Normy pre tvorbu softvéru riadiacich systémov

Dušan Mudrončík, Martin Gálik

Funkčná bezpečnosť riadiacich systémov bezpečnostne kritických systémov patrí k základným požiadavkám prevádzkovania bezpečnostne kritických systémov, ako sú napr. dopravné systémy, nukleárna energetika, environmentálne nebezpečné chemické prevádzky alebo farmaceutické technológie. Tento príspevok uvádza stručnú charakteristiku relevantných štandardov a ich implementáciu v priemyselných bezpečnostne kritických procesoch.
Kľúčové slová: softvér riadiacich systémov, funkčná bezpečnosť, riadiaci systém bezpečnostne kritického procesu.

The functional safety is important and desired feature of process control systems, which are called safety critical systems. Characteristic examples of such systems are traffic systems, nuclear systems, chemical or pharmaceutical plants. The paper presents a brief characterisation of relevant standards and their implementation in the industrial safety critical applications.
Key words: control system software, functional safety, safety related control system.

1. Úvod

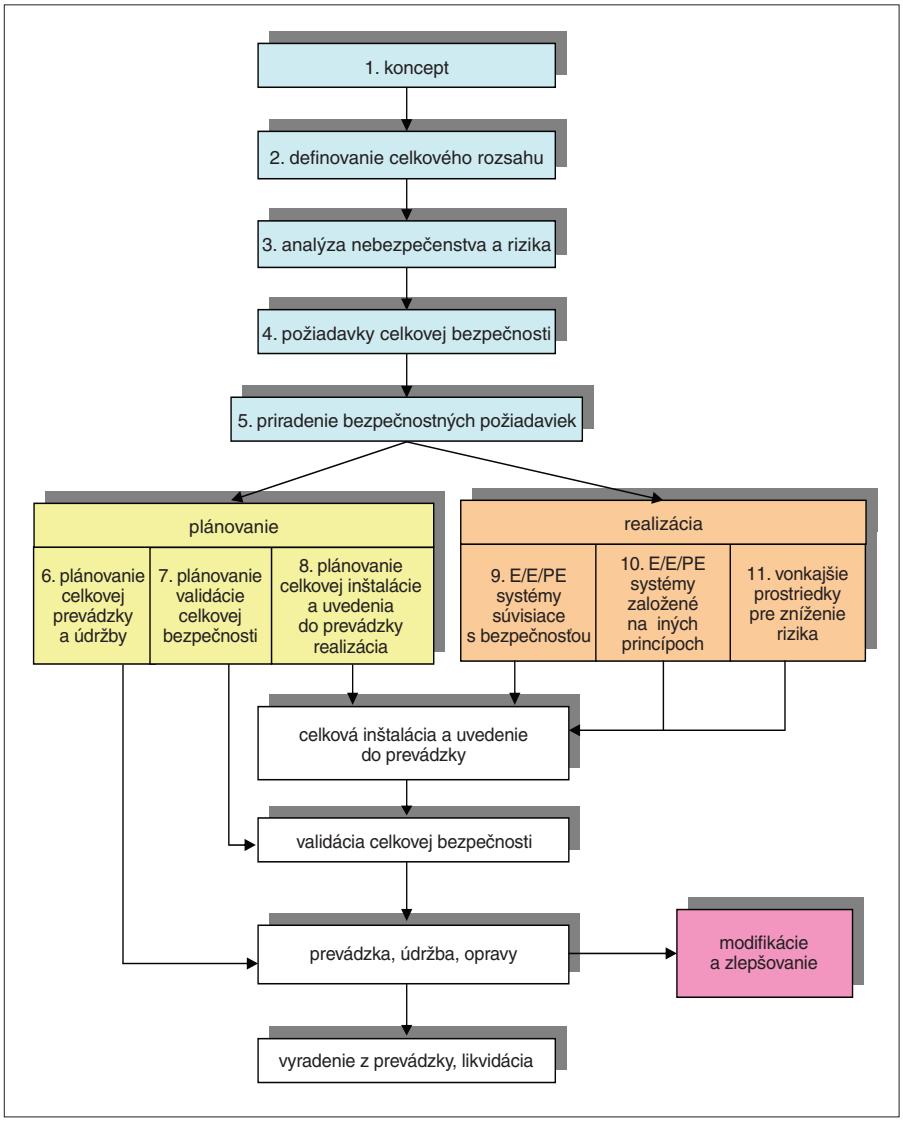
Riadenie bezpečnostne kritických procesov vyžaduje z hľadiska inžinierskej praxe špecifický prístup, ktorého prvoradý cieľ je eliminácia, resp. redukcia rizík vyplývajúcich z prevádzky bezpečnostne kritických technologických prevádzok. Spravidla sa pri realizácii návrhu a implementácii zásad funkčnej bezpečnosti vyžaduje preukázateľne dosiahnutá úroveň komplexnej bezpečnosti. Základné východisko k riešeniu naznačených problémov poskytujú jednotlivé časti štandardu IEC 61508 *Funkčná bezpečnosť elektrických/elektronických/ /programovateľných elektronických bezpečnostných systémov*. Použitie tohto štandardu v priemyslu usmerňuje a detailizuje nadväzujúca norma IEC 61511 *Funkčná bezpečnosť – bezpečnostné riadiace systémy spojitých technologických procesov*.

