Výběr přístrojů pro bezpečnostní systémy

Steffen Langner

V průmyslových závodech se spojitými technologickými procesy na sebe poutají stále více pozornosti i prostředků bezpečnostní přístrojové systémy (*Safety Instrumented System* – SIS; bezpečnostní systém). Podle nové mezinárodní normy IEC 61511 (ANSI/ISA 84.01-2003 v USA), vydané v roce 2003, bude třeba při prokazování dostatečnosti bezpečnostních systémů používat deterministické metody. Uživatelé budou muset současně dodržovat uvedené nové normy i dosahovat agresivně určovaných cílů v oblastech pohotovosti závodu a celkových nákladů na zařízení. V současné době jsou již dostupné nové typy provozních přístrojů vyznačující se tím, že přístroje z téže skupiny lze, při splnění určitých podmínek, použít nejen v základním systému řízení technologického procesu, ale i v bezpečnostním systému. Uživatelé tak budou moci plnit požadavky nových norem v oblasti funkční bezpečnosti a současně dosahovat větší spolehlivosti (pohotovosti) a menších celkových nákladů na zařízení než s dosavadními přístroji. Podle nových norem musí uživatelé v bezpečnostních systémech používat výhradně buď přístroje od základu navržené podle normy IEC 61508 část 2 a 3, nebo provozní přístroje se známou provozní historií podle ustanovení o průkazu na základě předchozího použití, jak ho definuje norma IEC 61511. V článku jsou diskutovány přednosti a nedostatky obou způsobů a je navržen nový postup typu „nejlepší praktiky“, který je jejich kombinací.

1. Úvod

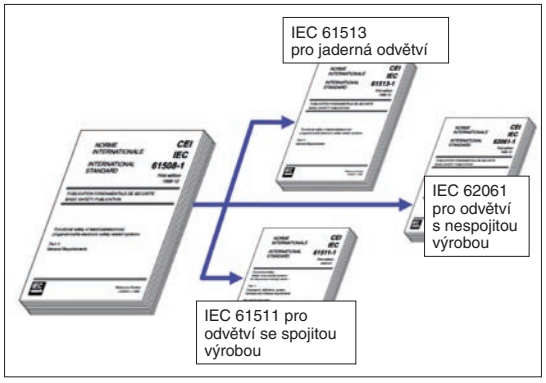
Cílem článku je představit postup typu „nejlepší praktiky“, vhodný pro výběr snímačů a akčních členů (dále „přístrojů“) pro bezpečnostní systémy vyhovující normě IEC 61511 (ISA 84.00.01-2004) při současné minimalizaci celkových nákladů vynaložených na zařízení během jeho životního cyklu (celkové náklady na zařízení).

Celkové náklady na zařízení se skládají z investičních nákladů (*Capital Expenditures* – CapEX), provozních nákladů (*Operating Expenditures* – OpEX) a nákladů na údržbu (*Maintenance Expenditures* – MaintEx), které jsou podskupinou OpEX. Co se týče těchto nákladů, jsou za prvé pro bezpečnostní systémy vyvinuty nové „bezpečnostně certifikované“ přístroje, které sice zajistí dostatečnou bezpečnost, ale často za cenu významného zvýšení výdajů na investice, provoz anebo údržbu. Za druhé projektanti strukturu bezpečnostních systémů mnohdy neuváženě předimenzovávají, což znamená větší investiční náklady. Za třetí mnoho společností zajistí funkční bezpečnost při použití přístrojů určených pro základní řídicí systém. S tím ovšem vyvstane potřeba realizovat nákladné programy průkazného sledování provozní historie přístrojů, čímž vzrostou náklady na údržbu. Nejlepší praktikou je vybrat snímač, který splňuje požadavky na funkční bezpečnost bez nutnosti realizovat programy dokumentující jeho provozní historii a současně je dostatečně provozně spolehlivý. Výsledkem jsou menší celkové náklady na zařízení.

2. Nové mezinárodní normy – přidaná hodnota pro provozní závody v odvětvích se spojitou výrobou

V roce 2003 byla pod označením IEC 61511 vydána nová norma pro oblast funkční bezpečnosti (*obr. 1*). Sestavili ji koneční uživatelé reprezentující mezinárodní konsorcium více než dvaceti zúčastněných zemí, včetně USA. Cílem normy je nabídnout jedinou sadu požadavků pokrývající celý životní cyklus bezpečnostního systému (identifikace, projekt, instalace, provoz a údržba, vyřazení z provozu) s přihlédnutím ke zvláštnostem odvětví se spojitými technologickými procesy (spojitou výrobou) tak, aby současně byla použitelná po celém světě. Norma má celkem sedm částí. Z hlediska předmětu tohoto článku jsou zejména důležité první tři:

– IEC 61511-1: Všeobecné požadavky,
– IEC 61511-2: Požadavky na hardware,
– IEC 61511-3: Požadavky na software.



