Funkčná bezpečnosť – apel bezpečnostného inžinierstva

Jozef Vass

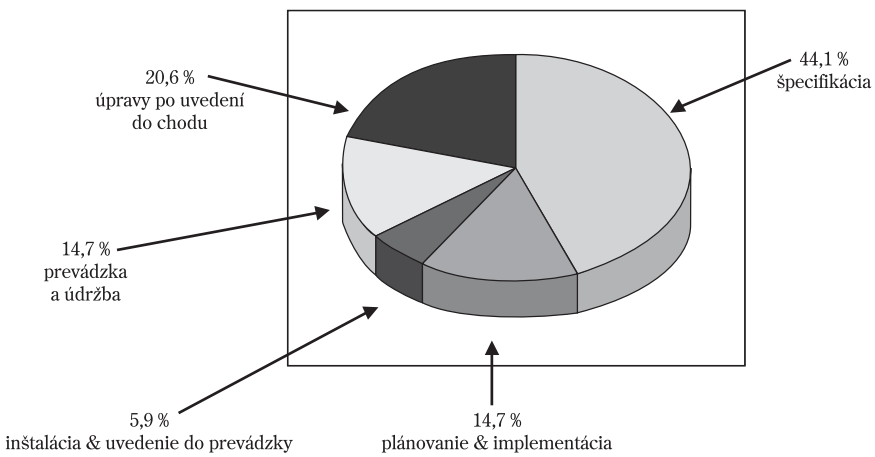
Článok sa zaoberá bezpečnostnými systémami z pohľadu najznámejších noriem, uvádza ich porovnanie, zaoberá sa prístupmi k politike riešenia bezpečnosti procesov a približuje problematiku koncepcie návrhu bezpečnostných systémov.

Úvod

Bezpečnosť prevádzkovania procesu je témou, ktorá sa nástojčivo dostáva na program dnešných dní aj tam, kde doteraz bola nepovšimnutá. Nájsť proces, ktorý by inherentne spĺňal podmienky bezpečnosti vztiahnuté na osoby, majetok a životné prostredie, je prakticky nemožné. Takmer všetky výrobné procesy môžu generovať operácie, ktoré môžeme označiť ako kritické. Pochody v technologických uzloch, napriek svojej opodstatnenosti v integrite celého procesu, znamenajú v prevádzkovaní isté nezanedbateľné riziko. Je to dané tým, že pri súčasnom stupni poznania majú technika a technologické postupy svoje ohraničenia. Navyše do nich zasahuje človek so všetkými svojimi obmedzeniami. Dramatické havárie vo svete v oblasti chemického, petrochemického a rafinérskeho priemyslu, ako aj v oblasti skladovania a prepravy ropných produktov, vedú tvorcov noriem k definovaniu stále exaktnejších prístupov na rozpoznanie úrovne rizika a zavedenie takých opatrení, aby prevádzkovanie bolo stále bezpečnejšie. Národné, nadnárodné a poisťovacie spoločnosti, ktoré sú na prevencii zainteresované, skúmajú aspekty havárií vo vzťahu „príčina – následok“. Napĺňajú sa databázy, ktoré na jednej strane nastavujú zrkadlo ľudskej nezodpovednosti a nedokonalosti použitej techniky, ale na druhej strane poskytujú cenné poznatky, ktoré vedú k prevencii. Uvádzané spoločnosti vyvíjajú tlak na legislatívu, výrobcov i používateľov a výsledkom tohto tlaku je stále bezpečnejšia technika, dokonalejšie technologické postupy a lepšie pripravený operátor procesu.

