KOMUNIKACIONI PROTOKOLI U SIL4 SISTEMIMA

Ivan Kokić, Marko Nikolić, Jovana Novaković, Željko Stojković
Univerzitet u Beogradu – Institut „Mihajlo Pupin“,
ivan.kokic@pupin.rs, marko.nikolic@pupin.rs,
jovana.novakovic@pupin.rs, zeljko.stojkovic@pupin.rs

Rezime: *U ovom radu je predstavljena evaluatorska jedinica brojača osovina koja se koristi za kontrolu zauzetosti železničkih odseka. Realizovani evaluator ispunjava SIL4 (nivo integriteta bezbednosti 4) definisan standardom EN 50129. Opisane su funkcije koje obavlja evaluatorska jedinica, njeni interfejsi i blok šema u kojoj su predstavljeni podsistemi evaluatora. Detaljnije su opisani komunikacioni protokoli korišćeni u evaluatoru, a koji zadovoljavaju standard EN 50159. Definisane su moguće pretnje koje utiču na bezbednost komunikacije, kao i odgovarajuće kontramere kojima se smanjuju bezbednosni rizici. Na kraju, dat je proračun verovatnoće hazardnog događaja usled grešaka u komunikaciji. Dokazano je da je ova verovatnoća manja od dozvoljene verovatnoće hazardnog događaja za SIL4.*

Ključne reči: *bezbednost, brojač osovina, hazard, SIL.*

1. Uvod

Brojač osovina je uređaj koji se koristi za kontrolu zauzetosti železničkih odseka. Sastoji se od evaluatorske jedinice i senzora točka šinskog vozila. Evaluator je direktno povezan sa senzorima i od njih prima informacije o njihovom trenutnom stanju, odnosno da li je točak detektovan ili nije. Senzori točka se uvek montiraju u paru, tako da je obezbeđena informacija o smeru kretanja točka, odnosno šinskog vozila. Na osnovu informacija dobijenih od senzora, evaluator izračunava trenutni broj osovina u odseku. Kada taj broj postane jednak nuli brojač osovina proglašava odsek slobodnim. Evaluator se montira unutar relejne prostorije železničke stanice, putnog prelaza ili automatskog pružnog bloka, dok su senzori točka montirani direktno na šini.

Evropska regulativa zahteva da brojač osovina zadovolji SIL4 (nivo integriteta bezbednosti 4; eng. *Safety Integrity Level* - SIL) iz standarda EN 50129 [1]. Osim ovog standarda, moraju biti zadovoljeni zahtevi propisani standardima EN 50126 [2], EN 50128 [3] i EN 50159 [4]. Pored ovih opštih standarda, postoji i specijalizovani standard koji se odnosi na brojač osovina EN 50617-2 [5].

Na početku razvoja evaluatora brojača osovina proučena su dotadašnja rešenja poznatih svetskih i regionalnih proizvođača u ovoj oblasti: *Frauscher* [6] [7], *Siemens* [8], *Thales* [9] i *Altpro* [10]. Treba napomenuti da su dostupne samo tehničke karakteristike

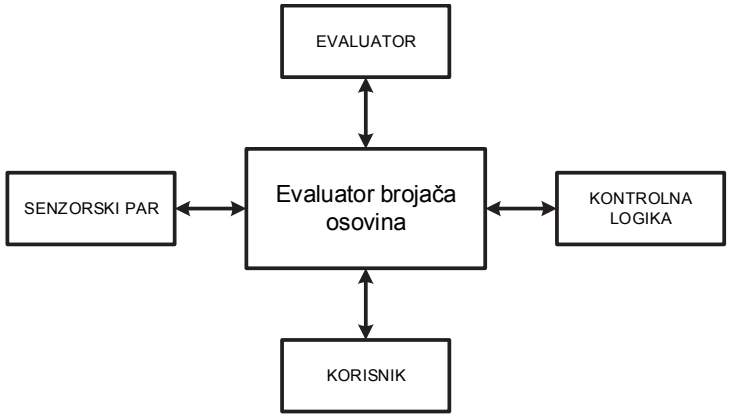
brojača osovina namenjene korisnicima, dok arhitektura i detalji realizacije ovih sistema nisu. Od pomenutih brojača osovina svi koriste relejne izlaze, osim [7] u kom se koristi *Ethernet* interfejs. U većini slučajeva brojač osovina kontroliše više odseka, osim [6] koji kontroliše samo jedan odsek. Komunikacija između senzora i evaluatora je uglavnom jednosmerna, pri čemu se koristi amplitudski [6] ili frekvencijski modulisan signal [8]. Protokol komunikacije između evaluatora i senzora je korišćen u [10].

