Sonja Steffens,
Walter Valvoda

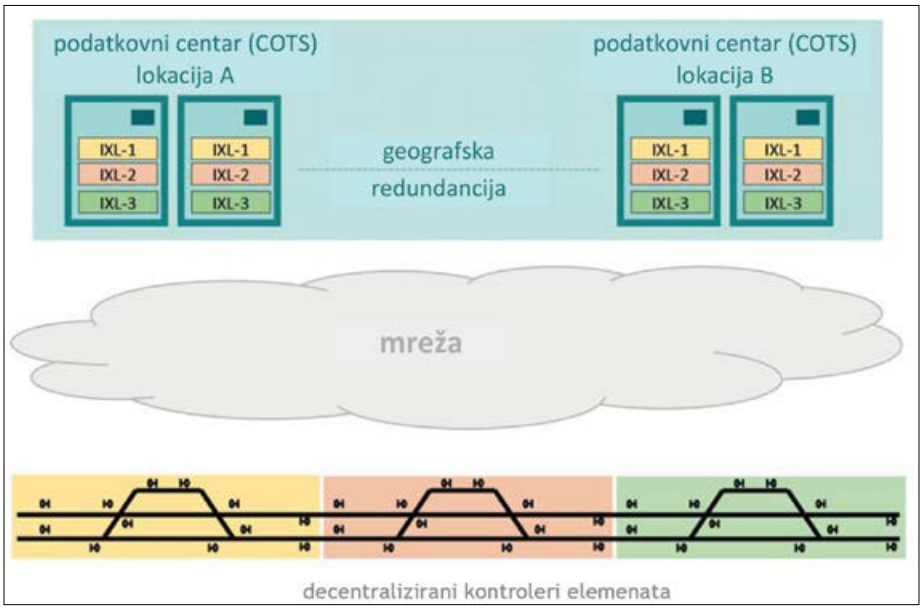
RAZVOJ NOVE SIGURNOSNE PLATFORME DS3 – OD ISTRAŽIVAČKOGA PROJEKTA DO PUŠTANJA U RAD

1. Uvod

Željeznice u sklopu projekata Neupro na nacionalnoj i Eulynx na međunarodnoj razini već više od deset godina sudjeluju u projektiranju i standardizaciji arhitekture željezničkih pruga. Vlasnička, nestandardna rješenja za cjelokupnu funkcionalnost „kolodvorskoga signalno-sigurnosnog uređaja" dijele se na logiku SS uređaja (SSU) i na „samosigurno" upravljanje odnosno kontrolu vanjskih uređaja (npr. svjetlosnih signala, brojača osovina) sa standardiziranim komunikacijskim sučeljima temeljenima na IP protokolu. Prelazak na digitalni kolodvorski SSU (DSSU) nudi mogućnost potpune centralizacije željezničkih signalno-sigurnosnih sustava kao što su logika kolodvorskoga SSUa i logika RBCa. Za standardizaciju hardvera u središnjim podatkovnim centrima i korištenje dostupnih tehnologija za implementaciju vremenski intenzivnih računalnih željezničkih aplikacija te mogućnost potpune centralizacije s geografskom redundancijom za najveću moguću raspoloživost sustava sljedeći korak prema digitalizaciji željezničkog sustava zahtijeva korištenje uobičajenih komercijalno dostupnih (*Commercial-off-the-Shelf* – COTS) industrijskih višejezgrenih računala.

2. Istraživački projekt (od 2013. do 2015.)

Mogućnost korištenja komercijalno dostupnih višejezgrenih računalnih sustava bez ikakva specifičnog hardvera ogroman je korak za signalno-sigurnosne uređaje na kojima Siemens Mobility radi već dugi niz godina.