Príčiny závažných havárií

Na ilustráciu uvádzam obr. 1 o príčinách 34 prípadov havárií, ktoré preskúmala nezávislá technická komisia. Graf naznačuje, že príčiny havárií sa vyskytujú počas celej doby životnosti zariadení počnúc návrhom, cez jeho realizáciu, až po využitie a modifikáciu v priebehu využívania. Kto sa raz pohyboval v priemyselnom prostredí, musí vedieť, koľko nedokonalostí sa počas celej doby životnosti zariadení vyskytuje. Porovnanie percentuálneho rozloženia dobre vystihuje pomery, ktoré „vládnu“ pri príprave riešenia, jeho implementácie, pri užívaní produktu i jeho modifikácii. Alarmujúce bolo zistenie, že vyše 44 % chýb spôsobili tí, ktorí mali špecifikovať či už systém riadenia, bezpečnostný systém alebo sa mali podieľať na špecifikácii nebezpečných miest v technológii. Čo, alebo koho treba vidieť za týmto číslom? Je to kontraktor, licencor, technológ existujúcej prevádzky alebo nedostatok podkladov v existujúcich databázach, o ktorých sme v predchádzajúcich odstavcoch hovorili? Prevádzkovanie, údržba a dodatočné úpravy systému tvoria viac ako 35 %. Je úplne bežné, že sa mnohokrát pracuje s neúplnou dokumentáciou, že k zariadeniu sú niekedy postavení ľudia, ktorým používateľ „nedoprial“ školenie u výrobcu alebo že tento zveril úpravy existujúceho systému nekompetentnej servisnej spoločnosti.



Obr.1 Rozdelenie chýb po celú dobu životnosti

Napriek týmto zisteniam stále pretrvávajú akési kváziekonomické prístupy zodpovedných manažérov pri príprave výstavby technologických objektov, kde je snaha šetriť za každú cenu, niekedy aj za tú najvyššiu. Podceňovanie situácie a hľadanie ciest, ako sa tomu vyhnúť, je javom, ktorý sa ešte stále a dosť často vyskytuje. Je však potešiteľné, že v porovnaní s deväťdesiatymi rokmi takýchto prejavov je stále menej. Znepokojujúce ostáva, že tí, ktorí by mali byť iniciátormi progresívnejších a bezpečnejších riešení sa často stávajú nekompetentnými oponentmi tých, ktorí majú svoj zrak upriamený na nové a dokonalejšie riešenia a ktorí ich suplujú v zodpovednosti.

Pokroky v riešeniach

V tomto príspevku by som sa chcel zaoberať technickým hľadiskom bezpečnostných systémov v kontexte bezpečnostného inžinierstva, ako aj vo väzbe na existujúcu legislatívu. Ostatné väzby bezpečného prevádzkovania z pohľadu „človek – stroj“ prenechám kompetentným odborníkom pre túto oblasť.

Prístupy k posilňovaniu bezpečnosti sa postupom rokov zdokonaľujú. V začiatkoch na posilnenie bezpečnosti prevádzkovania zariadení postačovala modernejšia technika. Skutočne, už samotná modernizácia riadeného procesu prinášala zlepšenie a spoľahlivejší riadiaci systém posúval hranicu bezpečnosti. Nástup mikroprocesorovej techniky, ako sa predpokladalo, mal vyriešiť nielen zvyšujúce sa nároky na riadenie, ale aj naplniť požiadavky bezpečnosti prevádzkovania. Prax však ukázala, že technika v takom chápaní nie je samospasiteľná. Bežné PLC (Programmable Logic Controler) nie je bezpečným systémom z toho dôvodu, že vnútorné poruchy v PLC môžu viesť k nedefinovaným stavom, ktoré môžu vyvolať nežiaduce zásahy do riadeného objektu. Neurčitosť správania stále komplexnejších mikroprocesorových systémov so svojimi operačnými systémami sa nedala prehliadať, nehovoriac už o neurčitosti používateľského softvéru so všetkou obtiažnosťou vykonania auditu a nepripravenosti obsluhy vykonávať stále zložitejšie zásahy do riadenia procesu. Bolo potrebné zaoberať sa s bezpečnosťou

omnoho hlbšie. Napriek tomu, že vývoj v tejto oblasti pokročil a k bežným PLC pribudli bezpečnostné, niektoré krajiny stále zotrvávajú v istej nedôvere voči programovateľným automatom a preferujú použitie HV systémov alebo „pevne zadrôtovaných" pre nebezpečné procesy, resp. presadzujú ich ako doplnok k PLC. Je známe, že pre najvyššiu formu bezpečnostného systému zvolili niektorí výrobcovia takúto architektúru. Ďalší výrobcovia zvolili HV systémy pre každú úroveň bezpečnosti, teda aj pre tú najnižšiu. Táto rôznorodosť prístupov vôbec nie je na škodu, ba práve naopak, vytvára pestré konkurenčné a porovnávacie pole, pričom dáva príležitosť na verifikáciu nielen na základe deklarovaných parametrov, ale aj na základe výsledkov overených v praxi.