Evaluator brojača osovina BROS, razvijen u Institutu „Mihajlo Pupin“, kontroliše do osam odseka i direktno dobija informacije od najviše dvanaest senzorskih parova. Senzori šalju informaciju o svom stanju slanjem frekvencijski modulisanog signala. Evaluator daje informaciju o zauzetosti odseka korišćenjem relejnih izlaza, imajući u vidu da je namenjen, pre svega, Železnicama Srbije u kojima je dominantna relejna logika upravljanja. Predlog arhitekture brojača osovina dat je u radu [11], dok rad [12] predstavlja prototip brojača osovina koji je prethodio sertifikovanoj verziji.

Evaluator BROS dobio je SIL4 sertifikat od strane ovlašćenog tela. U procesu sertifikacije je dokazano da evaluator zadovoljava sve zahteve propisane standardima. U slučaju brojača osovina jedini hazardni događaj je da on proglasi neki od odseka slobodnim, a da je on u stvarnosti zauzet. Cilj analize hazarda je da se identifikuju svi mogući uzroci usled kojih hazardni događaj može da se desi i da se definišu kontramere kojima se verovatnoća hazardnog događaja smanjuje na prihvatljivu vrednost za dati nivo integriteta bezbednosti. Ta dozvoljena verovatnoća hazardnog događaja se naziva prihvatljivi nivo opasnosti (eng. *Tolerable Hazard Rate* – THR). Jedan od uzroka hazardnog događaja su greške u komunikaciji. Ovaj rad detaljnije opisuje komunikacione protokole korišćene u brojaču osovina. Definisane su moguće bezbednosne pretnje u komunikaciji, kao i odgovarajuće kontramere, a zatim su dati osnovni elementi proračuna verovatnoće hazardnog događaja usled grešaka u komunikaciji i na osnovu toga je pokazano da komunikacioni protokoli zadovoljavaju SIL4.

2. Kratak opis evaluatorske jedinice

Evaluator poseduje četiti interfejsa koja omogućavaju njegovu punu funkcionalnost, što je prikazano na slici 1.



Slika 1. Interfejsi evaluatorske jedinice brojača osovina

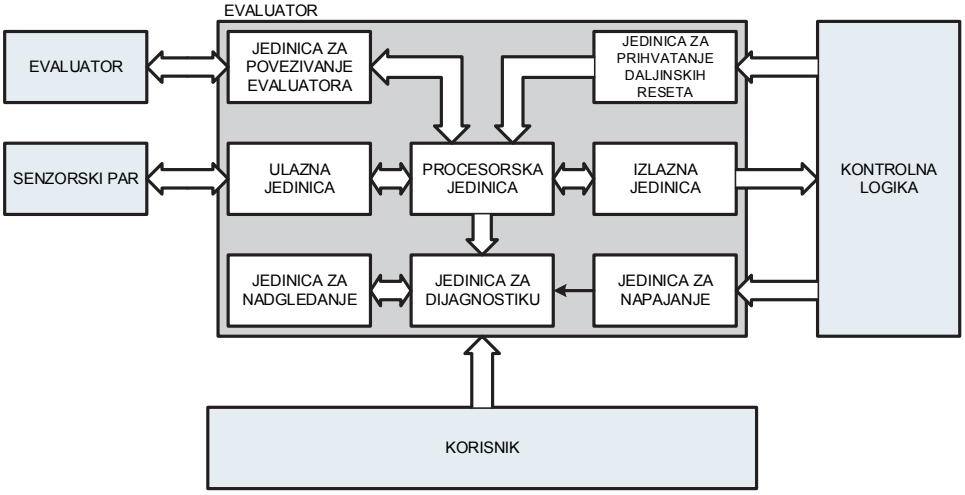
Interfejs za povezivanje sa senzorskim parom služi za napajanje senzorskog para i prijem informacija od svakog pojedinačnog senzora iz senzorskog para o njegovom trenutnom stanju.

Interfejs za povezivanje sa drugim evaluatorima se koristi u slučajevima kada evaluator ne dobija direktno informacije od svih senzorskih parova koji učestvuju u kontroli odseka, već su oni direktno povezani na drugi evaluator. Tada je potrebno dobiti te informacije od odgovarajućeg evaluatora.

Interfejs za povezivanje sa kontrolnom logikom stanice, putnog prelaza ili automatskog pružnog bloka omogućava napajanje potrebno za rad evaluatora i prijem signala za daljinsko razrešenje (resetovanje) odseka. Sa druge strane, evaluator šalje informaciju o trenutnom stanju svih odseka koje kontroliše pomoću relejnih izlaza.

