Dean Lalić, dipl. ing. građ., Eurail-ing

EUROPSKI PROJEKT SAFETY4RAILS

1. Uvod

Projekt SAFETY4RAILS jest multidisciplinarni projekt koji financira Europska unija u sklopu programa Horizon 2020, koji se u jednome dijelu odnosi na provedbu istraživačkih i inovacijskih aktivnosti u cilju zaštite ljudi, infrastrukture i usluga te gospodarstva od ugroza koje se mogu pojaviti u suvremenome društvu. Projekt SAFETY4RAILS počeo se provoditi 1. listopada 2020. i trajat će dvije godine. Cilj je projekta razviti metode i sustave za povećanje razine sigurnosti željezničkih te drugih tračničkih sustava kao i intermodalnih sustava koji uključuju željeznicu. Uključuje obuku i stručno usavršavanje korisnika za uporabu pojedinih komponenti sustava SAFETY4RAILS, demonstraciju primjene sustava u stvarnim uvjetima te korištenje dostupnih podataka i rezultata o postojećim kriznim situacijama.

Željeznica jest siguran, učinkovit, pouzdan i ekološki prihvatljiv modalitet masovnoga prijevoznika ljudi i roba, a u vremenu koje je pred nama njezina će važnost biti u stalnome porastu u svjetlu rješavanja klimatskih problema te sve veće razine svijesti o neophodnosti poduzimanja aktivnosti za njihovu kontrolu i ublažavanje. S obzirom na stratešku važnost koju željeznica već sada ima za normalno funkcioniranje gospodarstva i društva u cjelini, postoji opravdana opasnost da postane meta za razne vrste napada, od kibernetičkih do fizičkih (terorističkih). Pritom su podjednako izloženi svi segmenti željezničkoga prometa, uključujući infrastrukturu i prijevozničke kapacitete.

U fokusu su projekta kibernetički napadi kao što je to bio napad računalnoga crva WannaCry u svibnju 2017., fizički napadi poput napada bombom na prigradski vlak u Madridu 2014. te kombinirani napadi. Projekt SAFETY4RAILS promatra ponašanje sustava u slučaju velike koncentracije putnika i željezničkih vozila, na primjer, u vrijeme najveće gužve ili masovnih događanja poput velikih sportskih događanja koja se održavaju na više lokacija kao što su to Olimpijske igre. Kada se incidentna situacija dogodi, upravitelji infrastrukture i željeznički prijevoznici moraju djelovati brzo i učinkovito te uzeti u obzir mnoge aspekte kako bi osigurali sigurnost putnika i tereta koji se prevozi. Pritom je ključno analizirati prijetnje, održavati svijest o situaciji, uspostaviti krizno komuniciranje te toduzeti korake za ublažavanje posljedica i informiranje putnika i drugih korisnika.

Slika 1. Digitalizacija željeznice donosi nove sigurnosne izazove
Izvor: https://www.mobility.siemens.com

Projekt SAFETY4RAILS poboljšat će postupanje u takvim incidentnim situacijama kroz holistički pristup. Analizirat će cyber-fizičku otpornost željezničkih sustava te razviti strategije za ublažavanje posljedica i za učinkovit odgovor. Osim toga, kako bi ostali sigurni u svjetlu novih rizika koji se redovito pojavljuju, sustav SAFETY4RAILS omogućuje stalno prilagođavanje rješenja novim rizicima. Simulacijske vježbe bit će organizirane u različitim operativnim okružjima za testiranje i procjenu rješenja SAFETY4RAILS (platforma S4RIS) s krajnjim korisnicima željezničkih sustava i uz potporu vanjskoga savjetodavnog odbora.