Tento príspevok prezentuje stručný prehľad obsahu uvedených štandardov a rámcovo uvádza možné spôsoby ich implementácie v reálnych podmienkach.

2. IEC 61508 – stručný prehľad

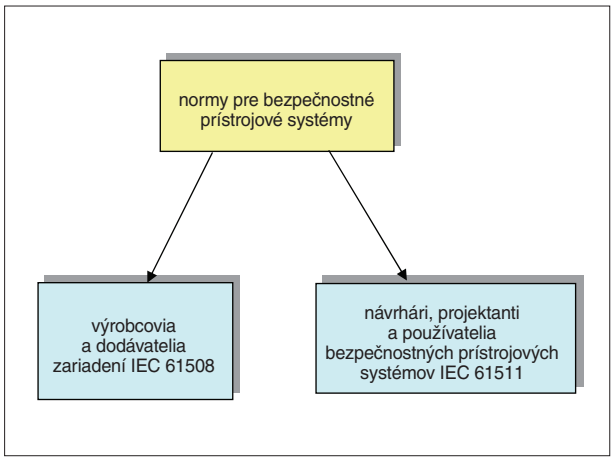
Súčasné riadiace systémy sú spravidla budované ako distribuované riadiace systémy s niekoľkoúrovňovou hierarchickou štruktúrou. Najnižšia, prevádzková úroveň zabezpečuje priame napojenie riadiaceho systému na technologický proces. Ako technické prostriedky sa používajú programovateľné elektronické zariadenia – priemyselné regulátory a programovateľné automaty (PLC). V niektorých úlohách sa vyžaduje, aby okrem štandardných funkcií riadiaceho systému, ako sú napr. zber a prvotné spracovanie údajov, monitorovanie riadeného procesu, spracovanie alarmov, výpočet a vykonávanie akčných zásahov atd., systém poskytoval dostatočnú úroveň komplexnej bezpečnosti. V takom prípade sa hovorí o funkčnej bezpečnosti riadiaceho systému.

