Foundation Fieldbus SIF: budoucnost bezpečnosti procesů (část 1)

Larry O'Brien, Dick Hill

Systém bezpečnostních přístrojových funkcí využívající komunikační sběrnici Foundation Fieldbus (*Foundation Fieldbus Safety Instrumented Functions* – FF-SIF) ve své beta verzi úspěšně prošel zkouškami a výrobci začnou brzy dodávat výrobky odpovídající jeho specifikaci. To znamená velké změny na trhu s bezpečnostními přístrojovými systémy (*Safety Instrumented System* – SIS, tj. systémy určené k zajišťování funkční bezpečnosti spojitých technologických procesů). Změní se také způsob, jakým k systémům typu SIS budou přistupovat jejich koneční uživatelé. Autoři, pracovníci známé poradenské společnosti ARC Advisory Group z USA, specializované na automatizaci v průmyslu, v článku diskutují o významu techniky FF-SIS pro globální trh s bezpečnostními přístrojovými systémy a konečné uživatele. U čtenářů se předpokládají základní znalosti v oboru průmyslových komunikačních sběrnic, zejména sběrnice Foundation™ Fieldbus (FF), a bezpečnostních přístrojových systémů.

Foundation Fieldbus Safety Instrumented Functions (FF-SIF) have been successfully beta tested and products conforming to the FF-SIF specification will be available soon. This means big changes for the safety system market and a change in the way end users will approach safety instrumented systems (SISs). In the article the authors from well-known ARC Advisory Group discuss the implications of FF-SIF technology for the global plant safety system market and end users. Readers are expected to be familiar with basics of fieldbus technology, especially Fieldbus Foundation´s one, and safety instrumented systems technology as well.

1. Systém FF-SIF je rozhodující součástí automatizační infrastruktury Foundation Fieldbus

1.1 Foundation Fieldbus není jen náhrada analogové techniky 4 až 20 mA

Společnost ARC je pevně přesvědčena, že systém Foundation Fieldbus (FF) je více než jen pouhá komunikační síť a že je od základu vybudován tak, aby přinesl více než jenom digitální náhradu techniky 4 až 20 mA. Toto platí jak pro bezpečnostní systémy a systém FF-SIF, tak i pro použití systému FF v základních řídicích systémech technologických procesů (*Basic Process Control System* – BPCS). Systém FF představuje jednotnou infrastrukturu, jejímž prostřednictvím lze spravovat data, komunikační prostředky, výrobní zařízení a události v závodě při zajištění vysokého stupně distribuce řídicích činností a interoperability mezi zařízeními a subsystémy (*obr. 1*).

Užitné vlastnosti i technika umožňující jich dosáhnout jsou jistě významné, avšak samy o sobě nezakládají důvod k pořízení jakéhokoliv zařízení nebo softwaru, zejména při současné nechuti investovat. Koneční uživatelé věnují v současné době značnou pozornost otázkám hospodárnosti, a veškerá technika tudíž musí obstát při hodnocení podle ekonomických kritérií. Ve společnosti ARC sledujeme, jak jsou v odvětvích se spojitými technologickými procesy opakovaně vznášeny stále tytéž požadavky diktované ekonomikou – na zvýšení spolehlivosti chodu procesů cestou péče o jejich tzv. celistvost, na zavedení efektivních postupů agregace dat a informací v podniku (*business intelligence*) a na vytvoření rozšiřitelného společného prostředí použitelného jak při realizaci malých řídicích úloh, tak při řízení velkých provozních celků, kdy je nutné spolu integrovat mnoho různých řídicích domén. Systém FF pomáhá řešit všechny tři uvedené okruhy požadavků a je třeba na něj nahlížet jako na techniku umožňující dosáhnout komplexních přínosů (*obr. 2*).

