Obr. 2. HARTING jako Solution Partner dodává firmě Siemens mj. speciální kabely pro větrné turbíny, které Siemens vyvíjí, dodává a uvádí do provozu po celém světě

Partnerství s firmou Siemens

Společnost Harting je oficiálním partnerem firmy Siemens (Siemens Solution Partner). V rámci dlouhými lety prověřeného partnerství vyvinula divize HCS množství řešení přesně podle zadání společnosti Siemens. Typicky jde o kabely a spojovací techniku pro výrobní linky v automobilovém průmyslu, dopravníky zavazadel na letištích nebo linky na třídění zásilek (*obr. 1*), stroje ve strojírenství, dřevozpracujícím nebo plastikářském průmyslu. Na *obr. 2* je příklad úspěšné spolupráce v energetice: Harting dodává osazené kabely pro větrné turbíny, které navrhuje a dodává Siemens. Výhodami dlouhodobého partnerství je úzká spolupráce a intenzivní výměna zkušeností. Společnost Harting tak dodává firmě Siemens z jednoho zdroje spojovací techniku pro běžné produkty i pro řešení navržená na zakázku.

Pro oblast automatizace dodává společnost Harting firmě Siemens široký sortiment konektorů a osazených kabelů pro rozvod napájení, včetně speciálních stíněných motorových kabelů, i pro rozvod signálů a dat s konektory M12 nebo RJ45.

Sdílení dat v cloudu

Významnou roli při spolupráci se zákazníkem hraje sdílení dat v cloudu. Obě strany mají k dispozici aktuální návrh řešení a mohou o něm diskutovat. Všechny procesy výběru, objednávky, výroby i dodání kabelů a propojovací techniky jsou digitálně mapovány.

Využití cloudu vnáší do výroby výhody globalizace. Produkty navržené divizí HCS ve spolupráci se zákazníkem potom mohou být vyráběny tam, kde je to nejvýhodnější: ve výrobních závodech firmy HARTING v Evropě, Asii nebo v USA.

(HARTING, foto: HARTING)

PLCopen vydává verzi 2.0 dokumentu Bezpečnostní specifikace

V únoru 2006 vydala organizace PLCopen dokument *Bezpečnostní specifikace, část 1 – Koncepty a přehled funkčních bloků pro bezpečnostní funkce*. Na tento dokument navazovaly uživatelské příručky a další části. Původní dokument popisuje funkce a rozsáhlé stavové diagramy, které přispívají k porozumění dané problematice. Text se odkazuje na příslušné normy, popisy chybových chování, ověření funkcí a identifikaci chybových kódů, přičemž rozlišuje různé úrovně programování. Jako takový je dokument ideální platformou pro subjekty implementující bezpečnostní software. Pro uživatele jsou potřebné další informace o bezpečnostních zařízeních, přípojkách a kódování.

Po tolika letech byla nutná aktualizace, což vedlo k vytvoření verze 2.0 příslušného dokumentu. Tato verze obsahuje mnohé změny:

– začleňuje původní část 3, zejména sekci o diagnostice a dalších pěti funkčních blocích,
– je doplněn popis syntaxe *Structured Text* (ST), stejně jako dodatečné datové typy a funkce,
– veškeré původní funkční bloky byly aktualizovány s ohledem na kód diagnostiky, požadavky na bezpečnost výstupů a vyžadované vynulování, přičemž funkce vynulování byla rozšířena prostřednictvím definice nových funkčních bloků,
– byly odstraněny tři funkční bloky související s řízením pohybu, přičemž tyto bloky byly připojeny k dokumentaci Safe Motion.

Principy nového standardu

Konstruktéři technických zařízení musí vyhovět mnoha bezpečnostním předpisům. Je velmi nákladné, a v některých případech dokonce nereálné všechny tyto standardy zohlednit. I přesto jsou konstruktéři zodpovědní za bezpečnost jimi navrhovaných zařízení. Tato nebezpečná situace není správná, zejména z důvodu dalších legislativních omezení vztahujících se na dodavatele zařízení. Přitom jejich odpovědnost je čím dál větší.

V současné době je často jednoznačně určena hranice mezi bezpečnostní a funkční složkou zařízení. Toto oddělení může být zajištěno použitím jiných systémů pro interakci zařízení s okolím, jiných nástrojů, a dokonce i oddělením zainteresovaných skupin pracovníků. Toto oddělení však často vede k tomu, že bezpečnostní funkce jsou přidávány až na samém konci vývoje zařízení, a nejsou tak integrovány do celkové koncepce systému už od samého počátku. Část funkcí je navíc pouze omezeně verifikována. Tato situace nepřispívá ke splnění celkových bezpečnostních požadavků.