Pritom će pozornost posebno biti usredotočena na aktivno uključivanje krajnjih korisnika, upravitelja infrastrukture i prijevoznika, od početka (definiranje zahtjeva i potreba te osmišljavanje i izvođenje scenarija i demonstracija) do kraja projekta (ocjenjivanje programskih platformi) kako bi se dobile kvalitetne povratne informacije potrebne za daljnji razvoj programskih sustava. Sudionici projekta SAFETY4RAILS organizirani su u konzorcij koji se sastoji od 31 partnera iz 13 zemalja (Njemačka, Francuska, Španjolska, Turska, Italija, Belgija, Švicarska, Ujedinjeno Kraljevstvo, Grčka, Finska, Mađarska, Izrael i Nizozemska). Oni predstavljaju željezničke prijevoznike, upravitelje željezničke infrastrukture, istraživačke centre, akademsku zajednicu i

dobavljače industrije te donose niz komplementarnih vještina potrebnih za taj multidisciplinarni projekt.

2. Ciljevi projekta

Cilj projekta SAFETY4RAILS jest razviti metode i sustave za povećanje razine sigurnosti željezničkoga prometa te drugih vrsta tračničkoga prometa u odnosu na prijetnje poput kibernetičkih napada, fizičkih (terorističkih) napada ili kombiniranih kibernetičkih napada. Kada se incidentna situacija dogodi, upravitelji infrastrukture i željeznički prijevoznici moraju djelovati brzo i učinkovito te uzeti u obzir mnoge aspekte kako bi osigurali sigurnost putnika i tereta koji se prevozi. Projekt SAFETY4RAILS nastoji kroz holistički (cjeloviti) pristup poboljšati postupanje u slučaju nastanka incidentnih događaja u cilju zaštite života i zdravlja ljudi te stabilnih i mobilnih željezničkih kapaciteta.

U sklopu projekta cilj je razviti sustavnu optimizaciju za upravljanje i povećanje razine otpornosti željezničkih infrastrukturnih sustava integriranjem fizičkih i informatičkih sustava u jedan upravljački sustav. Različiti alati razvijeni u sklopu projekta SAFETY4RAILS mogu se koristiti kao podrška u različitim slučajevima i fazama incidentnih situacija. Cilj je potaknuti korištenje automatiziranih alata i umjetne inteligencije za bolje razumijevanje, predviđanje i odgovor u kriznim situacijama.

Kao primjer informatičkoga napada spominje se računalni crv WannaCry koji je uzrokovao globalni kibernetički napad u svibnju 2017. Spomenuti je crv ciljao računala s operativnim sustavom Microsoft Windows šifriranjem podataka te zahtijevao otkupninu u kriptovaluti bitcoin. Napadu su bile posebno izložene informatičke mreže koje su koristile starije sustave Windows na kojima nisu instalirani novi sigurnosni alati i softverske zakrpe koje je proizveo Microsoft. Procjenjuje se da je napad zahvatio više od 200 000 računala u 150 zemalja te da je ukupna šteta iznosila od stotinu milijuna do milijardu dolara.

Računalni crvi jesu računalni programi koji umnožavaju sami sebe. Pritom koriste računalne mreže da bi se kopirali na druga računala, često bez sudjelovanja čovjeka. Za razliku od virusa, svojim djelovanjem ne moraju inficirati druge programe. Mogu stići i kao privitak u elektroničkoj pošti te im pristup računalu omogućuju propusti u operativnim sustavima i aplikacijama. Crvi otežavaju rad mreže, a mogu oštetiti podatke i kompromitirati sigurnost računala. Računalni virus jest računalni program koji može „zaraziti" druge programe tako da u njih unese kopiju samoga sebe, koja može biti modificirana. Virus se može proširiti računalnim sustavom ili mrežom koristeći se ovlastima korisnika koji su zaraženi. Svaki program koji je zaražen postaje virus i tako se zaraza širi.

