NADZOR U SISTEMU UPRAVLJANJA ROBOTIZOVANOG RENTGENA ZA VISOKU BEZBEDNOST U RADU
MONITORING IN THE CONTROL SISTEM OF ROBOTIZED MEDICAL ROENTGEN DEVICE FOR HIGH FUNCTIONAL SAFETY

Milun Jevtić, Goran S. Đorđević, *Elektronski fakultet, Niš*

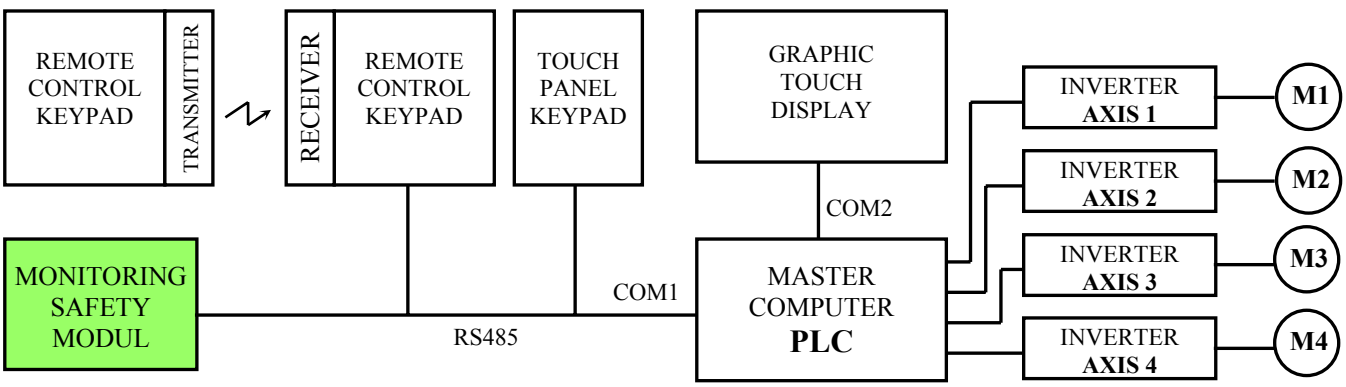
Sadržaj - *Za ostvarivanje visoke bezbednosti u radu robotizovanog rentgena realizovan je i u radu prikazan poseban nadzorni modul u upravljačkom sistemu rentgena. Zasnovan je na posebnom mikroračunaru sa povećanom sigurnošću sopstvenog funkcionisanja. Zadatak modula je da nadzire korektnost izvršavanja svih zadataka u upravljačkom sistemu rentgena. Prikupljajući redundantno sa upravljačkom jedinicom informacije od brojnih senzora, nadzire korektnost realizacija robotizovanih funkcija rentgena, i detektuje ekscesne događaje. Nadzorom i razmenom poruka sa uređajima upravljačkog sistema pravovremeno detektuje i eventualni otkaz nekog od uređaja. U slučaju detektovanja bilo koje nekorektnosti tokom rada rentgena, modul aktivira odgovarajući proces postavljanja robotizovanog robota u bezbednu poziciju. Sveukupno, realizovano je potpuno predvidivo ponašanje robotizovanog rentgena.*

Abstract - *Robotized medical roentgen device must operate as a high safety device during its lifetime. Therefore the control system must include a safety monitoring module. One such safety monitoring module is described in this paper. The module design is based on the microcontroller with increased dependability. The main task of the module is to monitor the correctness of the tasks performances during regular or irregular operation of the medical roentgen. It accepts all the commands and all the signals from the sensors, safety components and from inverters, to detect possible dangerous events. By monitoring and by exchange of the messages the safety module also detects malfunctioning in each of the motion control components. In the event of a failure, the module activates the process to guide the roentgen device into the safe state. Altogether, the controller along with the safety monitoring module provides fully reliable and predictable operation of the robotized roentgen device.*

1. UVOD

Robotizacija rentgena ima za cilj da unapredi manipulaciju operatera rentgenom - automatizuje proces snimanja i smanji opasnost izlaganja operatera zračenju. Međutim pri robotizaciji se zahteva i nešto više, a to je sigurnost u radu, odnosno uvek predvidivo ponašanje sistema koje će garantovati bezbednost pacijentu i pri pojavi otkaza. U ovom radu se upravo razmatra kako je u upravljačkom sistemu robotizovanog rentgena to postignuto.

