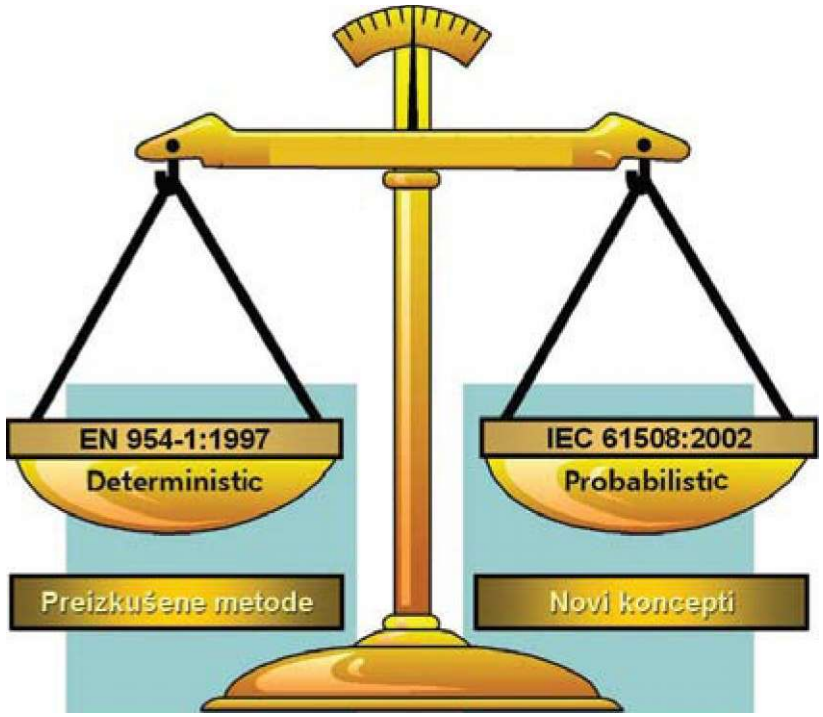
Načrtovanje varnih strojev v skladu s harmoniziranim standardom EN 13849-1

Novi standard EN ISO 13849-1 s področja varnega načrtovanja strojev bo stopil v veljavo 29. decembra 2009 skupaj z uveljavitvijo nove strojne direktive 2006/42/EC, s katero je tudi harmoniziran. Nadomestil bo standard EN 954-1, ki se še vedno uporablja za načrtovanje varnostnih funkcij krmilnih sistemov strojev. Standard je zelo pomemben za razvijalce, konstruktorje, načrtovalce strojev in varnostne inženirje, ki delajo na področju varnosti in zdravja pri uporabi strojev.



Razmerje med deterističnim in verjetnostnim pristopom

AVTOR:
Nešo Savić, univ. dipl. inž. el.,
SICK, d. o. o.,
Cesta dveh cesarjev 403, Ljubljana

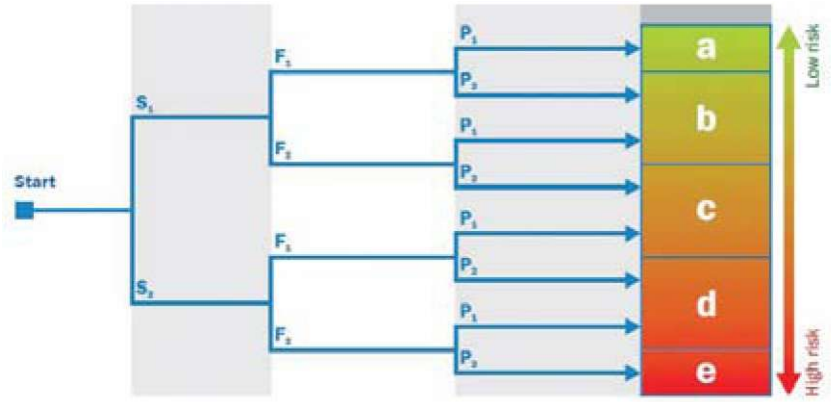
EN ISO 13849-1 se nanaša na varnostne komponente krmilnega sistema. Ta standard lahko uporabljamo za pravilno načrtovanje z varnostjo povezanih delov krmilnega sistema SRP/CS (safety-related parts of controled system). Uporaben je za vse tipe strojev ne glede na vrsto uporabljene tehnologije ali energije, uporabljene za delovanje stroja (električne, hidravlične, pnevmatične, mehanske itd.).

