Kreiranje industrijskih upravljačkih sistema na bazi sigurnosnog PLK-a

Suad Ibrahimkadić
Služba održavanja mašina
Fabrika duhana Sarajevo
Sarajevo, Bosna and Hercegovina
sicon.sarajevo@gmail.com

Slobodan Lubura
Odsjek za automatiku i elektroniku
Elektrotehnički fakultet
Istočno Sarajevo, Bosna and Hercegovina
slobodan.lubura@etf.unssa.rs.ba

Sažetak – **Moderni sistemi upravljanja koji se danas koriste u industriji bazirani su na programabilnim logičkim kontrolerima (PLK). Takođe, i sigurnosni segment upravljačkog sistema, koji je ranije bio realizovan relejnom logikom, biva zamijenjen namjenski razvijenim uređajima - sigurnosnim PLK-ovima (engl. Functional safety PLC ili FS PLC). Cilj ovog rada je da pojasni osnovne postavke na kojima počivaju sigurnosni PLK-ovi, njihove osnovne karakteristike, te da kroz jedan konkretan primjer pruži uvid u mogućnosti koje se otvaraju u projektovanju sigurnosnog segmenta industrijskih upravljačkih sistema upotrebom ovakvih uređaja.**

Ključne riječi - sigurnosni PLK; industrijski upravljački sistemi;

I. UVOD

Segment upravljačkog sistema koji se odnosi na sigurnost ljudi i opreme u industrijskom okruženju, tradicionalno je realiziran upotrebom relejne logike, odnosno fiksno povezanih elektromehaničkih komponenti.

Razvojem PLK-ova postepeno se segment upravljačkog sistema zadužen za ispunjavanje sigurnosnih zahtjeva realizirao i korištenjem konvencionalnih PLK-ova. Zavisno od konkretne aplikacije, koristili su se različiti pristupi:

1) korištenje paralelnog, redundantnog kontrolera,
2) korištenje dodatnih U/I modula za nadzor izvršnih organa za povećanje stepena sigurnosti
3) korištenje namjenskih softverskih rješenja za nadzor, upravljanje i dijagnostiku sigurnosnog sistema
4) korištenje posebnih signala za testiranje U/I modula sigurnosnog sistema

Analizom troškova ovakvih sistema, kao i njihovih karakteristika kada su u pitanju fleksibilnost, rokovi implementacije, troškovi potrebnog inženjeringa itd, zaključilo se da je potrebno razviti namjenske uređaje koji će svojim karakteristikama moći zadovoljiti postavljene sigurnosne zahtjeve u upravljačkim sistemima.

A. Osnovne razlike između konvencionalnog i sigurnosnog PLK-a

Razlike između konvencionalnog u sigurnosnog PLK potiču iz različitih zahtjeva koji se nameću na funkcionalno sigurne upravljačke sisteme u odnosu na konvencionalne upravljačke sisteme [2]. Ovi se zahtjevi u osnovi različito realiziraju, pa se po načinu realizacije ove razlike mogu svrstati na softverske i hardverske, iako su neke od njih međusobno zavisne.

1) Softverske razlike

Za razliku od konvencionalnih, sigurnosne PLK karakterišu operativni sistemi sa implementiranim različitim tehnikama za obezbjeđivanje pouzdanosti softvera. Ovi operativni sistemi se također odobravaju od strane nezavisnih tijela ovlaštenih za takvu vrstu provjera.

U aplikativnom dijelu, sigurnost softvera je povećana kroz strožije uslove za omogućavanje izmjena aplikativnog koda (upotreba lozinki, njihova kombinacija sa serijskim brojem hardvera), zatim opsežne dijagnostičke mogućnosti, upotrebu programskih jezika ograničenih mogućnosti, kako bi se korisnik prisilio da koristi dokazane funkcijske blokove i instrukcije itd.