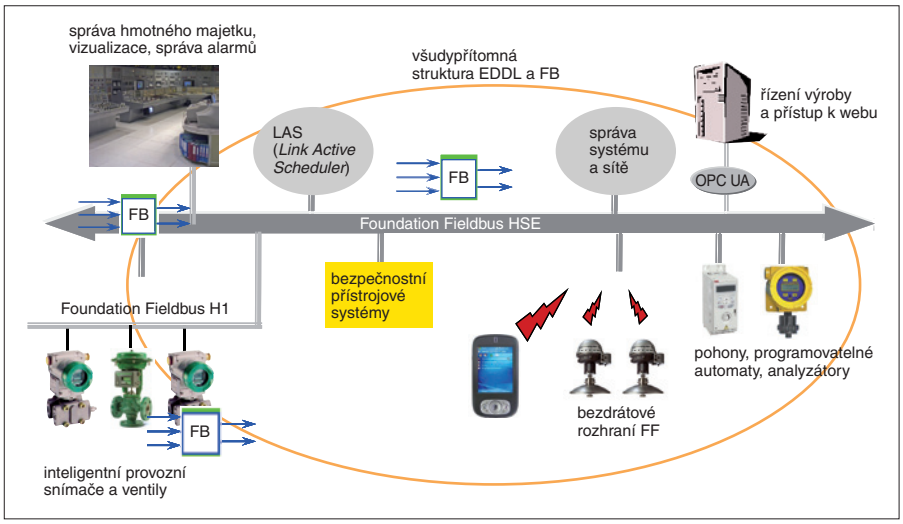
1.2 Systém FF zajistí především celistvost procesu

Technologický proces je celistvý tehdy, je-li závod udržován v dobrém stavu a funguje co možná nejspolehlivěji při současném uplatňování strategie proaktivní údržby. Vznikne-li v takovém závodě mimořádná situace a je třeba ho zastavit, děje se tak logickým a řízeným způsobem, který zamezí vzniku nepoužitelného odpadu a, což je ještě důležitější, také újmě na zdraví lidí a životním prostředí. Současně je ale důležité vyhnout se bezdůvodným, falešným zásahům bezpečnostního systému, které negativně ovlivňují produktivitu, aniž by vzrostla bezpečnost.

Jako podpora postupů *business intelligence* je požadován globální a spolehlivý přístup k datům, umožňující uživatelům v různých rolích v závodě získat kdykoliv a z libovolného místa v systému data, která aktuálně potřebují. Data přitom musí být prezentována způsobem umožňujícím je snadno pochopit a poté jednat.

Požadavek na otevřenost a rozšiřitelnost infrastruktury řídicího systému je diktován potřebou zbavit se nákladů na zakázkovou integraci systému a umožnit vybraným nejlepším produktům svého druhu bezproblémově spolupracovat v otevřeném prostředí.

Otevřená automatizační infrastruktura FF vychází všem těmto uvedeným požadavkům vstříc několika různými cestami.

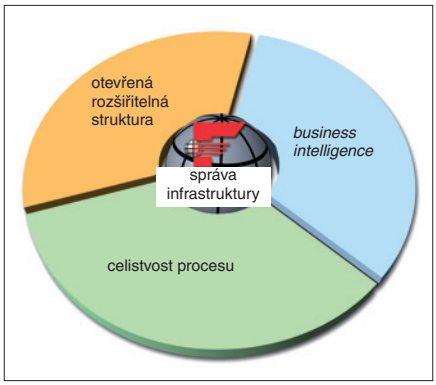


Obr. 1. Bezpečnostní přístrojové funkce (SIF) jsou přirozeným rozšířením automatizační infrastruktury Foundation Fieldbus (FF)

1.3 Význam integrace bezpečnostních funkcí

Systém FF-SIF představuje společnou základnu pro realizaci bezpečnostních i vlastních řídicích funkcí, kterou společnost ARC obhajuje ve svém modelu „stejné, ale oddělené“, platném pro bezpečnostní systémy. Podle tohoto modelu spolu základní systém pro řízení technologického zařízení (BPCS) a systém zajišťující funkční bezpečnost zařízení (SIS) sdílejí tutéž řídicí síť a mohou používat společné zobrazovací a vývojové nástroje i systém správy hmotného majetku, zatímco logické operace se vykonávají pro každý z obou systémů samostatně. Sdílená společná základna znamená menší náklady na instalaci, eliminaci nákladů na zakázkovou integraci systému a možnost dosáhnout jednotného způsobu správy základního řídicího systému, technologického zařízení i bezpečnostního přístrojového systému.

