OpenSafety – stejné bezpečí pro všechny

Bezpečnostní komunikační protokol OpenSafety je první zcela otevřený protokol pro přenos dat spjatých s funkční bezpečností vhodný pro všechny oblasti průmyslové automatizace. V článku jsou uvedeny důvody vzniku, základní vlastnosti a přednosti tohoto univerzálního protokolu.

Trend v systémech zajišťujících funkční bezpečnost

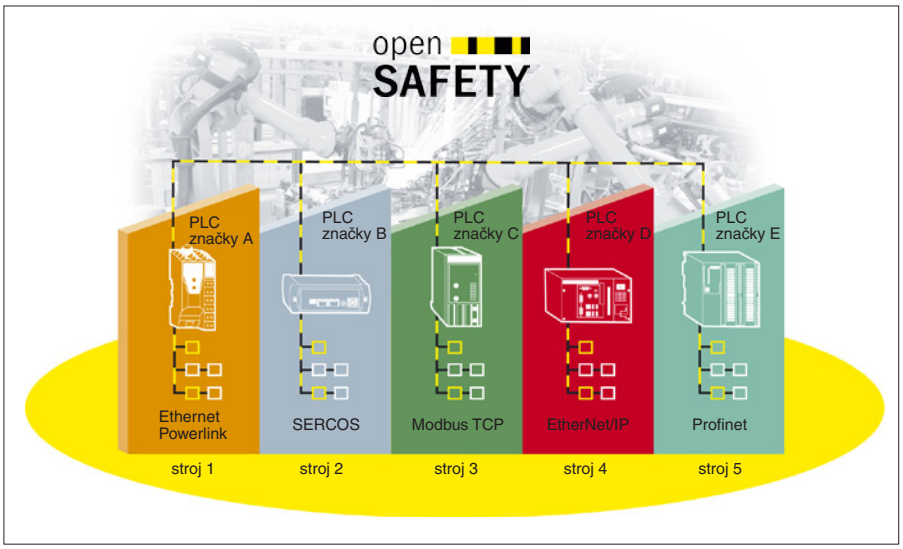
Asi před deseti lety se na trhu začaly objevovat první systémy zajišťující funkční bezpečnost strojů a strojních zařízení (bezpečnostní systémy), které pro bezpečný přenos zpráv mezi prvky systému používají komunikační sběrnice. Jejich přednosti oproti konvenčním, „zadrátovaným“ bezpečnostním systémům jsou nepřehlédnutelné a přispívají k rozvoji a upevnění pozice těchto nových systémů na trhu. K nesporným přednostem bezpečnostních systémů založených na komunikačních sběrnicích, zejména jsou-li integrovány do řídicího systému, patří:

- odstranění dosud nezbytné komplikované kabeláže a díky tomu eliminace notorického zdroje chyb a závad,
- těsná součinnost bezpečnostního systému a základního řídicího systému a sdílení údajů a informací mezi nimi,
- údaje z bezpečnostních senzorů není nutné vést paralelně do základního řídicího systému,
- snadná tvorba distribuovaných anebo modulárních systémů,
- centrální uložení hodnot parametrů prvků systému, takže odpadá riziko špatného nastavení bezpečnostních prvků při výměnách zařízení,
- zpravidla nejsou nutné žádné další nástroje pro parametrizaci bezpečnostních prvků,
- bezpečnostní systém „chytře“ reaguje na nebezpečné stavy, je programovatelný a reaguje adekvátně okolnostem, tedy ne vždy úplným vypnutím všeho,
- snadná a velmi variabilní integrace bezpečnostních funkcí do pohonů, které bývají z hlediska bezpečnosti tím nejožehavějším místem na strojích a strojních zařízeních.

Úskalí současného stavu

Většina velkých výrobců řídicí a automatizační techniky propaguje z uvedených i dalších důvodů „*safety*“ s použitím sběrnice typu průmyslového Ethernetu. Má to ale jeden háček. S jedinou výjimkou lze všechny tyto bezpečnostní systémy provozovat – a to buď z technických, nebo čistě marketingově-politických důvodů – jen společně s řídicím systémem nebo systémem I/O daného výrobce řídicí techniky. Přitom však mnoho výrobců strojů a zařízení je nuceno vybavovat své výrobky řídicími systémy podle přání svých odběratelů. Pokud jde jen o řídicí systém, znamená to programátorskou práci navíc. V případě bezpečnostních systémů však nejen to, ale i novou certifikaci celého způsobu řešení bezpečnosti stroje, čímž se náklady výrobce dostávají do úplně jiných výšin. Nemluvě o tom, že výrobci enormně narůstá různost používaných komponent a je navíc silně determinován v jejich výběru. Lze říci, že použití pevně „zadrátovaného“ systému je v tomto případě výhodnější, protože certifikace je nezávislá na použitém řídicím systému. To je vlastně ale i jediná přednost „zadrátovaných“ bezpečnostních systémů oproti integrovaným systémům sběrnicovým.

