Provozní přístroje a hledisko funkční bezpečnosti

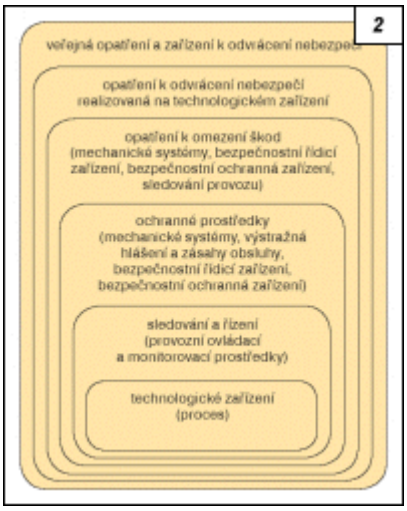
Požadavky na elektrické a elektronické komponenty a přístroje plnící při provozu technologických zařízení a jejich řídicích systémů tzv. bezpečnostní funkce jsou předmětem mnoha norem, směrnic a předpisů, v nichž je po jednotlivých činnostech popsán celý životní cyklus odpovídajících bezpečnostních systémů. V principu tímtéž způsobem jsou požadavky na bezpečnost průmyslových provozů stanoveny i v evropských normách IEC/EN 61508 a IEC/EN 61511, převzatých i jako směrnice německého Svazu pro elektrotechniku, elektroniku a informatiku VDE 0803 a VDE 0810 (odpovídající harmonizované české normy jsou IEC/ČSN EN 61508 a IEC/ČSN EN 61511 – *pozn. red.*). Tyto jmenovitě uvedené dokumenty jsou v současné době východiskem k systematickému posuzování tzv. funkční bezpečnosti technologických zařízení (procesů) v průmyslu. Základem je přitom určení příslušného stupně požadavků na bezpečnost (*Safety Integrity Level* – SIL) v závislosti na míře hrozícího rizika, a to s použitím *grafu rizik*. Při výběru komponent vhodných pro bezpečnostní systémy je třeba vedle hlediska bezpečnosti respektovat také jejich reálné provozní podmínky a další požadavky.

Platí jednotná mezinárodní pravidla

V oblasti provozních přístrojů došlo v souvislosti se zajišťováním funkční bezpečnosti technologických zařízení (procesů) prostředky měřicí, regulační a řídicí techniky založených na činnosti elektrických a elektronických přístrojů anebo komponent (*Safety Instrumented System* – SIS, bezpečnostní systémy) k významné změně. Od 1. srpna 2004 se totiž při posuzování funkční bezpečnosti technologických zařízení uplatňuje „nový pohled„ regulatorních předpisů a norem. Namísto dosavadních místních a firemních norem a předpisů vstoupily v platnost DIN EN 61508/VDE 0803 [1], normy nezávislé (generické) na technickém řešení a oblasti použití, a DIN EN 61511/VDE 0810 [2], dokumenty důležité především pro provozovatele spojitých technologických procesů. Tyto normy a směrnice poskytují návod k tomu, jak objektivně kategorizovat technologické zařízení a jeho řídicí systém podle celkové míry ohrožení, kterou společně představují pro své relevantní okolí. Postup spočívá v identifikaci a analýze všech hrozících nebezpečí a

Obr. 1. Princip uspořádání bezpečnostního systému (bezpečnostní smyčka)

stanovení skutečné a přípustné úrovně rizika vzniku každého z nich. Na základě zjištěného rozdílu mezi skutečnou a přípustnou úrovní rizika se stanovují určité minimální požadavky, které musí bezpečnostní systém za všech okolností splňovat. Bezpečnostní systém přitom zahrnuje všechny komponenty – včetně elektrických i elektronických, a to i programovatelných – potřebné k zajištění bezpečnostní funkce od vstupu veličiny do snímače až po zásah provedený akčním členem (*obr. 1*).



Základními pojmy, na nichž dále staví dokumenty DIN EN 61508/VDE 0803 a na ně navazující DIN EN 61511/VDE 0810, jsou pojmy celkový životní cyklus bezpečnosti a úroveň integrity bezpečnosti (SIL).