Obr. 1. Norma IEC 61508: titulní list a dílčí normy IEC 61511, IEC 61513 a IEC 62061

Nová norma má pro provozovatele a integrátory zejména bezpečnostních systémů v odvětvích se spojitou výrobou velký význam. Za prvé, přestože lze očekávat, že jednotlivé standardizační orgány po světě přizpůsobí tuto normu specifickým podmínkám svých zemí, si firmy mohou pro bezpečnostní systém vytvořit standardizované procesy vyhovující převážné většině globálních požadavků. Za druhé se norma důsledně přidržuje přístupu vycházejícího ze životního cyklu bezpečnosti. Tento přístup uživatelům pomáhá navrhovat a realizovat bezpečnostní systémy plnící požadované bezpečnostní funkce (*Safety Instrumented Function* – SIF) v závodě, a to při uvážení celého životního cyklu zamýšlené bezpečnostní funkce, od jejího koncipování až po vyřazení z provozu.

Norma IEC 61511 vznikla v rámci normy IEC 61508, která je ovšem obecným dokumentem určeným pro všechna odvětví průmyslu, a stanovuje tedy i požadavky na výrobce komponent používaných v bezpečnostních systémech. Na rozdíl od normy IEC 61508 byla norma IEC 61511 vytvořena speciálně pro odvětví se spojitou výrobou a obsahuje pouze požadavky na konečné uživatele a integrátory bezpečnostních systémů v těchto odvětvích.

Norma IEC 61511 vyjmenovává požadavky na konečné uživatele a integrátory. Od výrobců a dodavatelů zařízení použitých v bezpečnostních systémech požaduje, aby se řídili ustanoveními uvedenými v normě IEC 61508 v části 2 (hardware/systém) a části 3 (software). To je velmi významný rozdíl, ilustrovaný na *obr. 2*.

Norma uvádí: IEC 61511-1, rozsah (b): „(Tato norma) se použije, když zařízení vyhovuje požadavkům normy IEC 61508, nebo části 11.5 normy IEC 61511 („předchozí použití“ nebo „osvědčené v praxi“) a je integrováno do celkového systému určeného k použití v odvětví se spojitou výrobou, *ale nemohou ji použít výrobci, chtějí-li prohlašovat, že zařízení je vhodné k použití v bezpečnostním systému* pro odvětví se spojitou výrobou.“

Norma IEC 61511 dále jasně říká, že výrobci zařízení použitého v bezpečnostním systému se musí řídit požadavky částí 2 a 3 normy IEC 61508 vyjma případu, že konečný uživatel splňuje požadavky části 11.5, za-

vádějící metodu průkazu vycházející z tzv. *předchozího použití* („*prior-use*“, „*proven-in-use*“). Je třeba si povšimnout, že výrobce nemůže prohlásit, že plní požadavek předchozího použití podle normy IEC 61511. To je odpovědnost konečného uživatele. Výrobci se musí řídit ustanoveními o předchozím použití uvedenými v normě IEC 61508.

3. Požadavky na přístroje použité v bezpečnostních systémech

Norma IEC 61511 stanovuje specifické požadavky na přístroje (snímače a koncové akční členy) použité v bezpečnostním systému. Koneční uživatelé mají při jejich výběru jen dvě možnosti:

– vybrat přístroj od samého počátku zkonstruovaný podle požadavků normy IEC 61508 část 2 a 3 (přístroj navržený podle IEC 61508),
– vybrat přístroj na základě ustanovení o předchozím použití podle normy IEC 61511 (tzv. osvědčený v praxi).

Uvedené požadavky platí bez ohledu na to, kterému (měřicímu) principu se v daném případě dává přednost.

Norma IEC 61511 uznává přínosy ke zvýšení bezpečnosti plynoucí z použití přístrojů od základu zkonstruovaných s ohledem na funkční bezpečnost (*safety designed instruments*, bezpečné přístroje), přičemž excelentním nástrojem je v tomto ohledu norma IEC 61508 část 2 (hardware) a část 3 (software). Norma také připouští možné problémy provázející použití bezpečných přístrojů, zejména:

– nedostatek výrobců nabízejících přístroje navržené podle normy IEC 61508,
– nedostatek informací o spolehlivosti nových konstrukcí vedoucí k možnému častějšímu výskytu neopodstatněných zásahů,
– výrobní závody mohou mít s používáním existující přístrojové techniky v bezpečnostních systémech mnohaleté zkušenosti.

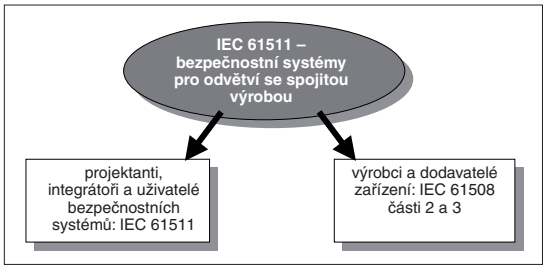
K řešení uvedených problémů norma umožňuje konečným uživatelům využít druhou možnost (*obr. 3*). Tou je metoda vycházející z ustanovení o předchozím použití přístroje („osvědčení se v praxi“).