Výrobci strojů a zařízení ale profitují z integrovaných a rychlých bezpečnostních systémů i jinak. Rychle reagující systém umožňuje reagovat na nebezpečné situace později či používat větší provozní rychlosti. Zjednodušeně řečeno, rychlý systém pohyb bezpečně „ubrzdí“ z větší rychlosti za stejnou dobu jako pomalý systém z menší rychlosti. Ne proto, že by brzdil intenzivněji, ale proto, že zareaguje rychleji, vydá povel k brzdění dříve než ten pomalý, a má tak na samotné brzdění více času. Anebo při téže rychlosti si rychlý systém může dovolit zareagovat na nebezpečný stav později. První případ vede ke konstrukci zařízení s větší provozní rychlostí, a tudíž s větším výkonem (produktivitou) i při bezpečně omezené provozní rychlosti. A druhý případ vede ke konstrukci zařízení s menším obestavěným prostorem (např. světelná závora nemusí být tak daleko od nebezpečné zóny). Oba dva parametry pro finálního výrobce (OEM) znamenají konkurenční výho-



Obr. 1. Systém OpenSafety je jednotný komunikační standard pro systémy zajišťující funkční bezpečnost strojů a strojních zařízení nezávisle na výrobci řídicího systému a použité komunikační sběrnici

Hlavní přednosti protokolu Open Safety:

- celosvětový standard použitelný se všemi významnými provozními komunikačními sběrnicemi,
- nejvyšší úroveň produktivity díky přímé křižné komunikaci,
- zkrácení dob potřebných k uvedení do provozu a k údržbě bezpečnostního systému,
- automatické nastavování hodnot bezpečnostních parametrů,
- ideální metoda k realizaci bezpečnostních obvodů na modulárně koncipovaných strojích,
- jediný zcela otevřený bezpečnostní systém, technicky i právně,
- nejrychlejší komunikační systém pro úroveň SIL 3 podle normy IEC 61508,
- naprosto bezpečná investice: postup ověřování shody je certifikován organizací TÜV.

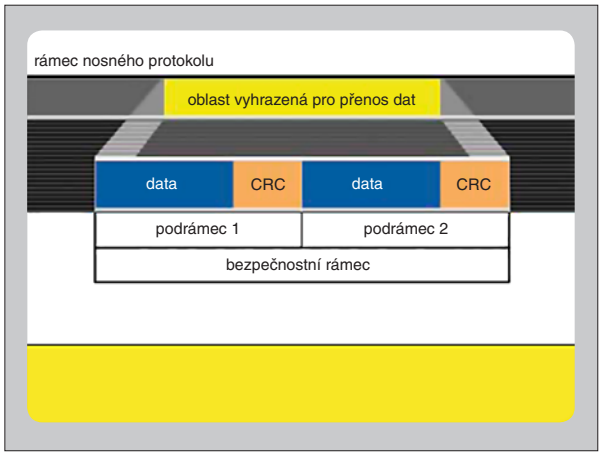
O organizaci EPSG

Nezávislá organizace *Ethernet Powerlink Standardization Group* (EPSG) byla založena v roce 2003 předními firmami z oborů automatizační techniky a techniky pohonů za účelem standardizace a dalšího vývoje komunikačního protokolu Ethernet Powerlink, který jako první zavedla společnost B&R v roce 2001. Jde o velmi výkonný komunikační systém navržený tak, aby zajistil přenosy zpráv v reálném čase s dobou odezvy řádu mikrosekund. Deterministického chováním je u něj dosaženo výhradně softwarově, a to rozšířením protokolu ethernetového standardu IEEE 802.3. Organizace EPSG spolupracuje s předními standardizačními orgány, např. se sdružením CiA (*CAN in Automation*) a s IEC. Hlavním představitelem organizace EPSG je v současné době Anton Meindl, vedoucí úseku řídicích systémů společnosti B&R.

du, zvláště při vědomí toho, že fyzikální závislosti s tím spojené jsou vesměs kvadratické – brzdná dráha roste se čtvercem času, nárazová energie roste ze čtvercem rychlosti atd.

