pro zajištění rychlé a efektivní reakce na incidenty na moři a v pobřežních oblastech. Námořní záchranné služby jsou vybaveny moderními plavidly a technikou pro různé druhy záchranných operací na vodě.

Dobrovolnické a humanitární organizace

Dobrovolnické a humanitární organizace, jako je Finský Červený kříž, hrají podpůrnou roli v rámci finského IZS. Tyto organizace poskytují pomoc při záchranných operacích, první pomoc, distribuci humanitární pomoci a jsou také aktivně zapojeny do preventivních aktivit a vzdělávání veřejnosti. Dobrovolnické týmy často spolupracují s profesionálními záchrannými složkami při zvládání rozsáhlých mimořádných událostí a katastrof.

3.2.3.2 Porovnání s Českou republikou

Finský záchranný systém je charakterizován svou decentralizovanou strukturou, která klade velký důraz na regionální autonomii a prevenci. Každá z 21 záchranných oblastí ve Finsku má vysokou míru samostatnosti při řízení a provádění záchranných operací, což umožňuje efektivní a rychlou reakci na místní potřeby a rizika. Tento přístup podporuje preventivní opatření, jako jsou pravidelné inspekce, vzdělávací kampaně a aktivní zapojení veřejnosti do prevence a připravenosti na mimořádné události.

Naopak, český IZS je více centralizovaný, s výraznou koordinací na celostátní úrovni prostřednictvím HZS ČR. Český systém klade důraz na centralizované plánování a koordinaci, což umožňuje jednotný a konzistentní přístup k záchranným operacím po celé zemi.

Jedním z rozdílů mezi těmito dvěma systémy je přítomnost námořních záchranných služeb ve Finsku. Finsko, s rozsáhlým pobřežím a množstvím vodních ploch, musí mít efektivní a dobře vybavené námořní záchranné služby, které zajišťují bezpečnost na moři a poskytují pomoc při námořních nehodách a katastrofách. Tyto služby jsou nezbytné pro zajištění ochrany jak vnitrozemských vodních ploch, tak i Baltského moře.

3.2.4 Norsko

Norský integrovaný záchranný systém, známý jako Norwegian Search and Rescue Service (SAR), zahrnuje řadu záchranných služeb pro moře, pevninu a vzduch. Tento systém je koordinován prostřednictvím dvou hlavních center – Joint Rescue Coordination Centres (JRCC) – které se nacházejí v Bodø a Stavangeru. Tyto koordinační centra jsou podřízena Ministerstvu spravedlnosti a veřejné bezpečnosti.

Norwegian SAR Service je organizován tak, že zahrnuje spolupráci mezi vládními agenturami, dobrovolnými organizacemi a soukromými společnostmi. Tyto složky společně poskytují záchranné služby po celé zemi. Kromě dvou hlavních koordinačních center existuje také 28 regionálních záchranných center, které zajišťují reakce na místní události.

3.2.4.1 Organizační struktura

Policie

Norská policie hraje podstatnou roli v záchranném systému, zvláště při koordinaci akcí při záchraně na pevnině a v případech pohřešovaných osob. Policie je rozdělena do 12 okresů, každý s vlastním operačním centrem, které řídí a koordinuje operace.

Hasičský sbor

Hasičské služby v Norsku jsou dostupné prostřednictvím více než 300 hasičských stanic, z nichž většina je tvořena dobrovolnými hasiči. Celkem je zde asi 12 500 hasičů, z nichž pouze přibližně 3 500 jsou profesionální hasiči na plný úvazek. Hasičský sbor je odpovědný za požární ochranu a reakce na mimořádné události, včetně chemických a biologických hrozeb.

Zdravotnická záchranná služba

Zdravotnické záchranné služby zahrnují pozemní i leteckou ambulanci. Norsko má rozsáhlou síť ambulantních vozidel a leteckých záchranářů, kteří jsou schopni rychle reagovat na zdravotní nouze. Letecká záchranná služba ročně obslouží až 20 000 pacientů a zahrnuje 14 vrtulníků rozmístěných po celé zemi.

Letecká a námořní záchrana

Letecká a námořní záchrana je klíčovou součástí norského SAR systému. Patří sem také používání speciálně vybavených vrtulníků, jako je například Sea King, které jsou nasazovány pro záchranné operace na moři i v horách. Norsko má také rozsáhlou pobřežní stráž, která je připravena asistovat 24/7.

3.2.4.2 Porovnání s Českou republikou

Oba systémy mají za úkol koordinovat různé složky záchranných a bezpečnostních sil, aby poskytovaly efektivní a rychlou pomoc v nouzových situacích. Mezi hlavní složky v obou zemích patří zdravotnická záchranná služba, hasičský a záchranný sbor, policie a civilní ochrana.

V Norsku je Norwegian Search and Rescue Service (SAR) koordinován prostřednictvím dvou hlavních center, Joint Rescue Coordination Centres (JRCC), které se nacházejí v Bodø a Stavangeru. Tyto koordinační centra jsou podřízena Ministerstvu spravedlnosti a veřejné bezpečnosti. V České republice je Integrovaný záchranný systém koordinován Ministerstvem vnitra a zahrnuje centrální koordinační centrum a krajská koordinační centra.

V Norsku probíhá koordinace na národní, regionální a místní úrovni. Domácí SAR operace jsou delegovány na jedno z 28 regionálních záchranných podcentrů, které zajišťují místní reakce. V České republice je koordinace také na národní a krajské úrovni, kde krajská koordinační centra hrají klíčovou roli v regionální koordinaci, zatímco místní úroveň je řízena přímo prostřednictvím místních složek IZS.

Norský SAR systém je řízen různými právními normami a královskými dekrety, které stanovují odpovědnosti a úkoly jednotlivých složek. V České republice je právní rámec stanoven zákonem č. 239/2000 Sb., o integrovaném záchranném systému, který definuje fungování a strukturu IZS.

V Norsku mohou být vojenské složky povolány na podporu civilních záchranných operací při velkých katastrofách nebo mimořádných situacích. V České republice jsou vojenské složky zapojovány podobně, ale jejich použití je obvykle omezeno na specifické situace, kdy jsou vyžadovány specializované schopnosti nebo zdroje.

Všechny vládní agentury zapojené do SAR operací v Norsku hradí své náklady ze svých běžných rozpočtů. Komerční podniky jsou placeny podle běžných tržních sazeb a dobrovolné organizace dostávají náhradu za přímé výdaje. V České republice jsou náklady na operace IZS hrazeny ze státního rozpočtu a dalšími zdroji financování podle zákona o IZS.

3.2.5 Maďarsko

V Maďarsku se ekvivalent českého Integrovaného záchranného systému nazývá Nemzeti Veszélyhelyzet-kezelési Rendszer (NVKR), což znamená Národní systém řízení nouzových situací. Tento systém zahrnuje různé záchranné a bezpečnostní složky, které spolupracují při řešení nouzových situací a katastrof. NVKR je koordinován hlavně prostřednictvím Katasztrófavédelmi Koordinációs Kormánybizottság (KKB), tedy Koordinačního výboru pro ochranu před katastrofami, který je řízen ministrem vnitra.

3.2.5.1 Organizační struktura

Maďarská zdravotnická záchranná služba

Maďarská zdravotnická záchranná služba poskytuje rychlou zdravotnickou pomoc a transport pacientů do zdravotnických zařízení. Tato organizace zajišťuje provoz sanitních vozů vybavených moderními zdravotnickými přístroji, které umožňují poskytování první pomoci přímo na místě události. Kromě pozemní záchranné služby disponuje také leteckou záchrannou službou, která je schopná rychle přepravovat pacienty na větší vzdálenosti, zejména v těžko dostupných oblastech nebo při kritických stavech vyžadujících urgentní lékařský zásah.

Hasičský a záchranný sbor

Hasičský a záchranný sbor je zodpovědný za hašení požárů a provádění záchranných prací při dopravních nehodách, přírodních katastrofách a dalších nouzových situacích. Tento sbor je vybaven špičkovou technikou a školeným personálem, který je připraven zasáhnout v jakékoli nouzové situaci. Kromě hašení požárů poskytuje technickou pomoc při nehodách a katastrofách, jako jsou například úniky nebezpečných látek nebo zřícení budov. Hasičský a záchranný sbor také spolupracuje s ostatními složkami NVKR a zajišťuje ochranu majetku a životního prostředí.

Policie

Policie zajišťuje veřejný pořádek a bezpečnost. Její hlavní úkoly zahrnují prevenci a potírání trestné činnosti, kontrolu dopravy a zajišťování bezpečnostních opatření při veřejných akcích. Policie je vybavena moderními technologiemi a má k dispozici specializované jednotky, jako jsou například kriminalisté, pořádková policie a dopravní policie. Spolupracuje s ostatními složkami NVKR a zajišťuje rychlou reakci na krizové situace.

Civilní ochrana

Civilní ochrana koordinuje záchranné operace při přírodních katastrofách, chemických, biologických, radiologických a jaderných hrozbách. Její úkolem je také poskytování informací a podpory obyvatelstvu během nouzových situací. Civilní ochrana se zaměřuje na přípravu a realizaci evakuačních plánů, školení obyvatelstva v oblasti první pomoci a bezpečnostních opatření a spolupracuje s médii na šíření důležitých informací během krizových situací. Organizace také udržuje pohotovostní zásoby a zajišťuje rychlou distribuci potřebných prostředků v případě nouze.

Vojenské složky

Vojenské složky mohou být povolány na podporu civilních záchranných operací při velkých katastrofách nebo mimořádných situacích. Armáda poskytuje logistickou podporu, specialisty a techniku, která je nezbytná pro řešení rozsáhlých krizových situací. Vojenské jednotky jsou připraveny zasáhnout v případě potřeby a jejich nasazení je koordinováno s ostatními složkami NVKR. Vojenské složky také zajišťují ochranu kritické infrastruktury a mohou poskytovat humanitární pomoc jak na národní, tak na mezinárodní úrovni.

3.2.5.2 Porovnání s Českou republikou

Porovnání systémů integrovaného záchranného systému v Maďarsku a České republice ukazuje na několik společných rysů, ale i významné rozdíly v jejich organizaci a fungování.

Oba systémy mají za úkol koordinovat různé složky záchranných a bezpečnostních sil, aby poskytovaly efektivní a rychlou pomoc v nouzových situacích. Mezi hlavní složky v obou zemích patří zdravotnická záchranná služba, hasičský a záchranný sbor, policie a civilní ochrana. V obou zemích je kladen důraz na spolupráci mezi těmito složkami, které jsou koordinovány prostřednictvím centrálního řídícího orgánu. V Maďarsku je to Katasztrófavédelmi Koordinációs Kormánybizottság (KKB), zatímco v České republice je to Integrovaný záchranný systém pod Ministerstvem vnitra.

V Maďarsku je NVKR koordinován prostřednictvím KKB, který je řízen ministrem vnitra a zahrnuje vysoké představitele různých ministerstev a národních organizací. Naproti tomu v České republice je IZS koordinován Ministerstvem vnitra a zahrnuje centrální koordinační centrum a krajská koordinační centra.

Koordinace v Maďarsku probíhá na národní, regionální a místní úrovni. KKB zajišťuje celostátní koordinaci, zatímco regionální operační pracovní tělesa operují na regionální úrovni a místní obranné výbory na úrovni místní. V České republice je koordinace také na národní a krajské úrovni.

Maďarský systém NVKR je řízen zákonem o prevenci katastrof, který určuje úkoly a odpovědnosti jednotlivých složek a koordinujícího orgánu. V České republice je právní rámec stanoven zákonem č. 239/2000 Sb., o integrovaném záchranném systému, který definuje fungování a strukturu IZS.

V Maďarsku mohou být vojenské složky povolány na podporu civilních záchranných operací při velkých katastrofách nebo mimořádných situacích. V České republice jsou vojenské složky zapojovány podobně, ale jejich použití je obvykle omezeno na specifické situace, kdy jsou vyžadovány specializované schopnosti nebo zdroje.

3.3 Definice mimo EU

3.3.1 Jižní Korea

Jihokorejský integrovaný záchranný systém, známý jako Korean Disaster and Safety Management System, je spravován Ministerstvem vnitra a bezpečnosti (MOIS). Tento systém zahrnuje různé záchranné a bezpečnostní složky, které spolupracují při řešení nouzových situací a katastrof, a je navržen tak, aby zajišťoval rychlou a efektivní reakci na různé typy hrozeb.

3.3.1.1 Organizační struktura

Ministerstvo vnitra a bezpečnosti (MOIS)

Ministerstvo vnitra a bezpečnosti (MOIS) prostřednictvím svého oddělení pro řízení katastrof a bezpečnosti (DSMD) dohlíží na koordinaci úkolů v oblasti katastrof a bezpečnosti, které vykonávají centrální a místní vlády. DSMD každých pět let sestavuje Národní základní plán bezpečnosti, který určuje celkový směr vládních bezpečnostních politik. Na základě tohoto plánu připravují příslušná ministerstva roční akční plány.

MOIS také zajišťuje průběžné vzdělávání a školení členů záchranných složek, pravidelně vyhodnocuje operační plány a na základě těchto vyhodnocení upravuje strategie pro zvýšení jejich efektivity. Mezi další úkoly patří analýza a revize rozpočtů na projekty související s katastrofami a bezpečností, zajišťování bezpečnostních standardů a pořádání veřejných bezpečnostních kampaní.

Národní hasičská agentura (National Fire Agency, NFA)

NFA je hlavní složkou pro prevenci požárů, hašení, záchranu a poskytování první pomoci. NFA řídí také Národní ústředí záchranné služby 119, které se specializuje na velké záchranné operace. Pod dohledem NFA fungují městská a provinční hasičská velitelství, která koordinují místní hasičské stanice a akademie. Tato struktura zajišťuje, že jsou hasičské služby dostupné a efektivně řízené na všech úrovních.

Zdravotnická záchranná služba

Zdravotnická záchranná služba zahrnuje rozsáhlou síť ambulancí a záchranářů, kteří jsou schopni rychle reagovat na zdravotní nouze. Tato služba je úzce integrována s dalšími složkami záchranného systému, aby byla zajištěna koordinovaná a efektivní reakce na různé incidenty. Zdravotnické týmy jsou vybaveny moderní technikou a školeným personálem, což umožňuje poskytování vysoké úrovně péče na místě.

Pobřežní stráž a námořní záchranná služba

Pobřežní stráž je klíčovou složkou při záchranných operacích na moři. Je zodpovědná za pátrání a záchranu, reakci na námořní nehody a ochranu pobřežních oblastí. Pobřežní stráž využívá specializované vybavení a technologie k efektivnímu provádění záchranných operací v námořním prostředí.

Central Disaster and Safety Countermeasures Headquarters

V případě rozsáhlé katastrofy je svolán Ústřední štáb pro řešení katastrof a bezpečnosti, který dohlíží na koordinaci reakce a obnovy. Tento štáb zahrnuje zástupce z různých organizací a slouží jako hlavní řídící centrum pro koordinaci veškerých záchranných a obnovovacích činností. Ústřední štáb spolupracuje s místními úřady a dalšími relevantními agenturami, aby zajistil rychlou a efektivní reakci na krizové situace.

3.3.1.2 Porovnání s Českou republikou

V Jižní Koreji je systém známý jako Korean Disaster and Safety Management System a je řízen Ministerstvem vnitra a bezpečnosti (MOIS). Tento systém zahrnuje různé složky, které spolupracují prostřednictvím Integrated Disaster and Safety Information System (IDSIS), který podporuje komunikaci a spolupráci mezi vládními agenturami na všech úrovních. V České republice je systém IZS a je koordinován Ministerstvem vnitra. Tento systém zahrnuje centrální koordinační centrum a krajská koordinační centra, která hrají klíčovou roli při regionální koordinaci.

Koordinace v Jižní Koreji probíhá na národní, regionální a místní úrovni, přičemž důležitou roli hraje Ústřední štáb pro řešení katastrof a bezpečnosti. Tento štáb je svoláván při rozsáhlých katastrofách a zahrnuje zástupce z různých organizací, kteří dohlížejí na reakci a obnovu. V České republice probíhá koordinace rovněž na národní a krajské úrovni.

Jihokorejský systém se vyznačuje rozsáhlým využíváním moderních technologií, jako jsou big data a umělá inteligence, pro zlepšení řízení rizik a reakce na katastrofy.

Český systém je zaměřen na širokou mezinárodní spolupráci v rámci EU a Visegrádské skupiny, a to především v oblasti společných cvičení a výměny informací.

Financování a výcvik jsou v obou zemích zajišťovány státními rozpočty, přičemž v Jižní Koreji jsou komerční podniky a dobrovolné organizace placeny za přímé výdaje související se záchrannými operacemi. V České republice jsou náklady na operace IZS hrazeny ze státního rozpočtu a dalšími zdroji financování.

4 Legislativa a regulace v oblasti PPDR

4.1 Legislativa a regulace pro Českou republiku

4.1.1 Závazek aukce

V březnu 2020 vyhlásil Český telekomunikační úřad (ČTÚ) aukci kmitočtů v pásmech 700 MHz a 3400–3600 MHz. Tato aukce měla za cíl podpořit rozvoj 5G sítí v České republice a zajistit poskytování specifických služeb pro veřejnou bezpečnost a krizovou komunikaci.

Aukce stanovila závazky pro komerční mobilní operátory, aby umožnili přístup k národním roamingovým službám a prioritním širokopásmovým službám pro PPDR. Účastníci aukce museli splnit podmínky pokrytí a kvality služeb, což je klíčové pro efektivní práci IZS.

Cílem aukce bylo vytvořit podmínky pro efektivní využití rádiových kmitočtů a podporu několika klíčových oblastí. Mezi hlavní cíle patřilo:

Podpora hospodářské soutěže v oblasti služeb elektronických komunikací.

Zajištění efektivního využití rádiových kmitočtů ve prospěch koncových uživatelů.

Rozvoj nových služeb elektronických komunikací prostřednictvím bezdrátových vysokorychlostních sítí.

Vytvoření podmínek pro technologickou inovaci sítí a služeb elektronických komunikací, zejména s ohledem na budoucí rozvoj sítí 5G a služeb na nich poskytovaných.

Dalším důležitým cílem bylo podpořit budoucí řešení komunikace pro veřejnou bezpečnost a krizovou komunikaci v souladu s usnesením vlády č. 293 ze dne 16. května 2018.

4.1.1.1 Podmínky

Účel závazků PPDR:

Zajištění mobilní krizové komunikace složek PPDR.

Komunikace prostřednictvím neveřejné mobilní sítě elektronických komunikací pro účely krizové komunikace.

Závazek Prioritního BB-PPDR:

Obsah závazku Prioritního BB-PPDR:

- Držitel přídělu musí poskytnout oprávněnému zájemci o PPDR přístup k síti provozované s využitím rádiových kmitočtů v pásmu 700 MHz.
- Přístup musí zahrnovat interoperabilitu s jádrem sítě BB-PPDR sítě oprávněného zájemce o PPDR a podporu řízení provozu oprávněným zájemcem o PPDR.
- Přístup může být rozšířen o sítě v pásmu 800 MHz za podmínky, že nebude omezena kompatibilita koncových zařízení oprávněného zájemce.

Rozsah služeb Prioritního BB-PPDR:

- Širokopásmové datové služby pro mobilní krizovou komunikaci a hlasové služby poskytované prostřednictvím širokopásmového připojení.
- Specifické služby zahrnují:
  - Služby „Push to Talk“ pro potřeby řešení krizových situací (Mission Critical Push to Talk – MCPTT)

- Přenos videa pro potřeby řešení krizových situací (Mission Critical Video – MCV)
- Přenos dat pro potřeby řešení krizových situací (Mission Critical Data – MCD)
- MCX (Mission Critical Common Functionalities) včetně zajištění eMBMS (evolved Multimedia Broadcast Multicast Services)
- IOPS (Isolated E-UTRAN Operation for Public Safety)
- QPP (QoS, priority, pre-emption, access-class barring) a eMPS (enhanced Multimedia Priority Service)
- LCS (Location Based Services)
- PWS (Public Warning System) využívající CBS (Cell Broadcast Service)
- Vyšší vysílací výkon HPUE (High Power User Equipment)
- Komunikace v přímém režimu ProSe (Proximity Services)

Prioritní provoz:

- Služby pro uživatele specifikované oprávněným zájemcem o PPDR musí mít vždy přednost před komerčními službami ostatních uživatelů.
- V případě různých úrovní priority musí být úroveň priority služeb stanovena v souladu se specifikací oprávněného zájemce.

Závazek Národního Roamingu pro PPDR:

- Obsah závazku Národního Roamingu pro PPDR:
  - Držitel přídělu musí poskytnout oprávněnému zájemci o PPDR přístup k veřejným komunikačním sítím v pásmu 700 MHz a 800 MHz.
  - Přístup musí být v rozsahu tzv. „Full-MVNO“ s architektonickým roamingovým modelem s S8 rozhraním, Home Routed Roaming definovaným dle technické specifikace 3GPP/ETSI.
- Rozsah a kvalita služeb:
  - Přístup k sítím musí být bez územních a kvalitativních omezení.
  - Rozsah, kvalita a skladba služeb poskytovaných oprávněnému zájemci o PPDR nesmí být horší než pro komerční uživatele na bázi technologií 4G a 5G.
- Podmínky platnosti:
  - Závazek národního roamingu pro PPDR se neuplatňuje po dobu, kdy držitel přídělu poskytuje Prioritní BB-PPDR.

4.1.1.2 Výsledky aukce

Výsledky aukce v kmitočtovém pásmu 700 MHz jsou následující:

Kmitočtový úsek	Velikost	Držitel	Platnost do
703–713 / 758–768 MHz	2×10 MHz	O2 Czech Republic a.s.	1,190 mld.
713–723 / 768–778 MHz	2×10 MHz	T-Mobile Czech Republic a.s.	1,400 mld.
723–733 / 778–788 MHz	2×10 MHz	Vodafone Czech Republic a.s.	1,400 mld.

4.1.2 Vyhrazení spektra

Český telekomunikační úřad (ČTÚ) vyhradil specifické kmitočty v několika pásmech pro účely PPDR (Public Protection and Disaster Relief). Tyto kmitočty mají zajistit kvalitní a spolehlivou komunikaci pro složky integrovaného záchranného systému, které jsou klíčové pro veřejnou bezpečnost a krizovou komunikaci.

Vyhrazené spektrum má následující charakteristiky:

Pásmo 700 MHz: Vyhrazeno především pro širokopásmové služby PPDR, které zahrnují datové a hlasové komunikace, přenosy videa a další specifické služby jako Mission Critical Push to Talk (MCPTT), Mission Critical Video (MCV), a Mission Critical Data (MCD). Toto pásmo je klíčové pro zavádění moderních 5G technologií, které umožňují vysokorychlostní přenosy dat a spolehlivou komunikaci i v krizových situacích.

Pásmo 800 MHz: Slouží jako doplněk pro zajištění širokopásmových služeb PPDR a podporuje interoperabilitu a rozšíření pokrytí v případě potřeby. Použití tohoto pásma zajišťuje robustní pokrytí a podporu pro hlasové i datové komunikace v celé zemi.

Pásmo 400 MHz: Poskytuje úzkopásmové služby pro hlasovou komunikaci a některé datové přenosy, využívané zejména v síti PEGAS, založené na technologii Tetrapol. Toto pásmo je klíčové pro stávající technologie a infrastrukturální řešení pro krizovou komunikaci. Umožňuje stabilní a spolehlivou hlasovou komunikaci mezi složkami IZS.

Pásmo 450 MHz: Může být využito pro širokopásmové PPDR služby, poskytující vysokorychlostní data a hlasové služby. Nabízí dostatečné pokrytí a je vhodné pro komunikaci na větší vzdálenosti, což je ideální pro použití v méně hustě osídlených oblastech. Toto pásmo je také zvažováno pro budoucí rozšíření PPDR služeb, které vyžadují vyšší kapacitu datových přenosů.

Jaký bude datový tok, závisí na počtu účastníků a minimální kapacitě nutné ke správě spojení. LTE za předpokladu bloku celých 5 MHz může dosáhnout rychlosti až 150/75 (upstream) Mbps podle ETSI peak performance 8.1.1 na sektor. Toto odpovídá 30 bps/Hz pro downlink a 15 bps/Hz pro uplink. Z toho odvozujeme, že se bude jednat o cca 10 komunikačních kanálů s kapacitou cca 6,5 MHz[8].

Pásmo 160 MHz: Tradičně používáno pro analogovou komunikaci složek IZS, zahrnuje zejména komunikaci Hasičského záchranného sboru a Policie České republiky. Toto pásmo je důležité pro základní hlasovou komunikaci v krizových situacích a poskytuje spolehlivou platformu pro okamžitou komunikaci.

Další pásma: Pro PPDR služby mohou být využívána i další frekvenční pásma, například v rozsahu 3,5 GHz pro specifické vysokorychlostní datové přenosy, které mohou podporovat rozšířené služby a aplikace v rámci IZS.

Povinnosti stanovené v aukci se primárně vztahují na kmitočty v pásmu 700 MHz. Ostatní služby a frekvence, jako jsou pásma 400 MHz, 450 MHz a 160 MHz jsou často využívány v rámci stávajících technologií a infrastrukturních řešení. Například síť PEGAS, založená na technologii Tetrapol, využívá pásmo 400 MHz pro svou činnost a poskytuje úzkopásmové hlasové a datové služby pro složky IZS.

4.1.2.1 Zdůvodnění požadavku na užití rádiového spektra

Ideální rozsah rádiového spektra k užití v pásmu 700 MHz – 2x13 MHz a 2x5 MHz rezerva

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

- Účel – plošná rádiová přístupová síť pro krizovou komunikaci.
- Řeší aktuální a budoucí kapacitní požadavky pro krizovou komunikaci, a to jak pro širokopásmové datové služby, tak i úzkopásmové hlasové služby.
- Globálně standardizované pásmo (band 28 3GPP).
- Velkým trh infrastruktury i koncových zařízení = úspory z rozsahu, zamezení vendor lock-in, mezinárodní harmonizace a interoperabilita, standardizovaná řešení, dlouhodobá perspektiva provozu a rozvoje.
- Jediný volný úsek vhodného rádiového spektra, který lze pro potřeby bezpečnostních a záchranných složek do roku 2030 využít – stát (ČTÚ) nedisponuje žádnou alternativou.

Option D–733-736 MHz (uplink) / 788-791 MHz (downlink) – 2 3 MHz

- Účel – specifické služby, scénáře a komunikační prostředky – služby pro blízkou komunikaci (tj. komunikace v přímém režimu), autonomní systémy (např. IoT), izolované systémy taktického nasazení, komunikace s leteckými prostředky atd.
- Umožňuje provoz výše uvedených specifických služeb a scénářů bez kapacitních dopadů na plošnou rádiovou přístupovou síť (Option A, 2x10 MHz) a eliminuje vzájemné rušení.
- Globálně standardizované pásmo (band 28 3GPP) ale s omezeními vyplývajícími z umístění v ochranném pásmu.

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

- Účel – rezerva do roku 2028 – využitelná až po vyřešení technických omezení (minoritní standardizované pásmo, band 68 3GPP).

Option B – kombinace Option C a Option D – 2x8 MHz

Odůvodnění užití rádiového spektra v rozsahu minimálně 2x10 MHz

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

Dnešní operační a taktické postupy využívané složkami jsou primárně závislé na hlasových službách. Zvýšení efektivity a bezpečnosti zasahujících složek lze dosáhnout tím způsobem, že pro svá rozhodování získají novou informační dimenzi. A toho lze dosáhnout pouze za předpokladu dostupnosti bezpečných vysokorychlostních datových služeb. Výhody dostupnosti těchto služeb jsou zřejmé – vytvoří podmínky pro nasazení a rozvoj široké škály aplikací pro podporu výkonu činností složek, tak jako se staly nepostradatelnou součástí běžného / civilního života. Jedná se zejména o poskytnutí detailních informací složkám zasahujícím v terénu (např. vizuální informace z místa zásahu před příjezdem; vyspělá navigace; využití biometrických prvků při kontrole, ztotožnění a evidenci osob) či předání detailních informací z místa zásahu vzdáleným řídicím složkám (např. přenos videa v reálném čase) které jsou klíčové pro zvyšování efektivity a bezpečnosti výkonu činností složek při zásahu.

Komunikační potřeby bezpečnostních a záchranných složek jsou v čase téměř konstantní. Potřebují v daném okamžiku předat či získat informaci potřebnou k rozhodování. Zatímco dnes jsou tyto informace verbálního charakteru, je patrná rostoucí poptávka po dalších informačních zdrojích souvisejících zejména s výměnou situačních informací, a to před / během / po zásahu, a také během rutinních denních aktivit příslušných složek. Jde zejména o rychlou dostupnost přesných informací bez zkreslení (zejm. ve formě videa a fotografie). Již dnes jsou např. PČR hojně využívány vysokorychlostní datové služby umožňující rychlé lustrace (mobilní bezpečná platforma PČR). Dalším způsobem získávání informací je masové zapojení chytrých koncových zařízení, sond a především aplikací, která potřebná data získávají a předávají odpovědným složkám již zpracované informační vstupy. Výhled do budoucna tak počítá s výrazným zapojením technologií pro sběr a vyhodnocení informací a jejich distribuci jednotlivým složkám.

Vyplývá z analyzovaných potřeb bezpečnostních a záchranných složek na mobilní komunikace (zejm. CEPT ECC Report 199 a další viz níže), kdy je stěžejní zavedení širokopásmových datových služeb.

- Minimální rozsah 2x10 MHz pokrývá zavedení širokopásmových datových služeb, nepokrývá stávající úzkopásmové hlasové služby a specifické scénáře (AGA, DMO, mobilní/autonomní/taktické systémy, m2m, IoT atd.)
  - Kalkulace pro migraci úzkopásmových hlasových služeb na systém BB-PDPR vede k požadavku na dodatečné rádiové spektrum v rozsahu 2x3,2 MHz
  - Pro další uvedené specifické scénáře v současnosti neexistuje standardizované řešení a jejich implementace se může výrazně lišit a lokalizace a rozsah rádiového spektra závisí na konkrétních uživatelských scénářích a požadavcích (DMO předpoklad jednotek MHz, AGA předpoklad desítek MHz, mobilní/autonomní/taktické systémy předpoklad vyšších jednotek až desítek MHz, m2m a IoT předpoklad jednotek MHz) – potřeba dalšího rádiového spektra (z tohoto důvodu požadavek Strategie na 2x18 MHz a spolupráce s operátory a další navržené mechanismy dynamického uvolňování rádiového spektra).
- Aproximace odhadů dle metodiky CEPT ECC Report 199 pro podmínky ČR je součástí vyhrazeného materiálu Strategie mobilních komunikací bezpečnostních a záchranných složek:
  - nové komunikační služby – kapitola 2.2 (27),
  - současné komunikační služby – 2.3 (31),
  - stav technologické standardizace – 2.4 (42),
  - rádiové spektrum vhodné pro PPDR – 2.5. (52),
  - potřebné kapacity pro různé činnosti a operace PPDR - 2.5.2.4 (57).
- Již nyní je tedy požadavek Strategie mobilních komunikací bezpečnostních a záchranných složek v oblasti rozsahu požadovaného rádiového spektra kompromisní – předpokládá využití 2x10 MHz jak pro zavedení širokopásmových datových služeb, tak i pro stávající úzkopásmové hlasové služby.

CEPT ECC Report 199 – stěžejní kalkulace pro modelové situace:

- Další materiály poskytují kalkulace obdobného ne-li většího rozsahu požadavků na rádiové spektrum dle národních potřeb.
- Scénáře:
  - PP1: silniční nehoda nebo silniční kontrola – běžná operační událost
    - špičkový provoz „generovaný“ jednou událostí pod scénářem PP1 (tj. 1 incident) odpovídá 1300/1300 Kbps:
    - klíčovými informacemi pro kalkulaci nutného rádiového spektra je tudíž popis operační události s využívanými komunikačními prostředky, velikost buňky, počet současných operačních událostí v rámci buňky, lokalizace události v rámci buňky, spektrální účinnost, linkový budget a další,
  - PP2: královská svatba (plánovaná událost velkého rozsahu) nebo nepokoje v Londýně 2011 (neplánovaná událost velkého rozsahu),
  - DR: scénář katastrofické situace (např. povodeň).

– Scénář PP1

  - 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

– Scénář PP2

  - Královská svatba – 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

  - Londýnské nepokoje – 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

– Scénář DR – odpovídá scénáři PP2, ale dochází k němu na větším území (více buňek).

Rozsah rádiového spektra musí tedy pokrývat širokou škálu operačních scénářů, kdy je z výše uvedeného zřejmé že ani rozsah rádiového spektra 2x10 MHz není v určitých situacích dostatečný a je nutné zajistit pro takové situace dodatečnou přenosovou kapacitu.

– Reference ke kapacitním požadavkům – STĚŽEJNÍ ČÁST ARGUMENTACE:

– CEPT ECC Report 199

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

– ETSI TR 102 628, zejm. kapitoly 8, A.5, F.4, F.5

– ITU-R Radiocommunication objectives and requirements for PPDR, zejm. Annex 7

– WIK PPDR Spectrum Harmonization in Germany, Europe and Globally

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

– Operations, and Spectrum Roadmap, zejm. kapitoly 1.3 a 3.8.3

– DRDC CSS 700 MHz Spectrum Requirements for Canadian Public Safety Interoperable Mobile Broadband Data Communications, zejm. kapitoly 5.1, 5.2.3 a conclusion

– APT, Report 38 on technical requirements for mission critical broadband PPDR communications, zejm. attachement 2 a example 2

– Andrew Seybold, Public Safety Broadband Real World Testing Results

– Strategie správy rádiového spektra (ČTÚ), zejm. kapitola 6.4.7

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

– Motorola, Barricaded suspect incident analysis

4.1.2.2 Proč ne jenom Option B (nespojitých 2x8 MHz)?

Důvody jsou součástí vyhrazeného materiálu Strategie mobilních komunikací bezpečnostních a záchranných složek, a to konkrétně kapitoly 2.5.2.3 resp. nevyhrazeného výtahu ze Strategie, a to konkrétně kapitoly 2.4.1.3, jde zejména o:

– **Nevhodnost k výstavbě celonárodní sítě** (funkční, kapacitní, finanční, provozní) což je dáno primárně využitím ochranných pásem s významnými regulačními omezeními s minoritním trhem zařízení a technologií umožňujících úspory z rozsahu a využití typizovaných produktů (COTS):
  – nedostatečná šířka pásma – nenaplnění uživatelských požadavků na kapacitu a přenosové rychlosti,
  – riziko „vendor lock-in“ (uzamčení zákazníka) - v oblasti terminálů i LTE/5G technologie,
  – negativní ekonomické dopady – vyšší ceny terminálů, technologií a vyšší provozní náklady spojené s provozováním upravené standardní technologie.

Pásma nejsou v současnosti samostatně (bez alokace v Option A) perspektivní, a to zejména kvůli mizivé velikosti komerčního trhu koncových zařízení – v současnosti žádná země takovouto alokaci pro účely běžné krizové a nekrizové komunikace nerealizovala (Francie pilotuje a plánuje pouze izolované taktické systémy):

– veškerá koncová zařízení by byla na objednávku (analogie s operátorem U:fon nebo s technologií TETRAPOL) – omezenost a nedostatečnost portfolia, vysoké ceny (odhad +30 % technologie, +30 % provozní náklady a +50-100 % terminály), riziko vendor lock-in, nejistota dlouhodobé udržitelnosti,

– jednotlivé země s touto alokací v současnosti zvažují, jak využít toto pásmo, resp. jak zajistit dostatečnou kapacitu – bude se vesměs jednat o doplňkové řešení pro realizaci taktických systémů, viz např. Francie, Německo.

Specifické (přísnější) evropské požadavky pro band 68 3GPP (pokrývající Option C) jsou stanoveny tak, aby nedošlo k rušení digitálního televizního vysílání (DTT). Zpřísnění způsobilo, že v současnosti není k dispozici potvrzení hlavních výrobců čipových sad, že budou tuto variantu vůbec vyvíjet.