4. Přístroje navržené podle IEC 61508 část 2 a 3

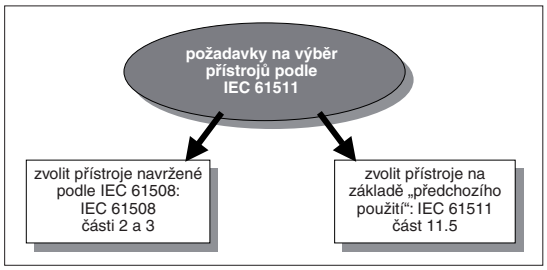
Jako přístroje „navržené (s certifikátem) podle IEC 61508“ se označují provozní přístroje, jejichž konstrukce odpovídá požadavkům na hardware, systémové vlastnosti a software podrobně popsaným v normě IEC 61508 část 2 a 3. Tato norma vychází z tabulky úrovní integrity bezpečnosti (*Safety Integrity Level* – SIL), s jejímž použitím stanovuje úroveň bezpečnosti daného provedení přístroje.

Výrobce použije k dosažení shody přístroje s normou IEC 61508 obvykle tento postup:

– sestaví specifikace požadavků na bezpečnost a požadavků na bezpečnostní funkce,
– navrhne strukturu přístroje a jeho hardware podle „pravidel“ v části 2 normy,
– navrhne, ověří, potvrdí a zkontroluje software a systémy podle „pravidel“ v části 3 normy s ohledem na požadovanou SIL (úroveň bezpečnosti zařízení),
– k ověření funkce diagnostiky provede zkoušky zaváděním poruch,
– zavede do systému změnového řízení kontrolní procedury,



Obr. 2. Cílové skupiny uživatelů norem IEC 61511 a IEC 61508



Obr. 3. Požadavky na výběr přístrojů podle normy IEC 61511

– zavede systém řízení kvality výroby, který zajistí, že nedojde k degradaci úrovně bezpečnosti přístroje,
– provede analýzu možných poruch přístroje, jejich projevů a možností diagnostiky (*Failure Modes, Effects and Diagnostic Analysis* – FMEDA) a na základě výsledků určí poruchovost, podíl bezpečných poruch (*Safe Failure Fraction* – SFF) a pravděpodobnost poruchy při vyžádání funkce (*Probability of Failure on Demand* – PFD),
– podrobně stanoví požadavky na zkoušku prokazující jmenovitou hodnotu PFD,
– uzavře s oprávněnou organizací smlouvu o přezkoumání požadavků na přístroj, jeho hardwaru, softwaru a systémových funkcí a systému řízení jakosti třetí stranou,
– oprávněná organizace vydá zprávu a certifikát třetí strany,
– výrobce dodá „bezpečnostní uživatelskou příručku“, informující konečného uživatele o správném způsobu použití daného přístroje v bezpečnostním systému.

Oprávněnými organizacemi jsou např. TÜViT-Augsburg, Německo; TÜV Automotive München, Německo; Factory Mutual, USA a mnohé další. V některých případech se výrobci při plnění daných požadavků obrátí na průmyslové experty. Příslušné poradenské společnosti, jako je např. Exida, nejsou oprávněnými organizacemi, mají však zkušenosti s plněním požadavků normy IEC 61508 a jsou schopny zajistit specifické činnosti, např. provedou analýzu typu FMEDA a sestaví požadavky na bezpečnost.

Použít v bezpečnostním systému přístroje navržené podle IEC 61508 je pro konečné uživatele velmi výhodné. Získávají tím:

– možnost snadno dosáhnout shody s normou IEC 61511, protože za průkaz dosažení požadované úrovně bezpečnosti přístroje odpovídá dodavatel,
– jistotu, že hodnoty poruchovosti a PFD jsou platné a správné,
– jistotu, že při vývoji a výrobě přístroje bylo postupováno podle správných inženýrských postupů zavedených v oblasti bezpečnostních systémů, jak jsou definovány v mezinárodní normě IEC 61508 (zejména důležitých z hlediska minimalizace systémových chyb v softwaru),
– jistotu, že výrobce má zavedeny postupy změnového řízení pokrývající celý životní cyklus výrobku,
– bezpečnostní uživatelskou příručku a zprávy o certifikaci k podpoře správného použití daného přístroje v bezpečnostním systému.

Ačkoliv jsou přístroje navržené podle normy IEC 61508 pro projektanty velmi užitečné, ti musí k jejich použití v bezpečnostních systémech přistupovat nanejvýš uvážlivě. Při výběru přístroje je třeba mít na zřeteli zejména tyto skutečnosti:

– bezpečnostní certifikát sám o sobě neznamená, že byla ověřena spolehlivost zařízení – „bezpečný“ neznamená „spolehlivý“; aby bylo možné posoudit možnou četnost výskytu neopodstatněných zásahů, je třeba pečlivě prověřit údaje o poruchovosti,
– co se týče předchozích zkušeností s jejich použitím, představují přístroje navržené podle IEC 61508 „nepopsaný list“ – žádná taková zkušenost se od nich nevyžaduje; použití nevyzkoušených a použitím v praxi neprověřených zařízení v bezpečnostních systémech je ovšem nanejvýš riskantní; dříve, než je takto použijí, by si uživatelé měli zařízení vyzkoušet jinde,
– údaje o poruchovosti přístrojů dodávané jejich výrobci *nezahrnují* poruchovost rozhraní mezi přístroji a technologickým celkem, což je při výběru přístroje velmi důležité; velká hodnota SSF (*Safe Failure Fraction*), tj. malý podíl potenciálně nebezpečných poruch přístroje, sama o sobě nestačí, neboť nebude zahrnovat nebezpečné

poruchy typu ucpání, zamrznutí nebo výskytu nečistoty v potrubí nebo úniku plynu,
– je třeba pečlivě číst dokumenty ohledně certifikace i bezpečnostní uživatelskou příručku,
– bezpečnostní certifikáty mnoha výrobků platí jen při významně častém či pracném prověřování jejich stavu anebo ve velmi úzkém rozsahu jejich provozních podmínek.

5. Přístroje vybrané na základě ustanovení o předchozím použití

Mezinárodní výbory, které připravily normy IEC 61508 a IEC 61511, uznaly, že uživatelé si mohou pro účely certifikace komponent určených pro smyčky bezpečnostních systémů zvolit také jiná kritéria. Proto normy obsahují ustanovení o předchozím použití („osvědčení v praxi“). Toto ustanovení nabízí uživatelům metodiku umožňující jim používat v bezpečnostních systémech i takové snímače a akční členy, které nebyly navrženy podle normy IEC 61508 část 2 a 3.

V ustanoveních o předchozím použití říká norma IEC 61511 mj. toto: *IEC 61511-1, část 11.5.3.1:* „Musí být k dispozici *přiměřené důkazy*, že komponenty a subsystémy jsou vhodné k použití v bezpečnostním přístrojovém systému.“

V případě přístrojů je „přiměřeným důkazem“ jedině dokumentovaný případ použití daného typu přístroje, jehož dokumentace obsahuje (viz IEC 61511-1, část 11.5.3.2):
– důkladné posouzení výrobce z hledisek jeho kvalit, manažerského řízení a systémů pro správu konfigurace,
– dostatečnou identifikaci a specifikaci přístroje, jeho komponent anebo subsystémů,
– demonstraci chování přístroje (komponent, subsystémů) v podobných režimech činnosti a provozních podmínkách.

Norma umožňuje uživatelům prokázat požadovanou provozní zkušenost s použitím údajů jak z činnosti základního řídicího systému, tak i bezpečnostního systému. Nicméně ale požaduje, aby provozní zkušenost byla získána ve stejných podmínkách jako při plánovaném použití v bezpečnostním systému a aby nashromážděná data byla statisticky významná. Právo prohlásit jakékoliv zařízení za ověřené předchozím použitím ve smyslu normy IEC 61511 má navíc pouze jeho konečný uživatel – výrobci takové prohlášení vydat nemohou.

Prohlásit přístroj za ověřený předchozím použitím a použít ho v bezpečnostním systému je pro konečného uživatele v mnoha ohledech výhodné. Za prvé si tím zajišťuje, že jsou vybrány přístroje se známou spolehlivostí. Tím se zmenší pravděpodobnost výskytu neopodstatněných zásahů i výdaje na výměnu porouchaných přístrojů. Za druhé vybrané přístroje již velmi dobře znají jak projektanti, tak i údržbáři. Postupy při instalaci mohou být tytéž jako při jejich použití v základním řídicím systému a není třeba ani doškolovat údržbáře, ani rozšiřovat sklad náhradních dílů. Za třetí, historie poruch těchto přístrojů bude obvykle zahrnovat také poruchy jejich rozhraní s technologickým celkem. To je důvod, proč norma IEC 61511 dovoluje prohlásit přístroje za ověřené předchozím použitím jen konečnému uživateli, a nikoliv výrobcům nebo dodavatelům.

Přestože použití ustanovení o předchozím použití nabízí konečným uživatelům určité výhody, nese s sebou i mnoho skrytých nákladů a rizik:
– konečný uživatel musí vést záznamy o provozních hodinách, pracovních podmínkách a poruchách přístrojů (náklady na údržbu),
– riziko výskytu systémových chyb zaviněných softwarem je vyšší, protože způsob vývoje softwaru u výrobce pravděpodobně nebude na té úrovni kvality, kterou požaduje norma IEC 61508 část 3 (provozní náklady),
– nepříznivě se projevuje nevyhnutelné změnové řízení; výrobci přístroje neustále pozměňují, ať už z důvodu zastarávání součástek, přidávání dalších funkcí nebo snižování nákladů; tyto změny mají vliv na dokumentaci zachycující provozní historii přístroje u uživatele a mohou – ve smyslu provozní zkušenosti – přivést uživatele až do situace, kdy nezbude než začít s průkazem použitelnosti znovu o začátku (investiční náklady, náklady na údržbu).