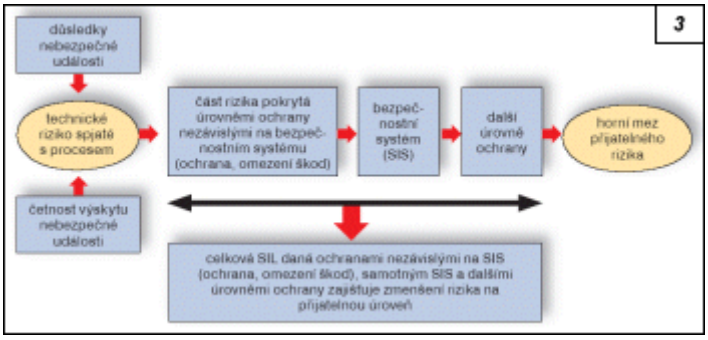
Obr. 2. Obvyklé metody zmenšování rizika při zajišťování funkční bezpečnosti technologických zařízení (procesů) na přípustnou anebo nižší úroveň

Životní cyklus bezpečnosti v sobě zahrnuje všechny nezbytné činnosti spjaté s existencí bezpečnostního systému od návrhu jeho prvotní koncepce, přes projektování, realizaci, uvedení do chodu, obsluhu a údržbu až po vyřazení z činného provozu a likvidaci. Bezpečnostní systémy mohou být založeny na nejrůznějších principech, technikách a prostředcích (chemické, hydraulické, pneumatické, elektrické, elektronické, v podobě programovatelných elektronických zařízení atd.).

Podrobněji o SIL a současně o nabídce společnosti Endress+Hauser ohledně bezpečnostních systémů informuje text vložený ve větším z rámečků. Pro čtenáře s hlubším zájmem o problematiku funkční bezpečnosti je v menším rámečku vložen seznam přehledových článků, které k tomuto tématu vyšly v poslední době v časopisu Automa (*pozn. red.*).

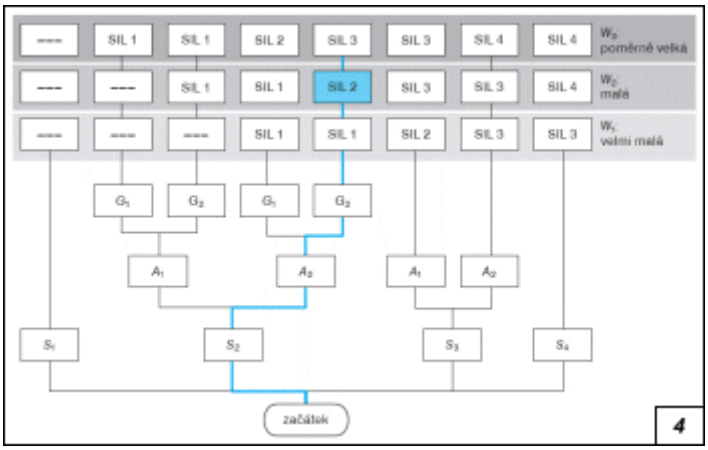
Nutné zmenšení rizika

Stěžejní veličinou, s níž se pracuje při zajišťování funkční bezpečnosti podle uvedených norem, je nutné zmenšení rizika. Jde o kvantitativní veličinu, jejíž hodnota udává, o kolik je třeba zmenšit riziko zjištěné při analýze nebezpečí, aby se dosáhlo přijatelného rizika, a to pro určitou konkrétní situaci. Koncepce nutné minimalizace rizika je základem postupu určování úrovně integrity bezpečnosti požadované od bezpečnostních systémů a jejich prvků.



Obr. 3. Riziko a koncepce úrovně integrity bezpečnosti (SIL)

Bezpečnostní systém v případě potřeby realizuje požadované bezpečnostní funkce, jejichž prostřednictvím uvede řízené zařízení (proces) do bezpečného stavu nebo ho v bezpečném stavu udržuje, a tím přispívá ke zmenšení skutečného rizika na přijatelné riziko. Celkového nutného zmenšení rizika lze dosáhnout bezpečnostními systémy nebo jinými metodami ochrany na různých úrovních, popř. kombinací obou způsobů (*obr. 2*). Součástí bezpečnostních systémů, a tudíž nositeli bezpečnostních funkcí mohou být také osoby, které po obdržení informace o stavu výrobního zařízení (procesu) učiní na jejím základě příslušná bezpečnostní opatření.