– Option C je nouzové řešení uměle vyjmuté z ochranného pásma DTT. To přináší nezanedbatelné riziko opačného rušení, tj. rušení od vysílačů DTT, a tedy snížení spolehlivosti či kapacity komunikační sítě v blízkosti vysílačů DTT

4.1.2.3 Posouzení využitelnosti jednotlivých frekvenčních pásem pro implementaci systému BB-PPDR

Teoretické přenosové rychlosti pro pásma 400 a 700 MHz

Pásmo	Frekvence	Šířka pásma	Modulace DL	Modulace UL	MIMO	Přenosová rychlost DL	Přenosová rychlost UL
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

Možnosti realizace BB-PPDR

Využití sítí mobilních operátorů:

– pásmo 410-430 MHz,

– pásmo 450-470 MHz,

– komerční pásma vč. pásma 700 MHz.

Využití spektra v dalších pásmech 700 MHz mimo jeho hlavní část (guard band, SDL).

4.1.2.4 Využití sítí mobilních operátorů – pásmo 410-430 MHz

Není pod kontrolou státu, vlastníkem oprávnění je Nordic Telecom.

– Dle ČTÚ je nutná změna oprávnění pro poskytování služeb výhradně pro PPDR.

Možné jako služba v několika režimech:

– Vyhrazení části spektra na sdílené infrastruktuře.

– Vyhrazení kompletního spektra (nelze bez změny oprávnění).

– Sdílení kompletního spektra a infrastruktury s komerčním provozem.

Standardizace tohoto pásma pro technologii LTE/5G probíhá:

– Omezené množství dodavatelů části síťové technologie (jádro i rádiová přístupová síť vyžadující úpravy) – částečný vendor lock-in.

– Významně omezené portfolio koncových zařízení – jednotky výrobců, patrně zakázková výroba, vysoké ceny a částečný vendor lock-in.

– Problematické zajištění přeshraniční interoperability do doby standardizace a s ohledem na využívání pásma okolními státy.

– Kmitočtová koordinace – nutné bilaterální úmluvy.

– Ve standardizaci se v současnosti angažují zejména Maďarsko a Francie.

Max 2x4,25 MHz, reálně 2x3 MHz (vyhrazení části) což je kapacitně samostatně nedostatečné

– Užití 2x4,25 MHz není plně v souladu s 3GPP bloky (1.4, 3, 5, 10, 20)

– V případě využití 2x3 MHz umožní teoreticky rychlosti cca 15/7,5 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MiMo)

– V případě využití 2x4,25 MHz umožní teoreticky rychlosti cca 20/10 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MiMo)

Nesplňuje požadavky uživatelů, vlastníka ani provozovatele (nedostatečná kapacita, nestandard, riziko vendor lock-in, sdílení infrastruktury, vlastnictví, kontrola, bezpečnost, interoperabilita…).

4.1.2.5 Využití sítí mobilních operátorů – pásmo 450-470 MHz

Není pod kontrolou státu, vlastníkem oprávnění je O2:

– dle ČTÚ je nutná změna oprávnění pro poskytování služeb výhradně pro PPDR.

Možné patrně jen jako služba na klíč vč. jádra sítě bez sdílení s komerčním provozem (nelze bez změny oprávnění).

Příděl se částečně kryje se standardizovaným pásmem „band 31“ a plně s nově standardizovaným pásmem „band 72“:

– pro band 72 nadále probíhá standardizace síťové technologie,

– omezené množství dodavatelů části síťové technologie (jádro i rádiová přístupová síť vyžadující úpravy) pro oba bandy 31 i 72- částečný vendor lock-in,

– významně omezené portfolio koncových zařízení pro oba bandy – jednotky výrobců, patrně zakázková výroba a částečný vendor lock-in,

– ve srovnání s pásmem 410-430 MHz je situace v oblasti počtu dodavatelů lepší, ale zdaleka se nepřibližuje stávajícím komerčním pásmům nebo v budoucnu pásmu 700 MHz.

– problematické zajištění přeshraniční interoperability s ohledem na využívání pásma okolními státy,

– kmitočtová koordinace – nutné bilaterální úmluvy.

Max. 2x 4,4 MHz (v současnosti reálně 2x 3 MHz, pro využití 4,4 MHz nutnost refarmingu pásma ze strany O2) což je kapacitně samostatně nedostatečné:

– Užití 2x 4,4 MHz není plně v souladu s 3GPP bloky (1.4, 3, 5, 10, 20).

– V případě využití 2x 3 MHz umožní teoreticky rychlosti cca 15/7,5 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MiMo).

– V případě využití 2x 4,4 MHz umožní teoreticky rychlosti cca 20/10 Mbps (DL – 16QAM, UL – 16QAM, 2x2 MiMo).

S výjimkou alokace spektra ze základního pásma v 700 MHz se jedná o nejméně problematickou alternativu:

  – Strategie zvažovala využití této varianty na přechodné období pro co nejrychlejší zajištění širokopásmových datových služeb s vysokou mírou bezpečnosti a dostupnosti.

– V rámci zpracování Strategie to byla jedna z potenciálních možností vyhnutí se modernizaci systému PEGAS, což složky IZS (zejména HZS ČR) rázně odmítly a požadovaly zachování systému PEGAS min. do roku 2025, což v kontextu zdržení schválení Strategie a dostupnosti spektra v pásmu 700 MHz k 30.06.2020 vede k tomu, že tato varianta pozbyla v současnosti smysl, ale nelze ji vyloučit v souvislosti s otevřeným zadávacím řízením.

– Částečně splňuje požadavky uživatelů, vlastníka a provozovatele (nedostatečná kapacita, probíhající vývoj, riziko vendor lock-in, vlastnictví, kontrola, bezpečnost, interoperabilita…)

– O2 zájem o spolupráci s MV po dopracování Strategie ke konci roku 2017 stáhla, v roce 2018 jej znovu obnovila.

4.1.2.6 Využití sítí mobilních operátorů – hlavní komerční pásma

Stávající příděly ve vlastnictví T-Mobile, Vodafone a O2 - 800/900/1800/2100/2600/3700 MHz, v budoucnu pak 700 MHz.

Velké množství technických způsobů realizace výstavby, provozu a rozvoje – očekává se zpracování návrhu komerčních subjektů popisujících zejm. technické, provozní, komerční a právní aspekty v rámci realizace zadávacího řízení s návrhem řešení.

Kapacitně pravděpodobně nejlepší varianta – lze předpokládat přenosové rychlosti až v řádu stovek Mbps.

Varianta preferovaná ČTÚ a mobilními operátory je nicméně bez konkrétní specifikace technických způsobů řešení, kterých existuje velké množství:

- Závazky do budoucí aukce pásma 700 MHz jsou jedna z možností.
- Další možností je pak realizace otevřeného zadávacího řízení bez podmínek v aukci pásma 700 MHz.
- Samotný návrh je v přímém rozporu s usnesením řídícího výboru pro přípravu Strategie – nesplňuje požadavek na plnou kontrolu nad provozem a rozvojem infrastruktury, technologií a služeb – jedná se o eliminaci stále narůstajících bezpečnostních rizik (kybernetická bezpečnost, fyzická bezpečnost) a v souladu se strategií státu na snižování závislosti na komerčních subjektech.
    - Spolupráce s a využití sítí mobilních operátorů je nicméně nedílnou součástí Strategie pro zajištění služeb pro krizovou komunikaci, ale jde o doplňkový (pro zvýšení dostupnosti, kapacity) a ne hlavní komunikační prostředek.

Využití sítí komerčních operátorů přináší množství oblastí, které se musí promítnout do legislativy, regulace nebo závazků do aukce, např.:

- pokrytí území,
- specifické funkcionality,
- vysoká dostupnost,
- vysoká bezpečnost,
- kontrola nad komunikačními prostředky
- atd.

Model v současnosti nasazuje jediná země, a to Velké Británie, jsou indikována zpoždění a objevují se potřeby zásadních kompromisů zejména v oblasti funkčních požadavků (např. přímá komunikace) a zvýšení dostupnosti.

Další země (např. Finsko) po odprodeji pásma 700 MHz operátorům čelí obdobným výzvám, kdy nelze (bez legislativních a/nebo regulačních úprav včetně rozsáhlých závazků do aukce pásma 700 MHz) efektivně a na komerční bázi zajistit požadovanou úroveň služeb krizové komunikace splňující požadavky uživatelů, provozovatele a vlastníka.

Nesplňuje požadavky uživatelů, vlastníka a provozovatele (sdílení infrastruktury, vlastnictví, kontrola, bezpečnost, …).

Vyhrazení a využití těchto kmitočtů jsou nezbytné pro zajištění, že komunikace mezi složkami IZS bude spolehlivá, bezpečná a interoperabilní. To zahrnuje i závazky stanovené pro vítěze aukce, které zahrnují povinnost poskytovat národní roaming a prioritní širokopásmové služby pro PPDR.

4.1.2.7 Detaily kmitočtových pásem

Pásmo 700 MHz:

Primárně určeno pro širokopásmové služby PPDR.

Zahrnuje specifické služby jako MCPTT, MCV, MCD.

Klíčové pro zavádění 5G technologií.

Pásmo 800 MHz:

Slouží jako doplněk k pásmu 700 MHz.

Podporuje rozšíření pokrytí a interoperabilitu.

Pásmo 400 MHz:

Používáno pro úzkopásmové hlasové služby.

Využíváno v síti PEGAS založené na technologii Tetrapol.

Pásmo 450 MHz:

Podpora přidělování a využívání frekvencí 400/450 MHz Aliancí 450 MHz[9].

Vhodné pro širokopásmové datové a hlasové služby.

Nabízí dostatečné pokrytí pro méně hustě osídlené oblasti.

Pásmo 160 MHz:

Tradičně pro analogovou komunikaci IZS.

Poskytuje základní hlasovou komunikaci.

Další pásma:

Pásmo 3,5 GHz pro vysokorychlostní datové přenosy a rozšířené služby IZS.

4.2 Legislativa

Legislativa, která upravuje využití kmitočtů pro PPDR a obecně pro krizovou komunikaci, je klíčovým prvkem zajištění bezpečné a efektivní komunikace pro složky IZS. Následující právní předpisy a vyhlášky stanovují rámec pro využití rádiových kmitočtů, technické požadavky a podmínky pro interoperabilitu služeb

4.2.1 Právní předpisy v České republice

Vyhláška č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích): Tato vyhláška upravuje podmínky využívání rádiových kmitočtů a stanovuje pravidla pro poskytování služeb elektronických komunikací. Je zásadní pro určení podmínek, za kterých mohou mobilní operátoři a další subjekty poskytovat PPDR služby.

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon): Tento zákon stanovuje pravidla pro krizové řízení, včetně využití informačních systémů krizového řízení. Upravuje odpovědnosti orgánů krizového řízení a stanovuje, jakým způsobem mají být zajištěny komunikační prostředky pro krizové situace.

Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů: Tento zákon definuje složky integrovaného záchranného systému a jejich odpovědnosti. Stanovuje, jakým způsobem mají být zajištěny komunikační prostředky pro jednotlivé složky IZS, jako jsou Hasičský záchranný sbor, Policie České republiky a poskytovatelé zdravotnické záchranné služby.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury: Toto nařízení vlády definuje kritéria pro určení prvků kritické infrastruktury, které jsou zásadní pro zajištění bezpečnosti státu a jeho obyvatel. Stanovuje také požadavky na ochranu a bezpečnost těchto prvků, včetně komunikačních systémů.

4.2.2 Technické specifikace a standardy

Implementace PPDR služeb musí splňovat specifické technické požadavky a standardy, které zajišťují spolehlivost, bezpečnost a interoperabilitu komunikačních systémů.

Technické specifikace 3GPP/ETSI: Tyto specifikace definují požadavky na mobilní komunikační technologie, včetně širokopásmových služeb a interoperability mezi různými systémy a operátory. Jsou zásadní pro zajištění kvalitních a bezpečných komunikačních služeb pro PPDR. Konkrétní specifikace zahrnují:

3GPP TS 23.501: Definuje architekturu systémů 5G.

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

3GPP TS 23.401: Specifikace pro systémovou architekturu LTE a její rozšíření na podporu PPDR služeb.

Standardy pro interoperabilitu: Standardy jako jsou Mission Critical Push to Talk (MCPTT), Mission Critical Video (MCV) a Mission Critical Data (MCD) zajišťují, že různé komunikační systémy mohou efektivně spolupracovat při řešení krizových situací. Tyto standardy zahrnují:

MCPTT: Poskytuje spolehlivé a okamžité hlasové služby pro krizové situace.

MCV: Umožňuje přenos videa v reálném čase pro lepší povědomí o situaci.

MCD: Zajišťuje datové služby, které podporují různé aplikace a služby potřebné v krizových situacích.

4.2.3 Povinnosti stanovené v aukci kmitočtů

Podle dokumentů ČTÚ, závazky pro poskytování PPDR služeb byly stanoveny pro operátory, kteří získali kmitočty v pásmu 700 MHz. Tyto povinnosti zahrnují:

Národní roaming: Povinnost poskytovat národní roaming pro nové účastníky aukce, kteří nejsou stávajícími operátory.

Prioritní BB-PPDR: Poskytování prioritních širokopásmových služeb pro PPDR v pásmu 700 MHz. Toto zahrnuje interoperabilitu s jádrem sítě PPDR a podporu řízení provozu pro složky IZS.

4.2.4 Dokumenty evropské unie a mezinárodní úmluvy

Implementace PPDR služeb v České republice je také ovlivněna dokumenty Evropské unie a mezinárodními úmluvami, které stanovují rámec pro využívání rádiových kmitočtů a technických standardů:

EU Radio Spectrum Policy Programme (RSPP): Stanovuje cíle a opatření pro efektivní využívání rádiového spektra v EU.

ECC Decision (16)02: Doporučení pro harmonizaci frekvenčních pásem pro PPDR služby v Evropě.

4.3 Informace ze zahraničí

Evropská unie se zaměřila na harmonizaci spektra pro PPDR služby, přičemž klíčovým pásmem je 700 MHz. Tento krok má za cíl zajistit dostupnost spektra pro všechny členské státy a podporovat interoperabilitu mezi nimi. Harmonizované spektrum umožňuje nejen snadnější spolupráci při přeshraničních incidentech, ale také zajišťuje, že technologie a zařízení používané v různých zemích budou kompatibilní.

Mobilní operátoři, kteří získají příděly v pásmu 700 MHz, mají povinnost poskytovat služby PPDR. Tyto služby zahrnují prioritní přístup pro krizovou komunikaci, zajištění kvality služeb (QoS) a národní roaming. To znamená, že v případě nouze budou mít složky IZS přednostní přístup k síti, což je klíčové pro rychlou a efektivní komunikaci během krizových situací.

Přechod na širokopásmové technologie, jako jsou LTE a 5G, je jedním z hlavních cílů strategie. Tyto technologie nabízejí vyšší rychlosti a větší kapacitu než stávající systémy TETRA. V rámci standardů 3GPP jsou specifikovány funkce pro kritické komunikace, jako je Mission Critical Push-to-Talk, Mission Critical Data a Mission Critical Video. Tyto specifikace zajišťují, že nové technologie budou schopny podporovat všechny potřebné služby pro PPDR.

Klíčovým spektrem pro PPDR v EU je pásmo 700 MHz, kde je vyhrazeno 2x10 MHz pro širokopásmové služby PPDR. Některé země navíc využívají další bloky spektra v pásmu 700 MHz, například 2x5 MHz nebo 2x3 MHz (733–736 MHz (uplink) a 788–791 MHz (downlink)). Kromě toho jsou zvažována také pásma UHF, zejména 400 MHz (410-430 MHz a 450-470 MHz), která mohou poskytovat doplňkové služby PPDR, obzvláště v oblastech, kde spektrum 700 MHz nemusí být dostačující.

Mnoho zemí v EU plánuje postupnou migraci stávajících sítí TETRA na moderní širokopásmové sítě založené na LTE a 5G. Tento proces zahrnuje vypracování časového plánu migrace, realizaci pilotních projektů a testování nových technologií. Důležitým krokem je zajištění kontinuity služeb během přechodného období, aby nedošlo k narušení krizové komunikace.

Pilotní projekty a testování nových technologií jsou nezbytné pro ověření jejich schopnosti podporovat PPDR. Tyto projekty se zaměřují na testování pokrytí, kapacity a interoperability mezi různými systémy a zařízeními. Zajištění, že různé systémy mohou spolupracovat bez problémů, je klíčové pro efektivní krizovou komunikaci.

Jednou z hlavních výzev je zajištění dostatečného geografického pokrytí, zejména v odlehlých nebo těžko dostupných oblastech. Financování modernizace sítí a zajištění návratnosti investic představují další ekonomické výzvy, kterým čelí mnoho členských států.

Celkově je strategie 5G pro PPDR v EU zaměřena na modernizaci technologických platforem, zajištění interoperability a kvality služeb. Přestože existují výzvy, jako jsou financování a pokrytí, závazky jednotlivých členských států ukazují na silnou vůli k modernizaci krizových komunikací a zvýšení bezpečnosti a efektivity veřejné ochrany a reakce na mimořádné události.

4.3.1 Rakousko

Od roku 2006 zavádí regionální sítě TETRA, dokončení v roce 2019.

Síť TETRA je v soukromém vlastnictví, ale provozuje a spravuje ji rakouské ministerstvo vnitra.

Vyhrazené spektrum: 2 x 8 MHz v pásmu 700 MHz pro PPDR.

Plány na využití UHF (410-430 MHz, 450-470 MHz) zatím neexistují.

4.3.2 Belgie

Jedna z prvních celostátních sítí TETRA pro veřejnou bezpečnost, zřízena v roce 1998 (operátor ASTRID).

Spektrum 700 MHz (2 x 30 MHz) bude vydraženo s podmínkou podpory MCPTT.

Harmonizováno: 2 x 8 MHz v pásmu 700 MHz pro PPDR.

Možnost vyhrazení pásma 68 (2 x 5 MHz) pro ASTRID.

4.3.3 Bulharsko

Jedna z prvních sítí TETRA, vybudována na konci 90. let, v roce 2017 zásadní upgrade.

Plán uvolnění spektra pro 5G: 2x20 MHz v pásmech 700 MHz a 800 MHz.

Vyhrazené spektrum pro PPDR: dolní 2x5 MHz (pásmo 68 (698-703 MHz a 753-758 MHz)).

4.3.4 Dánsko

DBK vybudovala celostátní síť TETRA s 99,5 % pokrytím.

Motorola Solutions navrhla vyhrazení 2x10 MHz (713-723 / 768-778 MHz) pro PPDR.

Vláda vydraží 2x30 MHz a 20 MHz s požadavky na pokrytí.

4.3.5 Finsko

Provozována síť VIRVE TETRA, plán migrace na 3GPP širokopásmové řešení do roku 2025.

Aukce spektra 700 MHz v roce 2016.

Pásmo 700 MHz nevhodné pro PPDR kvůli blízkosti Ruska.

4.3.6 Francie

Síť Tetrapol bude vypnuta do roku 2024.

Aukce spektra 700 MHz v roce 2015, přidělení 2x8 MHz pro PPDR.

Pásmo 700 MHz nedostačující pro budoucí potřeby PPDR.

4.3.7 Německo

Největší síť TETRA (BDBOS), dokončena v roce 2016, pokrývá více než 99% území.

Síť TETRA bude funkční alespoň do roku 2030.

Zkoumání možností spektra v pásmu 400 MHz a 450 MHz.

4.3.8 Maďarsko

Národní síť TETRA spravovaná firmou Pro-M.

NMHH navrhuje 2 x 8 MHz v pásmu 400 MHz pro BB-PPDR.

Plány na využití 410-430 MHz a 450-470 MHz pro veřejnou bezpečnost.

4.3.9 Nizozemí

Rozhodnutí nahradit síť C2000 TETRA, nová smlouva na 8-10 let.

Aukce spektra 700 MHz pro 5G v roce 2020.

Zájem o ochranná pásma 700 MHz a duplexní mezeru.

4.3.10 Norsko

Celostátní síť TETRA dokončena v roce 2016, přidání TEDS na jednu třetinu základen.

Doporučení zpřístupnit spektrum 700 MHz pro komerční služby.

PPDR potřeby zajistí komerční operátoři.

4.3.11 Slovinsko

Celostátní síť TETRA, hledání hybridního řešení pro PPDR.

Spektrum 700 MHz s povinností nabídnout národní roaming pro bezpečné veřejné MVNO.

Vyhrazeno: 2x3 MHz a 2x5 MHz v pásmu 450-470 MHz.

4.3.12 Švédsko

Největší síť TETRA (RAKEL), žádné plány na vypnutí.

Návrh LTE kritické komunikace s 2 x 10 MHz FDD v pásmu 700 MHz.

Aukce 700 MHz v roce 2018, dva mobilní operátoři získali 2x20 MHz.

4.3.13 Švýcarsko

Aukce spektra pro 5G v roce 2019, pásmo 700 MHz pro komerční využití.

Zájem o ochranná pásma 700 MHz, pásmo 450-470 MHz přetížené.

4.3.14 Velká Británie

Síť TETRA pro tísňové služby zřízena v roce 1996, migrace na LTE.

Aukce spektra 700 MHz.

Možnost využití ochranných pásem 700 MHz nebo 450-470 MHz pro PPDR zatím není.

5 Krizové stavy a komunikace dle krizových stavů

5.1 Příklady komunikační prostředky vybraných složek IZS

PROSTŘEDEK	VEŘEJNÁ/NEVEŘEJNÁ	SLA
PEVNÁ SÍŤ	Veřejná / Neveřejná	Veřejná: kvalita služby daná smluvně dohodnutým scénářem. U hlasové služby SLA nejsou. Stejné, jako pro residenční zákazníky. Neveřejná: hlasové i datové služby řešeny individuálně nastavitelnou kvalitou.
MOBILNÍ SÍŤ	Veřejná	Není, kvalita služby stejná jako pro ostatní uživatele. Priorita volání, těžce vymožitelná, těžce přístupná.
TETRAPOL IP	Neveřejná	Hlasové i datové služby řešeny individuálně nastavitelnou kvalitou. Kvalitu si řeší MV samo.
DMR (160 MHZ)	Neveřejná	SLA řešená na úrovni technologických možnostech spektra, kde nelze garantovat nezarušitelnost služby.
JEDNOTNÝ SYSTÉM VAROVÁNÍ A VYROZUMĚNÍ	Neveřejná	Zabezpečená datová služba s individuálními SLA a pravidelnou kontrolou funkčnosti.
SPECIÁLNÍ PROPRIETÁRNÍ SYSTÉM	Neveřejná	SLA se zde mnohdy řeší, a to z důvodu malého dopadu na množství uživatelů.
SATELIT	Veřejná	Není, kvalita služby stejná jako pro ostatní uživatele. Priorita volání, těžce vymožitelná, těžce přístupná.
ANALOG RADIO (160 MHZ)	Neveřejná, s možností zachycení neoprávněnými osobami	SLA řešená na úrovni technologických možnostech spektra, kde nelze garantovat nezarušitelnost služby. Zde hrozí riziko odposlechu/narušení důvěrnosti.
TETRA (400 MHZ)	Neveřejná	Kvalitativní parametry jsou uvedeny ve všeobecných podmínkách pro koncové uživatele neveřejně dostupných sítí elektronických komunikací a nejsou ovlivněny jinými službami pro retailové koncové uživatele.

5.1.1 Základní rozčlenění typů sítí elektronických komunikací

Základem prvkem telekomunikačních sítí je tzv. **pasivní infrastruktura**, která je v zákoně o elektronických komunikacích č. 127/2005 Sb. v platném znění (ZoEK) definována jako **přiřazený prostředkem** přiřazené služby §2 čl.2 a) - (*spadají sem prostředky fyzické infrastruktury a jiná zařízení nebo prvky související se sítí elektronických komunikací nebo službou elektronických komunikací, které umožňují nebo podporují poskytování služeb prostřednictvím této sítě nebo služby nebo jsou toho schopny, a zahrnují budovy nebo vstupy do budov, kabelové rozvody v budovách, antény, věže a jiné podpůrné konstrukce, kabelovody, potrubí, stožáry, vstupní šachty a rozvodné skříně*.)

Pomocí pasivní infrastruktury a aktivních prvků jsou realizování **sítě elektronických komunikací** ZoEK §2 čl.2 b) - (*sítí elektronických komunikací přenosové systémy, bez ohledu na to, zda jsou založeny na trvalé infrastruktuře nebo jsou centralizovaně kapacitně řízené, nebo nikoli, a popřípadě i spojovací nebo směrovací zařízení a jiné prostředky, včetně neaktivních síťových prvků, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými*

prostředky, včetně družicových sítí, pevných sítí okruhově nebo paketově komutovaných včetně internetu, mobilních sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na typ přenášené informace)

Sítě elektronických komunikací se dále dělí na:

Veřejnou komunikační sítí síť elektronických komunikací §2 čl.2 d), která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání,

Neveřejné komunikační sítě (nejsou popsány v ZoEK) – jsou popsány v Národním plánu rozvoje sítí VHCN[10]

- **Neveřejné sítě kritické infrastruktury:** Kritická infrastruktura podléhá zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, který upravuje působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.
- **Neveřejné sítě veřejné správy:** Neveřejnou síť veřejné správy lze definovat jako datovou síť nové generace založenou zcela nebo zčásti na technologii využívající optické komunikační prvky a provozovanou orgánem veřejné moci (státními orgány nebo orgány územní samosprávy, popř. jimi pověřenými subjekty) pro potřeby výkonu veřejné správy a veřejných služeb. Do kategorie neveřejných sítí veřejné správy se zahrnují zejména krajské a obecní sítě. Síť není využívána domácnostmi ani soukromoprávními subjekty, s výjimkou organizací zakládaných nebo zřizovaných obcemi, kraji nebo státem. Síť nesmí být dále komerčně pronajímána a za její provoz nejsou uživatelům účtovány žádné úhrady.
- **Ostatní neveřejné sítě:** Ostatní neveřejné sítě zahrnují např. sítě podnikových areálů, které slouží k zabezpečení provozu výrobních a zpracovatelských linek. Tyto sítě zpravidla nepodléhají regulaci a ani sběru dat v rámci zeměpisného mapování.

Z pohledu kvalitativních parametrů a podmínek poskytování služeb na daných sítích:

Veřejně dostupná služby elektronických komunikací (případně neveřejná kom. služba), pokud je provozována na veřejné komunikační síti elektronických komunikací – minimální kvalitativní parametry jsou dány ZoEK a příslušnými vyhláškami a OOP vydávané ČTÚ – popis musí být uveden ve všeobecných podmínkách pro koncové uživatele veřejně dostupných sítí elektronických komunikací.

Neveřejná komunikační služba je poskytována na neveřejné komunikační síti – nemají předem definované minimální parametry. Kvalitativní parametry jsou uvedeny ve všeobecných podmínkách pro koncové uživatele neveřejně dostupných sítí elektronických komunikací.

Typy služeb elektronických komunikací:

- **hlasová** – interpersonální komunikační službu,
- **datová** – službu přístupu k internetu,
- **služby spočívající zcela nebo převážně v přenosu signálů**, například přenosové služby používané pro poskytování služby komunikace mezi stroji a pro rozhlasové a televizní vysílání,
- **radiokomunikační službou** je komunikační činnost, která spočívá v přenosu, vysílání nebo příjmu signálů prostřednictvím rádiových vln,
- **tísňovou komunikací komunikace** pomocí interpersonálních komunikačních služeb mezi koncovým uživatelem a centrem tísňové komunikace, jejímž cílem je požadovat a získat od tísňových služeb pomoc při mimořádných událostech.

Vliv tytu služby elektronických komunikací na proces výstavby a povolování.

V rámci realizace sítě bude nutno zohlednit i procesy výstavby.

	Lze využít pro **Veřejné sítě** elektronických komunikací	Lze využít pro **Neveřejné sítě** elektronických komunikací
Stavba dle Stavebního zákona 183/2006 Sb.		
§ 79 (Rozhodnutí o umístění stavby) • Antény do výšky 8 m (BTS) • Výměna vedení tech. Infrastruktury	**Ano**	**Ano**
§ 81 (Rozhodnutí o změně vlivu užívání stavby na území)	**Ano**	**Ano**

[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/

§ 103 (Stavby, terénní úpravy, zařízení a udržovací práce nevyžadující stavební povolení ani ohlášení), • odst. 1, písm. e) **bod 4** (ÚR o umístění stavby, Územní souhlas, VPS nahrazující ÚR), ZÚŘ • odst. 1 písm. e) **bod 10** (přípojky EK)	**Ano**	**Ano**
• **§ 104 až § 107 (Ohlášení)** výjimečně například pro centrální prvky sítě	**Ano**	**Ano**
§ 108 (Stavební řízení) • vše co není dle §103 až §107 • velmi výjimečně například pro Datová centra	**Ano**	**Ano**

Stavba dle zákona 416/2009 Sb. Liniový zákon – zákon o urychlení výstavby		
§2i, odst. 1) (tzv. přípojka do 100 m)	**Ano**	**NE*)**
§2i, odst. 3) a 4) (tzv. přípolože)	**Ano**	**NE*)**

**)§1 odst. 11 zákona 416/2009 Sb. Liniový zákon (Infrastrukturou elektronických komunikací se pro účely tohoto zákona rozumí stavba komunikačního vedení veřejné komunikační sítě jako technické infrastruktury elektronických komunikací a související komunikační zařízení, včetně jejich elektrických přípojek.)*

5.1.2 Pevná síť

Pevná síť se vztahuje k infrastruktuře, která poskytuje telekomunikační služby prostřednictvím pevně stanovených kabelových tras (například optických nebo měděných kabelů). Tato síť zajišťuje přístup k telefonním a datovým službám, jako je internet nebo televizní vysílání, prostřednictvím pevných spojů. Pevné sítě jsou stabilnější a méně náchylné k výpadkům způsobeným environmentálními faktory ve srovnání s bezdrátovými sítěmi.

5.1.2.1 Veřejná síť

Pevná síť (veřejná) je označována jako Public Switched Telephone Network (PSTN), což je globální síť veřejných telefonních sítí, které jsou propojené a orientované na hlasové služby. PSTN je tradiční telefonní síť založená na přepojování okruhů, která byla v provozu od konce 19. století. Tato síť zahrnuje všechny telefonní sítě na světě, které jsou provozovány lokálními, národními nebo mezinárodními operátory. Tyto sítě poskytují infrastrukturu a služby pro veřejnou telekomunikaci. Pevné linky, také známé jako PSTN, pevné telefonní služby nebo tradiční telefonní linky, používají podzemní měděné dráty pro spolehlivou komunikaci.

PSTN je kombinace telefonních sítí používaných po celém světě, zahrnující telefonní linky, optické kabely, přepínací centra, celulární sítě, satelity a kabelové systémy. Umožňuje uživatelům provádět pevné telefonní hovory mezi sebou.

5.1.2.2 Neveřejná síť

Soukromé telefonní systémy jsou nezávislé telefonní systémy, které jsou vlastněny nebo pronajímány společností nebo jednotlivcem. Tyto systémy zahrnují klíčové telefonní systémy (KTS), pobočkové ústředny (PBX), počítačovou telefonii (CT), bezdrátové PBX, telefonii na bázi lokálních sítí (LAN telephony) a multimediální komunikaci, například videokonference. Soukromé telefonní systémy se skládají především z telefonů (tzv. stanic nebo terminálů), místního kabelového propojení a přepínacích systémů. Telefonní stanice jsou rozhraním mezi uživatelem a telefonní sítí. Kabely propojují telefonní stanice s přepínacími systémy nebo distribučními body. Místní kabelové propojení v soukromých systémech může sahat od sdílených linek (klíčové systémy) až po individuální linky (digitální stanice). Přepínací systémy vzájemně propojují stanice nebo je připojují na vnější telefonní linky či vnitropodnikové propojení.

Neveřejná síť je určena pouze pro specifickou skupinu uživatelů a není přístupná široké veřejnosti. Tyto sítě často využívají speciální technologie a jsou provozovány pro interní potřeby organizací, jako jsou sítě pro krizovou komunikaci, podnikové sítě a sítě státních institucí. Sítě pro krizovou komunikaci jsou používány například složkami integrovaného záchranného systému pro zajištění bezpečné a spolehlivé komunikace v případě nouze. Podnikové sítě slouží pro interní komunikaci a přenos dat v rámci firem a institucí, zatímco sítě státních institucí jsou určeny pro komunikaci a správu mezi různými státními orgány. Neveřejné sítě mají často vyšší úroveň zabezpečení, omezený přístup a mohou být navrženy tak, aby splňovaly specifické požadavky na dostupnost a spolehlivost.

5.1.3 Mobilní síť

5.1.3.1 Mobilní bezpečná platforma

Mobilní bezpečná platforma (MBP) je inovativní systém vyvinutý především pro účely Policie České republiky. Tento systém umožňuje bezpečný přístup k interním databázím a informačním systémům přímo z mobilních zařízení, jako jsou chytré telefony a tablety. Hlavní funkcionalitou MBP je poskytování okamžitého přístupu k informacím o osobách, vozidlech a dalším relevantním datům, což zefektivňuje práci policistů v terénu a snižuje závislost na centrálních operačních střediscích.

Platforma byla navržena tak, aby zajistila vysokou úroveň bezpečnosti přenášených dat. Toho je dosaženo pomocí šifrování a použitím zabezpečených komunikačních kanálů, které chrání citlivé informace před neoprávněným přístupem. MBP podporuje různé typy mobilních zařízení a je integrována s širokou škálou aplikací, které zajišťují, že policisté mohou rychle a efektivně provádět lustrace, přistupovat k registrům a zadávat data přímo z místa události. Tato flexibilita a okamžitý přístup k datům přímo v terénu jsou klíčovými faktory, které přispívají k rychlejší a efektivnější reakci v krizových situacích.

MBP je využívána zejména pro lustrace a přístup k informačním systémům Policie ČR, jako jsou registr obyvatel, registr vozidel nebo systém pátrání po osobách a vozidlech. Díky tomuto systému mohou policisté na místě provádět okamžité ověřování totožnosti osob a vozidel, a tím zvyšovat efektivitu své práce. Systém je také navržen tak, aby umožňoval rychlé a bezpečné sdílení dat mezi jednotlivými hlídkami a operačními středisky, což přispívá k lepší koordinaci a řízení policejních operací v reálném čase.

SLA a zabezpečení těchto sítí je nastaveno na potřeby veřejně dostupné sítě elektronických komunikací. Fungování a parametry sítí jsou definovány zákonem o elektronických komunikacích č. 127/2005 Sb. v platném znění a návaznými vyhláškami.

5.1.3.2 Virtuální privátní síť

Virtuální privátní síť (VPN) je technologie, která umožňuje vytvoření bezpečného spojení přes veřejné nebo nezabezpečené sítě, jako je internet. VPN šifruje data přenášená mezi zařízením uživatele a cílovým serverem, čímž chrání komunikaci před neoprávněným přístupem. Toto šifrování je obzvláště důležité při používání veřejných Wi-Fi sítí, kde existuje zvýšené riziko odposlechu. Kromě toho VPN skrývá skutečnou IP adresu uživatele a nahrazuje ji IP adresou VPN serveru, čímž poskytuje anonymitu a ochranu soukromí.

VPN rovněž umožňuje přístup k obsahu, který je geograficky omezený, což znamená, že lze obcházet cenzuru nebo regionální blokace a získat přístup k webovým stránkám a službám, které by jinak nebyly dostupné v dané oblasti. Tato technologie je často využívána firmami pro zabezpečené připojení zaměstnanců k firemním sítím, což umožňuje bezpečný přístup k interním zdrojům a aplikacím odkudkoliv, čímž se zvyšuje flexibilita pracovníků na dálku.

Používání VPN zabraňuje poskytovatelům internetových služeb a dalším subjektům sledovat online aktivity uživatele, čímž zajišťuje, že vyhledávání, navštívené stránky a další internetové aktivity zůstávají soukromé. VPN vytváří šifrovaný „tunel“ mezi zařízením a VPN serverem, což zabezpečuje data a zabraňuje jejich snadnému zachycení nebo dešifrování.