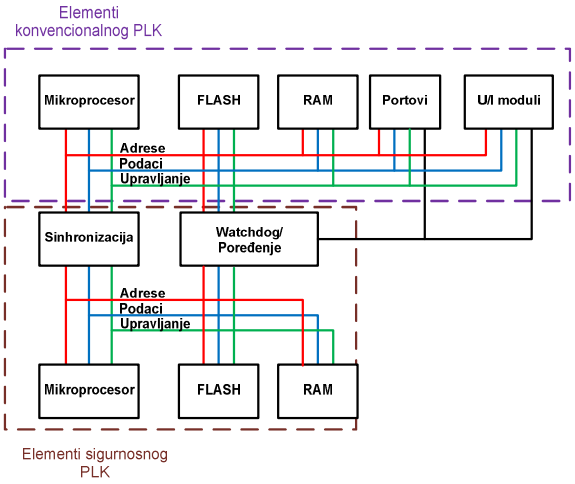
2) Hardverske razlike

Postoje tri fundamentalne razlike među hardverskim komponentama konvencionalnih i sigurnosnih PLK-ova [1]:

a) Arhitektura
b) Ulazni moduli
c) Izlazni moduli

a) Arhitektura: Ukoliko uporedimo arhitekture konvencionalnog i sigurnosnog PLK-a, kao što je to prikazano na Sl. 1, uočava se da konvencionalni PLK ima jedan mikroprocesor koji izvršava korisnički program, jednu FLASH memoriju za čuvanje programa, jednu RAM memoriju za smještanje međurezultata, portove za komunikaciju i U/I module za vezu sa periferijom, odnosno za razmjenu fizičkih signala.

Arhitektura sigurnosnih PLK je nešto složenija, jer pored navedenih elemenata, sadrži i dodatni (redundantni) mikroprocesor, *FLASH* i RAM memoriju, koji se kontinuirano nadziru od strane *Wachdog timera* i kola za sinhronizaciju.

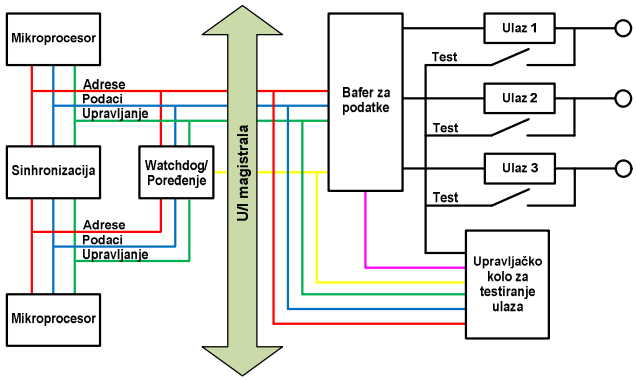


Slika 1: Arhitektura sigurnosnog PLK-a

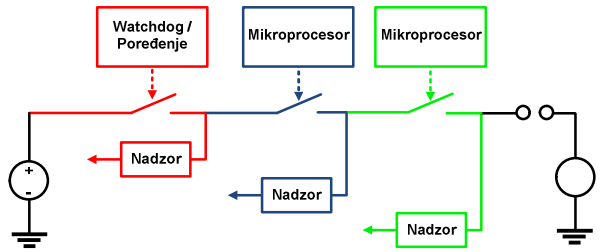
b) Ulazni moduli: Konvencionalni PLK ne vrši nikakve interne provjere funkcionalnosti ulaznih modula. Za razliku od njega, sigurnosni PLK u okviru svojih ulaznih modula imaju ugrađene dodatne testne linije koje se koriste za testiranje funkcionalnosti modula. U normalnom radu, preko ovih testnih linija u kratkim vremenskim ciklusima šalju se testni signali, kako bi se verifikovala funkcionalnost ulaznih modula. Arhitektura ulaznih modula sigurnosnih PLK prikazana je na Sl.2.

c) Izlazni moduli: Konvencionalni PLK u svom izlaznom modulu ima samo jedan prekidački element po izlazu, dok sigurnosni PLK u izlaznom modulu ima više prekidačkih elemenata (kanala) koji su vezani u seriju. Status svakog prekidačkog elementa se provjerava i koristi kao uslov za aktivaciju izlaza.

Za donošenje odluke o prelasku sigurnosnog PLK-a u sigurno stanje (detektovan je sigurnosni problem), mogu da se koriste različiti uslovi. Ovi se uslovi prema IEC 61508 označavaju kao "MooN" (*engl. "M out of N"*), gdje je N ukupan broj korištenih kanala, a M broj kanala koji moraju biti verifikovani kao ispravni za normalan rad kontrolera.



Slika 2: Arhitektura ulaznog kola sigurnosnog PLK



Slika 3: Arhitektura izlaznog modula sigurnosnog PLK

Tako npr. arhitektura "1oo2" ima toleranciju greške 1, jer će PLK normalno raditi kada se verifikuje rad bar jednog izlaznog kanala od 2 moguća. U arhitekturi 2oo2, ova je tolerancija 0 i detekcija kvara na bilo kojem kanalu dovodi do prelaska sigurnosnog PLK u unaprijed definisano sigurno stanje.

