

Funkcijska varnost strojev

S spremembami standardov so bile odstranjene ovire za uporabo elektronskih in programirljivih komponent v varnostnih sistemih strojev, s čimer se je na področju načrtovanja in izgradnje strojev uveljavil nov pojem – funkcijska varnost.



Uvod

Povečanje zanesljivosti elektronskih komponent in potrebe po vedno bolj kompleksnih proizvodnih procesih in avtomatizirani strojni opremi so povzročile tektonske premike tudi na področju uporabe elektronike in informatike pri načrtovanju ter izgradnji z varnostjo povezanih delov krmilnih sistemov strojev. Vse bojazni so bile že pred leti odpravljene in presežene v nekaterih tehnološko najbolj naprednih vejah industrije.

Razvoju so sledile tudi spremembe in prilagoditve v standardih, ki opisujejo osnovna pravila za načrtovanje z varnostjo povezanih delov krmilnih sistemov strojev. Krmilni sistem je lahko niz električnih, elektronskih, pnevmatskih, hidravličnih in mehanskih komponent, ki je načrtovan za upravljanje stroja, tako da ta služi svojemu namenu. Navzven najbolj viden in tudi sicer zelo pomemben del krmilnega sistema so krmilne naprave, s katerimi operater upravlja stroj (zunanj

Avtor:

mag. Ivan Božič, univ. dipl. inž. el.
ZVD Zavod za varstvo pri delu d. d.
Chengdujska cesta 25
1260 Ljubljana Polje

del krmilnega sistema kot vmešnik med strojem in operaterjem). Posebna pravila za načrtovanje krmilnih naprav so podana v prilogi 1 strojne direktive 2006/42/EC, ki je začelo na koncu leta 2009.

V krmilni sistem stroja so pogosto vključene komponente in operacije, ki so namenjene samo preprečitvi nevarnih stanj – to so z varnostjo povezane funkcije oziroma deli krmilnega sistema. Njihova glavna naloga je, da zaznajo nepravilno ali nevarno delovanje stroja in ustrezno aktivirajo varnostni ukrep (pogosto je to ustavitev stroja ali delov stroja), ki naj prepreči nastanek nevarnosti za operaterja. V direktivi najdemo le splošne zahteve, bolj natančna pravila za načrtovanje z varnostjo povezanih delov krmilnega sistema pa najdemo v posebnih harmoniziranih standardih tipa B.

S pravilnim načrtovanjem krmilnega sistema lahko varnost strojev zelo povečamo. Pogoji za to so zlasti primerno načrtovane in izvedene, z varnostjo povezane funkcije krmilnega sistema, ki so ustrezno integrirane v celoten krmilni in napajalni sistem stroja. To je ena od težjih nalog načrtovalcev krmilnih sistemov. Uporabo preizkušenih metod in načel delovanja v skladu z bistvenimi zahtevami stare strojne direktive 98/37/EC je omogočal predvsem standard SIST EN 954-1, ki ga je konec leta 2011 dokončno nadomestil standard SIST EN ISO 13849-1.

Standard SIST EN 954-1 je obrav-

naval 5 kategorij z varnostjo povezanih delov krmilnega sistema (B, 1, 2, 3 in 4). Razvrstitev v ustrezno kategorijo se je izvajala glede na odpornost proti napakam in glede na ravnanje, ki je sledilo po napaki. Slednje je bilo odvisno od strukture z varnostjo povezanih delov, prepoznavo napak in/ali njihovo zanesljivostjo. Kategorije niso opredeljevale stopnje varnosti in niso bile navedene v hierarhičnem zaporedju. Šele ocena tveganja je dala načrtovalcu krmilnega sistema smernice za pravilen izbor varnostnih naprav in njihovo integracijo v celoten krmilni sistem stroja.