Tradičním způsobem, jak zajistit funkční bezpečnost technologického zařízení, je přidat k němu komponenty chránící personál pracující na nebezpečných místech závodu nebo

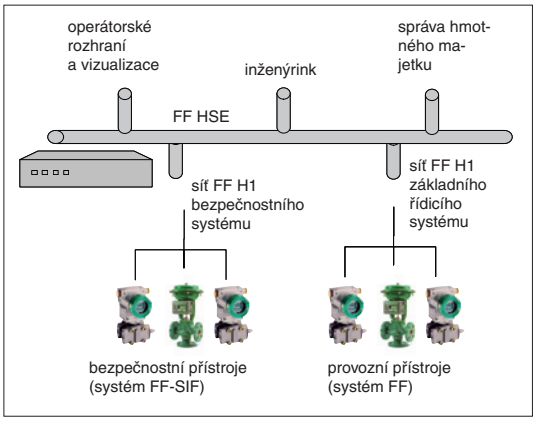


Obr. 2. Hlavním přínosem automatizační infrastruktury Foundation Fieldbus je schopnost zajistit celistvost procesů

blízko nich před zraněním nebo usmrcením a podnik před ekonomickou ztrátou. Moderní přístupy k zajištění funkční bezpečnosti tento tradiční rámec ovšem daleko překračují. Mnoho konečných uživatelů si nyní uvědomuje, že při použití inteligentních, integrovaných bezpečnostních systémů mohou dosahovat lepších hospodářských výsledků a současně zvýšit bezpečnost procesů i personálu.

Použití tradičních samostatných bezpečnostních systémů vede k rozdílným projektovým a provozním požadavkům na základní řídicí systém a systém bezpečnostní. Primární úlohou základního řídicího systému je udržovat předem stanovené hodnoty určitých provozních proměnných bez ohledu na změny v okolním prostředí. Bezpečnostní přístrojový systém je oproti tomu statický, vyčkávající na příležitost k akci, která uvede řízený proces do bezpečného stavu v případě, že se stal neovladatelným a samotný základní řídicí systém ho již nedokáže udržet v bezpečných mezích. Výsledkem byl vznik systémů dvojího typu – systémů pro řízení procesu a systémů pro zajištění funkční bezpečnosti – se samostatnými operátorskými rozhraními, inženýrskými pracovními stanicemi, konfiguračními nástroji, archivy dat a událostí, systémy péče o zařízení a komunikačními sítěmi. Toto vše má nepříznivý vliv na náklady na pořízení infrastruktury, měřicího a řídicího hardwaru a kabeláže, na integraci systémů, na projektové činnosti i na instalaci a spouštění zařízení v závodě.

Při tradičním přístupu jsou větší i další výdaje během životního cyklu zařízení, např.



Obr. 3. Společná struktura realizovaná s použitím systému FF-SIF snižuje náklady na instalaci i provoz a zvyšuje provozní spolehlivost zařízení

na náhradní díly, technickou podporu, školení, údržbu a servis. Další náklady jsou vyvolány tím, že příslušná rozhraní jsou technicky náročná a jejich údržba a synchronizace vyžadují kvalifikovanou odbornou pracovní sílu. Pro konečné uživatele je to drahé řešení, zejména při vědomí, že pokud se nic neporouchá, nelze u výdajů na bezpečnostní systém kalkulovat s určitou návratností.

Donedávna měli uživatelé jen malou šanci postupovat jinak, než použít pro řízení a pro zajištění bezpečnosti zcela samostatné systémy. Někteří z nich dokonce trvali na tom, aby základní řídicí systém a bezpečnostní systém byly dodány různými výrobci. K tomu, aby bezpečnostní funkce na jedné a řídicí funkce na druhé straně byly zajišťovány různými řídicími jednotkami, je i nadále mnoho pádných důvodů, např.:

– *nezávislost poruch*, tj. minimalizace rizika současné poruchy řídicího a bezpečnostního systému (porucha se společnou příčinou),
– *informační bezpečnost*, tj. potřeba zbránit tomu, aby změny provedené v základním řídicím systému způsobily změnu nebo degradaci funkcí přidruženého bezpečnostního systému,
– *odlišné požadavky na bezpečnostní řídicí jednotky*, neboť bezpečnostní systém je běžně zkonstruován tak, aby se popř. porouchal předvídatelným a bezpečným způsobem, zatímco základní řídicí systém je obvykle navržen se snahou po maximální spolehlivosti; bezpečnostní systém má také některé zvláštní vlastnosti, jako např. rozšířené diagnostické funkce, speciální kontrolu chyb softwaru, chráněnou paměť dat a odolnost proti poruše.

