Funkcionalna varnost

Marjan Kreslin, u.d.i.e.
Fakulteta za elektrotehniko, računalništvo in informatiko
Smetanova 17, 2000 Maribor, Slovenija
Lek Farmacevtska družba d.d.
FAU, Proizvodnja Lendava
Trimlini 2d, 9220 Lendava, Slovenija
marjan.kreslin@lek.si

Functional safety

Abstract: What is functional safety? Functional safety is the probability that a process functions correctly and safely.The goal of safety technology is to keep the potentional hazards for man and the environment as low as possible by applying and utilizing the appropriate technology.

1 Kaj je funkcionalna varnost?

Cilj varnih tehnologij je, da se potencialne verjetnosti za poškodbe ljudi in možni škodljivi vplivi na okolje vzdržujejo na najnižjem možnem nivoju. Danes se pojavljajo vedno višje zahteve po varovanju ljudi in okolja. Posamezne države področje regulirajo z različnimi zakonskimi predpisi. Pri nas je to Zakon o varnosti in zdravju pri delu. Ker pa je vse več družb povezanih z zunanjimi podjetji, tako preko partnerskih poslovnih odnosov kot tudi lastninskih, v uveljavljanje prihajajo tako interni akti teh družb, prav tako pa tudi nacionalni predpisi njihovih držav in držav na katerih tržiščih podjetja nastopajo. Enako velja tudi glede prilagajanja zakonodaji EU. Za podjetja pa ni pomembno le varovanje zdravja ljudi in varovanje okolja, pomembna je tudi poslovna varnost. V primerih havarij prihaja tako do poškodb ljudi, okolja kot tudi do izpadov poslovne dejavnosti. To je danes, v času trdega boja za obstoj podjetij, ohranjanja tržnih deležev in konkurenčnih prednosti, izredno pomemben dejavnik, ko se razmišlja o nivoju varnosti v proizvodnih procesih.

Do danes je bila najpogostejša praksa ustrezno zavarovanje ljudi in premoženja. Predvsem zavarovalne premije za premoženje, ki so primerno visoke, so breme za poslovanje malih, srednjih pa tudi velikih podjetij. Zato se jih vse več, predvsem pa tista, ki so kapitalsko povezana z zunanjimi družbami, odloča za ukinjanje teh zavarovanj. S tem prehajajo finančne odgovornosti za kritje škodnih primerov v primeru havarij neposredno na podjetja, to pa so tudi razlogi, da se na varnostne sisteme glede z drugačnimi očmi.

Ocene tveganja

Skozi ocene tveganja in raziskavo najneugodnejših situacij se danes izdelujejo scenariji vplivov možnih havarij na varnost, zdravje ljudi, varovanje okolja in poslovno uspešnost podjetij. Take študije prinašajo zahteve po dodatnih tehnoloških in tehničnih ukrepih za zmanjševanje tveganj. Predvsem analize potencialnih povzročiteljev nevarnosti, nas vodijo do obravnavanja različnih načinov varnosti. Srečujemo se s termini požarne varnosti, varnosti pred nastankom eksplozije, kemične varnosti, biološke varnosti, električne varnosti in tudi **funkcionalne varnosti**. O funkcionalni varnosti govorimo takrat, ko je posledično varnost v najširšem pomenu besede odvisna od pravilnega delovanja naprav. Vsaka okvara oz. nepravilno delovanje pa ima lahko za posledico ogrožanje zdravja ljudi, škodljiv vpliv na okolje in uničenje premoženja.