V zadnjih desetletjih smo pričeli skokovitemu razvoju elektronike in informatike, ki se vse bolj uporabljata tudi pri avtomatizaciji strojne opreme. Elektronika je dolgo veljala za preveč tvegano za uporabo na področju varnostnih sistemih strojev in zato tudi v varnostnih standardih ni bila dovoljena. Dolgo je namreč veljala za dokaj občutljivo na različne motnje in naj bi kot najšibkejši člen varnostne verige zniževala stopnjo varnosti stroja, kar je začelo zavirati razvoj na tem področju.

Povečanje zanesljivosti elektronskih komponent in potrebe po vedno bolj kompleksni in zmogljivi strojni opremitvi ter vedno višji avtomatizaciji proizvodnih procesov so povzročile velike premike tudi na tem področju. Vse bojazni so bile že pred tem odpravljene in presežene v nekaterih tehnološko najbolj na-

prednih vejah industrije. Razvoju so nujno sledile tudi spremembe in prilagoditve v standardih, ki opisujejo pravila za načrtovanje z varnostjo povezanih delov krmilnih sistemov.

S spremembami standardov ovir za uporabo elektronskih in programirljivih komponent v z varnostjo povezanih delih krmilnih sistemov strojev ni več. Ti so zdaj lahko integrirani v ustrezno načrtovan elektronsko programirljiv krmilni sistem stroja. Z uporabo teh komponent se je na področju načrtovanja in izgradnje strojev uveljavil nov pojem – funkcijska varnost.

Funkcijska varnost strojev

Funkcijska varnost (»Functional Safety«) je tisti del celotne varnosti stroja in krmilnega sistema stroja, ki je odvisen od ustreznega delovanja:

- varnostnih funkcij elektronskega kontrolnega sistema,
- z varnostjo povezanih delov ostalih tehnologij (pnevmatika, hidravlika ...) in
- zunanjih dejavnikov, ki zmanjšujejo tveganja.

Funkcijske varnosti ni mogoče določiti brez upoštevanja sistema kot celote in okolja, ki vpliva na sistem. V nadaljevanju so predstavljene glavne zahteve standarda SIST EN 60204-1, ki so omogočile uporabo principa funkcijske varnosti pri načrtovanju in izgradnji strojev, ter osnovni standardi na tem področju.