Kromě toho dnes pokračující technická inovace přináší digitální komunikační sběrnice, které vyhovují příslušným bezpečnostním předpisům. Navíc dochází, a to i v oblasti bezpečnostních systémů, k odklonu od hardwarových systémů využívajících pev-

né propojení kabely k řešením s univerzálním hardwarem a softwarem vytvořeným na míru. Paralelu lze spatřovat s odklonem od logiky realizované pomocí relé k programovatelným logickým automatům (PLC). Takový trend s sebou nese změnu postoje dotčených subjektů. Změna tohoto typu však vyžaduje čas, rozsáhlou podporu průmyslu jako celku, stejně jako vzdělávacích institucí a certifikačních úřadů.

Ke komplexnosti problému navíc přispívají požadavky různých vládních organizací. Příkladem je americký FDA (*Food and Drugs Administration* – Úřad pro kontrolu potravin a léčiv), který stanovil přísné regulatorní předpisy, jež musí být v daném oboru dodržovány. Jejich nedodržení vyústuje ve vysoké finanční postihy. Zboží navíc nesmí být propuštěno na trh nebo musí být staženo.

Společné základní požadavky všech příslušných bezpečnostních norem na bezpečnostní aplikace, které musí konstruktéři zařízení zohlednit, jsou:
- rozlišení bezpečnostních funkcí a funkcí, které na bezpečnost zařízení nemají vliv,
- použití standardizovaných programovacích jazyků a podmnožin těchto jazyků,
- použití validovaných bloků softwaru,
- použití platných směrnic pro programátory,
- použití uznávaných opatření pro snížení výskytu chyb během životního cyklu bezpečnostních aplikací.

Úsilí, které musí uživatelé vynaložit ve snaze splnit uvedené požadavky, by mělo být minimalizováno. Toho lze dosáhnout využitím standardizovaných řešení, která usnadňují implementaci typických funkcí. Standardizace funkčních bloků, jejich integrace a podpora softwarovými nástroji umožňuje programátorům zohlednit bezpečnostní aspekty vyvíjených aplikací od samého počátku bez toho, aby tím byla nepříznivě ovlivněna jejich funkce či výkon, popř. vznikaly vícenáklady.

Pro dosažení těchto cílů pracují výbory PLCopen na dvou úrovních:
1. standardizace designu a uživatelského komfortu vztahující se k bezpečnostním funkčním blokům,
2. integrace standardizovaných procedur při vývoji prostředí.

Standardizace designu a uživatelského komfortu bezpečnostních funkčních bloků

Aby bylo vývojářům usnadněno využití bezpečnostních funkcí, musí být zvýšen komfort programovacího prostředí. Toho může být dosaženo standardizací designu a snadností ovládání bezpečnostních funkčních bloků. Tím může být bezpečnostní funkce lépe definována a využívána nezávisle na použitém řídicím systému. Není přitom zapotřebí přeškolení a tendence vytvářet speciální bezpečnostní funkce na míru je eliminována.

Navíc tento postup usnadňuje činnost certifikačním institucím. Specifikace a ověření bezpečnostního softwaru se tak stávají značně jednodušší, a proto rychlejší, bezpečnější a méně nákladné. Implementace funkčních bloků na vyšší úrovni je činí méně závislými na fundamentální architektuře hardwaru. Systémy s jednotlivými prvky propojenými kabely, systémy obsahující bezpečnostní vstupní a výstupní moduly a systémy propojené s komunikačními sítěmi mohou být vybaveny stejnými funkčními bloky. Díky tomuto řešení vyšší úrovně mohou být detaily implementace před uživateli skryty, což dělá implementaci bezpečnostního softwaru daleko snazší a méně nákladnou.