2 Industrija in funkcionalna varnost

Vsakdo ki se ukvarja z avtomatizacijo v proizvodnih procesih in vzdrževanjem sistemov

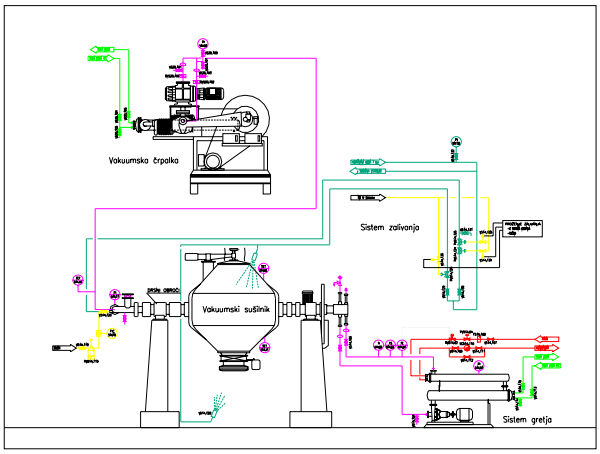
za nadzor in vodenje, se je prav gotovo že srečal z vprašanji kot so:

- Ali je sistem avtomatizacije ustrezen?
- Ali je dovolj zanesljiv in varen?
- So izbrane komponente zanesljive?
- Kakšne so posledice v slučaju nedelovanja?
- Ali se napake lahko hitro odkrijejo in odpravijo?

To so vprašanja, ki jih imamo več ali manj pred sabo v odvisnosti od tega kakšen sistem gradimo in za kakšno funkcijo. Dostikrat so nam pri odločitvah v pomoč interni standardi, ki veljajo za določeno vejo industrije (primer jederskih elektrarn, ki imajo lastne standarde v zvezi z varnostjo, eksplozijsko nevarna območja v industriji za katera prav tako veljajo posebni predpisi, avtomatizirana skladišča kjer ni vprašanje ali se bo postavil redundanten sistem nadzora ali ne in podobno) in narekujejo nivo kompleksnosti sistemov. Vendar pa ni povsod tako. Kjer ni posebnih predpisov, je vsaka odločitev o tem eno veliko tehtanje med kompleksnostjo in varnostjo sistemov ter njihovo ceno. Resnici na ljubo je že tako, da raje investiramo nekaj manj kot pa kaj preveč. Pa to ni edina dilema. Ko smo se že odločili, predvsem preko ocen tveganj (tu je potrebno slediti smernicam), da je potrebno postaviti zanesljiv kompleksen sistem, pridemo do vprašanja o izbiri komponent. So ustrezne za predvideni namen? So dovolj zanesljive in varne?

Poglejmo si primera iz prakse. ki sta se zgodila na isti napravi. Gre za rotacijski vakuumski sušilnik za sušenje produkta, ki je prepojen z organskimi topili. Celoten proces poteka, zaradi prisotnosti topil, v eksplozijsko nevarnem območju.

Slika 1 shematsko prikazuje sušilnik in sistem aktivne požarne zaščite. Sam proces sušenja je kontroliran s tremi med seboj neodvisnimi temperaturnimi sondami. Gre za uporovni princip merjenja s sondami Pt-100 in pretvorniki temperature v tokovni merilni signal v glavi sonde, glej sliko 2. Signal se preko drsnih obročev, ker se sušilnik med procesom sušenja vrti, prenaša v sistem vodenja – PLC. Samo temperaturno merjenje je namenjeno tako vodenju procesa sušenja, kot tudi aktiviranja sistema gašenja – takojšnjega zalivanja z vodo v slučaju vžiga produkta znotraj sušilnika. Zalivanje lahko aktiviramo tudi ročno s pritiskom na zaskočno tipko (enaka tipka kot se uporablja za izklop v sili na napravah in procesih). Uporabimo jo le, če kako drugače zaznamo nenormalen pojav v procesu sušenja in sumu na vžig znotraj sušilnika. Le takojšnja reakcija in popolno zalitje notranjosti sušilnika sta učinkovita v primeru vžiga. Tipka je nameščena v omarici pod steklom, ki ga je potrebno pred aktiviranjem razbiti.