Slika 1. Centralizirani DSSU (IXL-1/2/3) u podatkovnim centrima temeljenima na uobičajenom komercijalno dostupnim sustavima s geografskom redundancijom

Izvor [1]

Krajem 2011. u organizaciji istraživačke udruge SafeTRANS pokrenut je projekt ARAMiS za korištenje višejezgrenih računalnih sustava u automobilskoj, željezničkoj i zrakoplovnoj industriji (*Automotive Railway Avionics Multicore Systems*; vidi https://news.safetrans-de.org/ausgabe-2012-02/aramis.html) koji financira Njemačko savezno ministarstvo za obrazovanje i istraživanje (BMBF). Cilj je toga projekta priprema za širu upotrebu višejezgrenih računalnih sustava koji moraju ispunjavati visoke zahtjeve ne samo u pogledu sigurnosti i pouzdanosti, već i zaštite od neovlaštenoga pristupa.

Radi istraživanja odgovarajuće hardverske i softverske arhitekture te metoda primjerenih za virtualizaciju i korištenje višejezgrenih računalnih sustava u početku su u projektu bila zastupljena samo automobilska i zrakoplovna industrija.

Početkom 2013. ARAMiS-u su se pridružili i Siemens Mobility i TÜV Rheinland. Istraživanja su pokazala to da su višejezgreni sustavi u osnovi prikladni za korištenje u željezničkim signalno-sigurnosnim sustavima.

Konkretni zahtjevi bili su:

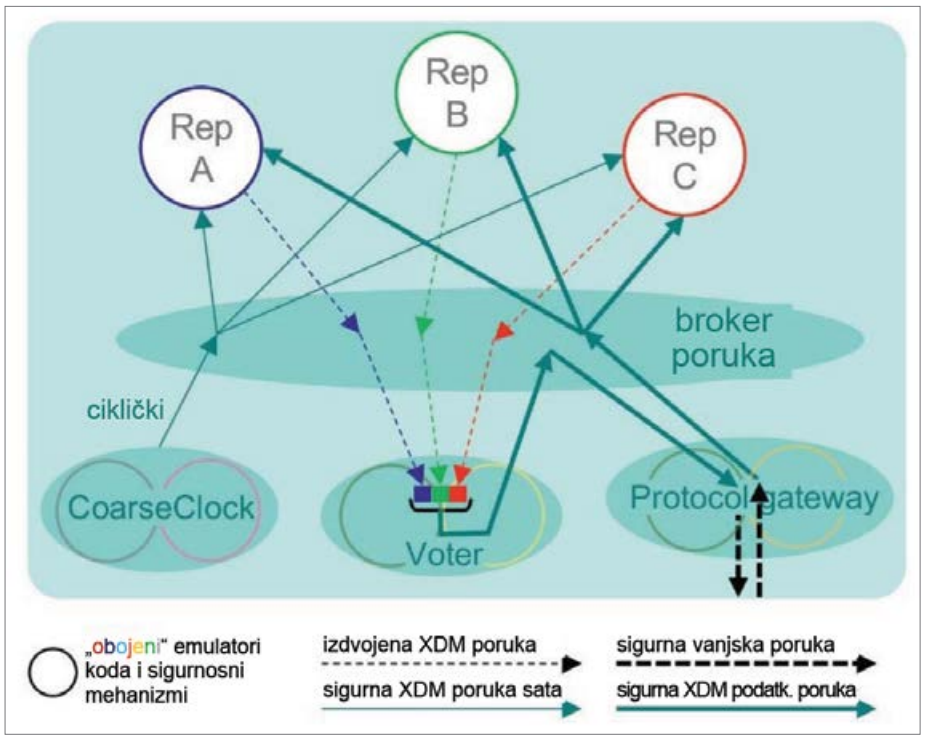
- primjena uobičajenih komercijalno dostupnih višejezgrenih računalnih sustava
- postizanje ciljeva sigurnosti i raspoloživosti za primjenu na željeznici kroz centralizaciju i geografsku redundanciju
- skalabilnost za mogućnost integracije bilo koje primjene na bilo kojoj razini sigurnosti („mješoviti SIL")

na istome komercijalno dostupnom hardveru
- fleksibilnost komunikacijske arhitekture za sudionike na bilo kojoj razini sigurnosti.