Tab. 1. Přínosy integrace bezpečnostních a řídicích systémů a související problémy

Přínosy	bez přenosů (mapování) dat
	jediná sada inženýrských nástrojů
	výrazně menší pracnost integrace
	menší celkové náklady na zařízení
Problémy k řešení	vložení hardwarových a softwarových bariér mezi bezpečnostní a řídicí systémy
	zajištění odpovídajících zábran proti nežádoucímu přístupu
	zajištění vizuálního rozlišení řídicího a bezpečnostního prostředí na úrovni pracovních stanic

Výrobní útvary jsou v současné době tlačeny k tomu, aby nepřetržitým zvyšováním výkonnosti výrobního zařízení co nejvíce zlepšovaly hospodářské výsledky svých společností. V současné době jsou sledovány zejména dvě metriky, a to návratnost investic do hmotného majetku (*Return on Assets* – ROA) a celková efektivita zařízení (*Overall Equipment Efficiency* – OEE), které dohromady nejvýrazněji ovlivňují vzdálenost dělící firmu od ideálního celkového cíle – dosažení tzv. provozní excelence (*Operational Excellence* – OpX). „Osudovým údělem“ všech výrobců je neplánovaná odstávka – neočekávané zastavení výroby z důvodu závady na zařízení, chyby obsluhy nebo neopodstatněného zásahu bezpečnostního systému. Systém FF-SIF nejenže nabízí zdokonalenou diagnostiku minimalizující riziko falešných spuštění bezpečnostních funkcí. Ještě důležitější je, že ho lze integrovat přímo do standardních řídicích struktur a využít jejich pokročilé metody správy zařízení a událostí, a tak minimalizovat pravděpodobnosti rizika vzniku poruchy (*obr. 3*). Základní přínosy i problémové stránky integrace bezpečnostních a řídicích funkcí jsou uvedeny v *tab. 1*.

2. Historie a bezpečnostní koncept systému FF-SIF

2.1 Historie systému

Začátkem roku 2006 organizace Fieldbus Foundation oznámila, že certifikační orgán

TÜV Rheinland vydáním dokumentu typu *Protocol Type Approval* odsouhlasil její specifikace pro oblast bezpečnostních přístrojových systémů (Foundation Fieldbus Safety Instrumented Systems – FF-SIS), navržené v souladu s normou IEC 61508, určující požadavky na funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů spjatých s bezpečností až do úrovně SIL 3 (*Safety Integrity Level 3*) včetně.

Dokument TÜV Protocol Type Approval umožňuje realizovat na bázi sběrnicového systému FF úplná řešení v oboru bezpečnostních přístrojových systémů (SIS) pro širokou paletu úloh řešených v průmyslových provozech a závodech. Specifikace umožňují výrobcům řídicí techniky konstruovat zařízení odpovídající normě IEC 61508. Certifikát potvrzující, že jde o zařízení vhodné k použití v bezpečnostních přístrojových systémech, vydá TÜV. Výrobci předpokládají, že začnou předkládat TÜV svoje výrobky ke schválení během roku 2009. Skutečné produkty s certifikátem od TÜV lze tudíž očekávat na trhu během roku 2010 a realizaci větších projektů pravděpodobně v roce 2011. Koneční uživatelé si poté budou moci vybírat z množiny zařízení vyhovujících požadavkům normy IEC 61511 (funkční bezpečnost: bezpečnostní přístrojové systémy pro spojité technologické procesy) od mnoha dodavatelů namísto dosavadní omezené nabídky zařízení zkonstruovaných speciálně k použití s jedním jediným proprietárním systémem.