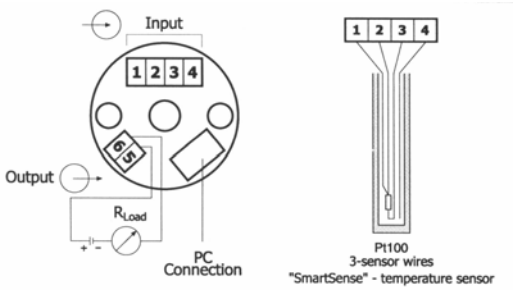


Slika 1: Shema sistema vakuumskega sušilnika

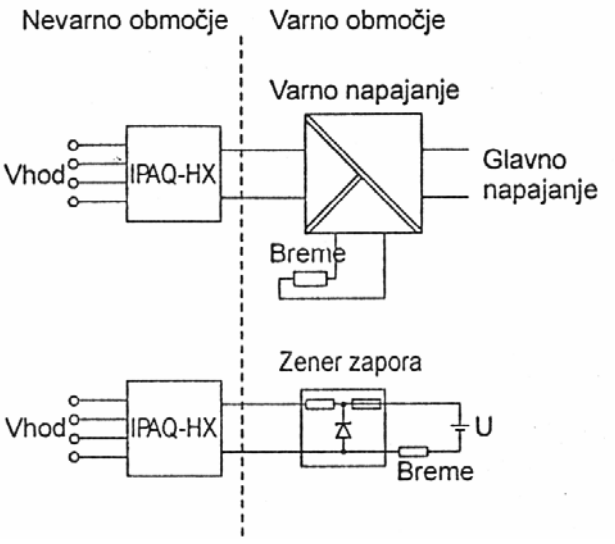
Primer 1:

Prišlo je do zalitja notranjosti sušilnika med procesom sušenja. Po pregledu arhiviranih podatkov smo ugotovili, da se je sistem aktiviral po predvidenem scenariju. Evidentirana sta bila pojava visoke temperature v dveh merilnih točkah (zalivanje se aktivira le, če se v dveh, od treh, temperaturnih merilnih točkah pojavi alarmno visoka temperatura), nakar je sledilo takojšnje zalitje sušilnika. Po analizi dogodkov pridemo do ugotovitve, da vzroka za pojav previsokih temperatur ni bilo. Kaj se je torej zgodilo? Kot že navedeno, se tokovni signal temperature prenaša preko drsnih obročev. Prvotno je bil pretvornik izza drsnih obročev, to pa je imelo za posledico večkratne pojave

alarmov visokih temperatur zaradi grafitne umazanij (ostankov grafita ščetk) na drsnih obročih (trenutni pojav visoke upornosti = visoka temperatura). Kaj je bil torej vzrok za aktiviranje zalitja zdaj, ko se preko drsnih obročev prenaša tokovni signal, prekinitve pa pomenijo izgubo signala oz. nizko temperaturo? Leži vzrok tudi v drsnih obročih? Da in ne. Zaradi slabega stika na drsnih površinah, zaradi prisotnosti grafitne umazanije, prihaja do prekinjanja tokovne zanke. To pomeni tudi prekinjanje napajanja temperaturnih pretvornikov, ki sta v sistemu zaščite lastna varnost*. Zaradi trenutne prekinitve in ponovne vzpostavitve napajanja pretvornikov, so se na njunih izhodih postavljale različne nedefinirane vrednosti. Posledica hkratnega pojava previsokih vrednosti na obeh izhodih pretvornikov pa pomeni aktiviranje zalitja sušilnika. Sam sistem zaščite se je ustrezno odzval, zahteva po varnosti je bila izpolnjena, vendar na napačno informacijo, kar je imelo za posledico izgubo produkta in poslovno škodo. Zakaj se izhodi pretvornikov postavljajo na nedefinirane vrednosti pri prekinitvi napajanja? Ali so pretvorniki, ki smo jih izbrali funkcionalno zadosti varni? So komponente pretvornika dovolj zanesljive? Enaka vprašanja si zastavljamo verjetno vsi, ko pride do okvar in izpadov sistemov. Smo bili preveč varčni pri postavitvi sistema in uporabi komponent? To so bila vprašanja, ki smo jih tudi mi postavljali potem, ko smo odkrili vzroke za pojav, verjemite, ni jih bilo enostavno odkriti. Kako pa naj vemo, kake naprave vgraditi, da bodo sistemi dovolj varni?
Odgovore najdemo v predpisih – regulativi, ki jo navajam v nadaljevanju.



