UNIVERZA V MARIBORU
FAKULTETA ZA STROJNIŠTVO
FAKULTETA ZA ELEKTROTEHNIKO,
RAČUNALNIŠTVO IN INFORMATIKO

Jernej ŽOLGER

NADZORNI SISTEM ZA IZVAJANJE VARNOSTNIH TESTOV STROJA

Magistrsko delo
študijskega programa 2. stopnje
Mehatronika

Maribor, september 2019

Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko

Fakulteta za strojništvo

NADZORNI SISTEM ZA IZVAJANJE VARNOSTNIH TESTOV STROJA

Magistrsko delo

Študent:	Jernej ŽOLGER
Študijski program:	študijski program 2. stopnje Mehatronika
Mentor FS:	izr. prof. dr. Karl GOTLIH
Mentor FERI:	doc. dr. Miran RODIČ
Somentor:	Timi KARNER

Maribor, september 2019

ZAHVALA

Zahvaljujem se mentorjema izr. prof. dr. Karlu Gotlihu in doc. dr. Miranu Rodiču ter osebju SMM, d. o. o., za pomoč, vodenje in koristna navodila pri opravljanju magistrskega dela. Prav tako se zahvaljujem podjetju SMM, d. o. o., za ponujeno priložnost izdelave magistrskega dela v njihovem podjetju.

Posebna zahvala gre mojim najbližjim, ki so mi vsa leta študija stali ob strani in me podpirali.

NADZORNI SISTEM ZA IZVAJANJE VARNOSTNIH TESTOV STROJA

Ključne besede: PLC, HMI, varnost strojev, standardi, funkcionalna varnost, varnostni test

UDK: 620.1.051:681.518.52(043.2)

Povzetek

Tematika magistrske naloge je razvoj in implementacija nadzornega sistema za izvajanje varnostnih testov stroja. Predstavljena je pot, kako priti do frekvence omenjenega izvajanja testov. Varnost strojev je v osnovi predpisana s standardom ISO 12100, ki daje generalne smernice za njihovo oblikovanje. Uporablja se tudi standard ISO 13849, ki predstavlja splošna načela za načrtovanje in validacijo varnostnih delov krmilnih sistemov. V delu je podrobno analiziran ta standard, saj poda smernice funkcionalne varnosti strojev, kar zajema tudi dodatna varnostna načela, med katera spada varnostni preizkus. Nadzorni sistem se izvaja z dvema PLC-jema, povezanima s HMI aplikacijo. V drugem delu sta opisana program in vizualizacija, ki služita za spremljanje varnostne opreme in izvajanje varnostnih testov stroja.

CONTROL SYSTEM FOR THE IMPLEMENTATION OF MACHINERY SAFETY TESTS

Key words: PLC, HMI, Machine safety, Standards, Functional safety, Safety Test

UDK: 620.1.051:681.518.52(043.2)

Abstract

The topic of this master's dissertation is the development and implementation of the control system of machinery safety tests. Its purpose is to present the process of reaching the frequency of its implementation. The safety of the machinery starts with the ISO 12100 standard which provides general guidelines for the designing of the machinery. Then the standard ISO 13849 comes into consideration which represents general principles for the design and validation of the safety components of control systems. This standard is analyzed in detail, because it provides the guidelines for the functional safety of the machinery among which are additional safety principles that also incorporate a safety test. The supervisory system is executed with two PLCs connected to the HMI application. In the second part there are the description of the program and the visualization that serve the monitoring of safety equipment and the execution of the supervisory system of machinery security tests.

KAZALO

KAZALO SLIK

KAZALO TABEL

SEZNAM UPORABLJENIH SIMBOLOV IN KRATIC

RA	Rockwell Automation
AB	Allen Bradley
FT	FactoryTalk
PLC	Programabilni logični krmilnik (Programmable logic controller)
ISO	Mednarodna organizacija za standardizacijo (International Organization for Standardization)
PPE	Osebna zaščitna oprema (Personal protective equipment)
SS	Varnostni sistem (Security Systems)
CEN	Evropski odbor za standardizacijo (European Committee for Standardization)
EN	Evropski normativi (European normative)
SRP/CS	Varnostni deli nadzornega sistema (Safety-Related Part of a Control System)
E-STOP	Naprava za izklop v sili (Emergency stop)
PL_r	Zahtevana raven zmogljivosti (Required performance level)
PL	Raven učinkovitosti (Performance level)
PL_a	Raven učinkovitosti a (Performance level a)
PL_b	Raven učinkovitosti b (Performance level b)
PL_c	Raven učinkovitosti c (Performance level c)
PL_d	Raven učinkovitosti d (Performance level d)
Pl_e	Raven učinkovitosti e (Performance level e)
$MTTF_d$	Povprečni čas do nevarnega izpada vsakega kanala (Mean time to dangerous failure)
DC_{avg}	Povprečna diagnostična pokritost (Average diagnostic coverage)
PFH_d	Verjetnost nevarne okvare na uro (Probability of a dangerous failure per hour)
DC	Diagnostična pokritost (Diagnostic coverage)
CCF	Odpoved skupnega vzroka (Common cause failure)
IEC	Mednarodna komisija za elektrotehniko (International electrotechnical commission)
SIL	Stopnja varnostne celovitosti (safety integrity level)
Cat.	Kategorija (Category)
B_{10D}	Število ciklov, dokler 10 % komponent odpove

T_{10D}	Povprečni čas, dokler 10 % komponent odpove
h_{op}	Povprečen čas delovanja [h/d]
d_{op}	Povprečen čas delovanja [d/y]
t_{cycle}	Povprečen čas delovanja med začetkom dveh zaporednih ciklov komponente [s/cikel]
λ_d	»Nevarna« odpoved
λ_{dd}	Zaznane »nevarne« odpovedi
λ_{du}	Nezaznane »nevarne« odpovedi
DC%	Diagnostična pokritost (Diagnostic coverage) [%]
HSE	Britanska agencija za zdravje in varnost (Health and Safety Executive)
FMEA	Analiza napak in učinkov (Failure mode and effects analysis)
ANSI	Ameriški državni inštitut za standarde (American National Standards Institute)
CSA	Podjetje za certificiranje izdelkov – organizacija standardov
HFT	Toleranca napake strojne opreme (hardware fault tolerance)
OSSD	Varnostni izhod (Output signal switching device)
SAP	Programska oprema za posel
HMI	Vmesnik človek–stroj (Human machine interface)
OP	Operacijski panel (Operation panel)

1 UVOD

Dandanes, ko gre razvoj industrije v smeri industrije 4.0, je njeno bistvo predvsem v povezavi pametnih tovarn in preostale pametne infrastrukture, ki povezuje tako ljudi kot stroje. Vendar trenutno to še ni povsem realizirano, saj zajema avtomatizacija večino procesov v tovarni, ki so neodvisni in le delno avtomatizirani. Med drugim so to tudi namenski stroji, ki za svoje delovanje vseeno potrebujejo človeško roko. Pri teh sta največjega pomena prav varnost in zdravje človeka, ki sta poleg družine dve najpomembnejši vrednoti.

Za doseganje varnosti stroja se morajo proizvajalci dodobra poglobiti v varnostne standarde. Vsak stroj mora namreč izpolnjevati varnostne in zakonske zahteve. V ta namen so v industriji že vrsto let prisotni varnostni elementi. Varnostne opreme je na tržišču vse več, najbolj razširjena pa je varnostna gobica. Med varnostne elemente sodijo tudi varnostni industrijski krmilniki za krmiljenje varnosti stroja. Poleg omenjene varnostne opreme obstajajo še varnostna vrata, zavese, preproge itd. Tako je v 21. stoletju prav vsak stroj opremljen z varnostnimi elementi in mednje sodi tudi naš.

Konfekcijski stroj za izdelavo gum je sestavljen iz varnostnega krmilnika in nekaj drugih krmilnikov, ki skrbijo za njegovo delovanje. V opremi na stroju je tudi varnostna oprema, ki pa tako kot večina elementov ni 100-odstotno zanesljiva. V industriji se tako poleg varnostnih elementov preverja tudi njihovo delovanje. V stroj bi se zato integrirala funkcija za izvajanje varnostnih testov. Ti bi se morali izvajati na koncu oz. na začetku vsake izmene. Varnostni test v industriji pomeni, da se testira celotna oprema, stroj pa medtem ne obratuje. V tem času se preveri, če vsi oz. vsaj določeni varnostni elementi delujejo brezhibno in v tem primeru lahko stroj nemoteno deluje do konca izmene. V primeru okvare se ta zazna, preden bi lahko v naslednji izmeni prišlo do nesreče. Danes se pri večjih kompleksnih strojih izvaja varnostni test prav zaradi morebitnih okvar in posledično nesreč. Z omenjeno integracijo bi torej lahko zagotavljali popolno varnost stroja, kar je tudi v skladu z zakonskimi zahtevami.

1.1 Cilj magistrskega dela

Konfekcijski stroji za izdelavo gum so vodeni preko dveh krmilnikov podjetja Rockwell Automation (RA), znamke Allen Bradley (AB), ki sta povezana skupaj v razširitvi. Krmilnika imata tudi svojo vizualizacijo, ki poteka na dveh panelih, na katerih je naložen operacijski sistem Windows in FactoryTalk (FT) Machine Edition View, ki deluje kot integriran sistem znotraj operacijskega sistema. Stroj je sestavljen iz kar nekaj servo osi, ventilov, senzorjev in varnostnih stikal ter varnostnega programirljivega logičnega krmilnika (PLC).

Stroj deluje povsem avtomatsko do trenutka, ko se aktivira kakšna ročna funkcija ali se sproži kakšen varnostni element. Po standardih strojegradnje mora biti vsak premik dobro zaščiten z varnostnimi elementi, da ne pride do nesreč. Prav tako lahko varnostni elementi kdaj zatajijo oz. lahko pride do njihove okvare. Da bi se okvaram oz. nesrečam preventivno izognili, se uporablja poseben protokol, ki opisuje varnostne teste stroja. Pri tem se testira celotna varnostna oprema ali pa zgolj njen del.

Cilj dela oz. nadgradnje stroja je dodajanje dodatnih funkcij, med katere spada tudi varnostni test. Ta se izvaja bodisi avtomatsko po koncu oz. začetku vsake izmene ali pa se sproži ročno. Pri tem je treba upoštevati, da varnostni test izvaja operater stroja, kar pomeni, da mu mora biti ta prilagojen, zato mora biti vizualizacija lahko učljiva oz. prilagodljiva.

2 VARNOST STROJEV

Področje strojev je pomemben del strojne industrije. Družbene stroške zaradi nesreč, ki jih neposredno povzroči uporaba strojev, je mogoče znižati že z varno zasnovo strojev ter z njihovo pravilno montažo in vzdrževanjem. Podjetja so odgovorna za zagotavljanje zdravja in varnosti oseb, zlasti delavcev, predvsem v povezavi s tveganjem, ki nastaja zaradi uporabe strojev [1].

Proizvajalci strojev morajo uporabljati vse varnostne ukrepe v skladu z rezultati ocene tveganja, ob upoštevanju predvidene uporabe strojev in kakršne koli razumno predvidljive napačne uporabe. Podrobnejše smernice za izvajanje varnostnih ukrepov so na voljo v standardih in direktivah. V »DIREKTIVI 2006/42/ES EVROPSKEGA PARLAMENTA IN SVETA« je zapisano:

> *»Države članice so na svojem ozemlju odgovorne za zagotavljanje zdravja in varnosti oseb, zlasti delavcev in potrošnikov in, kadar je to potrebno, domačih živali in blaga, predvsem v povezavi s tveganjem, ki nastaja zaradi uporabe strojev.«* [2]

Nadalje velja tudi:

> *»Proizvajalec ali njegov pooblaščeni zastopnik bi moral za stroje, ki jih želi dati na trg, zagotoviti tudi izvedbo ocene tveganja. V ta namen bi moral ugotoviti, katere bistvene zdravstvene in varnostne zahteve se uporabljajo za njegove stroje in v zvezi s katerimi mora sprejeti ukrepe.« [2]*

Proizvajalci in uporabniki strojev morajo upoštevati vse tehnične in organizacijske ukrepe, ki so na voljo za zagotavljanje varnosti upravljavcev strojev, saj so zaščitni ukrepi bistveni za zaščito delavcev pred nepotrebnimi in preprečljivimi poškodbami na strojih. Mehanska oprema, orodja in drugi stroji lahko predstavljajo nevarnosti za uporabnike, vključno s točkami stiskanja, točkami striženja, točkami zdrobitve itd.

Pravilo, ki si ga velja zapomniti, je: »Vsak strojni del, funkcija ali postopek, ki se premika, lahko povzroči poškodbo in mora biti varovan.« Če lahko delovanje stroja ali nenamerni stik z njim poškoduje uporabnika ali druge v bližini, morajo biti nevarnosti nadzorovane ali odpravljene [4].

2.1 Standardi na področju varnosti strojev

Proizvajalci strojev morajo uporabljati tudi vse varnostne ukrepe v skladu z rezultati ocene tveganja, ob upoštevanju predvidene uporabe strojev in kakršnekoli razumno predvidljive napačne uporabe.

Zahteve je mogoče izpolniti z uporabo varnostnih standardov za stroje:

- Standardi tipa A (osnovni varnostni standardi) dajejo osnovne koncepte, načela za načrtovanje in splošne vidike, ki se lahko uporabljajo za vse stroje.
- Standardi tipa B (splošni varnostni standardi) obravnavajo en varnostni vidik ali eno vrsto zaščitnih ukrepov, ki se lahko uporabljajo v številnih strojih:
    - standardi tipa B1 za določene varnostne vidike (npr. varnostne razdalje, temperatura površine, hrup);
    - standardi tipa B2 za zaščitne ukrepe (npr. krmiljenje z dvema rokama, zaporne naprave, naprave, občutljive na pritisk, zaščita).
- Standardi tipa C (standardi za varnost strojev) obravnavajo podrobne varnostne zahteve za določen stroj ali skupino strojev.

Splošna načela načrtovanja varnosti strojev, ocene tveganja in zmanjšanja tveganja so predstavljena v varnostnem standardu ISO 12100. Osnovni namen standarda ISO 12100 je oblikovalcem zagotoviti splošen okvir in smernice, ki jim omogočajo izdelavo strojev, ki so varni za njihovo predvideno uporabo. Zagotavlja tudi strategijo za oblikovalce standardov. Pojem varnosti strojev upošteva zmožnost stroja, da v svojem življenjskem ciklu opravlja svoje predvidene funkcije, če je bilo tveganje ustrezno zmanjšano [3].

V okviru magistrskega dela je najpomembnejši standard ISO 13849, ki predstavlja splošna načela za načrtovanje in validacijo varnostnih delov krmilnih sistemov in bo predstavljen kasneje.

Slika 2.1 Logotip ISO [25]

3 OCENA TVEGANJA

Tudi če se škoda ne pojavi, lahko obstaja možnost tveganja in škode. Zaradi tehnološkega napredka se danes uporablja veliko različnih strojev in kemičnih snovi, kar lahko privede do večje možnosti za tveganje in škodo. Poleg tega je za zmanjševanje nesreč treba izvajati varnostne in sanitarne ukrepe na preventiven in ne na reaktiven način.

Ocena tveganja je torej metoda za potrditev varnosti, zagotovi se varnost delavcev in drugih posameznikov ter zmanjša se možnost škode. V splošnem je ocena tveganja kombinirano prizadevanje za:

- ugotavljanje in analiziranje potencialnih nevarnosti, ki lahko imajo negativen vpliv, in
- presojo »o dopustnem tveganju na podlagi analize tveganja« ob upoštevanju raznih dejavnikov [15].

Poenostavljeno ocena tveganja analizira, kaj gre lahko narobe, koliko verjetno bo prišlo do izpostavitve nevarnosti, kakšne so potencialne posledice in koliko dopustno je ugotovljeno tveganje [15].

Slika 3.1 Ocena tveganja [41]

3.1 Nevarnosti

Tveganje je opredeljeno kot »kombinacija verjetnosti nastanka škode in resnosti te škode«, lahko ga zapišemo tudi z enačbo [11]:

$$Tveganje = Resnost\ škode \times Verjetnost\ nastanka\ škode \tag{3.1}$$

- Mehanske nevarnosti, povezane s strojem, strojnimi deli ali površinami, orodji, obdelovanci lahko povzročijo razna drobljenja, striženja, rezanja in podobno.
- Električna nevarnost lahko povzroči poškodbe zaradi električnega udara ali opeklin.
- Toplotna oz. termična nevarnost lahko povzroči razne opekline in oparine zaradi stika s predmeti ali materiali z ekstremno temperaturo ter zaradi plamenov, eksplozij ali sevanja iz virov toplote.
- Nevarnost zaradi hrupa lahko povzroči trajno izgubo sluha in druge učinke, kot sta utrujenost in izguba zavesti.
- Nevarnosti zaradi vibracij se lahko prenesejo na celotno telo, zlasti na roke in roke [3].

Glede na zapisano obstaja veliko nevarnosti, ki jih lahko povzročijo stroji oz. deli stroja.

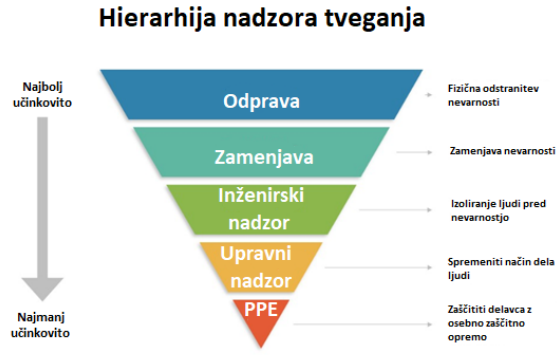
3.2 Osnovna strategija za zmanjšanje tveganja

Predpostavlja se, da bo nevarnost, če je prisotna na stroju, prej ali slej povzročila škodo, če se ne sprejme zaščitnih ukrepov. Ti so kombinacija ukrepov, ki jih sprejmeta oblikovalec in uporabnik.

Ocena tveganja je prvi korak k zmanjšanju tveganja, kateremu so izpostavljeni uporabniki strojev. Drugi korak je zmanjšanje tveganja, ki se včasih imenuje nadzor tveganja ali zmanjšanje tveganja.

Cilj je kar najbolj zmanjšati tveganje. Sistem se imenuje hierarhija, ker se mora vsako raven uporabiti po vrstnem redu, po katerem se uvrščajo na seznam [3].

Hierarhija na sliki 3.1 je bila v zadnjih 20 letih razvita v številnih različnih standardih, pri čemer je vodilni mednarodni standard ISO 12100. Zamisel je bila zagotoviti skupno strukturo, ki bi oblikovalcem pomagala pri nadzoru tveganja [11].



Slika 3.2 Hierarhija nadzora tveganja [12]

Vsaka plast v hierarhiji ima določeno stopnjo učinkovitosti, ki je odvisna od načinov odpovedi, povezanimi z nadzornimi ukrepi, in relativne učinkovitosti pri zmanjšanju tveganja v tem sloju. Kar zadeva učinkovitost pri zmanjševanju tveganja, je najučinkovitejša prva raven v hierarhiji, zadnja pa najmanj[12].

3.3 Odprava nevarnosti ali zmanjšanje tveganja z zaščitnimi ukrepi

Ta cilj se lahko doseže z odstranitvijo nevarnosti ali z zmanjšanjem – ločeno ali sočasno – vsakega od dveh elementov, ki določata tveganje:

a) resnost škode zaradi obravnavane nevarnosti,
b) verjetnost nastanka škode.

Vsi zaščitni ukrepi, namenjeni dosegi tega cilja, se uporabijo v skladu z naslednjim zaporedjem, imenovanim »tristopenjska metoda« (glej sliko 3.3):

- Inherentno varni projektni ukrepi: ta faza je edina, pri kateri je mogoče odpraviti nevarnosti, s čimer se izognemo potrebi po dodatnih zaščitnih ukrepih, kot so zaščita ali dopolnilni zaščitni ukrepi.
- Varovanje in morebitni dopolnilni zaščitni ukrepi.
- Informacije o prisotnosti preostalega tveganja.

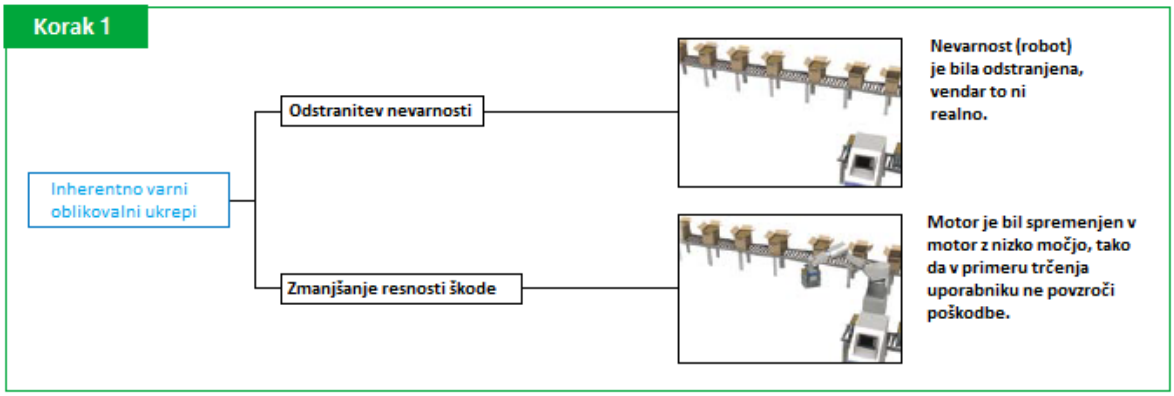
Informacije za uporabo ne smejo nadomestiti pravilne uporabe varnih oblikovnih ukrepov ali zaščitnih ali dopolnilnih zaščitnih ukrepov [3].

Slika 3.3 Tristopenjska metoda [11]

Inherentno varna zasnova

Inherentno varna zasnova je oblikovanje pristopa, ki je sam po sebi varen in je najučinkovitejši varnostni ukrep za zmanjšanje tveganja. Sestavljajo ga:

- odstranitev ali zmanjšanje nevarnosti v največji možni meri s pravilno izbiro konstrukcijskih značilnosti stroja in
- zmanjšanje osebne izpostavljenosti nevarnostim z zmanjšanjem števila potrebnih posegov v nevarnih območjih [12].