Integrace standardizovaných procedur

Jakmile se zmíněné funkce stanou součástí funkčních bloků, musí být v další fázi rozhodnuto o jejich kombinaci do podoby bezpečnostních programů. Na této úrovni by uživateli měly maximálně usnadnit práci příslušné softwarové nástroje. Za tímto účelem byl zaveden nový datový typ Boolean, který lze využít v bezpečnostním prostředí a který umožňuje rozlišit booleovské proměnné s vazbou a bez vazby na bezpečnostní funkce. To poskytuje základ nástroje pro vývoj programů, díky kterému lze identifikovat části programu kritické z pohledu bezpečnostních funkcí a který uživateli nabízí přípustné odkazy a naopak zabraňuje deklaraci nesprávných propojení. Tímto způsobem může být implementována podpora pro různé úrovně bezpečnostních standardů.

Dokument IEC 61508, část 7, zavádí omezení počtu preferovaných programovacích jazyků pro různé úrovně bezpečnostní integrity (SIL) – „vysoce doporučené“, „doporučené“ a „nedoporučené“. Na základě této klasifikace jsou preferovanými grafickými jazyky schéma funkčních bloků (FBD – *Function Blok Diagram*) a jazyk kontaktních schémat (LD – *Ladder Diagram*) se svými definovanými podskupinami. Tyto grafické jazyky poskytují jasný přehled o bezpečnostním programu jako takovém a vývojáři nástrojů mohou implementovat daleko kvalitnější úroveň podpory a návodu pro uživatele. Tím je vytvořen základ pro snadnější zprovoznění bezpečnostních programů. Kromě toho norma doporučuje jazyk ST (*Structured Text*) jako textový jazyk pro využití rozšířené úrovně programování.

To představuje významný přínos pro akceptovatelnost a použití bezpečnostních funkcí a tím eliminaci některých v současnosti existujících překážek, zejména z pohledu oboru konstrukce zařízení.

Tyto cíle byly identifikovány a Technickou komisí pro bezpečnost PLCopen (*Safety Technical Committe*) splněny:
- definice knihovny standardních funkčních bloků (FB) pro bezpečnostní funkce,
- kombinace těchto funkčních bloků s aplikačním programem.

To vyžaduje prostředí vhodné pro bezpečnostní aplikace. Požadavky a omezení vztahující se na tato prostředí jsou částečně uvedeny v popisovaném standardu.

Další splněné cíle jsou:
- přijetí konceptů a funkcí ze strany potenciálních certifikačních úřadů, čímž je položen základ certifikovatelným funkčním blokům,
- vytvoření nabídky uživatelsky přívětivého rozhraní k bezpečnostním funkcím,
- poskytnutí společného základu pro terminologii a odkazy,
- aktualizace souvisejících existujících bezpečnostních standardů,
- vytvoření „průvodce stylem“ pro dodatečné/budoucí funkční bloky,
- poskytnutí uživatelských návodů a příkladů,
- zajištění opakovatelné využitelnosti aplikačních programů nezávisle na platformě.

Pro zahrnutí dalších oblastí nad rámec konstrukce zařízení jsou předpokládány další doplňky. Tato doplnění mohou být realizována formou budoucích příloh k existujícímu dokumentu. Příslušná specifikace má být chápána jako otevřený rámec nezávislý na použitém hardwaru, který umožňuje implementaci na různých platformách. Vlastní implementace funkčních bloků není součástí uvedených standardů. Programování „bezpečnostní“ logiky a logiky bez vztahu k bezpečnostním funkcím má být ze strany programátora jednotné.

Na základě zmíněných cílů sestavila PLCopen specifikaci splňující základní bezpečnostní požadavky. Tato specifikace zahrnuje:
- reprezentaci softwarové architektury,
- definici programovacích jazyků a jejich podskupin,
- prezentaci bezpečnostních datových typů,
- definici uživatelských úrovní pro snadné programování a prevenci vytváření chybných příkazů,
- koncept diagnostiky a nápravy chybných příkazů,
- definici generických bezpečnostních funkčních bloků,
- definici množiny 22 bezpečnostních funkčních bloků,
- definici postupu při certifikaci shody s požadavky PLCopen v kombinaci s využitím loga PLCopen Safety.

Tento dokument se skládá ze tří hlavních částí:
- omezení počtu programovacích jazyků a funkcí pro usnadnění vytváření bezpečnostních aplikací,
- obecná pravidla pro bezpečnostní funkční bloky,
- definice množiny funkčních bloků zaměřených na bezpečnost.

Tato nová verze 2.0 dokumentu PLCopen *Bezpečnostní specifikace – část 1* je dostupná ke stažení z webové stránky www.PLCopen.org.

[Tisková zpráva PLCopen, srpen 2018.]

(Jiří Hloska)