Korisnički interfejs omogućava korisniku uvid u trenutno stanje uređaja, kao i pregled svih događaja koji se upisuju u trajnu memoriju uređaja.

Evaluatorska jedinica se sastoji od nekoliko funkcionalnih celina, pri čemu samo neke od njih imaju uticaj na bezbednost. Blok šema evaluatora je prikazana na slici 2.



Slika 2. Blok šema evaluatorske jedinice brojača osovina

Jedinica za napajanje se povezuje na spoljašnje napajanje koje obezbeđuje kontrolna logika i od njega proizvodi napajanja potrebna za ispravno funkcionisanje evaluatora.

Jedinica za dijagnostiku treba da prati rad celog sistema u pozadini i da obezbedi dijagnostičke informacije pomoću kojih korisnik može lako da utvrdi trenutno stanje uređaja, kao i da analizira prethodni rad uređaja. Dijagnostička jedinica sadrži nezavisnu memoriju u kojoj se čuvaju sve dijagnostičke informacije.

Jedinica za nadgledanje treba da pošalje dijagnostičke informacije koje je dobila od jedinice za dijagnostiku centru za nadgledanje rada brojača osovina [13].

Jedinica za povezivanje evaluatora treba da obezbedi prosleđivanje informacija o stanju senzora i stanju odseka između dva evaluatora.

Jedinica za prihvatanje daljinskih reseta treba da obezbedi prihvatanje signala za daljinsko resetovanje odseka i njihovo prosleđivanje procesorskoj jedinici.

Ulazna jedinica treba da obezbedi napajanje za senzorski par, prihvatanje i kondicioniranje senzorskih signala i njihovo prosleđivanje procesorskoj jedinici.

Izlazna jedinica treba da obezbedi informaciju o procenjenom stanju odseka kontrolnoj logici korišćenjem relejnih izlaza, u skladu sa komandom koju dobija od procesorske jedinice i da pošalje informaciju o stvarnom stanju relejnih izlaza procesorskoj jedinici.

Procesorska jedinica predstavlja centralni deo evaluatora brojača osovina i ima glavnu ulogu u odlučivanju. Ova jedinica prima sve potrebne ulazne informacije, pre svega od senzora, obrađuje ih i na osnovu njih odlučuje kakvo stanje odseka treba da bude. Na osnovu procenjenog stanja odseka, procesorska jedinica šalje odgovarajuću komandu izlaznoj jedinici.

3. Opšti principi projektovanja brojača osovina prema standardima

Standard EN 50126 [2] definiše životni ciklus sistema kao niz faza, pri čemu svaka faza ima jasno definisane zadatke i ciljeve. On pokriva život sistema od inicijalne zamisli, preko projektovanja, instalacije, primene, do njegovog uklanjanja i odlaganja. Standard daje smernice kako planirati, upravljati, kontrolisati i pratiti sve aspekte sistema pojedinačno za svaku fazu njegovog životnog ciklusa kako bi se dobio željeni proizvod. Standardom su predviđene sledeće faze životnog ciklusa sistema: (1) koncept; (2) definisanje sistema i uslova primene; (3) analiza rizika; (4) definisanje sistemskih zahteva; (5) definisanje sistemske arhitekture i dodela sistemskih zahteva; (6) projektovanje sistema; (7) proizvodnja; (8) ugradnja; (9) validacija sistema; (10) prihvatanje sistema, (11) rukovanje i održavanje; (12) uklanjanje i odlaganje.

Proces razvoja nekog sistema je često iterativan, što znači da je potrebno više puta proći kroz neke faze životnog ciklusa dok se ne dođe do prihvatljivog rezultata, odnosno do sistema koji zadovoljava definisane zahteve. Takođe, tokom razvoja sistema u bilo kojoj fazi njegovog životnog ciklusa može doći do određenih izmena i proširenja.

Osnovni cilj standarda jeste da se praćenjem smernica koje on definiše dobije proizvod koji zadovoljava propisane RAMS zahteve koji se odnose na pouzdanost, dostupnost, održivost i bezbednost sistema (eng. *Reliability*, *Availability*, *Maintainability*, and *Safety*). Glavni parametar za klasifikaciju sistema je nivo integriteta bezbednosti. Integritet bezbednosti predstavlja verovatnoću da će sistem na zadovoljavajući način izvršiti propisane bezbednosne funkcije pod svim navedenim uslovima u navedenom vremenskom periodu. Standard definiše četiri različita nivoa integriteta bezbednosti koji su dati u tabeli 1.