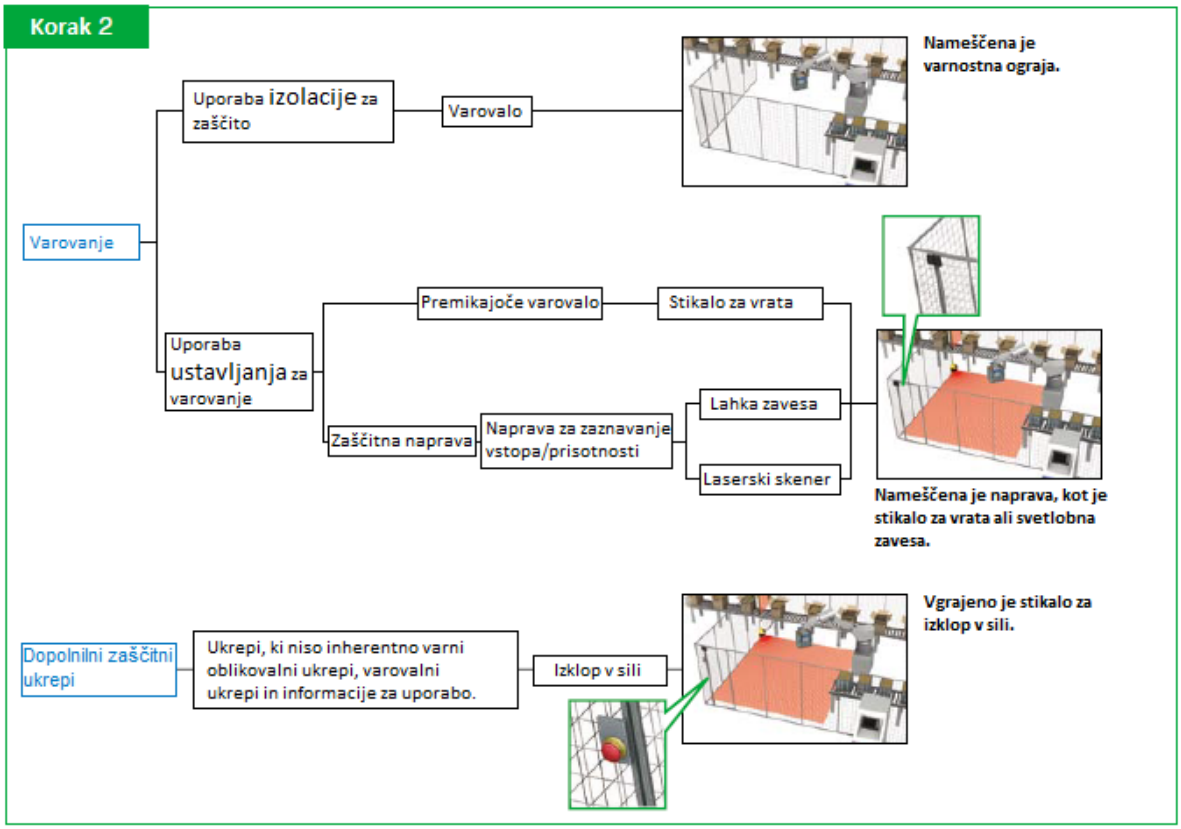
Slika 3.4 Inherentno varna zasnova [11]

V zvezi s tem osnovno pravilo za konstrukcijo strojev določa, da morajo biti ob dostopu vsi dostopni deli stroja brez ostrih robov, vogalov, grobih površin, štrlečih delov itd. Te je mogoče odpraviti z izbiro pravilnih oblik in uporabo pravilne razporeditve mehanskih delov [11].

Dopolnilni zaščitni ukrepi

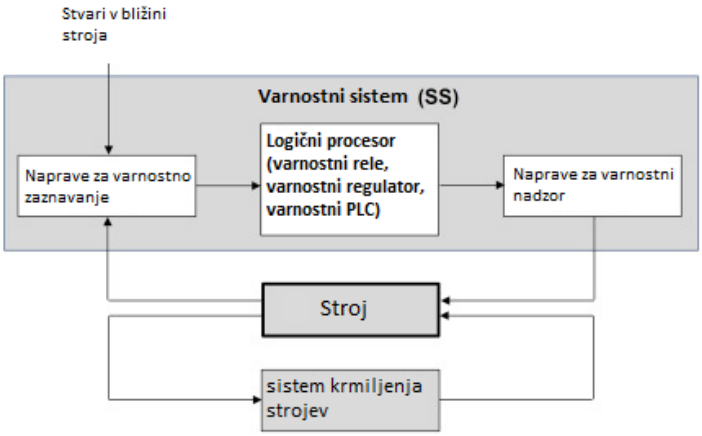
Varovanja in izvajanja dopolnilnih zaščitnih ukrepov se poslužujemo takrat, ko z uporabo inherentno varnega pristopa nevarnosti ni mogoče odpraviti [12].

Zaščitni ukrepi so običajno razdeljeni v dve skupini: varovanje z uporabo izolacije in uporabo ustavljanja. Med prvimi se najpogosteje uporabljajo varovala, kot je zaščitna ograja. Med ukrepe varovanja z ustavljanjem pa sodijo lahke zavese ali laserski skenerji. Dodatni zaščitni ukrepi (npr. stikala za izklop v sili) so ukrepi, ki so potrebni za varovanje zaradi predvidene uporabe in razumno predvidljive napačne uporabe stroja. Ne sodijo med inherentno varne konstrukcijske ukrepe, zaščito ali informacije za uporabo [11].



Slika 3.5 Zaščitni ukrepi [11]

Če je potreben občasen ali pogost dostop do stroja, se uporabljajo varnostni sistemi (SS). Ti skrbijo, da naključne napake na strojni opremi, sistematične napake pri načrtovanju ali človeške napake ne povzročijo okvare varnostnih funkcij, s potencialno posledico poškodbe ljudi, nevarnosti za okolje, izgube opreme ali proizvodnje [12].



Slika 3.6 Varnostni sistem (SS) [12]

V nasprotju s proizvodnim sistemom, ki je osredotočen na delovanje samo, se SS na zaščito osredotoča na naslednje načine:

- Spremljanje in nadzorovanje pogojev obratovanja stroja, ki so nevarni sami po sebi.
- Delovanje, ki je neodvisno in vzporedno s sistemom krmiljenja stroja.
- Delo s SS (samostojni rele, modularni rele, varnostni krmilnik ali varnostni PLC) za logično obdelavo.
- Izvajanje ene ali več varnostnih zank za vsako nevarnost, ki spremlja in nadzira njeno oskrbo z energijo, kot je določeno v oceni tveganja [12].

SS sestavljajo tehnične zaščitne naprave (zaznavanje, logični procesor in nadzor), ki zagotavljajo varnost in produktivnost hkrati. Značilna področja, kjer so potrebne tehnične zaščitne naprave, so:

- blokiranje/zaklepanje fizičnih varoval,
- zaščita dostopa,
- zaščita pred nevarnimi območji,
- nevarna zaščita točk,
- varno spremljanje položaja,
- varni ukazi itd.

Tipične varnostne zaznavne naprave so:

- varnostna stikala za zaznavanje položaja, kot so premična varovala, varni ukazi za stroje itd.,
- zapore, ki preprečujejo odpiranje varovala,
- varnostna svetlobna zavesa za zaščito dostopa ali nevarne točke,
- varnostni laserski skener za zaščito pred nevarnimi območji.

Varnostna zaznavna naprava zazna spremembe fizičnih pogojev in jih sporoči procesorju varnostne logike za nadaljnjo obdelavo [12].

Slika 3.7 Dodatna varnostna oprema [31]

Tipični varnostni logični procesorji so:

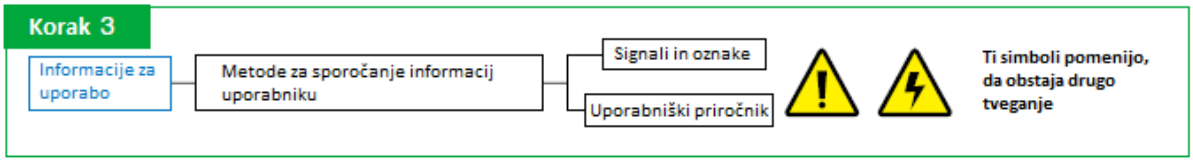
- varnostni releji,
- varnostni krmilniki,
- varnostni PLC itd.

Ti nadzorujejo signale iz varnostno zaznavnih naprav, jih obdelujejo z vnaprej vgrajeno logiko in vozijo varnostne krmilne naprave za krmiljenje stroja ali njegovo varno vzpostavitev, če je to potrebno [5].

Tipične varnostne krmilne naprave so kontaktorji, zaganjalniki, pogoni itd. To so pravzaprav aktuatorji, ki izvajajo končne ukaze, katere varnostni logični procesorji izdajo stroju [28].

Informacije za uporabo

Zadnji korak je zagotavljanje informacij za uporabo. Gre za končno metodo, ki se jo uporabi, kadar tveganja ni mogoče odpraviti ali zmanjšati z varnostno oblikovanimi ukrepi ter zaščitnimi in dopolnilnimi zaščitnimi ukrepi, opisanimi zgoraj [11].



Slika 3.8 Informacije za uporabo [11]

Priprava informacij za uporabo je sestavni del konstrukcije stroja. Informacije za uporabo so sestavljene iz komunikacijskih povezav, kot so besedila, besede, znaki, signali, simboli ali diagrami, ki se uporabljajo ločeno ali v kombinaciji za posredovanje informacij uporabniku [11].

Uporabniku je potrebno zagotoviti informacije o predvideni uporabi stroja, pri čemer je potrebno upoštevati vse njegove načine delovanja. Vsebovati morajo vsa navodila, potrebna za varno in pravilno uporabo stroja, uporabnika tudi obveščajo in ga opozarjajo na preostalo tveganje. Informacije morajo vsebovati:

- podatek, ali je potrebno usposabljanje,
- podatek, ali je potrebna osebna zaščitna oprema,
- podatek o morebitni potrebi po dodatnih varovalih ali zaščitnih napravah.

Vizualni signali (npr. utripajoče luči) in zvočni signali (npr. sirene) se lahko uporabijo za opozarjanje na bližajoči se nevarni dogodek, kot je zagon stroja ali prekoračitev hitrosti. Opozorilne naprave morajo biti zasnovane in nameščene tako, da je preverjanje enostavno. Informacije za uporabo predpisujejo redno preverjanje opozorilnih naprav [28].

4 FUNKCIONALNA VARNOST

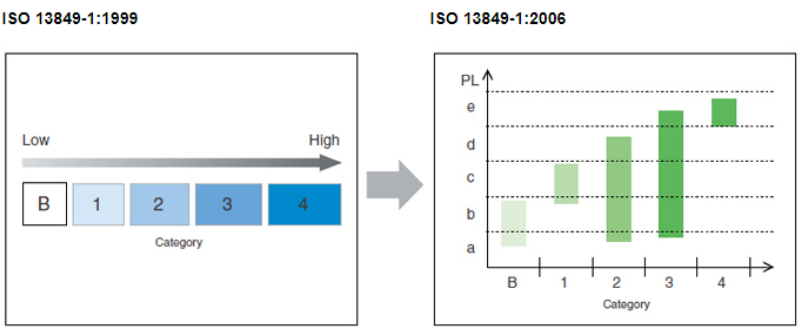
Kot del celotne strategije zmanjšanja tveganja na stroju se je pogosto treba zateči k uporabi zaščitnih ukrepov, ki uporabljajo eno ali več varnostnih funkcij.

Leta 1996 je CEN objavil pomemben standard za proizvajalce strojev – EN 954-1, »Varnost strojev – Varnostni deli nadzornih sistemov – 1. del: Splošna načela za načrtovanje.« [29] Ta standard je postavil izhodišče za določitev zanesljivosti nadzora v sistemih za varovanje strojev in uvedel kategorije zanesljivosti, ki so postale vseprisotne [11].

Mednarodni standard za »Varnost strojev – Varnostni deli nadzornih sistemov ISO 13849-1« je bil leta 2006 revidiran. Podlaga za revizijo so bili polprevodniški deli, kot so tranzistorji in MOS-FET. Ti so se uporabljali v delih stroja za skrb varnostnih delov nadzornih sistemov in so predstavljali spremembo kontrolnih metod, kar pomeni, da je bil mogoč tudi nadzor s pomočjo programske opreme.

Po konvencionalnem načinu razmišljanja o kategorijah je bila varnost določena po sistemskih strukturah. Uporabljale so se predvsem mehanske varnostne naprave in releji, ki niso omogočali zadostne varnosti v smislu zanesljivosti delov. V teh okoliščinah so bili primorani urediti mehansko varnost glede na funkcije in zanesljivost [31].

Ta način razmišljanja se imenuje »**Funkcionalna varnost**«. Funkcionalna varnost je tako več kot le verjetnost, da varnostni sistem ne bo deloval, kadar se to od njega pričakuje [11].



Slika 4.1 Razvoj standarda ISO 13849 od leta 1999 do 2006 [11]

4.1 Varnostni deli nadzornega sistema – SRP/CS

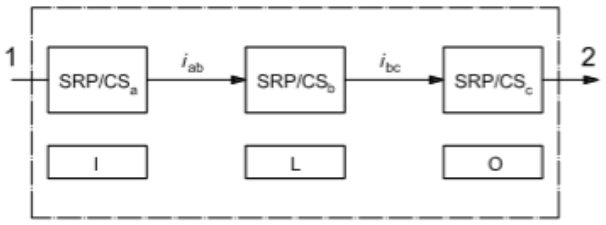
Deli krmilja, ki skrbijo za zagotavljanje varnostnih funkcij, se imenujejo varnostni deli nadzornega sistema (SRP/CS) in so lahko sestavljeni iz strojne in/ali programske opreme, lahko pa so tudi ločeni od krmilnega sistema stroja. SRP/CS zagotavljajo varnostne funkcije pri PL, ki dosegajo zahtevano zmanjšanje tveganja. Združeni varnostni deli nadzornega sistema se začnejo na točki, kjer se sprožijo vhodni signali, povezani z varnostjo, in končajo na izhodu [29].

Oblikovanje SRP/CS

Varnostno funkcijo lahko izvaja en ali več SRP/CS in več varnostnih funkcij lahko deli en ali več SRP/CS. Možno je tudi, da en SRP/CS izvaja varnostne funkcije in standardne nadzorne funkcije [29].

Tipična predstavitev varnostne funkcije je prikazana na sliki 4.2. Na njej lahko vidimo kombinacijo varnostnih delov kontrolnih sistemov (SRP/CS) za:

- vhod (SRP/CS_a),
- logiko/obdelavo (SRP/CS_b),
- elemente za nadzor izhoda/moči (SRP/CS_c) in
- medsebojno povezovalno sredstvo (i_{ab}, i_{bc}) (npr. električno, optično).



Slika 4.2 Shema SRP/CS [29]

4.2 Specifikacija varnostnih zahtev

Specifikacija varnostnih zahtev se zdi precej težka, vendar je dejansko treba zagotoviti samo veliko informacij, ki so potrebne za analizo in oblikovanje varnostnih sistemov.

Varnostne funkcije vključujejo vse funkcije stroja, ki imajo neposreden zaščitni učinek za delavca, ki stroj uporablja. Vendar pa lahko s to opredelitvijo ignoriramo nekatere pomembne funkcije. Dopolnilni zaščitni ukrepi, kot je ustavitev v sili, se lahko izpustijo, saj se v večini primerov poškodba zgodi pred pritiskom na E-STOP in tako ne moremo reči, da ima »neposreden zaščitni učinek.« [31]

Med pregledom opredelitev lahko najdemo:

> *»Varnostne funkcije: Delovanje stroja, katerega okvara lahko povzroči takojšnje povečanje tveganja.«* [28]

Glede na oceno tveganja je vsako nadzorovano tveganje, ki delavce ščiti pred vplivi delovanja stroja z uporabo nadzornih funkcij, varnostna funkcija. Te funkcije so lahko tudi funkcije za nadzor procesov, toda možnost za takojšnje povečanje tveganja zaradi okvare je tisto, zaradi česar so te funkcije varnostne funkcije.

Tabela prikazuje nekaj primerov različnih vrst varnostnih funkcij, ki jih lahko najdemo na strojih. Obstaja sicer veliko več varnostnih funkcij od navedenih v tabeli. Naša naloga je zgolj, da ugotovimo, katere potrebujemo na stroju.

Predmet	**Opis**
Identifikacija varnostnih funkcij	Ime ali druga referenca "blokada dostopa do vrat" ali "nevarno območje 2"
Funkcionalne značilnosti	- Predvidena uporaba ali predvidena napačna uporaba stroja, ki ustreza varnostni funkciji - Načini delovanja, pomembni za varnostno funkcijo - Čas cikla stroja - Odzivni čas varnostne funkcije
Nujna varnostna operacija	Je to funkcija v sili? Če je odgovor "DA", katere vrste nujnih primerov bi lahko zmanjšala ta funkcija?
Interakcije	Kateri načini delovanja zahtevajo, da ta funkcija deluje? Ali obstajajo načini, pri katerih ta funkcija zahteva namerni "bypass"? Sem lahko spadajo običajni načini delovanja (avtomatski, ročni, ...)
Vedenje	Kako se sistem obnaša ob sprožitvi varnostne funkcije, se moč takoj odstrani s funkcijo zaustavitve kategorije 0 in gibi robota se ustavijo s funkcijo zaustavitve kategorije 1 s pomočjo vhoda robota za varnost. Ali Vsi vodoravni pnevmatski gibi se ustavijo v trenutnih položajih. Navpični gibi se vrnejo v dvignjene ali uvlečene položaje.
...	...

Tabela 4.1 Tabela primerov različnih vrst varnostnih funkcij [29]

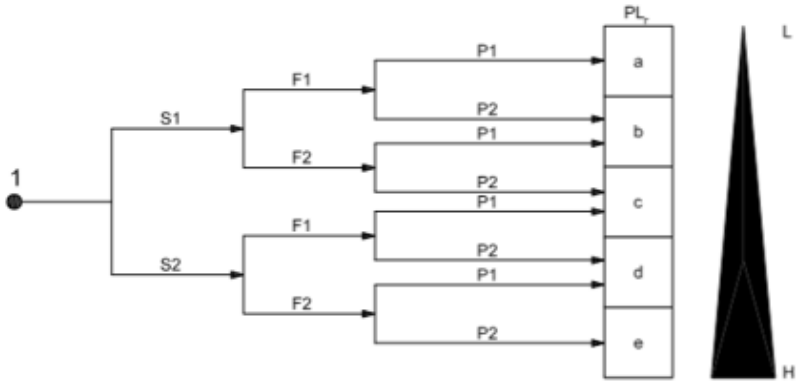
4.3 Zahtevana raven zmogljivosti (PL_r)

Za vsako izbrano varnostno funkcijo, ki jo izvede SRP/CS, se določi zahtevana raven zmogljivosti (PL_r). Določitev zahtevane ravni učinkovitosti je rezultat ocene tveganja in se nanaša na znesek zmanjšanja tveganja, ki ga izvedejo varnostni deli nadzornega sistema [31].

Pri določanju PL_r predvidene varnostne funkcije se lahko upošteva zmanjšanje tveganja z drugimi tehničnimi ukrepi, neodvisnimi od nadzornega sistema ali dodatnih varnostnih funkcij.

Resnost poškodbe »S« je relativno enostavno oceniti. Za pogostost pojavljanja se uporabijo pomožni parametri za izboljšanje ocene. Ti parametri so:

- pogostost in čas izpostavljenosti nevarnosti (F) in
- možnost izogibanja nevarnosti ali omejevanja škode (P).



Legenda:

1 Izhodišče za oceno prispevka varnostnih funkcij k zmanjšanju tveganja
L Nizek prispevek k zmanjšanju tveganja
H Velik prispevek k zmanjšanju tveganja
PLr Zahtevana raven učinkovitosti

Parametri tveganja:

S Varnost poškodbe
S1 Rahlo (običajno reverzibilna poškodba)
S2 Resno (običajno nepopravljiva poškodba)
F Pogostost in/ali izpostavljenost nevarnosti
F1 Redko do manj pogosto in/ali čas izpostavljenosti je kratek
F2 Redko do neprekinjeno in/ali čas izpostavljenosti je dolg
P Možnost preprečevanja nevarnosti ali omejitev škode
P1 Možno pod posebnimi pogoji
P2 Komaj mogoče

Slika 4.3 Specifikacija zahtevane ravni učinkovitosti [29]

Večji je znesek zmanjšanja tveganja, ki ga zahteva SRP/CS, višji je PL_r.

Resnost poškodbe S1 in S2

Pri oceni tveganja, ki izhaja iz okvare varnostne funkcije, se upoštevajo le manjše poškodbe, hude poškodbe in smrt.

Frekvenca in/ali čas izpostavljenosti nevarnosti, F1 in F2

Splošno veljavnega časovnega obdobja, ki se izbere za parameter F1 ali F2, ni mogoče določiti.

F2 je potrebno izbrati, če je oseba pogosto ali stalno izpostavljena nevarnosti. Frekvenčni parameter je treba izbrati glede na pogostost in trajanje dostopa do nevarnosti. Obdobje izpostavljenosti nevarnosti je treba ovrednotiti na podlagi povprečne vrednosti, ki jo lahko vidimo glede na celotno časovno obdobje, v katerem se oprema uporablja. Če je dostop potreben le občasno, je potrebno izbrati F1 [29].

Možnost izogibanja nevarnosti P1 in P2

Pomembno je vedeti, ali je nevarno situacijo mogoče prepoznati in se ji izogniti, preden pride do nesreče.

Kadar pride do nevarne situacije, je potrebno izbrati P1, če obstaja realna možnost izognitve nesreči ali znatno zmanjšanje njenega učinka. Če ni skoraj nobene možnosti za izognitev nevarnosti, je potrebno izbrati P2 [29].

4.4 Raven učinkovitosti – PL

Raven učinkovitosti (PL) je bila uvedena v standardu ISO 13849 in je izražena kot zanesljivost varnostnih delov nadzornega sistema, vključno z diagnostičnim pokritjem ali stopnjo napak [11].

Na tej točki je znana ocena tveganja in dodeljena zahtevana raven zmogljivosti za vsako varnostno funkcijo. Nadalje je treba razmisliti o treh vidikih zasnove sistema:

- arhitekturna kategorija,
- srednji čas do nevarne okvare ($MTTF_d$) in
- diagnostična pokritost (DC_{avg}).

PL je vrednost, ki se uporablja za določanje zmožnosti varnostnih delov nadzornih sistemov za izvajanje varnostne funkcije v predvidljivih pogojih. Po drugi strani pa se za doseganje zahtevanega zmanjšanja tveganja za vsako varnostno funkcijo uporablja PL_r. Zato mora biti PL varnostnih delov nadzornega sistema enaka ali višja od PL_r [29].

V standardu ISO 13849 so ravni zmogljivosti opredeljene v smislu verjetnosti nevarne okvare na uro PFH_d. Določenih je pet stopenj učinkovitosti, z določenimi razponi verjetnosti nevarne napake na uro.

