

# Profisafe a Profibus přispívají k dostupnosti a bezpečnosti spojitých technologických procesů

David W. Humphrey, Paul Miller

Automatizační technika pro řízení spojitých technologických procesů v poslední době výrazně profituje z obecného technického pokroku. Měřitelné přínosy konečným uživatelům mezi jinými poskytují např. distribuovaná inteligence, síťové bezpečnostní protokoly, průmyslový Ethernet, bezdrátové sítě atd. V současnosti poutají pozornost zejména dvě témata – průmyslové komunikační sběrnice a jejich otevřené bezpečnostní protokoly. Důvodem je možnost snížit celkové náklady a zdokonalit diagnostiku v závodě. Tomuto zájmu jde vstříc mezinárodní konsorcium dodavatelů automatizační techniky Profibus International, které spojuje funkční bezpečnost a sběrniceovou techniku a nabízí systémy s „vestavěnou bezpečností“ pro síť Profibus-DP, Profibus-PA a Profinet i pro bezdrátovou techniku. Jde o systémy, při jejichž použití koneční uživatelé mohou sjednotit strukturu svých sítí, obejít se bez další, paralelní sběrnice a současně dosahovat úrovní bezpečnosti až SIL 3.

Process automation has profited tremendously from technology advances in recent years. Distributed intelligence, network safety protocols, Industrial Ethernet, and wireless networking are just a few of the enabling technologies that have brought measurable value to process manufacturing. Two topics in particular – process fieldbuses and open fieldbus safety protocols – have caught the attention of process users in recent years thanks to the potential to cut costs and improve diagnostics. In this field, Profibus International, an industrial consortium of automation suppliers, has mated safety with industrial networking to create solutions for built-in safety based on all available media, including Profibus-DP and -PA, Profinet, and wireless technology. End-users are now taking advantage of these solutions to unify their network architectures and eliminate the need for a second, parallel bus while achieving safety integrity levels up to SIL 3.

## 1. Bezpečnost a dostupnost: rub a líc téže mince

Integrované bezpečnostní systémy v provezech se spojitými technologickými procesy zajišťují dvě oddělené a rozdílné úlohy – funkční bezpečnost a dostupnost technologického zařízení. Pro provozovatele těchto procesů jsou přitom obě úlohy kritické. Dobrá zpráva je, že integrované bezpečnostní systémy podporují obě úlohy s použitím téhož hardwaru, což znamená, že bezpečnost a dostupnost jsou ve skutečnosti jen dvěma stranami téže mince. Důvody, proč je třeba uvedené úlohy řešit, a cíle úloh se přesto liší.

Cílem sledovaným při řešení úloh funkční bezpečnosti (*functional safety*) je udržet v řádném stavu bezpečnostní systémy (obvody, funkce), a zabránit tak újmě na zdraví obslužného personálu např. odpojením nebezpečných prvků od přívodu energie. Typicky používanou mírou úrovně funkční bezpečnosti je veličina označovaná jako *Safety Integrity Level* (SIL), která vyjadřuje, jaká je pravděpodobnost vzniku nebezpečné poruchy bezpečnostního obvodu během jedné hodiny jeho chodu (např.  $1 \cdot 10^{-7}/h$  pro SIL 3). Funkční bezpečnost je důležitá v těch odvětvích, kde obsluha pracuje v těsné blízkosti běžícího strojního zařízení nebo kde nežádoucí událost v technologickém procesu může mít za následek požár, výbuch či jiný nebezpečný stav.

Řešit dostupnost systému (*system availability*) naproti tomu znamená zabývat se odolností systému proti poruchám (*fault tolerance*) ve smyslu schopnosti systému zachovat si říditelnost i v případě poruch jeho komponent. Vysoká úroveň dostupnosti je důležitá v případech, kdy v důsledku zastavení technologického procesu může dojít k rozsáhlým poškozením zařízení a velkým ztrátám v důsledku přerušení výroby. Jako příklad lze uvést přímo vytápěný ohřívák nebo katalytickou krakovací jednotku v rafinerii, oboje s endotermickým procesem, který ale bez řízení, ponechán sám sobě, může přivést zařízení k výbuchu. Jindy poruchy nemusí být nebezpečné, ale mohou způsobit znehodnocení celých výrobních šarží nebo dlouhá zpoždění dodávek produktů v důsledku složitých postupů při spouštění zařízení.

Typicky lze dosáhnout větší dostupnosti zařízení při použití redundantní řídicí jednotky. Dostupnost se obvykle vyjadřuje jako podíl doby, po kterou bylo zařízení skutečně provozuschopné, k celkové době, po kterou provozuschopné mělo být. Obvykle lze za minimální přijatelnou považovat dostupnost 99,99 % nebo větší. Protokoly Profibus a Profisafe lze v takovýchto úlohách použít s redundancí i bez ní. Protokol Profisafe má navíc důležitou roli v systémech s velkou dostupností dosahovanou při použití metody známé jako *Flexible Modular Redundancy* (FMR).