Tabela 1. Nivoi integriteta bezbednosti

Nivoi integriteta bezbednosti (SIL)	**Prihvatljiv intenzitet opasnosti (THR)**
4	$10^{-9} \leq THR < 10^{-8}$
3	$10^{-8} \leq THR < 10^{-7}$
2	$10^{-7} \leq THR < 10^{-6}$
1	$10^{-6} \leq THR < 10^{-5}$

Što je veći nivo integriteta bezbednosti nekog sistema, to je manja verovatnoća da će on otkazati pri izvršavanju posmatrane bezbednosne funkcije. Za različite nivoe

integriteta bezbednosti standard predviđa različite korake po fazama koje je neophodno i preporučljivo sprovesti da bi sistem bio zadovoljavajući. Faze životnog ciklusa sistema i njihov redosled jeste isti za sve nivoe, ali su zadaci i očekivani rezultati po fazama vrlo različiti, pri čemu se težina povećava sa povećanjem nivoa integriteta bezbednosti. Za stvaranje pouzdanih sistema treba identifikovati faktore koji mogu da utiču na RAMS sistema, treba proceniti njihove posledice, a uzrocima ovih posledica treba upravljati tokom celog životnog ciklusa sistema primenom odgovarajućih kontramera.

Sistem može da bude definisan kao skup podsistema koji su zajedno povezani na odgovarajući način kako bi se postigla potrebna funkcionalnost. Svakom podsistemu se dodeljuje odgovarajuća funkcija. Funkcionisanje sistema u celini zavisi od funkcionisanja njegovih podsistema, odnosno ukoliko neki podsistem nije ispravan, funkcija sistema u kojoj učestvuje posmatrani podsistem neće biti ispravna. Otkazi u sistemu imaju uticaja na rad sistema, a samim tim i na RAMS sistema. Na RAMS se utiče na tri načina: (1) sistemski uslovi – izvori otkaza koji su interno uneti u sistem u nekoj fazi životnog ciklusa sistema; (2) radni uslovi – izvori otkaza koji se javljaju u sistemu tokom njegovog rada; (3) uslovi održavanja – izvori otkaza uneti u sistem tokom procedure održavanja.

Dok svi otkazi loše utiču na pouzdanost sistema samo neki specifični otkazi imaju loš uticaj na bezbednost. Ovo su bezbednosni otkazi. Potrebno ih je sve identifikovati, odrediti na koju funkciju utiču, a zatim izvršiti procenu rizika za svaki pojedinačni bezbednosni otkaz. Kada je nivo integriteta bezbednosni dodeljen funkciji i kada su identifikovani svi bezbednosni otkazi koji utiču na tu funkciju, na osnovu procenjenog rizika se predviđaju odgovarajuće kontramere u cilju smanjenja rizika ispod prihvatljivog nivoa. Standard predviđa korišćenje odgovarajućih arhitektura, metoda, alata i tehnika za implementaciju bezbednosnih funkcija. Standard EN 50128 [3] definiše metode, alate i tehnike za razvoj softverskih sistema, dok standard EN 50129 [1] definiše postupke prihvatanja i odobravanja elektronskih sistema (odnosi se uglavnom na hardver). Integritet bezbednosti se može posmatrati kao kombinacija elemenata koje se mogu kvantifikovati (slučajni otkazi) i elemenata koji se ne mogu kvantifikovati (sistematski otkazi). Integritet bezbednosti obuhvata dve komponente: integritet na sistematske otkaze i integritet na slučajne (nasumične) otkaze.

Integritet na sistematski otkaz je nekvantitativni deo integriteta bezbednosti i odnosi se na opasne sistematske neispravnosti koje su izazvane ljudskim propustima u raznim fazama životnog ciklusa sistema. Integritet na sistematske otkaze se postiže korišćenjem odgovarajućih sistema za kontrolu kvaliteta i kontrolu bezbednosti. Pošto nije moguće oceniti integritet na sistematske otkaze pomoću kvantitativnih metoda, standard predviđa metode, alate i tehnike koje, kada se koriste efikasno, pružaju odgovarajući nivo pouzdanosti da će sistem biti realizovan sa navedenim nivoom integriteta.

Integritet na slučajne otkaze se odnosi na opasne nasumične neispravnosti, najčešće zbog konačne pouzdanosti hardverskih komponenata. Kvantitanivna procena integriteta na nasumične otkaze se vrši pomoću probabilističkog proračuna. Oni se zasnivaju na poznatim podacima za intenzitet otkaza hardverskih komponenti i na vremenima otkrivanja nasumičnih hardverskih otkaza.