Na Sl. 3 dat je simbolički prikaz arhitekture "2oo2", sa dva mikroprocesora koji nisu međusobno komunikacijski povezani.

II. INTERNACIONALNI STANDARDI KAO OSNOVA ZA REALIZACIJU SIGURNOSNOG PLK

Sigurnosni PLK je tipični predstavnik grupe E/E/PE sigurnosnih sistema. Kao i za druge elemente iz ove grupe, razvoj i korištenje E/E/PE sigurnosnih sistema je definisano i odgovarajućim međunarodnim standardima.

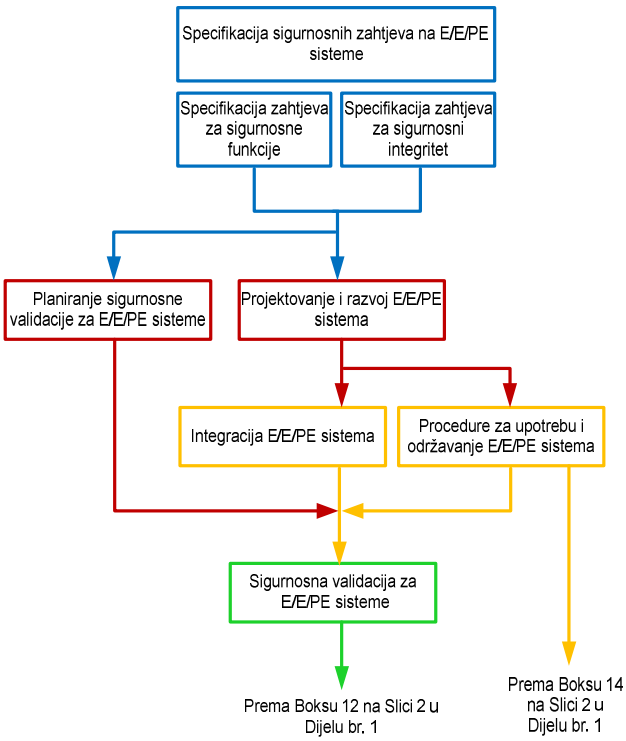
A. IEC 61508

Godine 1998. objavljen je prvi dio internacionalnog standarda poznatog pod oznakom IEC 61508 - "Funkcionalna sigurnost električnih/elektronskih/programabilnih elektronskih (E/E/PE) sigurnosnih sistema" [4].

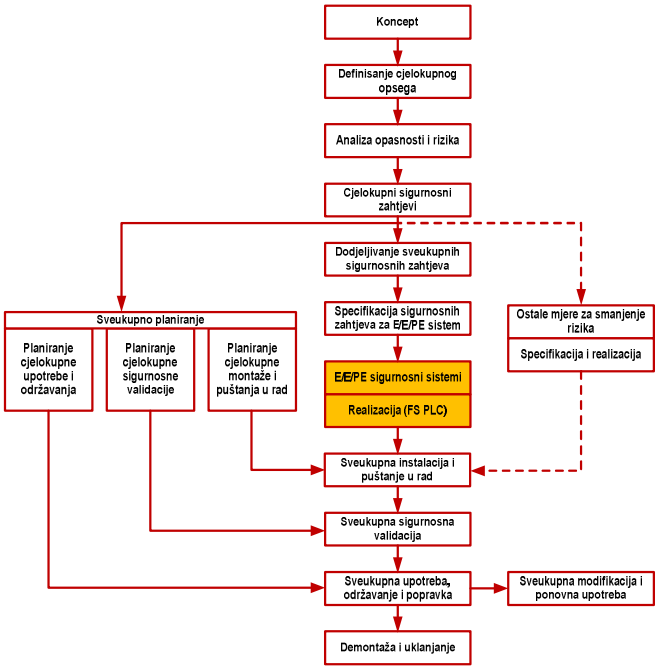
Ovaj standard se sastoji od 7 dijelova, pri čemu su neki od njih naknadno objavljivani:

1) *Dio 1:* Opšti zahtjevi (razvoj, instalacija, puštanje u rad, validacija, održavanje i sl.)
2) *Dio 2:* Zahtjevi za E / E / PE sigurnosne sisteme
3) *Dio 3:* Zahtjevi na softver
4) *Dio 4:* Definicije i skrćenice
5) *Dio 5:* Primjeri metoda za određivanje nivoa sigurnosti (SIL)
6) *Dio 6:* Vodič za primjenu Dijela 2 i Dijela 3
7) *Dio 7:* Pregled tehnika i mjera

Obzirom da se prilikom realizacije E/E/PE sigurnosnih sistema mogu koristiti i hardverski i softverski elementi, to su i za njihovo korištenje nadležni različiti dijelovi standarda, kako je to prikazano na Sl. 4.