5.1.4 DMR (160 MHz)

Digitální mobilní rádio (DMR) v pásmu 160 MHz je moderní komunikační technologie, kterou využívají některé záchranné služby a další profesionální organizace v České republice. Tento systém poskytuje spolehlivou a bezpečnou komunikaci, což je zajištěno hardwarovým šifrováním na úrovni terminálů. Použití šifrovacích algoritmů, jako je ARC4 nebo AES, garantuje vysokou úroveň ochrany dat před neoprávněným přístupem.

DMR technologie je zpětně kompatibilní s tradičními analogovými systémy, což usnadňuje přechod na novější technologie bez nutnosti okamžité výměny všech zařízení. Díky technologii časového multiplexu TDMA DMR efektivně využívá dostupné frekvenční kanály, což umožňuje současné vedení dvou nezávislých hovorů nebo přenos dat. To přináší vyšší efektivitu oproti tradičním analogovým systémům.

Kromě vysoké kvality hovoru a stabilního signálu nabízí DMR pokročilé funkce, jako jsou individuální a skupinové hovory, nouzové hovory, GPS sledování polohy a textové zprávy. Tyto funkce zvyšují flexibilitu a možnosti použití systému v různých situacích, včetně krizových. DMR systémy jsou navíc energeticky úspornější, což prodlužuje životnost baterií a snižuje provozní náklady, čímž se stávají ekonomicky výhodnými pro profesionální použití.

5.1.5 Jednotný systém varování a vyrozumění

Jednotný systém varování a vyrozumění je klíčovým nástrojem pro ochranu obyvatelstva před mimořádnými událostmi v České republice. Tento systém, budovaný od roku 1991, zahrnuje síť poplachových sirén a vyrozumívacích center, jejichž hlavním úkolem je včasné a efektivní varování obyvatel prostřednictvím akustických signálů a následných slovních informací o povaze hrozby. Varování obyvatelstva je zajišťováno obecními úřady, krajskými hasičskými záchrannými sbory a dalšími složkami, které k tomuto účelu provozují jednotný systém varování a vyrozumění.

Systém je tvořen koncovými prvky varování a přenosovou soustavou. Přenosová soustava zahrnuje samostatné radiové vysílače, které jsou rovnoměrně rozmístěné po kraji. Tyto vysílače zajišťují přenos a šíření radiového signálu, kterým jsou koncové prvky ovládány. Koncovými prvky varování jsou rotační sirény, elektronické sirény a dálkově ovládané obecní rozhlasy. Rotační sirény jsou umisťovány v obcích s více než 500 obyvateli nebo v oblastech ohrožených povodněmi. Elektronické sirény a obecní rozhlasy poskytují nejen akustické signály, ale také následnou verbální informaci o charakteru ohrožení.

Jednotný systém umožňuje z centrálního operačního střediska krajského hasičského záchranného sboru ovládat sirény jednotlivě nebo ve skupinách, případně spouštět všechny sirény najednou. Toto centrální ovládání je klíčové pro rychlou a koordinovanou reakci na krizové situace, což zvyšuje šanci na ochranu zdraví a životů obyvatel. Informace o umístění a druzích koncových prvků varování jsou dostupné na místních úřadech, které mohou poskytnout podrobnosti obyvatelům.

Jednotný systém varování a vyrozumění je tak nezbytným prvkem pro zajištění včasného varování a informování obyvatel v případě hrozby, což umožňuje efektivní zahájení opatření na ochranu jejich zdraví a bezpečnosti.

5.1.6 Speciální proprietární systém

Proprietární rádiové sítě jsou uzavřené komunikační systémy, které jsou navrženy a spravovány konkrétním výrobcem. Tyto sítě poskytují vysokou úroveň zabezpečení a kontroly, což je činí ideálními pro aplikace, kde je klíčové zajistit bezpečnou komunikaci, jako například v průmyslu nebo v bezpečnostních operacích.

Jednou z hlavních výhod těchto sítí je jejich schopnost být optimalizovány pro specifické potřeby dané aplikace. To zajišťuje, že jsou schopny poskytovat vysoký výkon a spolehlivost v náročných podmínkách, kde standardizované systémy nemusí vždy vyhovovat. Avšak jejich uzavřená povaha znamená, že nejsou kompatibilní s jinými technologiemi, což může vést k vyšším nákladům a omezené flexibilitě při potřebě rozšiřování nebo změn technologie.

V oblasti internetu věcí (IoT) a průmyslových aplikací jsou proprietární rádiové sítě často využívány pro své specifické vlastnosti, které zahrnují nízkou latenci a vysokou spolehlivost. Tyto sítě umožňují přenosy dat s požadovanou úrovní zabezpečení a rychlosti, což je zásadní pro monitorování a řízení průmyslových procesů.

Proprietární rádiové sítě tedy představují specializované řešení pro aplikace vyžadující bezpečnou a efektivní komunikaci, avšak za cenu omezené interoperability a závislosti na konkrétním výrobci.

5.1.7 Satelit

Satelitní komunikace využívá družice k přenosu signálů na velké vzdálenosti, čímž poskytuje globální pokrytí i v oblastech bez přístupu k tradičním komunikačním sítím. Tato technologie je klíčová pro zajištění spolehlivé komunikace v odlehlých a těžko dostupných oblastech, kde pozemní infrastruktura není dostupná nebo je nepraktická.

Jednou z hlavních výhod satelitní komunikace je její nezávislost na pozemní infrastruktuře, což umožňuje spolehlivé spojení bez ohledu na geografické nebo politické hranice. Satelitní systémy poskytují flexibilní a rychle nastavitelné komunikační řešení, což je zásadní při krizových situacích, jako jsou přírodní katastrofy, kdy je nutné rychle zajistit spojení.

Satelity podporují různé typy služeb, včetně hlasové komunikace, datových přenosů a internetového připojení, což z nich činí všestranný nástroj pro mnoho aplikací. Díky své odolnosti a spolehlivosti zajišťují nepřetržité spojení i v náročných podmínkách.

5.1.8 Analog Radio (160 MHz)

Analogový systém komunikace v pásmu 160 MHz, známý jako Analog Radio (AR), je používán Hasičským záchranným sborem jako sekundární komunikační systém. Na tento systém jsou napojeny i jednotky sborů dobrovolných hasičů, což umožňuje jeho

široké využití v rámci záchranných operací. Díky své univerzálnosti má tato technologie velmi nízkou úroveň zabezpečení, což znamená, že komunikace není chráněna před neoprávněným přístupem nebo odposlechem.

Analog Radio se využívá primárně pro hlasovou komunikaci a přenos kódů typických činností, jako jsou statusy jednotek. Tato technologie nepodporuje přenos dat, což omezuje její funkčnost na základní komunikační potřeby. V případě potřeby mohou být sítě PEGAS a Analog Radio propojeny pomocí jednokanálového převodníku instalovaného ve vozidle HZS na místě zásahu. Tento převodník umožňuje koordinovanou komunikaci mezi různými systémy.

Řízení zásahů prostřednictvím Analog Radio je zabezpečováno velitelem zásahu, který je vybaven dvěma samostatnými terminály nebo kombinací terminálu a analogové radiostanice. Dispečink má přístup k oběma sítím, což zajišťuje efektivní koordinaci a řízení záchranných operací. Ve vybraných složkách záchranné služby jsou také používána hybridní koncová zařízení, která umožňují komunikaci jak přes DMR, tak i Analog Radio, čímž rozšiřují možnosti komunikace v terénu.

5.1.9 TETRA (400 MHz)

Síť TETRA (Terrestrial Trunked Radio) v pásmu 400 MHz je moderní digitální radiokomunikační systém využívaný záchrannými službami v několika krajích České republiky. TETRA je privátní síť, která využívá hardwarové šifrování na úrovni terminálů, což zajišťuje vysokou úroveň zabezpečení komunikace. Tento systém byl vyvinut k tomu, aby poskytoval bezpečnou, spolehlivou a efektivní komunikaci mezi složkami integrovaného záchranného systému a dalšími bezpečnostními orgány.

Technologie TETRA podporuje jak hlasovou, tak omezenou datovou komunikaci. I když tato technologie nabízí základní datové služby, ve srovnání s moderními 5G sítěmi má omezené možnosti a nedokáže plně uspokojit budoucí potřeby složek IZS, které budou vyžadovat vyšší přenosové rychlosti a pokročilé datové služby. Systém TETRA je však stále klíčovým nástrojem pro krizovou komunikaci, díky své schopnosti zajistit nepřetržitou a stabilní komunikaci v náročných podmínkách.

Síť TETRA je tvořena řadou základnových stanic, které zajišťují pokrytí rozsáhlých území a umožňují mobilním jednotkám snadno přecházet mezi jednotlivými stanicemi podle kvality signálu, podobně jako u mobilních telefonů v sítích komerčních operátorů. Tento systém také podporuje skupinové hovory, které jsou nezbytné pro efektivní koordinaci záchranných operací. Využívání TETRA technologií umožňuje zajištění bezpečné komunikace i mimo dosah běžné infrastruktury, což je zásadní pro operace v terénu.

V ČR je v současné době v provozu 13 sítí na bázi technologie TETRA. První síť od roku 2002 (summit NATO) má hlavní město Praha, kde je registrováno více než 4000 radiostanic (městská policie cca 1500, dopravní podnik cca 2500, krizový štáb cca 100, technická správa komunikací cca 80). Dalšími sítěmi disponují letiště Praha – Ruzyně, vojenské letecké základny Kbely, Čáslav, Pardubice a Přerov, vojenské prostory Doupov a Libavá, městské radiové systémy jsou v Brně, Liberci a Českých Budějovicích a podnikové radiové systémy mají Hyundai Nošovice a Chemopetrol Litvínov.

5.1.10 PEGAS (TETRAPOL – 380 MHz)

PEGAS je privátní celoplošná komunikační síť ve standardu TETRAPOL, operující v pásmu 380 MHz. Tato síť má přibližně 230 základnových stanic a pokrývá 68 % území České republiky, což z ní činí hlavní komunikační prostředek pro složky IZS. PEGAS je využíván všemi základními složkami IZS, včetně Hasičského záchranného sboru, Policie ČR a Zdravotnické záchranné služby. Síť sdružuje regionální dispečerská pracoviště odpovídající jednotlivým krajům ČR.

Díky privátnímu charakteru sítě a hardwarovému šifrování na úrovni terminálů (End to End) je hlasová komunikace v síti PEGAS vysoce bezpečná. V současnosti probíhá technologický upgrade sítě, který zahrnuje přechod na IP technologii mezi radiovou a síťovou vrstvou (ústředny). Tento upgrade prodlouží životnost technologie. PEGAS je čistě hlasový komunikační systém a ani po upgradu nebude podporovat vysokorychlostní datové služby. Podpora pro stávající upgradované řešení je zasmluvněna do roku 2027. Po této době lze očekávat navýšení servisních nákladů kvůli životnosti IT prvků, jak je běžné na trhu.

5.1.10.1 Rozsah technologie Tetrapol

219 základnových stanic

25 opakovačů

43 radiových ústředen

digitální trasy a další technologie a software

1868 dispečerských pracovišť

16 269 ručních radiostanic

7 659 vozidlových radiostanic

1 191 vozidlových adapterů pro ruční radiostanice

390 aplikaci GPS

6 Technologické možnosti řešení

Technologické možnosti řešení mobilní komunikace pro bezpečnostní a záchranné složky v České republice jsou klíčové pro efektivní a rychlou reakci na krizové situace. S neustále rostoucími požadavky na rychlost a spolehlivost komunikace je nezbytné modernizovat současné technologie a systémy, aby lépe odpovídaly současným a budoucím potřebám. Současný stav využívaných technologií zahrnuje různé komunikační platformy, které jsou často omezené ve své funkčnosti a vzájemné interoperabilitě.

V rámci analýzy současného stavu byly identifikovány klíčové technologie a koncová zařízení, které jsou v současnosti využívány složkami IZS. Tato analýza odhalila řadu nedostatků a omezení, které je třeba řešit, jako například omezená podpora datových služeb, nedostatečné zabezpečení komunikace mimo proprietární sítě a omezený teritoriální dosah těchto sítí.

Na základě těchto zjištění byly navrženy možné postupy pro modernizaci a zlepšení komunikačních schopností složek IZS. Tyto postupy zohledňují technologické, ekonomické a bezpečnostní aspekty, aby bylo možné vybrat nejvhodnější řešení pro současné a budoucí potřeby IZS.

6.1 Současný stav využívaných technologií

V rámci analýzy současného stavu byly identifikovány následující technologie, které jsou v současnosti využívány základními složkami IZS:

PEGAS Tetrapol IP

- AGNET hlasová komunikace
- Datová komunikace – nízká rychlost

Satelitní datová komunikace

- Hlasová komunikace
- Datová komunikace

Jednotný systém varování a vyrozumění (JSVV)

- Technologie Pocsag, postupně digitální rádio
- Data – analogová komunikace

Služby na mobilních veřejných sítích – bez QoS

- MBP Policie
- GINA – hasiči
- POINTX – hasiči

Dočasné bezdrátové připojení

- Hlasová komunikace
- Datová komunikace

pTRACK

Data – Mash komunikace pátracích týmů

IoT čidla

Data – dohledy krizové komunikace (voda, ovzduší, radiace) - ve vývoji a testování

Rádiová síť pasivních přijímačů, přenos videa z vrtulníku, systém SOVA 2GHz, letová hladina 300m nad zemí

Videopřenos, jednodrát

Připravovaný projekt na rozšíření stanovišť a snížení letové výšky nad terénem na 150m

SCO – systém centralizované ochrany 400MHz

Datová konektivita pro ochranu objektů – potřeba záložní komunikace Policie, rušení od BS Tetrapol

Fixní připojení po pevné síti (metalické/optické/bezdrát)

Hlasová komunikace

Datová komunikace

Komunikace pro skryté použití

Hlasová komunikace

Řízení dopravy – k analýze

Datové řízení a ovlivnění řízení plynulosti dopravy dle potřeb složek IZS

Záloha do autonomně řízeného vozidla

Dispečerská pracoviště

Nebyla analyzována vazba na nové služby dispečerských pracovišť

Tato analýza bude pokračovat po stabilizaci potřeb složek IZS

Radio 160MHz

Hlasová komunikace – analogová

Hlasová a datová komunikace – DMR

TETRA

Hlasová a datová komunikace

Současný systém krizové komunikace je postaven především na hlasové komunikaci, zatímco datové služby jsou podporovány pouze v omezené míře. Tento stav omezuje efektivitu a flexibilitu krizové komunikace. Navíc, různé komunikační platformy nejsou vzájemně propojené, což znamená, že dispečink musí hrát podstatnou roli při koordinaci komunikace mezi složkami IZS.

Technologické možnosti a správa současných platforem jsou často neflexibilní a vybavenost uživatelských terminálů je nedostatečná. Mnohé z těchto technologií jsou zastaralé a neodpovídají moderním požadavkům. Proprietární sítě jako PEGAS a TETRA poskytují vysokou úroveň zabezpečení komunikace, zatímco ostatní platformy splňují bezpečnostní požadavky jen částečně nebo jsou pro budoucí potřeby krizové komunikace nedostačující.

Dalším problémem je omezený teritoriální dosah proprietárních sítí, což může být překážkou při rozsáhlých krizových situacích. Současné využívání datových služeb je ve složkách IZS pouze podpůrné, avšak jejich význam při krizové komunikaci a řízení je nezpochybnitelný. Modernizace a inovace při řízení zásahů jsou často omezovány nemožností využití vysokorychlostních datových přenosů, což představuje významnou překážku pro zvýšení efektivity a bezpečnosti těchto operací.

6.2 Možné postupy řešení

Existují čtyři možné postupy řešení pro zajištění a rozvoj mobilních komunikací bezpečnostních a záchranných složek:

6.2.1 Ponechat a rozvíjet Tetrapol IP

Koncem roku byl dokončen přechod na Tetrapol IP. Tento postup by umožnil pokračovat ve využívání a rozvoji stávající infrastruktury. Zachování této technologie by zajistilo kontinuitu a umožnilo další optimalizace systému, což by mohlo vést ke zvýšení efektivity a spolehlivosti komunikace.

6.2.2 Ponechat Tetrapol IT v současné konfiguraci a uzavřít dlouhodobou smlouvu s mobilními operátory

Tento postup zahrnuje paralelní využití současné konfigurace Tetrapol IT a dlouhodobou smlouvu na poskytování služeb s mobilními operátory bez SLA pro MVČR. Tento přístup by mohl nabídnout flexibilitu a nákladovou efektivitu tím, že využije existující infrastrukturu a zároveň využije komerční mobilní sítě pro podporu.

6.2.3 Implementovat BB PPDR/NR PPDR

Tento postup zahrnuje implementaci širokopásmové sítě pro krizovou komunikaci, avšak nese značná rizika, včetně finanční nákladnosti a nedostatečných podmínek SLA. Standardní mobilní technologie (3GPP) poskytují vysokou kapacitu, robustnost a bezpečnost, což by mohlo být klíčové pro úspěšnou implementaci širokopásmových sítí pro veřejnou ochranu a krizovou komunikaci.

6.2.4 Vybudovat vlastní síť po dohodě s Armádou

Tento postup zahrnuje vybudování vlastní sítě postavené na stávajících vysílačích Tetrapol a zasmluvnění překryvu s mobilními operátory. Symbiotická síť, která kombinuje komerční a vládní infrastrukturu, může nabídnout potřebnou flexibilitu a zajištění komunikace i v případě výpadků nebo zvýšených nároků na kapacitu. Tento přístup by umožnil sdílení zdrojů mezi vládními a komerčními sítěmi, což by zlepšilo celkovou odolnost a dostupnost služeb.

6.3 Síť propojující více technologií pro zajištění kritické komunikace

Jedním z moderních řešení pro zajištění efektivní a bezpečné krizové komunikace je implementace sítě, která kombinuje více technologií. Tento přístup využívá kombinaci komerčních mobilních sítí a dedikovaných vládních sítí k vytvoření flexibilního a robustního komunikačního systému, který dokáže vyhovět nárokům na krizovou komunikaci i v těch nejnáročnějších podmínkách.

6.3.1 Konfigurace sítě

Tato síť umožňuje vládní kritické síti interagovat s komerčními sítěmi, čímž obě strany získávají významné výhody. Tento přístup umožňuje komerčním sítím fungovat jako kapacitní zesilovač, zatímco vládní síť může sloužit jako záložní komunikační kanál. Architektura sítě zajišťuje, že v případě výpadků nebo zvýšené poptávky po kapacitě je komunikace stále spolehlivě udržována.

Hlavní komponenty sítě zahrnují statickou a dynamickou infrastrukturu. Statická infrastruktura zahrnuje dedikované geo-redundantní jádrové sítě, které poskytují celkovou kontrolu nad zařízeními a datovým provozem, a to včetně funkcí jako správa předplatitelů, řízení nabíjení a politik.

Dynamická infrastruktura obsahuje mobilní jednotky a dočasné základnové stanice, známé jako Cell-on-Wheels, které mohou být nasazeny pro zvýšení pokrytí a kapacity podle potřeby. Tyto jednotky mohou být rychle rozmístěny v oblastech, kde je to nutné, například při přírodních katastrofách nebo velkých krizových situacích.

6.3.2 Klíčové schopnosti

Síť nabízející více technologií poskytuje několik klíčových schopností, které jsou nezbytné pro efektivní krizovou komunikaci. Jednou z nich je podpora národního roamingu mezi vládními a komerčními sítěmi, což umožňuje rozšíření pokrytí a kapacity, což je zásadní pro zajištění nouzové komunikace v krizových situacích. Dále je to koncept Network Slicing, který umožňuje logické dělení sítě na více virtuálních částí, které mohou být využívány různými poskytovateli služeb. Každý „slice“ sítě může být nakonfigurován tak, aby splňoval specifické požadavky na šířku pásma, latenci a bezpečnost.

Další schopností této sítě je bezpečnost a ochrana dat. Zajišťuje separaci a šifrování citlivých informací, stejně jako prioritizaci nouzové komunikace.

6.3.3 Techniky pro podporu sítě

Pro podporu jak dedikovaných vládních sítí, tak sítí kombinujících více technologií jsou nutné některé techniky a standardy. Standardy 3GPP popisují různé scénáře roamingu, které umožňují propojení vládních a komerčních sítí. Tyto standardy zajišťují, že uživatelé mohou plynule přecházet mezi sítěmi, aniž by došlo k narušení služeb.

Virtuální a softwarově definované sítě umožňují flexibilní rozdělení zdrojů a dynamickou správu uživatelů. Součástí je možnost dynamicky měnit politiky pro směrování a autorizaci uživatelských relací, což zajišťuje vysokou míru flexibility a škálovatelnosti. Dnešní LTE a budoucí 5G sítě nabízejí širokou škálu kapacitních možností a spolehlivé geografické pokrytí. Tato technologie podporuje masivní počet připojených zařízení a splňuje vysoké požadavky na šířku pásma a spolehlivost pro krizové aplikace.

Proximity Services umožňuje zařízení v nouzových vozidlech přenášet síťové připojení do budov nebo oblastí se špatným pokrytím, což efektivně rozšiřuje dosah veřejné bezpečnostní sítě. Přesné určování polohy je využitelné pro lokalizaci mobilních volajících v nouzi, komunikačních zařízení záchranářů a specifických zdrojů nebo vybavení připojených k síti. Moderní technologie umožňují dosažení vysoké přesnosti při lokalizaci.

6.3.4 Implementace a výhody sítě

Implementace sítě zahrnuje několik kroků. Prvním je analýza specifických požadavků a nároků IZS na komunikaci. Následuje plánování a design, který zahrnuje vytvoření architektonického návrhu zahrnujícího statickou a dynamickou infrastrukturu. Dalším krokem je nasazení potřebného hardwaru a softwaru, včetně základnových stanic a mobilních jednotek. Proces končí testováním a optimalizací, které ověří funkčnost a optimalizují výkon sítě.

Výhody této sítě zahrnují zvýšenou kapacitu a pokrytí, což umožňuje lepší pokrytí v geograficky náročných oblastech a vyšší kapacitu během krizových situací. Flexibilita a škálovatelnost umožňují snadné přizpůsobení měnícím se potřebám a rychlé rozšíření kapacity. Ekonomická efektivita je dalším významným přínosem, protože využití existujících komerčních technologií a infrastruktury snižuje náklady na vývoj a údržbu.

Implementace této sítě pro IZS v České republice představuje krok vpřed směrem k moderní, robustní a efektivní krizové komunikaci, která je schopna reagovat na výzvy současného světa. Tento přístup nejenže zvyšuje efektivitu a spolehlivost komunikace, ale také přináší značné úspory a možnosti pro budoucí rozvoj a inovace v oblasti krizového řízení.

Příkladem realizace těchto služeb na úrovni generálního ředitelství HZS jsou projekty, které jsou součástí žádostí o dotace poskytované Ministerstvem pro místní rozvoj (MMR). Tyto projekty zahrnují implementaci sítě, která propojuje více technologií, aby zajistila efektivní krizovou komunikaci.

6.3.5 Projekt implementace video přenosů přes 5G sítě pro IZS

Projekt implementace video přenosů přes 5G sítě pro IZS má několik klíčových cílů, které jsou zásadní pro zlepšení krizové komunikace a zvýšení efektivity zásahů v nouzových situacích. Hlavním cílem projektu je umožnit složkám IZS rychleji a efektivněji reagovat na krizové situace. Díky reálnému přenosu videa z místa události do dispečinků a dalších koordinujících center mohou záchranáři získat aktuální a přesné informace v reálném čase. Tím se zvyšuje schopnost přijímat rychlá a informovaná rozhodnutí.

Efektivní koordinace mezi různými složkami IZS (hasiči, policie, záchranná služba) je nezbytná pro úspěšné zvládání krizových situací. Projekt si klade za cíl zlepšit komunikaci a spolupráci mezi těmito složkami prostřednictvím integrace pokročilých technologií. Přenos videa v reálném čase zajišťuje, že všechny složky mají přístup ke stejným informacím, což usnadňuje koordinaci a snižuje riziko nedorozumění. Dalším cílem projektu je zajistit vysoce kvalitní a stabilní přenos videa z místa události

do dispečinků. Technologie LiveU a 5G sítě poskytují vysokorychlostní přenosy dat s nízkou latencí. Použití více přenosových cest (WiFi, 4G, 5G) zajišťuje stabilitu přenosu i v náročných podmínkách.

Bezpečnost a ochrana dat jsou zásadní aspekty krizové komunikace. Projekt si klade za cíl zajistit, aby všechny přenosy videa byly šifrovány a zabezpečeny proti neoprávněnému přístupu. Technologie LiveU využívá vlastní patentovaný protokol LRT (LiveU Reliable Transport), který poskytuje vysokou úroveň zabezpečení a spolehlivosti přenosu. Dalším cílem projektu jsou flexibilita a škálovatelnost systému. Systém je navržen tak, aby mohl být snadno přizpůsoben měnícím se potřebám a rozšířen podle aktuálních požadavků. Modulární řešení a možnost rychlé změny konfigurace umožňují snadné nasazení technologie v různých situacích a prostředích.

Projekt podporuje různé scénáře využití, jako je telemedicína, vzdálená podpora operačních zákroků a urgentní příjem v nemocnicích. Přenos videa v reálném čase zlepšuje nejen krizovou komunikaci, ale také umožňuje rychlé a efektivní rozhodování v různých oblastech. Dalším cílem je zajistit plnou integraci projektu s existujícími systémy IZS. To zahrnuje kompatibilitu s různými typy zařízení a přenosových cest, což zajišťuje hladký přechod na nové technologie bez nutnosti rozsáhlých úprav stávající infrastruktury. Projekt také zahrnuje demonstrace a praktické testy technologie v reálných podmínkách. Tyto testy pomohou ověřit funkčnost a výkonnost systému, identifikovat případné problémy a optimalizovat technologie pro maximální efektivitu a spolehlivost.

6.3.6 Klíčové komponenty projektu

Projekt implementace video přenosů přes 5G sítě pro integrovaný záchranný systém zahrnuje několik komponent pro zajištění efektivní a spolehlivé krizové komunikace. Tyto komponenty zahrnují technologii LiveU, 5G sítě a mobilní kodéry LiveU, které společně umožňují přenos videa v reálném čase z místa události do dispečinků a dalších koordinujících center.

6.3.6.1 Technologie LiveU

LiveU je světovým lídrem v oblasti přenosu živého videa přes mobilní sítě. Tato technologie poskytuje zabezpečený přenos videa v profesionální kvalite. LiveU využívá kodek H.265 HEVC, který umožňuje přenosy v HD nebo 4K kvalitě s nastavitelným datovým tokem až 70 Mbit/s. Tento systém je modulární, což umožňuje rychlou a jednoduchou rekonfiguraci komponent dle potřeby. LiveU technologie byla ověřena v praxi včetně nasazení během válečných zón a přírodních katastrof, což dokazuje její spolehlivost a robustnost.

Na přiloženém obrázku je znázorněn systém přenosu videa z místa události do dispečinků IZS pomocí technologie LiveU. Tento systém zajišťuje efektivní krizovou komunikaci mezi složkami IZS, jako jsou hasiči, policie, záchranná služba a nemocnice.

Drony a PTZ kamery na strategických místech snímají video a přenášejí jej v reálném čase. Kamery na vozidlech záchranářů a osobní kamery (BodyCam) na uniformách záchranářů poskytují důležité záběry přímo z terénu. Mobilní kodér LiveU přenáší video signál z různých zdrojů do zabezpečené sítě pomocí WiFi, 4G a 5G. Patentovaný protokol LRT zajišťuje spolehlivý a zabezpečený přenos videa.

LiveU Decoder dekóduje video signál a umožňuje jeho zobrazení na monitorovacích zařízeních v dispečinku.

LiveU Ingest automaticky nahrává a ukládá přijaté video, zatímco Video Return umožňuje zpětné vysílání videa zpět na místo události pro lepší koordinaci.

Přenos videa umožňuje připravit se nemocnicím na urgentních příjmech na přijetí zraněných. Dispečink monitoruje a koordinuje zásahy složek IZS. Mobilní dispečink vybavený technologií LiveU přenáší video přímo z terénu. Video Management System spravuje a analyzuje přijatá videa a umožňuje jejich sdílení. Monitoring na tabletu nebo mobilním telefonu zvyšuje mobilitu a dostupnost informací pro záchranáře.

6.3.6.2 5G sítě

Využití 5G technologií je klíčovým prvkem projektu, protože umožňuje vysokorychlostní přenosy dat s nízkou latencí. 5G sítě poskytují široké geografické pokrytí a podporují masivní počet připojených zařízení. Technologie Network Slicing, která je součástí 5G, umožňuje logické dělení sítě na více virtuálních částí, které mohou být využívány různými poskytovateli služeb. Každý "slice" může být nakonfigurován tak, aby splňoval specifické požadavky na šířku pásma, latenci a bezpečnost.

6.3.6.3 Mobilní kodéry LiveU

Mobilní kodéry LiveU, známé také jako "batohy", umožňují přenos video signálu z terénu. Tyto kodéry podporují různé typy připojení, včetně LTE, 5G, WiFi a satelitního spojení. Jsou vybaveny dotykovými displeji a umožňují přenosy v různých kvalitách

a datových tocích, což zajišťuje vysokou flexibilitu a spolehlivost. Například jednotka LU600 je kompaktní, nativní 5G 4K HDR HEVC pole jednotka pro živé streamování s top výkonem v HEVC bonding unit. Nabízí maximální datový tok až 70 Mbp/s a přenos 1-4 video kanálů.

6.3.6.4 Reálný přenos videa

Díky využití technologií LiveU a 5G sítí je možné přenášet video z míst zásahů v reálném čase do dispečinků a dalších koordinujících center, což zlepšuje situaci na místě a umožňuje rychlejší a efektivnější rozhodování.

6.3.6.5 Zlepšení koordinace

Obraz a zvuk v reálném čase umožňují lepší koordinaci mezi různými složkami IZS, což vede k rychlejšímu a efektivnějšímu zásahu. Přenos videa v reálném čase zajišťuje, že všechny složky mají aktuální a přesné informace.

6.3.6.6 Bezpečnost a zabezpečení

Přenosy jsou šifrovány a zabezpečeny, což zajišťuje ochranu citlivých informací. Technologie LiveU využívá vlastní patentovaný protokol LRT pro přenos přes negarantované spojení s vysokou úrovní zabezpečení, kryptování AES-128, stabilitu i v náročných podmínkách, a dynamickou korekci chyb.

6.3.6.7 Flexibilita a škálovatelnost

Modulární řešení a možnost rychlé změny konfigurace umožňují snadné přizpůsobení měnícím se potřebám a rychlé rozšíření kapacity. Systém je navržen tak, aby byl snadno škálovatelný a přizpůsobitelný specifickým potřebám různých situací.

6.3.6.8 Široké využití

Projekt podporuje různé scénáře využití, včetně telemedicíny, vzdálené podpory operačních zákroků a urgentního příjmu v nemocnicích. Přenos videa v reálném čase zlepšuje nejen krizovou komunikaci, ale také umožňuje rychlé a efektivní rozhodování v různých oblastech.

Obrázek demonstruje výhody kombinace přenosových technologií pro zajištění kvalitního video přenosu.

V horní části obrázku je ukázán přenos dat využívající pouze LAN a WiFi. Kvalita videa je zjevně narušena a obraz je rozpadlý, což indikuje problémy s přenosovou kapacitou a stabilitou spojení.

Naopak v dolní části obrázku je zobrazen přenos dat využívající kombinaci LAN, WiFi a 5G s bonding technologií. Kvalita videa je zde výrazně lepší, obraz je čistý a stabilní.

Použití více technologií zajišťuje vyšší celkovou přenosovou kapacitu a stabilitu spojení, což je klíčové pro spolehlivý přenos videa i při výpadku některé z technologií.

7 Možnost dalšího rozvoje technologií

S rostoucími nároky na šířku pásma, rychlost přenosu dat a bezpečnost komunikace je nezbytné, aby se technologie používané těmito složkami neustále vyvíjely a modernizovaly. Pokrok v komunikačních technologiích umožňuje nejen rychlejší a spolehlivější komunikaci, ale také integraci pokročilých aplikací a datových služeb, které mohou výrazně zlepšit koordinaci a efektivitu záchranných operací.

Moderní krizové scénáře vyžadují komunikaci, která překračuje tradiční hlasové služby a zahrnuje přenos velkého objemu dat, jako jsou videozáznamy, senzorová data a real-time informace z terénu. Technologický pokrok, zejména v oblasti širokopásmových mobilních sítí, jako je LTE a nadcházející 5G, představuje obrovský potenciál pro zlepšení těchto schopností. Širokopásmové technologie poskytují vyšší kapacitu a rychlost přenosu dat, což umožňuje záchranářům přístup ke kritickým informacím v reálném čase a zlepšuje jejich schopnost rozhodovat se na základě aktuálních údajů.

Jedním z aspektů dalšího rozvoje je přechod na 5G technologie, které slibují výrazné zlepšení nejen v rychlosti a kapacitě sítí, ale také v jejich spolehlivosti a latenci. 5G technologie umožní nasazení nových aplikací, které mohou zahrnovat například vzdálenou lékařskou diagnostiku, autonomní drony pro průzkum nebezpečných oblastí nebo rozšířenou realitu pro lepší orientaci v terénu.

Bezpečnost komunikačních sítí je další oblastí, která musí být řešena v kontextu technologického rozvoje. S rostoucím množstvím přenášených dat a jejich citlivostí je nezbytné zajistit vysokou úroveň ochrany proti kybernetickým hrozbám a ztrátě dat. Moderní šifrovací technologie a bezpečnostní protokoly hrají klíčovou roli v ochraně komunikace a zachování integrity informací.

Další podstatnou oblastí je modernizace koncových zařízení, která využívají příslušníci bezpečnostních a záchranných složek. Nová zařízení musí být schopna nejen využívat pokročilé komunikační technologie, ale také být odolná vůči náročným podmínkám, ve kterých tito profesionálové často pracují. Podstatnými faktory jsou ergonomie, robustnost a dlouhá životnost baterií, které ovlivňují efektivitu a spolehlivost těchto zařízení.

Celkově lze říci, že technologický rozvoj v oblasti mobilní komunikace pro bezpečnostní a záchranné složky přináší mnoho výzev, ale zároveň otevírá nové možnosti pro zlepšení krizového řízení a záchranných operací. Integrace moderních technologií, jako jsou 5G sítě, pokročilé aplikace a bezpečnostní protokoly.

7.1 Přechod na 5G

7.1.1 Technologické Aspekty Přechodu na 5G

Vyšší rychlost a kapacita dat: 5G sítě poskytují mnohem vyšší rychlosti přenosu dat než 4G sítě, což umožňuje rychlejší přenos velkého objemu dat, jako jsou videozáznamy a senzorová data. Zlepšená kapacita je využitelná pro aplikace, které vyžadují okamžitou reakci a vysokou datovou propustnost, jako jsou drony, nositelná zařízení a pokročilé senzorové systémy.

Nízká latence: Latence je doba, kterou trvá, než data cestují z jednoho bodu do druhého. 5G technologie snižuje latenci na úroveň několika milisekund, což je zásadní pro aplikace, které vyžadují okamžitou reakci, jako je dálkové ovládání robotů a dronů nebo real-time video komunikace mezi záchranáři v terénu.

Spolehlivost a dostupnost: 5G sítě jsou navrženy tak, aby poskytovaly vysokou úroveň spolehlivosti a dostupnosti. To zahrnuje robustní infrastrukturu, která je schopna odolat různým druhům výpadků a krizových situací, jako jsou přírodní katastrofy nebo teroristické útoky. To je umožněno například použitím záložních systémů a dočasných míst pokrytí.

Podpora pokročilých aplikací: S přechodem na 5G technologie je možné nasadit nové typy aplikací, které by na starších sítích nebyly proveditelné. Mezi tyto aplikace patří vzdálená lékařská diagnostika, autonomní průzkum nebezpečných oblastí pomocí dronů, rozšířená realita pro lepší orientaci v terénu a mnoho dalších.

Energetická efektivita: 5G technologie je navržena s důrazem na energetickou efektivitu, což znamená nižší spotřebu energie pro přenos dat ve srovnání s předchozími generacemi mobilních sítí. To je zvláště důležité pro nasazení v odlehlých oblastech a pro zařízení s omezenou kapacitou baterií.