V souhrnu norma IEC 61511 připouští, aby koncoví uživatelé používali v bezpečnostních systémech jak přístroje navržené podle normy IEC 61508, tak „certifikované“ podle ustanovení o předchozím použití. Oba způsoby mají svoje přednosti i nedostatky. Každý z nich sám o sobě plní požadavky na bezpečnost, v obou případech však mohou být negativně ovlivněny celkové náklady na zařízení. Přístup typu „nejlepší praktiky“ spočívá v kombinaci metody „navržen podle normy IEC 61508“ s prvky metody založené na ustanovení o předchozím použití podle normy IEC 61511.

6. Přístup k výběru přístrojů pro SIS typu „nejlepší praktiky“

6.1 Princip

Přístup typu „nejlepší praktiky“ k výběru přístrojů pro bezpečnostní systém je vybrat přístroj navržený podle normy IEC 61508 část 2 a 3 a přitom žádat přístroj téhož typu, jaký je předepsán a používán v základním řídicím systému, a také s toutéž provozní spolehlivostí.

Jde o přístup, který má z pohledu koncových uživatelů významné výhody:
– zajišťuje shodu s normou IEC 61511 při dodávce veškeré dokumentace požadované výrobcem zařízení,
– minimalizuje možnost výskytu systémových chyb v softwaru, neboť software bude navržen a certifikován podle ustanovení normy IEC 61508 část 3,
– minimalizuje možnost výskytu neopodstatněných zásahů bezpečnostního systému, protože spolehlivost bude odpovídat spolehlivosti přístrojů použitých v základním řídicím systému,
– sjednocením veškerého školení personálu (projektantů i údržbářů) se dosahuje vyšší úrovně bezpečnosti při menších nákladech,
– společný sklad znamená menší náklady na náhradní díly a jejich skladování,
– lze použít jednotné postupy při instalaci prvků jak základního řídicího systému, tak i systému bezpečnostního, a dosáhnout tak větší bezpečnosti a menších nákladů.

Konečný uživatel může při použití uvedené praktiky dosahovat významných úspor specifikovaných v následujících odstavcích (v členění podle nákladových položek, které dohromady tvoří celkové náklady na zařízení).

6.2 Úspory investičních nákladů (CapEX)

Norma IEC 61511-1 požaduje od bezpečnostních systémů určitou minimální odolnost proti poruše, vycházející z jejich úrovně integrity bezpečnosti (SIL). Odolnost proti poruše je definována jako schopnost funkční jednotky pokračovat v plnění požadované bezpečnostní funkce za přítomnosti poruchy. Projektanti obvykle dosahují požadované odolnosti proti poruše použitím redundantních přístrojů s výstupy zavedenými do logické vyhodnocovací jednotky realizující určitý algoritmus výběru. Norma stanovuje minimální hodnoty odolnosti proti poruše, které projektant může poté upravit na konečnou hodnotu na základě použitých přístrojů a daných provozních podmínek.

V *tab. 1* jsou uvedeny minimální požadované hodnoty odolnosti proti poruše v závislosti na úrovni integrity bezpečnosti požadované od bezpečnostních systémů, jak je uvádí norma IEC 61511. Norma uvádí potřebnou minimální odolnost proti poruše, ale

Tab. 1. Odolnost hardwaru proti poruše (Hardware Fault Tolerance – HFT) podle normy IEC 61511

SIL	Odolnost proti poruše (FT)	Úprava 1[1)]	Úprava 2[2)]
1	0	0	1
2	1	0	1
3	2	1	2
4	3	2	3

[1)] Zmenšit FT o 1, jestliže konečný uživatel má přístroj odpovídající ustanovení o předchozím použití podle IEC 61511 („osvědčený v praxi“), nebo dodavatel nabízí přístroj navržený podle IEC 61508.
[2)] Zvětšit FT o 1, mohou-li na rozhraní s technologickým celkem vzniknout nebezpečné chybové stavy (např. ucpání potrubí).

dovoluje uživateli zmenšit její hodnotu o jedničku, jestliže:
– přístroj byl vybrán s použitím ustanovení o předchozím použití podle normy IEC 61511,
– přístroj byl navržen podle IEC 61508 část 2/3 (při použití tabulek odolnosti při poruše podle normy IEC 61508 část 2),
– jde o přístroj typu *smart*, u něhož však lze měnit pouze parametry zařízení (nikoliv firmware) a který je chráněn proti zápisu (buď hardwarově, nebo softwarově).