Slika 4: Dio životnog ciklusa E/E/PE sistema (faza realizacije)



Slika 5: Sigurnosni PLK u okviru cjelokupnog životnog ciklusa E/E/PE sigurnosnih sistema

Ukoliko se razvija neki E/E/PE sigurnosni sistem, tada se njegova hardverska struktura definiše u skladu sa IEC 61508-2 [5], dok se softverska arhitektura, kao i integracija hardverske i softverske arhitekture, te plan za njihovu realizaciju, kreiraju u skladu sa IEC 61508-3 [6].

B. IEC 61131-6

IEC 61131-6 predstavlja 6. dio međunarodnog standarda koji se odnosi na programabilne logičke kontrolere [11]. Ovaj dio standarda se bavi detaljnim opisivanjem specifičnih zahtjeva za primjenom principa IEC 61508 na PLK-ove.

Glavni ciljevi ovog standarda su:

1) da utvrdi i opiše elemente životnog ciklusa sigurnosnog PLK-a, usklađeno sa IEC 61508 -1/ -2 / -3.

2) da utvrdi i opiše zahtjeve za sigurnosni PLK hardver i softver koji se odnose na zahtjeve funkcionalne sigurnosti i zahtjeve za integritetom sigurnosti E/E/PE sigurnosnih sistema

3) da utvrdi metode ocjene sigurnosnih PLK-ova po osnovu različitih parametara: nivoa integriteta sigurnosti (engl. Safety Integrity Level - SIL), vrijednosti vjerovatnoće greške pri zahtjevu za rad (engl. Probability of Failure on Demand - PFD), prosječna frekvencija opasnih otkaza po satu (engl. Average frequency of dangerous failure per hour - PFH), frakcija sigurnih otkaza (engl. Safe Failure Fraction - SFF), tolerancija na grešku hardvera (engl. Hardware Fault Tolerance - HFT), pokrivenost dijagnostikom (engl. Diagnostic Coverage - DC) itd.

4) da utvrdi definicije i identifikuje principijelne karakteristike koje se odnose na izbor i primjenu sigurnosnih PLK-ova i pridruženih periferala

Položaj sigurnosnih PLK-ova u sigurnosnom životnom ciklusu E/E/PE sigurnosnih sistema prikazan je na Sl. 5.

C. IEC 61784-3

Ovaj standard [10] specificira i objašnjava osnovne principe koji se mogu koristiti u prijenosu sigurnosno-orijentiranih poruka među distribuiranim učesnicima u komunikaciji u okviru mreže koja koristi "*fieldbus*" tehnologiju, a u skladu sa zahtjevima prema IEC 61508 za funkcionalnu sigurnost.

Obzirom da se "fieldbus" tehnologija smatra dobro prihvaćenom i dokazanom, iskorištena je za prijenos sigurnosno-orijentiranih poruka u okviru sigurnosnih protokola. Tako se u okviru postojećeg "*fieldbus*" protokola, kreira poseban sloj koji se odnosi na sigurnosno-orijentirane podatke. Na ovaj način se omogućuje da se preko istog fizičkog medija (bakarna žica, optičko vlakno ili radio-talas) prenose paralelno i standardni i sigurnosno-orijentirani podaci. Za pouzdan prijenos podataka, odnosno da bi se jedan "*fieldbus*" protokol mogao koristiti u sigurnosnom sistemu, neophodno je dokazati da se u kontinuiranoj upotrebi od 100000 godina može pojaviti maksimalno jedna nedetektovana greška.