EN ISO 13849-1 združuje vsebino dveh različnih obstoječih standardov: EN 954-1: 1996 in IEC 61508: 1998-2000. Novi standard predstavlja kombinacijo dveh različnih pristopov - determinističnega in verjetnostnega, ki sta uporabljena znotraj omenjenih starih standardov, ter med njima ustvarja določeno ravnotežje.

Novost v standardu EN ISO 13849-1 predstavlja tudi novi grafzaocenotveganja.Parameter, s katerim ocenjujemo tveganje, je označen s PL (performance level). Faktor PL ima drugačen pomen kot varnostna kategorija, ki smo je vajeni iz standarda EN 954-1. Parameter PL nam pove, kakšna je zmožnost sistema SRP/CS, da realiziramo krmilno funkcijo varovanja, da z njo dosežemo pričakovano zmanjšanje tveganja. Sistem SRP/CS je tisti del krmilnega sistema stroja, ki se odziva na varnostne vhodne signale in generira izhodne signale za namene varovanja.

Faktor PL se deli na različne podrazrede: od PL »a« ... do PL »e« in s tem odraža različno zmožnost zmanjšanja preostalih tveganj. Ta se lahko odraža tudi kot verjetnost nastanka nevarne napake na uro PFHd (probability of dangerous failure per hour).

Vsaka varnostna funkcija na stroju, ki izhaja iz analize možnih nevarnosti, mora biti upoštevana



Graf ocene tveganja in faktor PL: S - resnost poškodb; F - čas ali frekvenca izpostavljenosti nevarnim situacijam; P - možnost zmanjšanja (zaznave in umika) nevarnosti

Definicija PL-a v povezavi s PFHd

in ustrezno realizirana. Z ustrezno analizo moramo dokazati, da smo dosegli zahtevani PL naše z varnostjo povezane funkcije krmilnega sistema. Za ustrezno realizacijo so v prvi vrsti potrebne ustrezne komponente oziroma gradniki, ustrezna povezava in programska oprema. Kot primere takih funkcij lahko naštejemo: zaustavitev stroja s pritiskom na tipko STOP, nadzor položaja premikajočih se delov varovalne opreme itd.

Pri načrtovanju in oceni tveganja se pojavi t. i. zahtevani parameter PLr (required Performance Level). Faktor PLr je rezultat ocene vseh tveganj in se nanaša na skupno število vseh izvršenih varnostnih operacij krmilnega sistema za doseganje zmanjšanja tveganja. V fazi načrtovanja, razvoja in proizvodnje stroja moramo doseči vsaj zahtevani nivo varnosti, ki izhaja iz PLr.
Pri ocenitvi in določitvi doseženega nivoja PL nekega dela sistema (kanala) in tudi končnega - skupnega nivoja se upošteva in zajema vse od »senzorja« (detekcije), »logike« (programske logike) do »aktuatorja« (izhodnega stikala). Skupni rezultat je torej kombinacija med deterministčnim in verjetnostnim pristopom, ki se skupno odražata pri določitvi faktorja PL na podlagi naslednjih komponent:

1. kategorija varnosti,
2. faktor MTTFd (mean time to dangerous failure),
3. faktor DC (diagnostic coverage),
4. faktor CCF (common cause failure),
5. preskušanje procesa.

MTTFd (mean time to dangerous failure)
MTTF je statistična vrednost, ki določa pričakovan čas delovanja brez izpadov. Če upoštevamo samo čase, ko pride do nevarnega delovanja oziroma nevarne napake, moramo upoštevati faktor MTTFd (ker ni vsaka napaka varnostnokritična napaka). Velja naslednja relacija: MTTFd > MTTF.
V spodnji tabeli vidimo tipične vrednosti faktorja MTTFd in MTTF elektronskih komponent. Samo elektronske komponente in varnostne naprave imajo že določene vrednosti MTTFd. Te lahko uporabimo kot kazalce za nastale napake, ki so neodvisne od obrabe in naprezanja materialov.

V primeru uporabe elektromehanskih ali hidravličnih naprav kot

Določanje varnostne funkcije sistema SRP/CS

tudi elektromehanskih komponent, kjer moramo upoštevati obrabo in naprezanje različnih komponent, si pri izračunu pomagamo z vrednostmi spremenljivke B10d. To je vmesna vrednost, ki jo uporabljamo za izračun vrednosti MTTFd, kjer upoštevamo pogoje, v katerih je aplikacija: čas trajanja uporabe, povprečen čas zahtevanja varnostne funkcije itd.