## 2. Ekonomické aspekty automatizace a bezpečnosti spojitých technologických procesů

### 2.1 Rozhodují ekonomická hlediska

Nová technika může být sebevíc zajímavá, přesto se provozovatelé zařízení při rozhodování spíše než o technické argumenty opírají o důkladné posouzení jejich ekonomických přínosů. Ekonomický přínos uvažovaných technických změn lze stanovit s použitím standardních podnikatelských metrik, a to počínaje dostupností systému, jako míry doby jeho provozuschopnosti, na principu obdobném nákupu pojistky proti nepředvídaným poruchám. Dostupnosti se dosahuje tím, že se pokud možno zabrání tomu, aby se proces probíhající spojitě v čase zastavil z důvodu poruchy jednotlivých komponent řídicího systému, např. procesorových jednotek nebo provozních přístrojů.

Systémy odolné proti poruchám garantují správné provedení bezpečnostních funkcí tím, že „promíjejí“ méně významné závady typu prostého selhání techniky. Takto lze výrazně zmenšit celkové vynaložené náklady (*Total Cost of Ownership* – TCO), a tudíž přímo zvýšit produktivitu podniku. Dalšími důležitými metrikami používanými při rozhodování o nákupu technologického zařízení jsou návratnost vloženého kapitálu (*Return on Assets* – ROA) a celková účinnost zařízení (*Overall Equipment Effectiveness* – OEE). Obě mají zásadní vliv na celkový cíl, kterým je vést podnik směrem k excelentní provozní výkonnosti (*Operational Excellence* – OpX).

### 2.2 Bezpečnostní systémy a bezpečné komunikační sběrnice jdou ruku v ruce

Bezpečnost procesů v tradičním pohledu spočívá v použití přídavných monitorovacích zařízení a prostředků pro nouzové vypnutí, které chrání osazenstvo závodu, výrobní prostředky a okolní prostředí před katastrofami, malými i velkými. Jinými slovy řečeno, tradičně jsou výdaje na zajištění bezpečnosti procesů nutným zlem. Doba se však změnila a moderní realita je jiná. Současné bezpečnostní systémy jsou nedílně integrovány do systémů pro řízení spojitých technologických procesů, což pomáhá celé zařízení zjednodušit a zkrátit dobu potřebnou na jeho vyprojektování a uvedení do provozu. Moderní bezpečnostní systémy navíc využívají před-

nosti komunikačních sběrnic s jejich „vestavěnou“ bezpečností ke snížení nákladů na kabeláž a ke zdokonalení diagnostiky výrobního zařízení a péče o ně.

Průmyslové komunikační sběrnice, jako např. Profibus, zaznamenaly od svého vzniku před deseti lety ohromný úspěch a jejich přínos provozovatelům spojených technologických procesů je téměř nezměrný. Sběrnice nahradily jediným kabelem nákladnou mnohočetnou kabeláž připojující moduly I/O a provozní přístroje, přidaly možnost snadno přizpůsobovat síť a usnadnily přístup k cenným údajům o stavu zařízení jako základu moderních metod péče o ně. Se sběrnicemi s přidanými vnitřními bezpečnostními funkcemi mohou uživatelé snáze kombinovat v jedné řídicí struktuře bezpečná a standardní zařízení.

### 2.3 Zdůvodňování investic do bezpečnosti zařízení

Podle logické úvahy by investice do systémů s velkou dostupností měly být přímo úměrné riziku poruchy zařízení. Vezme-li uživatel v úvahu následky přerušení výroby po dobu dnů, týdnů, nebo dokonce měsíců či až astronomické náklady na likvidaci důsledků havárie na zdraví a životy lidí a škod na zařízení závodu a na životním prostředí, lze snadno ospravedlnit i značné výdaje na pořízení redundantních bezpečnostních systémů a redundantních provozních přístrojů. Výsledkem je, že na trhu je patrný všeobecný intenzivní zájem o redundantní bezpečnostní systémy s podpůrnými redundantními a bezpečnými komunikačními sběrnicemi.