Medzinárodná norma IEC 61508 [6] *Funkčná bezpečnosť elektrických/elektronických/ programovateľných elektronických bezpečnostných systémov* podrobne stanovuje obecný prístup pre celý životný cyklus bezpečnosti systémov, ktoré obsahujú elektrické, elektronické a programovateľné elektronické (E/E/PES) časti využívané na zabezpečenie bezpečnostných funkcií ria-



Obr. 1. Celkový životný cyklus

diaceho systému. Norma obsahuje tieto časti:
– časť 1 – Všeobecné požiadavky,
– časť 2 – Požiadavky na elektrické/elektronické/programovateľné elektronické systémy súvisiace s bezpečnosťou,
– časť 3 – Požiadavky na softvér,
– časť 4 – Definície a skratky,
– časť 5 – Príklady metód určovania úrovní integrity bezpečnosti (SIL),
– časť 6 – Metodické pokyny pre použitie IEC 61508-2 a IEC 61508-3,
– časť 7 – Prehľad postupov a opatrení.



Obr. 2. Oblasť použitia noriem

Norma IEC 61508 uvažuje všetky dôležité fázy životného cyklu celkovej bezpečnosti, bezpečnosti E/E/EPS a bezpečnosti softvéru (počínajúc koncepciou, cez návrh, realizáciu, prevádzku a údržbu až po vyradenie z prevádzky) pri používaní E/E/EPS pre plnenie bezpečnostných funkcií. Poskytuje metodiku pre vypracovanie špecifikácie bezpečnostných požiadaviek potrebných pre dosiahnutie funkčnej bezpečnosti E/E/PES súvisiacich s bezpečnosťou a pre stanovenie celkovej úrovne integrity bezpečnosti pre bezpečnostné funkcie realizované E/E/PES súvisiace s bezpečnosťou používanou na úrovni bezpečnostnej integrity. Pre stanovenie úrovne komplexnej bezpečnosti používa metódy založené na analýze rizika. Norma ďalej stanovuje číselné hodnoty výslednej miery porúch pre E/E/PES súvisiace s bezpečnosťou, viazané na jednotlivé úrovne bezpečnostnej integrity. Používa model životného cyklu celkovej bezpečnosti ako technický rámec pre systematické vykonávanie všetkých činností, ktoré sú potrebné pre zaistenie funkčnej bezpečnosti E/E/PES súvisiacich s bezpečnosťou.

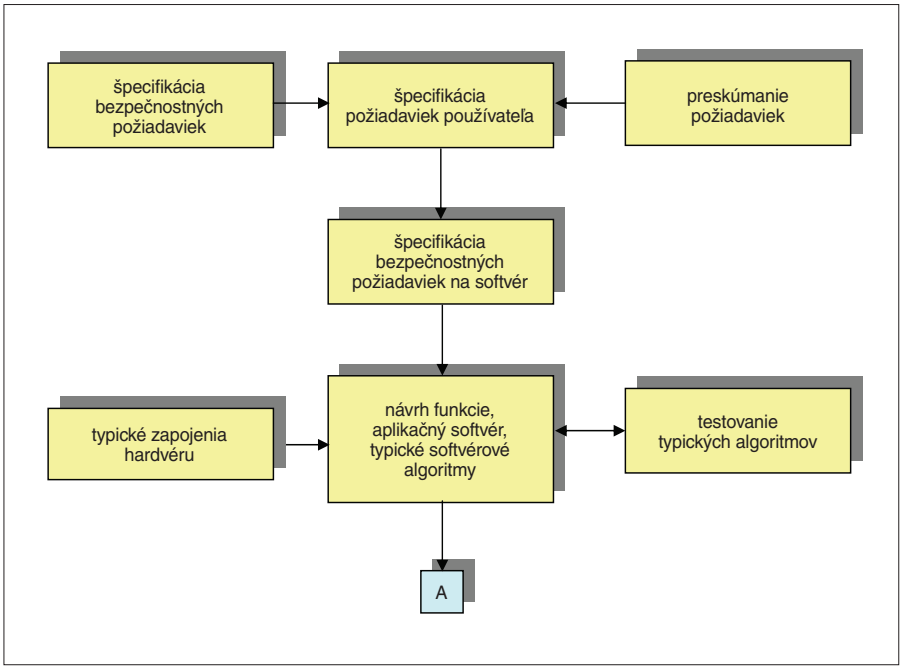
Celkový životný cyklus bezpečnosti E/E/PES je prehľadne znázornený na *obr. 1*.