Flexibilní architektura sítě: 5G sítě jsou založeny na flexibilní architektuře, která umožňuje dynamické přidělování zdrojů podle aktuálních potřeb. To znamená, že síť může být optimalizována pro různé typy služeb, jako jsou hlasové hovory, video přenosy a data z IoT zařízení.

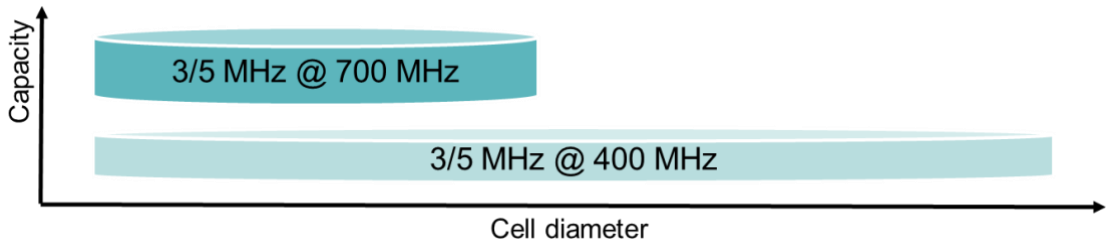
Edge computing: Integrace edge computingu s 5G sítěmi umožňuje zpracování dat blíže k místu jejich vzniku, což výrazně snižuje latenci a zvyšuje rychlost reakce na krizové situace.

***Pokročilé mobilní vysokorychlostní sítě**: Mobilní širokopásmové připojení se zaměřuje na uživatelské případy orientované na člověka pro přístup k multimediálnímu obsahu, službám a datům. Poptávka po mobilním širokopásmovém připojení bude nadále růst, což povede k pokročilým mobilním vysokorychlostním sítím. Tento scénář použití přinese nové oblasti aplikací a požadavky vedle stávajících aplikací mobilního širokopásmového připojení pro zlepšení výkonu a stále plynulejší uživatelskou zkušenost. Tento scénář použití zahrnuje řadu případů, včetně širokopásmového pokrytí a hotspotů, které mají různé požadavky. Pro případ oblastí s vysokou hustotou uživatelů, je potřeba velmi vysoká kapacita přenosu, zatímco požadavek na mobilitu je nízký a uživatelská rychlost přenosu je vyšší než u širokopásmového pokrytí. Pro případ širokopásmového pokrytí je žádoucí plynulé pokrytí a střední až vysoká mobilita, s mnohem zlepšenou uživatelskou rychlostí přenosu ve srovnání se stávajícími rychlostmi přenosu dat. Nicméně požadavek na rychlost přenosu může být uvolněn ve srovnání s hustotou uživatel.*

***Vysoce spolehlivá komunikace s nízkou latencí**: Tento případ použití má přísné požadavky na schopnosti, jako jsou propustnost, latence a dostupnost. Některé příklady zahrnují bezdrátové řízení průmyslové výroby nebo výrobních procesů, dálkové lékařské operace, automatizaci distribuce v chytré síti, bezpečnost dopravy atd.*

***Masivní komunikace mezi stroji/zařízeními**: Tento případ použití je charakterizován velmi velkým počtem připojených zařízení, která obvykle přenášejí relativně nízký objem dat, která nejsou citlivá na zpoždění. Zařízení musí být nízkonákladová a mít velmi dlouhou životnost baterie.*

7.1.2 Vliv radiového spektra na počet základnových stanic pro stejné pokrytí území



Vyhrazená síť v ochranných pásmech 700 MHz

Průměr buňky kolem 15 km

Šířka pásma 3 resp. 5 MHz (B28 resp. B68)

Garantovaná maximální rychlost internetu až 35 Mbit/s

1300-1700 eNB pro pokrytí 95 % území

Bezchybná přeshraniční spolupráce

Standardní terminály spolupracující s Tetrapolem

BBPPDR 400 MHz – vyhrazená síť

Průměr buňky až 35 km

Šířka pásma nyní 3, výhledově 5 MHz

Garantovaná maximální rychlost internetu až 35 Mbit/s

850-1100 eNB pro pokrytí 95 % území

Neexistující spolupráce na hranicích – nutné řešit speciálním pokrytím a směrováním

Standardní terminály spolupracující s Tetrapolem

7.1.2.1 Maximální vyzářený výkon

Srovnání provedeno v kontextu zkušeností se stávající technologií v pásmu 380MHz se službami v pásmech 410MHz a 450 MHz.

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

Pro pásma 380MHz, kde je provozován systém TETRAPOL je maximální vyzářený výkon koncových zařízení 10W.

Zdroj: ČTÚ – VO-R/1/12.2018-8 platné ke dni 18.12.2018

U systému TETRA a úzkopásmové technologie v pásmu 410MHz platí obdobné parametry jako u technologie TETRAPOL uvedené na obrázku níže.

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.

Zdroj: ČTÚ - VO-R/1/12.2018-8 platné ke dni 18.12.2018

Pro pásma postavené na standardu LTE 410MHz a 450 MHz platí maximální možný vyzářený výkon koncových zařízení 2W (při kanálu menším než 200kHz, jinak pouze 1W).

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.

Zdroj: ČTÚ - VO-R/1/12.2018-8 platné ke dni 18.12.2018

7.1.3 Standardy

Standardizace je klíčovým prvkem pro zajištění kompatibility a interoperability mezi různými zařízeními a systémy. Standardizace umožňuje různým organizacím a zemím efektivně spolupracovat a sdílet zdroje v krizových situacích. Organizace, jako je 3GPP (Third Generation Partnership Project), hrají zásadní roli ve vývoji a implementaci těchto standardů.

7.1.3.1 3GPP standardy pro PPDR

3GPP vyvíjí standardy pro mobilní komunikace, které zahrnují specifikace pro veřejnou bezpečnost a kritickou komunikaci. Verze 13 a novější zahrnují funkce specificky navržené pro PPDR. Rel.13 3GPP také přináší nové funkce pro 5G RAN, jako jsou nové typy antén, nové pásmo mmWave a nové metody přístupu k rádiovému spektru.

Nejčastěji aplikované MC (Mission Critical) služby se vztahují na[11]:

Mission Critical related items

Mission Critical Improvements general aspects

- Re-organizing the MCPTT Stage 1 documents
- Re-organizing the MCPTT Stage 2 documents
- MCPTT documents 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 Podpora standardů v 5G sítích

5G technologie zahrnují pokročilé funkce a standardy, které podporují potřeby PPDR. Patří sem:

QoS (Quality of Service): Zajištění, že hlasové, datové a video služby mají prioritu a jsou poskytovány s vysokou úrovní spolehlivosti a nízkou latencí.

Proximity Services (ProSe): Umožňuje přímou komunikaci mezi zařízeními bez nutnosti využití síťové infrastruktury, což je užitečné v situacích, kdy je síť nedostupná nebo přetížená.

Isolated Operation for Public Safety (IOPS): Umožňuje síťovým uzlům operovat nezávisle v případě, že dojde k odpojení od hlavní sítě, čímž se zajišťuje kontinuita služeb i v krizových podmínkách.

Standardizace také umožňuje mezinárodní spolupráci a interoperabilitu mezi různými zeměmi. Projekty jako je Evropská iniciativa Broadway, která se zaměřuje na vytvoření „borderless“ širokopásmové kritické komunikace, jsou příkladem toho, jak standardizace podporuje koordinaci a sdílení zdrojů na mezinárodní úrovni.

Při zavádění nových standardů je důležité zajistit zpětnou kompatibilitu s existujícími systémy, aby byl přechod na nové technologie hladký a aby byla zachována kontinuita služeb. To zahrnuje interoperabilitu s již zavedenými systémy, jako jsou TETRA a P25, které jsou široce používány v současných PPDR systémech.

7.1.4 Aplikace

Rozšířená realita (AR) umožňuje záchranářům a bezpečnostním složkám lépe se orientovat v terénu tím, že poskytuje důležité informace v reálném čase přímo do jejich zorného pole. AR aplikace mohou zobrazovat navigační pokyny, identifikovat nebezpečí, ukazovat plány budov a poskytovat instrukce pro první pomoc, čímž se zvyšuje povědomí o situaci a efektivita záchranných operací. Autonomní drony hrají klíčovou roli při průzkumu nebezpečných oblastí, kde by bylo nasazení lidského personálu příliš rizikové. Drony vybavené kamerami a senzory mohou poskytovat živé videozáznamy a senzorová data, která pomáhají při rozhodování a koordinaci záchranných operací. Navíc mohou drony doručovat léky, zdravotnické vybavení nebo jiné potřebné zásoby do těžko přístupných oblastí.

5G technologie umožňují provádět dálkovou lékařskou diagnostiku v reálném čase, což je možno využít pro poskytování rychlé a efektivní lékařské péče v krizových situacích. Zdravotničtí pracovníci mohou prostřednictvím videokonferencí a přenosu dat v reálném čase konzultovat s odborníky na dálku, diagnostikovat pacienty a poskytovat pokyny pro první pomoc. Tato technologie může výrazně zlepšit výsledky léčby a zachránit životy. Nositelné technologie, jako jsou chytré hodinky a zdravotnické senzory, mohou monitorovat zdravotní stav záchranářů a poskytovat údaje o jejich fyziologických parametrech v reálném čase. Tato data mohou být analyzována pro detekci únavy, stresu nebo jiných zdravotních rizik.

Inteligentní senzory a IoT zařízení mohou monitorovat prostředí a poskytovat důležitá data, jako jsou teplota, vlhkost, přítomnost nebezpečných látek a další. Tato data mohou být v reálném čase přenášena do řídících center, kde jsou analyzována pro lepší rozhodování a koordinaci záchranných operací. IoT technologie také umožňují sledování a řízení zdrojů, jako jsou vozidla a vybavení, což zlepšuje logistiku a efektivitu operací. Pokročilé komunikační platformy založené na 5G technologiích poskytují integrované hlasové, datové a video služby, které umožňují efektivní komunikaci mezi všemi účastníky záchranných operací. Tyto platformy podporují funkce jako je skupinová komunikace, prioritizace hovorů a zabezpečený přenos dat.

7.1.5 Datové služby

5G technologie přináší revoluci v oblasti datových služeb. Díky vysoké rychlosti a kapacitě 5G sítí mohou záchranáři a bezpečnostní složky přenášet a přijímat obrovské množství dat v reálném čase. To zahrnuje živé videozáznamy, fotografie, mapy, dokumenty a další důležité informace.

Jedním z hlavních přínosů 5G datových služeb je možnost real-time analýzy dat. To umožňuje bezpečnostním a záchranným složkám okamžitě vyhodnocovat situace a reagovat na ně s přesnými informacemi. Senzory a IoT zařízení umístěné v terénu mohou shromažďovat data o prostředí, jako jsou teplota, vlhkost, kvalita vzduchu a přítomnost nebezpečných látek. Tato data jsou pak přenášena do řídících center, kde jsou analyzována a použita k optimalizaci zásahových operací.

Dalším významným aspektem 5G datových služeb je podpora velkého množství zařízení připojených současně k síti. To je praktické pro nasazení rozsáhlých sítí senzorů a dalších IoT zařízení, které monitorují a reportují situaci v reálném čase. Tato schopnost umožňuje vytvoření komplexního a detailního obrazu o situaci.

5G technologie také zajišťují vysokou úroveň zabezpečení dat. Moderní šifrovací metody a bezpečnostní protokoly chrání citlivé informace před kybernetickými útoky a neoprávněným přístupem a slouží také na ochranu osobních údajů a citlivých informací, které jsou často součástí komunikace mezi bezpečnostními a záchrannými složkami.

Další významnou funkcí 5G datových služeb je možnost prioritizace provozu. To znamená, že během krizových situací mohou být data záchranářů a bezpečnostních složek přednostně přenášena, což zajišťuje, že kritické informace budou doručeny bez prodlení.

7.1.6 Koncová zařízení

Nová generace koncových zařízení pro PPDR zahrnuje pokročilé komunikační technologie, které podporují hlasové, datové a video služby na 5G sítích. Tato zařízení musí být schopna zvládnout vysoké rychlosti přenosu dat a nízkou latenci, které 5G nabízí.

Patří sem například chytré telefony, tablety a nositelné technologie, které jsou optimalizované pro náročné podmínky krizového řízení.

7.1.6.1 Robustnost a odolnost

Koncová zařízení používaná v PPDR musí být navržena tak, aby odolávala extrémním podmínkám, ve kterých záchranáři často pracují. To zahrnuje odolnost vůči vodě, prachu, nárazům a extrémním teplotám. Zařízení musí být také ergonomická, aby je bylo možné pohodlně používat po dlouhé hodiny, a musí mít dlouhou životnost baterie, aby zůstala funkční během dlouhých operací bez nutnosti častého nabíjení.

7.1.6.2 Bezpečnostní prvky

Bezpečnost je také relevantním prvkem koncových zařízení. Musí být vybavena pokročilými šifrovacími technologiemi a bezpečnostními protokoly, které chrání komunikaci před kybernetickými hrozbami. Kromě toho by měla mít zařízení víceúrovňové autentizační mechanismy, jako je biometrické ověřování a vícefaktorová autentizace, aby se zajistilo, že přístup k zařízení a přenášeným datům mají pouze oprávněné osoby.

7.1.6.3 Interoperabilita a kompatibilita

Koncová zařízení musí být interoperabilní s různými systémy a technologiemi používanými v PPDR. To zahrnuje kompatibilitu s různými komunikačními protokoly, jako jsou MCPTT, MCData a MCVideo, které jsou standardizovány v rámci 3GPP. Interoperabilita zajišťuje, že zařízení mohou efektivně komunikovat s různými systémy a zařízeními.

7.1.6.4 Integrace s IoT a senzory

Moderní koncová zařízení by měla být schopna integrovat se s různými IoT zařízeními a senzory, které poskytují data v reálném čase. To zahrnuje senzory pro monitorování prostředí, zdravotnické senzory a další IoT zařízení, která mohou zlepšit povědomí o situaci a efektivitu operací. Zařízení by měla být schopna shromažďovat, analyzovat a vizualizovat data z těchto senzorů.

7.2 Integrace a interoperabilita

7.2.1 Možnosti integrace stávajících a nových systémů

Integrace stávajících systémů s novými 5G technologiemi představuje jednu z největších výzev při modernizaci komunikačních systémů pro bezpečnostní a záchranné složky. Cílem je zajistit hladký přechod, který minimalizuje výpadky služeb a zároveň maximalizuje výhody nových technologií. Tento proces vyžaduje důkladné plánování a pečlivé provedení, aby byla zajištěna kontinuita provozu a využití nových funkcionalit.

Pro zajištění bezproblémové integrace je nutné, aby nová 5G zařízení byla kompatibilní s existujícími komunikačními systémy. To zahrnuje jak hardware, tak software, což umožňuje koexistenci starších a novějších technologií během přechodného období. Moderní komunikační zařízení musí být schopna fungovat v hybridním režimu, kde mohou komunikovat jak přes stávající sítě, tak přes nové 5G sítě. Tento přístup zajišťuje, že bezpečnostní a záchranné složky mohou postupně přecházet na nové technologie bez narušení jejich operačního provozu.

Použití middleware a softwarových bran může usnadnit integraci různých systémů. Tyto technologie umožňují přenos dat mezi nekompatibilními systémy a zajišťují, že informace mohou být sdíleny a využívány napříč různými platformami. Middleware může být navržen tak, aby podporoval různé komunikační protokoly a formáty dat, což usnadňuje integraci a zvyšuje flexibilitu celého systému. Tím se nejen zvyšuje efektivita, ale také se snižují náklady na přechod, protože není nutné nahrazovat všechny stávající systémy najednou.

Standardizované aplikační programové rozhraní (API) umožňuje snadnou integraci různých aplikací a systémů. API poskytuje definované metody komunikace mezi různými softwarovými komponenty, což umožňuje vývojářům snadno integrovat nové funkce a aplikace do stávajících systémů. Použití otevřených standardů pro API zajišťuje interoperabilitu a umožňuje spolupráci různých výrobců a vývojářů.

Jedním z aspektů integrace je schopnost efektivně spravovat a integrovat data z různých zdrojů. To zahrnuje nejen technické řešení pro přenos a zpracování dat, ale také zajištění datové integrity, kvality a bezpečnosti.

7.3 Budování odolného ekosystému pro krizovou komunikaci

Vývoj širokopásmových systémů pro krizovou komunikaci není jen volbou technologie, ale zahrnuje také důležité organizační, provozní a technické úvahy. Historicky byly sítě a organizace pro veřejnou bezpečnost často decentralizované, někdy podle geografických oblastí nebo disciplín. Postupně se však stala nezbytnou spolupráce mezi různými disciplínami a potřeba interoperability, což vedlo většinu vlád k vytvoření dedikovaných organizací a systémů. Přechod na ekosystém 3GPP otevírá nové možnosti pro telekomunikační poskytovatele a zpochybňuje relevantnost těchto dedikovaných organizací a systémů.

Výzvy a příležitosti pro orgány veřejné bezpečnosti: Orgány veřejné bezpečnosti budou čelit mnoha výzvám a příležitostem při přechodu na širokopásmové systémy. Klíčovým faktorem úspěchu je zapojení uživatelů před, během i po procesu nasazení a provozu systému, stejně jako jejich aktivní zapojení do formování reinvestic a evolucí sítě. Pro organizace, které jsou vedeny potřebami velkého počtu komerčních uživatelů oproti malému počtu uživatelů veřejné bezpečnosti, budou vždy tendence směřovat k tomu, co potřebují komerční uživatelé, což může být v rozporu s potřebami veřejné bezpečnosti.

Fragmentace trhu: Aplikace pro business-critical a krizové aplikace se sbližují směrem ke stejným technologiím založeným na 3GPP. To otevírá nové příležitosti pro aktéry, jako jsou mobilní operátoři (MNOs), dodavatelé privátních sítí, výrobci zařízení a další. Nicméně, jak mohou vlády zajistit nejvyšší úrovně důvěrnosti, bezpečnosti a interoperability služeb pro své uživatele, pokud se zapojí více třetích stran, zejména pokud řešení mohou cílit na ziskovost nad veřejným zájmem.

Rozpočet: Orgány veřejné bezpečnosti musí zajistit dostatečné rozpočty pro vybudování a provozování komponent krizové sítě při zajištění nákladové efektivity a finanční životaschopnosti nové sítě. Investice do stávajících systémů byly často zaměřeny na fáze vývoje a nasazení, což vedlo k vysokým provozním nákladům kvůli omezenému ekosystému dodavatelů. Naproti tomu prostředí širokopásmové krizové komunikace zahrnuje větší diverzitu aktérů, což by mělo vést ke snížení nákladů.

Orchestraci ekosystému: Budování a provozování systémů pro krizovou komunikaci vyžaduje orchestraci rozsáhlého ekosystému partnerů. Nutností je end-to-end vize sítě a služeb pro zajištění výkonu a flexibility a vyhnutí se uzamčení s konkrétním dodavatelem. Vytvoření robustního ekosystému, který zahrnuje širokou škálu aktérů, může orgánům veřejné bezpečnosti pomoci vyhnout se dlouhodobému uzamčení partnerů, jak tomu bylo v některých zemích.

Technologie: Orgány veřejné bezpečnosti budou muset zajistit, že sítě budou odolné a navrženy pro maximální výkon, odolnost, spolehlivost, bezpečnost, interoperabilitu a schopnost evoluce. Standardizace širokopásmových služeb je stále ve vývoji, což znamená, že technologie zatím nejsou dostatečně zralé na podporu všech požadavků a aplikací krizové komunikace. Orgány veřejné bezpečnosti musí zajistit, že používané sítě jsou robustní a odolné vůči budoucím technologickým změnám, novým řešením a možnostem propojení v širších ekosystémech, včetně mezinárodní spolupráce.

Přijetí a adaptace uživatelů: Koneční uživatelé – od velitelských center po první respondenty napříč všemi disciplínami – musí být středobodem transformační cesty, od návrhu systémů a služeb až po odpovídající školení a řízení změn. Veřejné bezpečnostní složky jsou obecně vázány na své komunikační nástroje a řešení, a proto bude pro orgány výzvou přesvědčit uživatele o potřebě evoluce nebo způsobu evoluce. Kampaň řízení změn bude nezbytná pro získání konsenzu a podpory od všech uživatelů v různých geografických oblastech, aby bylo zajištěno hladké přechodné období.

Migrace a načasování: Návrh, nasazení a testování nového end-to-end systému pro krizovou komunikaci trvá několik let. Kromě toho migrace všech disciplín na nová zařízení, služby a procesy vyžaduje pečlivé plánování. Časování je klíčové pro hladký přechod k novým technologiím. Výzvou je zajistit, aby orgány jednaly bez prodlení, aby zahájily transformační cestu, plánovaly migraci systémů a zařízení, technologické evoluce a zároveň zabezpečily důvěru uživatelů a mezinárodní integraci v širším ekosystému.

7.4 Příklady aplikací 5G pro různé složky krizového řízení

7.4.1 Policejní složky

Live streaming z palubních kamer a kamer na těle: 5G technologie umožňuje policejním složkám přenášet živé videozáznamy z palubních kamer a kamer na těle v reálném čase do centrálních řídících center. To umožňuje lepší povědomí o situaci, okamžitou reakci a koordinaci na základě aktuálních vizuálních informací z terénu.

Biometrické senzory a lokalizace: Použití biometrických senzorů v kombinaci s lokalizačními technologiemi umožňuje sledování zdravotního stavu a polohy jednotlivých policistů v reálném čase. Tato data mohou být využita pro zajištění bezpečnosti a efektivity operací.

Prediktivní hrozby a hodnocení rizik: S využitím pokročilých analytických nástrojů a umělé inteligence mohou policejní složky předpovídat možné hrozby a hodnotit rizika na základě různých datových vstupů. To umožňuje preventivní opatření a rychlou reakci na potenciální nebezpečí.

Monitoring chytrých měst: Integrace sítě senzorů a kamer v rámci konceptu chytrých měst umožňuje policii monitorovat různé oblasti městského prostředí v reálném čase. Tím se zvyšuje bezpečnost a efektivita policejních operací.

Reálná lokalizace terénních agentů: Technologie 5G umožňuje přesnou a reálnou lokalizaci terénních policistů, což zlepšuje koordinaci a efektivitu zásahů. Vedení může lépe řídit nasazení sil a prostředků podle aktuálních potřeb.

7.4.2 Hasičské jednotky

Připojené helmy: Hasiči mohou využívat připojené helmy vybavené kamerami a senzory, které přenášejí data v reálném čase do řídících center. To umožňuje lepší orientaci v terénu a efektivnější řízení zásahů.

Odolné tablety a smartphony: Použití odolných mobilních zařízení, která jsou navržena pro náročné podmínky, umožňuje hasičům přístup k digitálním nástrojům a informacím přímo na místě zásahu.

Autonomní drony: Drony mohou být využity pro průzkum nebezpečných oblastí, detekci požárů a poskytování živých videozáznamů z míst, která jsou pro hasiče těžko přístupná. To zvyšuje bezpečnost a efektivitu zásahů.

3D mapování a vnitřní lokalizace: Pomocí 3D mapování a technologií vnitřní lokalizace mohou hasiči získat přesný přehled o situaci uvnitř budov. To usnadňuje navigaci a plánování zásahů.

Live streaming zásahů: 5G technologie umožňuje přenos živých videozáznamů ze zásahů, což zlepšuje koordinaci mezi různými jednotkami a řídícími centry.

7.4.3 Zdravotnické a záchranné služby

Připojené sanitky s videohovory do nemocnice: Sanitky vybavené 5G technologií mohou přenášet data a videozáznamy v reálném čase přímo do nemocnice. To umožňuje lékařům připravit se na příjezd pacienta a poskytovat pokyny během převozu.

Senzory na pacientech: Senzory na pacientech mohou monitorovat vitální funkce a zdravotní stav v reálném čase. Tato data mohou být přenášena do nemocnice, což umožňuje lékařům sledovat stav pacienta ještě před jeho příjezdem.

Ochrana před násilím: Zdravotnický personál může být vybaven zařízeními, která poskytují ochranu před násilnými útoky během zásahů. To zahrnuje nouzová tlačítka a monitorovací systémy.

Podpora při dálkových operacích: Vzdálená podpora lékařských specialistů během operací může být poskytována pomocí video přenosů a konzultací v reálném čase. To zvyšuje kvalitu lékařské péče v terénu.

Mobilní přístup k pacientským datům: Zdravotničtí pracovníci mohou mít přístup k elektronickým zdravotním záznamům pacientů přímo v terénu, což umožňuje lepší a rychlejší rozhodování.

7.5 Další složky (obrana, celní správa atd.)

Důstojníci vybaveni připojeným zařízením: Použití připojených zařízení umožňuje důstojníkům mít přístup k datům a komunikovat v reálném čase, což zlepšuje efektivitu a koordinaci operací.

Taktické informační sdílení: Sdílení taktických informací v reálném čase mezi různými složkami zajišťuje lepší koordinaci a efektivitu zásahů.

Automatizované podávání zpráv: Automatizace procesů podávání zpráv snižuje administrativní zátěž a umožňuje se více soustředit na operativní činnosti.

Údržba a prediktivní logistika: Prediktivní údržba a logistika umožňují lepší plánování a prevenci problémů, což zajišťuje plynulý provoz a dostupnost potřebného vybavení.

Mobilní kancelář: Mobilní zařízení umožňují důstojníkům pracovat efektivně z různých míst, což zvyšuje jejich flexibilitu a dostupnost.

8 Příklady řešení PPDR sítí v zahraničí

Tato kapitola poskytuje náhled do systémů PPDR v zahraničí. Popisuje legislativní a technologickou stránku řešení, která jsou implementována v různých zemích. Je důležité poznamenat, že neexistuje jednotný postup pro zavádění PPDR sítí, protože každé řešení je specifické pro konkrétní zemi a její potřeby. Tím se zajišťuje, že systémy jsou přizpůsobeny místním legislativním požadavkům, technologickým možnostem a operativním potřebám záchranných složek a dalších bezpečnostních orgánů.

8.1 Německo – Digitalfunk BOS

Německo se rozhodlo modernizovat svůj komunikační systém pro veřejnou bezpečnost prostřednictvím implementace systému Digitalfunk BOS. Tento systém byl vyvinut, aby zajistil spolehlivou a efektivní komunikaci pro všechny záchranné a bezpečnostní složky na federální, státní a místní úrovni. Digitalfunk BOS je spravován Federálním úřadem pro digitální rádio bezpečnostních složek (BDBOS), který byl založen v roce 2007 s cílem vybudovat, provozovat a rozvíjet tento systém na dlouhodobé bázi.

Digitalfunk BOS je postaven na technologii TETRA (Terrestrial Trunked Radio), která je mezinárodním standardem pro digitální rádiovou komunikaci. Tento systém umožňuje efektivní a bezpečnou komunikaci, která je zásadní pro nouzové služby jako policie, hasičské sbory, záchranné služby a orgány pro ochranu před katastrofami. Systém poskytuje jak hlasovou komunikaci, tak přenos dat, což umožňuje flexibilní a rychlou reakci v krizových situacích.

Hlavním cílem Digitalfunk BOS je zajistit spolehlivou komunikaci i v těch nejnáročnějších podmínkách. Systém zahrnuje více než 5 000 základnových stanic, které pokrývají celé území Německa, a zahrnuje několik regionálních a tranzitních přepojovacích center, která zajišťují přenos dat a hlasu mezi různými regiony. Uživatelé systému využívají různé typy koncových zařízení, jako jsou přenosné a vozidlové radiostanice, které umožňují přímou komunikaci v rámci systému.

Mezi hlavní uživateli BDBOS patří:

- Policejní složky jednotlivých států;
- Federální policie;
- Spolková agentura pro technickou pomoc (THW);
- Spolková celní správa;
- Veřejné hasičské sbory a podnikové hasičské sbory zřízené nebo uznané podle zemského práva;
- Spolkové a zemské úřady pro ochranu před katastrofami a civilní ochranu a spolkové a zemské úřady pro ochranu ústavy.

Digitalfunk BOS představuje zásadní pokrok v oblasti komunikace pro nouzové a bezpečnostní služby v Německu. Díky pokročilé technologii a robustní infrastruktuře poskytuje systém několik klíčových výhod. Vysoká úroveň zabezpečení je zajištěna pokročilými šifrovacími metodami, které chrání komunikaci mezi uživateli před neoprávněným přístupem. Spolehlivost a dostupnost systému je zajištěna díky nouzovým napájecím systémům, které zajišťují nepřetržitou dostupnost služby i v krizových situacích, včetně výpadků elektrické energie.

Systém je rovněž navržen tak, aby byl kompatibilní s podobnými systémy v jiných zemích, což umožňuje mezinárodní spolupráci a zvládání přeshraničních krizových situací. Digitalfunk BOS je flexibilní a škálovatelný, což umožňuje jeho snadné rozšíření a úpravu podle měnících se potřeb a požadavků bezpečnostních složek a dalších uživatelů.

Tento moderní komunikační systém je navržen tak, aby splňoval náročné požadavky na komunikaci v oblasti veřejné bezpečnosti a zajišťoval efektivní a rychlou komunikaci i v krizových situacích, což je klíčové pro zajištění bezpečnosti občanů. Digitalfunk BOS představuje strategický krok k posílení efektivity a spolehlivosti komunikační infrastruktury Německa.

8.1.1 Vývoj a přechod na vlastní širokopásmovou síť Digitalfunk BOS

Mobilní širokopásmová komunikace přináší záchranným složkám mnoho nových možností, jak účinně pomáhat lidem, zachraňovat životy a zajišťovat bezpečnost. K tomu je nezbytná vlastní širokopásmová síťová infrastruktura.

Použití messenger služeb, odesílání a přijímání informací o situaci a pátrání, dotazování se na databáze, přenos vitálních dat a živé video přenosy – tyto nové aplikace mohou podporovat policii, hasiče a záchranné služby různými způsoby, aby úspěšně dokončily své mise. Technické možnosti zahrnují vysoce integrované systémy, které mohou poskytovat relevantní informace velkému počtu účastníků současně a v reálném čase. Moderní mobilní datová komunikace umožňuje lidem rychle získat potřebnou pomoc.

Současný standard TETRA, na kterém je digitální rádio BOS založeno, využívá dostupný technický potenciál pro přenos hlasu a krátkých dat, ale širokopásmový přenos dat není technicky možný. Některé spolkové státy proto dočasně spoléhají na komerční mobilní sítě jako přechodné řešení. Tyto sítě však nejsou dostatečně bezpečné ani spolehlivé pro kritickou komunikaci. Proto Německo společně s federálními a státními vládami plánuje vybudování vlastní širokopásmové digitální rádiové sítě BOS.

8.1.1.1 Vybudování vlastní širokopásmové sítě BOS:

Fáze 0: Příprava a využití komerčních sítí:

Ve fázi 0 bude záchranným složkám umožněn roaming a využívání dalších funkcí prostřednictvím komerčních mobilních sítí. Dojde k sjednocení individuálních smluv, které federální vláda a mnoho spolkových států uzavřelo s komerčními mobilními operátory.

Fáze 1: Výstavba základní širokopásmové sítě

Fáze 1 zahrnuje zahájení výstavby plánované širokopásmové sítě. Bude vyvinuta a vybudována vlastní širokopásmová základní síť. V této fázi budou nadále využívány rádiové a přístupové sítě komerčních mobilních operátorů.

Fáze 2: Rozšiřování vlastní sítě

Ve fázi 2 bude ve spolupráci s federálními a státními vládami postupně budována vlastní rádiová a přístupová síť po celém Německu.

Fáze 3: Přechod a migrace služeb

Ve fázi 3 se postupně sníží využívání komerčních sítí a dojde k migraci hlasových služeb. Veškerá hlasová a datová komunikace v digitálním rádiu BOS bude probíhat přes vlastní širokopásmovou síť BOS. Systémová technologie TETRA bude postupně vypnuta. Zahájení této fáze je plánováno na začátek 30. let 21. století.

8.1.2 Technická infrastruktura Digitalfunk BOS

8.1.2.1 Funkční a přístupová síť

Funkční a přístupová síť Digitalfunk BOS zahrnuje více než 5 000 základnových stanic (TETRA Base Stations – TBS), které pokrývají celé území Německa. Tyto základnové stanice jsou rozmístěny v jednotlivých buňkách sítě a zajišťují přenos hlasu a dat mezi uživateli a centrálními uzly sítě. Každá základnová stanice zpracovává příchozí a odchozí komunikaci v rámci své buňky, což umožňuje efektivní koordinaci a rychlou reakci bezpečnostních složek v terénu.

8.1.2.2 Jádrová síť

Jádrová síť je centrální částí systému Digitalfunk BOS a zajišťuje přenos dat a hlasu mezi různými regiony. Systém zahrnuje 64 regionálních přepojovacích center (Digital Exchange for TETRA – DXT) a 4 tranzitní přepojovací centra (Digital Exchange for TETRA Transit Type – DXTT), která zajišťují propojení mezi regionálními centry a umožňují meziregionální komunikaci. Jádrová síť také obsahuje systémy pro správu všech zařízení a uživatelských skupin, stejně jako centrální řídicí centra, která dohlížejí na celý systém.

8.1.2.3 Koncová zařízení

Uživatelé systému Digitalfunk BOS využívají různé typy koncových zařízení, včetně přenosných a vozidlových radiostanic a pevně instalovaných radiostanic v řídicích centrech. Tato zařízení umožňují přímou komunikaci v rámci systému, a to jak v síťovém režimu (Trunked Mode Operation – TMO), tak v přímém režimu (Direct Mode Operation – DMO), který umožňuje komunikaci mezi zařízeními bez použití infrastruktury sítě. V síťovém režimu zařízení komunikuje s nejbližší základnovou stanicí, která přenáší hlasové a datové informace dále do sítě.

8.1.2.4 Frekvence

Systém Digitalfunk BOS využívá specifické frekvenční pásmo pro zajištění bezpečné a spolehlivé komunikace. Základnové stanice vysílají v horním pásmu (downlink) v rozsahu 390–395 MHz, zatímco koncová zařízení vysílají v dolním pásmu (uplink) v rozsahu 380–385 MHz. Pro přímou komunikaci mezi zařízeními (Direct Mode Operation – DMO) se využívá frekvenční pásmo 406,1 – 410 MHz.

8.1.2.5 Zajištění napájení

Pro zajištění nepřetržitého provozu i v případě výpadků elektrické energie je infrastruktura Digitalfunk BOS vybavena nouzovými napájecími systémy. Ty zahrnují nepřerušitelné napájecí zdroje (UPS) a nouzové napájecí systémy (NEA), které zajišťují dlouhodobé napájení pomocí dieselových generátorů. Tato opatření zajišťují, že systém zůstane funkční i v krizových situacích.

8.1.3 Klíčové služby Digitalfunk BOS

Systém Digitalfunk BOS poskytuje širokou škálu klíčových služeb, které podporují efektivní fungování bezpečnostních složek a zajišťují bezpečnost obyvatelstva. Tyto služby zahrnují základní hlasovou komunikaci, pokročilé datové služby, a různé další funkce, které umožňují rychlý přenos informací a koordinaci.

8.1.3.1 Skupinová komunikace

Skupinová komunikace zahrnuje point-to-multipoint spojení pro hlasovou komunikaci mezi více komunikačními partnery. Skupinové volání se provádí střídavým mluvením, což znamená, že je zde jeden mluvící účastník a několik poslouchajících účastníků. Role mluvící osoby se může měnit, ale současné mluvení a poslouchání není možné.

Skupinová komunikace může být použita pro každou skupinu celostátně v celé síti nebo v rámci geograficky omezené oblasti volání. Účastníci mohou být současně členy několika skupin, ale aktivní mohou být pouze v jedné skupině najednou, tj. buď mluví nebo poslouchají. Správa skupinové komunikace je podporována nástroji pro administraci členství ve skupinách a oblastí volání.