Spolu s tím, jak dosahují větší dostupnosti zařízení a bezpečnosti pracovníků, se provozovatelé spojených technologických procesů učí, jak může strategie založená na využití inteligentních bezpečnostních zařízení přispět k dosažení finančních cílů podniku. Mezi příčinami zvýšené pozornosti v tomto směru jsou významné zejména:

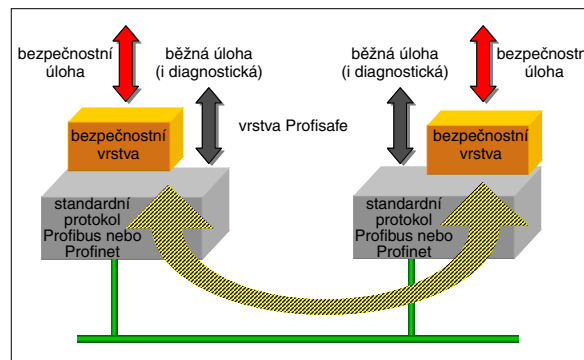
- touha provozovatelů omezit výši ručení za způsobenou škodu a zlepšit svůj obraz v očích veřejnosti,
- názor, že integrované bezpečnostní systémy umožní zvýšit dostupnost a celkovou účinnost zařízení a zlepšit návratnost kapitálu, a tím dosáhnout lepších hospodářských výsledků podniku,
- harmonizace mezinárodních bezpečnostních norem, umožňující výrobcům u uživatelům technologických zařízení vyvíjet a zavádět celosvětově použitelné bezpečnostní systémy.

### 2.4 Náklady a rizika při nedostatečné péči o bezpečnost technologického zařízení

Mnozí z provozovatelů technologických procesů v posledních několika letech zjistili, že jejich obraz v očích veřejnosti se zhoršil. Příčinou byly negativní zprávy v médiích

o katastrofických událostech, nebezpečných výrobcích a skandálech v představenstvech podniků s následnou ztrátou důvěry veřejnosti. Tato zkušenost poučila společnosti, jak důležité je aktivní propagaci jejich řešení na osvědčených provozních metodách a na dodržování těch nejpřísnějších pravidel bezpečnosti práce a ochrany životního prostředí udržovat obraz „dobrého souseda“. S růstem sociálního uvědomění ve společnosti se do popředí zájmu dostal nejen požadavek chránit lidi před zraněním nebo smrtí, ale i potřeba zajistit pracovníkům bezpečné a zdravé pracovní prostředí.

Vedle snahy zlepšit svůj veřejný obraz se provozovatelé závodů a integrátoři systémů snaží omezit svou odpovědnost za škodu pouze na ty oblasti a případy, které jsou schopni beze zbytku ovlivnit, jako je např. kvalita



Obr. 1. Protokol Profisafe souběžně s probíhajícími standardními přenosy dat po sběrnici Profibus nebo Profinet kontroluje integritu dat přenášených mezi bezpečnostními přístroji

výrobků, újma na zdraví pracovníků či poškození životního prostředí. V ostatních případech, kde předpisy mohou být nejasné nebo zatím neharmonizované, je dosud velké riziko obvinění z nedodržení shody s bytí nepovinnými praktikami, a společnosti proto alespoň demonstrují svou „dobrou vůli“ doložením shody se všemi průmyslovými postupy všeobecně uznávanými za správné. Takovéto taktiky lze uplatnit i u strategií v oblasti bezpečnosti. Zejména je používají ti výrobci technologických zařízení, kteří se na zahraničních trzích setkávají s rozdílnou bezpečnostní legislativou. Harmonizace norem sice zmenšuje pracovní zatížení, průkazní břemeno při prokazování shody s předpisy ale stále spočívá na výrobcích zařízení a na konečném uživateli.

## 3. Profibus a Profisafe představují základ funkční bezpečnosti procesů

### 3.1 Komunikační systém Profibus

Průmyslovým konsorciem odpovědným za vývoj a marketing komunikačního systému Profibus je v současnosti organizace *Profibus International* (PI), reprezentující celosvětovou komunitu více než 1 200 členských

fírem. Členské firmy konsorcia PI od vzniku standardu systému Profibus na začátku 90. let minulého století tento systém systematicky vyvíjejí a rozšiřují jeho možnosti podle konkrétních potřeb nejrůznějších uživatelů automatizační techniky, od automobilek až po např. rafinerie ropy. K realizaci dvouvoďových sítí pro sběr dat a řízení se používají sběrnice Profibus-DP (IEC 61158), typické při automatizaci nespojitě výroby, a Profibus-PA, nabízející jiskrovou bezpečnost často požadovanou v oblasti řízení spojených technologických procesů.

Sběrnice Profibus-PA využívá techniku MBP (*Manchester-encoded, buspowered*; IEC 61158-2) se současným přenosem dat i napájení jediným společným párem vodičů. V jiskrově bezpečném provedení MBP-IS (*Intrinsically Safe*) je tato technika, díky ochraně proti zkratu a omezení přenášeného výkonu, použitelná ke komunikaci s inteligentními provozními přístroji také v prostředích s nebezpečím výbuchu s klasifikací zóna 0, 1 a 2 (popř. ekvivalentních podle klasifikace používané v Severní Americe).