Greške u komunikaciji, prema IEC 61784-3 su:

1) Korupcija - greška koja može da se pojavi u okviru samog učesnika u komunikaciji, zatim u prenosnom mediju ili usljed međusobnog miješanja poruka

2) Neželjeno ponavljanje - stara, neažurirana poruka se ponavlja u pogrešnom trenutku

3) Netačna sekvenca - preddefinisana sekvenca sa nekog od učesnika u komunikaciji je netačna

4) Gubitak poruke - poruka nije primljena ili nije potvrđena

5) Neprihvatljivo kašnjenje - prijem poruke je zakašnjen duže od dopuštenog vremena

6) Insertovanje - poruka koja se prenosi odnosi se na neočekivani ili nepoznati izvor

7) Pretvaranje - poruka je dostavljena od prividno korektnog izvora, ali u stvarnosti nije sigurnosno orijentirana, a prijemnik je tretira kao sigurnosnu.

8) Adresiranje - sigurnosna poruka je poslana pogrešnom sigurnosnom uređaju, koji je onda tretira kao korektnu poruku

Mjere koje su prema IEC 61784-3 na raspolaganju za prevenciju grešaka u komunikaciji su: brojač sekvenci, vremenski pečat (*engl. time stamp*), očekivano vrijeme, autorizacija konekcije, povratna poruka, osiguranje integriteta podataka, redundancija sa provjerom, kriptografičke tehnike.

III. REALIZACIJA SIGURNOSNOG SISTEMA

U ovom poglavlju će biti opisana realizacija tipičnih zadataka sigurnosnog sistema upotrebom sigurnosnog PLK-a. Opisom će biti obuhvaćene dvije bitne funkcije:

1) Hitno zaustavljanje (engl. Emergency Stop)

2) Zabravljivanje pristupnih vrata (engl. Door Interlocking)

Za realizaciju je korištena oprema proizođača *Beckhoff* [15], ali je, zahvaljujući pomenutim standardima, na sličan način moguće koristiti i opremu drugih proizvođača PLK (*Siemens, ABB, Mitsubishi, Schneider itd*).

A. Karakteristike korištene opreme

Za realizaciju sigurnosnog sistema, odnosno navedenih funkcija, korišteni su sljedeći moduli:

1) EL1904 - modul za povezivanje četiri sigurnosna digitalna ulaza

2) EL2904 - modul za povezivanje četiri sigurnosna digitalna izlaza

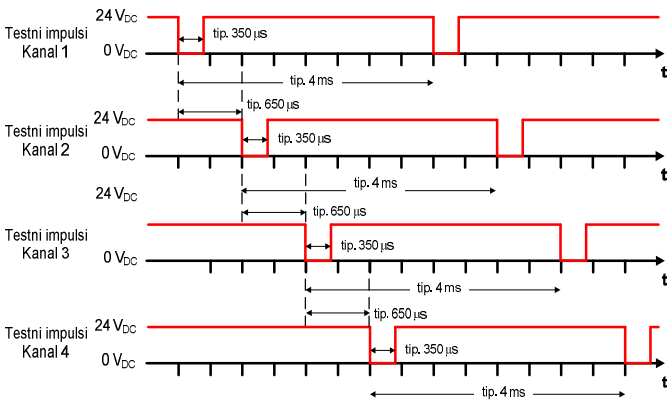
3) EL6900 - logički modul (FS PLK)

Kompletna konfiguracija, validacija kao i transfer sigurnosne aplikacije u logički modul vrši se iz jednog razvojnog okruženja - *TwinCAT System Manager* [16].

1) Ulazni modul

EL1904 predstavlja modul namijenjen za povezivanje sigurnosnih ulaza sa perifernim uređajima [7]. Osnovna razlika u odnosu na standardne ulazne module leži u činjenici da se kod ovakvih modula ciklično vrši testiranje funkcionalnosti ulaznih linija. Testiranje se sastoji u kratkotrajnoj promjeni stanja napojnog signala, kao što je prikazano na Sl. 6.

Za normalan rad, svakom ulaznom modulu je potrebno dodijeliti jedinstvenu adresu u okviru sigurnosnog sistema, što se vrši podešavanjem DIP prekidača na tijelu modula.