8.1.3.2 Individuální komunikace

Individuální komunikace je point-to-point spojení pro hlasovou komunikaci mezi dvěma účastníky, podobně jako telefonní hovor. Individuální volání mohou být prováděna střídavým mluvením (tj. vždy může mluvit jen jeden) nebo obousměrným mluvením (tj. oba mohou mluvit současně). Komunikační partneři mohou být oba v BOS digitální síti nebo může být jeden komunikační partner mimo ni, například v pevném telefonním síti. Správa pro využití individuální komunikace je podporována nástroji pro administraci oprávnění.

8.1.3.3 Tísňové služby

Tísňové služby zahrnují kromě běžného tísňového volání také dva další typy tísňových služeb: přednostní hlášení a místní volání o pomoc.

Při tísňovém volání, které je spuštěno stisknutím tísňového tlačítka na rádiovém zařízení, mohou být stávající hovory přerušeny a tísňové volání dostane prioritu. Navíc se při odeslání tísňového volání automaticky přenese aktuální GPS poloha odesílatele, což umožňuje jeho lokalizaci. Také se automaticky odešle taktický status „Nouzový stav“. Hlasová část tísňového volání, poloha a taktický status jsou automaticky přesměrovány na místně příslušné tísňové přijímací středisko.

Přednostní hlášení je vysíláno dispečinkem s prioritou tísňového volání. Díky této prioritě přeruší všechny ostatní hovory kromě tísňových volání. Slouží k předávání naléhavých informací zasahujícím jednotkám

Místní volání o pomoc je také zahrnuto do tísňových služeb, ale nemá prioritu tísňového volání. Místní volání o pomoc je automaticky přesměrováno na místně příslušné středisko. Slouží k získávání informací, například o zásahu nebo k orientaci v neznámých oblastech zásahu.

8.1.3.4 Alarming

Pod pojmem alarming se rozumí zaslání alarmové zprávy jednotlivým příjemcům alarmu nebo alarmové skupině v BOS digitální síti. Alarmová zpráva je odesílána jako krátká datová zpráva. Slouží k svolání zasahujících jednotek dispečinkem a k dálkovému ovládání, například spouštění sirén. Oznámení může být zasláno jak jednotlivým příjemcům alarmu, tak celé skupině příjemců. O využití služby alarming v digitální síti BOS rozhoduje příslušný stát a federální vláda pro podřízené BOS. BDBOS zajišťuje, že systémová technologie na straně sítě podporuje alarming.

8.1.3.5 Služba krátkých datových zpráv

Služba krátkých datových zpráv zahrnuje odesílání taktických stavových hlášení a krátkých datových zpráv.

Taktické statusové zprávy mohou být využity k předávání informací o stavu zásahu nebo například k přihlášení požadavku na mluvení. Krátkými datovými zprávami lze mimo jiné přenášet následující informace:

Textové zprávy, podobné SMS na mobilním telefonu

Místní zprávy, které přenášejí pozici zasahující jednotky do dispečinku

Alarmovací zprávy

Jak taktické statusové zprávy, tak krátké datové zprávy mohou být v zásadě zasílány jednotlivým adresátům nebo skupinám.

8.1.3.6 GPS založené sledování vozidel a osob

Tato služba umožňuje rádiovým zařízením automaticky odesílat svou polohu. Odesílají se zprávy s přesnými GPS souřadnicemi. Zprávy mohou být odesílány v pravidelných intervalech nebo po určité ujeté vzdálenosti, například každých 10 minut nebo po každých 100 metrech. Při tísňových voláních se zpráva s polohou odesílá automaticky.

8.1.3.7 Prioritizace

Tato služba určuje, které služby a zařízení mají v komunikaci v digitální síti BOS přednost před ostatními. Například zajišťuje, že tísňová volání mají vyšší prioritu než běžný rádiový provoz. Správa priorit je podporována nástroji, které umožňují správu priorit služeb a účastníků.

8.1.3.8 Komunikace přes letecké rádiové buňky

Rádiová zařízení instalovaná v letadlech využívají kromě pozemního rádiového pokrytí (TVFZ) také speciálně vytvořené letecké rádiové buňky (LFFZ) pro letecký prostor. Po dosažení určité letové výšky se tato rádiová zařízení automaticky přepnou z pozemního pokrytí na dostupnou leteckou buňku a používají ji až do přistání.

8.1.3.9 Provoz bran mezi síťovým a přímým režimem (TMO-DMO Gateway)

Pro podporu zásahů v oblastech s nedostatečným pokrytím sítí (TMO) může být užitečné použít TMO-DMO Gateway. Například jednotky zasahující v budovách, které nemají dostatečné venkovní pokrytí nebo nejsou pokryty základnovými stanicemi, mohou přes bránu v přímém režimu (DMO) komunikovat s řídicím střediskem v TMO. Brána umožňuje komunikaci mezi skupinou v TMO a skupinou v DMO.

8.1.3.10 Přechod do cizích sítí

Cizími sítěmi se rozumí TETRA sítě jiných organizací, například z německých sousedních států, nebo soukromých provozovatelů sítí, jako jsou dopravní podniky nebo letiště. Základní služba Přechod do cizích sítí upravuje používání služeb v těchto cizích sítích a komunikaci mezi jednotkami BOS digitální sítě a jednotkami v těchto cizích sítích.

8.1.3.11 Šifrování

Rádiová komunikace v BOS digitální síti splňuje požadavky na zabezpečenou hlasovou a datovou komunikaci. K tomu jsou nejprve šifrovány rádiové spojení a následně i hlas a krátká data. Rádiové spojení je zabezpečeno pomocí šifrování na úrovni

rádiového rozhraní. Hlas a všechna krátká data jsou dále chráněna šifrováním typu end-to-end. Tím je celá komunikace plně šifrována pomocí BOS kryptosystému.

Základní konfigurace všech služeb je jednotně dostupná všem zasahujícím jednotkám po celé zemi. Ve spolupráci s uživateli jsou průběžně vyvíjeny a zdokonalovány pokyny pro jednotné používání a přizpůsobení služeb dle potřeb.

8.1.4 Legislativní rámec Digitalfunk BOS

Legislativní rámec pro systém Digitalfunk BOS je definován zákonem o zřízení Spolkového úřadu pro digitální komunikaci bezpečnostních složek a organizací (BDBOS-Gesetz – BDBOSG). Tento zákon, který byl přijat 28. srpna 2006 a poslední změna byla provedena 19. prosince 2022, upravuje vznik, účel, úkoly a správu systému Digitalfunk BOS.

Podle zákona BDBOSG byla zřízena Spolková agentura pro digitální komunikaci bezpečnostních složek a organizací (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben – BDBOS). Tato agentura je právnickou osobou veřejného práva v rámci Spolkového ministerstva vnitra, výstavby a domoviny. Jejím hlavním účelem je výstavba, provoz a rozvoj jednotného digitálního hlasového a datového komunikačního systému pro bezpečnostní složky a organizace v Německu.

BDBOS má za úkol zajistit funkčnost a bezpečnost systému Digitalfunk BOS, což zahrnuje nejen technické aspekty, ale také organizační a administrativní podporu. Spolupráce mezi federální vládou a spolkovými zeměmi při provozu systému Digitalfunk BOS je upravena správní dohodou. Tato dohoda obsahuje ustanovení týkající se spolupráce, financování a účasti zemí na provozu a výstavbě systému.

Orgány BDBOS jsou prezident a správní rada. Prezident odpovídá za vedení úřadu a realizaci rozhodnutí správní rady, která dohlíží na činnost prezidenta a podporuje ho při plnění jeho úkolů. Správní rada je složena ze zástupců federální vlády a každé spolkové země, a rozhoduje o zásadních otázkách týkajících se BDBOS.

Financování BDBOS je zajištěno prostřednictvím společného rozpočtu federální vlády a spolkových zemí. Podrobné ustanovení o financování jsou upravena ve správní dohodě mezi federální vládou a spolkovými zeměmi. Tento společný rozpočet zajišťuje, že BDBOS má dostatečné prostředky na plnění svých úkolů.

Zákon BDBOSG zahrnuje klíčová ustanovení pro zajištění bezpečné a spolehlivé komunikace pro bezpečnostní složky v celém Německu, což je zásadní pro koordinaci při krizových situacích a pro zajištění veřejné bezpečnosti.

8.2 Finsko – Virve 2

Finsko se rozhodlo modernizovat svůj původní komunikační systém Virve na novou generaci, Virve 2, aby zajistilo vyhovění rostoucím nárokům na komunikaci ve veřejné bezpečnosti. Původní systém, spuštěný v roce 2002, zahrnoval 1 400 základnových stanic a poskytoval služby pro 41 000 uživatelských připojení. Každý týden bylo v síti uskutečněno přibližně 1,1 milionu skupinových hovorů a odesláno 50 milionů krátkých datových zpráv (SDS). Tento systém, spravovaný společností State Security Networks Group Finland (Erillisverkot), poskytoval spolehlivou komunikaci pro široké spektrum veřejných bezpečnostních složek a dalších klíčových organizací.

V roce 2016, Finské ministerstvo dopravy a komunikací (Finnish Ministry of Transport and Communications) vydražilo frekvence 700 MHz, které byly dříve využívány televizními vysílateli, komerčním teleoperátorům. Toto rozhodnutí umožnilo vytvoření robustní infrastruktury pro novou generaci komunikačních technologií, které tvoří základ pro Virve 2.

Podle průzkumu společnosti Erillisverkot z roku 2018 vyjádřilo 80 % uživatelů potřebu služeb, které by byly srovnatelné s komerčními mobilními sítěmi. Virve 2 proto zajišťuje pokročilé širokopásmové služby, které umožňují přenos vysoce kvalitního video materiálu a dat v reálném čase pro efektivní plnění úkolů veřejné bezpečnosti. Tento přechod na Virve 2 není pouze technologickou aktualizací, ale představuje strategický krok k posílení efektivity a spolehlivosti komunikační infrastruktury.

Virve 2 je navržena tak, aby upřednostňovala komunikaci bezpečnostních složek před komerčními uživateli při používání mobilních širokopásmových služeb. To znamená, že přístup a dostupnost služeb pro tyto složky bude zajištěna i při vysokém zatížení sítě. Systém také poskytuje rychlé a bezproblémové skupinové hovory a krátké datové zprávy (SDS).

Nový systém Virve 2 využívá kapacity komerčních mobilních sítí, což umožňuje široké pokrytí a vysokou spolehlivost. Tento přístup zajišťuje, že bezpečnostní složky mají přístup k nejnovějším technologiím a mohou využívat kapacitu a pokrytí komerčních mobilních sítí, což zaručuje spolehlivé a bezpečné připojení pro všechny klíčové služby. Přechod na Virve 2 je

realizován ve spolupráci mezi státními orgány a komerčními partnery. Erillisverkot zahájil v roce 2019 výběrové řízení na komerční operátory, aby zajistil, že služby budou splňovat potřeby veřejné bezpečnosti s využitím vítězné 4G sítě

Virve 2 využívá hybridní model (MOCN – Multi-Operator Core Network), který kombinuje dedikovanou síťovou infrastrukturu s komerčními mobilními operátory, což zajišťuje robustní a bezpečnou síťovou architekturu. Nasazení nové generace komunikační sítě, založené na technologiích LTE/5G, je plánováno na období 2023-2025.

Hlavními uživateli systému Virve 2 jsou:

- Záchranné služby
- Policie
- Sociální a zdravotnické služby
- Ozbrojené síly
- Pohraniční stráž
- Železniční operátoři
- Celní úřady
- Havarijní služby
- Finský úřad pro dopravu a komunikace
- Národní veřejnoprávní televize YLE

Virve 2 pokrývá celé území Finska a je navržena tak, aby splňovala náročné požadavky na komunikaci v oblasti veřejné bezpečnosti. Tento systém umožňuje efektivní a rychlou komunikaci i v případě krizových situací, což je klíčové pro zajištění bezpečnosti občanů.

8.2.1 Přechod na Virve 2

Přechod z původního systému Virve na jeho modernizovanou verzi, Virve 2, je komplexní proces, který zahrnuje postupnou migraci všech uživatelů na novou platformu, aby byla zajištěna plynulost a kontinuita služeb.

Přechod na Virve 2 je rozdělen do několika fází:

Plánování a příprava: Tento krok zahrnuje detailní plánování přechodu, legislativní změny a výběr dodavatelů. Proces začal v roce 2018 a zahrnoval důkladnou analýzu potřeb uživatelů a návrh nové infrastruktury.

Testování a pilotní provoz: Během let 2022 až 2024 probíhalo testování nových širokopásmových služeb a zařízení, včetně aktivace klíčových funkcí, jako jsou skupinová volání a datové služby, aby bylo zajištěno, že nová infrastruktura splňuje všechny požadavky na bezpečnost a spolehlivost.

Migrace uživatelů: Od roku 2024 do roku 2028 probíhá paralelní provoz starého systému Virve a nového systému Virve 2. Tento postup umožňuje uživatelům postupně přecházet na novou platformu bez narušení jejich každodenní činnosti a zajišťuje hladkou integraci nových funkcí.

Úplná implementace a ukončení starého systému: Od roku 2029 se očekává plná implementace Virve 2 a postupné ukončení původního systému Virve. Během této fáze budou probíhat nové tendry na další rozvoj služeb a zajištění, že systém bude splňovat i budoucí požadavky na komunikaci a bezpečnost.

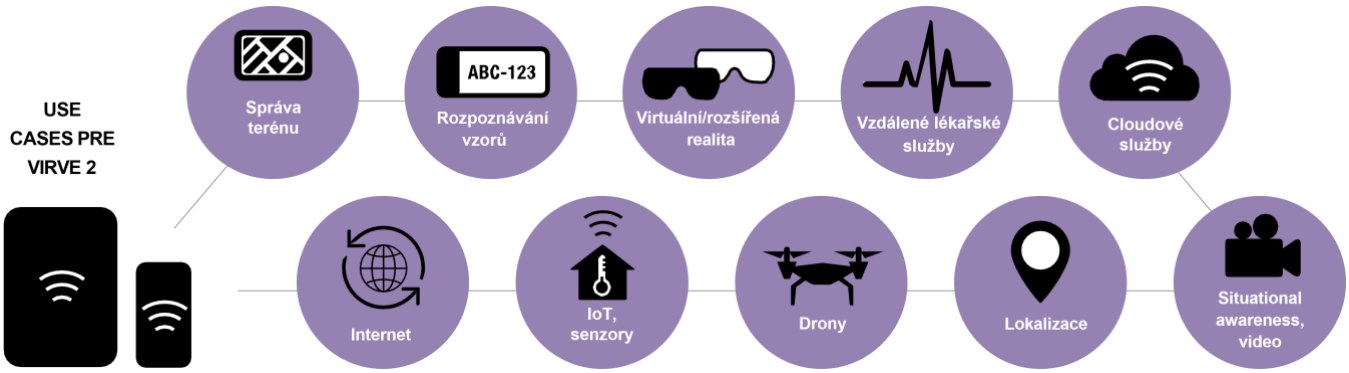
Virve 2 přináší významná zlepšení oproti původnímu systému, včetně vyšší kapacity pro přenos dat, lepšího pokrytí a zvýšené úrovně bezpečnosti.

Přechod na Virve 2 rovněž umožňuje integraci s obdobnými systémy v jiných zemích, čímž se zlepšuje mezinárodní spolupráce a schopnost efektivně zvládat přeshraniční krizové situace. Tento krok tedy nejen zlepšuje národní bezpečnost, ale také posiluje Finsko jako lídra v oblasti veřejné bezpečnostní komunikace na mezinárodní úrovni.

Virve 2 je moderní komunikační platforma, která poskytuje pokročilé služby a aplikace pro veřejné bezpečnostní složky a další organizace kritické infrastruktury. Tato nová generace komunikačního systému přináší významná vylepšení oproti původnímu

systému Virve, včetně širokopásmového připojení, vyšší kapacity pro přenos dat a rozšířených funkcí, které podporují efektivnější a bezpečnější provoz.

8.2.2 Klíčové služby Virve 2



8.2.2.1 Mission Critical Push-to-talk (MCPTT)

Virve 2 poskytuje pokročilé MCPTT služby, které zajišťují spolehlivou a okamžitou hlasovou komunikaci mezi týmy veřejné bezpečnosti v terénu. Systém podporuje jak skupinové hovory, tak individuální volání, což umožňuje efektivní koordinaci při krizových situacích. Tyto služby jsou navrženy tak, aby fungovaly i v náročných podmínkách a prioritizovaly hlasovou komunikaci před datovými přenosy.

8.2.2.2 Přenos videa a multimédií v reálném čase

Nový systém umožňuje přenos vysoce kvalitního videa a obrazových materiálů v reálném čase. To zahrnuje například přenos videa z dronů nebo kamer na uniformách.

8.2.2.3 Integrace Internetu věcí (IoT)

Na trhu již existuje široká škála samostatných IoT zařízení pro různé typy alarmů a monitorování, která mohou bezpečnostní složky integrovat do svých systémů. S rozvojem technologií NB-IoT a LTE-M se očekává, že tyto funkce budou dostupné s vyšší spolehlivostí a efektivitou. V budoucnu budou moci bezpečnostní složky shromažďovat data z vlastních, otevřených i komerčních zdrojů, což umožní efektivní monitorování prostředí, detekci hrozeb a rychlou reakci na incidenty.

8.2.2.4 Rozšířená a virtuální realita

Systém podporuje aplikace založené na rozšířené a virtuální realitě, které mohou být využity pro tréninkové účely nebo pro poskytování dodatečných informací v reálném čase během operací.

8.2.2.5 Automatizace a robotika

Virve 2 podporuje inovace v oblasti automatizace a robotiky, včetně používání autonomních zařízení, jako jsou drony a roboty, které mohou zlepšit efektivitu operací a bezpečnost pracovníků v terénu. Tyto technologie umožňují například provádění průzkumu nebezpečných oblastí bez nutnosti nasazení lidských sil.

8.2.3 Legislativa a její dopad na implementaci Virve 2

Současná rádiová síť Virve bude postupně nahrazena širokopásmovou sítí Virve 2.0, která je legislativně schválena. Tato změna má za cíl zlepšit bezpečnost a efektivitu zásahů záchranných složek. Legislativa potřebná pro tuto modernizaci zahrnuje tři zákony: Zákon o elektronických komunikačních službách, Zákon o záchranných službách a Zákon o prevádzke vládnej bezpečnostnej siete. Zákon o elektronických komunikačních službách a Zákon o záchranných službách, byly v roce 2019 aktualizovány.

Hlavní legislativní rámec zahrnuje následující zákony:

Zákon o elektronických komunikačních službách (917/2014) / Laki sähköisen viestinnän palveluista (917/2014)

Zákon o záchranných službách (379/2011) / Pelastuslaki (379/2011)

Zákon o prevádzke vládnej bezpečnostnej siete (10/2015)

8.2.3.1 Zákon o elektronických komunikačních službách (917/2014) / Laki sähköisen viestinnän palveluista (917/2014)

Zákon o elektronických komunikačních službách se zaměřuje na regulaci a správu elektronických komunikačních sítí a služeb ve Finsku. Cílem tohoto zákona je zajistit, aby komunikační služby byly spolehlivé, bezpečné a dostupné pro všechny občany, přičemž klade důraz na ochranu uživatelských dat, zabezpečení komunikace a podporu konkurenceschopnosti v oblasti elektronických komunikací.

Tento zákon upravuje povinnosti poskytovatelů elektronických komunikačních služeb, stanoví technické a organizační požadavky na zabezpečení sítí a služeb a definuje práva a povinnosti uživatelů těchto služeb. Důležitou součástí zákona je také regulace širokopásmových služeb a specifické požadavky na služby poskytované pro veřejné bezpečnostní sítě.

Zákon zdůrazňuje význam kvality a bezpečnosti komunikačních sítí a služeb. Poskytovatelé služeb musí zajistit, aby jejich sítě byly odolné vůči vnějším vlivům a hrozbám pro bezpečnost informací. Tento zákon také pověřuje Finský úřad pro komunikace, dopravu a infrastrukturu (Traficom) dohledem nad kvalitou, bezpečností a interoperabilitou komunikačních sítí a služeb.

Zákon rovněž stanoví rámec pro zajištění nepřetržité dostupnosti a spolehlivosti přenosu dat pro potřeby veřejné bezpečnosti. Poskytovatelé služeb musí implementovat technická a organizační opatření k ochraně před neoprávněným přístupem a zajistit důvěrnost a integritu přenášených dat. To zahrnuje také kontrolu přístupu a přidělování síťových zdrojů pro prioritní komunikaci orgánů veřejné správy.

Následující kapitoly 29 a 29a se zaměřují na specifické požadavky na širokopásmové služby pro veřejné bezpečnostní sítě a na zajištění bezpečnosti elektronických komunikačních sítí a služeb. Tyto kapitoly detailně upravují, jak by měly být sítě a služby navrženy, postaveny a udržovány, aby splňovaly vysoké standardy technické kvality a bezpečnosti.

Kapitola 29 - Širokopásmové služby pro veřejné bezpečnostní sítě

Tato kapitola se zaměřuje na regulaci širokopásmových služeb poskytovaných pro veřejné bezpečnostní sítě. Specifikuje požadavky na přenos dat, ochranu komunikací a zajištění bezpečnosti. Například, poskytovatelé služeb musí zajistit nepřetržitou dostupnost a spolehlivost přenosu dat pro potřeby veřejné bezpečnosti.

Blíže specifikované požadavky a regulace uvedené v této kapitole jsou:

Veřejné komunikační sítě a služby musí být navrženy, postaveny a udržovány tak, aby zajistily vysokou technickou kvalitu a bezpečnost informací. Musí být odolné vůči různým vnějším vlivům a hrozbám pro bezpečnost informací. Zajištění spolehlivého přístupu k tísňovým službám i při výpadcích sítě je klíčové.

Traficom (Finský úřad pro komunikace, dopravu a infrastrukturu) může vydávat předpisy týkající se kvality, bezpečnosti informací a interoperability komunikačních sítí a služeb. Tyto předpisy zahrnují například priority, napájení, integritu, redundantní trasy a ochranu sítí (Sekce 244).

Síťové zařízení nesmí ohrozit národní bezpečnost, a Traficom může nařídit odstranění takového zařízení z kritických částí sítě pro ochranu infrastruktury, jako jsou jaderné elektrárny, přístavy a letiště (Sekce 244a).

Poradní výbor pro bezpečnost sítí, zřízený vládou, hodnotí národní bezpečnost v komunikačních sítích, monitoruje vývoj a předkládá návrhy na zlepšení bezpečnosti sítí (Sekce 244b).

Úřady musí předkládat návrhy na provozní požadavky pro odposlechy a monitorování, a operátoři musí informovat úřady o změnách relevantních pro tyto činnosti (Sekce 245).

Poskytovatelé musí udržovat bezpečnost informací pro služby, komunikaci, údaje o provozu a poloze, přičemž opatření musí být úměrná hrozbám a technologickému vývoji (Sekce 247). Poskytovatelé online trhů, vyhledávačů a cloudových služeb musí řídit rizika pro sítě a systémy, včetně bezpečnosti systémů, řešení hrozeb, kontinuitu podnikání a dodržování mezinárodních standardů (Sekce 247a).

Operátoři musí minimalizovat obtěžování ostatních během výstavby, údržby nebo bezpečnostních opatření a dočasné výpadky musí být oznámeny dotčeným operátorům (Sekce 248).

Kapitola 29a – Zajištění bezpečnosti elektronických komunikačních sítí a služeb

Tato kapitola rozšiřuje požadavky na bezpečnost sítí a služeb. Stanoví povinnost poskytovatelů implementovat technická a organizační opatření k zajištění bezpečnosti a integrity sítí, což zahrnuje ochranu před neoprávněným přístupem a zajištění důvěrnosti a integrity přenášených dat.

Blíže specifikované požadavky a regulace uvedené v této kapitole jsou:

Předplatné pro využívání sítě veřejné správy a souvisejících komunikačních služeb může být nabídnuto orgánům a dalším důležitým skupinám, které plní úkoly spojené s národní bezpečností, veřejným pořádkem, záchrannými operacemi a dalšími klíčovými funkcemi státu. Ministerstvo dopravy a komunikací rozhoduje o těchto skupinách a počtu předplatných.

Poskytovatel služeb pro veřejnou správu musí zajistit, aby tyto služby měly přednostní přístup a dostatečnou kvalitu i v případě přetížení sítě. To zahrnuje kontrolu přístupu a přidělování síťových zdrojů pro prioritní komunikaci orgánů veřejné správy (Sekce 250b).

V případě potřeby musí telekomunikační operátoři poskytnout národní roaming pro komunikace veřejné správy, pokud není dostupná síť primárního poskytovatele služeb. Podmínky pro poskytování těchto služeb může rozhodnout Traficom, pokud se strany nedohodnou (Sekce 250d).

Telekomunikační operátoři musí připojit síť veřejné správy k veřejné komunikační síti bezplatně na požádání, aby zajistili potřebnou interoperabilitu a funkčnost (Sekce 250e).

8.2.3.2 Zákon o záchranných službách (379/2011) / Pelastuslaki (379/2011)

Zákon o záchranných službách (379/2011) v sekci 109 § stanovuje následující:

Pokud budova představuje vyšší riziko pro bezpečnost osob a stávající síť Virve nebo budoucí síť Virve 2 nemá dostatečné pokrytí signálem k zajištění potřeb záchranných složek, majitel budovy je povinen zajistit dostatečné pokrytí signálem Virve uvnitř budovy.

Vyšší riziko pro bezpečnost osob se vztahuje na budovy, kde je větší pravděpodobnost výskytu nebezpečných situací. To zahrnuje budovy s velkým množstvím lidí (např. obchodní centra, nemocnice, školy) nebo budovy, kde jsou uloženy nebezpečné látky.

Majitel budovy je odpovědný za to, že v případě nedostatečného pokrytí signálem zajistí technické řešení pro jeho zlepšení. Může jít například o instalaci repeaterů (zesilovačů signálu) nebo jiných technologií, které zajistí potřebnou kvalitu signálu uvnitř budovy.

Cílem této povinnosti je zajistit, aby záchranné a bezpečnostní složky mohly efektivně komunikovat i uvnitř budov, které představují zvýšené riziko. Tím se zvyšuje bezpečnost jak pro zasahující jednotky, tak pro osoby nacházející se v těchto budovách.

Tato povinnost je součástí širšího rámce zajištění bezpečnosti a efektivního fungování záchranných složek, který je v souladu se zákonem o elektronických komunikačních službách (917/2014) a dalšími relevantními legislativními úpravami.

8.2.3.3 Zákon o bezpečnostní síti veřejné správy (10/2015) / Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015)

Zákon o bezpečnostní síti veřejné správy, přijatý 13. ledna 2015, má za cíl zajistit plynulost a kontinuitu komunikace potřebné pro spolupráci vrcholového vedení státu a dalších autorit důležitých pro bezpečnost společnosti. Tento zákon se zaměřuje na bezpečnostní síť veřejné správy, její služby a infrastrukturu, přičemž se snaží zabezpečit dostupnost, integritu a důvěrnost informací nezbytných pro rozhodování a řízení státu

Podle zákona je povinnost používat bezpečnostní síť uložena orgánům státní správy, obranným silám, policii, pohraniční stráži, záchranným službám a dalším kritickým subjektům. Bezpečnostní síť zahrnuje komunikační síť, zařízení a další infrastrukturu nezbytnou pro zajištění vysoké připravenosti a bezpečnosti. Tento zákon také umožňuje používání bezpečnostní sítě jinými subjekty, pokud jejich činnost souvisí s bezpečností státu a jsou schváleny Ministerstvem financí.

Poskytovatelem síťových a infrastrukturních služeb bezpečnostní sítě je společnost Suomen Erillisverkot Oy, která je vlastněna státem a nemá generovat komerční zisk. Úkoly této společnosti zahrnují produkci, údržbu a rozvoj síťových služeb, správu zařízení a zajištění bezpečnosti a kontinuity služeb v normálních, narušených i výjimečných podmínkách. Poskytovatel technických služeb a integračních služeb je státní servisní centrum, které musí oddělit činnosti související s bezpečnostní sítí od ostatních aktivit.

Ministerstvo financí je odpovědné za celkovou kontrolu a dohled nad provozem bezpečnostní sítě, včetně strategického a finančního řízení a zajištění informační a komunikační bezpečnosti. Za účelem podpory Ministerstva financí při řízení a dohledu nad bezpečnostní sítí je zřízen poradní výbor.

Zákon také obsahuje přechodná ustanovení, která upravují organizaci úkolů, zavádění povinnosti používání bezpečnostní sítě a převod majetku na nového poskytovatele služeb. Tento zákon nabývá účinnosti 15. ledna 2015 a stanovuje, že příslušné autority musí začít používat služby bezpečnostní sítě nejpozději po ukončení platnosti stávajících smluv na obdobné služby. Přechodná ustanovení se rovněž vztahují na umístění informačních systémů do zařízení bezpečnostní sítě a na organizaci pracovního postavení personálu.

Zákon č. 10/2015 je klíčovým legislativním aktem, který má za cíl zvýšit připravenost a bezpečnost veřejné správy ve Finsku. Tímto zákonem se zabezpečuje bezpečná a nepřetržitá komunikace pro státní orgány a další důležité subjekty.

8.3 Belgie – ASTRID

Belgie se rozhodla modernizovat svou komunikační infrastrukturu pro veřejnou bezpečnost zavedením a neustálým rozvojem systému ASTRID (Agency for Safety and Emergency Response). Tento systém, spuštěný v roce 1998, je specificky navržen pro podporu komunikačních potřeb policie, hasičských sborů, zdravotnických služeb a dalších záchranných a bezpečnostních složek.

ASTRID je specializovaný telekomunikační operátor poskytující technologické služby pro všechny záchranné a bezpečnostní složky v Belgii. Efektivní, rychlá a bezpečná komunikace prostřednictvím sítě ASTRID zvyšuje bezpečnost všech občanů. Systém ASTRID využívá normu TETRA (TErrestrial Trunked Radio), což je evropský standard pro digitální radiokomunikaci, používaný téměř ve všech evropských zemích.

ASTRID byla založena jako akciová společnost veřejného práva a je stoprocentně vlastněna belgickým státem. Tento systém poskytuje jednotnou platformu pro komunikaci všech záchranných a bezpečnostních složek, čímž eliminuje technické bariéry minulosti a umožňuje lepší koordinaci a efektivitu při zásazích.

ASTRID zahrnuje několik klíčových služeb, které jsou zásadní pro efektivní fungování veřejných bezpečnostních složek:

Radiokomunikace: Poskytuje vysoce kvalitní hlasovou komunikaci s rychlým navázáním spojení pro týmy v terénu.

Paging: Zasílání výstražných zpráv pro hasiče a zdravotnické služby.

Noodcentrales (Tísňové centrály): Technické vybavení a software pro krajská střediska zpracovávající tísňová volání (100, 101, 112).

Mobilní širokopásmová data: SIM karty Blue Light Mobile poskytují prioritu na síti Proximus, což je důležité při přetížení sítě.

Poradenství a podpora: Stálý kontakt s uživateli pro zajištění jejich seznámení s technologií, poskytování školení a poradenství podle potřeby.

8.3.1 Modernizace a plány do budoucna

Systém ASTRID se inovuje, aby splňoval stále rostoucí požadavky na komunikaci v oblasti veřejné bezpečnosti. Plánovaná modernizace zahrnuje přechod na technologii 5G, která výrazně zvýší kapacitu pro přenos dat a zlepší spolehlivost a bezpečnost komunikace mezi záchrannými a bezpečnostními složkami.

V roce 2023 schválila belgická vláda čtvrtý správní kontrakt mezi státem a ASTRID, který stanovuje rámec pro tuto modernizaci. Vývoj nové 5G rádiové sítě bude zahájen v roce 2024, s cílem dokončit implementaci základních funkcí do roku 2026. Nová širokopásmová síť umožní bezpečný a spolehlivý přenos velkého množství dat. Tento krok zahrnuje přenos videa, využití senzorů a zlepšení situačního povědomí.

Modernizace zahrnuje hybridní model, který kombinuje infrastrukturu komerčních telekomunikačních operátorů s vlastní infrastrukturou ASTRID. Tento přístup zajišťuje vysokou míru flexibility a snižuje náklady na výstavbu nové infrastruktury. Mozek sítě, tedy její jádro, zůstane plně pod kontrolou ASTRID .

ASTRID rovněž plánuje zavedení nové generace tísňových center, která budou moci využívat moderní technologie, jako je umělá inteligence, senzory a video přenosy, což zlepší jejich proaktivní činnost a schopnost rychleji a efektivněji reagovat na incidenty. Pilotní projekty pro tato nová centra by měly být zahájeny v roce 2025, s plným nasazením plánovaným do roku 2027.

8.3.2 Klíčové služby ASTRID

ASTRID poskytuje klíčové služby, které jsou nezbytné pro efektivní fungování veřejných bezpečnostních složek v Belgii.

8.3.2.1 Radiokomunikace

Radiokomunikační systém ASTRID je navržen pro potřeby policie, hasičských sborů a záchranných služeb, využívá technologii TETRA (Terrestrial Trunked Radio). Tento evropský standard pro digitální radiokomunikaci poskytuje vysoce kvalitní hlasovou komunikaci, rychlé navázání spojení a umožňuje skupinové hovory, což je klíčové pro efektivní koordinaci při zásazích.

TETRA nabízí:

- Vysoce kvalitní hlasovou komunikaci bez šumu.
- Rychlé navázání spojení, důležité pro krizové situace.
- Skupinové hovory pro koordinaci mezi různými složkami.

Síť ASTRID pokrývá celé území Belgie s více než 520 základnovými stanicemi, což zajišťuje spolehlivou komunikaci i v odlehlých oblastech. Síť nabízí více než 99,98% dostupnost služeb, což výrazně převyšuje průmyslové standardy. Záložní systémy a generátory zajišťují nepřerušenou komunikaci během výpadků elektrické energie. Šifrování komunikace chrání proti neoprávněnému přístupu a zajišťuje důvěrnost informací. ASTRID umožňuje přímou komunikaci mezi různými bezpečnostními a záchrannými složkami, což zajišťuje efektivní koordinaci během zásahů a rychlejší reakci na krizové situace.

Radiokomunikační systém ASTRID nabízí také:

- Datové služby pro přenos krátkých datových zpráv (SDS).
- GPS sledování pro monitorování polohy jednotek.
- Prioritizaci hovorů během vysokého zatížení sítě, upřednostňující hovory záchranných složek.

Radiokomunikační systém ASTRID tak poskytuje robustní, spolehlivou a bezpečnou platformu pro všechny složky zapojené do veřejné bezpečnosti v Belgii.

8.3.2.2 Paging

Pagingový systém ASTRID je kritickým nástrojem pro rychlou a efektivní komunikaci v krizových situacích. Tento systém je navržen tak, aby umožňoval zasílání výstražných zpráv hasičům, zdravotnickým službám a dalším složkám civilní ochrany. Díky pagingovému systému mohou být výstražné zprávy okamžitě odeslány, což je klíčové pro rychlou reakci na mimořádné události. Síť paging pokrývá celé území Belgie, což zajišťuje, že zprávy mohou být doručeny i v odlehlých oblastech. Denně je prostřednictvím systému odesíláno více než 6 400 pagingových zpráv, což ukazuje na jeho spolehlivost a kapacitu.

Pagingový systém ASTRID umožňuje odesílání zpráv velkému počtu uživatelů současně, což je důležité pro koordinaci při rozsáhlých zásazích. V krizových situacích jsou výstražné zprávy upřednostňovány, což zajišťuje, že kritické informace jsou doručeny včas. Systém je také integrován s ostatními komunikačními systémy ASTRID.

Bezpečnost a spolehlivost jsou klíčovými aspekty pagingového systému. Stejně jako ostatní systémy ASTRID je i pagingový systém vybaven záložními bateriemi a generátory, což zajišťuje jeho nepřerušený provoz i během výpadků elektrické energie. Výstražné zprávy jsou šifrovány, aby byla zajištěna jejich bezpečnost a ochrana proti neoprávněnému přístupu. Tento robustní a spolehlivý systém je tedy nezbytným prvkem v infrastruktuře pro veřejnou bezpečnost, který významně přispívá k efektivitě a úspěchu zásahových operací.