Arhitektura robotizovanog rentgena data je u radu [1], a za nju globalna blokovska struktura upravljačkog sistema prikazana je na slici 1. Robotizovan rentgen ima kretanja po četiri ose. PLC upravlja kretanjima komandujući invertorima za svaku osu. U sistemu upravljannja, pored grafičkog displeja sa osetljivim ekranom na dodir kao glavnom mestu za interakciju sa serviserom i operaterom, postoji i funkcionalna tastatura na mestu snimanja za pozicioniranje aparature za snimanja, kao i mobilnu bežičnu funkcionalnu tastaturu za pripremu i samo snimanje [2]. Funkcionalne tastature kao *slave*-ovi sa PLC-jem kao *master* računarom povezane su preko *multipoint* RS485 veze. Kako se praktično preko te veze komanduje robotizovanim funkcijama rentgena



Slika 1. *Blok-šema upravljačkog sistema robotizovanog rentgena*

koje izvršava PLC, na toj vezi je i nadzorno sigurnosni modul MSM (Monitoring Safety Modul). Njegov zadatak je da obezbedi visoku sigurnost u radu robotizovanog rentgena, odnosno njegovo predvidivo bezbedno ponašanje čak i u slučaju pojave grešaka u upravljačkom sistemu. Zbog toga su na robotizovanom rentgenu postavljeni i brojni senzori koji na ovoj blokovskoj strukturi upravljačke jedinice nisu predstavljeni. Ali kroz prikaz ostvarivanja bezbednog rada robotizovanog rentgena oni će se sagledati.

2. FUNKCIJE MSM-A

Osnovna funkcija MSM modula je nadzor svega što može ugroziti bezbedno funkcionisanje robotizovanog rentgena i postavljanje sistema u bezbedno stanje u slučaju detektovanja neke nekorektnosti. Sam modul može biti u dva načina rada:

1. Servisni;
2. Funkcionalno bezbednosni.

U servisni način rada MSM se postavlja samo od strane autorizovanog servisera. Tada serviser može postavljati parametre rada sistema (programiranje parametara sekvenci kretanja, postavljanje graničnih vrednosti softverskih limita, itd.) i startovati posebne procedure interaktivnog testiranja. Inače MSM i u servisnom modu izvršava nadzor kao i u funkcionalno bezbednosnom - daje informacije o stanju sistema, ali ne aktivira funkciju bezuslovnog zaustavljanja kretanja po svim osama. To je neophodno da bi se pri testiranju mogla testirati kretanja i preko softevrskih limita i da bi serviser mogao sistem da izvede iz stanja bezuslovnog stopa pri pojavi uslova za koje se ne dozvoljava restartovanje sistema bez servisera.

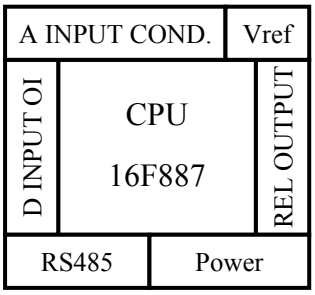
MSM u funkcionalno bezbednosnom načinu rada ostvaruje visoku bezbednost u radu robotizovanog rentgena kroz realizaciju sledećih zadataka:

- Po uključenju napajanja dozvoljava rad robotizovanog rentgena (ukida bezuslovni stop) tek pošto utvrdi da ne postojanja nijednog uslova za STOP.
- Nadzire da li su uređaji upravljačkog sistema povezani na *multipoint* vezu u funkciji, realizacijom savršenih detektora otkaza [3],[4]. Na taj način se detektuje eventualno nefunkcionisanje MSM-a i PLC-a, od kojih i ključno zavisi bezbedno funkcionisanje sistema.
- U periodičnoj razmeni poruka sa PLC-jem prepoznaje koje komande kretanja po osama su izdate od strane PLC-a i šalje status robotizovanog rentgena na osnovu nadzora stanja senzora u sistemu i prepoznavanja korektnih izvršavanja komandi.
- Da pravovremeno detektuje sve ekscesne događaje i preduzme odgovarajuće akcije kojima će se sistem postaviti u bezbedno stanje.
- Za pojedine ekscesne događaje generiše bezuslovni stop svih kretanja i onemogući naredne komande kretanja bez intervencije servisera.
- Za pojedine ekscesne događaje generiše bezuslovni stop svih kretanja, a zatim i omogući naredne komande kretanja ako se uslov koji je izazvao eksces ukine.
- Za ekscesni događaj aktiviranja *bumper* senzora zaustavlja kretanje, a zatim omogućava kretanje samo u suprotnom smeru.
- Realizuje funkcije samotestiranja sistema.