Uvedený životný cyklus funkčnej bezpečnosti sa odporúča používať ako základ pri uplatňovaní zhody s touto normou. Naproti tomu však, za predpokladu splnenia cieľov a požiadaviek všetkých častí tejto normy, sa môže použiť aj iný životný cyklus, ako je životný cyklus na *obr. 1*. Organizácie alebo jednotlivci, ktorí majú celkovú zodpovednosť za jednu alebo niekoľko fáz životného cyklu celkovej bezpečnosti, bezpečnosti E/E/PES alebo bezpečnosti softvéru, stanovujú, pokiaľ ide o tieto fázy, za ktoré majú celkovú zodpovednosť, všetky manažmentové i technické činnosti nutné k tomu, aby E/E/PES súvisiace s bezpečnosťou dosiahli a udržali svoju požadovanú funkčnú bezpečnosť.

3. IEC 61511 – stručný prehľad

Norma IEC 61511 [5] *Funkčná bezpečnosť. Bezpečnostné riadiace systémy spojitých technologických procesov* je zameraná na implementáciu životného cyklu bezpečnosti procesných riadiacich systémov, kde technologické veličiny majú prevažne spojitý charakter a aj riadenie je spojitého charakteru (nie logické riadenie).

Má tieto časti:
– časť 1 – Požiadavky na systémy hardvéru a softvéru, štruktúra, definície,
– časť 2 – Metodický pokyn pre používanie IEC 61511-1,
– časť 3 – Pokyny pre stanovenie požadovanej celkovej úrovne bezpečnosti.



Obr. 3. Životný cyklus bezpečnosti softvéru riadiaceho systému – fáza návrhu

Norma prezentuje systematickú metódu na vypracovanie všetkých postupov týkajúcich sa rizika. Špeciálny dôraz kladie na dizajn a potvrdenie platnosti systémov týkajúcich sa bezpečnosti.

Základom normy je riadenie a funkčná bezpečnosť. Stratégia na dosiahnutie bezpečnosti by mala byť opodstatnená a mali by byť stanovené všetky činnosti, vrátane spôsobu hodnotenia ich dosiahnutia. Toto by malo byť časťou manažmentu funkčnej bezpečnosti.

Z tohto dôvodu norma určuje bezpečnostný životný cyklus, ktorý istí všetky fázy životného cyklu samotného systému. Životný cyklus bezpečnosti zahrnuje činnosti súvisiace s prístrojovou bezpečnosťou, ktoré sú riadené všetkými zúčastnenými, ako sú inžinierski pracovníci, dodávatelia, integrátori a koneční užívatelia. Všetci musia zavádzať manažérsky systém funkčnej bezpečnosti v časti životného cyklu systému, ktorá spadá do ich kompetencie, a musia medzi sebou úzko spolupracovať, aby dosiahli očakávanú úroveň celkovej bezpečnosti počas jeho životnosti.

Norma platí pre bezpečnostné prístrojové systémy založené na E/E/PES. Základné princípy tejto normy, ktorá bola vytvorená aj v nadväznosti na IEC 61508 do oblasti priemyselných procesov, sa však môžu použiť taktiež pre senzory, snímače a koncové členy bezpečnostných prístrojových systémov bez ohľadu na použitú techniku.