SIST EN 60204-1: 2006

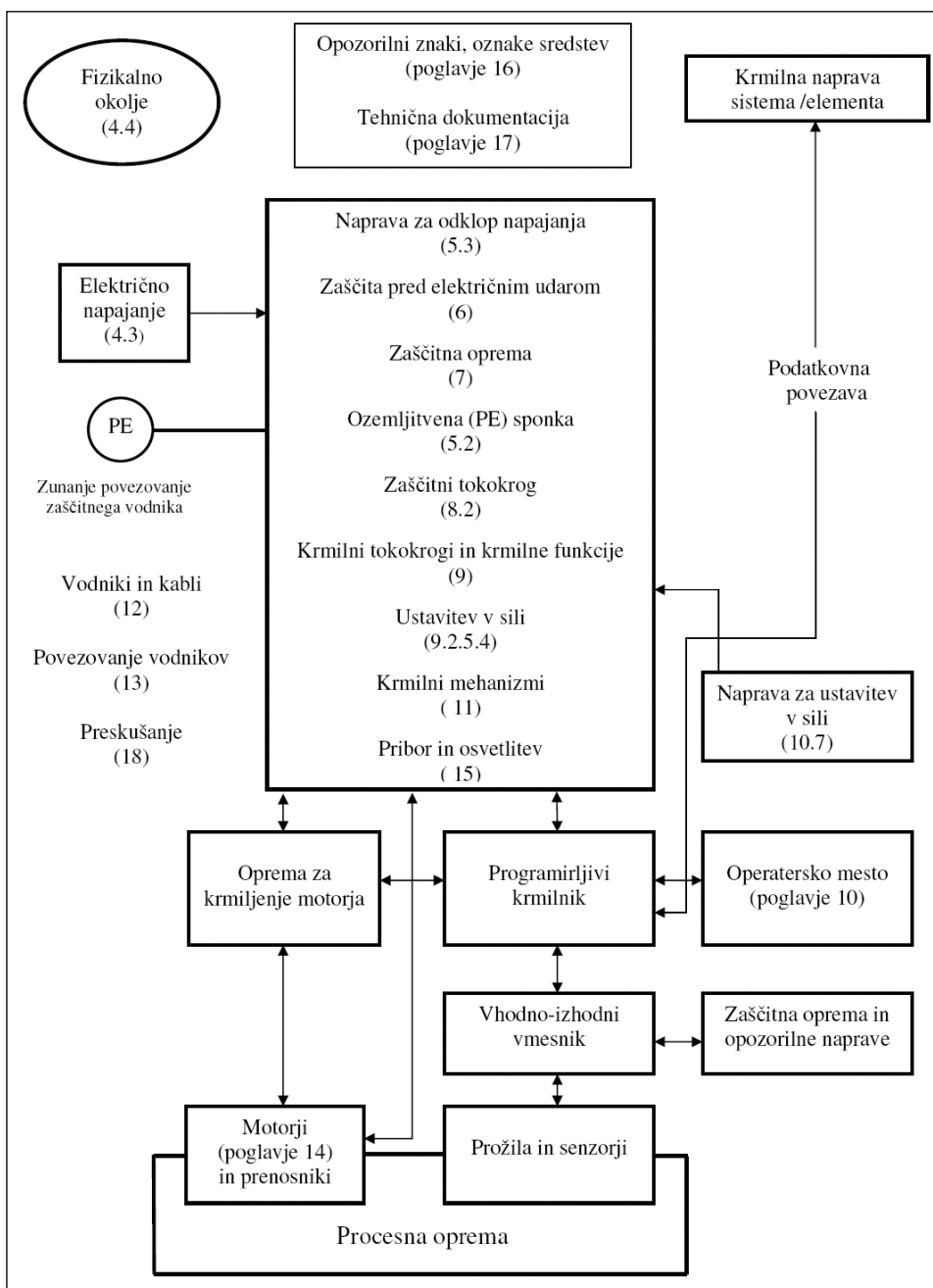
Varnost strojev – Električna oprema strojev

Osnovna pravila o načrtovanju krmilnih sistemov so eno ključnih poglavij standarda SIST EN 60204-1: 2006 Varnost strojev – Električna oprema strojev.

Standard se uporablja za električno, elektronsko in programirljivo elektronsko opremo na strojih, ki med delovanjem niso ročno prenosni, vključujoč skupino strojev, ki delujejo hkrati na usklajen način. Zahteve za opremo se začnejo pri točki priključitve stroja na napajanje. Nanašajo se na električno opremo ali dele električne opreme, ki deluje z nazivno napajalno napetostjo, ki ne presega 1000 V AC oziroma 1500 V DC ter nazivne frekvence do 200 Hz. Osnovni cilji številnih zahtev in priporočil so:

- ustrezna varnost oseb in imetja,
- doslednost krmilnih odzivov,
- enostavnost pri uporabi in vzdrževanju.

Skladnost stroja s standardom pomeni izpolnitev bistvenih varnostnih in zdravstvenih zahtev pravilnika oziroma strojne direktive, ki se nanašajo na električno opremo. Z upoštevanjem standarda so izpolnjene tudi zahteve nizkonapetostne direktive oziroma Pravilnika o električni opremi, ki je namenjena za uporabo znotraj določenih napetostnih mej (Ur. l. RS, št. 27/2004).



Slika 1: Blokovna shema tipičnega stroja (v oklepaju: poglavja in točke standarda SIST EN 60204-1)

Vir: [1]

Blokovna shema električne opreme tipičnega stroja je predstavljena na sliki 1. Na shemi so podana tudi osnovna poglavja standarda, med katerimi se številna neposredno ali posredno nanašajo na električni del krmilnega sistema.