PL (Raven učinkovitosti)	**povprečna verjetnost nevarne okvare na uro [1/h]**
a	$\geq 10^{-5}\ do\ > 10^{-4}$
b	$\geq 3\ \times 10^{-6}\ do\ > 10^{-5}$
c	$\geq 10^{-6}\ do\ > 3\ \times 10^{-6}$
d	$\geq 10^{-7}\ do\ > 10^{-6}$
e	$\geq 10^{-8}\ do\ > 10^{-7}$

Tabela 4.2 Ravni učinkovitosti v odvisnosti od povprečne verjetnosti nevarne okvare na uro PFH_d [29]

Verjetnost nevarnega izpada varnostne funkcije je odvisna od več dejavnikov, vključno:

- s strojno in programsko strukturo,
- z obsegom mehanizmov za odkrivanje napak – diagnostično pokritje (DC),
- z zanesljivostjo komponent – povprečen čas do nevarne odpovedi ($MTTF_d$),
- z odpovedjo skupnega vzroka (CCF),
- z obratovalno napetostjo,
- z okoliškimi pogoji in
- s postopki delovanja.

Ti vidiki se lahko združijo v dva pristopa v zvezi s postopkom ocenjevanja:

a) merljivi vidiki (vrednost $MTTF_d$ za posamezne komponente, DC, CCF, struktura);
b) količinsko neopredeljivi, kvalitativni vidiki, ki vplivajo na obnašanje SRP/CS.

Med merljivimi vidiki se lahko prispevek zanesljivosti (npr. $MTTF_d$, struktura) spreminja glede na uporabljeno tehnologijo. Na primer, v določenih mejah je za en sam kanal varnostnih delov visoke zanesljivosti v eni tehnologiji možno, da se zagotovi enaka ali višja vrednost PL kot na napake odporna struktura nižje zanesljivosti v drugi tehnologiji [31].

V standardih v skladu z IEC 61508 je sposobnost varnostnih kontrolnih sistemov za izvajanje varnostne funkcije podana preko stopnje varnosti (SIL). Tabela 4.3 prikazuje razmerje med dvema konceptoma PL in SIL.

PL nima ustreznosti na lestvici SIL in se v glavnem uporablja za zmanjšanje tveganja rahle, običajno reverzibilne poškodbe. Ker je SIL 4 namenjen katastrofalnim dogodkom, ki so možni v procesni industriji, ta obseg ni pomemben za tveganja na strojih. Tako je PL, ki ustreza SIL 3, opredeljena kot najvišja raven [29].

PL (Raven učinkovitosti)	**SIL (stopnja varnostne celovitosti)**
a	nobene korespondence
b	1
c	1
d	2
e	3

Tabela 4.3 Povezava med PL in SIL [29]

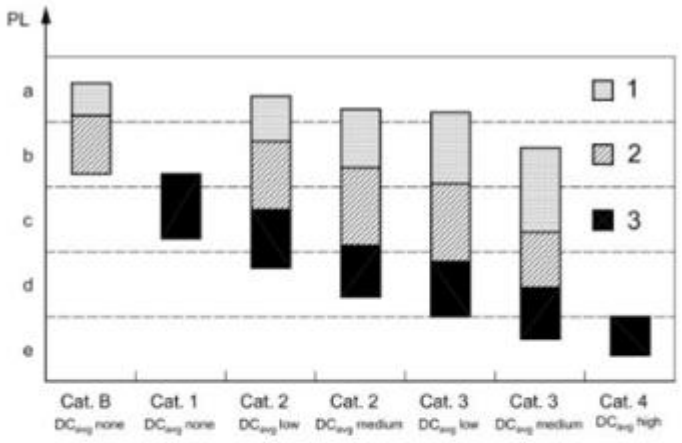
Za zmanjšanje tveganja se zato uporabita predvsem naslednja zaščitna ukrepa:

- Treba je zmanjšati verjetnost napak na nivoju komponent. Cilj je zmanjšati verjetnost okvar, ki vplivajo na varnostno funkcijo. To je mogoče doseči s povečanjem zanesljivosti komponent (npr. z izbiro dobro preizkušenih komponent in/ali z uporabo preizkušenih varnostnih načel, da bi zmanjšali ali izključili kritične napake ali okvare).
- Treba je izboljšati strukturo SRP/CS. Cilj je izogniti se nevarnemu učinku napake.

Oba ukrepa se lahko uporabita ločeno ali v kombinaciji. Pri nekaterih tehnologijah je zmanjšanje tveganja mogoče doseči z izbiro zanesljivih komponent. Z drugimi tehnologijami pa se lahko zmanjša tveganje preko redundantnega nadzorovanega sistema. Poleg tega je treba upoštevati tudi CCF [31].

Za doseganje določene ravni učinkovitosti je treba upoštevati, da nekateri vidiki zasnove dosežejo določeno raven učinkovitosti ali da predvidevajo stopnjo napake v smislu PFH_d.

Ker kategorije ne morejo doseči enake zanesljivosti, so PL in kategorije povezani, kot je prikazano na sliki 4.4. Ta diagram povzema povezavo treh osrednjih parametrov v standardu ISO 13849-1 v eni sliki.



Legeda

PL	Raven uspešnosti
1	MTTFd vsakega kanala = nizka
2	MTTFD vsakega kanala = medij
3	MTTFD vsakega kanala = visok

Slika 4.4 Povezava med DC, $MTTF_d$ vsakega kanala in PL [29]

Začenši s PL_r iz specifikacije varnostnih zahtev za prvo varnostno funkcijo, lahko s pomočjo slike 4.4 izberemo kategorijo in druge parametre, potrebne za načrtovanje.

Recimo, da ocena tveganja kaže, da je za sistem potrebna zaustavitev v sili. ISO 13850 zahteva, da funkcija za zaustavitev v sili zagotavlja minimalno PL_c. Glede na zgornjo sliko izberemo za osnovo navpično os. Vidimo lahko, da je PL_c mogoče doseči z uporabo arhitekture kategorije 1, 2 ali 3, od katerih ima vsaka ustrezne razlike v $MTTF_d$ in DC_{avg}. Na primer:

- kategorija 1, $MTTF_d$ = visoko in DC_{avg} = nič ali
- kategorija 2, $MTTF_d$ = srednja do visoka in DC_{avg} = nizka do srednja ali
- kategorija 3, $MTTF_d$ = nizka do visoka in DC_{avg} = nizka do srednja.

Opazimo lahko, da se $MTTF_d$ v kanalih zmanjša, ko se DC poveča. Oblika kompenzira nižjo zanesljivost komponent s povečanjem diagnostične pokritosti in dodajanjem redundance.

Razlika med kategorijama 3 in 4 je predvsem v povečanem DC. Medtem ko je kategorija 3 odporna na eno napako, ima kategorija 4 dodatne diagnostične zmogljivosti. Kar pomeni, da dodatne napake ne morejo povzročiti izgube varnostne funkcije. To seveda ni isto kot večkratna toleranca napak, saj je sistem še vedno zasnovan tako, da deluje le ob eni sami napaki.

Na tem mestu je potrebno omeniti, da ISO 13840 prepozna strukture samo z enokanalnimi in dvokanalnimi konfiguracijami.

Ko je zahtevan PL znan, je naslednji korak izbira arhitekturne kategorije.

4.5 Povprečen čas do nevarnega izpada vsakega kanala ($MTTF_d$)

Razumevanje srednjega časa do nevarne okvare ($MTTF_d$) je za funkcionalno varnost kritično. $MTTF_d$ torej pomeni povprečen čas do nevarne odpovedi, kar lahko z drugimi besedami opišemo tudi s pričakovanjem povprečnega časa do nevarne odpovedi oz. nevarnosti za osebje, okolje ali opremo. Nevarna odpoved je v tem primeru okvara, ki lahko povzroči, da je SRP/CS v nevarnem stanju ali stanju napake [16].

Vsaka komponenta lahko in sčasoma tudi bo odpovedala, vendar vemo, da ima vsaka izmed njih svojo stopnjo odpovedljivosti, saj je vsaka komponenta dizajnirana za svoj čas delovanja. Ta je lahko zelo kratek in komponenta lahko odpove že pri prvem vklopu ali pa je zelo dolg, včasih tudi na stotine let. Ne smemo pozabiti, da je to nekaj, kar se zgodi skozi čas. Pomembno je tudi, da je jasno, da govorimo o odpovedih in ne o napakah [17].

Na strojih, na katerih imamo več kot zgolj releje, ventile ali varnostni sisteme, imamo populacijo komponent, od katerih bo vsaka sčasoma odpovedala. Te odpovedi lahko seštejemo, jih povežemo in grafično prikažemo v obliki okvar v populaciji skozi čas.

Nekatere okvare bodo privedle do »varnega« stanja, npr. releji, pri katerih so vsi poli odprti, nekateri pa bodo odpovedali v potencialno »nevarnem« stanju, kot npr. normalno zaprt ventil, ki ima pomembno puščanje.

$MTTF_d$ je čas, izražen v letih, ko je verjetnost okvare relativno stalna. V spodnjem grafu je prikazana tipična krivulja stopnje napake, ki se imenuje »krivulja kopalne kadi«. $MTTF_d$ v grafu predstavlja ploskovni del krivulje. Za desni del krivulje se domneva, da je vključen v obratovalni čas [17].

Standard ISO 13849-1 pri tem predvideva čas poslanstva za vse stroje 20 let.

Slika 4.5 Krivulja kopalne kadi [17]

$MTTF_d$ vsakega kanala je podan v treh ravneh in se upošteva za vsak kanal posamično. ISO 13849 opredeljuje tri ravni $MTTF_d$, navedene meje v Tabeli 4.4 pa se predpostavljajo s točnostjo 5 %. Po $MTTF_d$ se lahko upošteva največja vrednost 100 let [17].

Oznaka vsakega kanala	Razpon vsakega kanala
Mala	3 Leta ≤ MTTFd < 10 Let
Srednja	10 Let ≤ MTTFd < 30 Let
Velika	30 Let ≤ MTTFd ≤ 100 Let

Tabela 4.4 Srednji čas do nevarne odpovedi vsakega kanala ($MTTF_d$) [29]

Za oceno $MTTF_d$ komponente se uporablja hierarhični postopek za iskanje podatkov v danem vrstnem redu:

a) uporaba podatkov proizvajalca,
b) uporaba raznih metod po ISO 13849,
c) izbira 10 let – deset let je namreč polovica predvidene življenjske dobe misije 20 let.

Pri standardu ISO 13840 lahko najdemo metodo »dobre inženirske prakse« za oceno $MTTF_d$, pri čemer se domneva, da proizvajalec ne zagotovi teh informacij. ISO 13849-2 ima tako nekaj referenčnih tabel, ki zagotavljajo nekatere splošne $MTTF_d$ vrednosti za nekatere vrste komponent. Deli, ki niso navedeni, pa se lahko izračunajo za pnevmatske, mehanske in elektromehanske komponente [17].

Preden preračunamo $MTTF_d$ za komponento, predstavimo nekaj spremenljivk.

B_{10D} – Število ciklov, dokler ne odpove 10 % komponent

T_{10D} – Povprečen čas, dokler ne odpove 10 % komponent

n_{op} – Povprečen čas delovanja [h/d]

d_{op} – Povprečen čas delovanja [d/y]

t_{cycle} – Povprečen čas delovanja med začetkom dveh zaporednih ciklov komponente [s/cikel]

Če poznamo nekaj podrobnosti, lahko izračunamo $MTTF_d$ z uporabo enačbe (4.1):

$$MTTF_d = \frac{B_{10D}}{0{,}1 \times n_{op}} \tag{4.1}$$

Za uporabo te enačbe, moramo najprej izračunati n_{op} z uporabo enačbe (4.2):

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \frac{s}{h}}{t_{cycle}} \tag{4.2}$$

Morda bomo potrebovali še en izračun, podan z enačbo (4.3):

$$T_{10D} = \frac{B_{10D}}{n_{op}} \tag{4.3}$$

4.6 Diagnostična pokritost (DC)

Razumevanje diagnostične pokritosti (DC), kot se uporablja v standardu ISO 13849-1, je ključnega pomena za analizo zasnove katerekoli varnostne funkcije, ocenjene z uporabo tega standarda.

Tri standardne arhitekture vključujejo avtomatske diagnostične funkcije, ki so kategorije 2, 3 in 4. Ko se sistemu dodeli diagnostiko, je potrebno vedeti, katere napake lahko diagnostika odkrije in koliko od teh jih je lahko nevarnih glede na skupno število odpovedi [18].

DC predstavlja razmerje med nevarnimi odpovedmi, ki jih je mogoče zaznati s skupnimi nevarnimi napakami, izraženimi v odstotkih. Pri tem lahko pride tudi do raznih nenevarnih odpovedi, ki pa so iz DC izključene, saj ni potrebno skrbeti zanje. Če se pojavijo, sistem ne bo padel v nevarno stanje [29].

Za izračun DC so potrebni določeni podatki, kar velja tudi za stopnje napak. ISO 13849-1 vsebuje nekaj tabel, ki navajajo nekatere najpogostejše vrste komponent in z njimi povezane stopnje napak. Posebno pozorni moramo biti nad viri podatkov o stopnji odpovedi, saj se pogoji, pod katerimi so podatki resnični, ne ujemajo popolnoma s podatki v standardu ISO 13849. Obstaja nekaj virov podatkov o stopnji odpovedi, npr. MIL-HDBK-217 (Vojaški priročnik za »Napoved zanesljivosti elektronske opreme«) . V vsakem primeru se priporoča uporabiti samo en vir za podatke o stopnji napak [18].

Spremenljivke, povezane s stopnjami napak, so [33]:

- $\boldsymbol{\lambda_d}$ – »nevarna« odpoved
- $\boldsymbol{\lambda_{dd}}$ – zaznane »nevarne« odpovedi
- $\boldsymbol{\lambda_{du}}$ – nezaznane »nevarne« odpovedi

Za razumevanje teh spremenljivk je potrebna njihova odvisnost, podana z enačbo (4.4):

$$\lambda_d = \lambda_{dd} + \lambda_{du} \tag{4.4}$$

Na podlagi te odvisnosti se lahko diagnostična pokritost izrazi kot odstotek:

$$DC\% = \frac{\lambda_{dd}}{\lambda_d} \times 100 \tag{4.5}$$

Za dejanski izračun DC (%) je v večini primerov mogoče uporabiti celoten postopek, podrobno predstavljen v standardu IEC 61508-2, ki precej natančno obravnava, kako določiti stopnjo napak in kako izračunati »frakcijo varne napake«. Lahko se uporabi tudi tabela v prilogi E standarda ISO 13489-1 za oceno DC (%), v kateri so podane informacije, kako uporabiti normativni del standarda [18].

Ko se določi DC za varnostno funkcijo, se mora ta primerjati z vrednostjo DC iz tabele 4.5. Pri tem ugotovimo, ali je DC dovolj za PL_r, ki se ga poskuša doseči. Tabela 4.5 uvršča rezultate DC v štiri razpone.

Oznaka	Razpon
Noben	DC < 60%
Mala	60% ≤ DC < 90%
Srednja	90% ≤ DC < 99%
Velika	69% ≤ DC

Tabela 4.5 Diagnostična pokritost (DC) [29]

Če je vrednost DC dovolj visoka za želeni PL_r, je delo s tem končano, v nasprotnem primeru pa bi se na sistem morale dodati dodatne diagnostične funkcije, s katerimi bi lahko dosegli večjo pokritost.

Več varnostnih funkcij

V večini primerov sestavlja celoten varnostni sistem več varnostnih funkcij. Pri tem je treba povprečne vrednosti DC določiti tako, da se določi DC za celoten sistem, kar je izraženo v enačbi (4.6) [18].

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \tag{4.6}$$

4.7 Okvara skupnega vzroka (CCF)

Obstajata dva podobno zveneča izraza, ki se pogosto zamenjujeta: skupna odpoved vzroka (CCF) in odpoved skupnega načina [29]. Omenjeni vrsti okvar sta sicer podobni, a sta vseeno različni. Skupni vzrok napake je napaka v sistemu, ko dva ali več delov sistema hkrati odpovejo iz enega samega skupnega vzroka. Pogost vzrok sta dva različna načina odpovedi v dveh različnih komponentah, vendar z enim samim skupnim vzrokom [34].

Skupni način napake se pojavi takrat, kadar dve komponenti ali deli sistema hkrati odpovejo na enak način. Napake lahko povzročijo isti ali različni vzroki, vendar je način odpovedi komponent enak.

Okvara skupnega vzroka vključuje napako skupnega načina, saj lahko skupni vzrok povzroči skupni način okvare v enakih komponentah, ki se uporabljajo v sistemu.

Obstajajo tri vrste napak glede na izvor:

- naključne,
- sistematične in
- okvare skupnega vzroka.

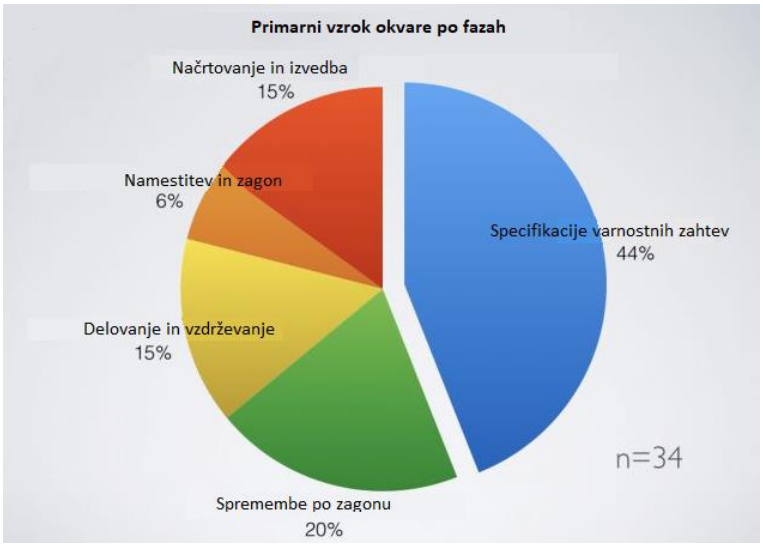
Naključne napake ne sledijo nobenemu vzorcu. Pojavljajo se naključno v nekem časovnem obdobju, pogosto zaradi izrabljenosti ali proizvodnih napak komponente. Naključne napake se lahko povečajo zaradi okoljskih ali procesnih dejavnikov, kot so korozija, obraba in druge preobremenitve komponent oz. podsistemov. Naključne napake se pogosto ublažijo z izbiro visoko zanesljivih komponent.

Sistematične napake vključujejo napake skupnih vzrokov in se pojavijo predvsem zaradi napačnih pristopov oz. postopkov. Nastanejo zaradi napak pri načrtovanju, specifikaciji, delovanju, vzdrževanju in namestitvi. Zmanjšamo ali odpravimo jih lahko z raznimi sistemi ali uporabo postopkov zagotavljanja kakovosti, ki služijo za preverjanje delovanja sistema. Sistematične napake so naključne in kompleksne, zato jih je težko statistično analizirati. Prav

tako so pomemben vir napak skupnih vzrokov, saj lahko vplivajo na redundantne komponente in so pogosto deterministične.

Redundanca se običajno uporablja za ublažitev sistemskih napak, saj povzročajo razlike v sestavi komponent ali podsistemov brez prekrivanja sistematičnih napak, kar zmanjšuje verjetnost okvare skupnega vzroka pri ustvarjanju okvar skupnega načina [34].

Slika 4.6 prikazuje rezultate študije, ki jo je leta 1994 izvedla HSE – Britanska agencija za zdravje in varnost, ki podpira idejo, da imajo sistematične okvare pomemben doprinos k okvaram v varnostnem sistemu. Študija je vključevala 34 sistemov (n = 34), zato graf morda ni najbolj prepričljiv, a je iz njega moč razbrati nekaj presenetljivih rezultatov [34].



Slika 4.6 Rezultat študije HSE glede sistematičnih okvar [34]

Kot lahko opazimo, so napake v specifikaciji varnostnih zahtev povzročile kar približno 44 % napak sistema. Na podlagi tega majhnega vzorca se zdi, da so sistematične napake pomemben vir okvar.

Ravnanje s CCF v standardu

ISO 13849-1 je namenjen poenostavljenemu standardu funkcionalne varnosti, zatorej je analiza CCF omenjena v prilogi. Pri tem je treba upoštevati, da je priloga v standardu informativna, kar pomeni, da je to samo pripomoček za uporabo standarda. Za ocenjevanje CCF se lahko uporabi IEC 61508 [34].

Št.	Ocenjevanje proti CCF	Rezultat
1	**Ločitev / Segregacija**	
	Fizična ločitev med signalnimi potmi, na primer: - ločitev pri ožičenju / cevovodih; - z dinamičnim preskusom zaznavanje kratkih stikov in odprtih vezij v kablih; - ločeno zaščito za signalno pot vsakega kanala; - Na ploščah s tiskanimi vezji zadostni odmiki in razdalja lezenja.	**15**
2	**Raznolikost**	
	uporabljajo se različne tehnologije / zasnovo ali fizikalna načela, na primer: - prvokanalni elektronski ali programirljivi elektronik in drugokanalni elektromehanski trdi kabel - različen začetek varnostne funkcije za vsak kanal (npr. položaj, tlak, temperatura), in / ali digitalno in analogno merjenje spremenljivk (npr. razdalja, tlak ali temperatura) in / ali Sestavni deli različnih izdelkov.	**20**
…		

Tabela 4.6 Postopek ocenjevanja in količinsko določanje ukrepov proti CCF [29]

V tabeli 4.6 je sicer navedenih šest skupnih ukrepov za ublažitev, med katerimi je treba doseči najmanj 65 točk od skupno 100. Zahtevan CCF mora izpolnjevati arhitekture kategorij 2, 3 in 4 za ustrezno uveljavitev PL [34].

4.8 Kategorija PL

Osnovne arhitekturne kategorije so bile prvotno uvedene v standardu EN 954-1: 1996. Nespremenjene so bile kasneje prenesene v prvo izdajo ISO 13849-1 v letu 1999, nakar so se v naslednjih izdajah ohranile in razširile. Gre za klasifikacijo varnostnih delov nadzornega sistema glede na njihovo odpornost na napake in njihovo poznejše obnašanje v stanju napake.

Najprej se moramo vprašati, kaj pomenijo kategorije.

To so arhitekture, ki se uporabljajo kot osnova za načrtovanje in analizo varnostnih funkcij. V preteklosti sta obstajali dve osnovni obliki: kategorije ANSI in različica CSA ter oblike CEN. Leta 1996 je CEN objavil pomemben standard za proizvajalce strojev – EN 954-1, »Varnost strojev – Varnostni deli nadzornih sistemov – 1. del: Splošna načela za načrtovanje«. Ta standard je postal izhodišče za določitev zanesljivosti nadzornega sistema za varovanje strojev in uvedel vseprisotne kategorije zanesljivosti [35].

Kategorije se uporabljajo za opis sistemskih arhitektur za varnostne nadzorne sisteme. Vsaka arhitektura prinaša vrsto zanesljivih zmogljivosti, ki jih je mogoče povezati s stopnjo zmanjšanja tveganja. Arhitekture se lahko uporabljajo tako za električne, elektronske, pnevmatske, hidravlične ali mehanske krmilne sisteme [35].