Slika 2. Sigurnost željeznice u digitalnome okružju pametnih gradova
lizvor: https://infrastructuremagazine.com.au

Pored informatičkih mreža i sustava predmet napada mogu biti ljudi (korisnici usluga te zaposlenici i partneri u željezničkome sustavu), fizička imovina (željeznička infrastruktura, željeznička vozila, građevine, hardver i komunikacijska oprema) te nematerijalna imovina (informacije i podaci, sigurnost upravljanja željezničkim prometom, kvaliteta usluge, povjerenje korisnika, javno mišljenje i dr.).

Krajnji cilj projekta SAFETY4RAILS jest stvoriti otporne sustave za upravljanje željezničkom infrastrukturom i mobilnim kapacitetima, koji će u svakome trenutku moći odgovoriti na ugroze s kojima se mogu susresti te na učinkovit način poduzeti aktivnosti potrebne za sprječavanje i ublažavanje posljedica te što prije vratiti sustav u normalno stanje. Pritom je, naravno, prioritet zaštita života i zdravlja ljudi.

3. Prijetnje i rizici

Prijetnja je bilo koji događaj ili okolnost, bilo vanjski bilo unutarnji, koji ima potencijal da uzrokuje štetu sustavu ili njegovim pridruženim aplikacijama ili informacijama. Prijetnja može prouzročiti neželjenu situaciju čija posljedica može biti nanošenje štete resursima željezničkih sustava. Šteta nastaje kao posljedica ostvarenja prijetnje, a prijetnja mora iskoristiti postojeću ranjivost resursa da bi se realizirala i rezultirala štetom. Prilikom analize prijetnji potrebno je detektirati izvor (unutarnja ili vanjska prijetnja), motiv (npr. ostvarenje financijske dobiti), učestalost pojavljivanja te razornu moć i oblik (prirodna ili uzrokovana ljudskim djelovanjem, slučajnim ili namjernim). Osim jačanja otpornosti na već poznate prijetnje ključno je otkrivanje i identificiranje novih prijetnji.

Pri implementaciji sustava upravljanja informacijskom sigurnošću posebnu pozornost potrebno je obratiti na upravljanje rizikom koji proizlazi iz korištenja informacijskoga sustava. Upravljanje rizikom jest proces koji omogućava upravi tvrtke da uravnoteži operativne i ekonomske troškove zaštitnih mjera za očuvanje sigurnosti korporativnoga informacijskog sustava. Upravljanje rizikom jest proces identifikacije rizika, procjene rizika i poduzimanja koraka da se rizik smanji na prihvatljivu razinu. Poboljšanje upravljanja rizicima i kriznim situacijama uključuje prognoze i upravljanje novim prijetnjama, razmjenu znanja s dionicima te analizu utjecaja rastućih prijetnji koje se razvijaju.

Rizik jest funkcija vjerojatnosti da će identificirani izvor prijetnje iskoristiti određenu ranjivost i učinka koji taj neželjeni događaj može imati na sustav. Sama prijetnja ne predstavlja rizik kada nema ranjivosti koja se može iskoristiti. U određivanju vjerojatnosti prijetnje potrebno je razmotriti prijetnje, potencijalne ranjivosti i postojeće kontrole. Ranjivost jest skup stanja koji mogu omogućiti nekoj prijetnji da utječe na predmet napada. Ranjivost jest slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti. Posljedica iskorištenja ranjivosti jest nanošenje štete, odnosno ispunjenje ciljeva napada. Poboljšanjem razine otpornosti i sigurnosti sustava na prijetnje postižu se uštede u vremenu odgovora uz podršku za donošenje odluka, smanjuju se troškovi poduzimanja odgovarajućih mjera, povećava se razina pouzdanosti i sigurnosti upravljanja u stvarnome vremenu te se omogućava multimodalni pristup.