8.3.2.3 Tísňové centrály (Noodcentrales)

Tísňové centrály (Noodcentrales) jsou součástí systému ASTRID a hrají roli v přijímání a zpracovávání tísňových volání. Tato krajská střediska, která zpracovávají tísňová volání na čísla 100, 101 a 112, jsou technicky vybavena a softwarem podporována tak, aby zajistila efektivní a rychlou reakci na mimořádné události. Centrály jsou odpovědné za přijetí tísňových hovorů a vysílání záchranných jednotek na místo incidentu.

Technické vybavení tísňových center zahrnuje moderní komunikační technologie, které umožňují rychlé a spolehlivé spojení s jednotkami v terénu. To zahrnuje nejen hlasovou komunikaci, ale i přenos dat a lokalizační služby, které pomáhají operátorům přesně určit polohu volajícího a nasměrovat pomoc na správné místo. Modernizace těchto center je neustálým procesem, který zahrnuje integraci nových technologií a systémů.

Nová generace tísňových center, která je v plánu, bude schopna využívat pokročilé technologie, jako je umělá inteligence a video přenosy. Tyto technologie umožní operátorům nejen přijímat a zpracovávat hovory, ale také analyzovat situace v reálném čase a poskytovat přesnější a rychlejší instrukce jednotkám v terénu. Pilotní projekty pro tato nová centra by měly být zahájeny v roce 2025, s plným nasazením plánovaným do roku 2027.

8.3.2.4 Mobilní širokopásmová data

Tato služba je poskytována prostřednictvím Blue Light Mobile, speciálního mobilního operátora zaměřeného na potřeby veřejné bezpečnosti. Blue Light Mobile využívá infrastrukturu komerčního operátora Proximus a nabízí prioritizované připojení pro záchranné a bezpečnostní složky. To znamená, že v případě přetížení sítě mají uživatelé Blue Light Mobile přednostní přístup k síťovým zdrojům, což je zásadní pro zajištění nepřetržitého a spolehlivého přenosu dat během krizových situací.

Mobilní širokopásmová data umožňují záchranným složkám přístup k internetu, datovým službám a aplikacím. Patří sem například:

Přenos videa v reálném čase: Umožňuje sdílení živých obrazů z místa zásahu, což je důležité pro situační povědomí a rozhodování.

Přístup k databázím a informačním systémům: Záchranné složky mohou v reálném čase získávat potřebné informace, jako jsou lékařské záznamy, plány budov nebo registr vozidel.

GPS a lokalizační služby: Pomáhají sledovat polohu jednotek v terénu a koordinovat jejich pohyb.

Blue Light Mobile je také navržen tak, aby byl odolný vůči výpadkům a poskytoval nepřetržitou službu i za nepříznivých podmínek. Síť je podporována záložními systémy a její infrastruktura je pravidelně udržována a aktualizována, aby splňovala nejvyšší standardy bezpečnosti a spolehlivosti.

8.3.2.5 Mobilní přístup k datům (ISLP)

Mobilní přístup k datům prostřednictvím Integrovaného systému lokalizace a přístupu (ISLP) je zásadní součástí systému ASTRID a umožňuje záchranným a bezpečnostním složkám přístup k důležitým informacím přímo v terénu, což zvyšuje efektivitu operací.

ISLP poskytuje mobilním jednotkám, jako jsou policie, hasiči a zdravotnické týmy, přístup k centrálním databázím a informačním systémům prostřednictvím mobilních datových terminálů (MDT). Tyto terminály jsou vybaveny technologií umožňující rychlý a bezpečný přenos dat.

Jedním z hlavních přínosů ISLP je možnost přístupu k důležitým informacím, jako jsou lékařské záznamy, plány budov, registr vozidel nebo kriminální záznamy. Tento přístup umožňuje jednotkám v terénu rychle získat potřebné údaje pro rozhodování a koordinaci zásahů. Například zdravotnické týmy mohou mít přístup k lékařským záznamům pacientů, což jim umožňuje poskytovat cílenou a efektivní péči na místě.

ISLP také podporuje GPS sledování, které umožňuje sledování polohy jednotlivých jednotek v terénu. Tato funkce je klíčová pro operační centra, která mohou monitorovat rozmístění a pohyb jednotek a efektivně řídit jejich nasazení. GPS sledování také přispívá k bezpečnosti zasahujících jednotek tím, že poskytuje přehled o jejich aktuální poloze a umožňuje rychlou reakci v případě nouze.

Dalším významným přínosem ISLP je jeho integrace s desktopovými aplikacemi prostřednictvím RDP (Remote Desktop Protocol). Tento přístup umožňuje mobilním jednotkám využívat stejné aplikace a systémy, které mají k dispozici na svých stacionárních pracovních stanicích. Tím se zajišťuje konzistence a dostupnost informací bez ohledu na místo, kde se jednotka nachází.

ISLP je navržen s důrazem na bezpečnost a spolehlivost. Veškerá komunikace a přenos dat jsou šifrovány, aby byla zajištěna ochrana citlivých informací proti neoprávněnému přístupu. Zároveň je systém vybaven záložními mechanismy, které zajišťují nepřerušený provoz i během technických problémů nebo výpadků elektrické energie.

8.3.3 Legislativa

Legislativní rámec týkající se zavedení a provozu systému ASTRID je klíčový pro zajištění jeho spolehlivosti, bezpečnosti a efektivity. Následující dokumenty tvoří základ tohoto rámce:

Zákon ze dne 8. června 1998 o radiokomunikacích pro pohotovostní a bezpečnostní služby (Loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité)

Tento zákon je základním právním dokumentem, který stanovuje obecný rámec pro vznik a fungování systému ASTRID. Definuje sociální cíl ASTRID, přiděluje specifické frekvenční pásmo, ustanovuje dohled a monitorování finanční situace systému. Zajišťuje, že ASTRID plní svůj veřejný závazek a podporuje fungování záchranných a bezpečnostních složek v Belgii.

Královský dekret stanovující čtvrtou správní smlouvu ASTRID (2023-2027) (Arrêté royal fixant le quatrième contrat de gestion d'ASTRID (2023-2027))

Královský dekret je legislativní akt, který formálně schvaluje smlouvu o správě mezi ASTRID a belgickou vládou na období 2023-2027. Tento dekret poskytuje smlouvě právní základ a závaznost. Stanovuje specifické povinnosti ASTRID, jako je údržba a modernizace infrastruktury, zajištění bezpečnosti a spolehlivosti služeb a podpora interoperability s jinými systémy.

Smlouva o správě 2023-2027 (Contrat de gestion 2023-2027)

Smlouva o správě 2023-2027 je detailní operativní dokument, který specifikuje povinnosti, práva a závazky mezi ASTRID a belgickou vládou pro uvedené období. Tato smlouva poskytuje jasný a transparentní rámec pro fungování, financování a rozvoj systému ASTRID. Je klíčovým nástrojem pro zajištění efektivní a bezpečné komunikace mezi různými složkami veřejné bezpečnosti.

Královský dekret týkající se financování a investičního rámce pro ASTRID (Arrêté royal concernant le financement et le cadre d'investissement pour ASTRID)

Královský dekret týkající se financování a investičního rámce pro ASTRID je základním dokumentem, který specifikuje finanční a investiční mechanismy pro zajištění dlouhodobé udržitelnosti a rozvoje systému ASTRID. Tento dekret poskytuje stabilní a předvídatelný finanční rámec, který umožňuje ASTRID efektivně plánovat a realizovat dlouhodobé investiční projekty, čímž přispívá k zajištění bezpečné a spolehlivé komunikace pro veřejné bezpečnostní složky v Belgii.

8.3.3.1 Zákon ze dne 8. června 1998 o radiokomunikacích pro pohotovostní a bezpečnostní služby

Zákon ze dne 8. června 1998 o radiokomunikacích pro pohotovostní a bezpečnostní služby (Loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité) je klíčovým právním předpisem, který vytvořil právní základ pro vznik a fungování systému ASTRID (All-round Semi-cellular Trunking Radio communication system with Integrated Dispatchings).

Tento zákon má několik hlavních funkcí a ustanovení:

Vytvoření ASTRID

Zákon stanovuje vytvoření ASTRID jako národního operátora pro komunikaci záchranných a bezpečnostních služeb v Belgii. Federální investiční společnost (Federale Investeringsmaatschappij/Société Fédérale d'Investissement) byla pověřena založením ASTRID. Tím se vytvořil institucionální rámec pro centralizaci a řízení komunikace mezi různými složkami veřejné bezpečnosti a dalšími klíčovými organizacemi.

Sociální cíl ASTRID

Zákon definuje sociální cíl ASTRID, který zahrnuje poskytování spolehlivých a bezpečných komunikačních služeb pro pohotovostní a bezpečnostní složky v Belgii. ASTRID má za úkol zajistit, aby tyto složky měly k dispozici vysoce kvalitní komunikační nástroje potřebné pro efektivní koordinaci a reakci v případě krizových situací. Složení představenstva ASTRID je rovněž stanoveno zákonem, což zahrnuje zástupce různých veřejných a soukromých institucí, aby byla zajištěna široká škála odborných znalostí a zkušeností. Zákon také řeší otázky týkající se kapitálu a financování.

Přidělení frekvenčního pásma

Jedním z klíčových prvků zákona je přidělení specifického frekvenčního pásma 380-385/390-395 MHz pro použití systémem ASTRID. Tento frekvenční rozsah je vyhrazen výhradně pro bezpečnostní komunikaci, což zajišťuje nezávislost a kvalitu přenosu dat a hlasu.

Dohled nad ASTRID

Zákon ustanovuje, že dohled nad ASTRID vykonávají ministr vnitra a ministr financí. Tento dohled zahrnuje sledování provozní efektivity a finanční stability systému ASTRID. Ministři jsou odpovědní za zajištění toho, aby ASTRID plnila své cíle a poskytovala vysokou úroveň služeb pro veřejné bezpečnostní složky.

Monitorování finanční situace

Finanční situaci ASTRID, roční účetní závěrky a zákonnost společnosti monitoruje skupina komisařů. Tito komisaři mají za úkol zajišťovat transparentnost a odpovědnost v řízení finančních prostředků ASTRID. Mechanismus kontroly je důležitý pro udržení důvěry veřejnosti a zajištění, že prostředky jsou využívány efektivně a v souladu s právními předpisy. Skupina komisařů pravidelně hodnotí finanční zdraví ASTRID a poskytuje zprávy ministrům vnitra a financí. Zprávy zahrnují analýzy finančních výsledků, identifikaci potenciálních rizik a doporučení pro zlepšení finančního řízení.

Další ustanovení zákona

Kromě výše uvedených klíčových bodů zákon také obsahuje ustanovení týkající se spolupráce mezi ASTRID a dalšími veřejnými a soukromými subjekty. Například integraci s jinými komunikačními systémy a zajištění interoperability na národní i mezinárodní úrovni. Zákon rovněž stanovuje rámec pro ochranu osobních údajů a bezpečnost komunikace. ASTRID musí splňovat přísné standardy ochrany dat a zajistit, že veškerá komunikace je bezpečná a chráněná proti neoprávněnému přístupu.

Celkově zákon o radiokomunikacích pro pohotovostní a bezpečnostní služby poskytuje komplexní právní rámec pro vytvoření, řízení a rozvoj systému ASTRID. Tento zákon přispívá k efektivní a bezpečné komunikaci mezi záchrannými a bezpečnostními složkami v Belgii, čímž zajišťuje lepší koordinaci a rychlejší reakci na krizové situace, což je klíčové pro ochranu a bezpečnost občanů.

8.3.3.2 Královský dekret stanovující čtvrtou správní smlouvu ASTRID (2023-2027)

Královský dekret stanovující čtvrtou správní smlouvu ASTRID (Arrêté royal fixant le quatrième contrat de gestion d'ASTRID) pro období 2023-2027 je klíčovým legislativním dokumentem, který oficiálně schvaluje a uvádí v platnost smlouvu o správě mezi ASTRID a belgickou vládou. Tento dekret poskytuje právní základ a závaznost pro operativní a finanční rámec, ve kterém ASTRID funguje.

Hlavní cíle a povinnosti

Zajištění služeb: Královský dekret stanovuje, že ASTRID musí poskytovat řadu specifických služeb zaměřených na podporu veřejné bezpečnosti. Služby zahrnují údržbu a modernizaci komunikační infrastruktury, zajištění spolehlivosti a bezpečnosti služeb a podporu interoperability s jinými národními i mezinárodními systémy. ASTRID je povinný zajistit, aby všechny její systémy byly neustále aktualizovány a připraveny čelit novým technologickým a bezpečnostním výzvám.

Modernizace infrastruktury: Dekret klade důraz na modernizaci a rozšíření komunikační infrastruktury. Zvláštní pozornost je věnována přechodu na širokopásmové technologie, jako je 4G a 5G, které umožňují vyšší kapacitu a rychlost datového přenosu. Investice do těchto technologií jsou nezbytné pro zajištění, že ASTRID může poskytovat vysoce kvalitní služby, které odpovídají současným požadavkům veřejné bezpečnosti.

Bezpečnost a spolehlivost: Zajištění bezpečnosti a spolehlivosti služeb je dalším aspektem dekretu. ASTRID musí implementovat pokročilé bezpečnostní opatření k ochraně proti kybernetickým hrozbám a zajistit nepřetržitou dostupnost služeb, zejména během krizových situací. To zahrnuje pravidelné testování a aktualizaci bezpečnostních protokolů, školení personálu a spolupráci s dalšími bezpečnostními organizacemi.

Financování

Roční financování: Dekret stanovuje mechanismy pro roční financování provozních nákladů. Belgická vláda vyčlenila roční dotaci ve výši 46,5 milionu EUR pro rok 2023 a pro každý následující rok až do roku 2027. Prostředky jsou určeny na údržbu systému, provozní náklady a další nezbytné výdaje, které zajišťují hladké fungování systému ASTRID.

Investiční projekty: Investiční projekty jsou financovány prostřednictvím předfinancování z vlastních zdrojů ASTRID, přičemž celková částka je následně pokryta ročními předplatnými uživatelů. Hodnota investiční činnosti ASTRID krytá příjmy z předplatného činí 117 milionů EUR. Tento model financování umožňuje flexibilní a dlouhodobě udržitelné investice do infrastruktury a technologií.

Sledování a vyhodnocování výkonu

Dekret stanovuje jasné mechanismy pro sledování a vyhodnocování výkonu ASTRID. To zahrnuje pravidelné zprávy o provozní a finanční situaci, které musí být předkládány dohledu a vládním orgánům. Systém monitoringu zajišťuje, že ASTRID plní své cíle efektivně a transparentně.

Transparentnost a odpovědnost

ASTRID je povinný pravidelně informovat veřejnost a uživatele o svých aktivitách a výkonech, což zahrnuje veřejné správy a konzultace s klíčovými zainteresovanými stranami.

Flexibilita a adaptabilita

Královský dekret také zajišťuje, že ASTRID má dostatečnou flexibilitu a schopnost se přizpůsobit měnícím se podmínkám a požadavkům. Zahrnuje možnost aktualizace smlouvy v průběhu jejího trvání na základě nových technických nebo provozních potřeb.

8.3.3.3 Smlouva o správě 2023-2027 (Contrat de gestion 2023-2027)

Smlouva o správě 2023-2027 (Contrat de gestion 2023-2027) je detailní operativní dokument, který upravuje vztahy mezi ASTRID, belgickou vládou a koncovými uživateli. Tato smlouva poskytuje jasný a transparentní rámec pro fungování, financování a rozvoj systému ASTRID během uvedeného období. Je klíčovým nástrojem pro zajištění efektivní a bezpečné komunikace mezi různými složkami veřejné bezpečnosti.

Smlouva definuje specifické služby, které musí ASTRID poskytovat. Tyto služby zahrnují:

Údržba a modernizace infrastruktury: ASTRID musí zajistit pravidelnou údržbu a modernizaci své komunikační infrastruktury, aby byla zajištěna její spolehlivost a výkon. To zahrnuje jak fyzickou infrastrukturu, jako jsou základnové stanice, tak softwarové systémy.

Zajištění bezpečnosti a spolehlivosti služeb: Bezpečnost a spolehlivost jsou klíčovými aspekty provozu ASTRID. Smlouva stanovuje, že ASTRID musí implementovat opatření k ochraně proti kybernetickým hrozbám a zajistit nepřetržitou dostupnost služeb, zejména během krizových situací.

Podpora interoperability: ASTRID je povinný zajistit interoperabilitu svého systému s jinými národními a mezinárodními komunikačními systémy. To zahrnuje technickou kompatibilitu a spolupráci s ostatními operátory a organizacemi, které se podílejí na veřejné bezpečnosti.

Smlouva detailně popisuje mechanismy financování, které zahrnují:

Roční financování provozních nákladů: Roční financování provozních nákladů (údržba systému a provozní náklady) je zajištěno prostřednictvím dotace z rozpočtu Ministerstva vnitra v rámci celkového rozpočtu. Belgická vláda vyčlenila roční dotaci ve výši 46,5 milionu EUR pro rok 2023 a každého z následujících čtyř let.

Investiční projekty: Investiční projekty jsou financovány prostřednictvím předfinancování z vlastních zdrojů ASTRID, přičemž celková částka je pokryta ročními předplatnými uživatelů. Hodnota investiční činnosti ASTRID krytá příjmy z předplatného činí 117 milionů EUR.

Technické požadavky:

Smlouva stanovuje technické standardy a požadavky na infrastrukturu, bezpečnost a interoperabilitu. ASTRID musí zajistit, že její systémy splňují vysoké standardy kvality a bezpečnosti, aby byly schopny efektivně podporovat pohotovostní a bezpečnostní složky.

Monitorování a hodnocení výkonu:

Smlouva obsahuje mechanismy pro sledování a vyhodnocování výkonu ASTRID – pravidelné zprávy o provozní a finanční situaci, které musí být předkládány dohledu a vládním orgánům.

Transparentnost a odpovědnost:

Transparentnost a odpovědnost jsou klíčovými zásadami fungování ASTRID. Smlouva vyžaduje, aby ASTRID pravidelně informovala veřejnost a uživatele o svých aktivitách a výkonech. To zahrnuje veřejné zprávy a konzultace se zainteresovanými stranami.

Flexibilita a adaptabilita:

Smlouva zajišťuje, že ASTRID má dostatečnou flexibilitu a schopnost se přizpůsobit měnícím se podmínkám a požadavkům. To zahrnuje možnost aktualizace smlouvy v průběhu jejího trvání na základě nových technických nebo provozních potřeb.

8.3.3.4 Královský dekret týkající se financování a investičního rámce pro ASTRID

Královský dekret týkající se financování a investičního rámce pro ASTRID (Arrêté royal concernant le financement et le cadre d'investissement pour ASTRID) je právní akt, který specifikuje finanční a investiční mechanismy potřebné pro dlouhodobou udržitelnost a rozvoj systému ASTRID. Tento dekret je klíčový pro zajištění, že ASTRID má dostatečné zdroje pro poskytování svých služeb a pro modernizaci své infrastruktury.

Dekret stanovuje mechanismy pro roční financování provozních nákladů ASTRID.

Dekret upravuje finanční rámec, který zahrnuje alokaci prostředků, zdroje financování a způsob jejich využití. Finanční rámec je navržen tak, aby zajistil stabilní a předvídatelné financování pro ASTRID.

8.4 Korea – Safe-Net

Jižní Korea vyvinula rozsáhlý systém pro ochranu veřejnosti a řešení katastrof známý jako Korea Safe-Net. Tento systém byl vytvořen na základě rozhodnutí z roku 2014, kdy se Jižní Korea rozhodla vybudovat dedikovanou mobilní širokopásmovou síť pro veřejnou bezpečnost. Hlavním důvodem pro toto rozhodnutí byla potřeba nahradit různé veřejné bezpečnostní sítě založené na různých technologiích, jako jsou analogové sítě, TETRA a iDEN, které nebyly interoperabilní. Cílem bylo zajistit interoperabilitu mezi všemi agenturami veřejné bezpečnosti.

Korea Safe-Net kombinuje tři LTE sítě: PS-LTE pro veřejnou bezpečnost, LTE-R pro železnice a LTE-M pro námořní uživatele. Tyto sítě sdílejí stejné frekvenční pásmo (B28 v pásmu 700 MHz). PS-LTE je plánováno pro použití 333 agenturami, které zahrnují hasiče, elektrárenské společnosti, pobřežní stráž, armádu, policii, zdravotnické služby, plynárenské společnosti a vládní úřady. Odhadovaný počet uživatelských zařízení je 240 tisíc pro PS-LTE, 10 tisíc pro LTE-R a 35 tisíc pro LTE-M.

Technologie Safe-Net byla ověřena ve dvou pilotních projektech v letech 2015-2018. Druhá fáze pilotního projektu poskytla podporu pro Zimní olympijské a paralympijské hry v Pchjongčchangu v roce 2018. Nasazení PS-LTE probíhalo ve třech fázích v letech 2018-2021. Pro provoz sítě jsou zřízena tři geograficky redundantní operační centra v různých regionech země: v Soulu, Daegu a Jeju. Tato centra poskytují jádrové služby LTE, služby MCPTT a správu sítě.

Pokrytí sítě PS-LTE bylo vybudováno pomocí dedikovaných rádiových stanic LTE (více než 17 tisíc základnových stanic). Pokrytí a kapacita dalších sítí mohou být také využity prostřednictvím sdílení sítě, včetně komerčních mobilních sítí a sítí LTE-R a LTE-M. Čtvrtým prvkem jsou nasaditelné sítě, buď založené na vozidlech, nebo přenosných řešeních. LTE-M poskytuje pokrytí až 100 km od pobřeží a LTE-R poskytuje pokrytí více než 4800 kilometrů.

Korea Safe-Net sleduje obchodní model založený na multi-aktorském dedikovaném síťovém modelu. Výstavba sítě PS-LTE byla zadána společnostem Korea Telecom (KT) a SK Telecom (SKT). KT je zodpovědná za dvě oblasti, zatímco SKT za jednu. KT byla také pověřena výstavbou operačních center. Ministerstva vlády dohlížejí na provoz sítě a služby MCPTT. Administrativa Safe-Net je sdílena mezi několika ministerstvy: Ministerstvo vnitra a bezpečnosti dohlíží na PS-LTE, Ministerstvo oceánů a rybolovu dohlíží na LTE-M a Ministerstvo země, infrastruktury a dopravy dohlíží na LTE-R. Fórum Safe-Net koordinuje výzkum, standardizaci a vládní politiky v rámci Safe-Net.

Služby PS-LTE byly zavedeny v roce 2020 a celostátní pokrytí bylo dosaženo v roce 2021. Migrace všech uživatelů veřejné bezpečnosti je plánována na období 2020-2027. Budoucí vývoj zahrnuje komunikaci mezi zařízeními a vzduch-země, IoT senzory ve veřejné bezpečnosti a postupné zavádění 5G technologie.

8.4.1 Technická infrastruktura

Technická infrastruktura Korea Safe-Net je navržena tak, aby poskytovala spolehlivou komunikaci mezi záchrannými a bezpečnostními složkami v celé zemi. Zahrnuje moderní technologie, rozsáhlé pokrytí a interoperabilitu mezi různými systémy a zařízeními.

8.4.1.1 PS-LTE technologie

Korea Safe-Net využívá Public-Safety Long Term Evolution (PS-LTE) technologii, která zajišťuje vysokorychlostní datovou a hlasovou komunikaci. PS-LTE je speciálně navržena pro potřeby veřejné bezpečnosti, poskytuje prioritu a přednostní přístup klíčovým uživatelům během mimořádných událostí.

8.4.1.2 Základní stanice a mobilní stanice

Infrastruktura sítě zahrnuje přibližně 17 000 základnových stanic, které pokrývají celé území Jižní Koreje. Kromě toho existuje kolem 200 000 mobilních stanic, včetně pevných mobilních stanic, vozidlových rádií, smartphonů a dvoucestných rádií. Základnové stanice jsou strategicky umístěny tak, aby zajistily plné pokrytí i v odlehlých a těžko přístupných oblastech. Mobilní stanice jsou vybaveny tak, aby poskytovaly spolehlivou komunikaci v terénu, a to jak během běžných operací, tak během krizových situací.

8.4.1.3 Zařízení a vybavení

Síť Korea Safe-Net využívá širokou škálu zařízení a vybavení od různých výrobců, aby zajistila robustnost a spolehlivost systému. Patří sem specializované terminály, rádiová zařízení, smartphony, vozidlové komunikační systémy a přenosné komunikační jednotky. Tato zařízení jsou navržena tak, aby splňovala specifické potřeby jednotlivých záchranných a bezpečnostních složek, a jsou pravidelně testována a certifikována, aby zajistila jejich funkčnost a kompatibilitu se systémem.

8.4.1.4 Interoperabilita a integrace

Jedním z klíčových cílů Korea Safe-Net je zajistit interoperabilitu mezi různými technologiemi a zařízeními, které jsou používány různými agenturami a organizacemi. Síť je navržena tak, aby byla možná integrace s existujícími systémy, jako jsou TETRA, iDEN, VHF, UHF a další. To zabezpečuje bezproblémovou komunikaci mezi různými složkami záchranného systému, ať už se jedná o policii, hasiče, zdravotnické záchranné služby nebo jiné agentury. Interoperabilita je zajištěna prostřednictvím standardizovaných protokolů a technologií, které zprostředkují vzájemné propojení a spolupráci mezi různými systémy.

8.4.2 Klíčové služby

8.4.2.1 Mission-Critical Push-to-Talk (MCPTT)

Jednou z nejdůležitějších služeb je Mission-Critical Push-to-Talk (MCPTT), která umožňuje rychlou a spolehlivou hlasovou komunikaci mezi záchrannými týmy. MCPTT má rychlejší odezvu než běžné LTE a je navržena tak, aby poskytovala prioritu komunikaci klíčových osob, jako jsou vedoucí krizových operací a prezident.

8.4.2.2 Skupinové volání a vysílání (GCSE a eMBMS)

Skupinové volání a vysílání (GCSE a eMBMS) umožňuje hromadnou komunikaci mezi více uživateli najednou.

8.4.2.3 Volání přes LTE (VoLTE)

Volání přes LTE (VoLTE) zajišťuje vysokou kvalitu hlasové komunikace.

8.4.2.4 Zařízení pro komunikaci mezi zařízeními (D2D)

Zařízení pro komunikaci mezi zařízeními (D2D) umožňuje přímou komunikaci mezi zařízeními, což se využívá v případě výpadků infrastruktury nebo v oblastech bez pokrytí. Služba zajišťuje, že záchranné týmy mohou komunikovat přímo mezi sebou bez nutnosti použití základnových stanic.

8.4.2.5 Přenos videa a dat v reálném čase

Korea Safe-Net umožňuje přenos videa a dat v reálném čase, což záchranným týmům dovoluje sdílet živé přenosy z místa události, mapové podklady a další důležité informace.

8.4.3 Směrnice pro aplikační služby

Směrnice pro aplikační služby v rámci Korea Safe-Net poskytují podrobný rámec pro vývoj, zavádění a aktualizaci aplikačních služeb, které mohou být využívány pro řízení katastrof a veřejnou bezpečnost.

Vývoj aplikačních služeb je zaměřen na tvorbu aplikací, které mohou být využívány různými organizacemi zapojenými do řízení katastrof a bezpečnosti. Aplikační služby jsou vyvíjeny na základě základních služeb a postupně se rozšiřují a aktualizují podle technologických pokroků a následných verzí 3GPP. Mezi typy těchto služeb patří služby zaměřené na prevenci, rychlou reakci a obnovu, jako je live streaming během krizových situací, mapové softwary pro lokalizaci a řízení kritických aktiv, a další aplikace pro monitoring a analýzu dat.

Proces implementace nových aplikačních služeb je detailně popsaný, aby bylo zajištěno, že služby budou plně funkční a bezpečné pro použití v rámci Korea Safe-Net. Organizace plánující zavedení nového zařízení nebo služby musí předložit plán a požádat o konzultaci s Ministerstvem veřejné bezpečnosti a ochrany. Před zavedením musí zařízení projít procesem technické verifikace, který zahrnuje bezpečnostní recenze a testování. Testování probíhá na zkušební síti a hlavní síti, po kterém následuje vydání testovacích zpráv a certifikátu verifikace. Služby jsou pravidelně aktualizovány v souladu s technologickými inovacemi a zpětnou vazbou od uživatelů.

Všichni uživatelé mají k dispozici školení zaměřená na standardní operační postupy (SOP) a využívání komunikační sítě a jejích aplikací v krizových situacích. Technická podpora je poskytována během celého procesu zavádění a používání nových zařízení a služeb, včetně konzultací a asistence při registraci a propojení zařízení.

Ministerstvo veřejné bezpečnosti a ochrany přezkoumává plány zavedení a schvaluje propojení zařízení s hlavní sítí. Uživatelské organizace podávají žádosti o registraci a propojení zařízení, které byly ověřeny a schváleny. Verifikační agentury stanovují technické specifikace a provádějí technickou verifikaci zařízení a služeb. Tyto směrnice a postupy zajišťují, že Korea Safe-Net je připravena reagovat na všechny typy krizových situací a poskytovat spolehlivou a bezpečnou komunikační infrastrukturu.

8.4.4 Legislativa

Legislativní rámec Korea Safe-Net je zásadní pro zajištění efektivního fungování a bezpečnosti této veřejné bezpečnostní komunikační sítě. Zahrnuje různé zákony, nařízení a instituce, které dohromady vytvářejí strukturu pro správu, provoz a ochranu systému.

8.4.4.1 Právní rámec

Právní základ pro Korea Safe-Net byl ustanoven v roce 2014, kdy Jižní Korea rozhodla o vytvoření dedikované mobilní širokopásmové sítě pro veřejnou bezpečnost. Tento krok zahrnoval alokaci rádiového spektra pro potřeby veřejné bezpečnosti. Hlavním důvodem bylo sjednotit různé existující bezpečnostní sítě, které používaly různé technologie jako analogové systémy, TETRA a iDEN, a které nebyly interoperabilní.

8.4.4.2 Zákony a nařízení

Korea Safe-Net je podporována několika klíčovými právními předpisy, které poskytují pevný právní základ pro vytvoření, provoz a údržbu této kritické komunikační sítě pro veřejnou bezpečnost. Mezi hlavní právní předpisy patří:

Zákon o komunikačních sítích pro katastrofy a bezpečnost (재난안전통신망법)

Zákon, schválený v roce 2021, představuje hlavní právní rámec pro vytvoření a provoz komunikační sítě určené pro katastrofy a veřejnou bezpečnost. Stanoví povinnosti různých vládních a nevládních agentur zapojených do provozu sítě, požadavky na infrastrukturu a nezbytná bezpečnostní opatření. Zákon rovněž definuje technické a operační standardy, které musí být dodrženy.

Nařízení o provozu a používání sítě pro katastrofy a bezpečnost (재난안전통신망 운영 및 사용 규정)

Nařízení poskytuje detailní pokyny pro každodenní provoz a používání Korea Safe-Net. Obsahuje pravidla pro registraci a verifikaci nových zařízení a služeb, která budou do sítě připojena. Nařízení také stanoví procedury pro testování a certifikaci zařízení. Dále se zabývá provozními postupy, které musí být dodržovány při běžném provozu i během krizových situací.

Zákon o prevenci terorismu a ochraně veřejné bezpečnosti (국민보호와 공공안전을 위한 테러방지법)

Zákon poskytuje širší rámec pro všechny činnosti související s veřejnou bezpečností, včetně prevence terorismu a ochrany kritické infrastruktury. Definuje role a odpovědnosti různých vládních orgánů a institucí při zajišťování veřejné bezpečnosti. Zákon zahrnuje opatření na ochranu informačních a komunikačních systémů před kybernetickými hrozbami a jinými bezpečnostními riziky.

8.4.4.3 Institucionální role

Administrace Korea Safe-Net je sdílena mezi několika klíčovými ministerstvy a institucemi, které mají specifické odpovědnosti za různé aspekty této veřejné bezpečnostní sítě. Multi-institucionální přístup zajišťuje, že všechny aspekty provozu, údržby a vývoje sítě jsou důkladně pokryty a koordinovány.

Ministerstvo vnitra a bezpečnosti (MOIS) dohlíží na Public-Safety LTE (PS-LTE), což je hlavní komponenta sítě určená pro potřeby veřejné bezpečnosti. Ministerstvo je zodpovědné za celkovou správu a koordinaci provozu PS-LTE, zajišťuje, že síť splňuje všechny technické a bezpečnostní standardy, a dohlíží na integraci s dalšími složkami veřejné bezpečnosti. MOIS také zajišťuje školení uživatelů a podporu při zavádění nových zařízení a služeb do sítě.

Ministerstvo oceánů a rybolovu je zodpovědné za LTE-M, což je komponenta sítě specificky určená pro námořní komunikaci. Toto ministerstvo spravuje infrastrukturu a služby LTE-M, zajišťuje pokrytí námořních oblastí a integraci s námořními záchrannými a bezpečnostními službami. Ministerstvo oceánů a rybolovu také koordinuje bezpečnostní opatření a krizové plány pro námořní oblasti.

Ministerstvo země, infrastruktury a dopravy spravuje LTE-R, což je komponenta sítě určená pro železniční komunikaci. Toto ministerstvo dohlíží na výstavbu a údržbu železniční komunikační infrastruktury, zajišťuje integraci LTE-R s dalšími částmi Korea Safe-Net a koordinuje komunikační potřeby železniční dopravy během krizových situací.

Fórum Safe-Net je další klíčová instituce, která koordinuje výzkum, standardizaci a vládní politiky týkající se Safe-Net. Fórum sdružuje zástupce různých ministerstev, technických agentur a dalších relevantních organizací, aby zajistilo, že všechny aspekty rozvoje a provozu sítě jsou řízeny konzistentně. Fórum také zajišťuje, že nové technologie a postupy jsou v souladu s mezinárodními standardy a osvědčenými postupy, a podporuje spolupráci mezi veřejným a soukromým sektorem v oblasti vývoje a implementace nových technologií.

8.4.4.4 Bezpečnostní opatření

Bezpečnostní opatření jsou klíčovou součástí legislativního rámce Korea Safe-Net a zajišťují, že všechny součásti sítě jsou chráněny před různými hrozbami a riziky. Před zavedením jakéhokoli nového zařízení nebo služby do sítě musí proběhnout důkladná technická a bezpečnostní verifikace.

Proces verifikace začíná bezpečnostními recenzemi, které provádí Národní zpravodajská služba ve spolupráci s dalšími technickými agenturami. Tato recenze zahrnuje hodnocení potenciálních bezpečnostních hrozeb, zranitelností a rizik spojených s novým zařízením nebo službou. Následuje technická verifikace, která zahrnuje podrobné testování zařízení nebo služby, aby bylo zajištěno, že splňují všechny požadované technické a bezpečnostní standardy. Testování se provádí na zkušební síti a zahrnuje simulaci různých krizových situací, aby byla ověřena spolehlivost a účinnost zařízení nebo služby v reálných podmínkách.

Po úspěšném dokončení bezpečnostních recenzí a technické verifikace je vydán certifikát verifikace. Tento certifikát potvrzuje, že zařízení nebo služba splňují všechny požadované standardy a mohou být začleněny do sítě Korea Safe-Net. Certifikát verifikace je nezbytný pro formální schválení a propojení nového zařízení nebo služby s hlavní sítí.

Ministerstvo veřejné bezpečnosti a ochrany přezkoumává plány zavedení nových zařízení a služeb a schvaluje jejich propojení s hlavní sítí. Tento proces zajišťuje, že všechna zařízení a služby splňují přísné bezpečnostní a technické standardy, čímž se minimalizuje riziko selhání nebo zneužití systému. Ministerstvo rovněž monitoruje provoz zařízení a služeb v síti, aby byla zajištěna jejich bezpečnost a spolehlivost.

8.5 Maďarsko – Unified Digital Radio Communications System (EDR)

EDR (Egységes Digitális Rádiórendszer) je národní systém veřejné bezpečnosti v Maďarsku, který používá technologii TETRA (Terrestrial Trunked Radio). Tento systém poskytuje spolehlivou komunikaci pro širokou škálu veřejných bezpečnostních agentur, včetně Maďarské armády, Národní policie, Národní pohraniční stráže, Národního ředitelství pro prevenci katastrof,

Daňového a celního úřadu, Národního zákona o prosazování práva, Národní ambulance a Národního ředitelství pro ochranu životního prostředí a vod.