Pojem *riziko* v daném kontextu označuje míru pravděpodobnosti výskytu určité nebezpečné události a jejích účinků. Úroveň integrity bezpečnosti (SIL) je oproti tomu mírou pravděpodobnosti, s jakou bezpečnostní systém, popř. jiné úrovně ochrany či kombinace několika způsobů realizují požadované bezpečnostní funkce (*obr. 3*).

Obr. 4. Příklad grafu rizik: zařazení technologického zařízení podle výsledku rozboru rizik do SIL 2 (vysvětlení symbolů je v textu)

Poté, co je stanoveno přijatelné riziko a kvalifikovaně odhadnuto nutné zmenšení rizika, je možné stanovit požadavky na úroveň integrity bezpečnosti bezpečnostního systému a jeho komponent.

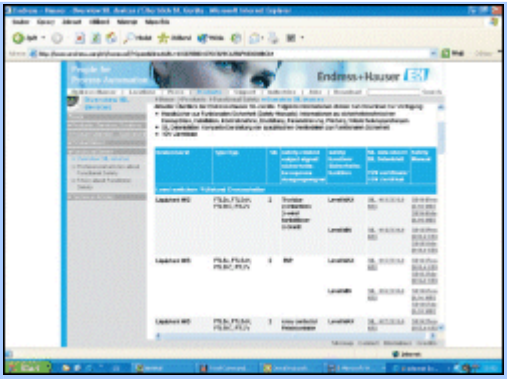
Tým pro určení SIL

Stupeň integrity bezpečnosti lze v jednotlivých případech v praxi stanovit různými způsoby. Záleží na mnoha aspektech, z nichž asi nejvýznamnější jsou:

- složitost úlohy,
- druh rizika a nutné zmenšení rizika, kterého je třeba dosáhnout,
- míra znalosti parametrů důležitých pro vznik rizika. Před projektováním technologického zařízení, a tudíž i bezpečnostního systému (jeho jednotlivých bezpečnostních smyček) musí být stanoveno, jaká SIL je od jednotlivých bezpečnostních smyček požadována. K tomu se

používá tzv. *graf rizik*, vycházející z principu, že riziko je úměrné době působení a četnosti vzniku nebezpečné události. Z toho vyplývají tyto charakteristické parametry rizika (*obr. 4*):

- účinky nebezpečné události *S*,
- doba setrvání v nebezpečné oblasti *A*,
- možnost vyloučit účinky nebezpečné události *G*,
- pravděpodobnost vzniku nežádoucí události *W*.



Co je SIL?

Koncept SIL (*Safety Integrity Level*) umožňuje objektivně stanovit riziko provázející provoz technologických zařízení (procesů) v průmyslu a zmenšit je na – a popř. i pod – přijatelnou úroveň. Příslušná norma DIN EN 61508/VDE 0803 (IEC/ČSN EN 61508 – *pozn. red.*), která je generickým standardem nezávislým na konkrétním řešení, popisuje obecné požadavky na komponenty a systémy zajišťující funkční bezpečnost průmyslových zařízení a procesů, včetně způsobu stanovení rizika (s použitím tzv. grafu rizik), a metody dimenzování příslušných bezpečnostních funkcí od snímačů, přes logické (řídicí) obvody až po akční členy tak, aby byly chyby buď vyloučeny (jde-li o systematické chyby), nebo udrženy pod kontrolu (chyby náhodné).

V normách DIN EN 61508 a návazné DIN EN 61511/VDE 0810 (IEC/ČSN EN 61511 – *pozn. red.*), která pokrývá specifickou oblast řízení spojitých technologických procesů, jsou definovány čtyři kategorie úrovně integrity bezpečnosti od SIL 1 (nejnižší úroveň bezpečnosti) po SIL 4 (nejvyšší úroveň bezpečnosti). Kategorie SIL reprezentuje výslednou pravděpodobnost výskytu nebezpečné poruchy dané bezpečnostní funkce. Pro každou SIL jsou stanoveny kvantitativní požadavky na pohotovost (*availability*) jednotlivých komponent bezpečnostního systému. Princip je ten, že čím více je třeba zmenšit riziko, tím větší požadavky jsou kladeny na systém, který riziko zmenšuje – tedy na jeho SIL.