Vedle fyzické vrstvy komunikační sběrnice bylo pracovními skupinami organizace PI vyvinuto mnoho aplikačních profilů určených k řešení specifických potřeb uživatelů v rozličných oblastech od např. řízení polohy a pohybu, přes vážení až po přenos údaje o čase vzniku události. Pro bezpečnostní úlohy vyvinula organizace PI protokol Profisafe, umožňující přenášet po sběrnici Profibus a Profinet i údaje spjaté s funkční bezpečností (tab. 1). V protokolu Profisafe jsou proto vestavěny nástroje k detekci poruch při přenosu, které standardní sběrnice nemají (tab. 2).

### 3.2 Bezpečný kabel: Profisafe umožňuje použít společnou sběrnici

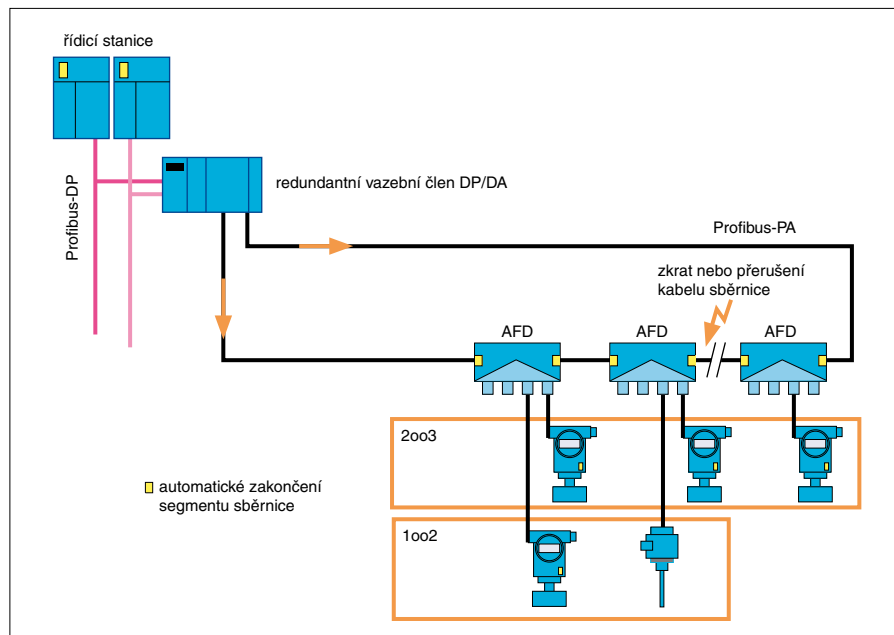
Současný koncepční přístup k automatizaci uznává, s ohledem na pokrok dosažený v poslední době v oblasti bezpečnostní techniky, že již není nutné používat dvě oddělené komunikační sběrnice, jednu pro bezpečnostní a druhou pro standardní provozní data. To má značný význam z hlediska nákladů, neboť uspořádání se dvěma sběrnicemi znamená dvojnásobný objem hardwaru i školení personálu a zbytečné komplikace při spouštění zařízení a odstraňování závad.

S příchodem bezpečnostního protokolu Profisafe jako součásti komunikačních protokolů sítí Profibus i Profinet se koncoví uživatelé mohou obejít bez zvláštní bezpečnostní sběrnice. Mohou tudíž zredukovat strukturu svých automatizačních sítí na jedinou sběrni-

ci. Protokol Profisafe rozšiřuje standardní komunikační protokol sběrnice Profibus o funkce umožňující mu plnit přísné požadavky bezpečnostních norem kladené na spolehlivost přenosu údajů s funkcí bezpečností. Přidané funkce, mezi nimiž jsou např. číslování zpráv a kontrola konzistence dat, umožňují bezpečnostním přístrojům připojeným k síti dosáhnout celkové spolehlivosti na úrovni až SIL 3 (*Safety Integrity Level*) podle mezinárodních norem (obr. 1). Protože protokol Profisafe je vestavěn do komunikačního protokolu jako takového, může být využit přístroji připojenými jak ke kterékoliv variantě fyzické vrstvy sběrnice Profibus, tj. Profibus-DP i Profibus-PA, tak i ke sběrnici Profinet. Tato metoda jediné společné sběrnice je výhodná zejména v potravinářství, při výrobě nápojů a ve farmaceutickém průmyslu jako odvětvích, kde má velký význam bezpečnost strojů.

### 3.3 Profibus-PA přináší bezpečnostní sběrnici do odvětví se spojitou výrobou

V mnoha klasických výrobních provozech se spojitými technologickými procesy ve skutečnosti existuje značný počet úloh typicky spojovaných s automatizací diskrétních výrobních procesů (továren), tj. oblastí, nichž se, pokud jde o nabídku konzorcía PI, uplatňuje sběrnice Profibus-DP. Jako příklad lze uvést chemické závody nebo čistírny odpadních vod, kde se spolu s technikou pro řízení spojitých procesů používají také řízené pohony či moduly diskrétních I/O. Čím větší je podíl dis-



Obr. 2. Redundantní sběrnice Profibus-PA s kruhovou topologií s aktivními rozváděči AFD a automatickým zakončováním sběrnice garantuje velkou dostupnost

krétních úloh, tím častěji je odvětví namísto jako „čistě spojitě“ označováno za „hybridní“.