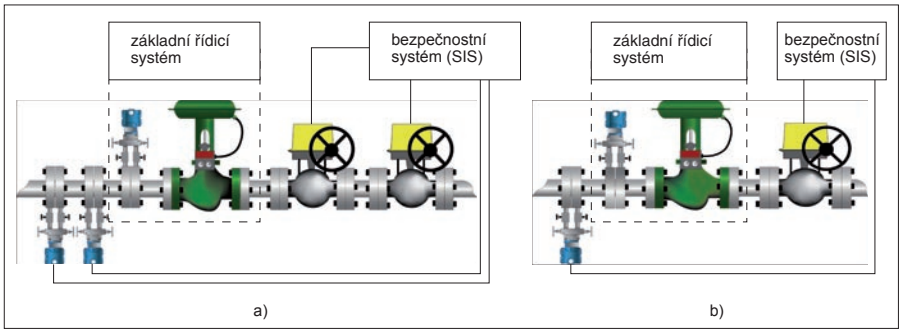
Dále norma IEC 61511 od projektanta požaduje, aby prověřil všechny možné vlivy a stavy na rozhraní mezi přístrojem a sledovaným zařízením nebo procesem, které by mohly vést k nebezpečnému poruchovému stavu. U přístrojů může jít o ucpání nebo zamrznutí potrubí, únik plynu apod. Existují-li jakékoliv možnosti vzniku nebezpečné poruchy, musí se hodnota odolnosti proti poruše opět o jedničku zvětšit. Popsaný rozhodovací strom je shrnut v *tab. 1*. Uvedená „úprava 1“ odpovídá snížení odolnosti proti chybě při použití přístroje dodaného s certifikátem podle normy IEC 61508 nebo vybraného na základě ustanovení o předchozím použití podle normy IEC 61511 a „úprava 2“ zvýšení požadované odolnosti proti chybě v případě, kdy na rozhraní mezi přístrojem a technologickým celkem potenciálně existují jakékoliv nebezpečné poruchové stavy.

Při použití přístroje prověřeného předchozím použitím podle ustanovení normy IEC 61511 nebo navrženého podle normy IEC 61508 a neexistují-li nebezpečné chyby, může uživatel odolnost proti chybě s výhodou zmenšit. Výsledkem pro něj je úspora investičních nákladů, protože k dosažení potřebné odolnosti proti poruše je zapotřebí o jeden přístroj méně. Příklad úlohy se SIL 3 je na *obr. 4*.

K vyřešení problémů s nebezpečnými poruchami lze využít diagnostické postupy. Například diagnostická funkce měření driftu čidla v převodníku teploty zjišťuje degradaci vlastního snímacího prvku vlivem pracovních podmínek. K tomu, aby bylo možné použít takovouto diagnostiku při hodnocení kvality bezpečnostní smyčky, je nutný systém pro správu výrobních aktiv (*Asset Management System* – AMS). Ten zobrazí informaci a vyzve údržbáře k vykonání potřebných kroků. V tomto bodě je třeba zdůraznit, že AMS, možná integrální součást logické vyhodnocovací jednotky, přispívá ke snížení provozních nákladů. Možnými zdroji úspor jsou:
– automatizované vedení dokumentace (např. záznamy provozní historie přístroje, kalibrace, dokládání ověřovacích zkoušek),
– možnost provádět ověřovací zkoušky *on-line*.

6.3 Úspory provozních nákladů (OpEX)

Použití přístrojů navržených podle normy IEC 61508 a současně osvědčených v praxi předchozím použitím v základním řídicím systému přispívá k úspoře provozních nákladů dvěma způsoby. Za prvé půjde o přístroje s ověřenou spolehlivostí, což může vést k menší četnosti případných neopodstatněných zásahů, a tudíž k větší pohotovosti závodu. Za druhé konečný uživatel tím, že použije zařízení navržené podle normy IEC 61508, nemusí realizovat program dokumentování provozní historie přístroje a ušetří významnou část režijních nákladů. Jsou-li v bezpečnostním systému použity přístroje s malou spolehlivostí, může to mít negativní vliv na pohotovost závodu. Příčinou neopodstatněných zásahů bezpečnostního systému jsou obvykle chybné signály došlé z přístrojů. Mnoho projektantů se bude pokoušet zmenšit četnost neopodstatněných zásahů zvýšením redundance. Tato cesta ovšem vede k vyšším investičním nákladům (CapEX). Nejlepší metodou je udržet redundanci na minimu cestou redukce četnosti případných neopodstatněných zásahů. Nejsnazší způsob, jak toho dosáhnout, je použít v obou systémech, základním řídicím i bezpečnostním, přístroje se stejnou spolehlivostí.



Obr. 4. Příklad použití HFT s kreditem: a) úloha SIL 3: HFT = 1, b) úloha SIL 3: HFT s kreditem při použití přístroje s certifikátem podle IEC 61508 nebo s průkazem „předchozího použití“ podle IEC 61511 (poznámka: rozhraní s technologickým celkem musí být zkontrolováno ohledně možnosti výskytu nebezpečných poruch)

6.4 Úspory nákladů na údržbu (MaintEX)

Uživatelé mohou dosáhnout úspor v mnoha položkách nákladů na údržbu, specifikují-li do bezpečnostního systému přístroje téhož typu, který používají v základním řídicím systému; samozřejmě za předpokladu, že tyto přístroje existují v provedení certifikovaném podle normy IEC 61508.