Rezultat istraživačkoga projekta bila je koncepcija tehničke arhitekture i sigurnosti u cilju definiranja sigurne softverske platforme *Distributed Smart Safe System* (DS3®) za primjenu sigurnosne razine SIL 4 na komercijalno dostupnim višejezgrenim računalima.

Koncept platforme DS3 temelji se na sljedećim bitnim obilježjima:

- Signalno-sigurnosna aplikacija (npr. logika kolodvorskoga SSUa) istodobno se izvodi paralelno na više instancija (tzv. replikanti – *Rep*) i na različitim fizičkim CPU jezgrama.
- Svaki replikant izvodi se u obliku cikličkoga zadatka (u taktu od npr. 200 m/s) koji kontrolira sigurni sat (*CoarseClock*).
- Rezultate (tj. izlazne informacije) pojedinačnih replikanata provjerava siguran *Voter.*
- Rezultati obrade u *Voteru* prosljeđuju se povezanim sustavima preko sigurnoga protokolnog pristupnika (*Protocol Gateway*).
- Sigurnosni koncept tretira fizičke jezgre višejezgrenoga računalnog sustava kao hardverske jedinice. Sigurne aplikacije izvode se na najmanje dvije fizičke jezgre u diverzitetnim („obojenim“) emulatorima programskoga koda s diverzitetno implementiranim sigurnosnim mehanizmima (npr. ciklička provjera memorije, samoprovjera, aritmetičke operacije, diverzitetno upravljanje memorijom, uključivanje kanala).
- Potrebna redundancija osigurava se na temelju povećanja broja replikanata u računalu i uspostave redundantnoga sustava s dvama računalima. Replikanti (odnosno računala) se nakon eventualnoga pada ponovno pokreću i sinkroniziraju s pokrenutim replikatorima.
- Sva komunikacija između komponenti teče preko novodefiniranoga XDM komunikacijskoga protokola temeljenog na IPu i mehanizmu „objava-pretplata“ (*Publish/Subscribe*) te središnjemu brokeru poruka (koji nije sigurnosno relevantan).



Slika 2. Osnovna arhitektura platforme DS3

Izvor [1]

Tijekom istraživačkoga projekta razvijen je grubi tehnički koncept platforme DS3 i izrađeni su demonstracijski prototipovi softverskih komponenti, dok je osnovnu prikladnost koncepta potvrdio procjenitelj iz TÜV Rheinlanda.

3. Studija izvodljivosti (od 2016. do 2017.)

Siemens Mobility prepoznao je potencijal koncepta DS3 još 2015. S obzirom na to da u to vrijeme još nisu svi bili uvjereni u stvarnu izvedivost i prihvatljivost toga koncepta, dodatno je provedena studija izvedivosti sa sljedećim ciljevima:

- rješavanje otvorenih pitanja koja nisu bila do kraja promišljena (npr. sigurni softverski *Voter* i sigurni sat *CoarseClock*)
- definiranje koncepta migracije za postojeće željezničke sustave
- razmatranje komunikacijskih protokola za *Eulynx/NeuPro*
- procjena sigurnosti i stručna procjena neovisnoga stručnjaka u vezi s ishođenjem odobrenja za željezničke sustave
- praktična potvrda izvedivosti na temelju prototipa i migracije specifičnoga kolodvorskog SSUa.

3.1. Pilot-sustav (kolodvorski SSU Trackguard Simis AT)

Kao pilot-sustav za praktični dio studije izvedivosti korišten je kolodvorski signalno-sigurnosni uređaj Trackguard Simis AT koji se temelji na računalnoj platformi Trackguard Simis ECC s aplikacijom sigurnosne razine SIL 4 za austrijske željeznice u računalu postavnice (STWR) te komunikacijskim sučeljima IP prema ulazno-izlaznim računalima

(EAR), susjednim kolodvorskim signalno-sigurnosnim uređajima (NSTW), prometno-upravljačkome sustavu (OCS) i dijagnostici.