Izračun vrednosti MTTFd:
• B10d nam dostavi proizvajalec komponent (vrednost (čas) obratovalnega cikla, v katerem ima statistično 10 % vseh testiranih vzorcev napake).

	Einnpla	MTTF [y]	MTTF„ [y]	MTTF, M wonl cnti	Dmyacus failures
	T01&. T09î. soTza	34.247	68493	6.845	KHt
		1*961	St.WS	3.1«	SC
	KS, KR MKT, MK	JJfiTi	114.1}}	11.416	M «
		ffJ.ISS	îse.in		WW
	SFH Glü	7.646	14,84«	1,464	

Vrednosti MTTF in MTTFd za različne električne komponente

• Srednja vrednost frekvence preklapljanja je odvisna od aplikacije in jo moramo sami določiti: npr. 0,2 Hz, iz česar sledi tcycle = 5s.
• Preračun iz B10d v MTTFd opravimo na naslednji način:

MTTFd = B10d/(0,1* nop)

kjer je:

nop = (dop*hop*3600s/h)/tcycle

nop = povprečna dolžina obratovalnega cikla v letu
dop = srednja vrednost obratovalnih dni na leto
hop = srednja vrednost obratovalnih ur na dan
tcycle = povprečna vrednost zahteve po varnostni funkciji v sekundah (npr. 4 x na uro = 1 x 15 min = 900s)

Diagnostic coverage (DC)

DC [vviļi;*k"r z;u a«J zaznanih ut-viuulli ftlhi-.Mij
Napak* urtutal* z;u adi vseli ii>v,n ulll ritnftfiji

DC je razmerje med vsemi zaznanimi napakami, ki lahko povzročijo nevarno stanje, in vsemi možnimi napakami ter možnostjo, da efektivno zaznamo in odpravimo napake, ki nastanejo v sistemu.
Iz tega lahko predpostavimo, da lahko pride do napak, kot je prikazano v izračunu za faktor MTTFd. Upoštevati pa je treba prav tako, da tudi mehanizmi za detekcijo takih napak med obratovanjem - trajanjem stroja niso enako efektivni in da obstaja možnost, da pride do določenih napak, ki jih ne zaznamo. Tema »prepoznavanje napak« je danes v zvezi z varnostjo še posebej pomembna in govori predvsem o tem, kako se izogniti napakam, da ne pride do njihove akumulacije, ki lahko posledično privede do odpovedi varnostne funkcije.
Pri določitvi faktorja PL moramo upoštevati povprečno vrednost DCavg. Pri tem uporabljamo utežnostne faktorje MTTFd za vsako preskušeno komponento posebej. Iz tega sledi:

Pri nepreskušenih komponentah upoštevamo, da je DC = 0. Tudi pri vseh komponentah, ki ne morejo demonstrirati izločanja napak, upoštevamo DC = 0.

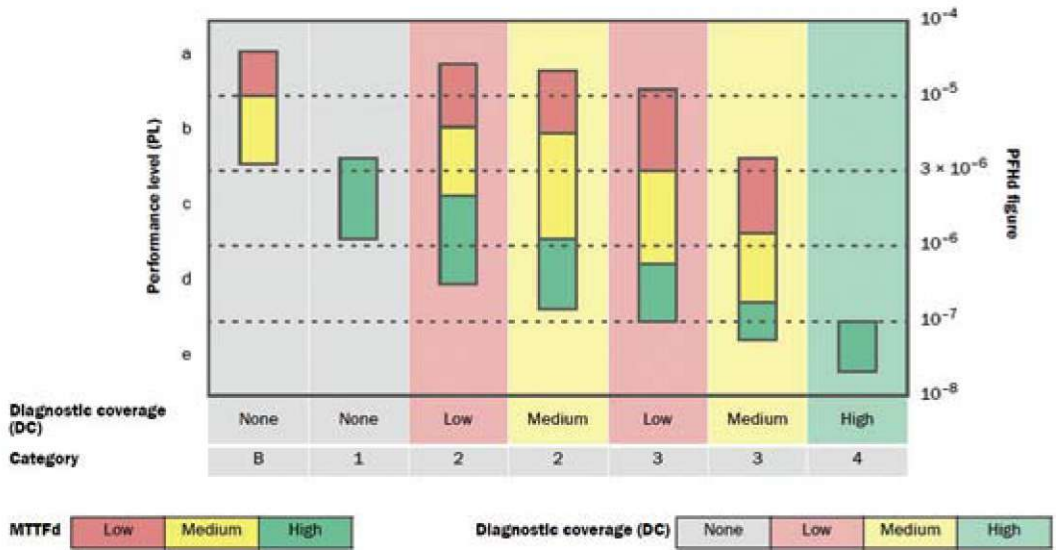
Designation NOTA	Hang« oc^eofe
Lbto	60-.: . DC< SO^i
Mlltfium	
Hitfi	M; DC