Zejména *odpadne sledování a dokumentování provozní historie pro průkaz „předchozího použití“*. Jak již bylo uvedeno, ustanovení o předchozím použití vyžaduje od uživatele, aby u přístrojů určených pro bezpečnostní systém zdokumentoval úplnou provozní historii přístroje během celého jeho životního cyklu. To může být velmi nákladné a pracné. Při použití přístrojů navržených podle normy IEC 61508 všechna tato starost odpadá. Pro konečného uživatele používajícího přístroje vybrané na základě ustanovení o předchozím použití je totiž značným rizikem změnové řízení. Výrobci své produkty neustále pozměňují, ať už z důvodu zastarávání součástek, zdokonalování vlastností nebo snižování nákladů. Tyto změny budou mít vliv na údaje posuzované podle ustanovení o předchozím použití a v mnoha případech donutí uživatele k tomu, aby s dokumentováním provozní historie přístroje začal znovu „od nuly“. Zařízení navržená podle IEC 61508 musí být během svého životního cyklu udržována a za dokumentaci a certifikaci v tomto případě odpovídají jejich výrobci.

Dále *ubude průkazných zkoušek*. Uživatelé musí určit, jak se budou provádět průkazné zkoušky bezpečnostních smyček, a vést o nich záznamy. Jako součást těchto zkoušek musí být provedena také verifikace komponent jednotlivých smyček. Například u snímačů to obvykle znamená provést každých dvanáct měsíců provozní kalibraci. U nových konstrukcí převodníků typu *smart* jsou kalibrační intervaly obvykle prodloužené, a to až na deset let. Při sjednocení použitých přístrojů lze prodloužit intervaly mezi ověřovacími zkouškami, a tím snížit náklady na provozní kalibrace. Při delším intervalu mezi ověřovacími zkouškami může konečný uživatel také synchronizovat příslušnou zkoušku s plánovanou odstávkou závodu. Tím odpadne nutnost provádět ověřovací zkoušky za chodu technologického procesu, které mohou mít vliv na bezpečnost závodu a znamenají riziko pro personál.

Nemalá může být také *úspora nákladů na správu zásob a výcvik personálu*. Použití přístrojů téže sady pro základní řízení i v bezpečnostním systému umožňuje uživateli minimalizovat sklad náhradních komponent. Je-li pro bezpečnostní systém vybrán nový přístroj, znamená to pro uživatele náklady na skladování jak nových přístrojů, tak přístrojů již používaných v základním řídicím systému. Použitím přístrojů jednoho typu se dosáhne nejen menších nákladů na výcvik týmu projektantů a údržbářů, ale také snížení rizika výskytu poruch metodické povahy zapříčiněných omyly techniků.

7. Další hlediska při výběru přístrojů pro bezpečnostní systém

Existují ještě další hlediska, k nimž musí projektant bezpečnostního systému při výběru určitého typu přístroje a jeho výrobce přihlédnout. Podrobnosti lze nalézt např. ve [4]. Zde se omezíme pouze na nejdůležitější aspekty výběru přístrojů pro libovolnou úlohu v oblasti řízení spojitých technologických procesů, zejména však k použití v bezpečnostním systému. Jsou celkem tři.

První zásadou je, že *přednost před ostatními nabízenými technikami mají převodníky typu* smart *v odolném průmyslovém provedení*. Zkušenost ukazuje, že nejvhodnějším typem např. snímačů pro bezpečnostní systémy jsou převodníky tlaku a teploty v provedení určeném pro odvětví se spojitou výrobou. Tyto přístroje jsou navrženy jako velmi spolehlivé za všech podmínek, s nimiž se lze setkat při řízení průmyslově provozovaných spojitých technologických procesů, a mají při nich dostatečnou výkonnost a doby odezvy i krátkou střední dobu potřebnou na zotavení (*Mean-Time-to-Restoration* – MTTR). Převodníky typu *smart* jsou také zdroji spojitého elektrického signálu, takže logické jednotky v bezpečnostním systému mohou zjistit, že z převodníku nepřichází žádný signál anebo že jsou iniciovány jeho vnitřní výstražné signály.

Za druhé jsou důležité *výkonnost a doba odezvy v provozních podmínkách*. Ke všem dodaným přístrojům výrobce přikládá prohlášení, v němž potvrzuje jejich výkonnost a dobu odezvy výstupu na změnu vstupu při určitém rozsahu provozních podmínek. Jde o údaje důležité pro projektanta bezpečnostního systému. Výkonnost mnohých přístrojů se může v důsledku tvrdých provozních podmínek měnit natolik, že je ovlivněna jejich schopnost iniciovat bezpečnostní signál. Dobu odezvy přístroje je třeba znát proto, aby projektant bezpečnostního systému mohl zaručit, že systém vykoná požadovanou bezpečnostní funkci za dobu, kterou na to má k dispozici.

Za třetí je třeba věnovat pozornost *způsobu instalace*. Z hlediska zajištění bezpečnosti jsou kriticky důležité jak projekt, tak i provedení instalace přístroje. Stav nebezpečný z hlediska jeho možné poruchy může vzniknout v důsledku mnoha různých událostí mimo vlastní přístroj, např. ucpání potrubí, koroze nebo úniku plynu atd. Správnou instalací lze takové systémové vlivy redukovat nebo zcela vyloučit.