Legislatívne podklady – porovnanie

Zásadný obrat v prístupe ku koncepčnému riešeniu bezpečnosti procesov predstavovalo to, čo naznačili tvorcovia normy v SRN. Začiatkom deväťdesiatych rokov prišla norma DIN V 19 250 s návrhom analyzovať všetky riziká vo vlastnom procese aj v korelácii s riadiacim systémom. Túto filozofiu si osvojili aj tvorcovia medzinárodnej normy IEC 61 508, ba čo viac, vyslovili potrebu zaoberať sa bezpečnosťou procesu od analýzy rizík, cez návrh bezpečného systému, starostlivosť o systém počas celej doby životnosti, až po ukončenie činnosti systému alebo jeho demontáž. Tento prístup bol iste reakciou na zistené príčiny, ktoré sú interpretované na obr. 2. Výhodou uvedeného prístupu je, že je založený takmer na vedeckom základe. Numerické metódy špecifikácie a návrhu úplného bezpečnostného systému sú možné, riziko môže byť kvantifikované a bezpečnostný systém môže byť šitý na mieru. Poddimenzovanie a predimenzovanie je menej pravdepodobné, čo napokon rieši viacerí výrobcovia poskytovaním variantných riešení.

Venujme teraz pozornosť normám (obr. 3), ktoré sú akceptované buď v celosvetovom, alebo národnom meradle. K najvyššej dokonalosti, ak to tak môžeme povedať, to doviedli normotvorcovia z organizácie IEC

DIN V 19 250/vydaná na začiatku 90-tych rokov
- nemecká norma/návrh
- prvý pokus o analýzu rizika
- podklad pre medzinárodné a národné normy (IEC 1 508 – návrh, S 84, ...)
- definuje 8 tried bezpečnostných systémov (AK – Anforderungsklasse)
- dopĺňa ju norma DIN V VDE 0801

S 84/vydaná v 90-tych rokoch, pripravovaná súbežne s IEC 61 508
- americká norma s plným názvom ANSI/ISA – S 84.01
- stavaná pre priemyselné procesy
- definuje 3 triedy bezpečnostných systémov SIS (Safety Instrumented System)
- zaoberá sa iba bezpečnostným systémom
- nepojednáva o celej dobe životnosti

IEC 61 508/vydaná v rokoch 1998 až 2000
- medzinárodná norma so všeobecným záberom
- popisuje celú dobu životnosti bezpečnostného systému, ale aj riadeného objektu
- najprepracovanejšia aj najúplnejšia norma v svojej oblasti
- definuje 4 triedy SIL (Safety Integrity Level)

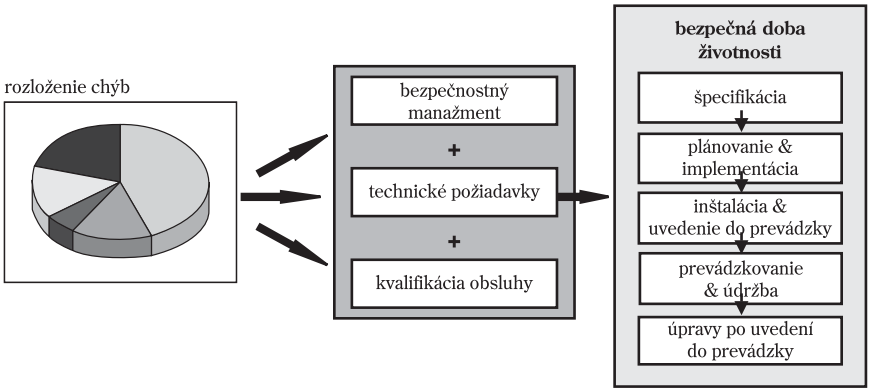
IEC 61 511/pripravované vydanie v záverečnej fáze
- medzinárodná norma špeciálne určená pre priemyselný sektor
- je v súlade s IEC 61 508
- predmetom analýzy rizika sú aj snímače, akčné orgány a rozhrania
- určuje tie isté triedy ako IEC 61 508