Upravljanje rizikom jest proces identificiranja rizika, procjene rizika i poduzimanja koraka da se rizik smanji na prihvatljivu razinu te održavanja rizika te razine. Upravljanje rizikom zahtijeva analizu rizika u odnosu na potencijalne koristi te uzimanje u obzir alternativa i primjenu onoga što se utvrdi kao najbolji tijek postupanja u odnosu na rizik. Procjena rizika jest prvi proces u metodologiji upravljanja rizikom. Organizacije koriste procjenu rizika da bi odredile opseg potencijalnih prijetnji i rizika koji prate jedan informacijski sustav. Ta aktivnost pomaže da se identificiraju odgovarajuće kontrole za smanjenje ili uklanjanje rizika tijekom procesa ublažavanja rizika. Da bi se odredila vjerojatnost budućih štetnih događaja, prijetnje željezničkome sustavu moraju se analizirati zajedno s potencijalnim ranjivostima i postojećim kontrolama. Utjecaj se odnosi na veličinu štete koja može biti uzrokovana iskorištavanjem ranjivosti od strane prijetnje. U procjeni prijetnji važno je razmotriti sve potencijalne izvore prijetnji koje mogu prouzročiti štetu u željezničkome sustavu i njegovoj radnoj okolini.

Prirodni izvori prijetnji jesu prirodne nepogode. Tehnički izvori prijetnji jesu tehnički kvarovi i druge neispravnosti željezničke infrastrukture i opreme. Ljudski izvori prijetnji mogu biti unutarnji (nestručnost, neodgovornost, zlouporaba položaja i ovlasti i drugo) i vanjski (zlonamjerni pojedinci izvana, kriminalne organizacije, strane obavještajne službe, komercijalne organizacije, terorističke organizacije, poslovna konkurencija i drugo).

4. Projektne aktivnosti

Europski istraživački projekt SAFETY4RAILS službeno je pokrenut 5. studenoga 2020. kada je bio održan početni sastanak na kojemu su bili svi sudionici projekta te predstavnici mjerodavnih tijela Europske komisije. U taj projekt uključen je i Odjel za sigurnost Međunarodne željezničke unije (UIC) radi koordinacije aktivnosti i sudionika u projektu, uzimajući u obzir njihove potrebe i osiguravajući da se njihovi zahtjevi i specifične karakteristike pravilno uzmu u obzir pri razvoju rješenja. UIC će također voditi planiranje, razvoj i evaluaciju simulacijskih vježbi u uskoj suradnji s krajnjim korisnicima. Tema prvoga sastanka bila je analiza podataka temeljena na sigurnosti i zaštiti u cilju otkrivanja, sprječavanja, ublažavanja i reagiranja na incidentne situacije na željezničkoj, transmodalnoj i podzemnoj tračničkoj mreži.

Slika 3. Sigurnost željeznice u interakciji s drugim prijevoznim modalitetima

Izvor: https://betracksmart.org

U današnje je vrijeme upravljanje fizičkim i kibernetičkim rizicima još uvijek potpuno različito i međusobno odvojeno, iako su ti rizici zapravo međusobno jako povezani. Za slučaju kada će rizici različitih vrsta konvergirati očito je potreban složeniji i višeslojni pristup. Projekt SAFETY4RAILS ima cjelovit pogled na fizičku i cyber sigurnost. To znači da će razvijena rješenja dodatno integrirati mjere koje se mogu poduzeti na fizičkome

i cyber području, no incident ili kriza ne mogu se uvijek izbjeći ni uz najveće mjere opreza i prevencije. Kada se incident dogodi, sudionici u željezničkome sustavu moraju reagirati promptno te u kratko vrijeme razmotriti mnoge aspekte kako bi zaštitili sigurnost sustava te sigurnost putnika. Moraju provesti analizu prijetnji, održati razinu svijesti o situaciji, uspostaviti kriznu komunikaciju i organizirati odgovarajući odgovor. Pored toga moraju poduzeti korake usmjerene na smanjivanje i ublažavanje posljedica te uspostaviti komunikaciju s korisnicima sustava i nadležnim tijelima.