Bistvene spremembe standarda SIST EN 60204-1:2006 glede na predhodno izdajo v zvezi s krmilnimi sistemi:

- nova določila omogočajo uporabo elektronske in programirljive opreme za zagotavljanje varnosti,

- izvedbo varnostnih krmilnih funkcij ustavitv v sili in ostale varnostne izklope (varnostna stikala, svetlobne zavese, fotocelice ...) je dovoljeno izvajati z električnimi in elektronskimi sredstvi,
- elektronska krmilna vezja morajo imeti ustrezno stopnjo varnosti, ki je bila določena s postopkom ocene tveganja. Upoštevati je treba zahteve standardov IEC 62061 in/ali ISO 13849-1, ISO 13849-2.

Standardi na področju funkcijske varnosti strojev

Točni naslovi (slovenski prevod in izvirno v angleščini) in letnice trenutno veljavnih izdaj najpomembnejših standardov na področju načrtovanja funkcijske varnosti strojev:

SIST EN 61508-1:2007 – Funkcijska varnost električnih/elektronskih/programirljivih elektronskih varnostnih sistemov – 1. del: Splošne zahteve (IEC 61508-1:1998 + popravek 1999)

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

SIST EN 61511-1:2007 – Funkcijska varnost – Sistemi z varnostnimi instrumenti za sektor procesne industrije – 1. del: Okvirno, definicije, sistem, zahteve za strojno in programsko opremo (IEC 61511-1:2003 + popravek 2004)

Functional safety - Safety instrumented systems for the process

industry sector - Part 1: Framework, definitions, system, hardware and software requirements (IEC 61511-1:2003 + corrigendum 2004)

SIST EN 62061:2005 – Varnost strojev – Funkcijska varnost na varnost vezanih električnih, elektronskih in programirljivih elektronskih krmilnih sistemov

Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

SIST EN ISO 13849-1:2006 – Varnost strojev – Z varnostjo povezani deli krmilnih sistemov – 1. del: Splošna načela za načrtovanje Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

SIST EN ISO 13849-1:2006

Standard določa varnostne zahteve in navodila za načrtovanje in vključevanje z varnostjo povezanih delov krmilnih sistemov za vse vrste strojev, vključno z načrtovanjem in zasnovo programske opreme, ne glede na vrsto tehnologije in energije, ki je pri tem uporabljena (električna, hidravlična, pnevmatska, mehanska itd.).

Če je bila izbira ustreznih varnostnih kategorij v preteklosti predvsem kvalitativnega značaja, je zdaj vedno bolj v ospredju kvantitativno določanje varnostnih zahtev za stroje, ki temelji predvsem na izračunu verjetnosti nevarne napake varnostnega sistema stroja. Standard SIST EN ISO 13849-1 uvaja namesto varnostnih kategorij ravni oziroma nivoje zmogljivi-

“generični”
električni
krmilni
sistemi



IEC/EN 61508 -

“procesni”
električni
krmilni
sistemi



IEC/EN 61511 -

“stroji”
električni
krmilni
sistemi



IEC/EN 62061 -

“stroji”
krmilni
sistemi
(vse tehnologije)



EN 954/ISO 13849

SIL

PL

Slika 2: Funkcijska varnosti strojev – najpomembnejši standardi in področje uporabe