3. STRUKTURA MSM-A

MSM je realizovaan kao poseban mikroračunar baziran na mikrokontroleru i softveru realizovanom po modelu namenskih operativnih sistema za rad u realnom vremenu.

Arhitektura hardvera MSM-a blokovski je prikazana na slici 2. Bazirana je na mikrokontroleru PIC 16F887 koji ima ugrađen *watchdog* tajmer sa sopstvenim oscilatorom. Time je omogućeno sigurno detektovanje neizvršavanje korektnog programa, a i testiranje samog *watchdog*-a. Digitalnih ulaza sa optokaplerskim razdvajanjem ima 24 i grupisani su u tri grupe sa mogućnošću korišćenja posebnih izvora napajanja za svaku. Devet digitalnih ulaza mogu svojim aktivnim stanjem generisati zahtev za interapt CPU-u. Realizovana su i kola za kondicioniranje analognih signala; četiri od potenciometarskog davača pozicije po svakoj osi kretanja i jedan od senzora sile na bazi otpornih traka u mostu. Radi korišćenja celog opsega A/D konvertora posebnim izvorom referentnog napona generisani su Vref- i Vref+ za A/D konvertor i referentni napon za pobudu senzora sile i potenciometara za detekciju pozicija. USART i RS485 drajveri realizuju priključak na komunikacioni kanal i komunikaciju sa PLC-om. Izvor napajanja generiše preko posebnik kola potrebne napone za napajanje digitalnih i analognih kola. Pri samoj realizaciji na štampanoj ploči posebno je vođeno računa o odvajanju analognog dela od digitalnog kako bi se minimizirao uticaj digitalnog šuma na tačnost informacije o analognoj veličini. Dva relejna izlaza su sa mirnim i radnim kontaktima.

