Funkční bezpečnost bez kompromisů

Funkční bezpečnost nelze zajistit jen použitím certifikovaných komponent. O bezpečnosti je třeba přemýšlet během celého životního cyklu zařízení a brát v úvahu také člověka, protože právě ten je nejčastějším zdrojem bezpečnostních incidentů. Zákazníci navíc požadují, aby bezpečnostní prvky byly co nejlépe integrovány do automatizačního prostředí závodu nebo výrobní linky.

Co je bezpečnost? Podle definice je to vyloučení rizika. Jenže riziko nelze vyloučit nikdy, vždy určité zbytkové riziko zbude. Výroba je zkrátka vždycky „riskantní".

Úlohou bezpečnostních systémů je omezit riziko na přijatelnou úroveň. Ovšem sebelepší technika není nic platná, jestliže se nebere v úvahu člověk.

Když Evropská komise analyzovala příčiny nehod v chemickém průmyslu, vyplynulo z údajů sbíraných od roku 1982 do současnosti, že více než 90 % nehod bylo primárně způsobeno chybami v organizaci práce nebo nedodržením jejích pravidel. Pod tím se nejčastěji skrývá práce ve stresu, nedbalost nebo jiná lidská selhání.

Problémy v průběhu implementace

Jestliže se implementuje systém funkční bezpečnosti, uživatelé musí počítat s těmito skutečnostmi:

- bezpečnost musí být zajištěna v každé době, v provozu i mimo něj,
- bezpečnostní systémy jsou v činnost uvedeny jen zřídka, ale přesto se jim musí věnovat zvláštní pozornost,
- pro dosažení maximální efektivity výrobního procesu musí být zachována co největší dostupnost zařízení,
- od výrobců a dodavatelů výrobních zařízení je třeba vyžadovat bezpečnostní expertizu dodaných komponent,
- bezpečnostní technika se musí vyrovnat s rostoucí složitostí procesů a jejich segmentací,
- bezpečnostní systém nesmí být nákladnější, než je nezbytné.

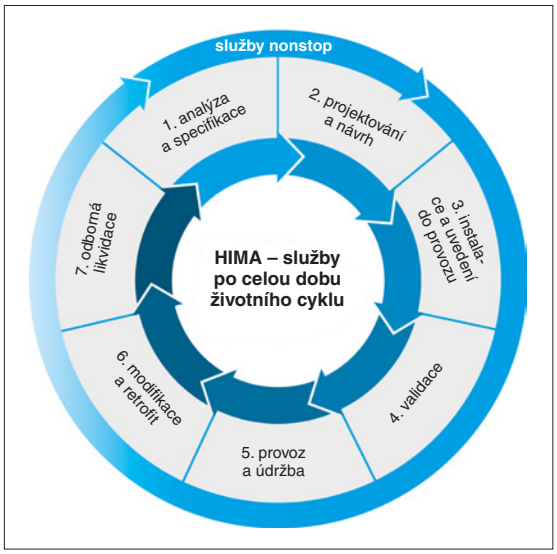
Funkční bezpečností se zabývají dvě mezinárodní normy, IEC 61508 a IEC 61511. Norma IEC 61508 se zabývá funkční bezpečností obecně, kdežto IEC 61511 se věnuje zvláště procesní výrobě.

Proč je pro mnoho firem problém implementovat funkční bezpečnost, když mají k dispozici uvedené normy? Protože to není jen otázka bezpečnostního systému, ale bezpečnostní kultury celého podniku.

Bezpečnost po celou dobu životního cyklu

Klíčovou součástí normy IEC 61511 je zajištění bezpečnosti po celou dobu životního cyklu. Má tři části: analýzu rizik, realizaci bezpečnostního systému a provoz zařízení. Další důležitý pojem je verifikace bezpečnosti na tzv. principu čtyř očí. Vše zastřešuje systém řízení funkční bezpečnosti.

Společnost HIMA podporuje své zákazníky po celou dobu životního cyklu bezpečnostního systému: poskytované služby zahrnují



Obr. 1. Společnost HIMA poskytuje svým zákazníkům úplné spektrum služeb

analýzu rizika ve fázi návrhu, integraci systému funkční bezpečnosti do DCS, poprodejní služby a školení (*obr. 1*). Odborníci firma HIMA pomáhají zákazníkům i při zavádění systémů řízení funkční bezpečnosti (FSM).

Systém řízení rizik a funkční bezpečnosti je povinný

Směrnice EU Seveso II nařizuje, že v podnicích s procesní výrobou musí být implementován systém řízení rizik a funkční bezpečnosti.

Systém FSM musí především jasně popsat procesy a stanovit odpovědnosti. Implementace systému FSM je složitá procedura a vyžaduje značné zkušenosti. Začíná pečlivým porovnáním existujícího systému s požadavky norem IEC. Následuje analýza, která stanoví stupeň shody a určí odchylky od ustanovení norem. Konečnou fází je adaptace celého systému tak, aby bylo dosaženo úplné shody s příslušnými normami.