Obr.3 Porovnanie niektorých noriem v oblasti bezpečnostných systémov

(International Electrotechnical Committee), aj keď údajne ochrancovia životného prostredia nie sú celkom spokojní s mierou akcentovania vplyvu havárií na životné prostredie. Ide predovšetkým o normu IEC 61 508 s plným názvom „Functional Safety of Electrical/Electronic/Programable Electronic Safety-related Systems", pričom predmet normy má svoju skratku E/E/PE alebo E/E/PES. Fyzická podoba normy je na obr. 4.

Fyzická norma IEC 61 508
Časť 1: Všeobecné požiadavky
Časť 2: HW požiadavky
Časť 3: SW požiadavky
Časť 4: Definície a skratky
Časť 5: Príklady
Časť 6: Sprievodca po častiach 2 a 3
Časť 7: Prehľady techniky a foriem tvorby SW

Obr.4 Fyzická norma IEC 61 508



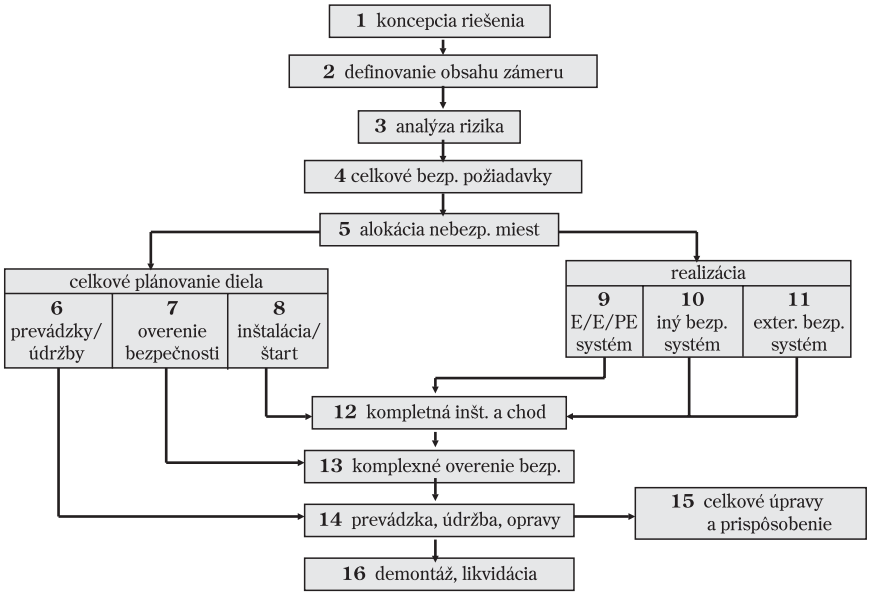
Obr.2 Stratégia funkčnej bezpečnosti bezpečnostných systémov

Norma IEC 61 508 na svojich asi 400 stranách je akoby kmeňovou normou, ktorá poskytuje komplexný obraz o tom, aké zásady musia byť dodržané pri konštrukcii bezpečnostného PLC, aké nároky sa kladú na periférne zariadenia, ako by mal pracovať bezpečnostný manažment, aké sú jeho povinnosti a úlohy. Všeobecne koncipovaná norma má slúžiť výrobcom zariadení, ale aj používateľom. Obsahuje množstvo praktických príkladov, ktoré usmerňujú navrhovateľa systému pri budovaní jeho architektúry. Môže slúžiť ako základ na vypracovanie špecifických odvetvových alebo národných noriem. Norma uvádza, že bezpečnostný systém nie je iba vlastná funkčná logika, ale aj snímače, akčné orgány a príslušné rozhrania. Toto treba zvlášť zdôrazniť vzhľadom na to, že na periférie investor ochotne zabúda. Ale rozdelenie chýb, ktoré sa podieľajú na haváriách, je neúprosným argumentom (snímače 35 %, funkčná logika 15 % a akčné orgány 50 %). Dá sa s tými číslami polemizovať, no neodškriepiteľný je fakt, že v automatizačnej technike hovoríme vždy o kompletných obvodoch, ktoré treba bezpodmienečne riešiť v kontexte bezpečnostného systému (obr. 5). Norma uvádza štyri triedy bezpečnostných systémov, SIL 1 až 4, tzv. Safety Integrity Level, pričom SIL 1 reprezentuje najnižšie požiadavky, SIL 4 najvyššie. Ako sú definované limity pre jednotlivé SIL ukazuje obr. 6.