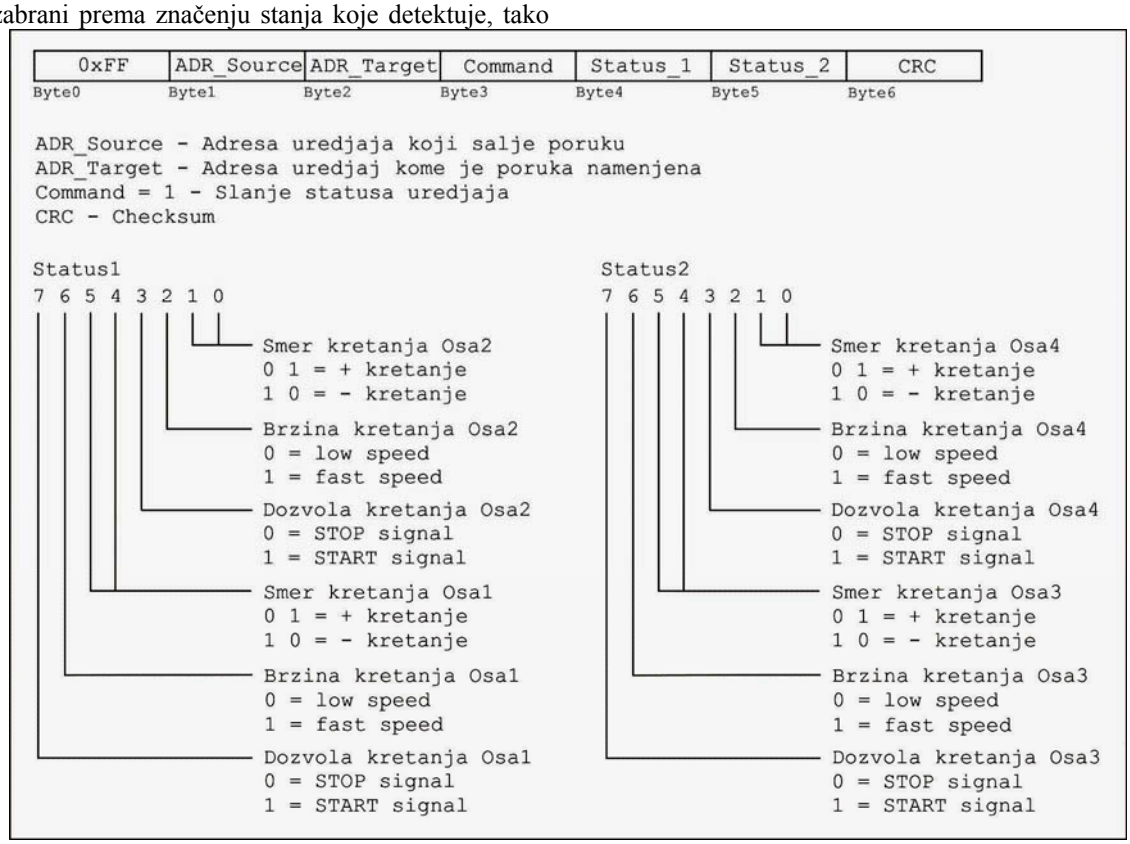


Slika 2. *Blokovska predstava hardvera MSM*

Vezivanjem radnog kontakta relejnog izlaza na red sa dva mirna kontakta prekidača (pečurke) bezuslovnih stopiranja realizovana je takozvana sigurnosna petlja čijim se prekidanjem deaktivira sklopka za dovođenje mrežnog napajanja invertorima. Radni kontakt drugog relejnog izlaza se koristi za dovođenje napajanja radi deaktiviranja elektromagnetne kočnice za osu kretanja. MSM aktivira relejne izlaze, čime daje dozvolu kretanja po osama po komandama iz PLC-a, tek nakon:

- uspešne sopstvene inicijalizacije,
- uspostavljanja komunikacije sa PLC-om,
- provere da ne postoji ni jedan aktivan ulaz koji zahteva STOP i
- provere da prethodno nije zbog nekog ekscesnog stanja postavljeno STOP sa obavezom da samo serviser omogućava ponovno funkcionisanje.

Senzori upotrebljeni u sistemu robotizovanog robota su pažljivo izabrani prema značenju stanja koje detektuje, tako da prekid u vezi sa senzorom, gubitak napajanja senzora i



Slika 3. *Poruka od PLC-a ka MSM-u*

otkaz samog senzora budu detektovani kao ekscesni događaj. Značenje senzora i njihov broj će se sagledati kroz analizu grešaka koje oni detektuju u sistemu.

Softver MSM-a je realizovan tako da obezbeđuje rigidne vremenske zahteve. Komunikacija se obrađuje preko interapta i aktiviranja niti (thread-a) kada je poruka primljena u predviđenom vremenskom intervalu. U nitima koje se periodično aktiviraju obrađuju se pojedine grupe senzora, a oni čije aktiviranje zahteva STOP se obrađuju prioritetno.

4. RAZMENA PORUKA IZMEĐU PLC-A I MSM-A

Razmena poruka između PLC-a i ostalih *slave* uređaja povezanih na zajednički *half duplex* komunikacioni kanal odvija se slanjem poruke od PLC-a kao mastera i odzivom *slave*-a u predviđenom vremenskom prozoru.

Osnovna poruka koju periodično na svakih *Tpor* =100 ms MSM dobija od PLC-a prikazana je na slici 3. Početak poruke je bajtom vrednosti 0xFF, koji se u samoj poruci ne može pojaviti, osim na kraju poruke kao CRC kod za proveru ispravnosti primljene poruke (što ne remeti detektovanje početka poruke jer se bajt 0xFF može i više puta uzastopno ponavljati). Ona daje informacije o statusu kretanja po pojedinim osama. Na osnovu toga MSM proverava korektnost kretanja koje se ostvaruje invertorima upravljanim PLC-em. Bit dozvole kretanja STOP/START po svakoj osi je bit koji označava kada je kretanje startovano i kada je izdata komanda invertoru za zaustavljanje kretanja. Znači to je različito od zahteva za STOP preko sigurnosnog kola u slučaju ekscesa ili aktiviranja prekidača pečurke za bezuslovni stop.

Ukoliko nakon isteka vremena *Tout* > *Tpor* MSM ne primi poruku od PLC-a zaustavlja se rad robotizovanog robota – aktivira se STOP. Po ponovnom prijemu poruke rad sistema se dozvoljava. Dve uzastopne greske u prenosu-prijemu poruka detektovane kao CRC-Error se karakterišu kao gubitak komunikacije. U tom slucaju se prekida rad robotizovanog rentgena postavljanjem u stanje STOP. Po ponovnom uspostavljanju komunikacije - prijemom korektne komande rad sistema se omogućava ukidanjem zahteva za STOP.