Projekt EDR byl zahájen v roce 2006 a dokončen v roce 2007, což zahrnovalo rychlou instalaci celonárodní sítě během jednoho roku a jednoho dne. Modernizace této sítě začala v roce 2013, s dalšími upgrady, které proběhly v roce 2016. Hlavní komponenty této sítě zahrnují 4 přepínače a 300 základnových stanic TETRA, které zabezpečují komunikaci pro více než 42 000 rádií a chrání přibližně 10 milionů obyvatel.

8.5.1 Pro-M Zrt. a budoucí síť PPDR

Pro-M Zrt., vedoucí inovátor v oblasti telekomunikačních technologií a poskytovatel komunikačních služeb pro pohotovostní služby v Maďarsku, oznámil pokročilý vývoj v oblasti sítí pro veřejnou ochranu a pomoc při katastrofách. Od roku 2020 se Pro-M Zrt. soustředí na plánování budoucích širokopásmových systémů, které jsou přizpůsobeny potřebám nouzových situací.

Hlavním cílem Pro-M Zrt. je vytvořit širokopásmovou datovou a video komunikaci, což zahrnuje přechod od současné sítě EDR založené na technologii TETRA k novým širokopásmovým řešením. Cílem je dosáhnout 99,99% dostupnosti infrastruktury, přičemž úplné pokrytí obyvatelstva je plánováno na konec roku 2024, s celonárodním pokrytím do roku 2026.

Pro-M Zrt. také plánuje zavést aplikace a služby, které zvýší efektivitu komunikace a správy v nouzových situacích, včetně nástrojů pro lokalizaci a řízení nasazení. Mezi hlavní patří MCX, aplikace pro kritickou hlasovou a video komunikaci, která umožňuje bezpečnou a vysoce dostupnou skupinovou komunikaci. Společnost se také připravuje na přechod na 5G technologie jako součást EU projektu, což zahrnuje testování 5G aplikací v uzavřené experimentální síti podél ukrajinské hranice.

8.5.2 Legislativa

8.5.2.1 Zákon o elektronických komunikacích (Elektronikus Hírközlési Törvény)

Zákon o elektronických komunikacích v Maďarsku poskytuje komplexní rámec pro správu rádiového spektra. Tento zákon hraje roli v zajištění efektivního a spravedlivého využívání rádiových frekvencí. Hlavním cílem je umožnit co nejširší a nejflexibilnější využití tohoto spektra s minimálními omezeními.

Jedním z klíčových principů tohoto zákona je technologická neutralita. To znamená, že rádiové frekvence mohou být využívány různými technologiemi bez předchozích omezení na specifické technologie. Tento přístup umožňuje zavádění nových a inovativních technologií bez potřeby změn v právním rámci, což podporuje technologický pokrok a inovace v oblasti elektronických komunikací.

Dalším důležitým principem je neutralita služeb, která umožňuje využití rádiových frekvencí pro různé druhy služeb bez specifických omezení. To poskytuje provozovatelům flexibilitu v reakci na změny v poptávce po různých typech služeb.

Zákon také klade důraz na efektivní a ekonomické využívání rádiového spektra. To zahrnuje pravidla pro přidělování frekvencí prostřednictvím aukcí a výběrových řízení, což má za cíl maximalizovat hodnotu spektra pro společnost jako celek. Transparentní a konkurenční proces přidělování frekvencí zajišťuje, že spektrum bude využíváno nejefektivnějším způsobem, což je prospěšné jak pro poskytovatele služeb, tak pro koncové uživatele.

Za správu rádiového spektra v Maďarsku je odpovědný Národní úřad pro média a infokomunikace (NMHH). NMHH zajišťuje přidělování frekvencí, dozor nad jejich využíváním a zajištění souladu s národními i mezinárodními pravidly. Kromě toho NMHH vydává dekrety a nařízení, které podrobně upravují specifické aspekty správy spektra, čímž zajišťuje, že jsou dodržovány principy stanovené zákonem o elektronických komunikacích.

8.5.2.2 Dekrety NMHH (Národní úřad pro média a infokomunikace)

NMHH Dekret č. 12/2011 (XII. 16.)

NMHH Dekret č. 12/2011, vydaný 16. prosince 2011, se zaměřuje na správu a přidělování rádiových frekvencí pro ne-civilní uživatele. Tento dekret je důležitý pro organizace zapojené do veřejné bezpečnosti a krizového řízení, jako jsou policejní a hasičské sbory, záchranné služby a další.

Dekret definuje specifická pravidla pro přidělování frekvencí ne-civilním uživatelům, což zajišťuje, že tyto frekvence jsou využívány pro účely veřejné bezpečnosti a krizového řízení. NMHH je pověřen správou těchto frekvencí a zajišťuje, že jsou dodržovány stanovené normy a předpisy – monitoring využívání frekvencí a zajištění, že nejsou rušeny jinými uživateli.

Navíc tento dekret umožňuje přidělování frekvencí pro specifické účely, jako jsou operace při přírodních katastrofách, teroristických útocích nebo jiných krizových situacích. Proces přidělování je navržen tak, aby byl rychlý a efektivní.

NMHH Dekret č. 7/2012 (I. 26.)

NMHH Dekret č. 7/2012, vydaný 26. ledna 2012, se zabývá správou frekvencí a podmínkami pro vydávání licencí pro civilní uživatele, s důrazem na aplikace veřejné bezpečnosti a pomoc při katastrofách. Upravuje podrobné postupy pro přidělování frekvencí civilním uživatelům, včetně podmínek a požadavků, které musí být splněny pro získání licencí. Tento administrativní proces zajišťuje transparentnost a spravedlnost při přidělování spektra. Specifické podmínky pro vydávání licencí zahrnují technické požadavky, provozní omezení a další kritéria, která musí být splněna.

8.5.2.3 Vládní nařízení č. 346/2010 (XII. 28.)

Vládní nařízení č. 346/2010, vydané 28. prosince 2010, je klíčovým právním předpisem, který specifikuje povinnosti a požadavky na používání systému EDR (Egységes Digitális Rádiórendszer) pro určité sektory kritické infrastruktury a vysoce rizikové závody v Maďarsku.

Nařízení vyžaduje, aby určité sektory kritické infrastruktury, jako jsou energetika, vodní hospodářství, doprava a komunikace, využívaly systém EDR pro svou interní i externí komunikaci. Používání EDR je povinné pro tyto sektory, aby byla zajištěna vysoká úroveň bezpečnosti a spolehlivosti komunikace v případě mimořádných událostí nebo krizových situací.

Nařízení stanovuje, že vysoce rizikové závody, které představují významné riziko pro veřejnou bezpečnost a životní prostředí, musí používat systém EDR pro svou komunikaci. To zahrnuje závody chemického průmyslu, rafinérie, jaderné elektrárny a další zařízení, která vyžadují zvýšenou úroveň zabezpečení a rychlou reakci v případě havárie.

Nařízení také definuje oprávnění pro velké národní poskytovatele veřejných služeb, jako jsou energetické společnosti, telekomunikační operátoři a další, k využívání systému EDR. Tyto společnosti mohou používat EDR na základě individuálního ministerského povolení, které je uděleno na základě specifických potřeb a požadavků dané společnosti, a tak i velké podniky, které hrají klíčovou roli v národním hospodářství a infrastruktuře, mají přístup k bezpečné a spolehlivé komunikační síti.

8.5.2.4 Organizace a řízení

Pro-M Zrt. je klíčovým poskytovatelem vládních komunikačních služeb v Maďarsku, odpovědným za provoz systému EDR (Egységes Digitális Rádiórendszer). Tato společnost, která je dceřinou společností NISZ Zrt., spravuje a provozuje systém EDR pod dohledem Ministerstva vnitra.

Pro-M Zrt. má na starosti zajištění, že systém EDR funguje spolehlivě a efektivně, aby mohl podporovat širokou škálu organizací zapojených do veřejné bezpečnosti a krizového řízení. Zahrnuje to koordinaci a spolupráci s různými složkami, jako jsou policie, hasiči, záchranné služby a další kritické infrastruktury.

Systém EDR je plánován k podpoře až do roku 2035, s cílem zajistit jeho dlouhodobou udržitelnost a adaptaci na nové technologické výzvy. Mezi hlavní budoucí plány patří přechod na širokopásmové datové služby, které umožní rychlejší a efektivnější přenos dat.

Dalším významným aspektem budoucího rozvoje je potenciální využití komerčních mobilních infrastruktur v hybridním modelu. Tento přístup by umožnil kombinaci veřejné a soukromé infrastruktury a zvýšit tak kapacitu a flexibilitu systému EDR. Hybridní model by také mohl přinést úspory nákladů a zlepšit dostupnost služeb v odlehlých oblastech.

8.5.2.5 Mezinárodní a evropská spolupráce

Maďarsko se při správě rádiového spektra řídí evropskými a mezinárodními standardy, díky čemuž zajišťuje harmonizaci a efektivní správu spektra pro aplikace PPDR. Tento přístup zahrnuje dodržování doporučení Evropské konference poštovních a telekomunikačních správ (CEPT) a Mezinárodní telekomunikační unie (ITU).

Evropské směrnice a rozhodnutí týkající se správy rádiového spektra jsou implementovány do národního právního rámce Maďarska. Tento proces zahrnuje přijetí a aplikaci legislativních aktů, které zajišťují, že národní předpisy jsou v souladu s evropskými požadavky. Implementace evropských směrnic zajišťuje, že Maďarsko dodržuje jednotné standardy a postup.

Dodržováním evropských a mezinárodních standardů Maďarsko zajišťuje, že jeho národní politika správy rádiového spektra je harmonizovaná s ostatními státy.

Doporučení CEPT a ITU

CEPT (Evropská konference poštovních a telekomunikačních správ) vydává doporučení a rozhodnutí, která stanovují harmonizované podmínky pro využívání rádiového spektra.

ITU (Mezinárodní telekomunikační unie) je specializovaná agentura OSN, která koordinuje globální správu rádiového spektra a vypracovává mezinárodní normy.

8.5.3 PPDR 5G projekt na maďarsko-ukrajinské hranici

Projekt 5G-PPDR (Public Protection and Disaster Relief) je zaměřen na zajištění vysoce kvalitní, bezpečné a odolné komunikace pro policii, pohraniční stráž a záchranné služby na maďarsko-ukrajinské hranici. Tento projekt, financovaný Evropskou unií, zahrnuje vývoj a implementaci širokopásmové mobilní sítě založené na technologii 5G. Hlavní cíle projektu zahrnují zajištění bezpečné komunikace, zvýšení bezpečnosti na hranicích, ekologické a klimatické přínosy a podporu digitalizace v EU.

Cílem projektu je vybudovat infrastrukturu pro 5G založenou na PPDR-BB na vnější hranici EU mezi Maďarskem a Ukrajinou. Tato síť má být odolná vůči katastrofám a zajistit bezpečnou a spolehlivou komunikaci v reálném čase pro národní ambulance, policejní a pohraniční jednotky. Projekt se zaměřuje na zvýšení bezpečnosti prostřednictvím ochrany schengenské hranice. Vzhledem k současné situaci na Ukrajině a rizikům spojeným s migrací a terorismem je tento aspekt projektu obzvláště aktuální. Projekt přispívá k ochraně životního prostředí a snižování emisí CO2 prostřednictvím přenosu reálného obrazu pomocí dronů. Zlepšuje také tok informací v případě místních přírodních katastrof a zajišťuje bezpečnější monitorování a sledování přepravy nebezpečných materiálů. PPDR 5G projekt podporuje digitalizační úsilí Evropské unie a zavádí osvědčené postupy, které mohou být využity na úrovni EU. Poskytuje širokopásmový přístup uživatelům a zvyšuje kvalitu veřejných služeb.

Výstavba sítě zahrnuje nasazení 17 základnových stanic nové generace (gNB) 5G a samostatné jádrové sítě 5G pro provoz služeb. Tyto základnové stanice a jádrová síť budou poskytovat minimální rychlosti stahování a nahrávání 3 Mbps a 2 Mbps s latencí pod 5 ms. Jádro sítě 5G bude privátní a založené na cloudových řešeních, což zajistí vysokou úroveň bezpečnosti. Aplikace vyvinuté v rámci projektu budou rovněž využívat privátní cloudová řešení.

Celkový rozpočet projektu je 5,3 milionu EUR, z toho 4 miliony EUR pochází z programu Connecting Europe Facility (CEF) Digital. Z dlouhodobého hlediska se na financování budou podílet nouzové služby, které nebudou platit poplatky díky veřejným službám.

Projekt je veden společností Pro-M Zrt., která je provozovatelem mobilní sítě a poskytovatelem telekomunikačních PPDR služeb. Mezi hlavní partnery patří IdomSoft Ltd, Národní záchranná služba, Národní policejní velitelství a Velitelství maďarských ozbrojených sil. Tito partneři budou využívat vytvořenou infrastrukturu a aplikace pro efektivnější reakci na nouzové situace a zajištění bezpečnosti.

Projekt poskytne 5G rádiové pokrytí v oblastech, které dosud nebyly pokryty, a jádrovou síť 5G. Bude nasazeno 17 základnových stanic a distribuováno 500 5G schopných chytrých zařízení. Rovněž bude vyvinuto několik aplikací pro podporu nouzových služeb. Projekt je plánován na období od 1. ledna 2023 do 31. prosince 2025.

9 Bezpečnostní hrozby

9.1 Kybernetické hrozby

Kybernetické hrozby zahrnují různé typy útoků, které mohou cílit na informační systémy a infrastruktury. Mezi nejčastější patří malware, ransomware, phishing, spear-phishing a útoky na dodavatelské řetězce. Specifické hrozby pro 5G sítě zahrnují útoky na síťovou architekturu, zneužití zranitelností v síťových protokolech a útoky typu Denial of Service (DoS).

5G sítě díky své složitější architektuře a vyšší propustnosti představují nové výzvy v oblasti kybernetické bezpečnosti. Vyšší počet zařízení připojených k síti, rozsáhlé využití softwarově definovaných sítí (SDN) a virtualizace funkcí sítě (NFV) může vést k novým zranitelnostem. Rozšíření použití IoT zařízení také zvyšuje riziko masivních botnetů, které mohou být zneužity k DDoS útokům.

9.1.1 Příklady kybernetických útoků a jejich dopad na PPDR

Ransomware útoky: Tyto útoky jsou zvláště nebezpečné pro PPDR, protože mohou zašifrovat kritická data a zablokovat přístup k důležitým systémům. Například útoky pomocí ransomwaru, jako jsou WannaCry nebo NotPetya, mohou paralyzovat infrastrukturu a vyžadovat vysoké výkupné za obnovení přístupu.

Phishing a spear-phishing: Tyto techniky sociálního inženýrství často cílí na zaměstnance s cílem získat přístupové údaje nebo infikovat systémy malwarem. Phishingové kampaně, které jsou čím dál sofistikovanější, mohou vést k únikům citlivých dat nebo kompromitaci interních sítí.

DDoS útoky: Útoky typu Distributed Denial of Service (DDoS) mohou přetížit servery a sítě, což vede k nedostupnosti služeb. V kontextu PPDR mohou DDoS útoky zabránit komunikaci a koordinaci mezi záchrannými složkami během krizových situací .

9.1.2 Opatření a technologie na ochranu proti kybernetickým hrozbám

Pro ochranu proti kybernetickým hrozbám je nutné implementovat komplexní sadu opatření a technologií, které zahrnují:

Zabezpečení síťové infrastruktury: Použití pokročilých firewallů, intrusion detection/prevention systémů (IDS/IPS) a šifrování komunikace jsou základními prvky zabezpečení. Implementace segmentace sítě a použití VPN pro zabezpečení komunikace mezi jednotlivými komponenty sítě může výrazně snížit riziko útoků .

Monitoring a detekce hrozeb: Proaktivní monitoring s využitím SIEM (Security Information and Event Management) systémů umožňuje včasnou detekci a reakci na podezřelé aktivity. Analýza síťového provozu a analýza mohou pomoci odhalit anomálie indikující probíhající útok.

Ochrana koncových zařízení: Nasazení antivirového a antimalwarového softwaru na koncové stanice a servery, pravidelné aktualizace a patchování systémů jsou klíčové pro minimalizaci zranitelností. Použití EDR (Endpoint Detection and Response) řešení poskytuje lepší kontrolu a ochranu proti pokročilým hrozbám.

Vzdělávání a školení: Pravidelná školení zaměstnanců zaměřená na rozpoznávání phishingových útoků a bezpečné chování při používání IT technologií jsou nezbytná pro snížení rizika.

Redundance a zálohování: Implementace redundantních systémů a pravidelné zálohování dat zajišťují kontinuitu provozu a rychlé obnovení činnosti po kybernetickém incidentu. Zálohy by měly být uloženy offline, aby byly chráněny proti ransomware útokům.

Spolupráce a sdílení informací: Spolupráce mezi veřejným a soukromým sektorem, sdílení informací o aktuálních hrozbách a incidentech je klíčové pro efektivní reakci na kybernetické útoky. V rámci ČR zajišťuje tuto spolupráci NÚKIB spolu s dalšími orgány a organizacemi.

9.2 Teroristické útoky

Teroristické útoky mohou mít formu fyzických útoků na infrastrukturu, kybernetických útoků na kritické systémy nebo kombinaci obojího. V souvislosti s PPDR jsou cílem teroristických hrozeb zejména komunikační sítě, energetické zdroje, zdravotnická zařízení a další prvky infrastruktury, které jsou nezbytné pro efektivní reakci na krizové situace.

9.2.1 Příklady teroristických útoků na komunikační infrastrukturu

Kybernetické útoky: Útoky na komunikační sítě a infrastrukturu zahrnují například útoky typu Denial of Service (DoS) a Distributed Denial of Service (DDoS), které mohou vyřadit klíčové komunikační kanály z provozu.

Fyzické útoky: Příklady fyzických útoků zahrnují bombové útoky na telekomunikační centra nebo sabotážní akce proti infrastruktuře, jako jsou vysílače a datová centra. Tyto útoky mohou způsobit rozsáhlé výpadky komunikačních služeb a ohrozit bezpečnost občanů.

9.2.2 Prevence a reakce na teroristické hrozby

Prevence a reakce na teroristické hrozby vyžaduje komplexní a koordinovaný přístup zahrnující několik opatření:

Monitoring a analýza: Prvním krokem je kontinuální monitoring a analýza potenciálních hrozeb. To zahrnuje sledování online aktivit, identifikaci radikalizovaných jedinců a skupin a analýzu informací z různých zdrojů. Důležité je také proškolení bezpečnostního personálu v metodách identifikace a hlášení podezřelých aktivit.

Zabezpečení infrastruktury: Implementace fyzických i kybernetických bezpečnostních opatření je klíčová. Patří sem například zpevnění a ochrana kritických zařízení, instalace pokročilých bezpečnostních systémů a pravidelná aktualizace softwaru a hardwaru.

Spolupráce a komunikace: Je nutná efektivní komunikace a spolupráce mezi bezpečnostními složkami, veřejností a relevantními subjekty.

Legislativa a regulace: Zavedení legislativních opatření, která umožní rychlou a efektivní reakci na teroristické hrozby. To zahrnuje například Nařízení Evropského parlamentu a Rady o potírání šíření teroristického obsahu online, které se zaměřuje na rychlé odstraňování teroristického obsahu z internetu a harmonizaci povinností poskytovatelů internetových služeb napříč EU.

Vzdělávání a osvěta: Pravidelné školení a vzdělávání všech relevantních aktérů, včetně veřejnosti, je klíčové pro zvýšení povědomí o teroristických hrozbách a schopnosti na ně efektivně reagovat.

9.3 Přírodní katastrofy

Přírodní katastrofy, jako jsou povodně, zemětřesení, hurikány, tornáda a lesní požáry – tyto katastrofy mohou způsobit fyzické poškození.

9.3.1 Příklady přírodních katastrof a následná reakce krizového řízení

Povodně: Povodeň v roce 2002 v České republice způsobila rozsáhlé výpadky telekomunikačních služeb, což výrazně ztížilo krizovou komunikaci a koordinaci záchranných prací. Krizové řízení se muselo spoléhat na záložní komunikační prostředky a improvizované systémy, aby zajistilo koordinaci záchranných operací.

Zemětřesení: Zemětřesení v Itálii v roce 2016 vedlo k rozsáhlému poškození infrastruktury včetně komunikačních sítí. Reakce krizového řízení zahrnovala rychlou mobilizaci záložních systémů a dočasných komunikačních prostředků, jako jsou satelitní telefony a mobilní základnové stanice.

Lesní požáry: Lesní požáry v Kalifornii v roce 2020 způsobil rozsáhlé výpadky elektrické energie a komunikačních sítí. Krizové řízení využilo dronů a mobilních komunikačních jednotek k obnovení komunikace a koordinaci evakuací a hasičských operací.

9.3.2 Environmentální bezpečnost v České republice

Environmentální bezpečnost je stav, kdy je pravděpodobnost vzniku krizové situace vyvolané narušením životního prostředí ještě přijatelná. Ve vztahu k ekosystémovým službám ji lze vymezit jako dlouhodobé udržení ekosystémových služeb určujících kvalitu lidského života. Účelem všech aktivit v environmentální bezpečnosti je propojení ochrany životního prostředí s bezpečnostními zájmy ČR. Ohroženy mohou být jednotlivé složky životního prostředí i celé ekosystémy s dlouhodobými i krátkodobými dopady. Je nutné zohlednit vzájemnou provázanost těchto rizik a vytvořit provázaný systém preventivních, mitigačních a adaptačních opatření. V ČR je gestorem této oblasti Ministerstvo životního prostředí (MŽP), které řídí strategii adaptace na změnu klimatu a strategický rámec Česká republika 2030.

9.3.3 Opatření na minimalizaci rizik a následků přírodních katastrof

Záložní a redundantní systémy: Implementace záložních systémů a redundantní infrastruktury pro zajištění kontinuity služeb – záložní napájecí zdroje, záložní servery a mobilní základnové stanice, které mohou být rychle nasazeny v případě výpadku.

Odolná infrastruktura: Stavba odolnější infrastruktury, která může lépe odolat přírodním katastrofám – použití materiálů odolných vůči vodě a zemětřesení a umístění kritických zařízení na bezpečnějších místech.

Monitorování a včasné varování: Implementace pokročilých systémů pro monitorování a včasné varování, které mohou detekovat přírodní katastrofy a umožnit rychlou reakci – senzory, drony a satelity, které poskytují aktuální data o stavu infrastruktury a přírodních podmínkách.

Školení a cvičení: Pravidelné školení a cvičení krizového řízení pro záchranné složky a další relevantní subjekty. To zajišťuje připravenost na krizové situace a zlepšuje schopnost rychle a efektivně reagovat na přírodní katastrofy.

Pro efektivní zvládnutí přírodních katastrof je nezbytné integrovat environmentální bezpečnost do krizového řízení, propojení ochrany životního prostředí s bezpečnostními zájmy České republiky.

9.4 Pandemie

Pandemie, jako například COVID-19, mají zásadní dopad na komunikační infrastrukturu a krizové řízení. Zvýšený objem komunikace, přetížení sítí a potřeba rychlého sdílení informací mezi krizovými složkami a veřejností vyžadují robustní a spolehlivé komunikační systémy. Během pandemie se stala kritickou také vzdálená práce a vzdělávání, což kladlo další nároky na kapacitu a stabilitu komunikačních sítí.

Během pandemie COVID-19 se ukázala důležitost rychlého a spolehlivého přenosu dat. Díky své vysoké rychlosti a nízké latenci, mohou 5G sítě významně přispět k efektivní krizové komunikaci. Umožňují rychlejší přenos velkých objemů dat, podporu telemedicíny, sledování kontaktů a další klíčové aplikace. Například v Jižní Koreji byly využívány 5G technologie pro sledování šíření viru a informování veřejnosti.

9.4.1 Prevence a připravenost na budoucí pandemie

Pro prevenci a připravenost na budoucí pandemie je žádoucí implementovat následující opatření:

Posílení infrastruktury: Zajištění robustní a odolné komunikační infrastruktury, která zvládne zvýšený provoz a umožní rychlé přepínání mezi primárními a záložními systémy.

Integrace 5G technologií: Využití 5G sítí pro rychlý přenos dat, podporu telemedicíny a vzdálené práce, ásadní pro efektivní krizové řízení a reakci na pandemie.

Vývoj aplikací pro sledování a informování: Implementace aplikací a systémů pro sledování šíření infekcí, sledování kontaktů a rychlé informování veřejnosti o aktuálních opatřeních a doporučeních.

Mezinárodní spolupráce: Sdílení informací, zdrojů a technologií mezi státy a mezinárodními organizacemi pro koordinovanou reakci na globální zdravotní hrozby.

9.5 Geopolitické konflikty

V posledních letech se mezinárodní bezpečnostní prostředí výrazně zhoršilo. Klíčovým faktorem této destabilizace je ruská válečná agrese proti Ukrajině. Tento konflikt není jen bojem o svrchovanost a územní celistvost Ukrajiny, ale představuje širší ohrožení mezinárodního řádu.

Konflikty, jako je válka na Ukrajině, krize na Blízkém východě nebo nestabilita v Africe, mají zásadní dopad na globální bezpečnost. Tyto konflikty ovlivňují nejen bezpečnostní situaci v daných regionech, ale mají i širší dopady na ekonomické a politické stability po celém světě.

Vojenské zpravodajství České republiky upozorňuje na narůstající kybernetické hrozby a informační operace ze strany cizích mocností. Tyto aktivity zahrnují cílené phishingové kampaně, tvorbu polymorfního malwaru a využití velkých jazykových modelů pro šíření propagandy a dezinformací. Zvláště nebezpečné jsou deepfake videa, která mohou být využita k diskreditaci veřejně známých osob nebo k manipulaci s veřejným míněním.

9.5.1 Prevence a připravenost

Pro minimalizaci rizik a následků geopolitických konfliktů je důležitá prevence a připravenost. Česká republika se zaměřuje na pravidelné aktualizace svých bezpečnostních strategií a krizových plánů, které zahrnují identifikaci potenciálních hrozeb a vyhodnocení jejich dopadů. V rámci prevence se provádějí školení a cvičení krizového managementu, zajišťující, že všechny složky státní správy i soukromého sektoru jsou připraveny na různé scénáře krizových situací.

Zvyšování kybernetické bezpečnosti: Kybernetické hrozby představují významné riziko pro národní bezpečnost. Česká republika proto investuje do zvyšování kybernetické bezpečnosti, ochranu kritické infrastruktury, posílení kapacit kybernetické obrany a vzdělávání odborníků v oblasti kybernetické bezpečnosti. Kromě toho se vyvíjejí nové technologie a postupy pro detekci a prevenci kybernetických útoků.

Mezinárodní spolupráce: Česká republika aktivně spolupracuje s NATO, EU a dalšími mezinárodními organizacemi na sdílení informací, koordinaci obranných strategií a společném výcviku.

Posilování ekonomické odolnosti: Geopolitické konflikty mohou mít výrazné ekonomické dopady. Aby se minimalizovaly tyto následky, Česká republika se zaměřuje na diverzifikaci svých ekonomických zdrojů a posilování strategických rezerv. Investice do inovací a technologického rozvoje přispívají k udržení ekonomické stability i v časech krize. Součástí ekonomické odolnosti je také podpora domácího zbrojního průmyslu.

Vzdělávání a informování veřejnosti: Pro posílení odolnosti společnost se realizují kampaně na zvyšování povědomí o bezpečnostních otázkách, vzdělávací programy a transparentní komunikace mezi vládou a občany.

Krizové řízení a reakce na krizové situace: Efektivní krizové řízení je základem pro minimalizaci dopadů geopolitických konfliktů. Česká republika má dobře vyvinutý systém krizového řízení, který zahrnuje bezpečnostní rady, krizové štáby a stálé pracovní skupiny, které jsou zodpovědné za koordinaci reakce na krizové situace, mobilizaci zdrojů a poskytování podpory postiženým oblastem.

9.6 Pohled ČR

Bezpečnostní strategie České republiky reflektuje dynamické a komplexní hrozby, kterým naše země čelí v současném globálním prostředí. Zásadní roli v této strategii hraje nejen zajištění svrchovanosti a územní celistvosti, ale také ochrana základních práv a svobod občanů, ekonomická stabilita a odolnost společnosti vůči různým typům krizí a konfliktů.

Česká republika se nachází ve středu Evropy a její geopolitická pozice vyžaduje aktivní účast v mezinárodních organizacích, jako jsou NATO a Evropská unie, které poskytují platformu pro kolektivní obranu a bezpečnost. V kontextu aktuálních bezpečnostních výzev si Česká republika uvědomuje důležitost mezinárodní spolupráce a solidarity.

9.6.1 Bezpečnostní priority

Obrana suverenity a územní celistvosti: Česká republika klade důraz na obranu svého území prostřednictvím modernizace ozbrojených sil a účasti v kolektivní obraně NATO.

Kybernetická a informační bezpečnost: S narůstajícím počtem kybernetických útoků a dezinformačních kampaní se Česká republika zaměřuje na posilování kybernetické bezpečnosti a ochranu kritických informačních systémů.

Ekonomická odolnost: Česká republika usiluje o diversifikaci svých dodavatelských řetězců a zajištění energetické bezpečnosti prostřednictvím investic do obnovitelných zdrojů a strategických rezerv.

Ochrana obyvatelstva a krizové řízení: Česká republika investuje do modernizace záchranných složek a zlepšování koordinace mezi jednotlivými aktéry krizového řízení.

Jedním z klíčových aspektů bezpečnostní strategie je propojení služeb armády a Ministerstva vnitra. V tomto ohledu hraje významnou roli Ředitelství služeb informačních a komunikačních systémů Ministerstva obrany (Ř SKIS MO), které funguje jako digitální zmocněnec Ministerstva obrany. Toto propojení umožňuje efektivní sdílení informací a zdrojů mezi ozbrojenými silami a civilními složkami krizového řízení.

9.7 Pohled EU

Evropská unie považuje geopolitické konflikty za významnou hrozbu pro bezpečnost a stabilitu v regionu a klade důraz na kolektivní obranu a spolupráci mezi členskými státy, aby čelila těmto výzvám apodporuje rozvoj obranných kapacit členských států prostřednictvím investic do moderních technologií a výzkumu.

Speciální pozornost je věnována kybernetické bezpečnosti, což je oblast, kde EU stanovila řadu iniciativ a standardů. Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) podporuje členské státy při zlepšování jejich kybernetické obrany a při vytváření společných bezpečnostních standardů pro technologie, jako je 5G. V rámci spolupráce s mezinárodními partnery, jako jsou NATO a OSN, EU rovněž usiluje o posílení globální bezpečnostní architektury.

9.7.1.1 NATO

Ve vztahu k veřejné ochraně a pomoci při katastrofách má Evropská unie a NATO klíčovou úlohu v zajišťování bezpečnosti a koordinaci efektivní reakce na krizové situace

Evropská unie využívá spolupráci s NATO k posílení své schopnosti reagovat na bezpečnostní hrozby a mimořádné události. Díky této spolupráci dochází ke sdílení informací, společnému plánování a výcviku, což vede k efektivní mobilizaci zdrojů a zajištění potřebné pomoci během krizových situací.

NATO rovněž přispívá k zajištění regionální stability a bezpečnosti v Euro-Atlantické oblasti, včetně podpory krizového řízení a reakce na katastrofy. Organizace jako Euro-Atlantic Disaster Response Coordination Centre (EADRCC) poskytují platformu pro koordinaci mezinárodní pomoci a podporu v případě katastrof, včetně činností souvisejících s PPDR.

Jedním z aspektů spolupráce mezi EU a NATO je harmonizace frekvenčních pásem a standardizace komunikačních technologií pro PPDR. Rezoluce ITU-R 646 (REV.WRC 15) nabádá administrativy, aby identifikovaly a harmonizovaly frekvenční pásma pro pokročilá řešení PPDR. Doporučuje využití frekvenčních pásem 380-470 MHz a 694-894 MHz, s preferovaným pásmem 380-385/390-395 MHz pro trvalé aktivity ochrany obyvatelstva.

Lisabonská smlouva, konkrétně článek 196, výrazně podporuje spolupráci v oblasti civilní ochrany a PPDR. Tento článek napomáhá spolupráci mezi členskými státy EU a partnery, jako je NATO, s cílem zlepšit schopnost reagovat na katastrofy a zajistit bezpečnost obyvatel. Díky Lisabonské smlouvě se daří efektivně koordinovat a sdílet zdroje mezi EU a NATO.

10 Aplikační možnosti

Ve světě mobilních komunikačních systémů existují tři hlavní kategorie použití, které se liší podle cílů uživatelů a odpovídajících konfiguračních požadavků (z hlediska koncových uživatelských zařízení, technologie, funkcí sítě, charakteristik, standardizace atd.). Komerční segment cílí na komerční uživatele pro jejich každodenní komunikační potřeby. Na druhém konci spektra se nachází kritické systémy, zahrnující především Business Critical a Mission Critical systémy, které vyžadují mobilní radiové systémy schopné poskytovat bezpečnou a spolehlivou komunikaci v nejextrémnějších nebo specifických podmínkách.

Business Critical systémy obecně slouží organizacím, které operují v prostředí s vysokou ekonomickou hodnotou a/nebo s citlivými informacemi.

Mission Critical systémy byly navrženy pro akce, kde selhání může mít za následek vážné bezpečnostní nebo zabezpečovací škody, zranění, ztrátu života nebo by významně poškodilo společnost nebo životní prostředí. Jejich uživateli jsou převážně aktéři PPDR.

Hlavním cílem kritických systémů obecně je zajistit účinnost a efektivitu systémů v kritických situacích. Mission Critical systémy mají jádro v bezpečnosti a zabezpečení společnosti, což znamená, že ziskovost je odsunuta na druhou kolej a prioritou je veřejný zájem.

10.1 Rozdělení komunikačních systémů

10.1.1 Komerční segment

Komerční segment se zaměřuje na běžné uživatele, kteří využívají mobilní komunikační systémy pro každodenní osobní a pracovní potřeby. Tyto systémy jsou navrženy tak, aby byly ziskové, konkurenceschopné a spolehlivé ve většině situací, ale nevyžadují takovou úroveň odolnosti a bezpečnosti jako kritické systémy.

10.1.2 Kritické systémy

Kritické systémy jsou navrženy, aby poskytovaly bezpečnou a spolehlivou komunikaci v náročných podmínkách. Tyto systémy se dělí na dvě hlavní kategorie: Business Critical a Mission Critical systémy.

10.1.2.1 Business Critical systémy

Business Critical systémy slouží organizacím, které operují v prostředích, kde je ohrožena významná ekonomická hodnota nebo citlivé informace.

10.1.2.2 Mission Critical systémy

Mission Critical systémy jsou určeny pro akce, kde selhání může mít za následek vážné bezpečnostní nebo zabezpečovací škody, zranění, ztrátu života nebo významné poškození společnosti či životního prostředí. Typickými uživateli těchto systémů jsou složky PPDR. Tyto systémy jsou navrženy, aby byly maximálně spolehlivé a dostupné za všech okolností, včetně krizí a výpadků.

10.2 Rozměry kritických systémů

V zahraničí se tyto systémy rozdělují na Business Critical (BC) a Mission Critical (MC). Tabulka níže porovnává tyto kategorie. My v tomto dokumentu, v kapitole 2, rozdělujeme zásahy do pěti kategorií, přičemž kategorie 1 (Malé události) a kategorie 2 (Střední události) jsou zařazeny do BC a kategorie 3 (Velké události) až kategorie 5 (Mezinárodní události) do MC. Celý systém nám definuje požadavky na komunikační systém. V zahraničí se uvádí, že na určité typy komunikace se využívají komerční sítě, ale pro MC by měly být vyhrazené a posílené sítě.

