ANALIZA KVAROVA - PARAMETRI POUZDANOSTI I SIGURNOSTI ŽELJEZNIČKIH SIGNALNO-SIGURNOSNIH UREĐAJA

Statistički podaci o radu opreme prometno-upravljačkog i signalno-sigurnosnog podsustava pokazuju da su opasni kvarovi suvremenih elektroničkih signalno-sigurnosnih uređaja rijetki događaji. Razlog tome je striktno pridržavanje sigurnosnih zahtjeva RAMS-a tijekom svih faza projektiranja, proizvodnje, ugradnje i održavanja uređaja. Osnova upravljanja RAMS-om je smanjivanje pojave kvarova i njihovih posljedica tijekom životnog ciklusa, a time i smanjivanje rizika na najmanju moguću mjeru.

Želimir Delač
dipl.ing.el.

Agencija za sigurnost željezničkog prometa
Zelimir.delac@asz.hr

UDK: 625.1+681.5

1. Uvod

Sigurnost željezničkih signalno-sigurnosnih uređaja (u nastavku: SS uređaji) postiže se učinkovitim sustavom RAMS-a (pouzdanost-raspoloživost-sposobnost održavanja-sigurnost) i to temeljem upravljačkog-organizacijskog sustava kojim će se tijekom životnog ciklusa tehničkog sustava (SS uređaja) otkloniti mogućnost pojave kvarova i njihove posljedice svesti na dozvoljenu razinu koja ne ugrožava sigurnost.

Sustav RAMS-a razrađen je u normama HRN EN 50126 ([2] i [3]) u kojima se opisuju specifikacije i daje cjeloviti prikaz pouzdanosti, raspoloživosti, mogućnosti održavanja i sigurnosti željezničkom sustavu – Generički postupak RAMS-a u Europskoj uniji te sustavni pristup sigurnosti. Cilj normi je uvođenje postupka upravljanja RAMS-om u željezničkom sustavu kojeg će dosljedno primjenjivati subjekti odgovorni za sigurnost – željeznički prijevoznici, upravitelji infrastrukture i njihovi dobavljači - industrija.

Dobro poznavanje kvarova – analiza njihovih uzroka, postupanje s kvarovima, stanja sigurnosti i praćenje (izračuni) parametara sigurnost – ima ključnu ulogu u projektiranju SS uređaja za koje se može dokazati vjerojatnost pojave kvara unutar dozvoljenih granica propisanih sigurnosnim ciljevima.

2. Strategije postupanja s kvarovima

U smislu upravljanja RAMS-om, mogu se primijeniti sljedeće strategije postupanja s kvarovima SS uređaja (koje se u praksi uglavnom primjenjuju u kombinaciji) [10]:

- otklanjanje mogućnosti nastanka kvarova,
- otklanjanje posljedica kvarova,
- ograničenje posljedica kvarova.

Otklanjanje mogućnosti nastanka kvarova - Svaka komponenta sustava koja je povezana sa sigurnošću mora imati strogo definirane tehničke karakteristike s kojima je osigurana tražena sigurnost. Otklanjanje mogućnosti nastanka kvara temeljem primjene takvih karakteristika može se provoditi jedino ako su one neodvojivi i sastavni dio komponenti sustava kroz čitav životni ciklus uređaja.

Komponente koje se koriste u željezničkom sustavu moraju imati visoku mehaničku i/ili električnu robusnost. To znači da vanjski utjecaji kao što su vibracije, temperatura, vlaga, povratne struje sustava za napajanje i sl., ne smiju imati utjecaj na projektirane funkcije uređaja. Ta se robusnost može postići s odgovarajućim materijalima (kao npr. izdržljivi kontaktni materijali, visoka temperaturna svojstva poluvodičkih elemenata i sl.), posebnom strukturom (npr. mehanička stabilnost, otpornost na elektromagnetske smetnje) i posebnim proizvodnim metodama (npr. korištenje kontrolnih lista i specijalnih automatiziranih procesa tijekom procesa proizvodnje i sl.).

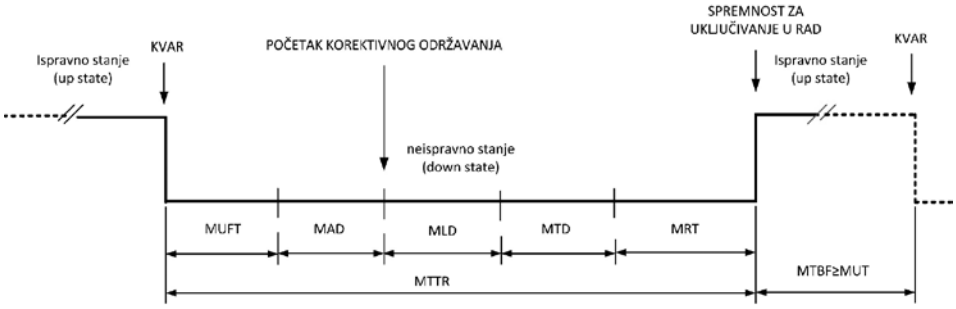
Otklanjanje posljedica kvarova - Ukoliko se ne može dokazati otklanjanje mogućnosti nastanka kvarova (kako je prethodno opisano; što je čest slučaj u praksi), tada se mora dokazati da su otklonjene posljedice kvara, što znači da sustav u slučaju kvara mora biti u sigurnom stanju (engl.: *safe state*). Ovaj dokaz temelji se na ispunjenju sljedećih sigurnosnih zahtjeva:

- kvar nije opasan,
- spriječeno je širenje kvarova,
- kvar je neovisan i nema utjecaja na svoje okruženje.

Bezopasni pojedinačni kvarovi **-** U sustavima povezanim sa sigurnošću, pojedinačni kvar nikada ne smije dovesti do opasnog stanja, već do dozvoljenog - sigurnog stanja. Ispunjenje ovog zahtjeva mora se dokazati u sigurnosnom predmetu (dokumentaciji). Ako se to ne može ostvariti, mora se promijeniti arhitektura sustava. U praksi to uglavnom znači primjena redundantnih sklopova (zalihost).