Norma vyžaduje zistenie všetkých bezpečnostných požiadaviek, aby boli posúdené nebezpečenstvá a riziká, vyžaduje, aby k bezpečnostným prístrojovým systémom boli pridelené bezpečnostné požiadavky, podrobne uvádza použitie niektorých činností v rámci manažmentu bezpečnosti, ktoré sa môžu použiť u všetkých metód funkčnej bezpečnosti, stanovuje požiadavky na architektúru systémov a konfiguráciu hardvéru, na aplikačný softvér a na integráciu systémov, na aplikačný softvér pre užívateľov a tvorcov softvérových bezpečnostných prístrojových systémov a obzvlášť špecifikuje:
– požiadavky na fázy životného cyklu bezpečnosti a činnosti, ktoré sa uplatňujú po-

Tab. 1. Dôležité skratky

C&E	*Causes and Effects*	matica príčin a následkov
E/E/PES	*Electrical/Electronic/Programmable Electronic*	elektrický/elektronický/elektronický programovateľný
FAT	*Factory Acceptance Test*	akceptačný test dodávateľa
HAZOP	*Hazard and Operative Report*	zdravotná a riziková analýza prostredia (metóda analýzy rizík)
ISO	*International Organization for Standartization*	Medzinárodná organizácia pre normalizáciu
IEC	*International Electrotechnical Commission*	Medzinárodná elektrotechnická komisia
PES	*Programmable Electronic System*	programovateľné elektronické systémy
PSM	*Process Safety Managment*	manažment procesu bezpečnosti
PLC	*Programmable Logic Controller*	programovateľný logický automat
SAT	*Site Acceptance Test*	prevádzkový akceptačný test
SIF	*Safety Instrumented Function*	bezpečnostná prístrojová funkcia
SIL	*Safety Integrity Level*	úroveň integrity bezpečnosti
SIS	*Safety Instrumented System*	bezpečnostný prístrojový systém
SRS	*Safety Requirement Specification*	špecifikácia bezpečnostných požiadaviek

čas návrhu a vývoja aplikačného softvéru – obsahujú požiadavky na použitie opatrení a techník dovoľujúcich zabrániť chybám v programe a kontrolovať vznik možných porúch,
- informácie o validácii bezpečnosti softvéru,
- informácie potrebné pre používateľa počas prevádzky a údržby.

Ďalej norma uvádza zoznam činností potrebných pre stanovenie funkčných požiadaviek a požiadaviek na integritu bezpečnosti pre bezpečnostné prístrojové systémy. Platí pre všetky fázy životného cyklu bezpečnosti, od začiatočného návrhu, cez implementáciu, prevádzku a údržbu až po vyradenie z prevádzky. Norma tiež stanovuje vzťah medzi IEC 61508 a IEC 61511. Používa sa pre široké spektrum výrob s prevahou kontinuálnych výrobných procesov, ako sú chemické výroby, ropné rafinérie, výroba benzínu a olejov, v nejadrových elektrárniach a výrobniach tepla.

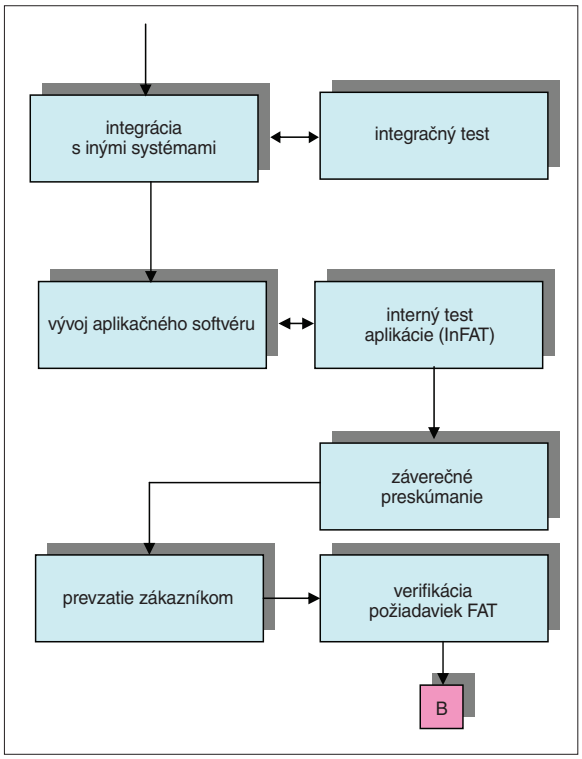
Oblasť použitia IEC 61508 a IEC 61511 v rámci noriem pre bezpečnostné prístrojové systémy je uvedená na *obr. 2*.