2.2 Foundation Fieldbus jako „černý kanál"

Dvě základní koncepce používané při vypracovávání návrhu komunikačních sítí v bezpečnostních systémech jsou koncepce tzv. *nespolehlivého média* (*black channel*) a její opak, koncepce tzv. *spolehlivého média* (*white channel*). Podle koncepce *white channel* je celý komunikační systém, zdola až nahoru, projektován s ohledem na požadavky bezpečnostních úloh. Veškerá jeho specializovaná zařízení včetně rozváděčů, přepínačů atd. musí být certifikována, což znamená náklady navíc. Koncepce *black channel* (podle známého *black box*) naopak využívá běžné přenosové systémy a běžný síťový hardware. Bezpečnostní vrstva, která v tomto konceptu zpracovává všechny úlohy a požadavky týkající se bezpečnosti, je integrální součástí komunikační struktury. Podle normy IEC 62280-1 se nachází mezi zásobníkem komunikačního protokolu a aplikační vrstvou. Protože ochranná vrstva je zde součástí sítě, uživatel může k bezpečnostní síti koncipované jako *black channel* připojit i zařízení bez bezpečnostního certifikátu. Všechna zařízení mohou sdílet jednu společnou síť, což znamená výrazně menší náklady.

V systému FF-SIF je síť typu *black channel* spojující přístroje systému SIS s jeho logickou vyhodnocovací jednotkou realizována při použití základního komunikačního protokolu FF H1. Ten nebyl pro použití v bezpečnostním systému nijak měněn; pouze byly přidány doplňková diagnostika zařízení a schopnost detekovat chybu při přenosu, což je realizováno ve vyšší vrstvě komunikačního protokolu. Vedle rozšířené diagnostiky zařízení je tedy základní předností systému FF-SIF ve funkci *black channel* možnost využít diagnostiku na úrovni bezpečnostní sítě. Tradiční analogové bezpečnostní sítě možnost detekovat šum, degradaci anebo poruchy v síti nenabízejí.

3. Registrace a certifikace v systému FF-SIF

Stejně důležitá jako certifikace výrobků pro systém FF-SIF zajišťovaná TÜV je jejich registrace u organizace Fieldbus Foundation. Koncepce a vlastní způsob certifikace zařízení pro sběrnici FF z hlediska jejich použitelnosti v přístrojových bezpečnostních systémech jsou schváleny TÜV, s výrobou zařízení i jejich předáváním do TÜV k certifikaci musí ovšem začít sami výrobci.

Tab. 2. Hlavní rozdíly mezi normami IEC 61508 a IEC 61511

IEC 61508	IEC 61511
základní norma v oblasti funkční bezpečnosti určená ke všeobecnému použití	odvětvová norma pro oblast funkční bezpečnosti spojitých technologických procesů
týká se všech přístrojů a systémů souvisejících s bezpečností a externích zařízení určených ke zmenšení rizika	týká se pouze bezpečnostních přístrojových systémů
určena především pro výrobce bezpečnostních systémů a zařízení	určena především pro projektanty, integrátory a uživatele bezpečnostních přístrojových systémů

Podobně však, jako musí být výrobky určené pro systém FF schváleny organizací Fieldbus Foundation z hlediska interoperability, je u výrobků uvažovaných k použití v bezpečnostních přístrojových systémech povinná jejich registrace. Jde o proces zcela oddělený od procesu certifikace v TÜV. Probíhá tak, že po schválení v TÜV lze přístroje a hostitelské systémy uvažované pro systém FF-SIF registrovat u organizace Fieldbus Foundation, která spravuje specifikace systému FF-SIF odděleně od standardních specifikací sběrnice FF. Oddělené je také změnové řízení. Příslušné soubory jsou udržovány v různých nezávislých datových úložištích. Požadavek na jakoukoliv technickou změnu je analyzován a popř. validován příslušným orgánem organizace, kterým je *Safety Review Committee*, a teprve poté zařazen k vydání v příští verzi dokumentů.

Pro zařízení určená pro přístrojové bezpečnostní systémy zavedla organizace Fieldbus Foundation rozšířený registrační proces. S ohledem na nové požadavky na zkoušky, které vyvstaly z důvodu přidání bezpečnostních funkcí, organizace postupně vyvíjí novou sadu zkušebních a registračních nástrojů dostupnou na uživatelské úrovni. Rozhodnou-li se dodavatelé podrobit svá zařízení validaci v oblasti funkční bezpečnosti, budou moci provést jejich zkoušky a pořídit z nich příslušné protokoly podle požadavků organizace Fieldbus Foundation, která poté zařízení přidělí registrační značku.