Iným produktom IEC je norma IEC 61 511 „Functional Safety Instrumented Systems for Process Industry Sector". Je to špecifická norma zaoberajúca sa priemyselnými procesmi, ktorá sa zameriava aj na snímače, akčné orgány a rozhrania. Nemenej významnou je tiež norma IEC 61 131-3, ktorá hovorí o programových prostriedkoch a venuje sa nielen PLC, ale všetkým zariadeniam, kde je aplikovaný µP, ako súčasť inteligentných prístrojov a zariadení.

Z ďalších noriem, ktoré sa viažu na kmeňovú normu, môžeme spomenúť IEC 61 513 pre jadrovú energetiku a IEC 62 061 pre výrobné priemyselné odvetvia.

Významnou normou je DIN V 19 250, ktorá bola prvou normou zaoberajúcou sa analýzou rizika. Jej presný názov je „Basic Safety Evaluation of Measuring and Control Protective Equipment". Pri definovaní ôsmich tried bezpečnostných systémov vychádza z analýzy rizika tak, ako je to znázornené na obr. 7. Triedy sú označované alfanumerickým znakom AK 1 až 8 (Anforderungs Klasse). Používa sa aj anglický výraz RC (Requirement Class). Nie je priama konverzia medzi SIL a AK, ale existuje približné porovnanie, uvedené



Obr.5 Úplný životný cyklus podľa IEC 61 508

Safety Integrity Level (SIL)	požiadavka na spôsob prevádzkovania (pravdepodobnosť chýba navrhnutého systému)	kontinuálne prevádzkovanie/ vysoké požiadavky (pravdepodobnosť 1 nebezpečnej chyby/hod)
4	$>= 10^{-5}$ up to $< 10^{-4}$	$>= 10^{-9}$ up to $< 10^{-8}$ h^{-1}
3	$>= 10^{-4}$ up to $< 10^{-3}$	$>= 10^{-8}$ up to $< 10^{-7}$ h^{-1}
2	$>= 10^{-3}$ up to $< 10^{-2}$	$>= 10^{-7}$ up to $< 10^{-6}$ h^{-1}
1	$>= 10^{-2}$ up to $< 10^{-1}$	$>= 10^{-6}$ up to $< 10^{-5}$ h^{-1}

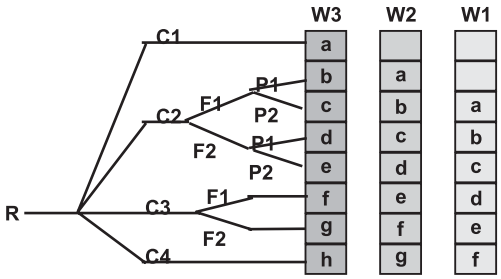
Rozdelenie miery chýb
35 % snímače
15 % funkčná logika
50 % akčné orgány

Obr.6 Safety Integrity Levels – smerné čísla chýb podľa IEC 61 508

na tej istej schéme. Napriek tomu, že ide len o návrh normy, spoločnosti ako napr. TÜV certifikujú naďalej v zmysle tohto návrhu. Nedostatkom návrhu je, že sa nezaoberá s celou dobou životnosti zariadení.

Norma IEC 61 508 bola prevzatá do sústavy európskych noriem, a následne v rámci harmonizácie s európskymi normami v roku 2002 sa dostala aj do sústavy slovenských technických noriem. Je na škodu rozvinutej aplikácie bezpečnostných systémov v slovenskom priemyselnom prostredí, že norma bola vydaná iba v anglickom jazyku. V harmonizácii zaostávame za Českou republikou, kde už túto európsku normu preložili. Platnosť všetkých iných noriem, ktoré sú v istom slova zmysle v rozpore s kmeňovou normou IEC/EN 61 508, ako je DIN v 19 250, DIN V 19 251, DIN VDE 0801, DIN VDE 0801/A1 sa končí dátumom 1. 8. 2004.