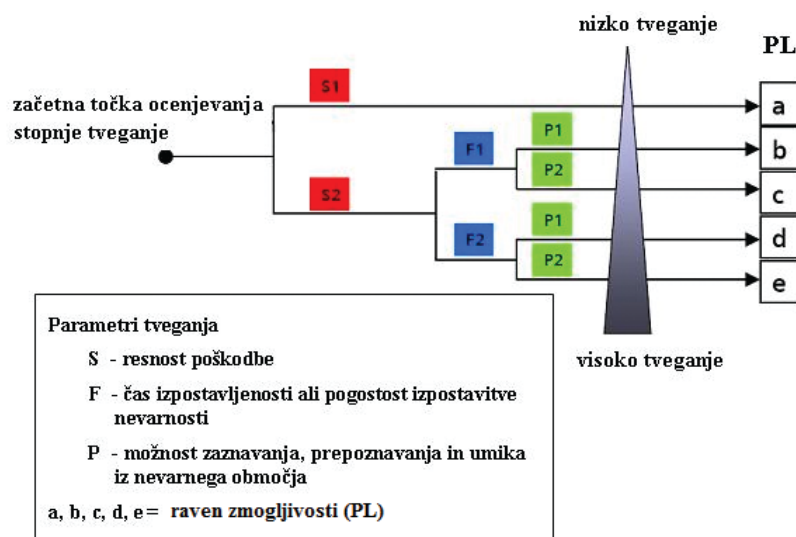
vosti (»Performance Level« – PL) a, b, c, d, e. Ravni/nivoji zmogljivosti so diskretne stopnje, ki določajo sposobnost z varnostjo povezanih delov krmilnega sistema, da izvedejo varnostno funkcijo pod predvidljivimi pogoji. Merilo za razvrstitev osnovnih komponent je verjetnost nevarne napake na uro (»Probability of dangerous Failure per Hour« (PFH)), tabela 1, ki jo lahko izračunamo tudi na podlagi povprečnega časa do odpovedi (»MeanTime To Failure« – MTTF).

PL	Povprečna verjetnost nevarne napake na uro – PFH (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 1: Merilo za uvrstitev v raven/nivo zmogljivosti (PL) je povprečna vrednost PFH

Vir: [3]

Podobno kot v standardu SIST EN 954-1 imamo tudi v novem SIST EN ISO 13849-1 graf tveganja (slika 3), s pomočjo katerega se zdaj namesto varnostne kategorije določi PL za posamezne podsisteme in sisteme z varnostjo povezanih delov krmilnih sistemov. Standard podaja tudi navodila in metode za določanje parametrov, ki vplivajo na določitev PL, tako za posamezne dele in komponente krmilnega sistema kot tudi za z varnostjo povezane dele kot celoto.



Slika 3: Graf tveganja za določanje ravni/nivojev zmogljivosti (PL)

Vir: [3]

Uvajanje standarda prinaša na področju strojev nove postopke pri načrtovanju z varnostjo povezanih delov krmilnih sistemov. Gre za iterativni proces v šestih korakih:

1. definiranje varnostnih zahtev,
2. določitev zahtevane ravni/nivoja zmogljivosti PLr,
3. načrtovanje in tehnična realizacija varnostnih zahtev,
4. določitev in ocenitev dosežene ravni/nivoja zmogljivosti PL,
5. verifikacija,
6. validacija.

Postopki so zelo zahtevni, zlasti pri bolj kompleksnih strojih. Poleg dobrega poznavanja področja ocenjevanja tveganj ter poznavanja vsebine in zahtev ustreznih direktiv in standardov zahtevajo številne vhodne podatke o sestavnih delih stroja, zlasti o delih krmilnega sistema, in tudi okolja, v katerem se stroj načrtuje in v katerem bo uporabljen. Na voljo je že nekaj programskih okolij z bogatimi bazami podatkov o sestavnih delih krmilnih sistemov, ki lahko zelo olajšajo delo načrtovalcem strojev.

SIST EN 61508-1:2007 (IEC 61508-1:1998 + popravek 1999)

Standard obravnava funkcijsko varnost električnih, elektronskih in programirljivih elektronskih varnostnih sistemov in je nastal predvsem v procesni, zlasti kemijski industriji. Namenjen je proizvajalcem kompleksnih elektronsko vodenih procesnih sistemov in v manjši meri strojni industriji. Standard zato tudi ni harmoniziran s strojno direktivo. Uvaja pojem življenjskega cikla sistema, ko je ta pomembno povezan z električno, elektronsko in/ali programirljivo elektronsko opremo. Standard se je razširil tudi na z varnostjo povezane sisteme, kjer se uporablja druga tehnologija.