4. Návrh životného cyklu celkovej bezpečnosti

Ďalej prezentovaný životný cyklus celkovej bezpečnosti je založený na implementácii opísanej normy IEC 61508, ale najmä IEC 61511. Detailný opis je uvedený v [4].

V základnej štruktúre pre zentovaného návrhu sa nachádzajú tri fázy: fáza návrhu, fáza realizácie a fáza vykonávania. Paralelne s týmito fázami prebieha riadenie, plánovanie a kontrola jednotlivých krokov životného cyklu. Tieto činnosti sa potom zabezpečujú v manažmente funkčnej bezpečnosti plánovania a verifikácie.

Štruktúra navrhovaného životného cyklu bezpečnostného riadiaceho systému je zobrazená v schéme na *obr. 3* až *obr. 5*.



Obr. 4. Životný cyklus bezpečnosti softvéru riadiaceho systému – fáza realizácie

Na záver príspevku nasleduje detailnejší opis jednotlivých blokov schémy životného cyklu bezpečnostného riadiaceho systému.

4.1 Požiadavky zákazníka

Požiadavky zákazníka alebo subdodávateľa by mali byť úplné, technicky čitateľné a jednoznačné. Zákazník by mal mať spracované:
- prvotnú dokumentáciu celkového životného cyklu bezpečnosti,
- posúdenie rizík (môže ich spracovať aj inžinierska organizácia),
- tabuľku (maticu) príčin a následkov (C&E),
- prevádzkové predpisy pre riadenie prevádzky,
- celkové požiadavky na SIF.

4.2 Špecifikácia bezpečnostných požiadaviek na aplikačný softvér

Na základe vstupných informácií od zákazníka alebo koncového používateľa je potrebné posúdiť funkčnú bezpečnosť softvérovej aplikácie zabezpečujúcej bezpečnostnú integritu bezpečnostného systému.

4.3 Základný návrh, funkčná špecifikácia a architektúra aplikačného softvéru

V tomto kroku procesu životného cyklu sa rozhoduje o celkovej architektúre softvérovej aplikácie; o tom, s akými typickými zapojeniami sa bude pracovať po celý čas vývoja softvérovej aplikácie. Dôležitým vstupom je projektová dokumentácia hardvéru, ktorá obsahuje typické zapojenia, celkovú hardvérovú konfiguráciu, elektronickú formu zoznamu obvodov, signálov a jednotlivé parametre všetkých obvodov.

4.4 Vývoj aplikačného softvéru

V tejto časti životného cyklu bezpečnosti softvérovej aplikácie sa realizujú pôvodné požiadavky zákazníka, súčasne so zapracovaním bodu 4.3.

4.4.1 Integrácia s inými systémami

Bezpečnostné softvérové aplikácie sú obvykle spojené s ďalším softvérovým systémom; môže to byť napr. systém SCADA, systém blokovania, systém na manažérskej úrovni apod. Z toho dôvodu je potrebné overiť a nastaviť komunikačné prepojenie medzi všetkými systémami a subsystémami podľa zásad bezpečnostných aplikácií. Aj v tomto