U sklopu projekta SAFETY4RAILS bit će razvijen i implementiran informacijski sustav S4RIS koji će analizirati utjecaj predloženih strategija u fazama prevencije i odgovora na prijetnje. Namjena sustava jest pružiti učinkoviti odgovor u slučaju nastupanja incidentne situacije. Pritom je u kratko vrijeme potrebno analizirati incidentni događaj (što se dogodilo, je li potrebna medicinska pomoć, koliko je ljudi pogođeno i kako bi se događaj mogao razviti), uspostaviti kriznu komunikaciju (uključiti sve nadležne službe, čuvajući sigurnost i izbjegavajući stvaranje panike) te pružiti odgovor (poduzeti aktivnosti da se sustav što prije vratiti u normalno stanje). Cilj navedenih aktivnosti jest otkrivanje, ublažavanje, sprečavanje, predviđanje i brzo reagiranje usmjereno na umjetnu inteligenciju, uz pristup u realnome vremenu.

Samo kada postoji stvarna, jasna i opsežna slika krizne situacije mogu se poduzeti odgovarajuće mjere. U današnje vrijeme informacije se još uvijek prikupljaju i prenose konvencionalnim sredstvima: senzorskim mrežama, telefonom, videokonferencijskim sustavima i drugim. Smatra se da se u tome pogledu još uvijek ne koristi puni potencijali suvremenih tehnologija. Predloženi informacijski sustav S4RIS prikupljat će, obrađivati i prezentirati podatke te omogućiti donositeljima odluka da učine ono što je potrebno u složenoj kriznoj situaciji.

5. Važnost projekta

Zašto je sigurnost željezničkih sustava važna? Kako bi se odgovorilo na to pitanje, ponajprije je potrebno definirati pojam „kritične infrastrukture". Nacionalnu kritičnu infrastrukturu čine sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti (Zakon o kritičnim infrastrukturama, NN 56/13).

U nacionalnu kritičnu infrastrukturu osobito su uključeni:

- energetika (proizvodnja, prijenos, skladištenje, transport, distribucija)
- komunikacijska i informacijska tehnologija (komunikacije, prijenos podataka, sustavi, usluge)
- promet (cestovni, željeznički, zračni, pomorski i promet unutarnjim plovnim putovima)
- zdravstvo (zdravstvena zaštita, proizvodnja, promet i nadzor nad lijekovima)
- vodno gospodarstvo (regulacijske, zaštitne i komunalne vodne građevine)
- hrana (proizvodnja i opskrba, sustav sigurnosti, robne zalihe)
- financije (bankarstvo, burze, investicije, sustavi osiguranja i plaćanja)
- proizvodnja, skladištenje i prijevoz opasnih tvari (kemijski, biološki, radiološki i nuklearni materijali)
- javne službe (osiguranje javnog reda i mira, zaštita i spašavanje, hitna medicinska pomoć)
- nacionalni spomenici i vrijednosti.

Kritičnu infrastrukturu čine fizički i digitalni sustavi koji su od ključne važnosti za funkcioniranje gospodarstva i društva u cjelini. Zaštitne aktivnosti i osiguravanje pouzdanosti te infrastrukture, koja je žila kucavica gospodarskoga i društvenoga života, neophodni su elementi za nacionalnu sigurnost i gospodarsku održivost. Sustavi koji čine kritičnu infrastrukturu međusobno su povezani i ovisni, pa u slučaju kvara mogu uzrokovati neispravnost drugih dijelova infrastrukture. Također, s obzirom na to da zaštita kritične infrastrukture nije samo nacionalno pitanje, potrebno je voditi računa o nužnosti i važnosti međunarodne suradnje. Europski program za kritičnu infrastrukturu (EPCIP), koji je na zahtjev Vijeća Europe usvojen 2006., definira kritične infrastrukture kao one koje se sastoje od fizičkih, informatičkih i tehnoloških elemenata, mreža, usluga i imovine, a koji, ako su prekinuti ili uništeni, imaju ozbiljan utjecaj na zdravlje, sigurnost, gospodarsku dobrobit građana i/ili na učinkovito funkcioniranje vlasti u državama članicama.