Varnostne zahteve za celoten sistem so določene na podlagi posameznih podsistemov, ki so opredeljeni z ustreznimi ravnmi/nivoji integritete varnostnega sistema (»Safety Integrity Level« – SIL). Nivoji niso povsem primerljivi z varnostnimi kategorijami po SIST EN 954-1 in ravnmi/nivoji zmogljivosti po SIST EN ISO 13849-1. Parametri za določitev oziroma razvr-

Safety Integrity Level (SIL)	Povprečna verjetnost nevarne napake na uro – PFH (1/h)	
	Kratki časi izpostavljenosti	Pogosta ali neprestana izpostavljenost
SIL 4	10^{-5} do 10^{-4}	10^{-9} do 10^{-8}
SIL 3	10^{-4} do 10^{-3}	10^{-8} do 10^{-7}
SIL 2	10^{-3} do 10^{-2}	10^{-7} do 10^{-6}
SIL 1	10^{-2} do 10^{-1}	10^{-6} do 10^{-5}

Tabela 2: Razvrstitev v SIL na podlagi PFH glede na čas izpostavljenosti operaterja

Vir: [2]

stitev z varnostjo povezanih delov stroja v določen SIL so odvisni tudi od časa oziroma pogostosti izpostavljenosti operaterja določeni nevarnosti. Osnovni kriterij za razvrstitev je tudi tu verjetnost nevarne napake na uro – tabela 2.

Določila in kriteriji za načrtovanje funkcijske varnosti električnih/elektronskih/programirljivih elektronskih varnostnih sistemov so se s standardom SIST EN 61508-1 s procesnokrmilnih razširila tudi na druga tehnološko strojna področja. Tako je na primer pri dvigalih že nekaj časa mogoče vgrajevati varnostne komponente, ki ustrezajo določenim nivojem integritete varnostnega sistema, ki so povzeti po tem standardu.

Približna primerjava oziroma ekvivalenca med kategorijami po SIST EN 954-1, nivoji zmogljivosti (PL) po SIST EN ISO 13849-1 in nivoji integritete varnostnega sistema (SIL) po SIST EN 61508-1 so podani v tabeli 3.

Kategorija B	PL a	-
Kategorija 1	PL b	SIL 1
Kategorija 2	PL c	
Kategorija 3	PL d	SIL 2
Kategorija 4	PL e	SIL 3

Tabela 3: Približna ekvivalenca med klasičnimi kategorijami, nivoji zmogljivosti in nivoji integritete

SIST EN 62061:2005

Standard SIST EN 62061 z naslovom Varnost strojev – Funkcijska varnost na varnost vezanih električnih, elektronskih in programirljivih elektronskih krmilnih sistemov je namenjen načrtovalcem električnih krmilnih sistemov strojev in manj kompleksnih krmilnih sistemov v strojništvu, ki vsebujejo tudi z varnostjo povezane krmilne funkcije. Za bolj kompleksne proizvodne sisteme se uporablja že omenjeni SIST EN 61508-1, ki je tudi pomembna referenca za nekatere vsebine standarda EN 62061. Standard je pospešil revizijo standarda o električni opremi strojev SIST EN 60204-1 in zamenjavo SIST EN 954-1 s standardom SIST EN ISO 13849-1, ki namesto varnostnih kategorij vpeljuje kvantitativno določene nivoje zmogljivosti (PL).

Najpomembnejše vsebine standarda so naslednje:

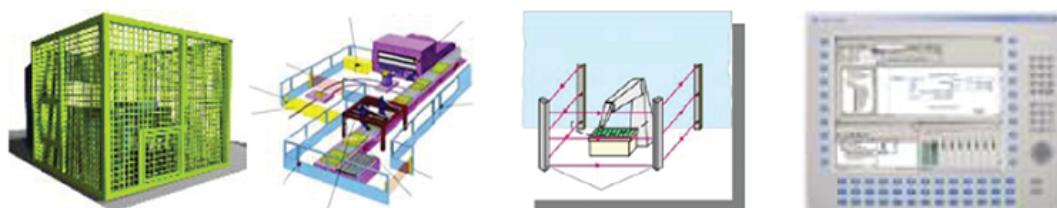
- podaja potrebne vodstvene in tehnične aktivnosti, ki jih morajo izvajati proizvajalci varnostnih naprav in krmilnih sistemov, da lahko dosežejo zahtevano funkcijsko varnost svojih proizvodov,
- skladno z zahtevami standarda