Sběrnice Profibus-PA umožňuje vytvářet síť s provozními přístroji v případech, kdy je požadována jiná fyzická vrstva sítě, než s jakou pracuje varianta Profibus-DP, např. při řízení v prostředí s nebezpečím výbuchu. Protože sběrnice Profibus-PA využívá stejný komunikační protokol jako sběrnice Profibus-DP, zařízení v obou sítích spolu mohou sdílet

bezpečnostní data prostřednictvím protokolu Profisafe, aniž je nutné instalovat jakékoliv mosty nebo brány mezi sběrnicemi.

### 3.4 Kruhová sběrnice Profibus-PA garantuje velkou dostupnost

V případech, kdy je vyžadována velká dostupnost zařízení, lze použít sběrnici Profibus-PA s kruhovou topologií, která díky vrozené redundanci zajistí spojení i v případě zkratu nebo přerušení sběrnice kabelu.

V kruhové struktuře sběrnice Profibus-PA jsou použity čtyřkanálové aktivní provozní rozváděče (*Active Field Distributor – AFD*), k nimž se jednotlivými odbočkami odolnými proti zkratu připojují vlastní provozní přístroje. Součástí této kruhové struktury je funkce automatického zakončování kabelu sběrnice, která při poruše okružního kabelu připojí samočinně na konec zbývajících segmentů sběrnice zakončovací člen, takže veškerá komunikace po sběrnici může pokračovat bez ohledu na poruchu (obr. 2).

Kruhová sběrnice Profibus-PA se připojuje redundantně, a to ke dvěma vazebním členům DP/PA, které mohou být připojeny k jednoduché nebo redundantní sběrnici Profibus-DP. Do kruhu může být zapojeno až osm rozváděčů AFD obsluhujících celkem až 31 provozních přístrojů s rozhraním Profibus-PA. Rozváděče AFD lze vyměňovat za provozu sběrnice.

### 3.5 Inteligentní průmyslové sběrnice umožňují používat inteligentní diagnostiku

Přínosem inteligentní diagnostiky provozních přístrojů mohou být nejen menší provozní náklady. Jestliže se metodami prediktivní údržby podaří vyloučit náhlé poruchy zaří-

Tab. 1. Sběrnice Profibus s protokolem Profisafe podporuje vysokou úroveň funkční bezpečnosti a dostupnosti technologického zařízení v různých provozních podmínkách

Nástroj	Profisafe	redundance	Profisafe a redundance
<b>Oblast použití</b>	automatizace nespojitě i spojitě výroby: lisy, roboty, hladinové spínače, bezpečnostní ventily, řízení hořáků, kabinové lanovky	automatizace spojitě výroby: chemická a farmaceutická výroba, rafinerie, mořské těžební plošiny	
<b>Vysoká úroveň dostupnosti</b>	–	žádné prostoje (odolnost proti poruše)	
<b>Funkční bezpečnost</b>	žádné nebezpečné poruchy (požadavek legislativy nebo pojišťovny)	samotná redundance není zárukou funkční bezpečnosti	žádné nebezpečné poruchy (požadavek legislativy nebo pojišťovny)

Tab. 2. Protokol Profisafe obsahuje doplňkové nástroje pro detekci chyb při přenosu dat, které standardní protokoly nemají

Opravný prostředek (o)/ příčina závady (p)	Typ závady (projev)			
	nesprávné pořadí	pozdní přijetí	chyba v označení vysílače/přijímače	nekonzistentní data
opakování	o	x		
odstranění	o	x	x	
vsunutí	o	x	x	
obnovení pořadí	o	x		
zkomolení dat	p			x
zpoždění	p		x	
maskování dat	p		x	x
porucha funkce FIFO ve směrovači	p		x	

zení, může současně vzrůst dostupnost celého závodu. Dosáhnout uvedených účinků lze ovšem jen při splnění dvou podmínek, a to existence:

- spolehlivého způsobu získávání a uchování informací,
- nástroje umožňujícího získané informace vyhodnotit a podle výsledku hodnocení jednat.