Kategorija B

Opredelitev kategorije B po standardu.

»SRP/CS morajo biti zasnovani, izdelani, izbrani, sestavljeni in kombinirani v skladu z ustreznimi standardi in z uporabo osnovnih varnostnih načel za specifično uporabo, ki jih je mogoče prenesti.

- *Pričakovane obratovalne napetosti, npr. zanesljivost v zvezi z zlomno zmogljivostjo in frekvenco,*
- *vpliv obdelanega materiala, npr. detergenti v pralnem stroju in*
- *druge pomembne zunanje vplive, npr. mehanske vibracije, elektromagnetne motnje, prekinitve napajanja ali motnje.*

V sistemih kategorije B ni diagnostičnega pokritja (DC_{avg} = nič), $MTTF_d$ vsakega kanala pa je lahko nizka do srednja. V takšnih strukturah (običajno enokanalnih sistemov) upoštevanje CCF ni pomembno.

Največja vrednost PL, ki jo je mogoče doseči s kategorijo B, je PL = b.« [29]

Standard nam omogoča tudi blokovne sheme. Blokovna shema za kategorijo B izgleda kot enokanalni sistem, prikazana je na sliki 4.7.

Legenda

i_m	sredstva za medsebojno povezovanje
I	vhodna naprava, npr. senzor
L	logika
O	izhodna naprava, npr. glavni kontaktor

Slika 4.7 Osnovna arhitektura kategorije B [29]

V blokovni shemi opazimo arhitekturo z enim kanalom, saj poteka od krmilnih vhodov do izhodov samo en kanal. Tudi varovalna zanka je en sam kanal. Napaka v katerikoli komponenti kanala lahko povzroči izgubo nadzora nad izhodom [35].

Za osnovna varnostna načela se moramo obrniti na standard, v katerem najdemo naslednje:

- uporaba primernih materialov in ustrezna proizvodnja,
- pravilno dimenzioniranje in oblikovanje,
- pravilna izbira, kombinacija, ureditev, montaža in montaža komponent/sistemov,
- uporaba načel takojšnjega odvzema napetosti,
- pravilno pritrjevanje,
- omejitev proizvodnje in/ali prenosa sile in podobnih parametrov,
- omejitev obsega okoljskih parametrov,
- omejitev hitrosti in podobni parametri,
- ustrezen odzivni čas,
- zaščita pred nepričakovanim zagonom,
- poenostavitev,
- ločevanje,
- pravilno mazanje,
- pravilno preprečevanje vdora tekočin in prahu [35].

Diagnostična pokritost

> *»V sistemih kategorije B ni diagnostične pokritosti (DC_{avg} = nič) …«* [29]

Sistemi kategorije B so v osnovi enokanalni. Ena napaka v sistemu bo povzročila izgubo varnostne funkcije. Ta stavek se nanaša na koncept »diagnostične pokritosti«, ki je bil uveden v standardu ISO 13849-1: 2007. V praksi to pomeni, da ni nadzora ali povratnih informacij od kritičnih elementov sistema.

Stopnje odpovedi komponent

> *»... $MTTF_d$ vsakega kanala je lahko nizka do srednja.«* [29]

Z vidika razumevanja kategorije B to pomeni, da v teh sistemih ni treba uporabljati komponent z visoko zanesljivostjo.

Pogosti vzroki napak

> *»V takšnih strukturah (običajno enokanalnih sistemov) upoštevanje CCF ni pomembno.«* [29]

Dovolj je omeniti, da se tehnike oblikovanja, kot tudi ločevanje kanalov, ki je nemogoče v enokanalni arhitekturi, in druge tehnike uporabljajo za zmanjšanje verjetnosti CCF v sistemih višje zanesljivosti.

Ravni učinkovitosti

> *»Največja vrednost PL, ki jo je mogoče doseči s kategorijo B, je PL = b.«* [29]

PL_b je definiran od 3×10^{-6} do $< 10^{-5}$ napak na uro ali enkrat v 10.000 do 100.000 urah oz. enkrat v 3.000.000 urah delovanja. To se zdi veliko, toda pri obravnavi verjetnosti so te številke dejansko precej nizke.

Kategorija 1

Standard ISO 13849-1 opredeljuje, da se SRP/CS kategorije 1 projektira in izdela ob uporabi dobro preizkušenih sestavnih delov in preizkušenih varnostnih načel [36].

V povezavi s tem je treba vedeti, kaj je dobro preizkušena komponenta.

Odgovor najdemo v standardu:

»Preizkušena komponenta za varnostno aplikacijo je tudi komponenta,

a) ki se je v preteklosti pogosto uporabljala z uspešnimi rezultati v podobnih aplikacijah ali
b) ki je izdelana in preverjena z uporabo načel, ki dokazujejo njeno primernost in zanesljivost za aplikacije, povezane z varnostjo.« [29]

Med dobro preizkušene komponente spadajo razni vijaki, vzmeti, zatiči ipd. Mednje ne sodijo razni kontaktorji, releji ali končna stikala. To predstavlja izziv, ki ga ni nemogoče premagati. Ključ do tega je ugotoviti, kako so izbrane komponente sestavljene. Če uporabljajo komponente in tehnike, ki so dobro preizkušene, se lahko sestavljena komponenta smatra za dobro preizkušeno.

Zanesljivost

Pravilno določene komponente bodo skupaj s predimenzioniranjem, z izvajanjem konstrukcijskih omejitev in uporabo varnostnih načel daleč najbolj pripomogle k izboljšanju zanesljivosti nadzornega sistema [36].

»$MTTF_d$ vsakega kanala mora biti visok.« [29]

»Največja vrednost PL, ki jo je mogoče doseči s kategorijo 1, je PL = c.« [29]

Iz standarda je moč razbrati, da je celovitost sistema kategorije 1 večja od sistema kategorije B, saj je $MTTF_d$ za vsak kanal sistema prešel v raven učinkovitosti PL_b ali PL_c [36].

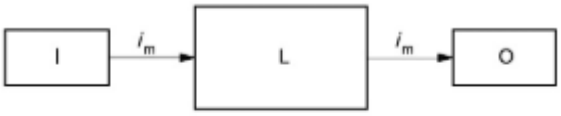
> *»V sistemih kategorije 1 ni diagnostičnega pokritja (DC_{avg} = nič). V takšnih strukturah (enokanalni sistemi) upoštevanje CCF ni pomembno.«* [29]

> *»Če se pojavi napaka, lahko pride do izgube varnostne funkcije. Vendar je $MTTF_d$ vsakega kanala v kategoriji 1 višja kot v kategoriji B. Posledično je izguba varnostne funkcije manj verjetna.«* [29]

Slika 4.4, predstavljena v poglavju 4.4 Raven učinkovitosti, kaže razliko v predvidenih letih do okvare. Kot lahko opazimo, $MTTF_d$ "High" povzroči napovedano stopnjo napak med 30 in 100 leti. To je zelo dober rezultat za preprosto izboljšanje komponent, ki se uporabljajo v sistemu [36].

Druga korist je povečanje celotnega PL. Kjer lahko arhitektura kategorije B v najboljšem primeru zagotavlja zmogljivost PL_b, kategorija 1 to doseže do PL_c [36].

Blokovna shema kategorije 1 izgleda enako kot blokovna shema kategorije B, saj se spremenijo samo v sistemu uporabljene komponente, arhitektura pa ne.



Legenda

i_m	sredstva za medsebojno povezovanje
I	vhodna naprava, npr. senzor
L	logika
O	izhodna naprava, npr. glavni kontaktor

Slika 4.8 Osnovna arhitektura kategorije 1 [29]

Kategorija 2

Tako kot kategorija 1 je kategorija 2 zgrajena na kategoriji B, zato veljajo zanjo enake zahteve, pri tem pa je treba upoštevati tudi dobro preizkušena varnostna načela. Poleg tega velja tudi, da mora biti SRP/CS kategorije 2 zasnovan tako, da se njegove varnostne funkcije v ustreznih časovnih presledkih preverijo s krmilnim sistemom stroja. Pri tem preverjanje varnostnih funkcij ne sme povzročiti nevarne situacije [37].

Varnostne funkcije stroja se preverijo:

- pri zagonu stroja,
- pred začetkom kakršne koli nevarne situacije (npr. začetek novega cikla) ali
- redno med delovanjem, če ocena tveganja in vrsta operacije pokažeta, da je to potrebno.

Preverjanje varnostnih funkcij ne sme povzročiti nevarne situacije [37].

Začetek preverjanja varnostnih funkcij je lahko samodejen. Če ob preverjanju delovanja varnostne funkcije napake niso odkrite, mora nadzorni sistem dovoliti delovanje sistema. Če se napaka odkrije, se, kadar je to mogoče, ustvari izhod, ki sproži ustrezno varno stanje. To se ohrani, dokler se napaka ne odpravi. Kadar to ni mogoče, mora izhod opozoriti na nevarnost [37].

Sistemi, ki izpolnjujejo kategorijo 2, morajo v zvezi s sestavnimi deli izpolnjevati vse enake zahteve kot za kategorijo B.

Kategorija 2 prinaša idejo diagnostike. Če so izbrane komponente pravilno določene (kategorija B) in se uporabljajo po »preizkušenih varnostnih načelih«, bi dodatna diagnostika sistemu omogočila, da ta zazna nekatere napake ali zmožnost varnega delovanja tudi v primeru, ko je del sistema v napaki [37].

Redno preverjanje je nujno. Pregledi se morajo izvesti vsaj vsakič, ko se pojavi potreba po sistemu, to pomeni, da se odprejo in zaprejo varovalna vrata ali pritisne in ponastavi gumb za zaustavitev v sili. Poleg tega je treba celovitost SRP/CS preizkusiti na začetku cikla ali

nevarnega obdobja in potencialno občasno med delovanjem, če ocena tveganja kaže, da je to potrebno. Frekvenca preizkušanja mora biti vsaj 100-kratna stopnja porabe [37]. Na primer svetlobna zavesa, ki se prekine vsakih 30 sekund med normalnim delovanjem, zahteva minimalno preizkusno hitrost enkrat na 0,3 s ali 200-krat na minuto ali več.

To zahteva skrben razmislek, saj morajo komponente varnostnega sistema medsebojno delovati s sistemom za nadzor procesa, da sprožijo in vzdržujejo varno stanje, če je varnostni sistem v napaki. Upoštevati je treba tudi, da v arhitekturi kategorije 2 ni mogoče uporabiti izključitve napak, ker sistem ni toleranten nanje.

Vse to vodi k zanimivemu vprašanju:

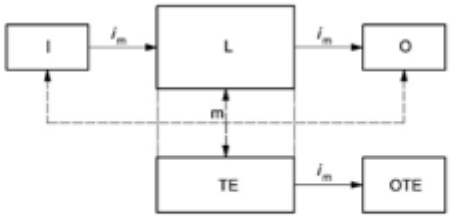
Ali lahko zagotovimo diagnostiko s standardnim PLC-jem, če je sistem ožičen preko delovnega kanala in vse komponente, ki se uporabljajo v tem kanalu, izpolnjujejo zahteve kategorije B?

Odgovor je DA, saj je testna oprema (imenovana TE na sliki 4.9) izrecno izključena, kategorija 2 pa NE zahteva uporabe dobro preizkušenih komponent, le dobro preizkušena varnostna načela. Nazadnje mora za napake, ki jih lahko odkrije nadzorni sistem, odkrivanje napake sprožiti varno stanje [37].

Oziraje se na kategorijo 2, v primeru nezmožnosti preverjanja vseh komponent funkcionalnega kanala sistema ne moremo zahtevati skladnosti s to kategorijo [37].

Izračun $MTTF_d$ in DC_{avg}

Za arhitekturo, prikazano na sliki 4.9 kategorije 2, se za izračun $MTTF_d$ in DC_{avg} upošteva samo bloke funkcionalnega kanala (tj. I, L in O na sliki 4.9) in ne blokov preizkusnega kanala (npr. TE in OTE na sliki 4.9).



Črtkane črte predstavljajo primerno izvedljivo odkrivanje napak.

Legenda

i_m	sredstva za medsebojno povezovanje
I	vhodna naprava, npr. senzor
L	logika
m	spremljanje
O	izhodna naprava, npr. glavni kontaktor
TE	Preskusna oprema
OTE	izhod iz preskusne opreme

Slika 4.9 Osnovna arhitektura kategorije 2 [29]

Potreben je izračun $MTTF_d$ vsake komponente v funkcionalnem kanalu in nato $MTTF_d$ celotnega kanala [37].

DC_{avg} se prav tako izračuna izključno na podlagi komponent v funkcionalnem kanalu, zato se pri določanju odstotka napak, ki jih lahko odkrije nadzorna oprema, upoštevajo samo napake v funkcionalnem kanalu. To poudarja dejstvo, da okvare sistema za spremljanje ni mogoče zaznati [37].

DC_{avg} celotnega SRP/CS, vključno z odkrivanjem napak, mora biti nizka. $MTTF_d$ vsakega kanala mora biti nizka do visoka, odvisno od PL_r.

Največja vrednost PL, ki jo je mogoče doseči s kategorijo 2, je PL = d [29].

Kategorija 3

Arhitektura sistema kategorije 3 je prva kategorija, za katero velja, da je podobna sistemom »Control Reliable«, ki so opredeljeni v severnoameriških standardih.

Kaj pomeni »Control Reliable«?

Ta izraz je skoval tehnični odbor ANSI RIA R15.06, ko je razvijal svoje opredelitve zanesljivosti nadzornega sistema, ki so bile prvič objavljene v izdaji standarda iz leta 1999. Sam izraz »Control Reliable« pomeni, da je krmilni sistem zasnovan z določeno stopnjo tolerance napak. Odvisno od opredelitev, je to lahko enostranska ali večkratna toleranca napak [38].

Opredelitev kategorije 3 po ISO:

> *»Za kategorijo 3 veljajo enake zahteve, kot so tiste za kategorijo B. Upoštevati je potrebno tudi dobro preizkušene varnostne principe. Poleg tega velja tudi naslednje, da je SRP/CS kategorije 3 zasnovan tako, da posamezna napaka v katerem koli od teh delov ne povzroči izgube varnostne funkcije. Kadar je to razumno izvedljivo, se posamezna napaka zazna ob ali pred naslednjim zahtevkom glede varnostne funkcije.«* [29]

Izbrane komponente morajo biti primerne za uporabo in pravilno določene za napetostne, tokovne, okoljske in druge pogoje. Pri načrtovanju je treba uporabiti preizkušena varnostna načela.

Omenjena opredelitev nadalje postavlja zahtevo za toleranco ene napake. To pomeni, da odpoved katerekoli komponente v funkcionalnem kanalu ne more povzročiti izgube varnostne funkcije. S tem pa ne bodo odkrite vse napake, kar pomeni, da lahko kopičenje neodkritih napak povzroči izgubo varnostne funkcije.

Za izpolnitev te zahteve je potrebna redundanca. Pri redundantnih sistemih lahko en kanal popolnoma odpove in stroj ne bo izgubil sposobnosti zaustavitve. Funkcijo sistema za spremljanje je mogoče izgubiti zaradi okvare ene same komponente, vendar je to sprejemljivo, dokler sistem še naprej zagotavlja varnostno funkcijo.

Zahteve MTTFd, DC_{avg}, CCF

»$MTTF_d$ vsakega kanala mora biti nizka do visoka, odvisno od PL_r.« [29]

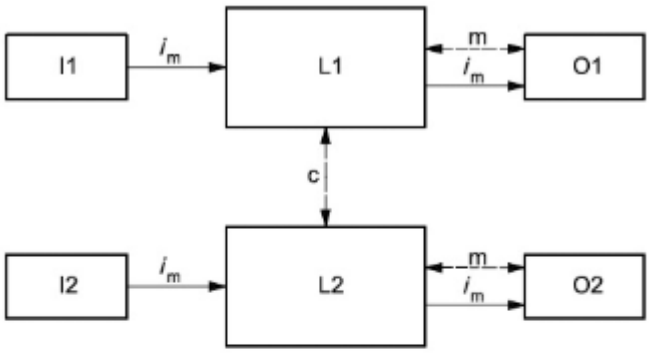
Odvisno od PL_r, ki se ga skuša doseči, je treba izbrati komponente z ustreznimi ocenami $MTTF_d$ in ta izbira je zelo pomembna. Če se sklicujemo na sliko 4.4, ki je predstavljena v poglavju 4.4 Raven učinkovitosti, opazimo, da lahko arhitektura kategorije 3 ustreza območju PL, vse od PL_a do PL_e [38].

Na podlagi tabele 4.5 mora biti DC_{avg} med 60 % in 90 %, pri čemer se upoštevajo vse komponente sistema.

»Uporabljajo se ukrepi proti CCF.« [29]

Da bi arhitektura modela ustrezala arhitekturi kategorije 3, so potrebni ukrepi CCF. Oblikovanje mora izpolnjevati vsaj 65 točk, da izpolnjuje minimalno raven zaščite CCF [38].

Na sliki 4.10 lahko jasno opazimo dva neodvisna kanala in povezavo navzkrižnega nadzora med kanali. Vhodnih naprav se v arhitekturi kategorije 3 ne spremlja, tako da se nadzoruje samo izhodne naprave. To je tudi razlog za uporabo dveh fizično ločenih vhodnih naprav za zaznavanje položaja zaščite. Tako je edini način odkritja napak v vhodnih napravah ta, da en kanal spremeni stanje, drugi pa ne.



Črtkane črte predstavljajo primerno izvedljivo odkrivanje napak.

Legenda

i_m	sredstva za medsebojno povezovanje
c	navkrižno spremljanje
I1, I2	vhodna naprava, npr. senzor
L1, L2	logika
m	spremljanje
O1, O2	izhodna naprava, npr. glavni kontaktor

Slika 4.10 Osnovna arhitektura kategorije 3 [29]

Komponente, ki se uporabljajo v sistemu, so kritične za končno oceno PL. Končni PL zasnove je odvisen od $MTTF_d$ posameznih komponent, ki se uporabljajo v vsakem kanalu. Izbira vhodnih in izhodnih naprav je pomemben dejavnik [38].

Kategorija 4

Najbolj zanesljiva od petih sistemskih arhitektur je kategorija 4. Je edina arhitektura, ki uporablja tehnike, tolerantne na več napak in ki pomagajo zagotoviti, da odpoved komponent ne povzroči nesprejemljive izpostavljenosti tveganju [39].

Opredelitev kategorije 4 po standardu [29]:

> *»Za kategorijo 4 veljajo enake zahteve kot za kategorijo B. Prav tako je potrebno upoštevati "dobro preizkušene varnostne principe". Poleg tega pa velja tudi naslednje, da se SRP/CS kategorije 4 oblikujejo tako, da*
>
> - *ena sama napaka v kateremkoli od teh varnostnih delov ne povzroči izgube varnostne funkcije in*
> - *posamezna napaka se zazna na ali pred naslednjim zahtevanjem varnostnih funkcij (npr. takoj ob vklopu ali na koncu delovnega cikla stroja).*
>
> *Če odkrivanje napak ni mogoče, potem kopičenje neodkritih napak ne povzroči izgube varnostne funkcije.«* [29]

Prvi del opredelitve nudi osnovno zahtevo za kategorijo od 2 do 4. Upoštevati je treba izbiro komponent glede na zahteve za napetostne, tokovne in stikalne zmogljivosti ter življenjsko dobo. V kategoriji 4 ni potrebe po uporabi dobro preizkušenih komponent, čeprav jih je priporočeno uporabiti za dodatno zanesljivost.

Različno od kategorije 3 pa v kategoriji 4 nobena posamezna napaka ne povzroči izgube varnostne funkcije, zato je potrebno preizkušanje, ki lahko zazna napake. Kopičenje neodkritih napak na koncu ne more privesti do izgube varnostne funkcije. Zahteva glede neodkritih napak, ki vodijo do izgube varnostne funkcije, pomeni, da jih je treba načrtno odpraviti. Če diagnostika ne more zaznati vseh napak, jo je treba izboljšati, tako da postanejo vse nevarne napake, ki jih ni mogoče zaznati, nevarne zaznavne napake. Povečanje diagnostičnih zmogljivosti sistema je temeljna razlika med kategorijo 3 in kategorijo 4.

Za obnašanje sistema kategorije 4 je značilno:

- nadaljevanje izvajanja varnostne funkcije ob eni sami napaki,
- pravočasno odkrivanje napak, da se prepreči izguba varnostne funkcije,
- upoštevanje kopičenja neodkritih napak.

Zahteve $MTTF_d$, DC_{avg}, CCF

> *»DC_{avg} celotnega SRP/CS je visoka, vključno s kopičenjem napak.«* [29]

Razlika med kategorijo 3 in kategorijo 4 je višji DC_{avg}. V kategoriji 3 mora biti DC_{avg} »vsaj nizek«, kar pomeni 60–90 %, v kategoriji 4 pa 99 % ali več [39].

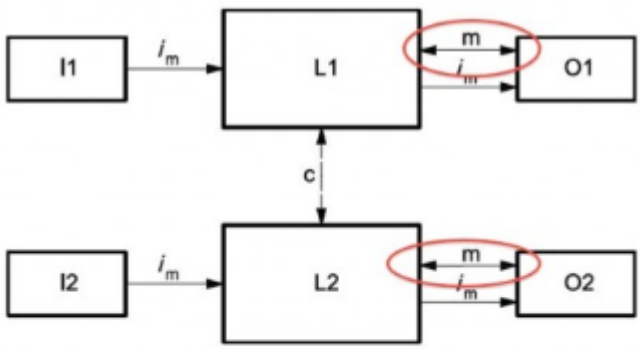
> *»$MTTF_d$ vsakega od odvečnih kanalov je visok.«* [29]

V povezavi z $MTTF_d$ vsakega kanala so potrebne boljše diagnostike in veliko višje zahteve za posamezno komponento [39].

> *»Uporabljajo se ukrepi proti CCF.«* [29]

Zmožnost samodejnega diagnosticiranja napak je kritični del zasnove, kot tudi uporaba zelo zanesljivih komponent, ki vodijo do zelo zanesljivih kanalov. Potrebna je tudi najmočnejša zaščita CCF [39].

Blok diagram za kategorijo 4, prikazan na sliki 4.11, je skoraj identičen diagramu kategorije 3, razlika je zgolj v upoštevanju, da so črte »m« trdne in ne prekinjene, kar predstavlja večji DC_{avg}.



Črtkane črte predstavljajo primerno izvedljivo odkrivanje napak.

Legenda

i_m	sredstva za medsebojno povezovanje
c	navkrižno spremljanje
I1, I2	vhodna naprava, npr. senzor
L1, L2	logika
m	spremljanje
O1, O2	izhodna naprava, npr. glavni kontaktor

Slika 4.11 Osnovna arhitektura kategorije 4 [29]

Glede na to, da so v zanesljivosti izbranih komponent in načinu izvedbe testiranja prisotne primarne razlike, je lahko osnovna fizična konstrukcija obeh kategorij enaka.