V USA a Kanade sa aplikuje norma ANSI/ISA S 84.01 „Application of Safety Instrumented Systems for the Process Industries“. Aj táto definuje takmer zhodne SIL ako IEC 61 508, avšak iba tri stupne – SIL 1 až 3 so zameraním len na priemyselné procesy. Norma sa nezaoberá celou dobou životnosti.



min. nutná redukcia rizika	Safety Integrity Level
–	bez bezp. pož.
a	bez špec. bezp. pož.
b, c	1
d	2
e, f	3
g	4
h	1 E/E/EPS nie je dostatočný

Dôsledok, rizikový parameter
C1 drobné poranenie
C2 vážne trvalé poranenie 1 alebo viacerých osôb, smrť 1 osoby
C3 smrť viacerých osôb
C4 smrť veľkého množstva osôb

Opakovateľnosť & čas pôsobenia
F1 zriedkavo až dosť často
F2 veľmi často až permanentne

Možnosť vyvarovať sa nebezpečným udalostiam
P1 je možné za určitých posmienok
P2 takmer nemožné

Pravdepodobnosť výskytu nežiadúcich udalostí
W1 veľmi malá pravdepodobnosť
W2 malá pravdepodobnosť
W3 relatívne veľká pravdepodobnosť

Obr.7 Graf rizík podľa DIN V 19 250

Funkčná bezpečnosť – analýza rizík

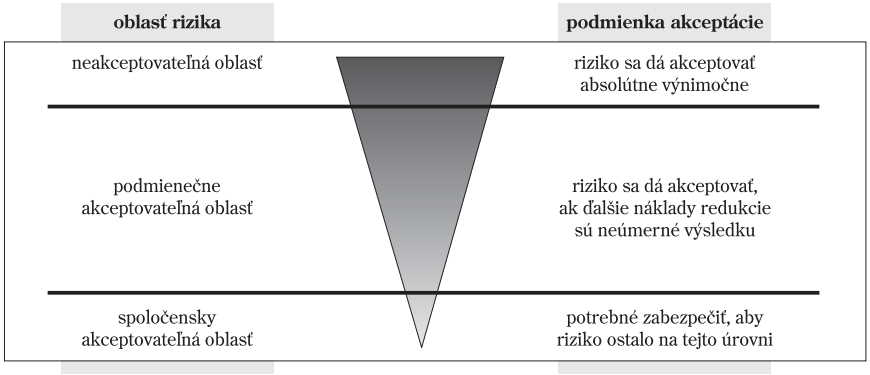
Historicky pred vydaním IEC 61 508 sa rozlišovali tri aspekty systému bezpečnosti: Prvý sa týkal primárnej bezpečnosti, ktorá bola zameraná na riziká pri styku so zariadením, ako je napr. riziko úrazu elektrickým prúdom, riziko popálenia atď. Druhým hľadiskom je funkčná bezpečnosť a tretím je nepriama bezpečnosť vyplývajúca z generovania takých výsledkov procesu, ktoré nespôsobia priame následky v čase generovania, ale ovplyvňujú následné rozhodovanie (napr. nesprávne analýzy v medicínskej praxi). Uvedené normy sa zaoberajú druhým aspektom, ktorý je viazaný na bezpečnú funkciu zariadenia EUC (Equipment Under Control), čo zahŕňa zariadenia, stroje a aparáty na produkciu, spracovanie, transport, skladovanie atď. Už z definície je jasné, že ide o komplex prostriedkov, ktorých činnosť je riadená tak, že na základe vstupných signálov sa generujú výstupné signály takého charakteru, aby proces prebiehal požadovaným smerom.

Normy sa zaoberajú rizikom EUC, ktoré vzniká v zariadení v interakcii s riadiacim systémom. Ak je úroveň tohto rizika príliš vysoká, je potrebné znížiť riziko EUC na spoločensky akceptovateľnú úroveň. Takto definované znížené riziko je referenčnou hodnotou (dá sa vyjadriť kvantitatívne alebo kvalitatívne), ktorá je základom pre návrh bezpečnostného systému (obr. 8).