Zkoušky předcházející přidělení registrační značky jsou u zařízení určených pro přístrojové bezpečnostní systémy přinejmenším stejně přísné jako zkoušky, kterými procházejí standardní zařízení určená pro provozní sběrnici FF H1. Ověřuje se chování všech vrstev v zařízení včetně elektronických obvodů (fyzická vrstva) i zásobníku komunikačního protokolu i použitelnost zařízení (vrstva funkčních bloků). U elektroniky se ověřuje např. schopnost činnosti včetně signalizace při minimálním provozním napětí. Při posuzování způsobilosti zásobníku protokolu, prováděném výhradně Fraunhoferovým ústavem pro zpracování informací a dat (*Institut für Informations- und Datenverarbeitung* – IITB), se ověřuje, zda zařízení dokáže správně sestavovat i interpretovat zprávy předávané po sběrnici. Závěrečná zkouška, vykonávaná s použitím sady *Interoperability Test Kit (ITK) for SIF*, potvrdí způsobilost a interoperabilitu zařízení při vlastním použití, včetně činnosti funkčních bloků. Je důležité zdůraznit, že registrační proces se v žádném směru netýká funkční bezpečnosti. Bezpečnostní aspekty zařízení jsou věcí jeho výrobce a příslušné třetí strany, kterou je servisní organizace typu např. TÜV.

4. Systém FF-SIF odpovídá mezinárodním normám pro oblast funkční bezpečnosti

Systém FF vždy odpovídal mezinárodním normám a systém FF-SIF v této tradici bez výjimky pokračuje. Odpovídá požadavkům normy IEC 61508 pro funkčně bezpečné systémy až do SIL 3 včetně a umožňuje uživatelům budovat bezpečnostní systémy podle normy IEC 61511, platné pro oblast funkční bezpečnosti spojitých technologických procesů v průmyslu (*tab. 2*).

Za dobu existence norem IEC 61508 a IEC 61511 výrazně vzrostl zájem uživatelů o důkladné analýzy v oblasti funkční bezpečnosti a o používání certifikovaných bezpečnostních přístrojových systémů. Tyto bezpečnostní normy poskytují návod, jak

v dané oblasti správně postupovat, a obsahují určitá doporučení, avšak v žádném případě ze svých uživatelů nesnímají odpovědnost za bezpečný chod jejich zařízení. Stanovují, že bezpečnost nelze dokládat zpětně, ale že musí být prokázána předem. Normy se tudíž zaměřují nejen na analýzu nebezpečí a rizik a stanovování požadavků na bezpečnostní systémy, ale především na celý životní cyklus bezpečnosti, zahrnující validaci instalovaných systémů a jejich provoz, údržbu a nakonec likvidaci. Předmětem normy je tedy péče o bezpečnost po celou dobu provozního života systému.

Normy sice vyžadují důkaz o odborné způsobilosti posuzujících osob, aniž by však trvaly na jejich formálním oprávnění nebo pověření. Uživatelé bezpečnostních přístrojových systémů však stále častěji požadují, aby certifikace vykonávali kompetentní a pro tuto činnost certifikovaní jednotlivci nebo organizace. V současnosti existuje mnoho národních i nadnárodních organizací zabývajících se vzděláváním, prověřováním kompetencí a certifikováním jednotlivců i firem provádějících audity v oboru funkční bezpečnosti. Z nich jmenujme např. organizace The 61508 Association a ISA.

(pokračování)

Larry O'Brien, analytik,
Dick Hill, editor,
ARC Advisory Group

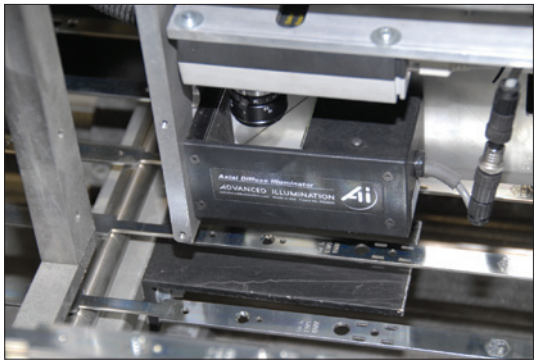
Optimalizace výroby použitím kamerového systému

Otevírání a vyklápění balkonových dveří či oken patří ke každodenním úkonům člověka, a málokoho zajímá, jak jsou systémy potřebné k vykonávání těchto úkonů technicky řešeny. Otočné i vyklápěcí závěsy pro okna i dveře vyrábí rakouská firma Mayer&Co, která je jedním ze tří největších dodavatelů těchto součástí. Nedávno se technikům této firmy podařilo vyřešit problém s obtížným místem ve výrobní lince použitím kamer firmy Cognex a technické podpory firmy Buxbaum Automation. Výsledkem je kvalitní výroba téměř bez zmetků. Vzhledem k úspěšnému využití kamer typu Cognex DVT 510 uvažují odborníci firmy Mayer&Co o tom, že kamery Cognex instalují i v jiných místech výrobních linek.