Določitev povprečne vrednosti faktorja DC celotnega sistema

CCF (common cause failure)
Common cause failure management (CCF) so napake različnih elementov nekega sistema, ki jih povzroči isti dogodek, vendar napake niso vzrok druga drugi. CCF upoštevamo, če imamo dvokanalne strukture. Take strukture imamo pri varnostni kategoriji 2 in več. Takrat moramo upoštevati ustrezne varnostne ukrepe, ki so namenjeni zmanjšanju napak in njihovih posledic, ki se običajno pojavljajo v takih sistemih. Posledice takih napak običajno pripeljejo oba varnostna kanala do varnostnokritičnih stanj. Do varnostnokritičnih stanj lahko pridemo iz različnih razlogov (npr. različni pogoji osvetlitve lahko vplivajo na preklapljanje stikal (napake) obeh kanalov).
Varnostni ukrepi, ki jih upoštevamo v boju proti takim napakam in imajo različno težo, so lahko:

• izvedemo ločene signalne poti (15 točk),
• uporabljamo raznolike komponente (20 točk),
• zaščitimo sistem proti izpadom/prevelikim pritiskom itd. (15 točk),
• uporabljamo testirane in preskušene komponente (5 točk),
• upoštevamo izobraženost/kompetentnost načrtovalcev (5 točk),
• filtriramo EMC valovanja in naredimo ustrezno zaščito proti motnjam (25 točk),
• preskušamo sistem na spremembe temperature, vibracije, tresljaje itd. (10 točk).

Cilj je doseči vsaj 65 točk.



Poenostavljen graf za določanje faktorja PL

Ko določimo vse ustrezne faktorje, ki določajo PL varnostne krmilne funkcije podsistema ali sistema, lahko iz grafov, ki so podani v standardu, določimo doseženi PL. Če ta ni enak zahtevani vrednosti oziroma PLr, je treba sistem ustrezno spremeniti, dopolniti, dograditi in ponovno preveriti doseženo varnost.

Preskušanje procesa

Na koncu moramo z ustreznimi preskusi preveriti in potrditi, da so bili zgoraj opisani vidiki pravilno implementirani v programsko in strojno opremo. Pomembna je tudi dosledna in dobra dokumentacija, da zagotovimo dobro sledljivost in vse potrebne informacije, pri tem pa upoštevamo različna orodja, ki so opisana v standardu. Prav tako je treba zagotoviti sistematičen nadzor nad ugotavljanjem in spremljanjem napak.

Upoštevati moramo na primer:

- organizacijo in kompetence,
- uporabljena pravila za načrtovanje,
- koncept in merila za preskušanje,
- upravljanje z dokumentacijo.

Zaključek

Standard EN13849-1 prinaša veliko novosti in precej spremenjen koncept načrtovanja z varnostjo povezanih delov in sistemov stroja. Poraja pa tudi veliko novih vprašanj. Številne načrtovalce in proizvajalce zanima predvsem, ali bodo morali popolnoma spremeniti svoje stroje, ki so bili načrtovani na podlagi do sedaj veljavnih standardov. Predpostavimo lahko, da bodo stari stroji ustrezali varnostnim zahtevam novih standardov, če so bili dejavniki, povezani z varnostjo, dobro premišljeni in izpeljani z ustrezno kvalitetnimi gradniki, tako da ne bo potrebnih bistvenih sprememb in popravkov. Predvsem pa je standard pomemben za razvoj novih strojev, kjer bo vedno več z varnostjo povezanih delov in sistemov zgrajenih z elektronskimi in mikroprocesorskimi orodji.