Bez iznimki, danas se informatičke tehnologije koriste u svim kritičnim infrastrukturama. Informatički sustavi upravljanja i nadzora (SCADA) temeljeni su na tehnologiji koja korisnicima omogućuju prikupljanje i uprav-

Slika 4. Sigurnost i digitalizacija željezničke infrastrukture
Izvor: https://threatpost.com

ljanje trenutačnim informacijama o njihovim sustavima te prolazak kroz šifrirane i kodirane signale i udaljene naredbene terminale povezane preko komunikacijskih kanala. U posljednje vrijeme, usporedo s tehnološkim razvojem i napretkom digitalizacije, kritična infrastruktura postala je meta kibernetičkih i kombiniranih napada. Svakodnevno smo svjedoci toga da na takve napade nisu imune ni najsofisticiranije informatičke mreže u vojnoj industriji, tajnim službama ili nuklearnim postrojenjima u najrazvijenijim državama.

Željeznički sustavi, koji se smatraju među najvažnije kritične infrastrukture, također su osjetljivi s obzirom na razne vrste napada. U cilju analize sadašnjega stanja sigurnosti i uspostavljanje naprednoga sustava zaštite pokrenut je projekt SAFETY4RAILS, koji pruža platformu upraviteljima infrastrukture i željezničkim prijevoznicima koji su se okupili iz raznih zemalja kako bi se upoznali s najnovijim tehnologijama razvijenima za pouzdaniji rad sustava kao i za međusobnu razmjenu informacija i iskustava.

Moramo se zapitati jesu li naši trenutačni željeznički infrastrukturni sustavi dovoljno otporni da se nose sa složenim incidentnim događajima koji su uzrokovani kombiniranim napadima ili multifunkcijskim kvarovima i u skladu s time se pripremiti. U tome smislu upravitelji infrastrukture planiraju ulaganja u povećanje razine otpornosti stabilnih infrastrukturnih kapaciteta kao što su kolosijeci, zgrade, signalno-sigurnosna i telekomunikacijska oprema i drugo te u isto vrijeme ulaganja u povećanje razine otpornosti informatičke infrastrukture. Pritom je važno uspostaviti integrirani pristup za optimizaciju otpornosti cijeloga infrastrukturnog sustava na reakcije na događaje s više opasnosti.

Slika 5. Sigurnost i digitalizacija upravljanja željezničkim vozilima
Izvor: https://infrastructuremagazine.com.au

U isto vrijeme i željeznički prijevoznici planiraju ulaganja u povećanje razine otpornosti mobilnih kapaciteta i prateće informatičke opreme. Razvoj okvira za optimiziranje troškova koje željeznički prijevoznici izdvajaju za poboljšanje razine otpornosti u svojim sustavima također je ključan, zbog čega se u sklopu projekta SAFETY4RAILS predlaže integrirani pristup za ostvarivanje učinkovitih akcija poboljšanja otpornosti u cijelome sustavu kako bi se maksimalno iskoristili i optimizirali raspoloživi resursi.

6. Zaključak

Kako bi željeznica zadržala svoju poziciju sigurnoga, učinkovitoga, pouzdanoga i ekološki prihvatljivoga modaliteta masovnog prijevoznika ljudi i roba, potrebno je kontinuirano poduzimati aktivnosti na njezinu osuvremenjivanju. Jedna od važnih aktivnosti na osuvremenjivanju željeznice jest i njezina digitalizacija, koja pored brojnih prednosti nosi i izazove s kojima se moramo suočiti, među kojima je i pitanje sigurnosti od kibernetičkih i kombiniranih napada. Opasnost od fizičkih (terorističkih) napada redovito je prisutna s obzirom na stratešku važnost željeznice za gospodarstvo i društvo u cjelini. Pritom su jednako izloženi željeznička infrastruktura te mobilni kapaciteti prijevoznika.