Kategorija se prav tako zanaša na redundanco, da bi zagotovila, da popolna izguba enega kanala ne povzroči izgube varnostne funkcije. To je koristno, če so odpravljene okvare skupnega vzroka, v nasprotnem primeru lahko en dogodek istočasno izbriše oba kanala, kar povzroči izgubo varnostne funkcije.

4.9 Varnostna programska oprema

Do sedaj je bil predstavljen zgolj osnovni postopek, ki se uporablja za načrtovanje varnostnih delov nadzornega sistema. Te tehnike se uporabljajo le za načrtovanje strojne opreme, ki se uporablja za varnostne namene. Seveda pa celotno delovanje sistema opredeljuje programska oprema.

Varnostna programska oprema je namenjena le zmanjšanju tveganja. Tako nekatere platforme, kot so Windows, MacOS in Linux niso primerne za varnostno programsko opremo, saj so na splošno ti operacijski sistemi preveč zapleteni in podvrženi nepričakovanim spremembam. Seveda ni nič narobe z uporabo teh sistemov za nadzorne funkcije, vendar morajo varnostne funkcije delovati na bolj predvidljivih in zanesljivih platformah [31].

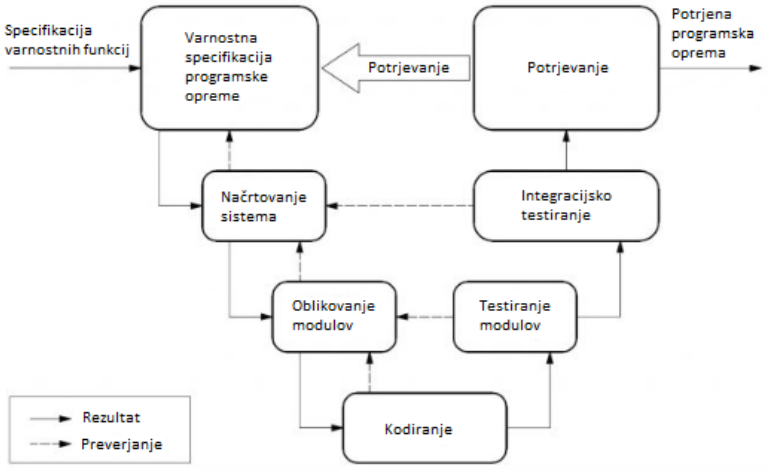
Metodologija, obravnavana v standardu ISO 13849-1, je uporabna do PL_d.

Za razvoj programske opreme, povezane z varnostjo, sta pomembna dva cilja:

- izogibati se napakam in
- ustvariti berljivo, razumljivo, preizkusno in vzdrževalno programsko opremo [31].

Izogibanje napakam

Slika 4.12 prikazuje V-Model za razvoj varnostne programske opreme. Ta pristop k oblikovanju programske opreme vključuje tako validacijo kot tudi preverjanje in če je izveden pravilno, bo programska oprema ustrezala specifikacijam [30].



Slika 4.12 V-Model za razvoj varnostne programske opreme [30]

Oziraje se na specifikacije varnostnih zahtev, je na sliki 4.12 prikazan vsak korak v postopku. Črtkane črte ponazarjajo postopek preverjanja na vsakem koraku.

Dva pristopa k oblikovanju programske opreme

Obstajata dva pristopa k oblikovanju programske opreme, ki ju je treba upoštevati:

- Prednastavljena programska oprema se običajno uporablja za konfiguriranje varnostnih PLC-jev ali programabilnih varnostnih relejev ali modulov. Vnaprej napisane funkcijske bloke za posamezne naprave predvidoma zagotavlja njihov proizvajalec, pri tem pa ima vsak blok svojo nalogo. Tako oblikovalec nima dostopa do kode, povezane z varnostjo. Z uporabo vnaprej konfiguriranih gradnikov dosežemo prvi cilj, izogibanje napakam, vsaj kar zadeva programsko kodiranje [30].
- Popolnoma prilagojena programska oprema se uporablja v primerih, v katerih se uporablja popolnoma prilagojena strojna platforma. V tem primeru je treba uporabiti celoten pristop »V-model-a« načrtovanja strojne in programske opreme [30].

4.10 Upoštevanje napak in izključitev napak

Standard ISO 13849-1 obravnava tudi odkrivanje in odpravljanje napak. Obravnava napak je postopek pregleda komponent in podsistemov, ki se uporabljajo v varnostnem delu nadzornega sistema. Pri obravnavi se izdela še seznam vseh napak, ki se lahko pojavijo v sistemu. Seznami napak so vhodni elementi v načrtih strojne in programske opreme.

Pri sistemih kategorije B in 1, kjer se diagnostika ne uporablja, je treba napake odpraviti z uporabo inherentno varnih konstrukcijskih tehnik. Pri sistemih kategorije 2, 3 in 4 je diagnostika del konstrukcije, seznami napak pa se v tem primeru uporabljajo za ocenjevanje DC. Odvisno od arhitekture, so za doseganje ustreznega PL zahtevane določene ravni DC [30].

Vse nevarne napake, ki jih je mogoče zaznati, morajo biti zajete v diagnostiki, pri tem pa mora biti DC dovolj visok, da ustreza PL_r za vsako varnostno funkcijo [31].

Upoštevanje napak

Prvi korak je razvoj seznama potencialnih napak, ki se lahko pojavijo na podlagi komponent in podsistemov, vključenih v SRP/CS. ISO 13849-2 vključuje sezname tipičnih napak za različne tehnologije.

Napaka upoštevanja	Izključitev napak	Pripombe
obraba / korozija	Da, v primeru skrbno izbranega materiala, (pre) dimenzioniranja, postopka izdelave, obdelave in ustreznega mazanja v skladu z določeno življenjsko dobo	Poglej ISO 13849-1: 2006, 7.3.
netesnitev / popuščanje	Da, v primeru skrbno izbranega materiala, postopka izdelave, zaklepnih sredstev in obdelave, glede na določeno življenjsko dobo	
zlom	da, v primeru skrbno izbranega materiala, (pre) dimenzioniranja, postopka izdelave, obdelave in ustreznega mazanja v skladu z določeno življenjsko dobo	
deformacija s prenapetostjo	da, v primeru skrbno izbranega materiala (pre) dimenzioniranje, obdelava in postopek izdelave v skladu z določeno življenjsko dobo	
togost / lepljenje	da, v primeru skrbno izbranega materiala, (pre) dimenzioniranja, postopka izdelave, obdelave in ustreznega mazanja v skladu z določeno življenjsko dobo	

Tabela 4.7 Napake in izključitve napak [30]

Sicer obstaja še veliko več napak, toda bistveno je, da je treba za vsak sistem razviti seznam napak in nato razmisliti, kako lahko vsaka napaka vpliva na delovanje sistema. Analiza napak in učinkov (FMEA) je običajno najboljši pristop za razvoj seznamov napak za komponente [30].

Pri obravnavi napak, ki so vključene v seznam, je treba upoštevati naslednje:

- če se po prvi napaki pojavijo druge napake zaradi prve, se lahko te napake združijo v eno samo,
- prav tako se lahko dve ali več posameznih napak s skupnim vzrokom obravnavajo kot ena napaka,
- večkratne napake z različnimi vzroki, ki se pojavijo hkrati, se štejejo za neverjetne in jih ni treba upoštevati [31].

5 DODATNE VARNOSTNE ZAHTEVE – VARNOSTNI TESTI

Sistemi ustavitve v sili in razna varovala se štejejo za »dopolnilne zaščitne ukrepe« v ključnih varnostnih standardih za stroje, kot sta ISO 12100 in CSA Z432, zato so ti sistemi glavni varnostni ukrepi. Po opredelitvi gre pri za situacijo, ki se ji oblikovalec strojev ni mogel izogniti [23].

Varnostni sistemi se sprožijo ročno in se običajno redko uporabljajo. Pomanjkanje uporabe pomeni, da se funkcionalno preizkušanje sistema ne zgodi med običajnim delovanjem stroja. Nekatere vrste napak se lahko pojavijo in ostanejo neodkrite, dokler se sistem dejansko ne uporabi. Napaka na tej točki je lahko katastrofalna, saj so primarni zaščitni ukrepi posledično že v okvari [22].

Da bi razumeli zahteve za testiranje, je pomembno razumeti zahteve glede tveganja in zanesljivosti, ki poganjajo zasnovo varnostnih sistemov. Tako lahko določimo ukrepe za obvladovanje tveganja. Kadar se nadzorni sistem uporablja kot del ukrepa za obvladovanje tveganja, je treba določiti varnostno funkcijo. Specifikacija varnostne funkcije vključuje PL, arhitekturno kategorijo, $MTTF_d$ in DC ali SIL in HFT, kot je opisano v standardu IEC 62061 [22].

Preizkušanje varnostnih sistemov, vključno z zaustavitvami v sili in raznimi zaščitnimi napravami za strojne aplikacije, je predmet obravnave, ki redno povzroča veliko različnih interpretacij, na katere je moč najti najrazličnejše odgovore s še bolj različnimi utemeljitvami.

Vprašanje, ki se poraja glede varnostnega testa:

Ali je nujno preizkusiti zaporne naprave, zaustavitve v sili in druge zaščitne naprave?

Odgovor je da**. Opremo je treba zaradi zagotovitve pravilnega delovanja funkcij, povezanih z varnostjo, pogosto preverjati.** Napaka, ki vpliva na samo delovanje stroja, je navadno vidna v zelo kratkem času. Vendar lahko napaka, ki je kritična za varnost sistema, dolgo ostane neopažena, razen če so v vzdrževalne dejavnosti vključene ustrezne varnostne kontrole. Če obstaja možnost, da varnostno kritične komponente odpovejo in povzročijo odpoved oz. napako na varovalni opremi in s tem takojšnje ali skrite potencialne nevarnosti, je potreben formalni sistem načrtovanega preventivnega vzdrževanja [23].

Naslednje vprašanje, ki se pojavi glede na to temo, se glasi:

Kako pogosto bi morali preizkušati zaustavitve v sili in razne zaščitne naprave?

Pomembno vlogo ima življenjska doba strojev. Avtorji standardov so se odločili za privzeto življenjsko dobo 20 let, kar pomeni, da je verjetnost nezaznavnih nevarnih napak manjša kot enkrat v dvajsetih letih delovanja [23].

Vsaka arhitekturna kategorija ima različne zahteve za testiranje. Preizkusne stopnje so povezane s »Stopnjo povpraševanja«, katere opredelitev po standardu se glasi:

»Stopnja povpraševanja – pogostost zahtev za varnostno dejanje SRP/CS.« [30]

Vsakič, ko se sproži varnostna komponenta, kot je zaustavitev v sili, se v sistem vstavi »povpraševanje«. Če pogledamo »Poenostavljen postopek za ocenjevanje PL«, ugotovimo, da standard predpostavlja naslednje: [23]

- *»čas misije 20 let,*
- *stalne stopnje napak v času delovanja,*
- *za kategorijo 2 je stopnja povpraševanja < = 1/100 testna stopnja,*
- *za kategorijo 2 je $MTTF_{dTE}$ večji od polovice $MTTF_{dL}$.«* [29]

Čas 20-letne misije je predvidena življenjska doba stroja. Ta številka podpira preostale izračune v standardu in temelji na ideji, da malo sodobnih kontrolnih sistemov deluje dlje kot 20 let, ne da bi jih nadomestili ali obnovili. Stalna stopnja napak kaže na miselnost, da bodo imeli uporabljeni sistemi komponente in nadzor, ki niso podvrženi napakam, niti niso dovolj stari, da bi lahko zaradi starosti začeli propadati, ampak da sistem deluje normalno [23].

Komponente, ki so bolj izpostavljene in so bolj podvržene odpovedi, so iz sistema odstranjene prej. Pričakuje se, da bodo tiste komponente, ki ne bodo izrabljene, dosegle to točko po 20 letih. V nasprotnem primeru morajo navodila za vzdrževanje sistema vključevati preventivne vzdrževalne naloge, ki zahtevajo zamenjavo kritičnih komponent, preden dosežejo predvideno $MTTF_d$ [23].

Kadar zaščitne naprave uporabljajo samodejno spremljanje, da dosežejo potreben DC za zahtevan PL/SIL, se opravi funkcionalni preizkus vsakič, ko naprava spremeni svoje stanje. S tem ni nič narobe, če naprava deluje pogosto, lahko pa obstajajo tudi zaščitne naprave, pri katerih je stopnja povpraševanja redka [23].

> *»Pogostost v zvezi z varnostnim sistemom opredeljuje visoko povpraševanje, kjer je pogostost zahtev za delovanje na varnostnem sistemu večja od enega na leto. Neprekinjeno povpraševanje se šteje za zelo veliko povpraševanje.«* [33]

Če je zahteva na zaščitni napravi redka, < 1 na leto, potem se naprava uporablja z dodatnimi ukrepi, in sicer zato, da se med zaporednimi funkcionalnimi preizkusi poveča verjetnost pojava neodkrite napake [22].

Kadar je za odkrivanje morebitnega kopičenja napak potreben ročni preizkus delovanja, ga je treba opravljati v naslednjih preizkusnih intervalih [22].

PLr	Kategorija	SIL	HFT	Minimalna frekvenca izvajanja	sklic
e	3&4	3	1	mesečno	EN 14119 (8.2)
d	3	2	1	Letno	EN 14119 (8.2)
≤c	1	1	0	mesečno	SES - Priporočena vrednost

Tabela 5.1 Minimalna zahtevana periodika varnostnih zapor [22]

Pri ročnem pregledovanju varnostnih sistemov mora to vključevati preverjanje odziva na nadzor. Z aktivacijo vhodne varnostne naprave se izvede ustrezen nadzorni odziv. Ob upoštevanju tega mora oseba, ki izvaja ročni funkcionalno varnosti test, vedeti, kakšen je pričakovani odziv nadzora [22].

Dodatne varnostne zahteve za kategorijo 3

Kategorija 3 je tolerantna na eno samo napako. To pomeni, da se, dokler ni zaznanih več neodkritih napak, lahko zanašamo na delovanje sistema, ki nas opozori na posamezno napako. Treba se je zavedati, da samodejni testi morda ne bodo zaznali vseh napak. V tem primeru se uporabi »dokazni test«, katerega opredelitev je predstavljena v IEC 61508-4 [23]:

> *»Periodični preizkus, ki se izvaja za odkrivanje okvar v varnostnem sistemu, tako da se lahko sistem po potrebi ponovno vzpostavi v „novo“ stanje ali čim bližje temu stanju.«* [40]

20-letna predpostavka življenjskega cikla, uporabljena v standardih, velja tudi za testiranje. Predvideva se, da dobijo strojne kontrole vsaj en preizkus odpornosti v svoji življenjski dobi. Preizkus testiranja mora biti zasnovan tako, da zazna napake, ki jih avtomatska diagnostika ne more zaznati [23].

Dodatne varnostne zahteve za kategorijo 2

Po standardu je PL_d mogoče doseči z uporabo arhitekture kategorije 3 in tudi z uporabo kategorije 2, dokler je $MTTF_d$ dovolj visok in obstaja vsaj nizka stopnja diagnostičnega pokritja.

Osrednji dejavnik kategorije 2 je preverjanje varnostne funkcije (brez povečane zanesljivosti), pri katerem bo povečana frekvenca preverjanja zmanjšala verjetnost nevarnih situacij. Z drugimi besedami, testiranje v prisotnosti napake zmanjša verjetnost delovanja stroja.

V okviru poenostavljenega postopka v standardu EN ISO 13849-1 se mora pregled v kategoriji 2 pojaviti **ob zagonu** in **nato v rednih časovnih presledkih**, pri čemer se predpostavlja, da frekvenca ustreza vsaj sto testom za vsako zahtevo glede varnostne funkcije. To je v skladu z določbo 4.5.4 standarda EN ISO 13849-1, kjer je za kategorijo 2 »stopnja povpraševanja <1/100 testna stopnja« [23].

Za sisteme, ki uporabljajo arhitekturo kategorije 2, mora biti hitrost samodejnega diagnostičnega testa vsaj 100-krat višja od zahtev. Preizkusna hitrost je običajno dosežena samodejno pri načrtovanju krmilnih elementov in je povezana samo z zaznavnimi varnimi ali nevarnimi napakami. Napake, ki jih ni mogoče zaznati, morajo biti verjetne manj kot enkrat v 20 letih in jih je treba odkriti s »preizkusom« [21].

V industriji funkcionalni varnostni test upravlja s preizkusno frekvenco v strojnih aplikacijah na dinamično preizkušenem OSSD (varnostni izhod v trdnem stanju) na svetlobni zavesi ali v aplikacijah z zelo nizkim povpraševanjem, kot je redko uporabljena zaustavitev v sili. Pri elektromehanskih napravah na varovalih, kot so zaporna stikala, končna stikala in magnetna varnostna stikala, preizkušanje pomeni aktiviranje (to je odpiranje in zapiranje zaščite) vsaj 100-krat med funkcijsko potrebo po odprtju zaščite [21].

To je lahko zelo neprijetno, saj se s tem ovira produktivnost ali pa je izvedba celo nemogoča zaradi velikega povpraševanja, ki je že postavljeno na varnostno funkcijo. Lahko si predstavljamo, da bi morali v dvominutnem proizvodnem ciklu 100-krat preizkusiti zaščitna vrata, kar pa ni praktično.

Zato je običajneje in bolj praktično PL_d doseči z dvokanalno arhitekturo kategorije 3 ali 4, ker izboljšuje zanesljivost s toleranco napak strojne opreme (brez zelo pogostih periodičnih preizkusnih ciklov) in avtomatsko diagnostično pokritost v sistemu [21].

Dodatne varnostne zahteve za kategorijo 1

Kategorija 1 nima diagnostike, zato v standardih ni navodil, ki bi pomagala pri teh sistemih.

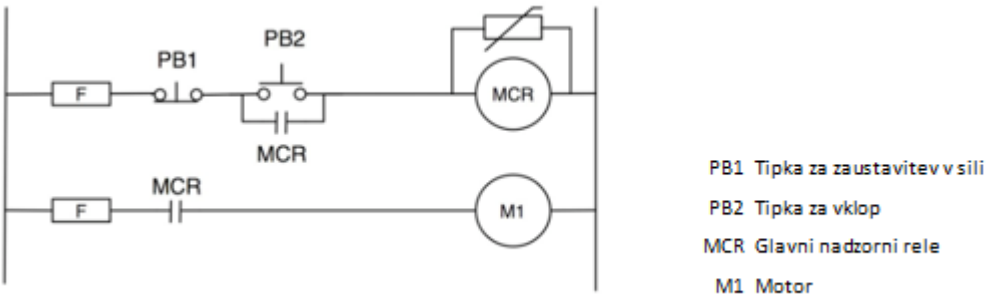
5.1 Minimalna frekvenca izvajanja varnostnega testa za izklope v sili

Če poznamo arhitekturo sistema za zaustavitev v sili, lahko določimo preizkusno hitrost glede na stopnjo povpraševanja. Bilo bi precej lažje, če bi standardi podali nekaj minimalnih testnih stopenj za različne arhitekture. Eden takšnih je standard ISO 14119 na zapornih napravah. Res, da ne vključuje funkcij za izklop v sili, saj je njegov poudarek na zapornih napravah, vendar so sistemi za povezovanje bolj kritični kot dopolnilni zaščitni ukrepi, zato bi bilo smiselno uporabiti enaka pravila. Če pogledamo klavzulo o ocenjevanju napak, najdemo te smernice:

> *»Za aplikacije, ki uporabljajo zaskočne naprave s samodejnim nadzorom, da se doseže potrebna diagnostična pokritost za zahtevano varnost, se lahko opravi funkcionalni preizkus (glej IEC 60204-1: 2005, 9.4.2.4) vsakič, ko naprava spremeni svoje stanje, npr. pri vsakem dostopu. Če je v takem primeru samo redko dostopen, se uporabi zaporna naprava z dodatnimi ukrepi, saj se med zaporednimi funkcionalnimi preizkusi poveča verjetnost pojava neodkrite napake.*
>
> *Če je za ugotavljanje morebitnega kopičenja napak potreben ročni preizkus delovanja, ga je treba opraviti v naslednjih preizkusnih intervalih:*
>
> *vsaj vsak mesec za PL_e s kategorijo 3 ali kategorijo 4 (v skladu z ISO 13849-1) ali SIL 3 s HFT (toleranca napake strojne opreme) = 1 (v skladu z IEC 62061);*
>
> *vsaj vsakih 12 mesecev za PL_d s kategorijo 3 (v skladu z ISO 13849-1) ali SIL 2 s HFT (toleranca napake strojne opreme) = 1 (v skladu z IEC 62061).*
>
> *OPOMBA: Priporočljivo je, da krmilni sistem stroja zahteva te preizkuse v zahtevanih intervalih, npr. z vizualno prikazovalno enoto ali signalno svetilko. Krmilni sistem mora nadzorovati preizkuse in zaustaviti stroj, če je preizkus izpuščen ali odpove.«* [23]

Še vedno nimamo testne frekvence za PL_c sisteme kategorije 1, za katere v teh standardih ni izrecnih smernic.

Lahko bi začeli s preučevanjem vrednosti $MTTF_d$ za vse podsisteme in komponente. [6] Standard zahteva, da ima sistem visoko vrednost $MTTF_d$, kar pomeni 30 let <= $MTTF_d$ <= 100 let [6, tabela 5]. Če je tako, potem je poskusni test enkrat na 20 let teoretično dovolj. Pogostejše testiranje, to je več kot enkrat v 20 letih, je vedno sprejemljivo [23].



Slika 5.1 Shema dvokanalne zaustavitve v sili [23]

Treba je upoštevati, da varovalke niso vključene, ker morda ne zadostujejo za varnost, in če predpostavimo, da so bile pravilno določene v prvotni zasnovi, niso podvržene enakim cikličnim učinkom staranja kot druge komponente.

Kadar je za katerokoli kategorijo sistema, zlasti v sistemih kategorije 1 ali 2, potrebno ročno preizkušanje kot del načrta, , mora nadzorni sistem uporabnika opozoriti na zahtevo in ne sme dovoliti delovanja stroja, dokler preizkus ni zaključen. To bo pomagalo zagotoviti, da so zahtevani testi pravilno zaključeni [20].