SIST EN 12100 določa postopke ocene tveganja, ki vodijo do sistematične izbire ustreznih nivojev integritete varnostnega sistema (SIL), s čimer se ustrezno zmanjša ali odpravi tveganje,

- določa postopke za kontrolo in preizkušanje krmilnih sistemov, da se zagotovi zahtevane in načrtovane varnostne nivoje, ki morajo biti zagotovljeni tudi po spremembah in modifikacijah,
- določa zahteve v zvezi z dokumentacijo, ki mora biti predana skupaj s strojem.

Zaključek

S trenutno veljavnimi standardi s področja krmilnih sistemov strojev so že nekaj let odstranjene ovire za uporabo elektronskih in programirljivih komponent v varnostnih sistemih strojev, s čimer se je na področju načrtovanja in izgradnje strojev uveljavil nov pojem – funkcijska varnost. Skupaj z napredno tehnologijo to omogoča gradnjo varnih in visokoproduktivnih strojev z zmogljivimi krmilnimi sistemi, v katere so integrirane tudi z varnostjo povezane krmilne funkcije.



varnostni princip	Machine Guarding	Control Interlocking	Operator Sensing	Integrated Systems Functional Safety
glavni cilji	Safety	Safety + Productivity	Safety + More Productivity	Increased Safety due to Flexibility + Productivity + Integration
uporabljene naprave tehnologije	Gates & Locks	- Interlock Switches - Safety Relays - Cable Pull Switches - Trapped Key	- Safety Light Curtains - Laser Scanners - Safety Mats - Conditional Access - Safety Controllers	- Safety PLC - Safety Networking - Networked Components - Intelligent Safety - Machine Metrics - Operator Status
osnovni standardi		National standards – then emergence of EN 292, EN 954, EN 1050 etc		Functional Safety Stds e.g IEC/EN 61508, 62061 + Device Specific Stds + Appl. Specific Stds

Slika 4: Razvojna obdobja pri načrtovanju in izgradnji strojev

Vir: [8]

Literatura

[1] SIST EN 60204-1: 2006 Varnost strojev – Električna oprema stroje – Osnovna pravila o načrtovanju krmilnih sistemov so eno ključnih poglavij standarda SIST EN 60204-1: 2006 Varnost strojev – Električna oprema strojev.

[2] SIST EN 61508-1:2007 – Funkcijska varnost električnih/elektronskih/programirljivih elektronskih varnostnih sistemov – 1. del: Splošne zahteve (IEC 61508-1:1998 + popravek 1999).

[3] SIST EN ISO 13849-1:2006 – Varnost strojev – Z varnostjo povezani deli krmilnih sistemov – 1. del: Splošna načela za načrtovanje.

[4] SIST EN 61511-1:2007 – Funkcijska varnost – Sistemi z varnostnimi instrumenti za sektor procesne industrije – 1. del: Okvirno, definicije, sistem, zahteve za strojno in programsko opremo (IEC 61511-1:2003 + popravek 2004).

[5] SIST EN 62061:2005 – Varnost strojev – Funkcijska varnost na varnost vezanih električnih, elektronskih in programirljivih elektronskih krmilnih sistemov.

[6] Machine safety guide, Schneider Electric, 2012, <http://www2.schneider-electric.com>.

[7] Guidelines for Safe Machinery – Six Steps to a Safe Machine, SICK, 2013, www.sick.com > ... > Home >

Products > Product Portfolio.

[8] <http://www.rockwellautomation.com>.