Kako bi se što kvalitetnije suočili s navedenim prijetnjama u željezničkome sektoru, pokrenut je projekt SAFETY4RAILS čiji je cilj razviti metode i sustave za povećanje razine sigurnosti željezničkih i drugih tračničkih sustava. Taj europski projekt donosi brojne izazove na putu da željeznički sustav učini sigurnijim i učinkovitijim. Njegova je snaga u tome što suradnja s velikim brojem dionika iz željezničkoga sektora stvara priliku za stvaranje održivoga sigurnosnog sustava koji će biti modeliran i testiran u realnim scenarijima.

Projekt ponajprije analizira potrebe krajnjih korisnika. Ti će se zahtjevi koristiti za daljnji razvoj i ažuriranje 18

različitih alata i njihovu primjenu u prototipu platforme informacijskoga sustava SAFETY4RAILS (S4RIS). Sustav S4RIS će se usredotočiti na procjenu rizika, smanjenje rizika, sprječavanje prijetnji, otkrivanje prijetnji, odgovor dionika na incidente i oporavak sustava. Na kraju će platformu testirati i ocijeniti krajnji korisnici u sklopu raznih simulacijskih modela i studija. To će omogućiti primjenjivost S4RIS-a u realnome okružju željezničkih sustava i potvrditi važnost projekt SAFETY4RAILS za razvitak sigurnosti željezničkoga prometa u cjelini.

Literatura:

[1] Project SAFETY4RAILS, https://safety4rails.eu/

[2] Union Internationale des Chemins de fer (UIC), https://uic.org/projects/safety4rails

[3] Zakon o kritičnim infrastrukturama (NN 56/13)

[4] European Programme for Critical Infrastructure Protection, Bruxelles, 2006.

UDK: 656.2+004.056

Adresa autora:

Dean Lalić, dipl. ing. građ., Eurail-ing
HŽ Infrastruktura d.o.o.
e-pošta: dean.lalic@hzinfra.hr

SAŽETAK

EUROPSKI PROJEKT SAFETY4RAILS

Cilj projekta SAFETY4RAILS jest razviti metode i sustave za povećanje razine sigurnosti željezničkih te drugih tračničkih sustava kao i intermodalnih sustava koji uključuju željeznicu. Projekt uključuje obuku i stručno usavršavanje korisnika za uporabu pojedinih komponenti sustava, demonstraciju primjene sustava u stvarnim uvjetima te korištenje dostupnih podataka i rezultata o postojećim kriznim situacijama. Krajnji je cilj projekta stvoriti otporne sustave za upravljanje željezničkom infrastrukturom i mobilnim kapacitetima, koji će u svakome trenutku moći odgovoriti na ugroze s kojima se mogu susresti te na učinkovit način poduzeti aktivnosti za sprečavanje i ublažavanje posljedica i što prije vratiti sustav u normalno stanje.

Ključne riječi: *Safety4rails, sigurnost željezničkih sustava, krizne situacije na željeznici, incidentni događaji na željeznici*

Kategorizacija: *stručni rad*

SUMMARY

EUROPEAN SAFETY4RAILS PROJECT

The SAFETY4RAILS project aims to deliver methods and systems to increase the safety of rail and other track systems, as well as intermodal systems involving railways. This project includes training and professional development of users for the use of individual system components, demonstration of the system application in real conditions, and the use of available data and results on existing crisis situations. The ultimate goal of the project is to create resilient systems for managing railway infrastructure and mobile capacities, which will be able to respond to the threats they may encounter at any time and take effective action to prevent and mitigate the consequences and return the system to its normal state as soon as possible.

Key words: *Safety4rails, railway system safety, railway crisis situations, railway incidents*

Categorization: *professional paper*