Důraz na kvalitu výroby

Firma Mayer&Co klade na kontrolu výrobního procesu velký důraz také vzhledem k tomu, že je první společností v průmyslu, která má certifikát podle normy DIN ISO 9001, vydaný společností AGQS.

Dveřní a okenní závěsy vyráběné v provozech této firmy v Salzburgu a Triebenu jsou distribuovány prostřednictvím rozsáhlé sítě dodavatelů po celém světě. Dominantním trhem je Evropa. V obou výrobních provozech se používá moderní strojní i nástrojové vybavení. Speciální stroje, např. pro montáž výrobků, navrhují i vyrábějí pracovníci firmy. Úspěch společnosti Mayer&Co byl vždy založen na kvalitě jejích produktů. Aby splnila očekávání zákazníků, zavedla přísné sledování výroby a kontrolu kvality produktů během celého výrobního cyklu od vývoje po dodávku.

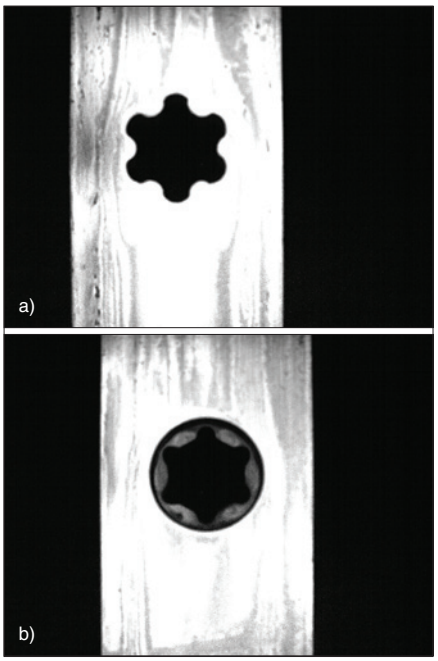


Obr. 1. Součástka (na obrázku dole) musí postupovat ke zpracování správnou stranou vzhůru – její poloha je kontrolována kamerou Cognex DVT 510 s difuzním osvětlovačem

Správný systém strojového vidění

Při výrobě součásti zachycené na *obr. 1* bylo třeba zajistit, aby byl polotovar uložen správnou stranou vzhůru. Instalovaná kamera Cognex DVT 510 detekuje, zda je součást uložena správně, a pokud ne, okamžitě pošle chybové hlášení řídicí jednotce stroje. Zvláštní mechanismus pak pootočí součástku do správné polohy a ta může postoupit k dalšímu zpracování. Kamera rozpozná správnou polohu podle zahloubení otvoru s ozubením (*obr. 2*).

Se všemi dříve zkoušenými systémy strojového vidění bylo řešení této úlohy složité a zdlouhavé. Podle vyjádření odborníků společnosti Mayer&Co se podařilo překonat všechny problémy při zavádění kontroly kamerou právě díky pokročilým funkcím a vlastnostem kamer DVT 510, mezi něž patří port pro Ethernet, kompatibilita se standardními sběrnicovými systémy, dálkové ovládání v reálném čase, obrazový čip CMOS, 32 MB datové paměti DRAM, 8 MB paměti flash a inteligence softwaru. Software se snadno ovládá a přitom poskytuje optimální možnosti pro nastavení přístroje. Odborníci společnosti Mayer&Co došli k závěru, že v úlohách strojového vidění není to nejdůležitější cena, ale kvalita použitého vybavení a odborná pomoc.



Obr. 2. Kamera detekuje polohu součástky podle zahloubení otvoru s ozubením: a) chybná poloha, b) správná poloha

Další informace o výrobcích a službách společnosti Cognex poskytne obchodní zástupce Jan Kučera, tel.: 724 819 719, e-mail: jan.kucera@cognex.com.

(*Cognex Germany Inc.*)