5.2 Najboljša inženirska praksa glede frekvence izvajanja varnostnega testa

Obstaja nekaj zapisov na podlagi najboljših inženirskih praks, saj izvajanje varnostnih testov v standardih ni točno opredeljeno. Ti pregledi temeljijo na naslednjih načelih:

- Ne glede na kategorijo mora biti pregledana oz. preizkušena vsa varnostna oprema, ki je fizično prisotna na stroju, kot so gumbi za zaustavitev v sili, zasilne vrvice, varnostna vrata, varnostni skenerji, plošče za brisanje in zaustavitev strojev ter varnostne preproge, občutljive na pritisk. Za pravilno delovanje jih je treba preizkušati pogosto.
- Ne glede na kategorijo varnostne naprave je treba sisteme, ki se uporabljajo za zaustavitev nevarnega gibanja stroja, kjer obstaja možnost mehanske okvare, redno preverjati. Ti sistemi vključujejo hidravlične in pnevmatske sklopke ter mehanske zavorne sisteme.
- Elementi z električnim napajanjem, ki nadzorujejo normalno delovanje stroja (npr. strojni primarni kontrolni element), so lahko sestavljeni iz relejev, kontaktorjev, elektromagnetnih naprav ali elektromehanskih naprav. Kadar se ti uporabljajo v povezavi z varnostno napravo, jih je treba za zagotovitev pravilnega delovanja redno preizkušati.
- Če naprava za zaznavanje ščiti upravljavca med več strojnimi nalogami in je vezana na več sistemov, ki se uporabljajo za zaustavitev nevarnega gibanja stroja, morata biti vsaka naloga in sistem vključena v postopek preverjanja.

Na podlagi najboljših inženirskih praks je pogostost pregledov varnostnih naprav prikazana v tabeli 5.2.

NAPRAVA	POSTOPEK IZVAJANJA TESTA	FREKVENCA	OSEBA KI IZVAJA TEST	POTREBNO DOKUMENTIRANJE
Varnostni drog	Aktiviacija varnostnega droga : a) Najprej morate izklopiti stroj b) Aktivirajte vrstico telesa c) Poskusite znova zagnati stroj	1 / Izmeno	Operater	Da
Preverjanje razdalje med ustavljanjem	Po vklopu izklopa v sili je potrebno izmeriti vrtenje valja	1 / teden	Vzdrževalec/tehniik	Da
Varnostne vrvice, zaustavitve v sili, udarne plošče, varnostne naprave občutljive na pritisk.	Posamezno varnostno napravo je potrebno aktivirati in preskusiti na naslednji način: a) Ustaviti stroj b) Vključiti varnostno napravo c) Poskusiti znova zagnati stroj d) Ponavljajti b) in c), dokler se ne preskusijo vse naprave.	· 1 / teden - Vse mehanske varnostne naprave, razen spodaj navedenih izjem. IZJEME · 1 / izmena - Varnostne naprave za T-obroče in nastavke za kroglice na pnevmatskih strojih · Naprave kategorije 3 ali 4 je treba pregledati vsaj 1 / mesec. · Varnostne naprave na kalandrih - 1 / vožnja ali največ 1 / izmena · 1 / mesec - Varnostna oprema na transportnih trakovih · Stroji, ki ne obratujejo dnevno, morajo biti med delovanjem pregledani z uporabo zgornjih zahtev glede frekvenc.	Operater	Da
Svetlobne zavese, laserski skenerji	Postopek prevzema (glejte spodnje dnevnike spodnjega primera)	· Ob zagonu · Vse večje spremembe ali zamenjave · Pri okvari naprave	Kvalificirana oseba	Da
Svetlobne zavese, Laserski skenerji	Preskusni postopek (glej spodaj navedene primerke).	· Ob zagonu · Mesečno za varnostne naprave in krmilne elemente, ki ne ustrezajo oceni zanesljivosti kategorije 3 ali 4. · Letno za varnostne naprave in nadzor, ki izpolnjujejo oceno zanesljivosti kategorije 3 ali kategorije 4. · Po vsakem vzdrževanju, nastavljanju, popravilih ali spremembah stroja ali varnostne naprave.	Kvalificirana oseba	Da

Tabela 5.2 Razporeditev pregledov varnostnih naprav [29][33]

Razpored pregledovanja varnostnih naprav mora biti objavljen ali takoj na voljo na vsakem stroju, da imajo upravljavci, vzdrževalci in inženirsko osebje enostaven dostop do informacij [33].

Evidence inšpekcij in testov je treba hraniti bodisi na papirju bodisi na elektronskih sistemih, kot je SAP [33].

6 IZVEDBA NADZORNEGA SISTEMA ZA IZVAJANJE VARNOSTNEGA TESTA

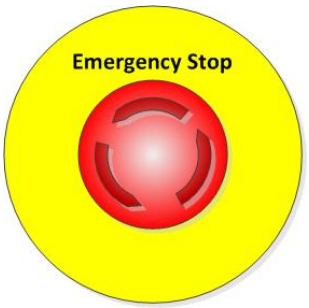
6.1 Varnostna oprema

Stroj je opremljen z varnostno opremo in varnostnimi funkcijami, ki so potrebne za varno delovanje in rokovanje s strojem. Treba je upoštevati navodila za varno delovanje. Stroj je opremljen z naslednjo varnostno opremo:

- mehanska zaščita,
- glavno stikalo,
- tipke za zaustavitev v sili,
- varnostne preproge,
- varnostna vrata,
- svetlobne zavese in
- laserski skenerji.

Tipke za zaustavitev v sili

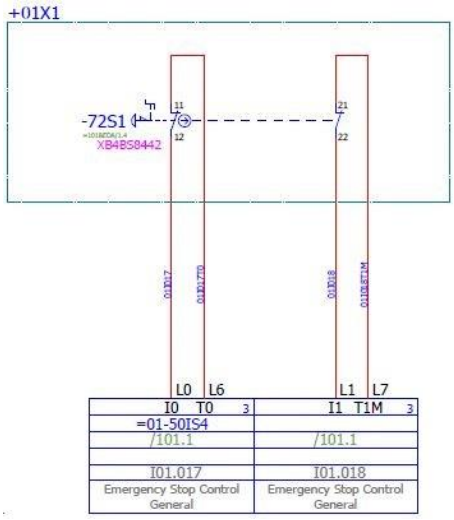
Stikalo za izklop v sili je stikalo, ki se uporablja kot varnostni ukrep za izklop električne naprave v izrednih razmerah (poškodba pri delu) in v primerih, ko električne naprave ni mogoče izklopiti na običajen način. Za razliko od običajnih stikal to stikalo v celoti izklopi električno napravo.



Slika 6.1 Tipka za izklop v sili

Ob pritisku na gumb za zaustavitev v sili, se vsi premiki na stroju takoj ustavijo.

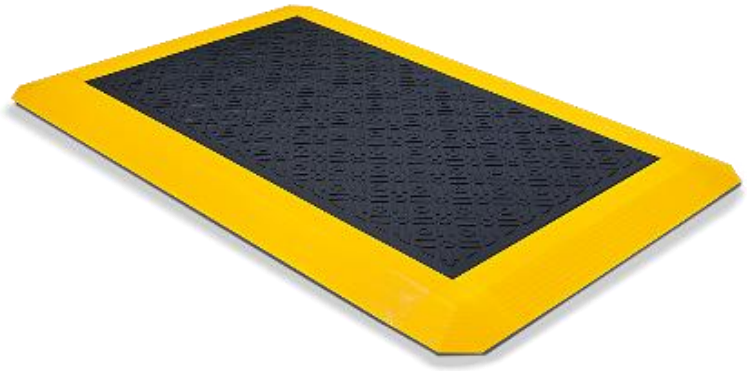
Oskrba s stisnjenim zrakom na ventilskih sponkah se v trenutku izključi. Prav tako se izklopi tudi napetost za pogone, vklopijo pa se zavore pogonov. Na računalniku oz. HMI-ju se prikaže sporočilo o napaki.



Slika 6.2 Arhitektura tipke za zaustavitev v sili

Varnostna preproga

Varnostne preproge so zaščitni elementi, ki so občutljivi na pritisk in so zasnovani za zaznavanje prisotnosti ljudi na zaznavnih površinah. Preproge imajo dve prevodni kaljeni jekleni plošči, ki ju ločita neprevodna stisljiva ločevalnika.



Slika 6.3 Varnostna preproga [32]

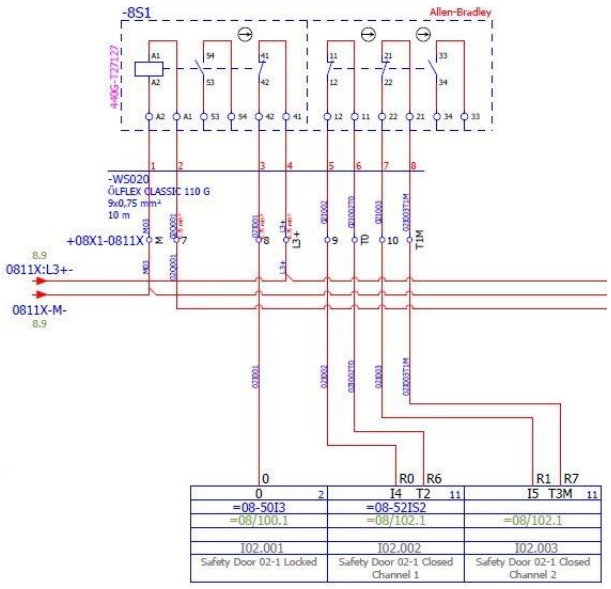
Gibanje stroja se izklopi, ko nekdo stopi na ustrezno varnostno podlogo.

Varnostna vrata

Varnostna vrata s funkcijo zaklepanja varno zaklepajo zaščitene stroje in preprečujejo dostop do nevarnih območij. Tako preprečijo, da bi ljudje vstopali v nevarna območja delovanja strojev.

Slika 6.4 Zaklep na varnostnih vratih

Ograja in varnostna vrata služijo za zaščito pred nevarnimi premiki na stroju. Odpiranje vrat je možno šele po opravljeni registraciji. Vrata se sprostijo oz. dobijo dovoljenje za odpiranje šele, ko se nevarno gibanje stroja ustavi in izklopi (pnevmatsko in električno). Na HMI-ju se prikaže sporočilo o napaki.



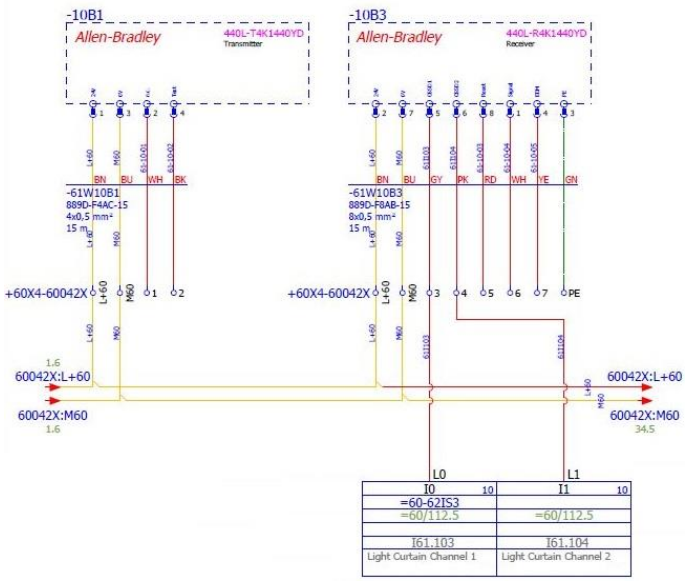
Slika 6.5 Arhitektura varnostnih vrat

Varnostne svetlobne zavese

Varnostne zavese so optoelektronske naprave, ki se uporabljajo za varovanje osebja v bližini premikajočih se strojev oz. delov stroja. Uporabljajo se kot alternativa mehanskim pregradam in drugim oblikam tradicionalnega varovanja stroja. Z uporabo varnostnih svetlobnih zaves je mogoče tudi izboljšati delovanje in učinkovitost strojev, saj omogočajo lažji dostop polavtomatskih postopkov.

Slika 6.6 Varnostna zavesa [32]

Premik z vstopom v območje skeniranja sproži zaustavitev stroja.



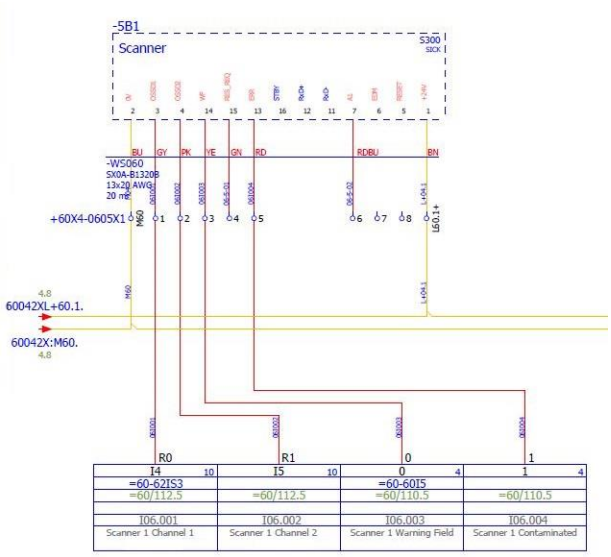
Slika 6.7 Arhitektura laserske varnostne zavese

Varnostni skenerji

Varnostni laserski skenerji so lahko mobilni ali stacionarni in so namenjeni zaščiti območja ali zaščiti dostopa. Z merjenjem časa in prisotnosti naprave pregledujejo okolico in merijo razdalje. Vgrajeno vrtljivo ogledalo omogoča, da se zaščitena območja spremljajo v dveh dimenzijah.

Slika 6.8 Varnostni skener

Premikanje vsakega modula z vstopom v območje skeniranja ali s sprožitvijo varnostnih skenerjev ustavi del zaščitenega stroja. Pri stroju so vsi trije skenerji nameščeni pred serverjem za izdelavo polizdelka.

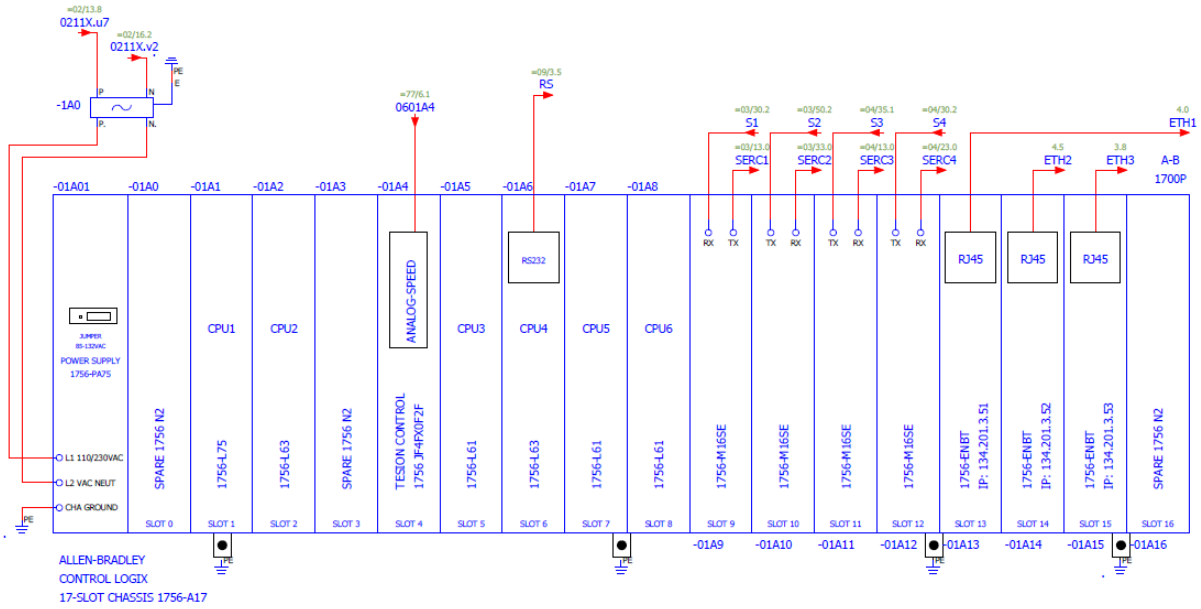


Slika 6.9 Arhitektura varnostnega skenerja

6.2 Nadzorna oprema

Krmilje stroja je razdeljeno na 2 ločena dela. Vsak del krmili PLC, ki pa je na vsaki strani povezan s še po dvema PLC-jema za nadzor gibanja. Tako celotno krmilje stroja sestoji iz 6 PLC-jev, ki so med seboj povezani v »racku«. Rack je sestavljen iz 17 rež, v katerih je 6 že omenjenih PLC-jev, nekaj vhodno-izhodnih kart in mrežne karte. Med njimi poteka komunikacija, ki je v osnovi speljana preko »Produced/Consumed« oznak, za varnostni test pa se uporabljajo »MSG« inštrukcije.

Stroj je opremljen s krmilniki proizvajalca Rockwell Automation, in sicer s krmilniki Allen Bradley serije 1756.



Slika 6.10 Uporabljen rack

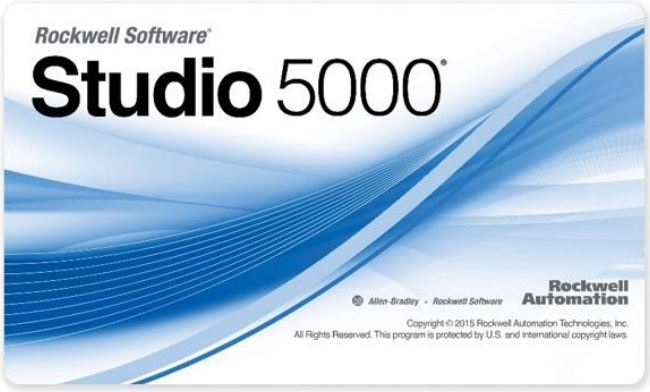
Glavni PLC 1756-L75 (v nadaljevanju PLC1) je najmočnejši krmilnik v racku in ima na voljo 32 MB pomnilniškega prostora. Ta skrbi za osnovno delovanje stroja, poleg tega pa služi tudi prikazu stanj in za delovanje celotne vizualizacije. Znotraj programa na tem krmilniku se izvaja tudi varnostni test. Nekaj varnostnih stanj prebere PLC1 preko komunikacije tudi iz PLC2, ki skrbi za delovanje drugega dela stroja.

Drugi PLC 1756-L63 (PLC2) služi za krmiljenje drugega dela stroja, na voljo pa ima 8 MB prostora. Nanj so vezani vhodi in izhodi, ki so na drugi strani stroja, prav tako pa se na njem izvaja delovanje tega dela stroja.

Drugi štirje krmilniki, ki služijo za delovanje osi in aktuatorjev, na sam varnostni test nimajo vpliva, zato tudi ne bodo posebej obravnavani.

6.3 Programska oprema in program

K uporabi krmilnikov Allen Bradley sodi tudi Studio 5000 Logix Designer. Je ena od aplikacij za konfiguriranje, programiranje in vzdrževanje celotne družine krmilnikov Allen Bradley in povezanih naprav. Program bo napisan znotraj omenjenega programskega okolja.



Slika 6.11 Studio 5000

Program za izvajanje funkcionalnega varnostnega testa se bi po teoriji moral izvajati ročno ali samodejno, in sicer v naslednjih preizkusnih intervalih:

- vsaj vsak mesec za Pl_e s kategorijo 3 ali 4 oz.
- vsaj vsakih 12 mesecev za PL_d s kategorijo 3.

Ker je v standardu določena zgolj mejna vrednost frekvence izvajanja varnostnega testa za določeno raven učinkovitosti, se v praksi ta preizkus izvaja bolj pogosto. Program je zasnovan tako, da se deli na mali in veliki varnostni test. Mali varnostni test, v katerem so zajeta stikala za izklop v sili, varnostni skenerji in varnostne preproge, se začne izvajati avtomatsko znotraj vsake izmene. S tem se zagotovi funkcionalno delovanje varnostno kritičnih elementov.

Veliki varnostni test, ki zajema vse varnostne elemente na stroju, se začne avtomatsko izvajati v tretjem dnevu vsakega tedna. Pri tem se mora preizkusiti celotna varnostna oprema.

Seveda je omogočeno tudi ročno proženje tako malega kot velikega varnostnega testa.

Program za izvajanje funkcionalnega varnostnega testa

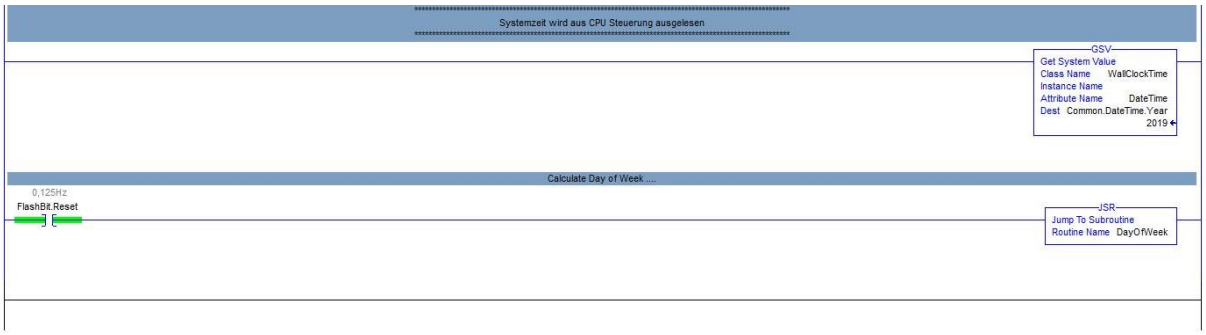
Kot že omenjeno, je program razdeljen na dva PLC-ja.

Program na PLC1

Celoten program za izvajanje varnostnega testa se izvaja na PLC1. Najprej je bilo treba sinhronizirati uro s PLC-jem in jo pretvoriti v strukturo, saj jo lahko le tako uporabimo za program. Struktura je razdeljena na:

- leto,
- mesec,
- teden,
- dan,
- uro,
- minuto in
- sekundo.

To pomeni, da je struktura za sistemsko uro narejena iz sedmih DINT podatkovnih tipov.



Slika 6.12 PLC1 Program 1: Pridobitev sistemske ure z inštrukcijo GSV

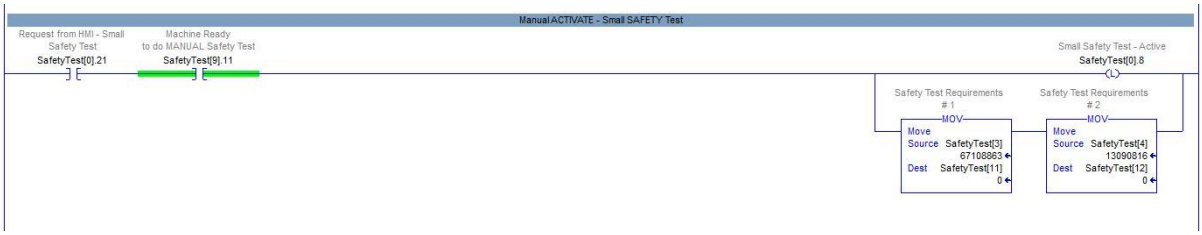
V programu že imamo definirano stanje, ki utripa s frekvenco 0,125 Hz. S tem stanjem sprožimo klic funkcije za določitev časa varnostnega testa.