Slika 6: Testiranje funkcionalnosti ulaznih linija za EL1904

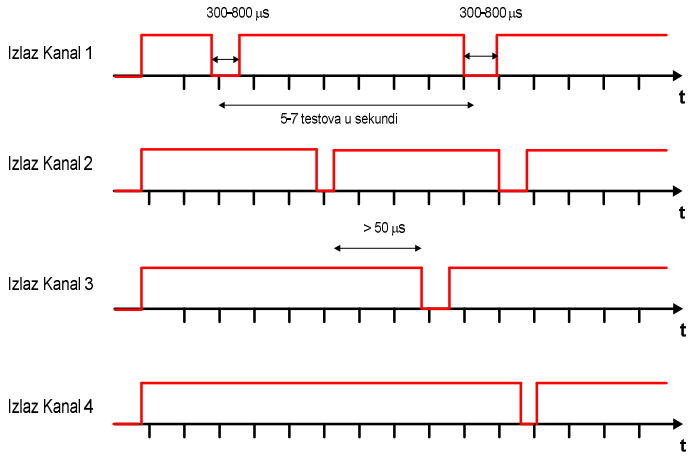
2) Izlazni modul

Izlazni modul EL2904 također karakteriše ciklično testiranje funkcionalnosti linija [8], kao što je to prikazano na Sl. 7. I ovaj modul posjeduje DIP prekidače za podešavanje jedinstvene adrese ovog modula u sigurnosnom sistemu.

3) Logički modul

EL6900 predstavlja modul koji povezuje signale ulaza i izlaza koristeći standardne funkcijske blokove, a u skladu sa odabranom aplikacijom [9]. Zadovoljava zahtjeve IEC 61508:2010 SIL 3. Korisniku je na raspolaganju 14 različitih funkcijskih blokova, koji su već certificirani, što značajno olakšava certificiranje i cjelokupnog sigurnosnog sistema realiziranog upotrebom ovakvog sigurnosnog PLK-a.

Sigurnosna aplikacija se kreira konfigurisanjem i parametriziranjem ovih funkcijskih blokova. Sve veze ulaznih i izlaznih signala grupisane su u blokove koji se nazivaju TwinSAFE grupe. Ukoliko neki od signala iz jedne grupe detektuje sigurnosni problem ili se detektuje greška nekog od elemenata u grupi, tada cijela grupa prelazi u sigurni režim, odnosno u beznaponsko stanje.



Slika 7: Dijagram testiranja funkcionalnosti izlaznih linija za EL2904

Zahvaljujući usklađenosti sa sigurnosnim standardima, dozvoljena je distribuirana konfiguracija, odnosno sigurnosni moduli se ugrađuju što bliže samim senzorima i izvršnim organima, pri čemu se ne umanjuje funkcionalnost cijelog sistema.

Sve informacije o statusu *TwinSAFE* grupe, kao i pojedinačnih funkcijskih blokova, moguće je mapirati u standardnu PLK aplikaciju i na taj način ih učiniti dostupnim za vizualizaciju, ali i za izdavanje komandi za reset greške, ponovno pokretanje rada grupe itd.

Kombinacijom ulaznih signala i npr. izlaza iz funkcijskih blokova, moguće je realizirati i kompleksnije sigurnosne funkcije.

Kada se radi o zaštiti od neautorizovanog pristupa, baš kako to standardi i predviđaju, moguće je definisati posebne lozinke za pristup, koje ni na koji način nisu vezane za standaradnu PLK aplikaciju. Prije svakog transfera aplikacije u logički modul, izvrši se validacija aplikacije alatom integriranim u razvojno okruženje. Tokom svake od ovih funkcija od korisnika se traži upisivanje jedinstvenih podataka: korisničko ime, serijski broj logičkog modula, te lozinke koja odgovara navedenom korisniku.

B. Funkcija hitnog zaustavljanja

Funkcija hitnog zaustavljanja predstavlja jednu od osnovnih sigurnosnih funkcija koja se koristi u projektovanju industrijskih mašina. Prema EN ISO 13850, funkcija hitnog zaustavljanja se definiše kao funkcija koja:

1) sprječava pojavu ili smanjuje postojeću opasnost za ljude, nastanak štete za mašine ili rad koji je u toku

2) pokreće se jednom akcijom čovjeka kada normalna funkcija zaustavljanja nije dovoljna za tu svrhu

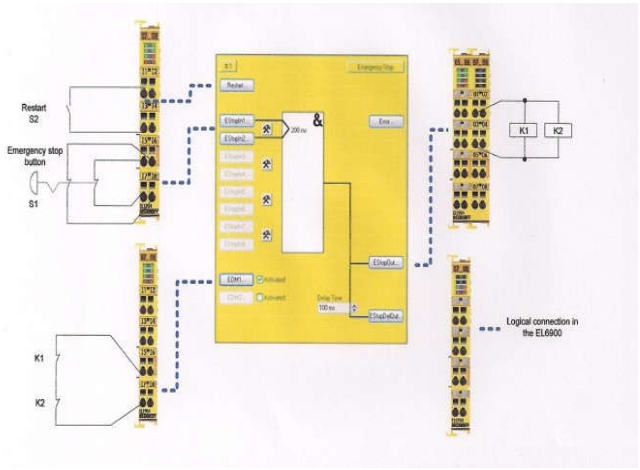
Uređaj za hitno zaustavljanje je ručno kontrolisan uređaj, a kao aktuator mogu da posluže taster u obliku gljive, konopci, žice ili sl. Prema važećim standardima, tasteri koji se koriste kao aktuatori na uređajima za hitno zaustavljanje moraju biti crvene boje, dok pozadina aktuatora za hitno zaustavljanje mora biti žute boje.