8. Souhrn a doporučení

V současné době jsou k dispozici nové mezinárodní normy pro přístrojové bezpečnostní systémy (SIS). Tyto normy ukládají uživatelům používat přístroje buď navržené podle IEC 61508, nebo vybrané na základě ustanovení o předchozím použití podle normy IEC 61511. Každá z obou metod sice splní požadavky na bezpečnost, ale současně může také způsobit nárůst celkových nákladů na zařízení. Přístup typu „nejlepší praktiky“ je použít kombinaci těchto alternativ a zvolit pro bezpečnostní systém přístroje navržené podle IEC 61508 část 2 a 3 a současně dostatečně spolehlivé. K tomu, aby si uživatelé byli jisti, že dodavatelé dokážou splnit již uvedené požadavky, musí od dodavatelů pro přístroje, které hodlají použít ve svých bezpečnostních systémech, požadovat:

- certifikaci podle normy IEC 61508 spolu s dokladem o průkazně zjištěné spolehlivosti (zkouškami nebo na základě známé provozní historie),
- certifikaci shody s normou IEC 61508 od třetí strany,
- žádné dodatečné instalace, další úkony při uvádění do provozu či zkoušky navíc oproti těm, které požaduje u přístrojů určených pro základní řídicí systém,
- hodnoty poruchovosti, PFD s požadovaným časovým intervalem mezi průkaznými zkouškami a četnosti neopodstatněných zásahů stanovené na základě výsledků FMEDA, údaje ze zkoušek spolehlivosti a detailní popis provozních vlastností přístroje,
- doklad o postupech používaných při změnovém řízení; ty musí zajistit, že během životního cyklu přístroje nenastanou změny, které by měly vliv na jeho shodu s normou IEC 61508.

Dodavatelé, kteří splní uvedené požadavky, dovolí uživateli použít při výběru přístrojů pro bezpečnostní systémy způsob odpovídající „nejlepší praktice“. Tedy praktice, která umožní dosáhnout požadované bezpečnosti při minimálních celkových nákladech na zajištění bezpečnostní funkce.

Literatura:

[1] *IEC 61511 (2003) Functional safety: Safety Instrumented Systems for the process industry sector – Part 1.*

[2] *ISA 84.00.01 (2004) Functional safety: Safety Instrumented Systems for the process industry sector – Part 1* (verze IEC 61511 používaná v USA).

[3] *IEC 61508 (1997–2000) Functional safety of electrical/electronic/programmable electronic safety-related systems.*

[4] MENEZES – BROWN: *Measurement Best Practices for Safety Instrumented Systems*. May 2003.

[5] *Guidelines for Safe Automation of Chemical Processes*. Center for Chemical Process Safety of the AICHE.

[6] LAYER, T. J.: *Selecting „Sensors“ for Safety Instrumented Systems per IEC 61511 (ISA 84.00.01 – 2004)*. ISA, 2004.

Steffen Langner,
Emerson Process Management

Z anglického originálu *Innovative Safety Concepts in Pressure and Temperature Transmitters Including Possibilities for Assessments*, Emerson Process Management 2004; překlad a svolení k otištění Emerson Process Management, s. r. o.; úprava redakce.

krátké zprávy

▶ TD 2008 – Diagon 2008: diagnostika, spolehlivost a bezpečnost v průmyslu

Univerzita Tomáše Bati ve Zlíně (UTB), Vysoké učení technické v Brně, Český národní komitét IMEKO a Academia Centrum UTB pořádají dne 15. května 2008 ve Zlíně 31. mezinárodní konferenci s výstavou *TD 2008 – Diagon 2008* se zaměřením na:

- *technickou diagnostiku*: aktuální otázky údržby strojů a zařízení, moderní metody a postupy v údržbě a jejich počítačová podpora, diagnostické přístroje a metody, diagnostika v distribuovaných systémech, prediktivní diagnostika, odhadování rizik, ekonomické přínosy diagnostiky atd., včetně zkušeností z praxe,
- *spolehlivost*: teoretické otázky spolehlivosti, bezporuchovosti a udržovatelnosti; matematické nástroje, modelování a analýzy spolehlivosti; systémy údržby; provozní spolehlivost; standardizace ve spolehlivosti; systémy managementu a ekonomické aspekty spolehlivosti, analýza nákladů během životního cyklu; spolehlivost a bezpečnost,
- *bezpečnost*: teoretické otázky a použití metod bezpečnostního inženýrství; použití matematických nástrojů v bezpečnosti, modelování úniků a jejich následků, analýzy bezpečnosti i zkušenosti z průmyslových havárií, vyšetřování havárií, legislativa v bezpečnosti – Seveso I a II ATEX i audit bezpečnosti, hodnocení rizik včetně environmentálních, bezpečnost práce, přijatelnost rizika.

Uzávěrka příjmu příspěvků je 23. března, přihlášek pasivních účastníků 31. března a přihlášek vystavovatelů 20. dubna 2008. Podrobné informace lze získat na adrese http://www.diagon.utb.cz, popř. přímo v sekretariátu konference (e-mail: grulichova@rektorat.utb.cz, tel.: 576 032 062, 606 777 238). *(sk)*