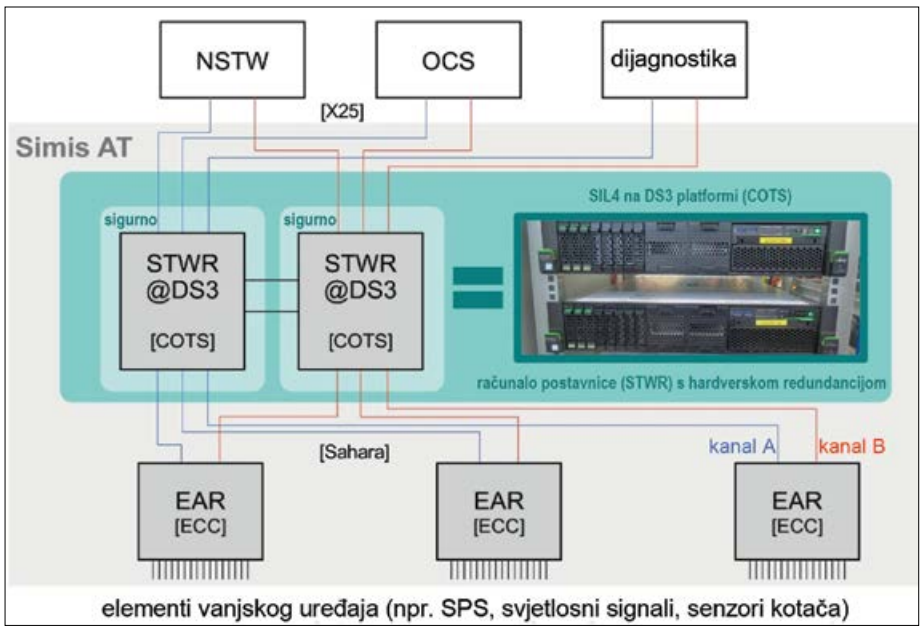
Za migraciju aplikacije računala postavnice na platformu DS3 korištena je sljedeća konfiguracija:

- Kao središnje računalo postavnice korištena je softverska platforma DS3 na dva komercijalno dostupna višejezgrena računala.
- Oba računala postavnice međusobno se kontinuirano sinkroniziraju. U slučaju pada jednoga računala aplikacija se sigurno izvodi dalje na drugome računalu.
- Sva komunikacija s povezanim računalima (protokol [X25] odnosno [Sahara]) teče u dvokanalnome načinu rada s dva transportna kanala (A/B) između obaju povezanih računala.
- Promjena platforme s ECC na DS3 nema nikakvog (povratnog) utjecaja na komunikacijska sučelja računala postavnice, odnosno posljedično na povezane sustave. Računalo postavnice pokazalo se kao idealan pilot-sustav za studiju izvedivosti koji je omogućio ispitivanje ne samo osnovne izvedivosti nove platforme, već i mogućnosti „migracije postojećih željezničkih sustava ECC na novu platformu DS3".

3.2. Migracija operativnoga sustava ECC

Kako bi se utjecaj na postojeću i odobrenu primjenu računala postavnice sveo na najmanju moguću mjeru, migracija računala obuhvaćala je i migraciju osnovnih usluga operativnog sustava ECC (*Basic ECC OS*) na novu platformu DS3.

Taj je aspekt bio vrlo važan jer treba utrti put migraciji i drugih željezničkih sustava temeljenih na sustavu ECC (npr. drugih kolodvorskih signalno-sigurnosnih uređaja i sustava RBC).



Slika 3. Arhitektura sustava Trackguard Simis AT s računalom postavnice na DS3 platformi

Izvor [1]

Za potrebe studije izvedivosti izrađeni su i prototipovi softverskih komponenti za platformu DS3 (npr. emulator koda, broker poruka, osnovno glasanje – ***voting***) te provizorno prilagođeni odgovarajući dijelovi operativnoga sustava ECC za rad na toj platformi.