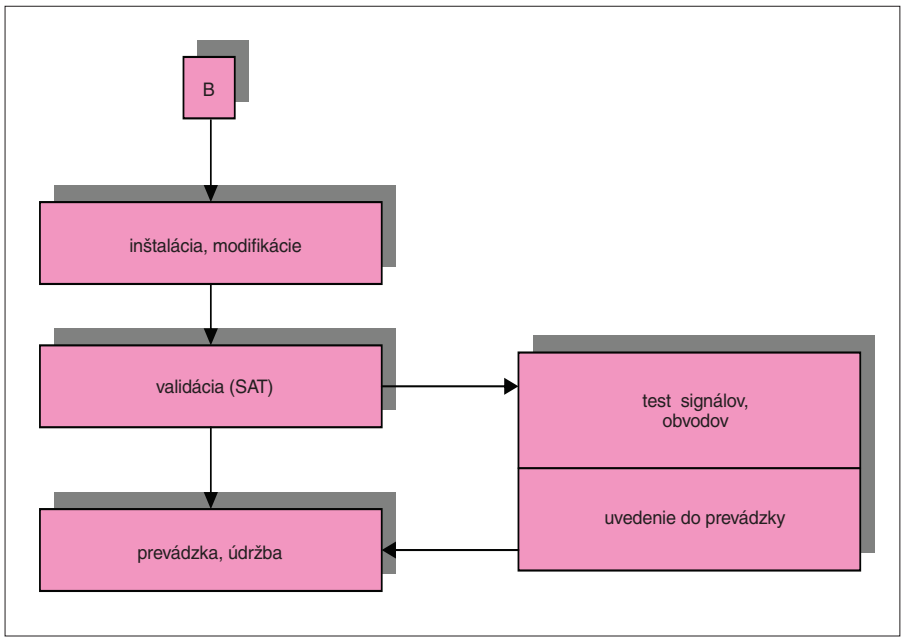
prípade každá bezpečnostná špecifikácia musí byť testovaná a dokumentovaná.

4.4.2 Tvorba aplikačného softvéru

Po vykonaní všetkých predchádzajúcich krokov sa pristúpi k samotnej tvorbe softvérovej aplikácie. Nové požiadavky zákazníka, ktoré by sa objavili v tejto časti životného cyklu, je potrebné prehodnotiť a posúdiť ich vplyv na celkovú bezpečnosť, a až potom zapracovávať do aplikácie.

4.5 Prevzatie zákazníkom

V procese preberania zákazníkom, ktoré je spravidla súčasťou FAT (akceptačné testovanie dodávateľom), zákazník kontroluje splnenie jeho používateľských požiadaviek a naplnenie požiadaviek celkovej bezpečnosti (SIS).



Obr. 5. Životný cyklus bezpečnosti softvéru – vykonávacia fáza

4.6 Inštalácia a modifikácie

SIS musia byť inštalované a uvedené do prevádzky v súlade s vhodným plánovaním. Všetky vykonané aktivity sa musia zároveň dokumentovať. Taktiež je potrebné dokumentovať výsledné riešenie, všetky modifikácie a spôsob odstránenia vyskytnutých chýb.

4.7 SAT – validácia

Keď je dokončené uvedenie SIS do prevádzky, uskutočňuje sa fáza celkovej validácie. Validácia sa musí vykonať v súlade s plánom celkovej validácie. Dôvodom je validovať systémy súvisiace s bezpečnosťou tak, aby spĺňali požiadavky týkajúce sa celkovej bezpečnosti. Návod, ako dokumentovať celú validáciu, je uvedený v normách IEC [1], [2] a [3]. Základné princípy a postupy testovania počas procesu validácie sú uvedené napr. v [7].

4.8 Manažment funkčnej bezpečnosti a plánovanie

Je treba dodržiavať zásady a odporúčania IEC 61511.

4.9 Prevádzka a údržba

Počas prevádzky a údržby systému s bezpečnostnými atribútmi sa musia zbierať prevádzkové údaje pre prípad výskytu chýb v systéme a nasledujúcej analýze príčin ich vzniku. Tieto údaje sa potom môžu použiť na verifikáciu, či predpoklady vykonané počas HAZOP boli správne, a takisto na verifikáciu, že intenzity porúch, ktoré boli použité vo výpočtoch SIL, boli skutočné. Ak sa vyskytne chybné spojenie, musia sa opakovať výpočty HAZOP a SIL. Operátori a personál údržby musia byť pravidelne školení (*refresh trainings*), aby sa udržiavala plná funkčná prevádzka a úroveň cieľovej integrity SIS vo validovanom stave.