Slika 2: Temperaturna sonda in merilni pretvornik



Slika 3: Temperaturni merilni pretvornik, lastna varnost

Primer 2:

Enak pojav zalitja sušilnika. Je prišlo do podobnega pojava kot v prvem primeru? Ne. Ob pregledu sistema smo ugotovili, da je bila vzrok za nastalo situacijo tipka za ročno aktiviranje zalivanja sušilnika, glej sliko 4. Kdo jo je uporabil in zakaj? Steklo izza katerega je tipka nameščena je bilo nepoškodovano. Je šlo za sabotažo? Ko smo tako razpredali variante pri neaktivirani tipki, se je le-ta kar naenkrat samodejno sprožila. Pojav se je kar ponavljal, ko smo večkrat tipko deaktivirali. Razlog zalitja je bil jasen. Kaj pa vzrok? Kaj se je kar naenkrat zgodilo z napravo? Je bila namenu primerno izbrana? Po katerih standardih o varnosti je bila izdelana?

Slika 4: Tipka za izklop v sili

Še več je primerov, ki bi jih lahko predstavil. Pojavljajo se tako na meroslovni opremi, regulatorjih, PLC-jih, drugih sistemih vodenja in izvršilnih elementih, v sistemih ki so namenjeni varnosti in v sistemih, ki so namenjeni izključno vodenju procesov.

Sistemov, ki so povezani z varnostjo (Safety-related systems - SRS) so na primer vsi:

- sistemi za izklop v sili v procesni industriji,
- požarni sistemi in detekcije plinov,
- indikatorji dovoljenih obremenitev v žerjavih in avto dvigalih,
- signalizacijski sistemi na železnici,
- kontrolni sistemi na parnih kotlih,
- sistemi zaščit pri strojih / zasloni in dvoročni vklopi (posebej stiskalnice),
- izklopi v sili na strojih,
- sistemi za vodenje gorilnikov v termo elektrarnah,
- sistemi za vodenje in nadzor v jederskih elektrarnah in mnogi drugi.

Danes najdemo v procesni industriji med 10% in 15% opreme, ki je namenjena varnosti. Vedno več je procesov, ki so avtomatsko vodeni. V sistemih vodenja razen senzorjev in izvršnih elementov nastopa vse več programabilne elektronike (inteligentnih regulatorjev, PLC-jev, SCADA sistemov,…). Za potrebe vodenja procesov so zadostne standardne zahteve za to opremo!? Za sisteme namenjene varnosti pa se postavljajo posebne zahteve, enako za opremo in dele opreme. Zahteva se:

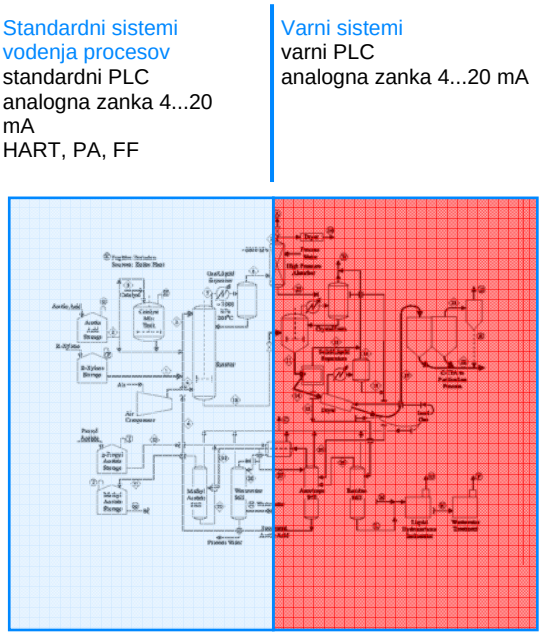
- zanesljivo delovanje delov sistemov za zaščito in nadzor in
- varna zaustavitev oz. postavitev v varna stanja, če pride do napak.