Kao rezultat toga aplikacija računala postavnice mogla se izravno i bez ikakve prilagodbe integrirati u novi operativni sustav ECC na platformi DS3 s uobičajenim komercijalno dostupnim hardverom, čime je praktički potvrđena funkcionalnost osnovnoga koncepta.

Nakon više od tridesetogodišnjega evolucijskog razvoja to je već treća generacija platforme za računala STWR sustava Trackguard Simis AT (1990. platforma SCM86, 2000. platforma ECC i 2018. platforma DS3).

3.3. Preliminarna analiza opasnosti

Usporedno s razvojem prototipa provedena su i arhitektonska poboljšanja tehničkoga koncepta te pripremljene i verificirane odgovarajuće procjene sigurnosti na temelju preliminarne analize opasnosti. Iz njih proizlazi to da „je platforma DS3 primjerena za aplikacije SIL 4 na komercijalno dostupnom hardveru", čime je postavljen smjer za pokretanje razvojnoga projekta za prvo izdanje platforme DS3.

4. Razvojni projekt (od 2017. do 2020.)

Razvojni projekt počeo je zadatkom razvoja potpuno novoga sustava na temelju kriterija odnosno specifikacija navedenih u nastavku.

4.1. „Mješoviti SIL" na platformi DS3

Komponentno orijentiranom arhitekturom platforme DS3 definirani su ne samo dijelovi važni za sigurnost (tj. radno okružje za izvođenje replikanata, „glasanje", sigurni sat *CoarseClock* i protokolni pristupnik), već i drugi dijelovi koji nisu povezani sa sigurnošću (broker poruka, dijagnostika, pokretanje sustava) i koji se mogu izvoditi na „nesigurnome" operativnom sustavu (*Windows, Linux*).

Aspekt korištenja raznolikih SIL razina na istoj platformi morao se uzeti u obzir

i za definiranje internoga komunikacijskog protokola platforme XDM te funkcionalne arhitekture softverskih komponenti DS3.

4.2. Protokol sigurne komunikacije XDM po načelu „objava-pretplata“ (*Publish/Subscribe*)

Novi komunikacijski protokol XDM kao temelj za komunikacijski orijentiranu arhitekturu platforme, koji je na principu objave i pretplaćivanja omogućio najbolju moguću fleksibilnost sustava, zahtijevao je i temeljitu promjenu funkcionalnoga i redundantnoga protoka podataka između pojedinih komponenti platforme DS3 (replikatori, ***Voter*** i drugi)

Pritom su definirani i sigurnosni mehanizmi protokola XDM, i to na način koji omogućuje sudjelovanje i nesigurnih komunikacijskih partnera u XDM komunikaciji.

Protokol XDM, koji je ugrubo definiran za vrijeme istraživačkoga projekta, tijekom razvojnoga projekta dodatno je preciziran na temelju pripadajućih procjena sigurnosti te je za vrijeme razvoja odnosno integracije poboljšan i na temelju novih saznanja.

Budući da su se do sada uglavnom koristili komunikacijski protokoli na temelju međusobnih veza (kao što je to RaSTA), XDM kao protokol emitiranja promjena je paradigme za sigurnu komunikaciju prema normi DIN EN 50159, pri čemu se sigurnosna načela te norme mogu primijeniti i na XDM.