Podobné procesy implementovala samotná HIMA již dávno před tím, než vstoupily v platnost jako normy IEC pro funkční bezpečnost. Systém FMS ve firmě HIMA je certifikován zkušebnou TÜV.

Již dlouho pomáhá HIMA implementovat systémy FMS také u svých zákazníků. Například už v roce 2004, krátce poté, co byly standardy pro funkční bezpečnost schváleny, pomáhala zavádět tento systém v rafinerii v Burghausenu (Německo; ve vlastnictví ÖMV Germany).

Kromě mnoha různých dílčích školení pořádá HIMA ve spolupráci s TÜV Rheinland také komplexní výukové kurzy, jejichž absolventi získají certifikát *Functional Safety Engineer*.

Certifikace sama bezpečnost nezaručí

Certifikace podle norem IEC 61508 a IEC 61511 je základem zajištění bezpečnosti, avšak mnohé negativní příklady z posledních let vyvolávají o účinnosti samotné certifikace značné pochybnosti. Někteří výrobci našli takové zalíbení ve hře s čísly, že bez uzardění „katapultují" svá zařízení do vyšší kategorie SIL např. prostě jen tím, že účelově zvýší počet bezpečných selhání, a tak ovlivní příslušný poměr bezpečných a nebezpečných selhání. Naštěstí tvůrci norem zareagovali a učinili takovým praktikám přítrž. Nicméně na trhu jsou stále zařízení, jejichž certifikace výrobci dosáhli podobným způsobem.

Samotný certifikát tedy bezpečnost nezajistí. Je dobré se zajímat o to, za jakých podmínek byl certifikát získán a co se píše v uživatelské příručce o tom, kdy výrobce zaručuje dodržení bezpečnostních funkcí a kdy tuto garanci přenáší na uživatele.

Intuitivní ovládání zabraňuje chybám

Zatímco řídicí systém je používán nepřetržitě, bezpečnostní systém je za normálních podmínek uveden v činnost jen zřídka. Z hlediska uživatele musí mít bezpečnostní systém intuitivní ovládání, které vede operátora při jeho rozhodování. A nejde jen o ovládání, stejně snadné a intuitivní by mělo být i programování, konfigurace, diagnostika a správa bezpečnostního systému.

Velký výpočetní výkon pro nové typy úloh

Velký výpočetní výkon bezpečnostních systémů HIMax (*obr. 2*) umožňuje realizovat složité bezpečnostní funkce založené ne-

jen na přímo měřitelných fyzikálních veličinách, jako je teplota, tlak nebo průtok. Body aktivace bezpečnostní funkce mohou být závislé na několika fyzikálních veličinách současně a určovány složitými matematickými vzorci. Díky tomu může být systém provozován blíže ke svým fyzikálním mezím, což zefektivňuje výrobu.

Jinou náročnou úlohou pro bezpečnostní systémy je řízení kompresorů a turbín. Díky vysokému výpočetnímu výkonu systému HIMax lze jediným systémem realizovat různé bezpečnostní funkce, např. ochranu proti překročení maximálních přípustných otáček, ochranu generátoru nebo řízení čerpadel. Přednostmi jsou úspora místa, úspora náhradních dílů, jednodušší obsluha a údržba, a tedy i nižší náklady.

Obr. 2. Nový bezpečnostní systém HIMax

Integrace založená na nezávislých standardech

Při integraci bezpečnostní techniky do provozního prostředí je třeba brát ohled na to, aby strategie nákupu negativně neovlivňovala strategii bezpečnosti. Oddělení nákupu často využívá seznamy osvědčených dodavatelů automatizačních systémů MAC (*Main Automation Contractor*) a přístrojového vybavení MIV (*Main Instrument Vendor*) a má snahu všechnu techniku, i tu bezpečnostní, nakupovat od těchto dodavatelů. Je to správné?

Jestliže je celá dodávka automatizační i bezpečnostní techniky přidělena jednomu dodavateli, je tu riziko, že dodávka sice bude vyhovovat všem standardům, ale – protože standardy připouštějí různé výklady – dodavatel ve snaze snížit náklady přece jen ušetří na kvalitě. Šetření na kvalitě řídicí techniky by se projevilo na snížení spolehlivosti a efektivity výrobních procesů. Ušetří-li se však na bezpečnostní technice, nikdo nic nepozná – dokud nedojde k havárii.

Podle normy EN 61511 musí být bezpečnostní technika (technika, který vykonává bezpečnostní funkce) nezávislá na činnosti běžné řídicí techniky (té, která vykonává funkce, jež nejsou spojeny s bezpečností). Tato nezávislost omezuje možnost výskytu systematických chyb a společných chyb obsluhy, které mohou způsobit narušení bezpečnosti.