Od svih delova evaluatora brojača osovina samo jedinica za dijagnostiku i jedinica za nadgledanje nemaju bezbednosnu funkciju i zato nisu bile predmet analiza u procesu sertifikacije. Naime, da bi se neki podsistem isključio iz dalje analize potrebno je uraditi analizu uticaja na podsisteme koji imaju bezbednosnu funkciju, odnosno potrebno je utvrditi da li ovi podsistemi mogu da poremete rad podsistema sa bezbednosnim

funkcijama tako da se njihov integritet dovede u pitanje. Kako ove dve jedinice ne generišu nikakve signale ka jedinicama koje imaju bezbednosne funkcije, već ih samo primaju nije bilo potrebno ispitivati njihov uticaj. Otkazi ove dve jedinice evaluatora ne smanjuju njegovu raspoloživost, već samo dovode do gubitka dijagnostičkih informacija.

Prilikom projektovanja jedinica koje imaju bezbednosnu funkciju primenjivane su sledeće tehnike: (1) različitost arhitektura; (2) redundatnost; (3) kompozitni *fail-safety*; (4) reaktivni *fail-safety*; (5) inherentni *fail-safety*.

Procesorska jedinica evaluatora poseduje dva odlučivačka elementa koji rade u paraleli u arhitekturi „2 od 2“. Oba odlučivačka elementa su realizovana pomoću mikrokontrolera koji zadovoljaju SIL3. Svaki odlučivački element prima svoju kopiju senzorskih signala i nezavisno ih obrađuje. Algoritmi za obradu senzorskih signala koje izvršavaju ovi odlučivački elementi se razlikuju. Ovim se povećava stepen nezavisnosti u odlučivanju i smanjuje verovatnoća greške sa istim uzrokom, odnosno da će greška jednog algoritma biti prisutna i u drugom. Pojava greške na jednom odlučivačkom elementu nema direktni uticaj na drugi odlučivački element.

Izlazna jedinica evaluatora koristi dva relea za generisanje stanja jednog odseka. Kada su relea neaktivna odsek je u stanju zauzeća, a kada su relea aktivna odsek je u stanju slobode. Sve dok su relea u istom stanju izlaz je regularan. Kada se stanja relea razlikuju izlaz nije regularan. Neregularan izlaz može da se prepozna od strane kontrolne logike. Kako su ova dva relea nezavisne komponente i imaju nezavisno upravljanje, mala je verovatnoća da će oba relea otkazati na isti način. Na ovaj način jednostruka greška može da bude prepoznata i otklonjena.

Odlučivački elementi evaluatora iako nezavisno donose odluku o stanju odseka konstantno međusobno razmenjuju svoje odluke i proveravaju da li su iste, i tek nakon što se uvere da su odluke iste ovi elementi će preduzeti odgovarajuće akcije. Ukoliko odluke nisu iste odlučivački elementi će proglasiti grešku u odlučivanju za stanje tog odseka. Samo ukoliko su odluke iste odlučivački elementi rade ispravno.

Procesorska jedinica evaluatora upravlja izlaznom jedinicom i stanjima relea. Pored toga, ona konstantno vrši nadgledanje trenutnog stanja relea i proverava da li se to stanje poklapa sa komandom koju šalje izlaznoj jedinici. Ukoliko se stanje relea razlikuje od željenog, procesorska jedinica proglašavaju grešku za odgovarajući odsek.

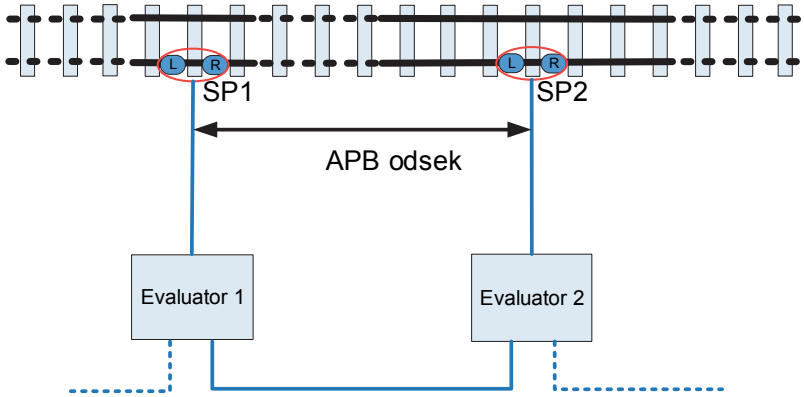
Evaluator je projektovan tako da u osnovnom stanju, ili kada je isključen, bude u bezbednom stanju, odnosno da su svi kontrolisani odseci u stanju zauzeća. Svi signali koji učestvuju u odlučivačkom lancu su dinamički, sa jasno definisanim parametrima i marginama. Bilo koje odstupanje parametara signala u lancu odlučivanja smatra se greškom, a odgovarajući odsek prelazi u bezbedno stanje.