4.3. Sigurnost i dostupnost

4.3.1. Platforma DS3

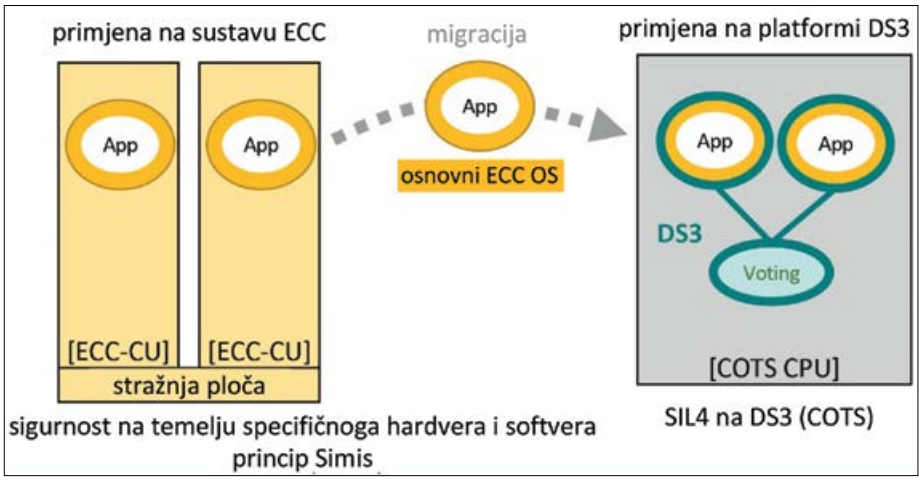
Za sigurnost platforme DS3 („glasanje“, sigurni sat *CoarseClock* i protokolni pristupnik) trebalo je definirati i implementirati tzv. sigurnosni uzorak (*Safety Pattern*).

Osim toga potreban je komponentno orijentiran koncept redundantnosti, što znači da sve komponente platforme DS3 moraju biti redundantne i da njihova funkcionalnost mora biti osigurana na oba komercijalno dostupna računala.

Svaki ispad komponente DS3 mora se detektirati i „otkloniti“ (ponovnim pokretanjem određene komponente). Tijekom ispada komponente cjelokupnu funkcionalnost mora preuzeti redundantna komponenta u drugome računalu.

Primjer:

Punu funkcionalnost sigurnoga sata *CoarseClock* za oba računala u slučaju ispada komponente na prvome računalu omogućava sigurni sat na drugome računalu.



Slika 4. Migracija operativnoga sustava ECC na platformu DS3

Izvor [1]

4.3.2. Aplikacija

Radi osiguranja zahtijevane razine sigurnosti i dostupnosti sustava trebalo je, među ostalim, definirati i realizirati odgovarajući uzorak paralelnoga i sigurnoga izvršavanja replikanata, uključujući postupak sigurnog „glasanja“ (*voting*). Sve neispravnosti otkrivene u replikantima treba identificirati, a neispravni replikant mora se zaustaviti te ponovno pokrenuti i sinkronizirati.

S tom namjenom primjenjuje se inteligentno većinsko „glasanje“ koje se prilagođava broju aktivnih, zaustavljenih i ponovno pokrenutih replikanata na oba uključena računala.

4.4. Automatizirani komunikacijski orijentirani ispitni sustav

Jedinično i integracijsko testiranje platforme DS3 zahtijevalo je i novi ispitni sustav s mogućnošću adresiranja i evaluacije novodefiniranih XDM sučelja testnih objekata ne samo u cilju testiranja pojedinih komponenti DS3, već i u cilju integracije većega broja komponenti DS3, što je izvedeno s najvišim mogućim stupnjem automatizacije u najrazličitijim testnim konfiguracijama.

5. Integracija u Simis AT

Migracijom operativnoga sustava ECC na platformu DS3 omogućen je prijenos aplikacije računala postavnice na platformu DS3 bez ikakvih prilagodbi i povratnih utjecaja na povezane sustave kao što su EAR, OCS i NSTW. Vrlo važan i koristan čimbenik u svim aktivnostima integracije bio je i zahtjev da aplikacija računala postavnice mora ostati nepromijenjena.

Integracija platforme DS3 u Simis AT provodila se istodobno sa studijom izvedivosti. U slučaju problema na testnome uređaju Simis AT uvijek je bilo jasno da njihov uzrok leži u novoj platformi. Zato na razini između računala postavnice i platforme DS3 nikada nije bilo upitno tko je što i zašto promijenio i zbog čega nakon toga „više ništa ne radi“.