Bezpečnostný systém:
- Je určený na dosiahnutie integrity bezpečnosti vo vlastnom EUC alebo pomocou E/E/PES, resp. využitím externého zariadenia nezávislého na EUC.
- Implementuje požadované bezpečné funkcie na udržanie EUC v bezpečnom stave.

Potlačenie rizík sa môže udiať na úrovni riadeného procesu a riadiaceho systému, ako aj pomocou iných opatrení alebo externých systémov nezávislých od EUC. Ak sa vyčerpali všetky dostupné a ekonomicky zvládnuteľné opatrenia (čo v praxi zvyčajne nesiaha až po akceptovateľnú mieru rizika), zvyšok musí saturovať bezpečnostný systém E/E/PES, konštruovaný a certifikovaný podľa požiadaviek medzinárodných noriem. Príklady akceptovateľnej úrovne rizika popisuje uvádzaná norma IEC 61 508 (obr. 9).

V nezávislej odbornej literatúre je možné nájsť údaje o frekvencii porúch technologických aparátov, ako aj automatizačných prvkov. Zdalo by sa, že vytvoriť scenár je



Obr.8 Interpretácia oblasti akceptovateľnosti rizika

veľmi jednoduché. Zložitým ho však robia vnútorné interakcie. V minulosti sa používal údaj o časovom intervale medzi poruchami (MTBF – Mean Time Before Failure) na zhodnotenie spoľahlivosti zariadenia. Metodika stanovovania MTBF nebola bez chýb, ale čo bolo najpodstatnejšie, nehovorila nič o dôsledkoch. Pre dnešnú prax už tento faktor nepostačuje. Analýzu rizika je možné vykonať napr. realizáciou štúdie HAZOP, ktorá jasne definuje riziko, pravdepodobnosť výskytu nebezpečných udalostí a úroveň nebezpečenstva. Analýza rizika je prvým krokom na stanovenie príslušného SIL, resp. AK (RC). Normy IEC 61 508 a S84.01 tiež uvádzajú príklady stanovenia existujúceho rizika.

Certifikácia periférií

Uvádzaná norma IEC 61 508 používateľom pripomína, že bezpečnostný systém netvorí len samotné bezpečné PLC alebo iný, hardvérový systém, ale že pozostáva aj z periférií, ako sú snímače, akčné orgány a rozhrania, ktoré by mali mať požadovanú spoľahlivosť a certifikát v zmysle tejto normy. V súčasnej dobe sú už na trhu snímače (ide hlavne o tie, ktoré sa frekventovane používajú ako vstupy pre PLC) a akčné orgány (zamerané na spoľahlivosť chodu pri „shut down" aplikáciách), ale aj rozhrania, ako napr. bezpečné izolátory na zaistenie iskrovej bezpečnosti, napájacie zdroje, solenoidové ventily atď. Pristavme sa v krátkosti ešte pri problematike ako sa s certifikáciou periférií vyrovnávajú výrobcovia.

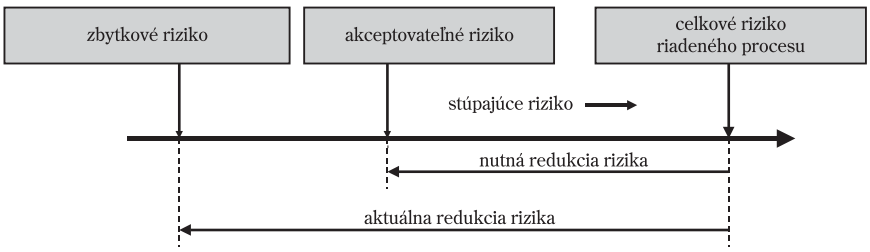
Mnohé z firiem vyhlasujú, že ich výrobok je v súlade s IEC 61 508 a vyhovuje jej požiadavkám bez toho, aby požiadali nezávislý orgán o certifikáciu. Takéto vyhlásenie je zavádzajúce, ak vychádza iba z vlastného posúdenia. IEC 61 508 sa zameriava nielen na vlastnosti produktu, ale aj na jeho výrobu. Bez certifikácie výrobku nie je možné tvrdiť, že výrobok vyhovuje požiadavkám normy. Napriek tomu, že nie všetky výrobky sú certifikované, je možné použiť ich v bezpečnostných obvodoch. Bližšie o tom vypovedajú normy. Jedným z riešení je dať si vypracovať nezávislou spoločnosťou (napr. Exida,) správu FMEDA (Failure Modes, Effects and Diagnostic Analysis). FMEDA je detailné preskúmanie obvodov a ich charakteristík, ktoré vedú k identifikácii druhu a frekvencii chýb a o schopnosti zariadenia diagnostikovať ich. Zahŕňa matematickú analýzu a fyzikálne testy. Správa kategorizuje bezpečné a nebezpečné diagnostikovateľné chyby a uvádza ich percentuálny výskyt, ktorý je použiteľný pri výpočte PFD (Probability of Failure on Demand) pre určitý stanovený stupeň SIL konkrétneho obvodu, ktorý je na základe analýzy determinovaný ako kritický. V prípade, že sa výrobca takouto správou nedokáže prezentovať, norma IEC odporúča redundanciu predmetného prvku (obr. 10).