Pored vizualnih, aktuator hitnog zaustavljanja mora da zadovolji i mehaničke karakteristike, prije svega funkciju zabravljivanja. Naime, nakon što se funkcija hitnog zaustavljanja aktivira, on ostaje u tom položaju sve dok se ponovo ručno ne vrati u početni položaj.

Pored toga, funkcija hitnog zaustavljanja mora biti izvedena tako da vraćanje mehaničkog prekidača u prvobitni položaj ne izaziva ponovno pokretanje kontrolisane mašine ili procesa, nego je za takvo što neophodna posebna komanda za start.

Na Sl. 8 su simbolički prikazani elementi za realizaciju sigurnosne funkcije hitnog zaustavljanja [12].

Dakako, prikazano rješenje predstavlja samo jednu od mogućnosti u rješavanju ove funkcije. Kakva će biti struktura konačnog rješenja u konkretnom slučaju zavisi i od traženog nivoa integriteta sigurnosti.



Slika 8: Realizacija hitnog zaustavljanja

Ostvareni nivo integriteta sigurnosti se računa pomoću vrijednosti pojedinih sigurnosnih parametara opreme koje daje proizvođač opreme, te uz upotrebu formula prema standardu EN13849-1.

Pored pomenutih hardverskih modula u realizaciji je iskorišten i funkcijski blok "*Emergency Stop*". Zahvaljujući parametrima ovog bloka, moguće ga je iskoristiti na različite načine.

Tako je npr. moguće:

1) konfigurisati ulaze kao NO ili NC kontakte

2) definisati maks. vremensku razliku između 2 signala na ulazu

3) pored direktnog, koristiti i zakašnjeli izlaz iz bloka

4) koristiti povratnu informaciju sa opreme na koju djeluje izlaz iz funkcijskog bloka

5) definisati poseban signal za reset funkcijskog bloka

6) omogućiti prijenos dijagnostičkih i statusnih informacija prema standardnoj PLK aplikaciji

C. Zabravljivanje pristupnih vrata (engl. Door Interlocking)

Prema IEC 14119, zaštitni uređaj za blokiranje (Engl. Interlocking device) predstavlja uređaj mehaničkog, električnog ili nekog drugog tipa, čija je svrha da spriječi upotrebu elemenata mašine pod specificiranim uslovima (općenito sve dok zaštitna ograda nije zatvorena) [13].

Postoje različiti principi realizacije ovih uređaja:

1) uređaji za blokadu bez zabravljivanja

2) uređaji za blokadu sa zabravljivanjem

Kod uređaja koji rade na prvom principu, uvijek je moguće otvoriti zaštitnu ogradu. Ukoliko ograda nije zatvorena, uređaj za blokadu generiše komandu za zaustavljanje.

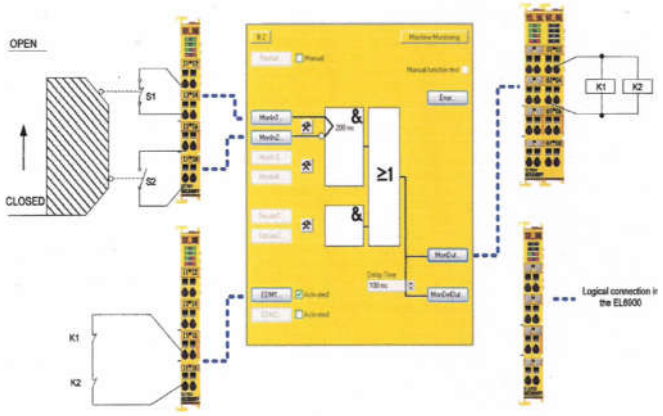
Kod uređaja koji rade na drugom principu, ograda se drži zatvorenom od strane samogu uređaja za blokiranje.