5.1. Konfiguracija platforme DS3 za računalo postavnice

Za primjenu platforme DS3 sa Simisom AT sustav je konfiguriran na sljedeći način:

- izvođenje aplikacije računala postavnice na dva višejezgrena komercijalno dostupna računala s po četiri (ukupno osam) replikanata
- ciklus obrade za aplikaciju računala postavnice od 200 m/s
- komunikacijski protokoli Sahara i X25 za povezana računala
- komercijalno dostupna platforma (procesor i operativni sustav) na temelju provjerenih industrijskih višejezgrenih računala *Windows* koja se već koriste u prometno-upravljačkim sustavima sigurnosne razine SIL 2.

5.2. Procjena i odobrenje

U vrlo ranoj fazi (tj. istodobno s integracijom platforme DS3) pokrenut je i postupak ocjenjivanja i odobravanja sustava Trackguard Simis AT. Sve ključne komponente sigurnosne arhitekture platforme DS3, uključujući migraciju operativnoga sustava ECC, su tijekom cijeloga razvoja usklađivane i razjašnjene s procjeniteljima i odobravateljima.

I u tom se slučaju kao vrlo koristan pokazao zahtjev za neprovođenjem izmjena na aplikaciji računala postavnice jer se tijekom regresijskih testova s postojećim testnim slučajevima moglo usredotočiti na sigurnosnu arhitekturu platforme DS3 s (ponovnom) potvrdom istovjetne funkcionalnosti odnosno karakteristika aplikacije na prethodnoj platformi ECC i na novoj platformi DS3.

6. Pilot-projekt „Simis AT@ DS3 na kolodvorskom SSUu Achau (ÖBB)“

S obzirom na to da je kao pilot-sustav za platformu DS3 odabran Trackguard Simis AT s primjenom kolodvorskog SSUa za Austrijske savezne željeznice, kao partner za izvedbu projekta za testiranje i uvođenje nove platforme odabrane su Austrijske savezne željeznice (ÖBB).

Radi implementacije novoga rješenja Siemens Mobility je s tvrtkom ÖBB Infrastruktur AG kao idealnim partnerom za planirani projekt sklopio ugovor za izvedbu projekta „Kolodvorski signalno-sigurnosni uređaj Achau“.

Pri odabiru pilot-postrojenja za kolodvorski SSU Achau već je u fazi projektiranja uzeto u obzir to da tijekom izgradnje, puštanja u pogon i eksploatacije ne smije dolaziti do ograničenja te da postrojenje mora raditi potpuno u skladu s važećim specifikacijama za promet i za održavanje.

Suradnja s tvrtkom ÖBB Infrastruktur AG i njezinim neovisnim stručnjakom (osoba ovlaštena za puštanje u uporabu prema članku 40. austrijskoga zakona o željeznici – EisbG) išla je ruku pod ruku ne samo u pogledu teorijskih razmatranja za odobrenje proizvoda Trackguard Simis AT, već i sa stajališta praktičnoga testiranja (npr. probne vožnje i pregledi naručitelja na licu mjesta, uključujući posebne prometne procedure, te testiranje na Siemensovu ispitnom postrojenju u Beču).

Sva testiranja na sustavu Simis AT tijekom razvoja nove platforme DS3 provedena su za konfiguraciju ispitnoga kolodvora Simis AT te odgovarajuću konfiguraciju uređaja naručitelja u Achauu.

Za testiranje na licu mjesta u Achauu komercijalno dostupna računala postavnice postavljena su neposredno uz operativno ECC računalo i zato su testovi na licu mjesta (npr. tijekom prekida prometa) bili relativno jednostavni. Za prebacivanje među uređajima samo su prespojeni odgovarajući mrežni LAN kabeli. Radi stjecanja dodatnih iskustava te izgradnju povjerenja u novu platformu, ta su testiranja također uključivala realno operativno ispitivanje otpornosti koje su provodili ÖBBovi stručnjaci priključenim realnim vanjskim uređajem.