4.10 Vyradenie SIS z prevádzky

Počas vyraďovacieho procesu musia byť všetky bezpečnostné prístrojové funkcie v prevádzke. Aby sa určil výsledný vplyv navrhovaného vyradenia na funkčnú bezpečnosť, musí byť urobená celková analýza. Tá musí obsahovať posúdenie celkovej bezpečnosti počas celého životného cyklu a musí vziať do úvahy funkčnú bezpečnosť aj počas vyraďovacích procesov, ako aj dopad vyradenia bezpečnostného prístrojového systému SIS na spolupracujúce prevádzkové jednotky.

5. Záver

Bezpečnostné riadiace systémy sú používané v prípadoch, kedy riadené procesy vyžadujú z hľadiska ich prevádzky zvýšenú úroveň bezpečnosti. Príkladom takých procesov sú dopravné systémy, potravinárske a farmaceutické technológie, chemické technológie s možnosťou zamorenia životného prostredia atď.

Aj keď spoľahlivosť a bezpečnosť navonok súvisia, treba zdôrazniť, že spoľahlivý systém nemusí byť bezpečný. Preto sú princípy návrhu bezpečného systému odlišné od návrhu spoľahlivého systému, a projektant teda musí zohľadňovať špecifiká bezpečnostných systémov.

Kritériá posudzovania dosiahnutej úrovne celkovej bezpečnosti môžu mať dvojaký charakter. Základné kritérium je počet nebezpečných udalostí (za jednotku času), ktorých následky znamenajú hmotné škody a zranenia alebo úmrtia osôb. Niekedy sa používa kritérium výšky nákladov na odstránenie následkov vzniknutých nebezpečných udalostí.

Tento príspevok predstavuje veľmi stručný pohľad na danú problematiku. V reálnej praxi implementácia relevantných štandardov, smerníc a odporúčaní znamená pre každú organizáciu značné zvýšenie nákladov na zavedenie manažérskych systémov, ich certifikáciu, ako aj udržiavanie a zlepšovanie súvisiacich procesov.

Literatúra:

[1] IEC 62337: *Commissioning of electrical, instrumentation and control systems in the process industry – Specific phases and milestones*. Ed. 1.0 English. IEC, 2006.

[2] IEC 62381: *Automation systems in the process industry – Factory Acceptance Test (FAT), Site Acceptance Test (SAT), and Site Integration Test (SIT)*. Ed. 1.0 English. IEC, 2006.

[3] IEC 62382: *Electrical and instrumentation loop check*. Ed. 1.0 English. IEC, 2006.

[4] GÁLIK, M.: *The safety development of SW industry application lifecycle according IEC 61508 and STN EN 61511*. Bc. Work. MtF STU Trnava, 2007, 48 p.

[5] IEC 61511: *Functional safety – Safety instrumented systems for the process industry sector – all parts*. Ser. Ed. 1.0 English. IEC, 2004.

[6] IEC 61508.2001. *Functional safety of electrical/electronic/programmable electronic safety related systems* – all parts. Ser. Ed. 1.0 English. IEC, 2005.

[7] TANUŠKA, P. – SCHREIBER, P. – VAŽAN, P.: *Testovanie softvérových systémov v procese validácie*. In: 7th International Scientific-Technical Conference PROCESS CONTROL 2006. Kouty nad Desnou, ISBN 80-7194-860-8.

prof. Ing. Dušan Mudrončík, CSc., MtF STU v Trnave (dusan.mudroncik@stuba.sk), Bc. Martin Gálik, ProCS, s. r. o., Šaľa (mgalik@procs.sk)

Recenzovali: Ing. Martin Hlinovský, Ph.D., FEL ČVUT v Praze, prof. Ing. Vilém Srovnal, CSc., FEI VŠB TU Ostrava