4. Komunikacioni protokoli evaluatora brojača osovina

Evaluator brojača osovina koristi komunikacione protokole na interfejsu između dva evaluatora i između dva odlučivačka elementa unutar procesorske jedinice. Prvo će biti detaljnije opisan komunikacioni protokol između dva evaluatora, a zatim i komunikacioni protokol između dva odlučivačka elementa procesorske jedinice.

Komunikacija između dva evaluatora je neophodna u slučaju kada oni kontrolišu isti železnički odsek, a pri tom se nalaze na različitim lokacijama. Tipičan primer za to je automatski pružni blok (APB), kod koga je svaki od evaluatora povezan na jedan senzorski

par, dok se informacije o stanju drugog senzorskog para koji učestvuje u kontroli odseka dobijaju od drugog evaluatora. Ovaj slučaj je prikazan na slici 3.



Slika 3. Prikaz automatskog pružnog bloka

Udaljenost između evaluatora može iznositi nekoliko kilometara. U slučaju kada se kao prenosni medijum koriste bakarni provodnici, jedinica za komunikaciju sa evaluatorom sadrži industrijski modem, dok u slučaju korišćenja optičkog vlakna, ova jedinica poseduje RS232 primopredajnik uz spoljašnji konvertor signala.

S obzirom da se koristi UART kao fizički interfejs između procesorske jedinice i modema, odnosno RS232 primopredajnika, samo jedan odlučivački element šalje komande ili podatke, dok odgovor od modema ili RS232 primopredajniku dobijaju oba odlučivačka elementa.

Protokol komunikacije zadovoljava standard EN 50159 [4]. Ovaj standard predviđa tri kategorije prenosnih sistema: Kategorija 1 – zatvoren prenosni sistem u kome su svi bezbednosni aspekti sistema pod kontrolom projektanta; Kategorija 2 – otvoren prenosni sistem u kome se ne može smatrati da su svi bezbednosni aspekti sistema pod kontrolom projektanta, ali je mogućnost malicioznih napada zanemarljiva; Kategorija 3 - otvoren prenosni sistem u kome postoji mogućnost malicioznih napada i zahtevaju se kriptografske mere zaštite.

Komunikacioni sistem između evaluatora brojača osovina pripada kategoriji 1, s obzirom da oni komuniciraju preko posebne parice ili posebnog optičkog vlakna i da je komunikacija tipa tačka-tačka. Fizički pristup evaluatorima je dozvoljen samo ovlašćenim licima, dok su parica ili optičko vlakno ukopani u zemlju.

Standardom EN 50159 [4] su definisane moguće bezbednosne pretnje u komunikaciji: ponavljanje poruke, brisanje poruke, umetanje poruke, promena redosleda poruka, promena sadržaja poruke i kašnjenje poruke. Istim standardom predviđeni su i zaštitni mehanizmi kojima se mogu umanjiti bezbednosne pretnje. Izabrano je da posmatrani komunikacioni protokol sadrži sledeće zaštitne mehanizme: (1) korišćenje broja poruke, čime se štiti od ponavljanja, brisanja, umetanja i promene redosleda poruka; (2) ograničeno vreme čekanja na odgovor, čime se štiti od kašnjenja poruka; (3) zaštitno kodovanje - omogućava se odbacivanje neispravne (izmenjene) poruke.

Komunikacija između evaluatora je realizovana po principu *master-slave*, pri čemu *master* inicira uspostavljanje veze i inicira razmenu poruka. Ako u prenosu poruka

dođe do greške, evaluator koji je *slave* u komunikaciji ne odgovara porukom, već evaluator koji je *master* čeka da istekne vreme predviđeno za odgovor i nakon toga ponavlja prethodnu poruku. Format poruka je isti za obe strane u komunikaciji i predstavljen je na slici 4.