7. Puštanje u rad pilot-projekta Achau (ÖBB)

Nakon gotovo sedam godina istraživanja, studija izvedivosti i razvoja platforme DS3, dana 14. studenoga 2020. konačno je došlo vrijeme za prebacivanje mrežnih LAN kabela s ECC računala na komercijalno dostupna računala platforme DS3 te za puštanje aplikacije postavnice na platformi DS3 u Achauu u rad – u početku samo za četverodnevnu fazu testiranja i ispitivanja s ograničenom funkcijom regulacije prometa (bez ovisnosti signala i s odgovarajućim prometnim procedurama), a od 18. studenoga 2020. i s neograničenom funkcijom regulacije redovitoga željezničkog prometa. Od tada se pilot-projekt Achau nalazi pod svakodnevnim nadzorom ÖBBova osoblja za održavanje (preko daljinskog pristupa servisnome računalu), pri čemu dnevna analiza podataka do isteka uredničkoga roka nije pokazala nikakve nepravilnosti u radu. Aplikacija računala postavnice na platformi DS3 radi bez ikakvih neregularnosti.

Platforma DS3 je za ÖBB važan korak prema digitalizaciji i odlučujući temelj za izgradnju buduće arhitekture kolodvorskih signalno-sigurnosnih uređaja.

8. Izgledi za budućnost

Pilot-projekt DS3 sa sustavom Trackguard Simis AT u cilju definiranja, procjene i implementacije nove sigurnosne platforme DS3 za realizaciju aplikacija sigurnosne razine SIL 4 na „nesigurnim“ višejezgrenim i komercijalno dostupnim računalima bio je prvi i najvažniji korak na putu prema ishođenju rješenja za podatkovne centre temeljene na uobičajenim komercijalno dostupnim računalima za primjenu u željezničkim signalno-sigurnosnim sustavima.

Slijede daljnja inkrementalna funkcionalna poboljšanja platforme DS3 kao što su:

- IT sigurnost
- rad u virtualizaciji
- inteligentni elementi vanjskoga uređaja

– rad s više poslužitelja i s distribuiranim računalnim sustavima za osiguranje geografske redundancije.

Sljedeći koraci obuhvaćaju i migraciju drugih sustava (npr. radio blok-centra) na DS3.

Radi se tek o prvome koraku na dugome (i još nezavršenome) putu prema razvoju nove sigurnosne platforme.

Napomena: Članak je bio prvi put objavljen u stručnom časopisu SIGNAL&DRAHT www.eurailpress.de/sd

Literatura:

[1] Siemens Mobility

UDK: 004.9:656.2

Adresa autora:

Sonja Steffens
voditeljica proizvoda za platformu DS3
Siemens Mobility GmbH
Adresa: Ackerstraße 22, D38126 Braunschweig, Njemačka
e-pošta: sonja.steffens@siemens.com

Walter Valvoda
voditelj proizvoda za Simis AT
Siemens Mobility Austria GmbH
Adresa: Siemensstraße 90, A1210 Beč, Austrija
e-pošta: walter.valvoda@siemens.com

SAŽETAK:

RAZVOJ NOVE SIGURNOSNE PLATFORME DS3 –OD ISTRAŽIVAČKOGA PROJEKTA DO PUŠTANJA U RAD

Prelazak na digitalne kolodvorske signalno-sigurnosne uređaje otvara mogućnosti potpune centralizacije željezničkih logističkih signalno-sigurnosnih sustava. Digitalizacija željezničkog sustava zahtjeva i primjenu višejezgrenih računalnih sustava. Stalni razvoj novih sustava temelji se na postizanju ciljeva sigurnosti i postizanja inteligentnih sustava željeznice.

Ključne riječi: *signalno-sigurnosni uređaj, višejezgreni računalni sustav, digitalizacija, centralizacija*

Kategorizacija: *stručni rad*

SUMMARY

DEVELOPMENT OF THE NEW SECURITY PLATFORM DS3 - FROM RESEARCH PROJECT TO USING

The transition to a digital station signalling device opens up the possibilities of full centralization of railway logistics signalling systems. The digitization of the railway system requires the application of multi-core computer systems. The continuous development of new systems is based on achieving safety objectives and achieving intelligent rail systems.

Keywords: *signalling device, multi-core computer system, digitalization, centralization*

Categorization: *professional paper*