Bezopasni višestruki kvarovi **-** Osim bezopasnih pojedinačnih kvarova, sigurnosni sustavi zahtijevaju slična svojstva i kod višestrukih kvarova. Ako bi istodobni kvarovi dviju ili više komponenti (koje su u interferenciji) mogli dovesti do opasnog stanja, te komponente u tom slučaju moraju biti neovisne jedna o drugoj što se postiže odgovarajućom tehničkom izvedbom sustava.

Sprječavanje širenja kvarova **-** Zahtjev za neširenjem (opasnih) kvarova u sigurnosnim sustavima ostvaruje se brzim otkrivanjem takvih kvarova i brzim popravcima. Vremena otkrivanja kvarova, popravaka i stavljanja sustava iz neispravnog (eng.: *down state*) u ispravno stanje (engl.: *up state*) imaju veliki utjecaj na razinu sigurnosti (slika 1). [2]



Slika 1. Vremena otkrivanja kvara, kašnjenja popravaka, popravaka; dovođenje iz neispravnog (***down state***) u ispravno stanje (***up state***), izvor: [2]

Važan parametar za sigurnosne sustave, pa tako i za SS uređaje je parametar MTTR – srednje vrijeme vraćanja u prvobitno stanje, koje se sastoji od vremena:

MTTR = MUFT + MAD+MLD+MTD+MRT
MTBF srednje (radno) vrijeme između kvarova (*engl. mean (operating) time between failures*)
MUT srednje vrijeme aktivnosti (*engl. mean up time*)
MUFT srednje vrijeme neotkrivenog kvara (*engl. mean undetected fault time*)
MAD srednje administrativno kašnjenje (*engl. mean administrative delay*)
MLD srednje logističko kašnjenje (*engl. mean logistics delay*)
MTD srednje tehničko kašnjenje (*engl. mean technical delay*)
MRT srednje vrijeme popravka (*engl. mean repair time*)
MTTR srednje vrijeme vraćanja u prvobitno stanje (za korektivno održavanje) (*engl. mean time to restore*)

Kašnjenja u postupku otklanjanja kvarova se ne mogu izbjeći. Međutim, ona moraju biti dovoljno niska u skladu sa sigurnosnim zahtjevima.

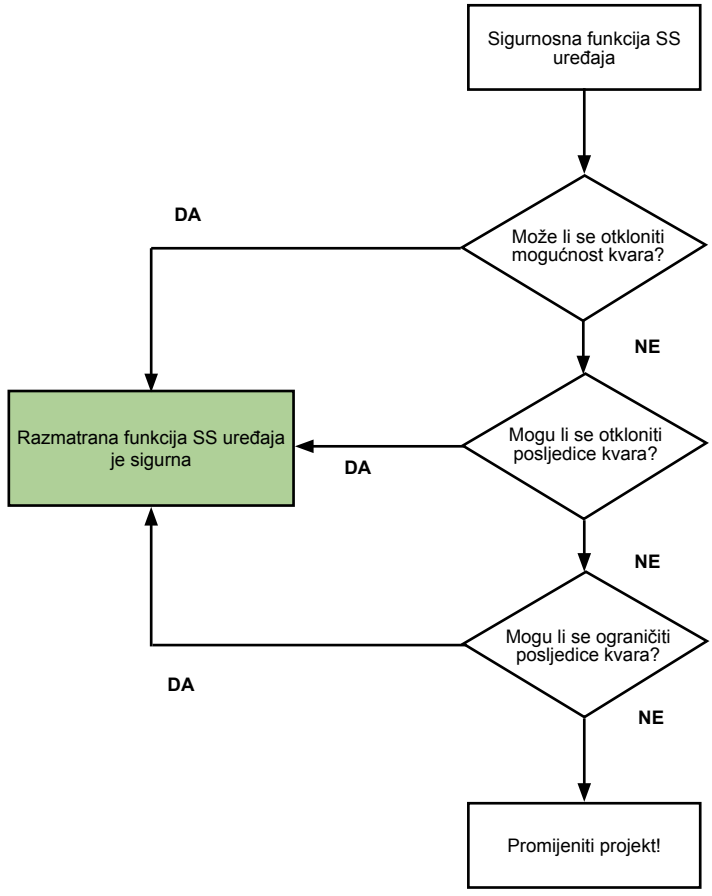
Kvar se mora otkriti prije izvršavanja sljedeće sigurnosne funkcije. Kod suvremenih elektroničkih SS uređaja, izvedenih mikroprocesorskom tehnikom, brzo otkrivanje kvarova postiže se provjerom sigurnosnih funkcija i analizom podataka koji se dobivaju iz samog uređaja u vrlo kratkim ciklusima nadzora (unutar mikroprocesorskog sklopa), obično daleko ispod jedne sekunde.

Gdje takvo otkrivanje kvara nije moguće, koristi se odgovarajuća inspekcija u redovitim vremenskim intervalima.

Neovisnost kvarova - Pored brzog otkrivanja i popravaka kvara, drugo rješenje da se pojedinačni kvar dalje ne širi je osiguranje neovisnosti komponenti u okruženju kvara. Takva neovisnost se često postiže redundancijom (zalihošću) kao prikladnom metodom za sprječavanje kvarova. Međutim, redundantne strukture zahtijevaju posebne metode i tehnike kako bi se stvarno osigurala njihova neovisnost. U suprotnom, kombinirani kvar u obliku sustavnog višestrukog kvara može dovesti do opasnog stanja sustava.

Dokazivanje neovisnosti kvara može ponekad biti teško provedivo u praksi jer jedan kvar može biti put uzroka nekoliko kvarova, iako je na prvi pogled ova neovisnost ispunjena. Na primjer, istovremeni kvar dvije redundantne upravljačke jedinice s različitim jedinicama napajanja smatra se gotovo nemogućim. Međutim, ako se ove jedinice napajaju preko istog izvora i ovaj izvor ostane bez napajanja, javlja se slučaj u kojem neovisnost kvara nije osigurana. Zbog takvih slučajeva, potrebno je točno definirati granice redundantnih sklopova kako bi se postigla neovisnost funkcija (i u ovom slučaju i napajanja moraju biti zasebno izvedena – za svaki kanal posebno).