1B	1B	2B	2B	1B
Početni bajt	***Broj poruke***	***Podaci za odsek N_1***	***Podaci za odsek N_2***	***CRC***

Slika 4. Format poruka u protokolu komunikacije između dva evaluatora

Početni bajt poruke ima fiksnu vrednost (A5h). Ako se na početku prijema poruke dobije bajt različit od A5h, prijemnik odbacuje taj bajt. Vrednost polja *Broj poruke* se svaki put inkrementira (po modulu 256) u slučaju da nema potrebe za ponavljanjem poruke. Na prijemu se očekuje samo jedna validna vrednost za polje *Broj poruke*. Evaluatori mogu da razmene informacije o dva odseka (polja *Podaci za odsek* N_1 i *Podaci za odsek* N_2). Ovo je urađeno zbog uštede u slučaju dvokolosečne pruge. Poruka se završava zaštitnim kodom (polje *CRC*). Kao zaštitni kôd se koristi 8-bitni CRC.

Evaluatori brojača osovina treba da razmene sledeće korisne informacije (polja *Podaci za odsek* N_1 i *Podaci za odsek* N_2): stanje odseka, stanje senzorkog para, broj osovina detektovanih nakon prethodne poruke, zahtev za razrešenje odseka i izvor zahteva za razrešenje odseka (lokalni ili daljinski).

Sve informacije koje razmenjuju evaluatori direktno utiču na bezbednost, pa kao krajnja posledica promene sadržaja poruke može doći do oslobađanja odseka, čak i u slučaju da je on stvarno zauzet. Uvođenjem protokola komunikacije sa zaštitnim mehanizmima značajno je smanjena verovatnoća ovakvog događaja. Bilo je potrebno izračunati ovu verovatnoću da bi se pokazalo da je ona manja od propisane vrednosti za SIL4 sistem.

Postoje tri načina da dođe do hazardnog događaja usled greške u komunikaciji dva evaluatora brojača osovina: (1) usled otkaza hardvera koji učestvuje u primopredaji, izuzimajući modul za proveru transmisionog koda (verovatnoća R_{H1}); (2) usled grešaka pri prenosu informacija (verovatnoća R_{H2}); (3) usled otkaza modula za proveru transmisionog koda (verovatnoća R_{H3}).

Verovatnoća hazardnog događaja u komunikaciji dva evaluatora je jednaka zbiru prethodne tri verovatnoće. Da bi se ispunio SIL4 treba pokazati sledeće:

$$R_{H1} + R_{H2} + R_{H3} \leq THR(SIL4) \tag{1}$$

gde je *THR*(*SIL4*) prihvatljiv intenzitet opasnosti za SIL4.

S obzirom da je modul za proveru transmisionog koda realizovan pomoću mikrokontrolera koji ispunjava SIL3 i da izvršava softver koji ispunjava SIL4, član R_{H3} se može zanemariti. Vrednost R_{H1} se izračunava na sledeći način [4]:

$$R_{H1} = R_{HW} \cdot p_{US} \cdot k_1 \tag{2}$$

gde je R_{HW} verovatnoća otkaza hardvera koji učestvuje u primopredaji poruka (izračunato u okviru RAMS analize), p_{US} je verovatnoća da se ne detektuje izmenjena poruka pomoću zaštitnog koda ($p_{US} = k \cdot 2^{-c}$, gde je c broj bita zaštitnog koda), a k_1 faktor hardverskih otkaza uključujući bezbednosnu marginu (uzeto je da je $k_1 = 5$ na osnovu preporuke iz standarda [4]). Prilikom izračunavanja verovatnoće p_{US} treba uzeti u obzir da pojedina polja imaju ograničen skup dozvoljenih vrednosti (npr. polje *Početni bajt* ima samo jednu validnu vrednost od mogućih 256).

Vrednost R_{H2} se izračunava na sledeći način [4]:

$$R_{H2} = p_{UT} \cdot p_{US} \cdot f_W \tag{3}$$

gde je p_{UT} verovatnoća da se ne detektuje izmenjena poruka pomoću transmisionog koda (slično zaštitnom kodu), a f_W verovatnoća izmenjenih poruka.

Proračun verovatnoća je pokazao da je $R_{H1} << R_{H2}$, a da je $R_{H2} = 5{,}89 \cdot 10^{-10}$, što znači da protokol komunikacije između dva evaluatora zadovoljava SIL4.

Protokol komunikacije između odlučivačkih elemenata procesorske jedinice evaluatora je takođe realizovan po principu *master-slave*. Odlučivački elementi su mikrokontroleri koji ispunjavaju SIL3. Mikrokontroleri se nalaze na istoj štampanoj ploči i komuniciraju preko CAN interfejsa, pri čemu su oni jedini povezani na CAN magistralu, odnosno veza je tipa tačka-tačka. CAN protokol koristi 16-bitni CRC kao transmisioni kôd. Format poruka je isti za obe strane u komunikaciji i predstavljen je na slici 5.