V teh sistemih pa je nujna funkcionalna varnost uporabljenih komponent.

Termin funkcionalne varnosti pokriva vse vidike za zaščito in obvladovanje nepravilnega delovanja naprav in opreme, ki je uporabljena v nadzornih sistemih, v naprav, kakor tudi osebja za zmanjševanje tveganja za:

- zaposlene,
- okolje in
- opremo.

Funkcionalna varnost temelji na obvladovanju naključnih napak in okvar ter na izključevanju in obvladovanju sistemskih napak. Na sliki 5 je prikazan primer uporabe različne opreme in principov v standardnih sistemih vodenja in varnih sistemih.



Slika 5: Standardni in varni sistemi

3 Regulativa

Kako je regulirano področje funkcionalne varnosti? Pri nas, glede na raziskavo in poizvedovanje, posebnih specifičnih predpisov, ki bi omenjeno področje opredeljevali, ni. Obstajajo le splošni akti s področja varovanja zdravja, varnosti, varovanja okolja, požarne varnosti, ki pa ne predpisujejo zahtev za uporabljene naprave in opremo, razen predpisov o eksplozijski zaščiti, ampak zahtevajo le uporabo sistemov za varovanje in predpisi, ki natančneje opredeljujejo varnost v specifičnih vejah industrije (primer proizvodnje električne energije v jederskih elektrarnah). V uporabi je še interna zakonodaja v podjetij, ki je zasnovana na različnih smernicah, ISO standardih, standardih dobre proizvodne prakse ter drugih predpisih, s katero si postavljajo merila za obvladovanje področja varnosti posamezna podjetja.

V Evropi pa je od leta 2002 v veljavi predpis, ki v najširšem obsegu opredeljuje področje varnosti in tako tudi funkcionalne varnosti. To je IEC 61508, ki navaja določila glede varnosti in funkcionalne varnosti, v pripravi oz. pripravljeni pa so še IEC 61511 posebej za področje procesne industrije, IEC 61513 za jedersko industrijo in IEC 62061 za proizvodno industrijo.

S temi predpisi so podane zahteve tako za dobavitelje kot za uporabnike varnostnih sistemov in naprav ter opreme za uporabo v teh sistemih.

4 Zaključek

Področje varnosti postaja vse pomembnejše v vseh vejah industrije. Če je bilo nekoč dovolj, da so bili le ustrezno kvalitetni produkti pogoj za uspešno nastopanje na domačih in tujih trgih, danes temu ni več tako. Vse bolj je pomembno, kako obvladujemo proizvodne procese in kakšni varnostni aspekti so pri tem upoštevani, predvsem okoljski vidiki. Za uporabnike v industriji je izredno pomembno, da so naprave, oprema in proizvodni procesi zanesljivi in varni, da ustrezajo nivojem celovite varnosti definiranim na predpisanih izhodiščih. Prav tako pa je tudi za proizvajalce pomembno, da so postavljena merila za proizvode, ki ustrezajo uporabi na različnih varnostnih nivojih.

*Zaščita lastna varnost se uporablja v conah eksplozijske ogroženosti, zasnovana pa je na principu omejevanja energije tokokroga, ki bi bila zadostna za vžig okoliške eksplozivne zmesi, če bi prišlo do napake.

5 Literatura

[1] IEC, *Functional safety and IEC 61508, A basic guide, November 2002*
[2] Siemens, *Aplication Manual, The Safety System for Industry*
[3] ENDRESS+HAUSER, *SIL – Functional Safety(IEC 61508/IEC 61511)*
[4] dr. Josef Börcsök, *Safety considerations*, HIMA Paul Hildebrandt GmbH + Co KG
[5] Eric Gilchrist, *Introduction and Overview to IEC 61508 - Functional Safety of Electrical/Electronic/ Programmable Electronic Safety Related Systems,* ABB