Společnost Siemens nabízí k získávání informací z provozních zařízení produkt zvaný *Simatic Process Device Manager (PDM)*, což je univerzální, na výrobci nezávislý programový nástroj ke konfigurování, uvádění do provozu, diagnostikování a údržbě inteligentních provozních přístrojů s rozhraním Profibus používaných při řízení spojitých technologických procesů. Jde o nástroj skutečně univerzální, umožňující v jednom a tomtéž prostředí přes jedno jediné uživatelské rozhraní konfigurovat velké množství typů provozních přístrojů různých značek. Nabízené funkce dovolují parametrizovat provozní přístroje, simulovat jejich různé pracovní režimy a kontrolovat hodnověrnost naměřených údajů. Z centrální inženýrské stanice s nainstalovaným nástrojem PDM může

a bezpečnostními systémy a průmyslovými komunikačními sběrnici lze sázet a včas detekovat závady na provozních přístrojích a procesorech i na ně reagovat.

Hlavní příčinou růstu zájmu o systémy typu PAM je naléhavá potřeba zastat více práce s menším počtem pracovníků. Dostávají-li pracovníci informace ve správnou dobu a ve správném kontextu, pracují lépe, a tedy s větší produktivitou. Důležité je si uvědomovat, že podmínkou úspěchu v současném „plochem“ světě, kde výrobní zařízení i pracovníci mohou být rozptýleni po celé zeměkouli, je místně neomezená dostupnost informací po 24 hodin denně a sedm dní v týdnu. Při použití sběrnice Profibus a dalších průmyslových komunikačních sběrnic lze takový způsob práce, nanejvýš přínosný pro celý podnik, realizovat.

### 3.6 Nabídka produktů s rozhraním Profisafe

Do současné doby bylo zákazníkům dodáno již více než 630 000 produktů s rozhraním Profisafe, které nyní nabízí mnoho výrobců automatizační techniky. K dispozici jsou pro-

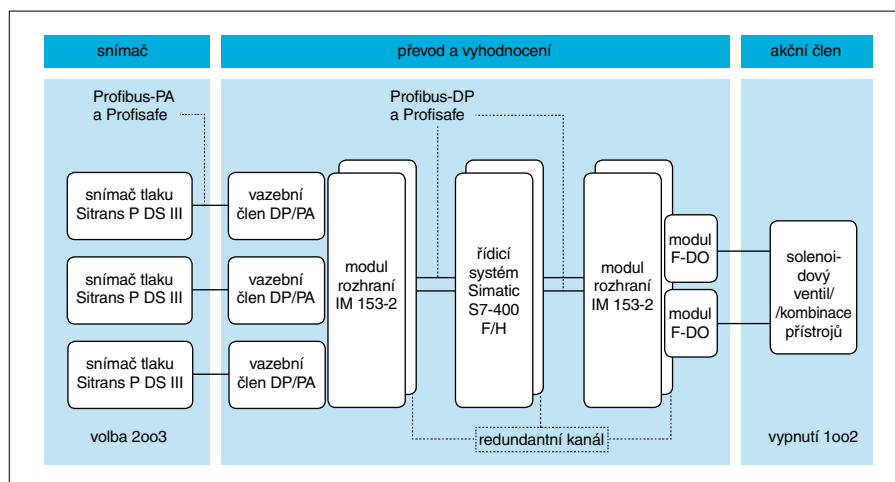
z interního oddělení inženýrů firmy Hamburg Gas Consult GmbH, a nyní má 250 zaměstnanců. Jako oficiální partner společnosti Siemens (*Siemens Solution Partner*) s certifikátem v oblasti bezpečnosti systému PCS 7 (*PCS 7 Safety Specialist*) společnost GreyLogix staví svoje dodávky standardně na distribuovaném řídicím systému Simatic PCS 7 značky Siemens.

Nedávno společnost GreyLogix modernizovala řídicí systém kompresorovny plynovodu v severním Německu. Stanice je jednou z mnoha stanic na trase plynovodu pro dopravu zemního plynu z Nizozemí do dvou distribučních sítí v Německu. K udržení potřebného dopravního tlaku po délce trasy se zemní plyn v každé stanici vždy znovu stlačuje. Požadovaný stupeň bezpečnosti těchto kompresoroven je velmi vysoký, zejména pokud jde o bezpečnostní obvody hlídající teplotu a tlak plynu. Při modernizaci stanice použila společnost GreyLogix k dosažení požadované celkové úrovně bezpečnosti (SIL) všech bezpečnostních přístrojových funkcí (*Safety Instrumented Function – SIF*) nejnovější řídicí a bezpečnostní techniku.

Rekonstruovaná kompresorovna byla původně postavena a uvedena do provozu na začátku 70. let minulého století. V 90. letech byla modernizována zavedením řídicího systému Teleperm M od společnosti Siemens. Ten však již není dodáván, takže zajistit náhradní díly bude stále obtížnější – což je u řídicího systému, který musí být vrcholně spolehlivý, skutečný problém. Zákazník se proto rozhodl převést řízení všech tří turbokompresorů turbín ve stanici na systém Siemens Simatic PCS 7.