Celý systém fungování IZS je potřeba propojit do jedné platformy nebo systému, který by umožňoval vzájemnou zastupitelnost a mohl se i doplňovat. Je možno to řešit na úrovni centra i koncového uživatele. U koncového uživatele je vhodné využít LiveU, zatímco centrální část by měla být spravována prostřednictvím CORE komunikační platformy.

Rozměry kritických systémů zahrnují několik klíčových aspektů, které určují jejich návrh, použití a výkon. Následující tabulka poskytuje přehled těchto rozměrů a porovnává systémy Business Critical (BC) a Mission Critical (MC Rozměry kritických systémů zahrnují několik klíčových aspektů, které určují jejich návrh, použití a výkon):

ROZMĚRY	BUSINESS CRITICAL (BC)	MISSION CRITICAL (MC)
DESIGNOVÉ PRINCIPY	Ziskovost, konkurenceschopnost a spolehlivost ve většině situací	Plná redundance, posílení, maximální spolehlivost, priorita a přednost
CÍLOVÁ SKUPINA	Komerční a průmyslové organizace, soukromí uživatelé	Veřejná bezpečnost a přidružené organizace
TYP SÍTĚ	Komerční sítě	Vyhrazené a posílené sítě
ŠKÁLOVATELNOST APLIKACÍ A FUNKCIONALITA	Vývoj a inovace podle tempa trhu	Potřeba standardizace před dosažením úrovně kritické pro misi
DOSTUPNOST KOMUNIKACE	V běžných nebo mírně kritických podmínkách	Za všech okolností, včetně krizí a výpadků
DOPADY V PŘÍPADĚ SELHÁNÍ	Ekonomické ztráty nebo ohrožení citlivých informací	Riziko ztráty životů a významných materiálních škod
POKRYTÍ	≤ 99,5 % populace	≥ 99,5 % území
ZÁLOŽNÍ DOBA V PŘÍPADĚ VÝPADKU ELEKTŘINY	≤ 2 hodiny	≥ 8 hodin

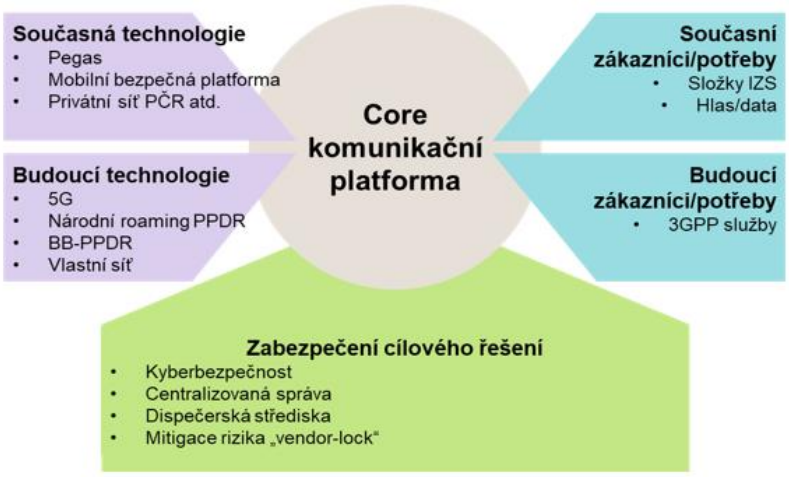
Celkově tato tabulka ilustruje, jak se požadavky na Business Critical a Mission Critical systémy liší v závislosti na jejich specifickém použití a potřebách, s důrazem na vyšší úroveň spolehlivosti, odolnosti a dostupnosti u MC systémů.

10.2.1 CORE komunikační platforma

Platforma CORE představuje prvek v rámci modernizace a zajištění robustní a bezpečné komunikační infrastruktury pro složky IZS v České republice. Vzhledem k neustále se měnícímu prostředí, technologickému pokroku a rostoucím nárokům na efektivitu a rychlost zásahů je nezbytné poskytnout složkám IZS moderní, spolehlivý a širokopásmový komunikační systém.

Platforma CORE je výsledkem komplexní analýzy potřeb a požadavků jednotlivých složek IZS, včetně Policie ČR, Hasičského záchranného sboru a Zdravotnické záchranné služby. Tato platforma má za cíl nahradit stávající, často nepropojené a zastaralé systémy, a vytvořit jednotnou a integrovanou komunikační infrastrukturu. Důraz je kladen na zvýšení kybernetické bezpečnosti, zlepšení interoperability mezi jednotlivými složkami a zajištění vysoké dostupnosti a odolnosti komunikačních prostředků i v krizových situacích.

Vznik platformy reflektuje také nezbytnost přechodu od tradičních hlasových komunikačních systémů k moderním datovým službám, které umožňují rychlou a přesnou výměnu multimediálních informačních toků. Implementace CORE je také úzce spjata s výsledky aukcí kmitočtů pro sítě 5G, které poskytují technické a legislativní základy pro rozvoj vysokorychlostních datových služeb.



Kromě zajištění bezpečné a efektivní komunikace mezi složkami IZS je důležitým aspektem i ekonomická efektivita, a to jak v oblasti investičních, tak i provozních nákladů. CORE komunikační platforma je navržena tak, aby umožnila optimalizaci stávajících zdrojů, využití moderních technologií a minimalizovala závislost na externích dodavatelích. Součástí je také zajištění interoperability a kompatibility s evropskými standardy a legislativními požadavky. Platforma CORE tak představuje nejen technologický, ale i strategický nástroj, který výrazně posiluje schopnosti a připravenost složek IZS reagovat na široké spektrum krizových situací.

10.3 Minimální požadavky na PPDR zařízení

Minimální požadavky na zařízení pro veřejnou bezpečnost a krizovou pomoc vycházejí z dokumentu "PPDR Rugged Handheld Device for Heavy Use" od NCCOM (Nordic Critical Communication Operators Meeting). Tento dokument poskytuje podrobné pokyny pro výrobce zařízení, aby porozuměli společným požadavkům uživatelů PPDR v severských zemích, a stanovuje minimální, doplňkové a budoucí požadavky na robustní ruční zařízení určená pro těžké použití v náročných podmínkách. Dokument byl vytvořen ve spolupráci PPDR operátorů v Dánsku, Finsku, Norsku, Švédsku a na Islandu a zajišťuje, že zařízení splňují vysoké standardy pro bezpečnost a spolehlivost.

Vzhledem k detailnímu nastavení a vysoké úrovni požadavků v severských zemích může tento dokument sloužit jako inspirace a referenční bod pro české mapování a implementaci podobných systémů. Cílem je zajistit, aby PPDR systémy dosáhly vysoké úrovně spolehlivosti a bezpečnosti.

10.3.1 Environmentální požadavky

Zařízení určená pro těžké použití v PPDR prostředí musí být schopná efektivně fungovat v náročných podmínkách a odolávat fyzickým hrozbám jako vlhkost, voda, prach, teplo a chlad. Zařízení musí být navržena tak, aby odolala opakovaným pádům z typických provozních výšek na tvrdé povrchy bez poškození. Dotykové obrazovky a další displeje musí být snadno čitelné za všech světelných podmínek.

10.3.2 Hardwarové specifikace

Tlačítko PTT: Zařízení musí být vybaveno dedikovaným tlačítkem push-to-talk (PTT), které je hmatatelné, snadno identifikovatelné a snadno ovladatelné, včetně možnosti ovládání v ochranných rukavicích.

Nouzové tlačítko: Zařízení musí mít dedikované nouzové tlačítko, které je hmatatelné, barevně odlišené (např. červené) a umístěné na horní části zařízení. Tlačítko musí být snadno přístupné a použitelné i v ochranných rukavicích.

Přepínač výběru hovorové skupiny: Zařízení musí být vybaveno snadno ovladatelnými tlačítky, která umožňují snadné a plynulé přepínání mezi hovorovými skupinami. Tlačítka musí být chráněna proti nechtěnému použití a ovladatelná i v ochranných rukavicích, bez potřeby vizuální pomoci.

Displej: Displej musí mít dostatečné rozlišení a velikost, aby podporoval efektivní interakci s aplikacemi MCX. Musí být odolný proti poškrábání a čitelný za jasného slunečního světla i v úplné tmě. Displej musí automaticky přizpůsobovat jas

měnícím se světelným podmínkám a umožňovat jeho vypnutí během PTT operací. Uživatelé musí být schopni ovládat dotykovou obrazovku i za mokra a v rukavicích.

Reproduktor a mikrofon: Zařízení musí obsahovat reproduktory a mikrofony, které umožňují jasnou komunikaci za všech běžných podmínek, včetně hlučného prostředí. Reproduktor/mikrofon musí být navrženy tak, aby zohledňovaly faktory jako vítr nebo hlasité sirény a zajišťovaly jasný zvuk pro účastníky hovoru, i v situacích se zapnutými sirénami. Dále musí zařízení a jeho příslušenství chránit uživatele před náhlými hlasitými zvukovými výbuchy a varovat před potenciálním nebezpečím.

Kamera: Zařízení musí být vybaveno přední kamerou s minimálním rozlišením 2 megapixely a zadní kamerou s minimálním rozlišením 8 megapixelů a bleskem. Kamery musí být schopny pořizovat vysoce kvalitní fotografie a videa s dostatečnou úrovní detailů pro identifikaci osob a objektů, jako jsou registrační značky. Kamery musí fungovat jak za denního světla, tak v podmínkách s nízkým osvětlením.

Baterie: Zařízení a jeho baterie musí být optimalizovány tak, aby:

– Duty cycle 80 % standby / 20% aktivní používání při +20 °C a–110 dBm RSRP signálu vydrželo minimálně 12 hodin při používání aplikace MCX.

– Duty cycle 80 % standby / 20% aktivní používání při -20 °C a–110 dBm RSRP signálu vydrželo minimálně 6 hodin při používání aplikace MCX.

– Po 1000 nabíjecích cyklech (20 % až 100% nabití) si baterie zachovala alespoň 85% původní kapacity.

Zařízení musí být schopno nabít se z 0 na 50 % za půl hodiny při použití vysokovýkonného rychlonabíječe. Baterie musí být snadno vyměnitelná uživatelem bez specializovaných nástrojů nebo odborných znalostí, aniž by byla narušena ochranná třída zařízení.

Konektory pro periferní zařízení: Všechny fyzické konektory pro periferní zařízení musí být vodotěsné, robustní a navržené pro těžké používání. Konektory musí poskytovat robustní, snadno použitelné a bezpečné uzamykací mechanismy, aby se zabránilo neúmyslnému odpojení. Kromě standardního konektoru USB-C jsou minimálně požadovány následující konektory:

– Audio jack (2,5 nebo 3,5 mm) s podporou PTT

– Boční nebo spodní konektor s podporou PTT, nouzového tlačítka a zvuku

– Exponované nabíjecí piny umožňující robustní nabíjení, např. pogo piny pro nabíjení v jedno – a vícedokovacích stanicích

– Bluetooth verze 5.0 nebo vyšší a NFC pro párování. Možnost blokace použití Bluetooth přes EMM. Bluetooth musí podporovat režim Secure Connections security mode 4, level 4.

Všechny konektory musí být použitelné současně, aby umožnily připojení více příslušenství, např. tělesně nositelné kamery, externí obrazovky a RSM.

10.3.3 Příslušenství

Výrobce zařízení musí být schopen poskytnout nebo podporovat několik příslušenství pro zařízení:

Jednoduché a vícedokovací stanice a nabíječky

Sluchátka s tlačítkem PTT připojená k zařízení přes boční konektor s robustním uzamykacím mechanismem, např. USB-C nebo audio jack.

Všechno příslušenství musí být vodotěsné, robustní a navržené pro těžké používání, schopné použít robustní, snadno použitelný a bezpečný uzamykací mechanismus zařízení, aby se zabránilo neúmyslnému odpojení.

10.3.4 Možnost Wi-Fi hotspotu

Zařízení musí mít schopnost fungovat jako Wi-Fi hotspot. Možnost blokace této funkce prostřednictvím EMM.

10.3.5 Komunikace zařízení se zařízením

TETRA DMO (direct-mode operation) bude používán do doby, než technologie 3GPP poskytne osvědčené řešení pro komunikaci zařízení s zařízením (D2D), a interoperabilita s PPDR TETRA DMO již nebude potřebná. Tato schopnost musí být podporována buď samotným zařízením, nebo ve spolupráci s příslušenstvím.

10.3.6 Výkon antény RF OTA

Výkon RF antény musí být co nejlepší, v souladu s kritérii RF OTA výkonu měřenými podle 3GPP TR 37.977 V17.0.0 a 3GPP TR 25.914 V17.0.0. Zařízení musí podporovat minimálně frekvenční pásma ITU Region 1 Band 8 (900 MHz), Band 20 (800 MHz), Band 28 (700 MHz), Band 3 (1800 MHz) a Band 1 (2100 MHz).

10.3.7 Bezpečnost a firmware

Zařízení musí splňovat základní úroveň bezpečnostních požadavků pro každou zemi, což je minimální úroveň požadovaná pro uživatele PPDR. Tyto požadavky jsou obvykle ekvivalentní s klasifikací RESTRICTED.

Podpora životního cyklu: Pro uživatele PPDR je důležitý dlouhý životní cyklus zařízení a schopnost poskytovat kontinuální podporu. To zahrnuje údržbu čipsetů, aktualizace firmwaru a bezpečnostní aktualizace. Aktualizace na nejnovější operační systém (OS) musí být k dispozici po celou dobu životního cyklu, spolu s nejnovějšími bezpečnostními a firmware aktualizacemi, včetně oprav chyb. Aktualizace obsahující nové funkce a opravy chyb musí být k dispozici v pravidelných intervalech. Bezpečnostní a nouzové aktualizace musí být k dispozici okamžitě. Výrobce zařízení musí poskytovat podporu pro zařízení minimálně po dobu pěti (5) let od jeho uvedení na trh.

Přístup k internetu: Zařízení musí být schopno plně fungovat bez spoléhání se na přístup k internetu během registrace nebo provozu.

Správa třetími stranami: Zařízení musí být schopno být spravováno řešením EMM třetí strany, které je instalováno na místě a může být omezeno na uzavřenou síť, tj. zcela izolované od veřejných internetových připojení, například pomocí AOSP (Android Open Source Project). Musí být možné spravovat všechny aktualizace softwaru prostřednictvím EMM.

Kontrola externích IP připojení: Pro zajištění bezpečnosti zařízení by výrobci měli poskytnout podrobné informace o odchozích připojovacích bodech během startu, aktivace a provozu zařízení atd. Tyto informace zahrnují IP adresy, názvy domén a komunikační protokoly. PPDR operátoři musí mít kontrolu nad těmito připojeními, aby mohli monitorovat, blokovat a povolit připojení podle potřeby. Bezpečnost zařízení vyžaduje spolupráci mezi výrobcem a PPDR operátorem na ochranu citlivých dat a prevenci bezpečnostních průniků.

Povolené aplikace: Pouze kritické systémové aplikace a ty, které jsou nezbytné pro správnou funkčnost zařízení a nutné pro aplikaci MCX, by měly být zahrnuty ve firmwaru a operačním systému. Výrobce musí PPDR operátorovi poskytnout seznam aplikací a podrobné informace o jejich účelu a důvodech, proč jsou na zařízení potřebné.

Přístup k zařízení: Zařízení musí podporovat různé metody zabezpečení přístupu, např. PIN, heslo, otisky prstů a odemykání obličejem. Pro zvýšení bezpečnosti musí zařízení podporovat nastavitelnou funkci pro neúspěšné pokusy o zadání hesla, která zahájí tovární reset po překročení specifikovaného počtu neúspěšných pokusů o zadání hesla. Počet neúspěšných pokusů musí být konfigurovatelný. Výrobce by měl poskytnout pokyny pro správu této funkce, aby bylo zajištěno optimální zabezpečení zařízení.

Standardizace a certifikace: Zařízení používaná v sítích PPDR na bázi LTE a 5G musí:

– Mít platnou CE značku
– Mít unikátní IMEI kód, který nebyl a nebude použit v jiných zařízeních
– Být certifikována Global Certification Forum (GCF) pro shodu s 3GPP
– Podporovat 3GPP Mission Critical Services včetně funkčnosti MCX klienta, která odpovídá specifikacím 3GPP pro kritickou komunikaci (release 16 nebo novější). Toto ověření je stanoveno poskytnutím certifikátu shody na základě postupů certifikace GCF Mission Critical Services.
– Být doprovázena testovací zprávou RF OTA.

Lokalizační služby: Zařízení musí být kompatibilní s přijímači globálních navigačních satelitních systémů (GNSS) a fungovat minimálně s Galileo a GPS systémy, spolu s lokalizací poskytovanou mobilní sítí. Služby lokalizace v interiéru musí být k dispozici pomocí existujících technologií, tj. Bluetooth nebo Wi-Fi.

10.4 Komplementární požadavky

Komplementární požadavky na PPDR zařízení poskytují další specifikace a mohou být přísnější než minimální požadavky. Tyto požadavky jsou navrženy tak, aby splňovaly specifické potřeby v náročnějších situacích nebo prostředích.

10.4.1 Dodatečné environmentální požadavky

V některých případech je potřeba zpřísnit environmentální požadavky pro zařízení určená pro těžké použití. Tato zařízení by měla podporovat:

Operační teplotní rozsah -30 až +55 stupňů Celsia

Odolnost proti pádům z výšky 3 metrů na tvrdé, hrubé povrchy bez poškození

Ochranné mechanismy pro kontakty, těsnění a pouzdra, aby se zabránilo korozi po kontaktu se slanou vodou

10.4.2 Dodatečné hardwarové požadavky

Programovatelná tlačítka: Zařízení by měla mít programovatelná tlačítka, která lze nastavit pomocí EMM (Enterprise Mobility Management). Každé tlačítko by mělo být programovatelné s konkrétními funkcemi v aplikacích, jako je druhé tlačítko PTT, odesílání předdefinovaných zpráv, nebo systémové funkce, jako je výběr hovorové skupiny a otevírání aplikací.

Baterie: Dodatečné požadavky na baterie zahrnují:

– Duty cycle 80% standby / 20% aktivní používání při +20 °C a -110 dBm RSRP signálu by mělo vydržet minimálně 16 hodin při používání aplikace MCX.

– Po 2000 nabíjecích cyklech (20% až 100% nabití) by si baterie měla zachovat 90% původní kapacity.

– Podpora bezdrátového nabíjení kompatibilního s Qi 1 a Qi 2.

– Baterie by měla být vyměnitelná bez přerušení komunikace MCX, což umožňuje hot swapping.

Konektory pro periferní zařízení: Zařízení by mělo být vybaveno externím konektorem pro anténu, který zlepšuje použitelnost a rozšiřuje možnosti použití.

10.4.3 Dodatečné příslušenství

Výrobce zařízení by měl být schopen poskytovat nebo podporovat následující příslušenství:

– Jednoduché a vícenabíjecí banky pro vyměnitelné baterie

– Vozidlové držáky, které umožňují nabíjení a usnadňují připojení k externím anténám, zvukovým příslušenstvím a displejům montovaným ve vozidle

10.4.4 Dodatečné bezpečnostní a firmware požadavky

Podpora životního cyklu: Kontinuální prodloužení životního cyklu je důležité, a výrobce zařízení by měl poskytovat plnou podporu zařízení po dobu šesti (6) let od jeho uvedení na trh.

Podpora MC služeb: Velké operace vyžadují řešení, která umožňují sdílení kapacity mezi mnoha uživateli. Zařízení by mělo podporovat vysílací/multicastové služby (eMBMS, MBS).

End-to-End Encryption (E2EE): PPDR organizace potřebují komunikovat a sdílet informace bez rizika zachycení nebo úniku citlivých informací. Zařízení by mělo mít schopnost podporovat řešení end-to-end šifrování, které jsou interoperabilní se stávajícími řešeními end-to-end šifrování v TETRA zařízeních. Tuto funkcionalitu poskytují třetí strany na základě smart karet, které jsou přidány do zařízení.

10.5 Budoucí požadavky

Budoucí požadavky na PPDR zařízení zohledňují rychlý vývoj mobilních technologií a standardizace. Dodavatelé by měli spolupracovat s komunitou PPDR, aby zajistili, že nové funkce a vylepšení budou neustále přidávány a že zařízení budou schopna podporovat nejnovější technologie a standardy.

10.5.1 Hardware

Výběr hovorové skupiny s otočným přepínačem: Pro usnadnění a plynulé přepínání mezi hovorovými skupinami, i při nošení ochranných rukavic a bez nutnosti vizuální pomoci, by mělo zařízení disponovat tlačítkem, které je snadno ovladatelné hmatem, jako je otočný přepínač.

Komunikace zařízení s zařízením: Uživatelé potřebují mít přístup ke spolehlivým a předvídatelným komunikačním službám i při absenci síťového připojení. Výrobci zařízení by měli sledovat a přispívat k nalezení standardizovaného řešení 3GPP, které nahradí současný DMO (direct-mode operation) a bude implementováno do zařízení.

Výkon antény RF OTA: Kromě minimálních a komplementárních požadavků na frekvence by mělo zařízení podporovat ITU region 1 B68 (698-703 MHz) a pro zvýšení pokrytí uvnitř budov n40 (2300 MHz), n22 (3500 MHz), n74 (1500 MHz), n258 26 GHz (24,25-27,5 GHz). Pro zajištění širokého geografického pokrytí a dosažení požadovaného výkonu RF OTA může být použito externí anténní řešení kompatibilní s frekvencemi pod 1 GHz.

– Agregace nosných zařízení by mělo podporovat následující kombinace pásmové agregace:
  – CA combo LTE B20 + NR28
  – CA combo LTE B1+ LTE B3 + LTE B20

Podpora životního cyklu: V budoucnu se očekává, že výrobci zařízení budou poskytovat plnou podporu zařízení po dobu šesti (6) let od jeho uvedení na trh.

Lokalizační služby: Přístup komunity PPDR ke spolehlivým pozičním a časovým informacím je nezbytný pro všechny operace kritických služeb. Uživatelé PPDR spoléhají na přesné a kvalitní pozice chráněné před vnějším vlivem. Zařízení by mělo podporovat Galileo Public Regulated Service (PRS), jakmile bude dostupné k implementaci. To mimo jiné znamená, že přijímač bude muset být schopný přijímat signál PRS na frekvenčních pásmech E1 a E6. Přijímač GNSS by měl mít ochranné mechanismy, které zabrání rušení (jamming) a maskování (spoofing).

Komunikace zařízení s družicí: Uživatelé PPDR operující v odlehlých oblastech bez pokrytí mobilní sítí jsou závislí na jiných způsobech komunikace. Výrobci zařízení by měli sledovat a ideálně přispívat k standardizačním iniciativám v rámci 3GPP a TCCA, aby nalezli řešení pro komunikaci zařízení s družicí (NTN), které bude implementováno do zařízení.

10.6 Klíčové fáze implementace širokopásmových MCS

Implementace širokopásmových komunikačních systémů pro MC (Mission Critical Communication Systems – MCS) zahrnuje několik klíčových fází. Každá z těchto fází má své vlastní aktivity a cíle, které jsou zásadní pro úspěch celého programu.

1 **Strategie:** Provedení komplexní studie požadavků na síť pro kritické akce, celkových cílů, potřeb a záměrů. Tato fáze je pro určení životaschopnosti projektu, včetně financování, přidělení spektra, identifikace pokrytí a zapojení zainteresovaných stran. Strategie také definuje obchodní model projektu a implementační plán.

2 **Koncepce:** Podrobný popis případů užití programu MCS, což pomáhá zpřesnit jeho celkové cíle. Na základě těchto případů užití se provádějí studie důkazu konceptu (proof of concept), aby se získala zpětná vazba a akceptace uživatelů těchto definovaných případů užití.

3 **Plánování a design:** Definuje podrobnou technickou architekturu systému MCS, pokrývající síťovou architekturu (budování nových stožárů, modernizace stávající infrastruktury) a technické a funkční specifikace pro jádro, RAN, uživatelské zařízení a aktivní síťové komponenty. Plánování a design také stanoví standardizované vybavení, protokoly a postupy pro zajištění interoperability.

4 **Nákup:** Jsou definovány různé modely nákupu na základě výběrových řízení (RFP) vyhlášených pro získání nabídek na vybudování síťové infrastruktury, nákup zařízení a potřebné služby. Tyto nabídky jsou technicky a komerčně vyhodnoceny, což zajišťuje, že nákupní procesy jsou transparentní a efektivní při vydávání objednávek a sjednávání smluv.

5 **Implementace:** Jakmile je smlouva udělena implementačním agenturám, implementační fáze zahajuje realizaci systému MCS na základě jeho podrobného návrhu a technické architektury. Následuje nasazení fyzické síťové infrastruktury, dodávku, instalaci, uvedení do provozu, testování uživatelských zařízení a aplikací a školení a programy pro budování kapacit pro koncové uživatele. V rámci této fáze koncoví uživatelé provádějí akceptační testování uživatelů (UAT), aby ověřili implementaci projektu a nastavili prostředí sandbox pro zajištění bezpečnosti a stability sítě.

6 **Optimalizace:** Během optimalizace je síť MCS testována a monitorována z hlediska výkonu, spolehlivosti a bezpečnosti. Na základě pozorování jsou prováděna vylepšení, která zvyšují výkon a služby. Pro zajištění kvality služeb a lepší uživatelské zkušenosti jsou monitorovány klíčové ukazatele výkonnosti (KPI) a SLA.

10.7 Faktory správné implementace MCS

Úspěšná implementace širokopásmového systému pro kritické mise (Mission Critical System – MCS) vyžaduje důkladné zvážení několika klíčových faktorů.

Alokace požadovaného financování: Zajištění dostatečných finančních prostředků pro implementaci širokopásmové komunikační sítě pro kritické mise často ovlivňuje časový harmonogram realizace.

Alokace spektra: Získání požadovaného spektra a šířky pásma je zásadní pro úspěch programu kritické komunikace.

Podpora zainteresovaných stran: Je nutné, aby všechny relevantní strany byly podporující, investovaly a byly odhodlané k úspěchu programu a plnily své role v jednotlivých fázích.

Problémy s interoperabilitou mezi různými agenturami veřejné bezpečnosti: Umožnění bezproblémové výměny informací mezi více agenturami veřejné bezpečnosti je nezbytné, protože každá agentura může být na jiné úrovni zralosti komunikačních systémů pro kritické mise.

Standardizace zařízení a protokolů: Kompatibilita a standardizace veškerého vybavení a protokolů jsou nezbytné k prevenci možných narušení provozu a k umožnění různých způsobů použití.

End-to-end bezpečnost: End-to-end bezpečnost komunikační sítě pro kritické mise je zásadní, včetně šifrování dat a ochrany proti kybernetickým útokům.

Pokrytí: Poskytnutí komplexní dostupnosti a pokrytí sítě v celém servisním území je důležité pro schopnost reagovat na krize v odlehlých oblastech.

Proces zadávání zakázek: Efektivní řízení procesu zadávání zakázek je důležité pro získání nejlepší hodnoty za investované prostředky a prevenci neočekávaných nákladů a zpoždění souvisejících s rozpočtem.

Přijetí uživateli: Podpora a usnadnění testování a používání sítě pro kritickou komunikaci všemi agenturami veřejné bezpečnosti je důležité pro maximalizaci jejich účinnosti a efektivity.

Škálování: Zajištění škálovatelnosti sítě pro splnění potřeb rostoucího počtu uživatelů agentur veřejné bezpečnosti je nutné, aby se předešlo narušení služeb kvůli nedostatečné kapacitě a vysoké zátěži.

Regulace: Dodržování relevantních vnitrostátních regulací a politik upravujících implementaci a používání sítě pro kritickou komunikaci je důležité pro legální a bezpečný provoz systému.

Veřejné přijetí: Informování a získání souhlasu veřejnosti s kritickou komunikační sítí je důležité, aby se předešlo možným zpožděním nebo zastavení projektu kvůli protestům či odporu, což by mělo být dosaženo v raných fázích implementace.

10.8 Klíčové aspekty kritických komunikačních systémů

Efektivní a spolehlivé kritické komunikační systémy musí splňovat několik zásadních kritérií, která zajišťují jejich funkčnost a dostupnost v jakýchkoli podmínkách. Následující grafický přehled znázorňuje hlavní faktory, které musí být zajištěny a optimalizovány během plánování, implementace a provozu kritických komunikačních systémů.

Hlasové služby a správy: Kritické komunikační systémy musí zajišťovat spolehlivou a kvalitní hlasovou komunikaci, která je klíčová pro efektivní koordinaci v krizových situacích.

Kvalita a bezpečnost: Bezpečnost dat a kvalita komunikace jsou základními požadavky. Systémy musí poskytovat vysokou úroveň šifrování a ochrany proti kybernetickým hrozbám.

Odolnost sítě: Sítě musí být navrženy tak, aby odolaly různým fyzickým a environmentálním vlivům, včetně extrémních teplot, vlhkosti a mechanických poškození.

Pokrytí sítě: Zajištění širokého geografického pokrytí je nezbytné pro dosažení spolehlivé komunikace i v odlehlých a těžko přístupných oblastech.

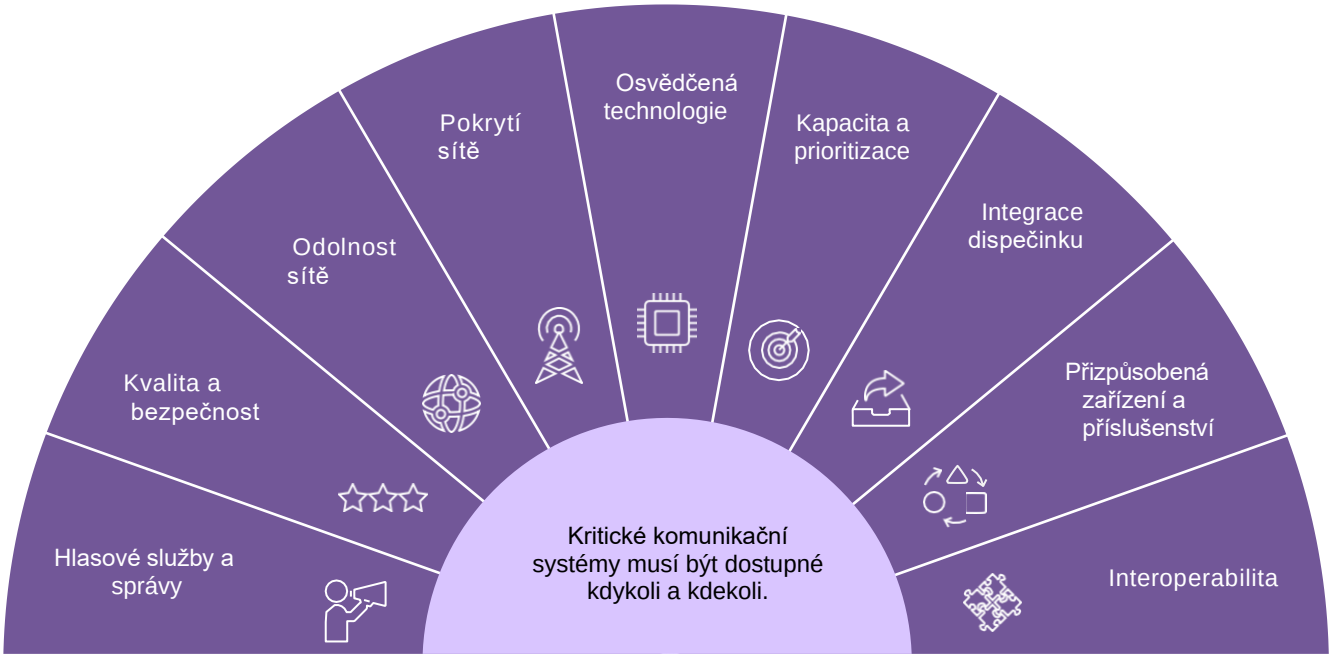
Osvědčená technologie: Používání osvědčených a standardizovaných technologií zajišťuje kompatibilitu a spolehlivost systému v různých podmínkách.

Kapacita a prioritizace: Systémy musí být schopny zvládat velké objemy komunikace a efektivně prioritizovat zprávy a hovory podle jejich důležitosti.

Integrace dispečinku: Integrace s dispečerskými systémy je klíčová pro zajištění koordinace a efektivního řízení zdrojů během krizových situací.

Přizpůsobená zařízení a příslušenství: Zařízení musí být přizpůsobena specifickým potřebám uživatelů v krizových situacích, včetně robustnosti a schopnosti fungovat v náročných podmínkách.

Interoperabilita: Zajištění interoperability mezi různými systémy a zařízeními je nezbytné pro efektivní spolupráci mezi různými agenturami a organizacemi veřejné bezpečnosti.



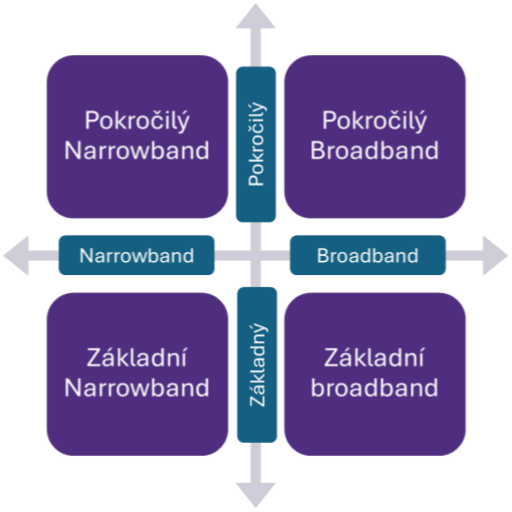
Tento obrázek poskytuje komplexní přehled klíčových aspektů, které musí být zajištěny pro dosažení efektivního a spolehlivého kritického komunikačního systému, který je schopen fungovat kdykoli a kdekoli.

10.9 Praktické implementace a příklady MCC-ECO

Reálné implementace ekosystému komunikačních systémů pro kritické mise (Mission Critical Communication Ecosystem – MCC-ECO) ukazují, jak různé země přistupují k vývoji a nasazení těchto systémů. Níže jsou uvedeny různé aspekty praktické implementace a konkrétní příklady z praxe.

10.9.1 Kategorizace podle technologie

Země lze kategorizovat podle jejich technologických implementací v oblasti komunikačních systémů pro MC. Tyto kategorie zahrnují:



Kritické komunikačné technológie vs. kategórie vyspelosti

Pokročilý Narrowband První uživatelé narrowband technologií předvídají požadavky uživatelů, s neustálými investicemi a postupně vylepšovanými implementacemi. Celonárodní implementace s vyhrazenými mechanismy řízení pro optimalizaci investic a zajištění univerzální podpory pro veřejné bezpečnostní agentury (PSA).

Pokročilý broadband Implementovaná celonárodní veřejná bezpečnost přes LTE, a dobře fungující MCC-ECO s jasností ve funkcích a odpovědnostech, robustní strukturou řízení, obchodními modely, odpovídající finanční strategií a začínají využívat nové technologie.

Základní narrowband Reaktivní přijetí narrowband technologií, založené na specifických potřebách uživatelů. Jednotlivé veřejné bezpečnostní agentury (PSA) pověřené implementací.

Základní broadband Zahájené diskuse o přípravě na implementaci broadbandu. To zahrnuje diskuse s OEM (Original Equipment Manufacturer) o výběru technologií, pilotní implementace, strukturu řízení programu, přidělování spektra, vymezení obchodního modelu pro podporu zainteresovaných stran a odpovídající finanční mechanismy.

10.9.2 Implementační programy podle zemí

Každá země se vydala na svou cestu k implementaci komunikačních systémů pro kritické mise ovlivněnou různými faktory, jako jsou potenciální dopady vnějších faktorů (včetně nehod, mimořádných událostí a potenciálních hrozeb), strategie financování, struktury správy, závislost na dodavatelích a dostupnost spektrální šířky pásma. Přestože každá země začíná tuto cestu z různých pozic a s různými alokacemi zdrojů, lze se mnoho naučit z osvědčených postupů průkopnických národů.

Níže na obrázku je uvedena implementace dle jednotlivých zemí dle studie "The shortest critical path to Next-Generation Public Safety Networks" od Pwc z roku 2022[12].

[12] https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/documents/critical-communications-world.pdf

Implementační programy dle jednotlivých zemí

Grant Thornton

www.grantthornton.cz