Odziv MSM-a na svaku primljenu poruku od PLC-a sledi po završetku prijema i kratkotrajnog tajmauta za okretanje linije. Na prethodno opisanu poruku od PLC-a MSM odgovara porukom prikazanom na slici 4. Poruka sadrži statuse pojedinih senzora kritičnih krajnjih pozicija i softverskih limita po pojedinim osama kretanja i statuse detektovanih grešaka u radu robotizovanog rentgena.

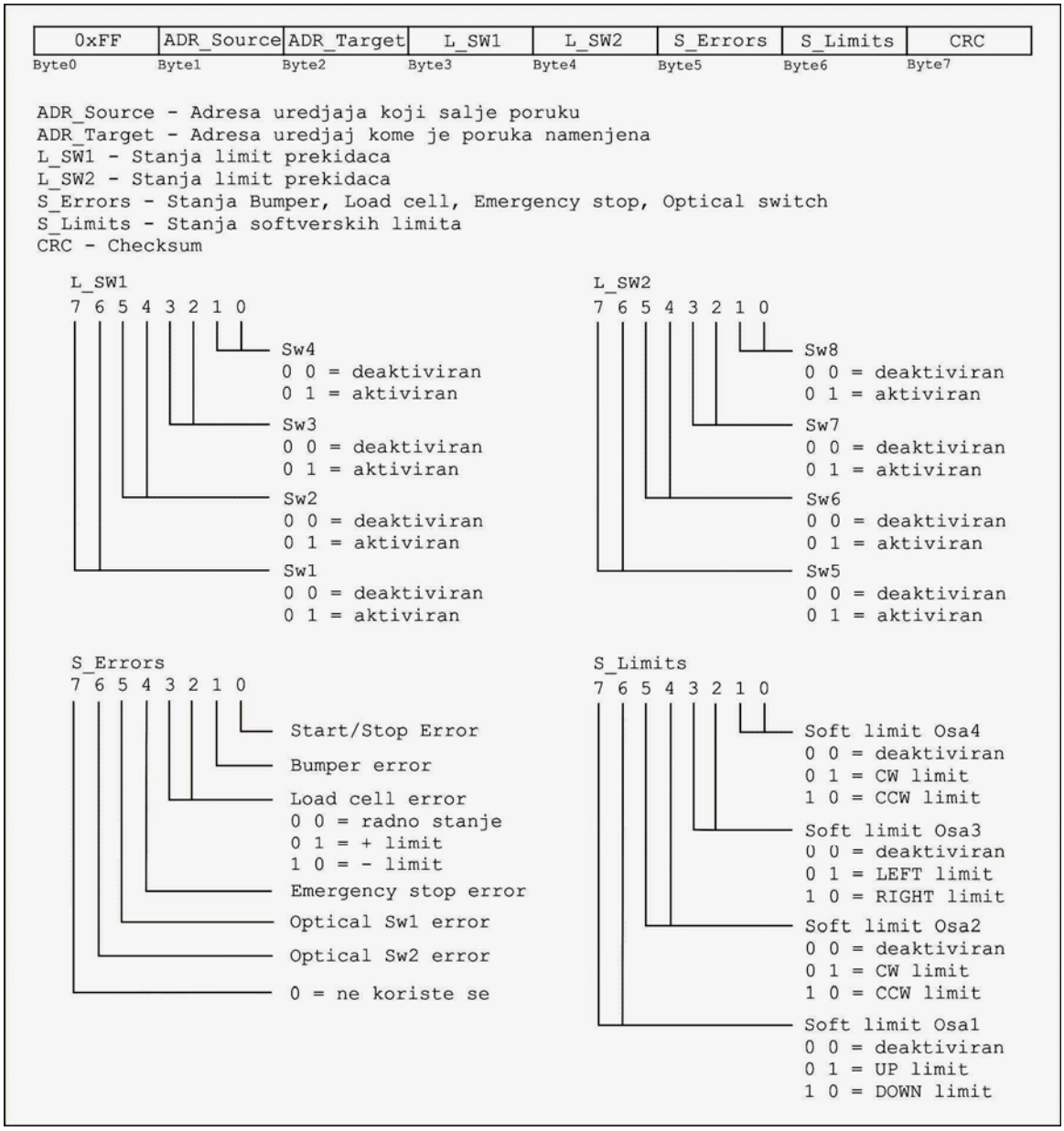
5. GREŠKE KOJE DETEKTUJE MSM I AKTIVNOSTI MSM-A PRI TOME

Senzori u sistemu robotizovanog rentgena čija se stanja vode na PLC i MSM koriste se za detektovanje sledećih grešaka i aktiviranje bezbednosnih aktivnosti:

1. Limit switch errors:

Ukoliko je neki od graničnh prekidača (Sw1 do Sw8) aktiviran sprovodi se sledeća akcija:

- Aktivira se STOP - zaustavljaju se ketanja u sistemu (rad robotizovanog rentgena) - OUT1_OFF, OUT2_OFF;
- Ponovno funkcionisanje sistema omogućava serviser.



Slika 4. *Poruka odziva MSM-a ka PLC-u*

2. Start/Stop error:

Ova greška se javlja ukoliko je PLC izdao komandu za kraj kretanja (MSM primio u STATUS_1 i STATUS_2 da nema dozvole kretanja) a ono i dalje postoji. Kada MSM detektuje pozicionim potenciometrom kretanje za više od 1-og santimetra po isteku vremena TSTOP (vreme zaustavljanja usled inercije) od trenutka primljene komande za kraj kretanja, MSM sprovodi sledeće akcije:

- Aktivira se STOP - zaustavlja se rad sistema postavljanjem relejnih izlaza u off stanje (OUT1_OFF, OUT2_OFF);
- Ponovno funkcionisanje sistema omogućava serviser.

3. *Bumper* error:

Ukoliko dodje do aktiviranja *Bumper* senzora pri kretanju po Osi_1 naniže ili Osi_2 u + smeru (suprotno od kretanja kazaljke na satu), PLC reaguje tako što započinje kretanje inverzno prethodnom do zadate pozicije. MSM reaguje na sledeci nacin:

- Startuje tajmer *Tbump* (*Tbump* je vreme potrebno da se uredjaj vrati u bezbednu poziciju).
- Ukoliko je po isteku vremena *Tbump bumper* senzor i dalje aktivan, aktivira se STOP - rad sistema se onemogućava: OUT1_OFF, OUT2_OFF.
- Ponovno funkcionisanje sistema (deaktivira se STOP) omogućava MSM kada *Bumper* senzor posatne neaktivan i ne postoji ni jedan drugi uslov za STOP.

4. Load cell error:

Greška se detektuje poređenjem trenutne vrednosti senzora sile *Vr_SS* sa graničnim vrednostima.

- Ako se pri kretanju po Osi_1 naniže i/ili 2._ose u – smeru (u smeru kretanja kazaljke na satu) detektuje *Vr_SS* < *LDVr_SS* (limit s donje strane – minimalno opterećenje kada nema koalizije i sajla nije pukla) u trajanju dužem od *Tkoal*,(kolizije) MSM generiše STOP i setuje grešku Load_Cell_Error = 10.
- Ako se u bilo kojoj drugoj situaciji (nema pomenutih kretanja) detektuje *Vr_SS* < *LDVr_SS* u trajanju dužem od *Tpusal* (pucanja sajle) MSM generiše STOP i setuje grešku Load_Cell_Error = 10 (rasterećenje sajle).
- Ako se pri kretanju 1._ose naviše detektuje *Vr_SS* > *LGVr_SS* (limit s gornje strane – maksimalno opterećenje kada nema greške u mehanici) MSM generiše STOP i setuje grešku Load_Cell_Error = 01 (preopterećenje sajle).
- Oscilacije *Vr_SS* izazvane polaskom i zaustavljanjem, kao i na neki drugi ne tako bitan način izazvane, nemaju uticaja jer su u opsegu koji ne premašuje limit vrednosti.
- Deaktivira se STOP (ponovno funkcionisanje sistema se omogućava po prijemu poruke od PLC-a) ako se izgubi uslov koji je generisao STOP, i kada nema drugih uslova koji bi aktivivrali STOP.

5. Emergency stop error:

Do greske dolazi aktiviranjem Emergency stop prekidaca.
MSM reaguje na sledeci nacin:
- Aaktivira STOP - zaustavlja se rad sistema OUT1_OFF, OUT2_OFF.
- Nakon deaktiviranja Emergency stop prekidaca, MSM proverava stanje sistema. Ukoliko ni jedan od senzora nije aktivan, to jest nema nijednog uslova koji bi generisao STOP, rad uredjaja se omogućava – deaktivira se STOP po prijemu poruke od PLC-a.
- Ukoliko je neki od senzora aktivan, to jest postoji neka greška, rad sistema se ne omogućava.