Kompresorovna běžně pracuje sama, bez obsluhy. Lze ji však také řídit z ústředního velínu. Uspořádání řídicího systému je takové, že redundantní server poskytuje všem čtyřem klientským operátorským stanicím údaje z projektu, hodnoty technologických veličin, výstražná hlášení a zprávy. Další server nepřetržitě poskytuje údaje pro potřeby přípojeného dispečerského centra (*Dispatch Center*). Systém pro řízení spojitých technologických procesů PCS 7 sleduje všechny důležité údaje, jimiž jsou zejména hodnoty tlaků, teplot a průtoků. Do řídicího systému jsou začleněny také systém nouzového vypnutí, požární systém a systém detekce úniku plynu, takže lze jednotným způsobem zobrazit všechny aspekty řízeného procesu. Použitý princip „jediného okna“ výrazně usnadňuje obsluhu celé stanice a současně sjednocuje způsob zpracování výstražných hlášení, vkládání časových značek, záznamu sekvencí událostí i správu výrobního zařízení.

Ke komunikaci s provozními přístroji se společnost GreyLogix rozhodla použít namísto klasické techniky proudové smyčky 4 až 20 mA sběrnici Profibus s protokolem Profisafe. Se sběrnici lze vedle redukce kabeláže a větší přesnosti měření dosáhnout také přímého přístupu k informacím o stavu přístro-



Obr. 3. Společnost GreyLogix použila k dosažení požadované vysoké úrovně dostupnosti a celkové bezpečnosti kompresorovny na úrovni SIL 3 řídicí systém Simatic S7-400 F/H v redundantním uspořádání

uživatel parametrizovat inteligentní zařízení a odstraňovat jejich závady na dálku po sběrnici Profibus. Nástroj PDM funguje jako komunikační základna systému pro správu výrobních zařízení.

Ke zpracování získaných informací jsou určeny systémy pro správu výrobních zařízení (*Plant Asset Management – PAM*). Jde o kombinaci hardwaru, softwaru a služeb zaváděnou proto, aby obsluhový personál mohl, periodicky nebo trvale, tj. v reálném čase, sledovat aktuální a předvídat budoucí stav výrobního zařízení v závodě za účelem zjistit potenciální problémy dříve, než mohou ovlivnit chod výrobního procesu nebo zapříčinit náhlou poruchu zařízení. Při těsnějším provázání systémů typu PAM s řídicími

gramovatelné automaty (PLC) i distribuované řídicí systémy (DCS), standardní i jiskrově bezpečné vzdálené moduly I/O, převodníky, pohony, bezpečnostní snímače atd.

### 4. Případová studie: GreyLogix používá protokol Profisafe v kompresorovně plynovodu

Společnost GreyLogix GmbH, integrátor řídicích systémů se sídlem ve Flensburgu v Německu, se specializuje na dodávky systémů pro řízení spojitých technologických procesů pro různá odvětví průmyslu od např. elektráren, přes plynovody, potravinářství a výrobu nápojů až po chemii. Společnost vznikla v roce 2000, kdy se vydělila

jů a jejich konfiguraci. Údaje spjaté s bezpečností se přenáší po standardní sběrnici Profibus rozšířené o protokol Profisafe. Při tomto uspořádání mohou na téže sběrnici koexistovat standardní údaje i údaje spjaté s bezpečností tak, že jsou splněny požadavky na bezpečnost až do úrovně SIL 3 včetně, aniž je nutné instalovat oddělenou bezpečnostní sběrnici. K ochraně před přepětím a bleskem zvolila společnost GreyLogix za fyzickou vrstvu sběrnice Profibus světlovodný kabel.

K parametrizaci, uvádění do provozu, diagnostice a údržbě provozních přístrojů používá společnost GreyLogix program Simatic Process Device Manager, což je nástroj pro správu údajů v provozních přístrojích podporující produkty od více než 100 různých výrobců. Přístroje se v prostředí PDM konfiguruji s použitím údajů obsažených ve standardním elektronickém štítku přístroje (*Electronic Device Description* – EDD) dodávaném výrobcem přístroje. V prostředí PDM mají operátoři přístup nejen k diagnostickým údajům o poruchách, ale i k podrobným návodům k použití přístrojů, s jejichž pomocí mohou snáze identifikovat a odstraňovat příčiny poruch.

Protože funkční bezpečnost kompresorovy je skutečně mimořádně důležitá, existuje v ní dohromady ne méně než 22 různých bezpečnostních obvodů pro sledování tlaků a teplot a pro detekci požáru. K dosažení požadované celkové úrovně bezpečnosti jsou nezbytné bezpečnostní funkce navrženy tak, aby bylo jisté, že kompresorovna bude vždy bezpečná, tj. že tlak plynu po stlačení za žádných okolností nepřekročí stanovené meze.