Ograničenje posljedice kvara - Ako u sigurnosnom predmetu nije moguće dokazati da se može otkloniti mogućnost nastanka kvara niti se njegove posljedice mogu izuzeti, vjerojatnost opasnih posljedica na sigurnost u tom slučaju mora biti dovoljno niska tj. ograničena. Točna vrijednost prihvatljive razine mora biti definirana u specifikacijama sigurnosnih zahtjeva.



Slika 2. Strategija postupanja s kvarovima, izvor: [autor]

Da bi se ograničila šteta kao posljedica kvara, jedan od pristupa je da se kvar brzo otkrije, a drugi je da se ograniče štetne posljedice. Primjer tome u željezničkoj signalizaciji često puta zna biti ograničenje brzine.
Najvažniji cilj u sigurnosti željezničkih SS uređaja je strategija potpunog otklanjanja kvarova. Međutim, tehnička i ekonomska ograničenja, složene sigurnosne mjere i tehnička rješenja temelje se na raznim drugim strategijama - u većini slučajeva to je otklanjanje posljedica kvarova ili, kao minimum, ograničavanje posljedica kvarova.

3. Stanja sigurnosti uređaja povezanih sa sigurnošću

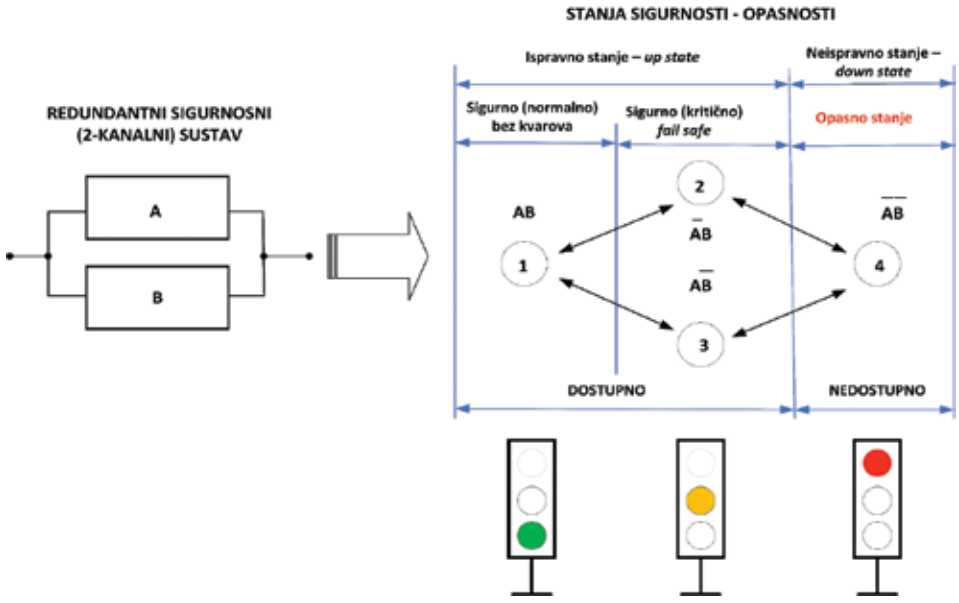
Sigurno stanje uređaja povezanog sa sigurnošću (S) se definira kao stanje u kojem tehnički sustav nema neprihvatljivog rizika. Stanja sigurnosti ilustrirana su na slici 3 na primjeru jednostavnog redundantnog dva-kanalnog sustava.

Sigurno (normalno) stanje (S_F) – ispravno stanje (*up state*) **–** osnovni zahtjev za sigurnost željezničkih SS uređaja je **stanje bez kvarova** (oznaka „1", slika 3).

Sigurno (kritično) stanje (S_C) – ispravno stanje - uređaj može prijeći u sigurno stanje i uz pojavu kvara (npr. kod kvara na jednom od kanala redundantnog sustava, uz uvjet da u isto vrijeme ostali kanali ispravno rade) – to je tzv. sigurno (kritično) stanje (*engl. critical up state*) **u kojem je sustav i dalje raspoloživ za uporabu** jer je uređaj u sigurnoj funkciji koju preuzima redundantni kanal (oznake: „2" i „3" na slici 3).

Pojava kvara u tom slučaju ne smije odvesti sustav iz sigurnog stanja. Ova značajka sustava povezanih sa sigurnošću naziva se još i princip **– stanje sigurnosti kod kvara (ili stanje zaštićenog kvara) - *engl. fail-safe***. Ovo se stanje mora održavati sve dok se ne uklone svi kvarovi. Napuštanje sigurnog stanja tijekom otklanjanja kvara smije biti moguće samo uz sudjelovanje posebno obučenog osoblja za održavanje.

Opasno stanje (S_H) – U praksi se opasno stanje samo rijetko može potpuno isključiti - u sigurnosnim sustavima **primjena *fail-safe* principa je ta koja osigurava da vjerojatnost opasnih stanja bude svedena na minimumu**. Ako sustav ipak



Slika 3. Stanja sigurnosti (opasnosti) za redundantni sustav s dva kanala, izvor: [4]

prijeđe u opasno stanje u kojem imamo pojavu opasnog kvara, mora se što prije prebaciti u sigurno stanje zbog opasnosti od nesreće. Stanje sustava u kojem postoji opasan kvar naziva se: **neispravno stanje (*down state*)** ili opasno stanje nezaštićenog kvara (S_H).