Norma IEC 61 508 zároveň odporúča akreditovaným tretím stranám vykonať požadovanú certifikáciu podľa schémy CASS (Conformity Assessment of Safety-related System). Mnohé z certifikujúcich spoločností túto schému využívajú.

Záver

Vybavenie technologického procesu príslušným SIS je zodpovedná úloha, ako to vyplýva z úvah, ktoré boli v článku uvedené. Jeho stanovenie prostredníctvom ne-

1) E/E/PE bezpečnostný systém
2) iné technické prostriedky
3) externé zariadenia



Obr.9 Prostriedky na aktuálnu redukciu rizika

$$PFD_{AVG} = \sum PFD_{SE} + \sum PFD_{LS} + \sum PFD_{PE}$$

PFD_{AVG} je stredná pravdepodobnosť výskytu prípustnej chyby E/E/PE bezpečnostného systému

PFD_{SE} je pravdepodobnosť výskytu prípustnej chyby snímača a pripojovacieho zariadenia

PFD_{LS} je pravdepodobnosť výskytu prípustnej chyby funkčnej logiky

PFD_{FE} je pravdepodobnosť výskytu prípustnej chyby akčného člena a pripojovacieho rozhrania

Obr.10 Kalkulácia pravdepodobnosti výskytu chyby

kvalifikovaného odhadu vedie k poddimenzovaniu alebo predimenzovaniu systému. Ani jedno z takýchto riešení nie je ekonomické, no poddimenzovaný systém je navyše nezodpovedne nebezpečný.

V súčasnosti prebieha proces harmonizácie sústavy STN (Slovenská technická norma) s európskymi normami takým tempom, ako sú na to vytvorené podmienky v zodpovedných inštitúciách. Treba konštatovať, že na rozdiel od rozvinutých krajín západnej Európy sme v mnohých oblastiach ešte nedosiahli potrebnú úroveň vybavenosti technologických procesov, akú by si vyžadovala ich povaha a riziká, ktoré v sebe skrývajú. Preto je na odborných pracovníkoch, aby dostávali do povedomia ľudí, ktorí o použitých investíciách rozhodujú, nutnosť zaoberať sa každým nebezpečným procesom. Ide o to, aby sa už v prípravnej fáze stavieb analyzovali riziká a aby sa navrhol taký systém, ktorý by ochránil proces pred nežiaducimi stavmi. Analýza rizík vedie k systému šitému na mieru, čo už v tejto fáze znamená úsporu investičných prostriedkov. Netreba zabúdať ani na existujúce technologické celky. Tam je už prevencia havárií zo strany štátnych orgánov postupne vyžadovaná.

Literatúra

[1] MTL: An Introduction to Functional Safety and IEC 61 508.

[2] ADLER, B.: Utilizing Safety Standard IEC 61 508 in the Chemical Processing Industry.

[3] NASH, M.: IEC 61 508 – Don´t Dice with Safety.

[4] TÜV: Automation Software Information Technology.

[5] Moor Industries: Process Interfaces Instrument.

[6] STN/EN 61 508.

Ing. Jozef Vass

D-Ex Limited, spol. s r. o.
e-mail: info@dex.sk