Na fyzickém oddělení bezpečnostního a řídicího systému je výhodné také to, že změna řídicího systému např. při změně sortimentu výroby nemá vliv na bezpečnostní systém a výrobní zařízení zpravidla není třeba znovu certifikovat.

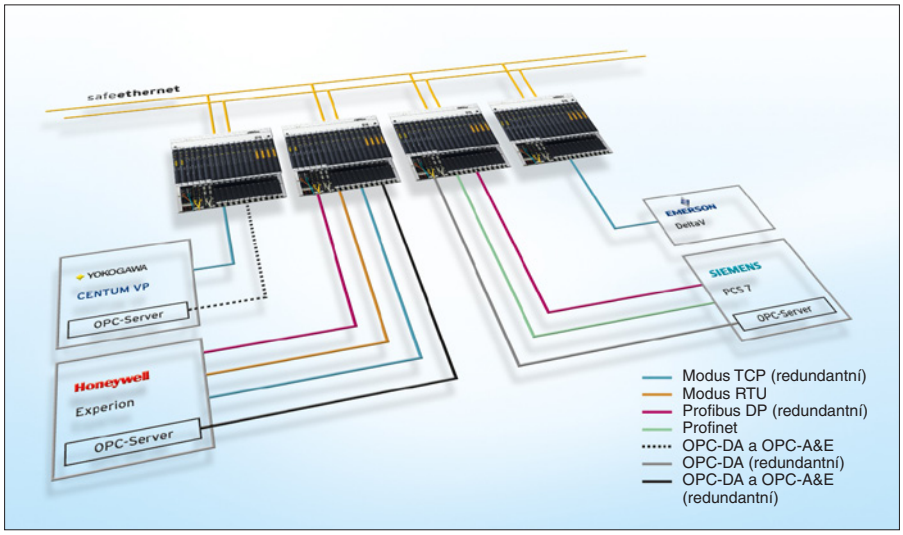
Stejný přístup, tj. vytvoření nezávislých zabezpečovacích linií, lze uplatnit i pro zajištění tzv. kybernetické bezpečnosti. Obrana se nejlépe zajišťuje několikaúrovňovým zabezpečovacím systémem. Poslední virové útoky na výrobní řídicí systémy jasně prokázaly, že nezávislost bezpečnostní techniky na řídicí je základní podmínkou pro to, aby se v takovém případě zabránilo velkým škodám.

Nejdůkladněji se nezávislost řídicí a bezpečnostní techniky zajistí tím, že jsou obě postaveny na odlišných platformách, vývojových principech a koncepci. Výhodou (i když ne podmínkou) je, když pocházejí od různých výrobců. Společnost HIMA nabízí bezpečnostní techniku s otevřenými komunikačními rozhraními, jež umožňují její kompletní, standardům zcela vyhovující integraci s mnoha systémy DCS známých značek.

Pro bezproblémovou integraci bezpečnostní techniky se systémy DCS je třeba mít dostatečné znalosti. Proto založila společnost HIMA speciální tým, který pomáhá zákazníkům na celém světě s integrací bezpečnostní techniky do DCS a poskytuje jim konzultace. Tým vytvoří pro zákazníka detailní dokumentaci, kde je integrace systémů popsána, a vykoná rozsáhlé testy integrace. Na jaře 2010 byl takový projekt realizován např. pro firmu Shell, která integrovala čtyři systémy HIMax se čtyřmi DCS (Yokogawa, Honeywell, Emerson a Siemens; *obr. 3*). Systém HIMax v testu obstál, dokázal své komunikační schopnosti a výkon a společnost Shell je s ním zcela spokojena.

Závěr

Systémy pro zajištění funkční bezpečnosti jsou kritickou součástí výrobních zařízení a vyžadují důkladnou analýzu situace a použití té nejmodernější techniky. Jen v takovém případě lze zajistit spolehlivý provoz výrobních zařízení bez kompromisů v oblasti bezpečnosti. Bezpečnostní systém musí být specifikován a vybírán nezávisle na DCS. Integrace založená na otevřených, na výrobci nezávislých komunikačních standardech je výhodná jak z hlediska funkční, tak kybernetické bezpečnosti a navíc zajišťuje velkou míru ochrany investic do nové techniky.



Obr. 3. Bezpečnostní systémy HIMax v projektu pro firmu Shell komunikují s DCS různých výrobců

Steffen Philipp, Thomas Hinzmann,
HIMA Paul Hildebrandt GmbH + Co. KG

(Článek je přeloženou a redakčně upravenou verzí plenární přednášky na generálním shromáždění NAMUR v listopadu 2010. Společnost HIMA byla generálním sponzorem tohoto shromáždění.)