1B	**1B**	**1B**	**promenljivo**	**1B**
Broj poruke	***Kôd komande (odgovora)***	***Dužina polja korisnih podataka***	***Korisni podaci***	***CRC***

Slika 5. Format poruka u protokolu komunikacije između dva odlučivačka elementa procesorske jedinice

U fazi inicijalizacije uređaja, odlučivački elementi razmenjuju konfiguraciju uređaja, pa samo u slučaju da su one potpuno identične započinju se normalne operacije. Nadalje se razmenjuju informacije o stanju odseka, s obzirom da odlučivački elementi stalno porede procenjena stanja odseka, pa se u slučaju različite procene stanja proglašava greška na odgovarajućem odseku.

Verovatnoća hazardnog događaja u komunikaciji dva odlučivačka elementa procesorske jedinice se izračunava na isti način kao i kod komunikacije dva evaluatora. I ovde su članovi R_{H1} i R_{H3} zanemarljivi, dok je $R_{H2}=5{,}13 \cdot 10^{-12}$, što znači i da komunikacija između odlučivačkih elemenata procesorske jedinice zadovoljava SIL4.

5. Zaključak

U daljem razvoju brojača osovina najverovatnije će doći do promene tipa izlaza prema kontrolnoj logici. Umesto relejnih izlaza, koristio bi se *Ethernet* interfejs, uz odgovarajući protokol komunikacije sa elektronskom stanicom za koji bi trebalo ponoviti istu proceduru koja je opisana u ovom radu.

Literatura

[1] *Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling*, Standard EN 50129, 2010.

[2] *Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Basic requirements and generic process*, Standard EN 50126-1, 2010.

[3] *Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems*, Standard EN 50128, 2011.

[4] *Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems*, Standard EN 50159, 2010.
[5] *Railway applications – Technical parameters of train detection systems for the interoperability of the trans-European railway system – Part 2: Axle counters,* Standard EN 50617-2, 2015.
[6] *Axle Counting System ACS2000*, *Frauscher,* 2012. Dostupno na: https://www.frauscher.com/assets/media/Datenblaetter/EN/Frauscher_ACS2000_Data_Sheet.pdf
[7] *Frauscher Advanced Counter FadC, Frauscher,* 2012. Dostupno na: https://www.frauscher.com/assets/media/Datenblaetter/EN/Frauscher_FAdC_Data_Sheet.pdf
[8] *Clearguard Az S 350 U Microcomputer Axle Counting System*, *Siemens*, 2010. Dostupno na: https://www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/rail-solutions/rail-automation/track-vacancy-detection/db-az-s-350-u-en.pdf
[9] *Axle Counter Az LM, Thales,* 2007. Dostupno na: https://myproducts-thales.com/brochures-documents/1-brochure-fieldtrac-6315-az-lm/file
[10] *Axle Counter BO23, Altpro,* 2010. Dostupno na: https://altpro.hr/upload_data/site_files/bo23-datasheet-en.pdf
[11] *M. Nikolić, M. Milanović, Ž. Stojković, N. Antonić, B. Kosić, "Predlog arhitekture brojača osovina u železnici", Zbornik radova TELFOR 2013, str. 608-611, Beograd, 2013.*
[12] *M. Nikolić, B. Kosić, M. Milanović, N. Antonić, Ž. Stojković, I. Kokić, "Railway Axle Counter Prototype", 2014 22nd Telecommunications Forum (TELFOR), Proceeding of Papers, pp. 694-697, Belgrade, 2014.*
[13] *I. Kokić, M. Nikolić, B. Kosić, M. Milanović, N. Antonić, Ž. Stojković, "Railway Axle Counter Remote Supervision System", 2014 22nd Telecommunications Forum (TELFOR), Proceeding of Papers, pp. 698-701, Belgrade, 2014.*

Abstract: *This paper presents evaluator unit of axle counter which is used to control occupancy of railway sections. Evaluator unit fulfills SIL4, defined by EN 50129 standard. Functions, interfaces and subsystems of evaluator unit are described. Communication protocols of evaluator unit are presented in more detail. They fulfill EN 50159 standard. Possible threats that can afftect safety communication are defined, as well as appropriate countermeasures, which can decrease risk level. At the end, probability of hazardous event due to communication errors is calculated. This probabilty is less than tolerable hazard rate for SIL4.*

Keywords: *axle counter, hazard, safety, SIL.*

COMMUNICATION PROTOCOLS IN SIL4 SYSTEMS

Ivan Kokić, Marko Nikolić, Jovana Novaković, Željko Stojković