4. Parametri pouzdanosti i sigurnosti

Parametre pouzdanosti i sigurnosti možemo izraziti sa sljedećim formulama (stohastička-eksponencijalna raspodjela), koje su prikazane u tablici 1. [4]

Tablica 1. Parametri pouzdanosti i sigurnosti i izrazi za izračun

Parametar	Opis	Formula
R(t)	Pouzdanost (engl.: *reliability*) – vjerojatnost rada bez kvara	$(e^{-\lambda t})$ ili $\exp(^{-\lambda t})$
λ	Učestalost kvara (engl.: *failure rate*) - konstanta	$\frac{1}{MTFF}$
$\lambda(t)$	Trenutačna učestalost kvara (engl.: *instantaneous failure rate*)	$\frac{1}{1 - F(t)} \frac{dF(t)}{dt}$
λ_D	Učestalost opasnog kvara (engl.: *dangerous failure rate*) - konstanta	$\frac{1}{T_D}$
MTTF	Srednje vrijeme do pojave zaštićenog kvara (*fail-safe*) (engl.: *mean time to failure*)	$\frac{1}{\lambda}$
F(t)	Vjerojatnost kvara (engl.: *probability function of the (operating) time to failure – failure probability*)	1-R(t)
$F_D(t)$	Vjerojatnost opasnog kvara (engl.: *dangerous failure probability*)	$F_D(t) = 1 - \exp(-\lambda_D t)$
$S_D(t)$	Vjerojatnost sigurnosti (engl.: *probability function of the (operating) time to failure (dangerous)*)	$1- F_D(t) = \exp(-\lambda_D t)$
T_D	Srednje vrijeme rada do opasnog kvara	$\frac{1}{\lambda_D}$

5. Određivanje prihvatljive razine opasnih kvarova SS uređaja

Statistički podaci o radu suvremene elektroničke opreme za PU-SS podsustav pokazuju da su opasni kvarovi elektroničkih SS uređaja rijetki događaji. Uzrok tome je striktno pridržavanje sigurnosnih zahtjeva u fazama razvoja, proizvodnje i rada sustava (uz pridržavanje RAMS zahtjeva) i primjena visokih sigurnosnih normi s niskom razinom pojave opasnih kvarova (SIL 4).

Da bi osigurali visoke sigurnosne normative, proizvođači SS opreme moraju riješiti dva temeljna zadatka. Prvo trebaju ostvariti potrebne sigurnosne zahtjeve – potrebnu funkciju uređaja i sigurnosne parametre (na osnovi provedene analize rizika prema zahtjevima RAMS-a). A, drugo, nakon proizvodnje, prije ugradnje i puštanja u rad, potrebno je kompletirati sigurnosni predmet (engl.: *safety case*) i potvrditi – dokazati postignutu razinu sigurnosti - prihvatljivu razinu pojave opasnih kvarova.

Prema [2], kvarovi sustava kategoriziraju se kao slučajni ili sustavni kvarovi. Slučajni kvarovi nastaju uslijed uzroka koje je moguće opisati statističkim raspodjelama (kako je opisano u ovom članku). Za razliku od slučajnih kvarova, sustavni kvarovi su kvarovi nastali uslijed pogrešaka u aktivnostima životnog ciklusa sustava – uređaja zbog kojih nastaje deterministički kvar u određenim kombinacijama ili pod određenim uvjetima (kao što je neispunjavanje uvjeta okruženja ili primjene). Sustavne kvarove obično izazivaju ljudske pogreške u raznim fazama životnog ciklusa sustava. Stoga se sustavni kvarovi uglavnom rješavaju primjenom odgovarajućih postupaka, metoda i organizacije.

Glavno obilježje razlike između slučajnih kvarova i sustavnih kvarova jest da slučajni kvarovi općenito nastaju uslijed događaja koje je moguće statistički pratiti pa se može procijeniti vjerojatnost njihove pojave. Sustavni kvarovi nastaju uslijed događaja za koje statistički podaci obično nisu raspoloživi pa vjerojatnost njihove pojave općenito nije moguće procijeniti.

Dakle, priroda pojave opasnih kvarova SS uređaja (kada uz pojavu kvara, sustav nije u sigurnom stanju) ne isključuje utjecaj ljudi i okoliša, tj. djelovanje sustava. Apsolutnu sigurnost na temelju upravljanja rizicima proizašlih samo iz statistički predvidivih (izračunatih) tehničkih kvarova nije moguće ostvariti. Razinu sigurnosti tehničkih sustava treba jasno razdvojiti od sustavnih kvarova i hazarda uzrokovanih ljudskom nepažnjom - nesmotrenim ili neplaniranim (štetnim) sustavnim djelovanjem u raznim fazama životnog ciklusa uređaja, o čemu treba provesti posebne analize rizika i što nije primarni predmet razmatranja ovog članka.

Nepredvidivost opasnih kvarova (kvarova uređaja) traži da se u sklopu upravljanja rizicima koriste razni koncepti za utvrđivanje prihvatljive razine hazarda. Prema [10], koriste se sljedeći koncepti:

- razumno dopuštena razina hazarda,
- zamjena rizika, i
- metoda normalizacije.

Prvi koncept - "razumno dopuštena razina hazarda", uzima u obzir da je za postizanje takve razine hazarda, odnosno pripadajućeg rizika, često potrebno razviti složena tehnička rješenja i uložiti znatne troškove za realizaciju sigurnosnih uređaja takvog tipa.

Vjerojatnost pojave nesreće od 10^{-6} (gubitak života jedne osobe u populaciji od 1.000.000 godišnje) je iskustveno prihvatljiva razina hazarda. Takva vrijednost odgovara vjerojatnosti smrti neke osobe u njenom domu kao posljedica nesretnog događaja. [10]

Spomenuti kriterij možemo koristiti kao prihvatljiv kriterij za pojavu opasnog kvara ($\lambda_{D)}$. Uzimajući da je vjerojatnost opasnog kvara: $F_D(t) = 10^{-6}$, t = 1godina = 8760 sati, dobivamo da je prihvatljiva učestalost opasnog kvara:

$$F_D(t) = \lambda_D t \rightarrow \lambda_{D=} 1{,}1 \times 10^{-10}\ (h^{-1}) \qquad [1]$$

Vrijednost (1) može se prihvatiti kao „razumna" osnova za određivanje kriterija za učestalost opasnih događaja i s njom se uspoređuju sigurnosni parametri različitih primjena.

Druga najčešća koncepcija koja se koristi za određivanje sigurnosnih kriterija je „zamjena rizika". Pri tome, sigurnosni parametri novog sustava ili opreme ne bi trebali biti ništa lošiji od istih parametara zamijenjenog sustava ili opreme.