Použitý způsob řešení lze ukázat např. na bezpečnostním obvodu sledujícím tlak plynu, jehož základem jsou snímače tlaku Sitrans P DS III. Pro stanovení hodnoty SIL byl bezpečnostní obvod rozdělen na tři části, a to snímač, převodní a rozhodovací blok a akční člen (*obr. 3*). Pro každý prvek v tomto řetězci byla stanovena mezní hodnota pravděpodobnos-

ti poruchy prvku, známá jako pravděpodobnost selhání při vyžádání funkce (*Probability of Failure on Demand* – PFD). Hodnota PFD, která je obvykle uvedena v návodu k použití přístroje nebo zařízení, značí střední pravděpodobnost, že přístroj při vyžádání tuto bezpečnostní funkci nevykoná. Protože se v dané úloze nepředpokládá, že by porucha řídicího systému stanice nastávala častěji než jednou za rok, jsou bezpečnostní přístrojové funkce bránící překročení mezního tlaku plynu navrženy jako funkce s malou četností vyžádání.

Ke stanovení hodnoty SIL bezpečnostního obvodu jako celku se hodnoty PDF všech jeho tří částí, snímače, převodního a rozhodovacího bloku a akčního členu, sečtou. Protože na kompresorových jednotkách jsou použity snímače tlaku Sitrans P DS III a použité komponenty pro zpracování signálu jsou certifikovány k použití na úrovni SIL 3 nebyl výpočet celkové hodnoty PDF příliš složitý. Snímač Sitrans P DS III má certifikaci pro SIL 2, a je-li použit redundantně v zapojení 2oo3 (tj. dva ze tří), je hodnota PDF bezpečnostní přístrojové funkce bránící překročení mezního tlaku rovna 0,000 13. Ta podle normy IEC 61508 vyhovuje požadavkům klade-ným na úrovni SIL 3. Použití sběrnice Profibus s protokolem Profisafe jako certifikované bezpečnostní sběrnice jednoznačně přispělo k dosažení požadované úrovně SIL.

## 5. Závěry

Nespornými přednostmi přenosu standardních a bezpečnostních dat po společné sběrnici s inherentní bezpečností jsou kratší doba potřebná k oživení a spuštění zařízení, menší náklady na kabeláž a dokonalejší diagnostika. V dlouhodobějším pohledu se k nim přidávají ještě efektivnější údržba a ochrana uživatelských investic. Přejít na tuto techniku bude ovšem pozvolný.

Na straně provozovatelů spojených technologických procesů je sice v posledních něko-

lika letech stále důležitějším tématem funkční bezpečnost používaných technologických zařízení i řídicí techniky. Důvodem jsou současné technická převaha a konkurenční výhody v podnikání, kterých lze tímto způsobem dosáhnout. Naproti tomu ale stojí počáteční náklady spojené s přechodem na novou techniku. Mají-li provozovatelé získat potřebný náhled, je třeba, aby znovu ohodnotili úlohu funkční bezpečnosti v rámci jejich výrobní strategie a zjistili si, jak jim nové metody mohou pomoci při dosahování jejich podnikatelských cílů.

Po technické stránce Profibus a další moderní průmyslové komunikační sběrnice nyní kombinují standardní vlastnosti sběrnic daného typu s bezpečnostními protokoly, jako je Profisafe. Je na výrobcích, integrátorech a konečných uživatelských technologických zařízeních a řídicích systémech, aby zjistili, jaké možnosti jim technika jediné společné sběrnice přináší v nových projektech automatizovaných systémů, tj. jak mohou jejím použitím snížit náklady jak na vlastní instalaci, tak i celkové náklady (TCO) budoucích výrobních zařízení.

Dodavatelé bezpečnostních komponent by měli vzít v potaz podnikatelskou příležitost nabízející se při podpoře průmyslových komunikačních sítí typu Profibus a Profinet s otevřeným bezpečnostním protokolem. S tím, jak se zákazníci postupně budou seznamovat s přednostmi struktury s jedinou sběrnici, poroste i poptávka.

David W. Humphrey, analytik,  
Paul Miller, editor,  
ARC Advisory Group  
([info@arcweb.com](mailto:info@arcweb.com))

Z anglického originálu *Profisafe and Profibus for High Availability and Safety in the Process Industries*, ARC White Paper, April 2009; překlad a úprava redakce; publikováno se souhlasem ARC Advisory Group ([www.arcweb.com](http://www.arcweb.com)).

Hamburg Messe

**We deal in solutions.**

Come meet the future

Acquire information, network with contacts, find solutions – visit NORTEC 2010 in Hamburg! This practice-oriented trade fair encompasses the entire process chain of industrial production. Be there and give your business new motivation!

Order tickets now at [www.nortec-hamburg.de](http://www.nortec-hamburg.de)

**NORTEC**  
12<sup>th</sup> Trade Fair for Manufacturing Technology  
**27 – 30 January 2010**