S programom, predstavljenim na sliki 6.13, dobimo leto in mesec, ki ga prepišemo iz PLC. Za vrednost »DayOfWeek« je določitev težja.

```
(*  Day of Week Routine - rdrast
    This version compensates for leap years and non-leap years, as well as the oddball leap century.

To use this routine, create a DINT array of 12 elements called "MonthValue", and assign it as follows:
MonthValue[0] := 0, 3, 3, 6, 1, 4, 6, 2, 5, 0, 3, 5
The final value, DayOfWeek is just that, Sunday = 0, Monday = 1, etc.
*)

Year         := Common.DateTime.Year;
Month         := Common.DateTime.Month;
DayOfMonth     := Common.DateTime.Day;


IF (((Year MOD 4) = 0) AND NOT ((Year MOD 100) = 0)) OR ((Year MOD 400) = 0)
THEN
    MonthValue[0] := 6;
    MonthValue[1] := 2;
ELSE
    MonthValue[0] := 0;
    MonthValue[1] := 3;
End_If;

DayOfWeek := (DayOfMonth + MonthValue[Month-1] + (Year MOD 100) + ((Year MOD 100) / 4) + 6) mod 7;
```

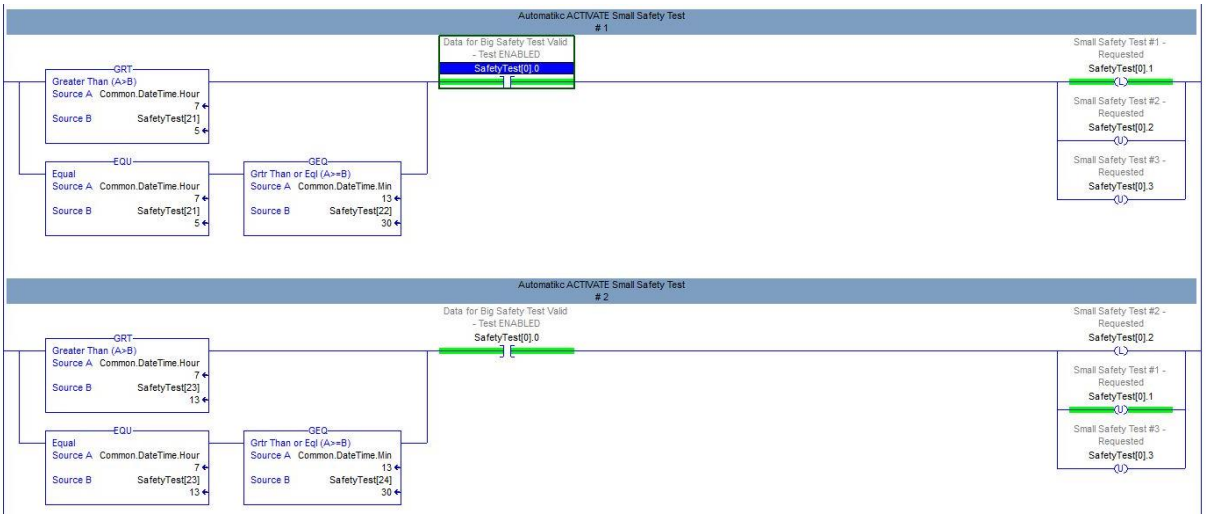
Slika 6.13 PLC1 Program 2: Določitev časa

Za začetek izvajanja varnostnega testa sta na voljo dva režima, avtomatski in ročni. Za proženje ročnega varnostnega testa je na HMI-ju gumb, ki omogoča izvajanje tako velikega kot malega varnostnega testa. Za ročno izvajanje varnostnega testa mora biti dosežen pogoj, da je stroj pripravljen. Sledi sprememba stanja, da je varnostni test aktiven, in zgodi se prepis vrednosti, ki si ga moramo predstavljati v dvojiškem zapisu. Število pove, katere vhode je treba preizkusiti.



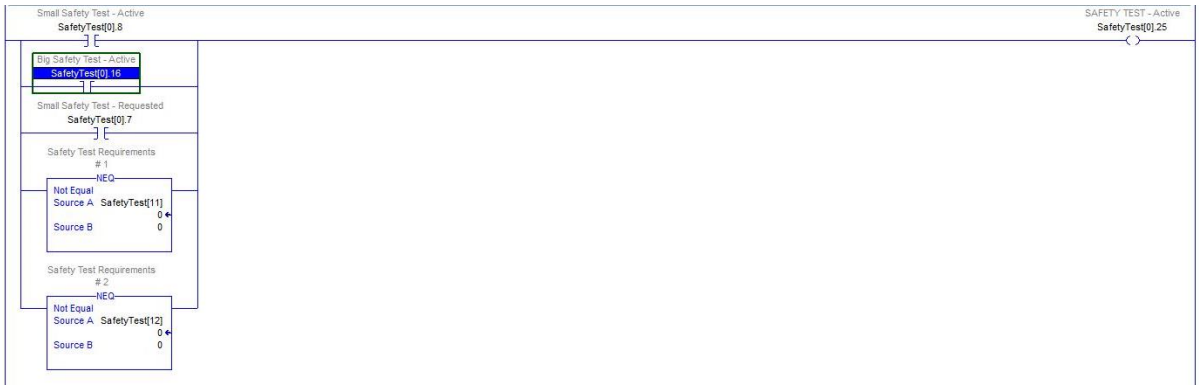
Slika 6.14 PLC1 Program 3: Ročno proženje začetka izvajanja varnostnega testa

Varnostni test se začne izvajati avtomatsko med izmeno. Program je zasnovan tako, da omogoča kar se da enostavno nastavitev ure, ob kateri se izvajanje varnostnega testa zažene. Aktiviran mora biti pogoj, ki določa omogočanje testa. S tem se postavi bit za avtomatsko aktivacijo varnostnega testa.



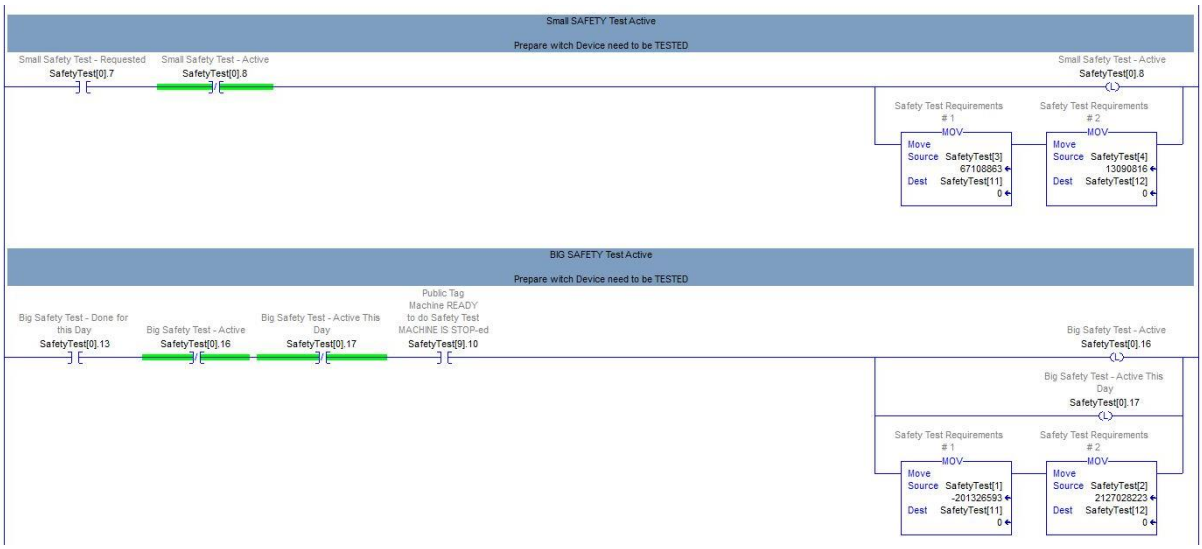
Slika 6.15 PLC1 Program 4: Avtomatska zahteva za začetek izvajanja varnostnega testa

Če je varnostni test aktiven, lahko preverimo z določenimi biti, ki se postavijo z začetkom izvajanja varnostnega testa. Za vsak slučaj se aktivnost varnostnega testa preveri tudi z vrednostmi, ki predstavljajo, kateri varnostni element se znotraj testa preverja. Ti dve vrednosti ne smeta biti enaki 0, kar pomeni, da je preizkus aktiven.



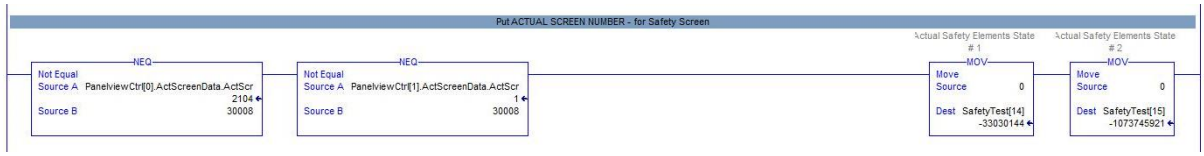
Slika 6.16 PLC1 Program 5: Avtomatski varnostni test aktiven

Ko dobimo signal, da je varnostni test zahtevan in še ni aktiven, se sproži aktivacija varnostnega testa in prepis bitov za preverjanje varnostnih elementov. Za lažje razumevanje se pri tem uporabi priloga [A].



Slika 6.17 PLC1 Program 6: Aktivacija velikega oz. malega varnostnega testa

HMI stroja je sestavljen iz mnogo zaslonov, vendar kot velja že pri programski opremi, tudi tukaj upoštevamo samo zaslon s številko 30008. Če se na HMI pomaknemo z zaslona 30008, na katerem lahko spremljamo varnost stroja in njegovo delovanje, se bo varnostni test ponastavil.



Slika 6.18 PLC1 Program 7: Ponastavitev varnostnega testa

Nekaj varnostne opreme je povezano na PLC2, zato je ta stanja treba prepisati na PLC1, kar storimo z inštrukcijo »MSG«. Znotraj inštrukcije je treba nastaviti pot, po kateri se berejo oz. prepišejo stanja. Določiti je treba tudi, katera stanja oz. tabele se berejo po nastavljeni poti in v katero stanje oz. tabelo se prepišejo. Branje vrednosti se izvaja s hitrostjo 4 Hz.

Slika 6.19 PLC1 Program 8: Branje stanj iz PLC2

Ko so stanja vseh varnostnih elementov na glavnem PLC1, si zaradi manjše možnosti napak ustvarimo prepis vrednosti v polje, ki ga imenujemo »mapping«. Prepisane vrednosti lahko kasneje uporabimo za delovanje varnostnega testa. Za varnostne elemente, ki so povezani na glavni PLC1, uporabljamo kar direktna stanja, medtem ko za varnostne elemente iz PLC2 uporabljamo »SafetySignal« stanja, ki smo jih prepisali v prejšnjem koraku.

Slika 6.20 PLC1 Program 9: »Mappiranje« vhodov v varnostni test

Celotni varnostni test deluje preko polja SafetyTest[20], zato naredimo še prepis varnostnih stanj. Tako dobimo dve polji SafetyTest[14] in SafetyTest[15], ki predstavljata dejansko stanje na varnostnem elementu.

Slika 6.21 PLC1 Program 10: Prepis stanj za izvajanje varnostnega testa

Ko je varnostni test enkrat aktiviran, se morajo preveriti še varnostni elementi. Ti se preverijo s primerjavo vrednosti SafetyTest[14] ali SafetyTest[15] z določeno vrednostjo znotraj bitov v DINT podatkovnem tipu. Vsak DINT ima namreč 32 bitov, ki jih primerjamo kar z vrednostmi. Ko se varnostni test aktivira, se na HMI-ju za določen varnostni element pojavi stanje, ki sporoča, da je varnostni element v fazi testiranja, vendar še ni preizkušen. Ko se varnostni element ponovno sproži, se to stanje na HMI-ju spremeni v stanje, da je varnostni element preizkušen.

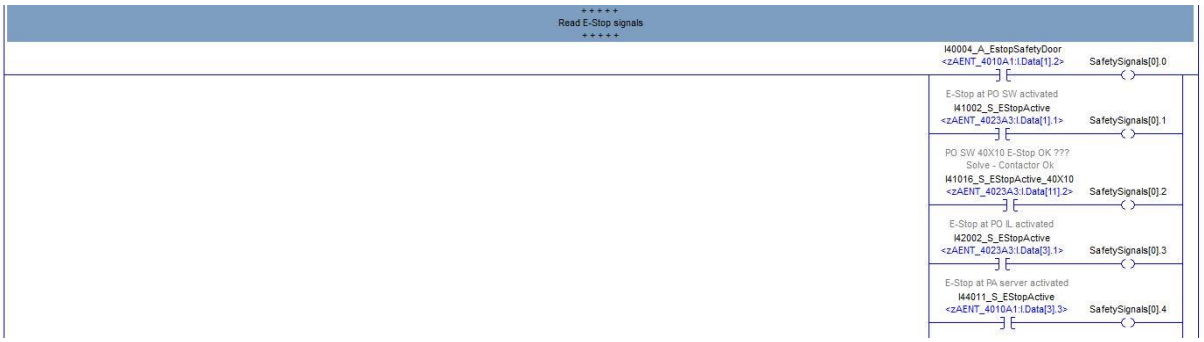
Slika 6.22 PLC1 Program 11: Preverjanje posameznega varnostnega elementa

Če so dobro preskušeni vsi varnostni elementi oz. samo elementi malega varnostnega testa, se postavi bit, ki ponazarja, da so vsi varnostni elementi v dobrem stanju, varnostni test pa je s tem zaključen. To lahko preverimo, ko je SafetyTest[14] in SafetyTest[15] enako FF, kar pomeni, da so vsi biti znotraj DINT podatkovnega tipa enaki 1.

Slika 6.23 PLC1 Program 12: Varnostni test končan – Varnostna oprema = OK

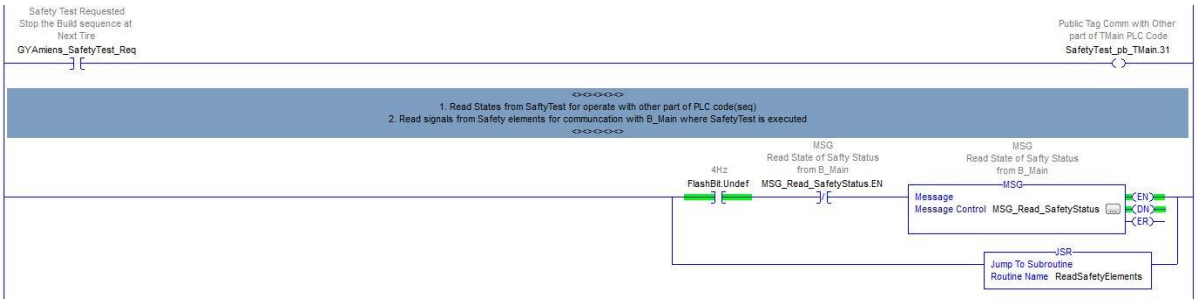
Program na PLC2

Kot že omenjeno, je nekaj varnostnih elementov vezanih na PLC2. Stanja varnostnih elementov tako prepišemo v polji SafetySignals[0] in SafetySignal[1], ki jih beremo preko inštrukcije MSG v PLC1.



Slika 6.24 PLC2 Program 13: Prepis varnostnih elementov v stanja za branje PLC1

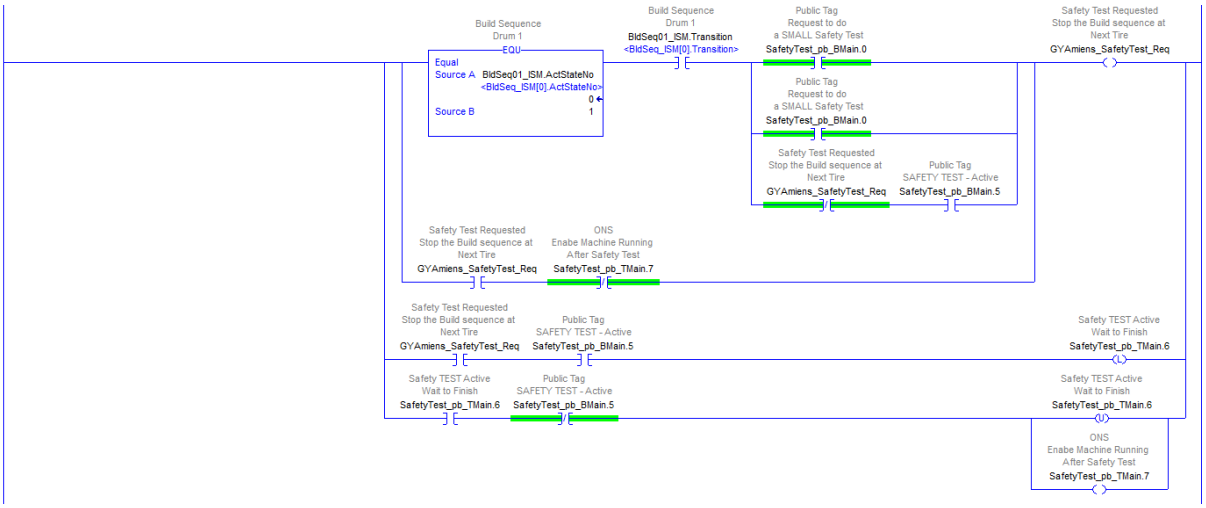
Varnostni test vpliva tudi na sekvenco delovanja drugega dela stroja, zato sta za pogoje delovanja potrebna 2 bita. Eden sporoča, da je varnostni test aktiven, drugi pa, da je varnostni test zaključen. Če je varnostni test aktiven, se sekvenca delovanja ne more začeti izvajati, nasprotno pa velja za bit, ki ponazarja, da je varnostni test končan.



Slika 6.25 PLC2 Program 14: Branje bitov varnostnega testa

Znotraj sekvence delovanja stroja je potrebnih nekaj sprememb.

Tako se v prvem koraku sekvence delovanja stroja preveri, v kakšnem stanju je izvajanje varnostnega testa, in sicer ali obstaja zahteva za varnosti test, ali se ta izvaja, in tako se postavi standardno stanje »GYAmiens_SafetyTest_Req«.

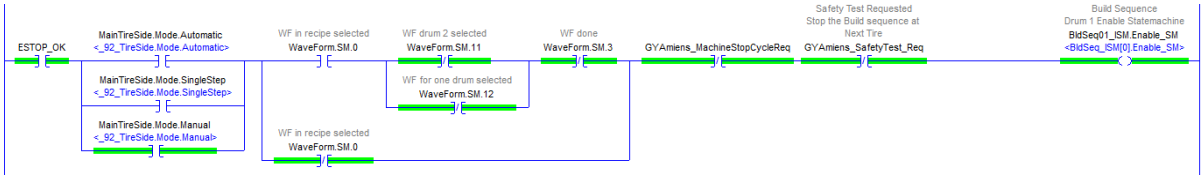


Slika 6.26 PLC2 Program 15: Sprememba sekvence delovanja

Omenjeno stanje pa postavi stroj v pripravljenost za izvajanje varnostnega testa. Pri tem moramo upoštevati, da je stroj v ročnem režimu delovanja in da sekvenca delovanja stroja ni aktivna.

Slika 6.27 PLC2 Program 16: Pogoji za izvajanje varnostnega testa

V zadnjem koraku so tako standardni pogoji za aktivacijo sekvence delovanja doseženi, dodati je treba le še novo stanje, ki ponazarja, da se izvaja varnostni test.



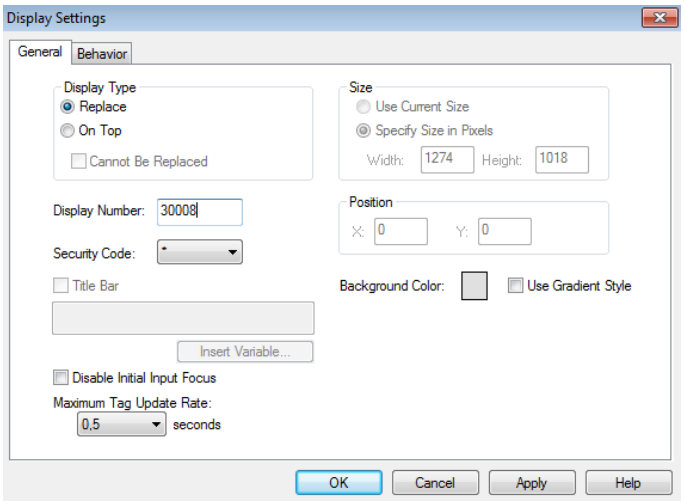
Slika 6.28 PLC2 Program 17: Pogoji delovanja stroja

6.4 Programska oprema za vizualizacijo in kreiranje vizualizacije

Program za izdelavo vizualizacije FactoryTalk View nudi robustno in zanesljivo funkcionalnost v HMI rešitvah. Na voljo so tako samostojni strojno-uporabniški HMI-ji kot tudi porazdeljene vizualizacije. Za naš primer smo uporabili samostojni strojni uporabniški vmesnik. Programski paket poleg celovite rešitve za izdelavo vizualizacije nudi tudi enostavno povezavo z Allen Bradley PLC-ji preko FactoryTalk Linx.

Slika 6.29 FT View Studio

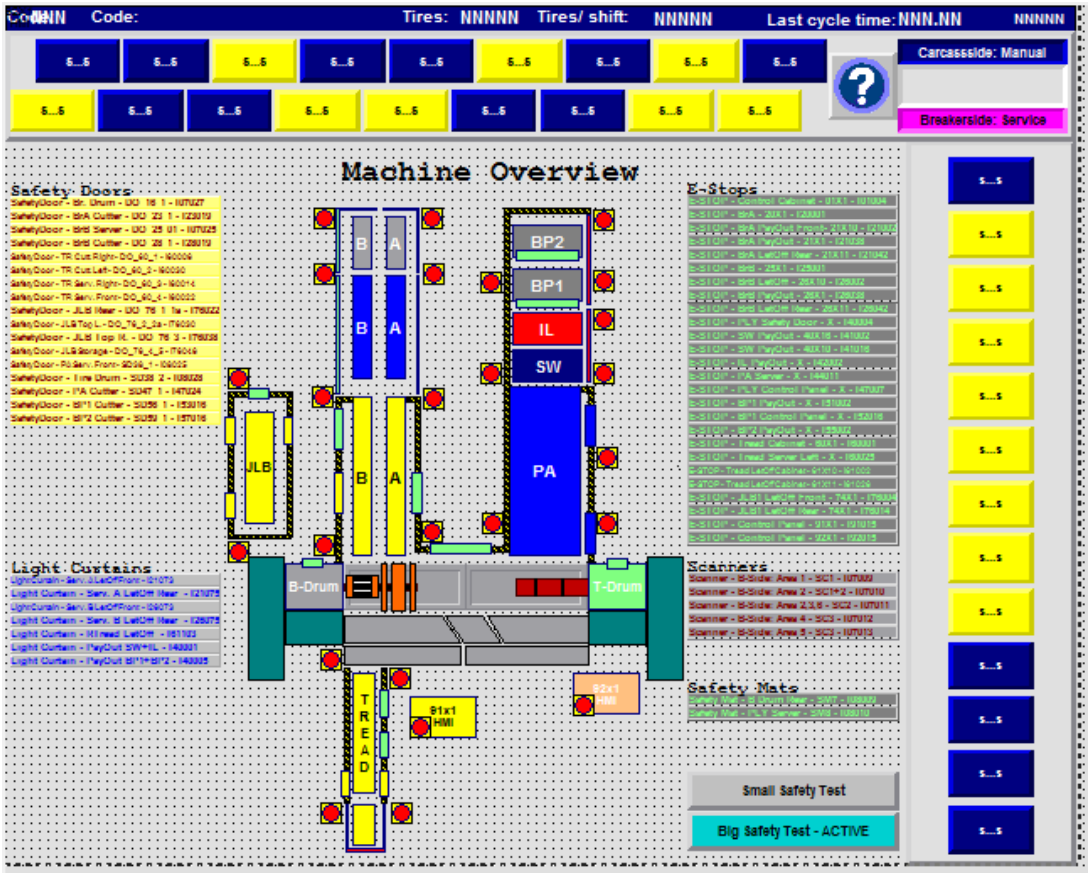
Varnostni test smo integrirali v že obstoječi stroj ter zgolj dodali oz. odstranili nekaj funkcij, podobno smo uredili tudi pri vizualizaciji. Za osnovo smo vzeli osnovno aplikacijo, ki jo je bilo treba zgolj dodelati. Na obstoječe stanje smo tako dodali dodaten zaslon pod številko 30008. Druge nastavitve zaslona, kot so »Display Type«, »Maximum Tag Update Rate« in druge, so ostale enake kot pri drugih že obstoječih zaslonih.