Kako su opasni kvarovi rijetki događaji, često nedostaju statistički podaci o sigurnosti rada sustava. U takvim slučajevima za ocjenu opasnih kvarova/zaštićenih kvarova može se koristiti izračun s koeficijentom asimetrije kvarova (Ka). Koeficijent Ka pokazuje omjer između stope opasnih i zaštićenih kvarova (engl: *fail safe*).

$$K_a = \frac{\lambda D}{\lambda} \qquad [2]$$

Normativna vrijednost koeficijenta K_a može se iskustveno procijeniti [10]:

$$K_a \cong 10^{-4} \qquad [3]$$

Sukladno (3), SS uređaj trebao bi imati stopu opasnih kvarova oko 10.000 puta nižu od stope zaštićenih kvarova (eng. *fail safe*).

Vrijednost Ka se koristiti kao normativna vrijednost za određivanje kriterija prihvatljivosti opasnih kvarova λ_D za složeni elektronički SS uređaj. Ako su npr. poznati statistički podaci za $\lambda < 10^{-5}\ h^{-1}$. Tada je procjena vrijednosti opasnih kvarova:

$$\lambda_D = K_a \cdot \lambda = 10^{-4} \cdot 10^{-5} = 1 \cdot 10^{-9}\ h^{-1} \qquad [4]$$

Vrijednost dobivena u izrazu (4) zapravo je vrijednost opasnog kvara kod uređaja koji odgovaraju sigurnosnoj integraciji SIL-4 (prema Tablici 3: $10^{-9} \leq TFFR < 10^{-8}$). Na temelju toga, možemo zaključiti da se kod sustava sa $\lambda < 10^{-5}\ h^{-1}$, očekuje da *će* se kvar (*fail safe*) pojaviti jednom u periodu od oko 11 godina.

Treća je „metoda normalizacije", koja se koristi ako novo ugrađeni uređaj ili sustav nema ispitanog prototipa. U tom slučaju, uzima se da je kriterij opasnih kvarova λ_D za takve uređaje definiran iz uvjeta da se može dogoditi samo jedan opasni kvar za cijeli skup uređaja jednog tipa tijekom cijelog (normiranog) razdoblja rada uređaja.[10]

Ako se, primjerice, uzme da se u skupu od N = 100.000 uređaja ne može dogoditi više od jednog opasnog kvara tijekom životnog vijeka (T_{op}) od 10 godina rada, tada je opasan kvar (prema [10]):

$$\lambda_D = \frac{1}{N \cdot Top} = 1{,}14 \cdot 10^{-9}\ h^{-1}, \qquad [5]$$

6. Izračun sigurnosnih parametara za dva-kanalni elektronički SS uređaj

Proizvođači SS uređaja i njihovi sigurnosni timovi (prema 5.3.4 HRN EN 50129:2018; *Safety organization*) moraju u sigurnosnom predmetu (engl.: *safety case*) prikazati i obrazložiti sigurnosne parametre (što se provjerava kroz ISA izvještaj (eng. *independent safety assessment*)). Svrha je dokazati da postignuta razina sigurnosti zadovoljava zadane kriterije. Izračun sigurnosnih parametara ovisi o odabranoj strukturi uređaja povezanog sa sigurnošću.

Danas su u elektroničkim SS uređajima povezanih sa sigurnošću široko prihvaćene dvije varijante redundantnih struktura uređaja povezanih sa sigurnošću: *dvokanalnih* i *trokanalnih* sustava (uglavnom danas primijenjen). Razmotrimo proračun sigurnosnih parametara na primjeru dva-kanalne strukture. Slika 4 prikazuje *dvokanalni sustav* s usporedbom stanja sigurnosti. U ovom pojednostavljenom modelu sigurnosnog sustava – SS uređaja, ugrađena su dva identična mikroračunala, paralelno povezana, koji rade istovremeno. Sigurnosni sklop za uspoređivanje - *komparator* uspoređuje izlazne signale mikroračunala i formira kontrolni signal. *Komparator* se smatra apsolutno pouzdanim.

Ako je poznata učestalost zaštićenih kvarova (λ) jednog od dva ista kanala mikroračunala, parametri pouzdanosti i kvarova: $R_1(t)$, $R_2(t)$, $F_1(t)$ i $F_2(t)$ za sustav ${}_1O^1$ i ${}_2O^2$, mogu se izračunati pomoću sljedećih formula (prema [4] i [10]):

$$R_1(t) = \exp(-\lambda t), \qquad R_2(t) = R_1^2(t) = \exp(-2\lambda t), \tag{6}$$

$$F_1(t) = 1- R_1(t) =1- \exp(-\lambda t), \qquad F_2(t) = 1- R_2(t) =1- \exp(-2\lambda t), \tag{7}$$

$$\lambda_1(t)= \lambda, \qquad \lambda_2(t)= 2\lambda, \tag{8}$$

$$MTTF_1=\frac{1}{\lambda}, \qquad MTTF_2=\frac{1}{2\lambda}, \tag{9}$$

Sigurnosni parametri ${}_2O^2$ sustava (opasni kvarovi) mogu se izračunati kao (prema [10]):

$$F_{D2}(t) = F^2_1(t) = (1-\exp(-\lambda t))^2, \tag{10}$$

$$S_{D2}(t) = 1- F_{D2}(t) =1- (1-\exp(-\lambda t))^2 = 2\exp(-\lambda t) - \exp(-2\lambda t), \tag{11}$$