Ovi se uređaji također dijele u dvije grupe:

1) uređaji koji se u svako doba mogu odbraviti od strane operatora

2) uređaji koji se mogu odbraviti samo nakon ispunjavanja nekog uslova, osiguravajući da je opasnost nestala.

Realizacija sigurnosne funkcije se sastoji u povezivanju kontakata brave uređaja za blokadu na modul za dig. ulaze, a komanda za napajanje pokretnog elementa se daje sa modula za dig. izlaze, kako je simbolično prikazano na Sl. 9 [12].



Slika 9: Realizacija nadzora pristupnih vrata

IV. ZAKLJUČAK

U posljednjih 15-tak godina u svijetu se intenzivno radi na usaglašavanju međunarodnih standarda koji se bave pitanjem sigurnosti ljudi, opreme i proizvoda. Posebno su se razvijali standardi kojima se definišu uslovi za primjenu električnih / elektronskih / programabilnih elektronskih uređaja u sigurnosnim upravljačkim sistemima [3].

Kao jedan od rezultata uloženih napora, razvijeni su namjenski, sigurnosni PLK-ovi, koji nesporno pružaju niz pogodnosti:

1) fleksibilnost rješenja sigurnosnog sistema

2) smanjeni troškovi inžinjeringa i ožičenja sistema

3) smanjeno vrijeme i trošak puštanja sistema u rad

Ipak, iskustva pokazuju da primjena sigurnosnih PLK-ova za rješavanje sigurnosnog sistema nije uvijek ekonomski opravdana, te da zavisi od kompleksnosti aplikacije. Zbog toga se prije donošenja odluke strogo preporučuje provođenje analize i upoređivanja troškova rješenja sa fiksno ožičenom logikom, sa troškovima rješenja sa upotrebom sigurnosnog PLK-om.

LITERATURA

[1] Rockwell Automation, "PLC vs Safety PLC - Fundamental and Significant Differences", White paper, 2002.

[2] JEMA: The Japan Electrical Manufacturers' Association, "Safety of Machinery – Guidelines of Functional Safety PLC", PLC Technical Commitee, 2011.

[3] International Electrotechnical Commission, "Functional Safety", Brochure, 2015

[4] IEC, "IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety related systems Part 1: General requirements", 1997.

[5] Indian Standard, "Functional safety of electrical /electronic/programmable electronic safety related systems Part 2: Requirements for E/E/PE safety-related systems", 2000.

[6] IEC, "IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety related systems Part 3: Software requirements", 1997.

[7] Beckhoff Automation Gmbh & Co.KG, "EL1904 TwinSAFE input terminal with 4 fail-safe inputs", Version 1.5.1, 2015.

[8] Beckhoff Automation Gmbh & Co.KG, "EL2904 TwinSAFE output terminal with 4 fail-safe outputs", Version 1.6.1, 2015.

[9] Beckhoff Automation Gmbh & Co.KG, "EL6900 TwinSAFE Logic terminal version 1.5.1", 2015.

[10] IEC, "IEC 61784-1: Industrial communication networks - Profiles – Part 1 – Fieldbus profiles", 2009.

[11] IEC, "IEC 61131-6: Programmable controllers - Part 6: Functional Safety", 2012.

[12] Beckhoff Automation Gmbh & Co.KG, "Application guide: TwinSAFE,Version 1.6.2", 2015.

[13] Japanese Industrial Standard, „JIS B 9710 (2006) (English): Safety of machinery – interlocking devices – Principles of design and selections", 2006.

[14] PROFIBUS Nutzerorganization e.V, „PROFIsafe System Description – Technology and apllication", 2010.

[15] Beckhoff Automation Gmbh & Co.KG, http://www.beckhoff.com

[16] Beckhoff Automation Gmbh & Co.KG, http://www.beckhoff.com /english/twincat/SysMang.htm?id=159876032042705

ABSTRACT

Modern industrial control system used today are based on programmable logic controller (PLC). Safety related part of the control system, earlier realized using relay logic, is replaced by specifically tailored devices - Functional safety PLCs.

The aim of this paper is to clarify basic foundations that functional safety PLCs rely on, as well as their basic characteristics, and, using a concrete example, to give an insight in the oportunities in industrial control system design when using such devices.

INDUSTRIAL CONTROL SYSTEM DESIGN BASED ON FUNCTIONAL SAFETY PLCs

Suad Ibrahimkadić, Slobodan Lubura