6. Optical SW1 error:

Ukoliko je Optical SW1 aktivan MSM su:
- Po prijemu poruke od PLC-a MSM analizira Status_1 i Status_2 radi provere da li je postavljena mala brzina kretanja.
- Ako ni posle primljene naredne (dve uzastopne) poruke ne utvrdi postavljanje male brzine kretanja, MSM aktivira STOP. Ovaj STOP se može deaktivirati kada O_SW1 postane neaktivan i kada ne postoje drugi uslovi za aktiviranje STOP-a;

7. Optical SW2 error:

Ukoliko je Optical SW2 aktivan pri kretanju Ose_1 naniže i/ili Ose_2 u + smeru (u smeru suprotnom od kretanja kazaljke na satu) MSM:
- Posle vremena *Tzaustavljanja* aktivivra STOP (PLC zaustavlja kretanje).
- Ovaj STOP se može deaktivirati kada O_SW2 postane neaktivan i kada ne postoje drugi uslovi za aktiviranje STOP-a;

8. Soft limits error:

Ukoliko stanje potenciometra bude jednako nekom od soft limita ili ga premašuje po toj osi MSM:
- Provera u narednom primljenom Status_1 i Status_2 da li je kretanje obustavljeno (postavljeno da nema kretanja);
- Ako ni posle primljene naredne (dve uzastopne) poruke ne utvrdi obustavljanje kretanja, MSM aktivira STOP;
- Ako MSM detektuje kretanje promenom stanja pozicionog potenciometra za više od 1-og santimetra po isteku vremena *TSTOP* od trenutka detektovanja Soft_limita, MSM aktivira STOP;
- Ako je kretanje obustavljeno i nema kretanja posle *TSTOP* MSM ne preduzima nikakvu akciju.
- Ako je aktiviran STOP ponovno funkcionisanje sistema omogućava serviser.

6. ZAKLJUČAK

Više hardvera u upravljačkom sistemu robotizovanog rentgena znači i veću verovatnoću nastanka otkaza u samom hardveru. Međutim, imlementacija dodatnog nadzorno sigurnosnog modula MSM u upravljačkom sistemu robotizovanog rentgena je neophodna radi obezbeđivanja bezbednog rada sistema u odnosu na pacijenta i moguće havarijske situacije u sistemu. Pri realizaciji funkcija MSM-a za bezbedan i uvek predvidiv rad sistema neophodno je koristiti analizu najgoreg slučaja i predvideti sve moguće ekscesne događaje koji mogu nastati zbog pojave nekog otkaza (prolaznog ili stalnog) u sistemu ili pogrešnog rukovanja sistemom. Uz sve realizovane funkcije MSM-a logično je realizovati i funkciju kreiranja arhive ekscesnih događaja koja nije u radu pomenuta.

7. LITERATURA

[1] Svemir Popić, Srđan Mladenović, Goran S. Đorđević, Konačna verzija prototipa robotizovanog radiografskog uređaja za primenu u medicini**,** *Zbornik radova* INFOTEH-JAHORINA 2009, Vol. 8, Ref. E1-9, p. 824-828, Mart 2009. ISBN-99938-624-2-8

[2] M. Božić, Miljan Milanović, "Upravljački interfejs za univerzalni rendgen stativ", *Zbornik radova* INFOTEH-JAHORINA 2009, Vol. 8, Ref. E1-1, st. 786-789, Mart 2009. ISBN-99938-624-2-8

[3] Milun Jevtić, Bojan Jovanović, Sandra Brankov, Marko Cvetković, "Jedna realizacija detektora kvara u upravljačkim sistemima robota", *Zbornik radova* INFOTEH-JAHORINA 2009, Vol. 8, Ref. E1-7, st. 814-818, Mart 2009. ISBN-99938-624-2-8

[4] C. Fetzer, "Perfect Failure Detection in Timed Asynchronous Systems," *IEEE Trans. Computers,* vol. 52, No. 2, pp. 99-112, Februar 2003.

Ključne reči: upravljanje, nadzor, sigurnost, bezbednost, predvidivo ponašanje, redundantnost, robot, rentgen