Neka je, na primjer, $\lambda = 10^{-5}\ h^{-1}$ i t = 1000 sati. Tada je:

$$R_1(t) = \exp(-0{,}01) = 0{,}99005, \tag{12}$$

$$F_1(t) = 0{,}00995;\ S_1(t) = 1- F_1(t) = 0{,}99005, \tag{13}$$

$$MTTF_1 = 10^5 \text{ sati} = 11{,}4 \text{ godina}, \tag{14}$$

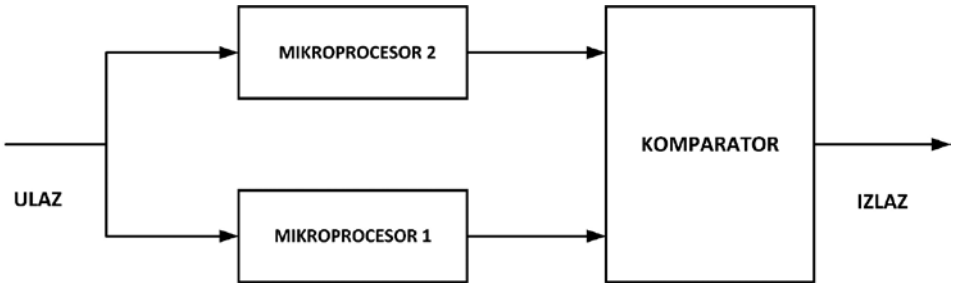
$$R_2(t) = \exp(-0{,}02)= 0.9802; \tag{15}$$

$$F_2(t) = 0{,}0198;\ S_2(t) = 1- F_2(t) = 0{,}9802\ ; \tag{16}$$

$$MTTF_2 = 5\cdot10^4 \text{ sati} = 5{,}7 \text{ godina}, \tag{17}$$

$$F_{D2}(t) = (1-\exp(-0{,}01))^2 = 0{,}000099, \tag{18}$$

$$S_{D2}(t) = 1- F_{D2}(t) = 0{,}999901, \tag{19}.$$



Slika 4. Dva-kanalni sustav i sigurnosni sklop za uspoređivanje, izvor: autor

Tablica 2. Stanja dva-kanalnog ${}_2O^2$ (redundantnog) sustava

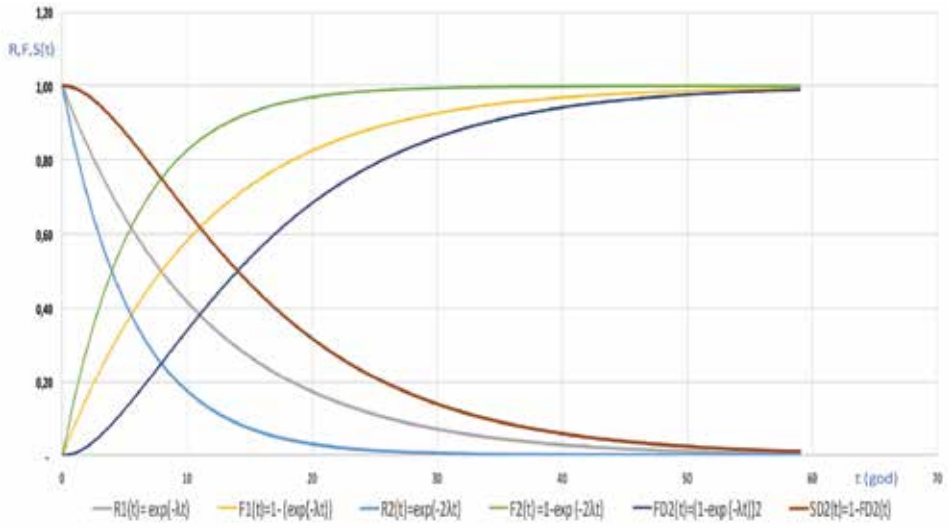
n	Stanje na ulazu		Stanje sustava na izlazu
	Mikroprocesor-Kanal1	Mikroprocesor-Kanal 2	
1	U funkciji	U funkciji	Sigurno-bez kvara (*up state*)
2	U funkciji	U kvaru	Sigurno-kritično (*fail safe; up state*)
3	U kvaru	U funkciji	Sigurno-kritično (*fail safe; up state*)
4	U kvaru	U kvaru	Opasno (*down state*)

Usporedba sustava ${}_1O^1$ i ${}_2O^2$ pokazuje da je:

- vjerojatnost pojave kvara $F_2(t)$ za ${}_2O^2$ sustav porasla za oko 1,99 puta;
- srednje vrijeme do zaštićenog kvara MTTF smanjeno je za faktor 2;
- vjerojatnost opasnog kvara $F_{D2}(t)$ za ${}_2O^2$ smanjena je (u odnosu na ${}_1O^1$) oko100 puta.

Daljnjim razmatranjem odnosa izraza za pouzdanost (6), možemo zaključiti da za bilo koji trenutak vremena vrijednost pouzdanosti *dvokanalnog* uređaja $R_2(t)$ (vjerojatnost da će dva-kanalni uređaj raditi bez kvara) je niža od pouzdanosti *jednokanalnog* uređaja $R_1(t)$ za $e^{\lambda t}$ puta. Pored toga, možemo zapaziti i da je vjerojatnost sigurnosti $S_{D2}(t)$ (vjerojatnost da će uređaj raditi bez opasnog kvara) veća od vjerojatnosti pouzdanosti (sigurnosti) $R_1(t)$ za 2-exp($-\lambda t$) puta.

Kako je $\lim_{t\to\infty} \frac{S_{D2}}{R_1} = \lim_{t\to\infty} (2\text{-exp}(-\lambda t)) = 2$, proizlazi da je sigurnosti *dvokanalnog* sustava (za $t\to\infty$) 2 puta veća od sigurnosti *jednokanalnog* sustava – što, definitivno, ukazuje na povećanu sigurnost (zaštitu od opasnih kvarova) *višekanalnog* sustava u odnosu na *jednokanalni* u svim fazama životnog ciklusa.



Slika 5. Karakteristike pouzdanosti i sigurnosti $_2O^2$ sustava (za SS sustav s dva kanala), izvor: autor

Ipak, temeljem prethodnih izraza, može se zaključiti da u *dvokanalnom* (*višekanalnom*) sustavu povećanje sigurnosti od opasnih kvarova ujedno prati i smanjenje pouzdanosti (nešto veća pojava zaštićenih kvarova). U tome se očituje i određen nedostatak koncepta *dvokanalnih* (*višekanalnih*) sustava – „sigurnost (od opasnih kvarova) je ostvarena po cijenu pouzdanosti".