Norma DIN EN 61511/VDE 0810 také stanovuje kritéria pro výběr komponent zajišťujících bezpečnostní funkce, mezi nimiž je např. požadavek používat jen provozně osvědčené snímače, řídicí prvky a akční členy. Tuto podmínku splňují komponenty tehdy, jestliže průzkum příslušné dokumentace o jejich dřívějším použití poskytuje dostatečné důkazy o tom, že jde o komponenty vhodné k použití v bezpečnostním systému. Dobu provozu jednotlivých komponent lze vzít v úvahu při výpočtech celkové doby provozu zařízení tehdy, byly-li komponenty v provozu po dobu nejméně jednoho roku.

Aby projektantům a provozovatelům bezpečnostních systémů usnadnila výběr přístrojů vhodných k použití v bezpečnostních systémech, nabízí společnost Endress+Hauser na své webové stránce na adrese http://www.endress.com/SIL aktuální přehled přístrojů pokrývající všechny významné veličiny měřené při sledování a řízení spojitých technologických procesů (poloha hladiny, tlak, teplota, průtok, fyzikálně-chemické parametry médií). Na uvedené adrese jsou současně nabízeny ke stažení dokumenty typu *Safety Manual*, katalogové listy přístrojů s důrazem na jejich bezpečnostní parametry a certifikáty TÜV obsahující veškeré údaje potřebné k projektování a provozování dotyčných přístrojů v bezpečnostní smyčce (*viz obrázek*).

Nezávisle na bezpečnostních parametrech definovaných v DIN EN 61508/VDE 0803 a DIN EN 61511/VDE 0810 je při výběru vhodných provozních přístrojů a komponent pro bezpečnostní systémy nutné respektovat také jejich skutečné pracovní podmínky (vibrace, rázy, znečištění, koroze, požadavky na EMC, teplota, krystalizace atd.).

Protože jeden člověk sám o sobě nemůže mít všechny zkušenosti potřebné k rozhodování o všech důležitých parametrech rizika, měl by být úkolem stanovit potřebnou SIL pověřen interdisciplinární tým. Do takového týmu zpravidla patří tyto osoby:

- specialista na příslušnou výrobní technologii,
- specialista v oboru řídicí techniky,

- zástupce vedení provozu (dílny, výrobního úseku),
- odborník na bezpečnost v průmyslu,
- provozovatel zařízení apod.

Technologické zařízení (proces) se s uvážením všech možných poruch a požadavků na bezpečnost s použitím grafu rizika zařadí do určité SIL, a to tím vyšší, čím větší je riziko (stupeň ohrožení) a pravděpodobnost vzniku poruchy.

Výhled do budoucnosti

Postup posuzování přístrojů a komponent v bezpečnostních systémech podle norem DIN EN 61508 a DIN EN 61511 bude začleněn mj. do aktualizované směrnice VDI/VDE 2180 [3]. Tento „nový pohled„ s jednoznačnými pravidly by měl být pro uživatele jednodušší. Důležité ovšem zůstává včasné zapojení odborníků. Jen tak může být výsledkem rozhodovacího procesu skutečně hospodárné zajištění funkční bezpečnosti technologického zařízení (procesu). Dále je důležité, aby výrobci i uživatelé nalezli cestu do normotvorných grémií a společně dospěli ke specifikaci ekonomicky přijatelného společného bezpečnostního standardu pro evropský průmysl.

Literatura:

[1] DIN EN 61508/VDE 0803: (Teil 1-7): *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme.* Beuth-Verlag, Berlin, 2002.
[2] DIN EN 61511/VDE 0810: (Teil 1-3): *Funktionale Sicherheit – sicherheitstechnische Systeme für den Bereiche der Prozessindustrie.* Beuth-Verlag, Berlin, 2004.
[3] VDI/VDE 2180: *Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik.* Beuth-Verlag, Berlin, 1998.

Karl-Heinz Gutmann,
Endress+Hauser Messtechnik GmbH & Co. KG,