Slika 6.30 Dodaten zaslon za spremljanje varnostne opreme

Celoten sistem je zasnovan tako, da celotna vizualizacija deluje preko CPU1, kar pomeni, da so številke zaslona pomembne, saj lahko z določenimi funkcijami operiramo tudi preko njih.

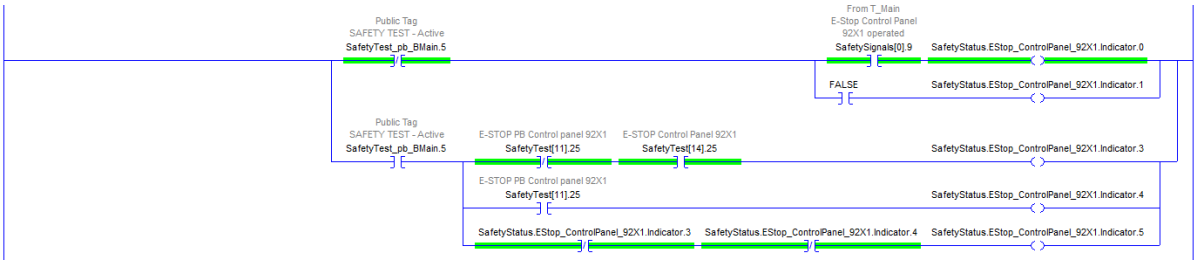
Na novi zaslon smo dodali indikatorje, ki predstavljajo delovanje celotnega stroja. Tako si lahko tudi preko vizualizacije predstavljamo, kateri del stroja obratuje oz. stoji. Celoten stroj sestoji iz več takih sklopov, od katerih ima vsak svojo funkcijo. Vsak sklop je opremljen z varnostno opremo, kot je prikazano na sliki spodaj.



Slika 6.31 Zaslon za spremljanje varnostne opreme

Celoten zaslon obratuje preko večstopenjskih indikatorjev, ki delujejo tako, da neka vrednost predstavlja določeno barvo, stanje, napis. Na zaslonu sta tudi dva gumba za izvajanje varnostnega testa, ki posredujeta tudi povratno informacijo v zvezi z aktivnostjo varnostnega testa.

Za vsak varnostni element smo ustvarili svojo podatkovno strukturo. Struktura je sestavljena iz DINT podatkovnega tipa, ki predstavlja stanje varnostne naprave, in BOOL podatkovnega tipa, ki sporoča, ali je ta naprava dejansko prisotna.



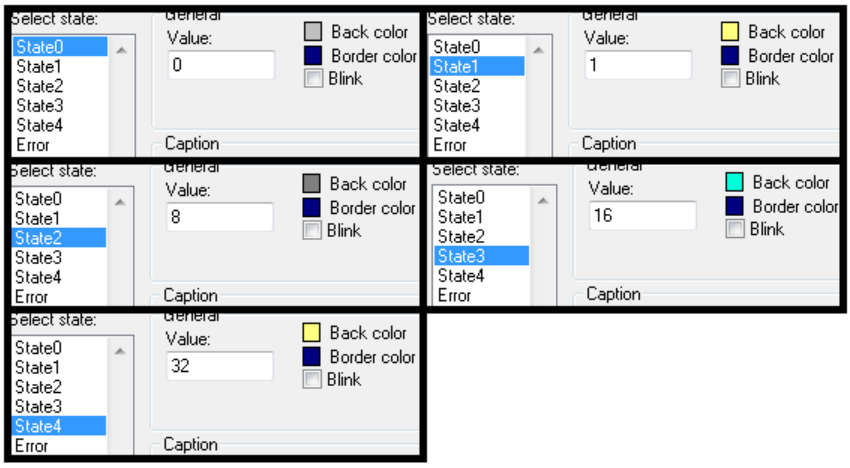
Slika 6.32 PLC1 Program za prikaz stanj varnostne opreme

DINT podatkovni tip za indikacijo varnostne naprave si moramo predstavljati kot številko za prikaz na panelu. Če varnostni test ni aktiven, prikazujemo dejansko stanje varnostne naprave. Ko je bit 0 postavljen, je vrednost števila enaka 1, drugače pa je vrednost števila enaka 0.

Če je varnostni test aktiven, obstaja več možnosti:

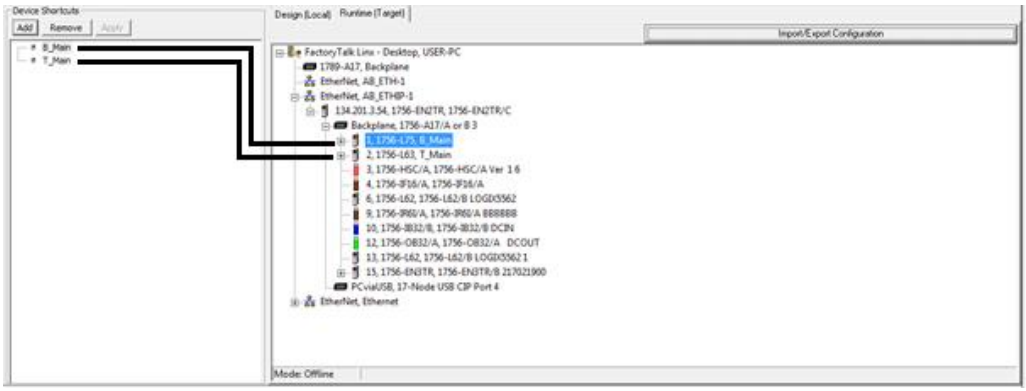
1. možnost: varnostni test je aktiven, varnostne naprave še nismo preizkusili.
2. možnost: varnostni test je aktiven, varnostna naprava je preizkušena.
3. možnost: varnostni test je aktiven, varnostna naprava je preizkušena, vendar je na njej napaka.

Vsako stanje ima znotraj enega večstopenjskega indikatorja svojo barvo, kot lahko vidimo na sliki spodaj. S takšnim večstopenjskim indikatorjem so predstavljene vse varnostne naprave.



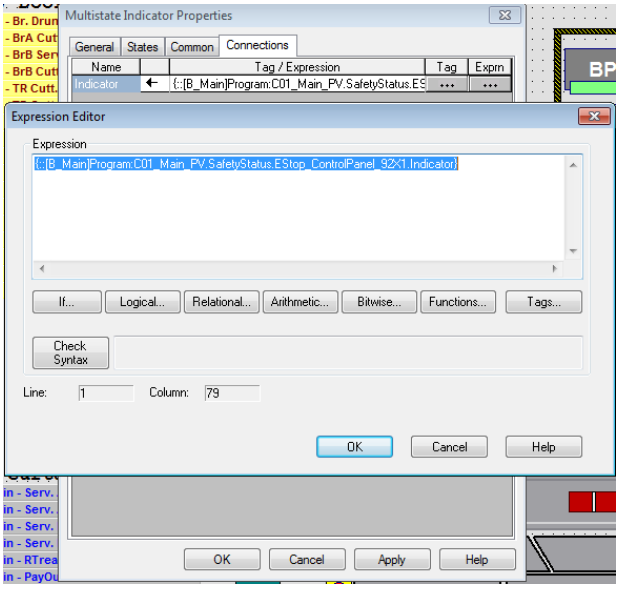
Slika 6.33 Opredelitev barv stanj varnostne opreme, prikazane na zaslonu

Pomembno je omeniti tudi komunikacijo med vizualizacijo in PLC-jem. Nastavitev komunikacije najdemo v drevesni strukturi pod imenom FactoryTalk Linx. Nastaviti je treba ime naprave, ki jo bomo povezali s HMI aplikacijo. V našem primeru imamo 2 PLC-ja z imeni »B_Main« in »T_Main«. Ime na levi strani povežemo s PLC-jem.



Slika 6.34 Nastavitev komunikacije PLC–HMI

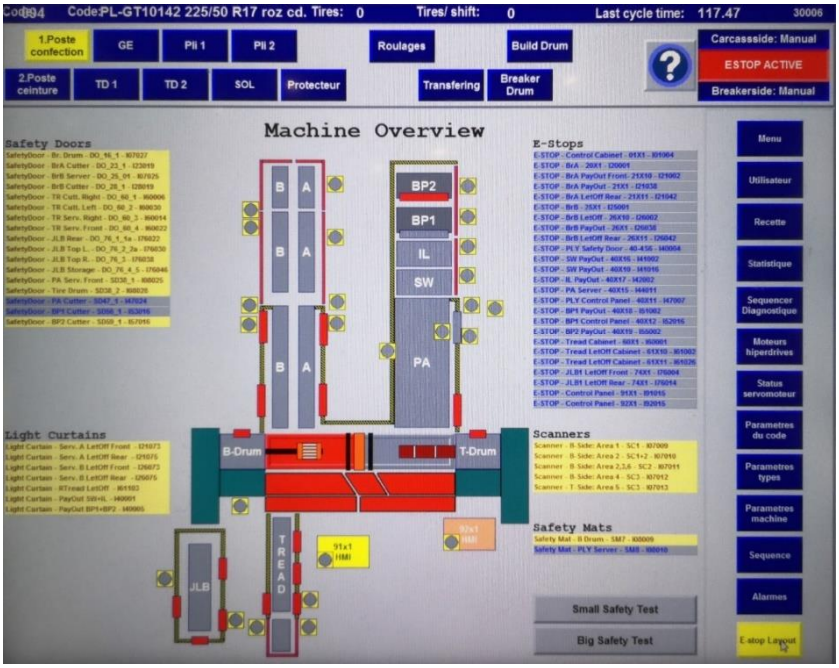
FactoryTalk Studio omogoča, da lahko vizualizacijo kreiramo preko lokalnih spremenljivk ali neposredno iz PLC-ja. Odločili smo se za neposredne spremenljivke, saj je posledično manj dela s kreiranjem dodatnih lokalnih spremenljivk, ki jih je treba na koncu v vsakem primeru povezati s spremenljivkami iz PLC-ja.



Slika 6.35 Uporaba neposrednih stanj

6.5 Testiranje

Zaslon je sestavljen iz navigacijskih tipk zgoraj in ob strani. Z zgornjimi navigacijskimi tipkami se prestavljamo po zaslonih sklopov stroja, navigacijske tipke na desni pa so namenjene za pomikanje med zasloni pregledov in nastavitev. Do varnostnega testa se dostopa z zaslonov »1. Stage« in »2. Stage«, ki sta tudi glavna zaslona oz. glavna pregleda delovanja stroja. Do njiju pridemo preko navigacijskih tipk na desni, med katerimi je tipka za varnostni test oz. varnostni zaslon zadnja oz. spodnja.



Slika 6.36 Pregled dejanskih stanj varnostne opreme

Na zaslonu lahko najdemo stanje vseh varnostnih elementov na stroju, katerih dejansko stanje prikazujejo različne barve.

Tabela barv varnostnih elementov ob oz. na stroju:

- Utripajoča rumena barva – varnostni element se aktivira in se ne ponastavi. Uporablja se za vsa varnostna vrata in svetlobne zavese.
- Utripajoča rdeča barva – varnostni element se aktivira in ne ponastavi curka. Uporabi se za vse gumbe E-stop.
- Siva barva – status varnostnega elementa je v redu.

7 SKLEP

Cilj magistrskega dela je bil razviti in implementirati program za izvajanje varnostnega testa po normah standarda ISO 13849. Za pridobitev podatka glede frekvence izvajanja preizkusov varnostne opreme smo morali standard najprej analizirati. Na začetku smo morali ugotoviti, kaj je funkcionalna varnost in kaj obsega. Spoznali smo, da obstaja znotraj standarda veliko informacij, ki jih je bilo treba obdelati, začenši s PL-om. Ob preučevanju standarda smo spoznali nekaj parametrov, ki so pomembni za funkcionalno varnost, kot so kategorija, $MTTF_d$, DC, CCF in drugi. Prepričali smo se, da varnostni test potrebujemo, saj smo ugotovili, da nobena komponenta ni 100-odstotno zanesljiva niti znotraj svoje življenjske dobe, saj možnost raznih sistematičnih in naključnih napak vedno obstaja.

V magistrskem delu je v prvem delu opisano ozadje funkcionalne varnosti in razlogi, zakaj varnostni test sploh potrebujemo. V drugem delu smo se osredotočili na nadzorni sistem, ki spremlja stanja varnostne opreme in nadzoruje izvajanje varnostnega testa. Te faze smo se lotili s preučevanjem varnostne opreme, ki je na stroju. Varnostni test smo razdelili na malega in velikega, saj vse varnostne komponente niso istega PL-a, dodaten razlog pa je bila tudi boljša učinkovitost. Mali varnostni test obsega tipke za zaustavitev v sili, varnostne skenerje in preproge. Je pomembnejši in se izvaja znotraj vsake izmene, medtem ko se veliki varnostni test, ki zajema vse varnostne elemente, izvede enkrat na teden. Celoten program je bilo treba izvesti tudi v okolju, primernem za operaterje, kar pomeni, da je bilo treba izdelati vizualizacijo. V obstoječe zaslone smo dodali nov zaslon, ki zajema samo varnostno opremo stroja. Na njem se lahko preko tipk začne ročno izvajati varnostni test, poleg tega pa prikazuje tudi stanja vseh varnostnih elementov.

Program smo uresničili do te mere, da omogoča spremljanje stanja varnostne opreme preko OP-ja. Prav tako smo preizkusili delovanje varnostnega testa, pri čemer v fazi testiranja na večje težave nismo naleteli.

V okviru magistrskega dela smo tako spoznali, kako pomembna je funkcionalna varnost strojev v industriji. Poleg tega smo ugotovili še, kako obsežni so standardi, saj so vezani na človekovo zdravje.

8 SEZNAM VIROV

[1] Aleš Kotnik, Zagotavljanje industrijske varnosti. Dosegljivo na: https://dk.um.si/ [Datum dostopa: 19. 5. 2019]

[2] Uradni list Evropske unije, DIREKTIVA 2006/42/ES EVROPSKEGA PARLAMENTA IN SVETA z dne 17. maja 2006 o strojih in spremembah direktive 95/16/ES

[3] International standard ISO 14120:2015, Safety of machinery – Guards – General requirements for the design and construction of fixed and movable guards, dosegljivo na: https://www.sis.se/api/document/preview/919651/ [Datum dostopa: 23. 5. 2019]

[4] Varnost strojev, dosegljivo na: http://lab.fs.uni-lj.si/lasok/index.html/gradivo_jerman_LASOK/TV_1_ZapiskiPredavanj.pdf [Datum dostopa: 26. 5. 2019]

[5] Safety of machinery and work equipment, dosegljivo na: https://oshwiki.eu/wiki/Safety_of_machinery_and_work_equipment [Datum dostopa: 26. 5. 2019]

[6] Physical Hazards of Machinery & Equipment, dosegljivo na: https://ehs.weill.cornell.edu/safety/general-safety/physical-hazards-machinery-equipment [Datum dostopa: 26. 5. 2019]

[7] Industrial safety system, dosegljivo na: https://en.wikipedia.org/wiki/Industrial_safety_system [Datum dostopa: 26. 5. 2019]

[8] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). OJ L 157, 9. 6. 2006 p. 24.

[9] METHODS OF MACHINE SAFEGUARDING, dosegljivo na: https://www.oshatrain.org/courses/mods/726m2.html [Datum dostopa: 28. 5. 2019]

[10] Basics of Machine Safeguarding, dosegljivo na: https://www.osha.gov/Publications/Mach_SafeGuard/chapt1.html [Datum dostopa: 28. 5. 2019]

[11] Introduction to Safety Standards, dosegljivo na: https://www.keyence.com/ss/products/safetyknowledge/introduction/ [Datum dostopa: 29. 5. 2019]

[12] Understanding the Hierarchy of Controls, dosegljivo na: https://machinerysafety101.com/2011/02/28/understanding-the-hierarchy-of-controls/ [Datum dostopa: 2. 6. 2019]

[13] Inherent safety, dosegljivo na: https://www.sciencedirect.com/topics/engineering/inherent-safety [Datum dostopa: 2. 6. 2019]

[14] Risk Assessment, dosegljivo na: https://safetyculture.com/topics/risk-assessment/ [Datum dostopa: 3. 6. 2019]

[15] Risk Assessment, dosegljivo na: https://en.wikipedia.org/wiki/Risk_assessment [Datum dostopa: 3. 6. 2019]

[16] MTTFd, dosegljivo na: https://en.wikipedia.org/wiki/MTTFd [Datum dostopa: 4. 6. 2019]

[17] MTTFd, dosegljivo na: https://machinerysafety101.com/2017/02/13/iso-13849-1-analysis-part-4/ [Datum dostopa: 4. 6. 2019]

[18] DC, dosegljivo na: https://machinerysafety101.com/2017/02/27/iso-13849-1-analysis-part-5/ [Datum dostopa: 5. 6. 2019]

[19] The Parametric Models for Common Cause Failure Analysis, dosegljivo na: https://www.weibull.com/hotwire/issue125/hottopics125.htm [Datum dostopa: 8. 6. 2019]

[20] Checking Emergency Stop Systems, dosegljivo na: https://machinerysafety101.com/2010/07/15/checking-emergency-stop-systems/ [Datum dostopa: 16. 6. 2019]

[21] Category 2 and Testing Intervals, dosegljivo na: https://machinerysafety101.com/2018/05/16/category-2-and-testing-intervals/?doing_wp_cron=1559246529.8076410293579101562500 [Datum dostopa: 20. 6. 2019]

[22] Protective Devices & Emergency Stops - when should we test them, doseglivo na: https://www.spierssafety.co.uk/articles/testing-safety-related-systems [Datum dostopa: 21. 6. 2019]

[23] Testing Emergency Stop Systems, dosegljivo na: https://machinerysafety101.com/2015/04/27/testing-emergency-stop-systems/ [Datum dostopa: 21. 6. 2019]

[24] Darko Dajčman, Tehnični predpisi – Varnost strojev, Gradivo za predavanje

[25] ISO – International Organization for Standardization, dosegljivo na https://www.iso.org/home.html [Datum dostopa: 7. 7. 2019]

[26] International standard ISO 14121-1:2007, Safety of machinery – Risk assessment, Part 1: Principles

[27] International standard ISO 12100-1:2003, Safety of machinery – Basic concepts, general principles for design, Part 1: Basic terminology, methodology

[28] International standard ISO 12100-2:2003 + Amd 1:2009, Safety of machinery – Basic concepts, general principles for design, Part 2: Technical principles

[29] International standard ISO 13849-1:2006 + Cor 1:2009, Safety of machinery – Safety-related parts of control systems, Part 1: General principles for design

[30] International standard ISO 13849-2:2003, Safety of machinery – Safety-related parts of control systems, Part 1: Validation

[31] ISO 13849 – 1 Analysis, dosegljivo na: https://machinerysafety101.com/series/how-to-do-a-13849-1-analysis/ [Datum dostopa: 10. 7. 2019]

[32] Sick – Sensor intelligence, dostopno na: www.sick.com [Datum dostopa: 8. 7. 2019]

[33] International Electrotechnical Commission IEC, IEC 61508 Functional safety

[34] ISO 13849 – 1 Analysis – CCF, dosegljivo na: https://machinerysafety101.com/2017/03/20/iso-13849-1-analysis-part-6-ccf/?doing_wp_cron=1564672632.0005691051483154296875 [Datum dostopa: 10. 7. 2019]

[35] ISO 13849 – 1 Cat. B, dosegljivo na: https://machinerysafety101.com/2010/07/21/interlock-architectures-pt-1-what-do-those-categories-really-mean/ [Datum dostopa: 14. 7. 2019]

[36] ISO 13849 – 1 Cat. 1, dosegljivo na: https://machinerysafety101.com/2010/07/28/interlock-architectures-pt-2-category-1/ [Datum dostopa: 14. 7. 2019]

[37] ISO 13849 – 1 Cat. 2, dosegljivo na: https://machinerysafety101.com/2010/08/24/interlock-architectures-%e2%80%93-pt-3-category-2/ [Datum dostopa: 14. 7. 2019]

[38] ISO 13849 – 1 Cat. 3, dosegljivo na: https://machinerysafety101.com/2011/09/19/category-3-architecture/ [Datum dostopa: 14. 7. 2019]

[39] ISO 13849 – 1 Cat. 4, dosegljivo na: https://machinerysafety101.com/2011/09/26/interlock-architectures-%e2%80%93-pt-5-category-4/ [Datum dostopa: 14. 7. 2019]

[40] International standard ISO 13850, Safety of machinery – Emergency stop – Principles for design

[41] Risk Assessment, dosegljivo na: https://easymanualhandling.com/equipment/risk-assessment/ [Datum dostopa: 24. 7. 2019]

[42] Mehatronika – 1. izd. – Ljubljanja: Pasadena 2009

[43] Factory talk – Manul, dosegljivo na: https://literature.rockwellautomation.com/idc/groups/literature/documents/um/viewme-um004_-en-e.pdf [Datum dostopa: 3. 9. 2019]

[44] Studio 5000 programming – manual, dosegljivo na: https://literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm001_-en-e.pdf [Datum dostopa: 3. 9. 2019]

9 PRILOGA

Priloga [A] – Tabela za izvajanje varnostnega testa – Maska

9.1 PRILOGA [A] – Tabela za izvajanje varnostnega testa – Maska