7. Razine sigurnosnih integracija (SIL)

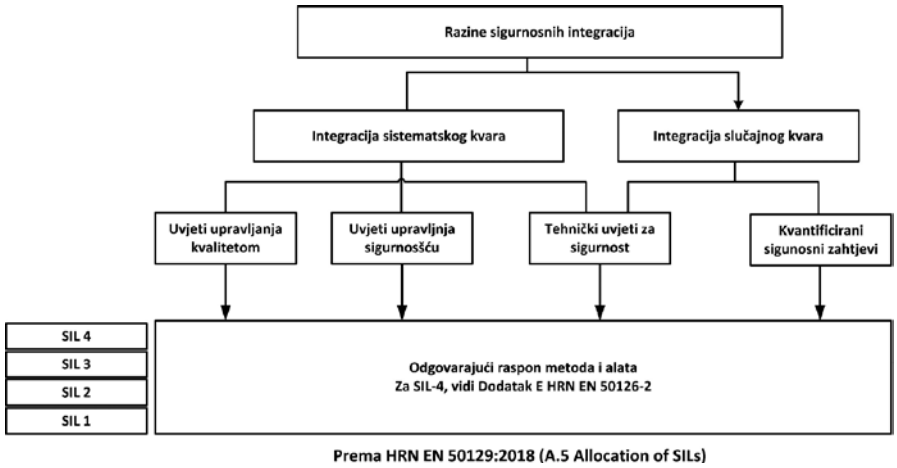
Stupanj sigurnosne integracije za sigurnosnu funkciju izražava se sa četiri diskretne razine sigurnosne integracije SIL (engl. *safety integrity level*; SIL 1 do SIL 4), gdje je SIL 4 ima najvišu razinu sigurnosne integracije, a SIL 1 najmanju. U normi HRN EN 50129 [5], termin SIL 0 je uveden kako bi se uputilo na funkciju koje nije povezana sa sigurnošću. Ovaj termin se više ne koristi i zato smo ga ispustili u daljnjim razmatranjima.

SIL je sigurnosni parametar koji se mora postići uz ostvarenje kvalitativnih faktora – sustava upravljanja kvalitetom, sigurnošću i tehničkih uvjeta za sigurnost (vidi sliku 6). [5]

Sigurnosne razine (SIL) su povezane sa vrijednošću parametra za učestalost opasnih (nezaštićenih) kvarova - TFFR (engl. *Tolerable Functional (unsafe) Failure Rate*).

Tablica 3. SIL razine

TFFR (po satu i po funkciji)	SIL
$10^{-9} \leq TFFR < 10^{-8}$	4
$10^{-8} \leq TFFR < 10^{-7}$	3
$10^{-7} \leq TFFR < 10^{-6}$	2
$10^{-6} \leq TFFR < 10^{-5}$	1



Slika 6. SIL razine sigurnosne integracije – integracija sa sistemskim i slučajnim kvarovima, izvor: [5]

8. Zaključak

Statistički podaci o radu suvremene elektroničke opreme PU-SS podsustava pokazuju da su opasni kvarovi elektroničkih SS uređaja rijetki događaji. Razlog tome je striktno pridržavanje sigurnosnih zahtjeva u fazama razvoja, proizvodnje i rada sustava (pridržavanje RAMS zahtjeva).

Osnovni načini na koje se rizici povezani s RAMS-om mogu smanjiti su poboljšanje pouzdanosti tako da se broj kvarova smanji na dopuštenu razinu skladno sigurnosnim zahtjevima i poboljšanje raspoloživosti na način da pojava kvara ne utječe na sigurnost.

Sigurnost željezničkih SS uređaja temelji se prvenstveno na strategiji potpunog otklanjanja kvarova. Međutim, tehnička i ekonomska ograničenja, mnoge složene sigurnosne mjere i tehnička rješenja u SS uređajima traže da se primjene i druge primjerene strategije, u većini slučajeva to su: strategije otklanjanja posljedica kvarova ili, kao minimum, ograničavanja njihovih posljedica.

Kvar SS uređaja mora biti doveden do sigurnog stanja (engl. *safe state*). Prvenstveni cilj je sigurno (normalno) stanje bez kvarova. Pored toga, uređaj mora prijeći u sigurno stanje kod pojave kvara (npr. kada se pojavi kvar na jednom kanalu redundantnog sustava) – to je tzv. sigurno (kritično) stanje (*engl. critical up state*) u kojem je sustav i dalje raspoloživ za uporabu uz ispunjenje zahtjeva za sigurnost.

Uređaj (ili sustav) u kojem je dokazano da su otklonjene mogućnosti za kvarove (na osnovi neodvojivih karakteristika komponenti) ne može biti doveden do opasnog stanja. Međutim, u praksi se opasno stanje samo rijetko može potpuno isključiti. U sustavima povezanim sa sigurnošću primjena principa *fail-safe* (stanje sigurnosti kod kvara) je ta koja osigurava da vjerojatnost opasnih stanja bude svedena na minimum. Ako sustav ipak prijeđe u opasno stanje, mora se što prije prebaciti u sigurno stanje kako bi se izbjegle nesreće. Stanje sustava u kojem postoji kvar i koje se ne može otkloniti sigurnosnim mjerama je neispravno stanje (*down state*) – opasno stanje.

Možemo zaključiti da u praksi ne možemo udovoljiti zahtjevima sigurnosti samo na temelju rada sustava (uređaja) bez kvaro-

va već radi osiguranja tražene (visoke) sigurnosti, sustavi se moraju dizajnirati tako da u slučaju kvara sustav odlazi u stanje sigurnosti kod kvara (*fail-safe*), a što se danas uglavnom rješava tako da se dodaju redundantni sklopovi (zalihost s više kanala) koji povećavaju raspoloživost sustava.

Primjenom suvremenih elektroničkih (mikroprocesorskih) redundantnih struktura u SS uređajima (sa najvećom sigurnosnom razinom SIL 4) osiguravaju se najveći sigurnosni normativi s kojima se značajno smanjuje vjerojatnost pojave opasnog kvara tehničkog sustava.

LITERATURA

[1] Zakon o sigurnosti i interoperabilnosti željezničkog sustava (Narodne novine broj: 63/2020)

[2] HRN EN 50126-1; Željeznički sustav – Specifikacije i prikaz pouzdanosti, raspoloživosti, mogućnosti održavanja i sigurnosti (RAMS) – 1. dio: Generički postupak RAMS-a (EN 50126-1:2017)

[3] HRN EN 50126-2; Željeznički sustav – Specifikacije i prikaz pouzdanosti, raspoloživosti, mogućnosti održavanja i sigurnosti (RAMS) – 2. dio: Sustavni pristup sigurnosti (EN 50126-2:2017)

[4] HRN EN 61703; Matematički izrazi za nazive koji se odnose na pouzdanost, raspoloživost, sposobnost održavanja i podršku održavanju (IEC 61703:2016; EN 61703:2016)

[5] HRN EN 50129; Željeznički sustav – Komunikacijska i signalna tehnika i sustavi obrade podataka - Elektronički sustavi za signalnu tehniku povezani sa sigurnošću (EN 50129:2018)

[6] Pravilnik o tehničkim uvjetima za prometno-upravljački i signalno-sigurnosni željeznički infrastrukturni podsustav (Narodne novine broj: 97/2015 (od 11.9.2025.))

[7] Uredba Komisije (EU) 2016/919 od 27. svibnja 2016. o tehničkoj specifikaciji za interoperabilnost u vezi s „prometno-upravljačkim i signalno-sigurnosnim" podsustavima željezničkog sustava u Europskoj uniji (Tekst značajan za EGP) (*OJ L 158, 15.6.2016, p. 1–79)*

[8] Izvješće o radu Agencije za sigurnost željezničkog prometa za 2021. (KLASA: 023-01/22-05/01); Agencija za sigurnost željezničkog prometa, Zagreb, listopad 2022.

[9] Izvješće o sigurnosti za 2021. godinu; HŽ Infrastruktura; Zagreb, svibanj 2022.

[10] Railway Signalling &Interlocking; International Compendium, 2nd Edition 2018; Editors: Georg Theeg, Sergej Vlasenko, 2018 PMC Media House GmbH

[11] HRN EN ISO/IEC 17020 - Ocjenjivanje sukladnosti -Zahtjevi za rad različitih vrsta tijela koja provode inspekciju (ISO/IEC 17020:2012; EN ISO/IEC 17020:2012)

[12] Provedbena uredba Komisije (EU) br. 402/2013 od 30. travnja 2013. o zajedničkoj sigurnosnoj metodi za vrednovanje i procjenu rizika i stavljanju izvan snage Uredbe (EZ) br. 352/2009 (Tekst značajan za EGP), (*OJ L 121, 3.5.2013, p. 8–25)*

[13] Željeznički sustav - Elektromagnetska kompatibilnost – 1. dio: Općenito (EN 50121-1:2017)

[14] Željeznički sustav - Elektromagnetska kompatibilnost – 2. dio: Emisija cjelokupnog željezničkog sustava u vanjski svijet (EN 50121-2:2017)

SAŽETAK

ANALIZA KVAROVA - PARAMETRI POUZDANOSTI I SIGURNOSTI ŽELJEZNIČKIH SIGNALNO-SIGURNOSNIH UREĐAJA

Sigurnost i izbjegavanje kvarova kod suvremenih elektroničkih signalno-sigurnosnih uređaja postiže se najučinkovitije kada se parametri RAMS-a kontinuirano kontroliraju kroz sve faze životnog ciklusa uređaja – od projekta, proizvodnje, ugradnje, tijekom održavanja – sve do izgradnje.

Kvarovi utječu na pouzdanost, raspoloživost, mogućnost održavanja i sigurnost sustava, pri čemu je razina tog utjecaja određena funkcionalnošću i dizajnom primijenjenog sustava. Rizik povezan s RAMS-om može se smanjiti poduzimanjem kombinacije mjera za smanjenje kvarova - smanjenjem učestalosti događaja koji rezultiraju kvarovima i smanjenjem njihove ozbiljnosti.

U praksi ne možemo izbjeći kvarove tehničkog sustava već radi osiguranja tražene (visoke) sigurnosti, sustavi se moraju dizajnirati tako da u slučaju kvara sustav odlazi u stanje „zaštićeno od kvara" (eng. „fail-safe"), a što se danas uglavnom rješava tako da se dodaju redundantni sklopovi (zalihost s više kanala).

Proračun sigurnosnih parametara pokazuje da redundantni višekanalni SS uređaji imaju veću raspoloživost i time se značajno smanjuje pojava opasnog kvara koji može ugroziti sigurnost – izazvati velike materijalne štete i smrtne posljedice.

Primjenom suvremenih elektroničkih (mikroprocesorskih) redundantnih struktura u signalnim uređajima (sa najvećom sigurnosnom razinom SIL 4) osiguravaju se najveći sigurnosni normativi s kojima se značajno smanjuje vjerojatnost pojave opasnog kvara tehničkog sustava.

Ključne riječi: *Sigurnost, signalni uređaji, kvarovi, održavanje sustava*

Kategorizacija: *Stručni rad*

SUMMARY

FAILURE ANALYSIS - RELIABILITY AND SAFETY PARAMETERS OF RAILWAY SIGNALING AND SAFETY DEVICES

Safety and failure avoidance of modern electronic signalling devices is most effectively achieved when RAMS parameters are continuously controlled through all phases of the device's life cycle - from design, production, installation, during maintenance - until construction.

Failures affect the reliability, availability, maintainability and safety of the system, where the level of this impact is determined by the functionality and design of the system. The risk associated with RAMS can be reduced by taking a combination of measures to reduce failures - reducing the frequency of events that result in failures and reducing their severity.

In practice, we cannot avoid failures of the technical system, but in order to ensure the required (high) safety, systems should be designed so that in the event of a failure, the system goes into a "fail-safe" state - today is mostly applied by redundant circuits (multi-channel redundancy).

The calculation of safety parameters shows that redundant multi-channel signalling devices have a higher availability and thus a significantly lower occurrence of dangerous failures that can threaten safety - cause great material damage and fatal consequences.

The application of modern electronic (microprocessor) redundant structures in signaling devices (with the highest safety level SIL 4) ensures the highest safety standards, which significantly reduces the probability of a dangerous failure of the technical system.

Key words: *Safety, signalling devices, failures, maintaince of the system*

Categorization: *Professional paper*