Z jiného úhlu nazírají na situaci koncoví uživatelé. Jestliže koncový uživatel skládá výrobní linku z různých strojů a částí vybavených různými řídicími systémy (což je velmi častý případ), musí také řešit bezpečnost linky jako celku. A není-li možná výměna bezpečnostně relevantních informací mezi jednotlivými úseky linky po sběrnici, nutně to opět vede k použití pevně „zadrátovaného“ bezpečnostního systému realizovaného paralelně k řídicím systémům, které se ale mezi sebou po sběrnicích domluvit už dokážou. Výsledkem je linka, která jako celek nedokáže těžit z předností moderních systémů s integrovanou bezpečností, ačkoliv jsou v jednotlivých částech linky použity, a jde tudíž vlastně technicky o krok zpět. I koncovému uživateli pak navíc roste různost použitých komponent, které musí udržovat v provozu.

Různost bezpečnostních protokolů pro jednotlivé sběrnice současně staví do svízelné situace také výrobce bezpečnostních komponent, zejména senzorů. Jednak trh není tak velký jako u konvenčních komponent a dále náklady na vývoj a zavedení do výroby bezpečnostních prvků jsou pětkrát až desetkrát větší než u srovnatelných konvečních komponent. To brzdí vývoj bezpečnostních komponent a prodražuje systém jako celek. V minulosti byli výrobci schopni mnohdy i se stejnou hardwarovou základnou pouhými úpravami firmwaru ve svých výrobcích relativně efektivně pokrýt celý rozsah protokolů průmyslového Ethernetu, avšak v případě bezpečnostních prvků to tak snadné není, právě vlivem složitých procesů spojených s certifikací.



Obr. 2. Bezpečnostní rámec OpenSafety je přenášen v oblasti pro uživatelská data standardního rámce nosného protokolu; skládá se ze dvou identických podrámců, z nichž každý je zabezpečen vlastním kontrolním součtem

Obr. 3. Bezpečnostní protokol OpenSafety je univerzálně použitelný ve všech průmyslových odvětvích

Protokol OpenSafety

Uvedené problémy lze vhodně vyřešit při použití jednotného komunikačního standardu pro systémy zajišťující funkční bezpečnost strojů a strojních zařízení. Organizace *Ethernet Powerlink Standardization Group* (EPSG) vytvořila a nyní nabízí ke všeobecnému použití bezpečnostní protokol OpenSafety, který je základem prvního zcela otevřeného protokolu pro přenos dat spjatých s funkční bezpečností vhodného pro všechny oblasti automatizace. Protokol OpenSafety s dobami trvání komunikačních cyklů v řádu mikrosekund je certifikován organizacemi TÜV Rheinland a TÜV Süd a zaručuje nejkratší doby odezev a nejvyšší úroveň bezpečnosti. Je vhodný k použití v bezpečnostních systémech kategorie až SIL 3.

Protože protokol OpenSafety je nezávislý na typu sběrnice, lze ho použít se všemi systémy průmyslových provozních sběrnic i průmyslového Ethernetu. Aby organizace EPSG předvedla interoperabilitu bezpečnostních systémů s různými přenosovými protokoly, představila v dubnu 2010 na strojírenském veletrhu v Hannoveru čtyři různé bezpečné komunikační systémy vytvořené s použitím protokolu OpenSafety v kombinaci s protokoly SERCOS III, Modbus TCP, EtherNet/IP a Ethernet Powerlink, k nimž v listopadu téhož roku na veletrhu SPS/IPC/Drives v Norimberku přibyl ještě protokol Profinet (*obr. 1*). Uvedená pětice protokolů má 90% podíl instalací průmyslového Ethernetu a je to vůbec poprvé, kdy je úplný certifikovaný bezpečnostní komunikační systém k dispozici uživatelům nejen systému Ethernet Powerlink, ale i jiných systémů průmyslového Ethernetu. Ačkoliv ostatní organizace uživatelů již delší dobu ohlašují vývoj protokolů pro přenos bezpečnostních údajů, pouze EPSG nabízí použitelný produkt fungující nad všemi přenosovými protokoly – protokol OpenSafety.

Princip „black channel“

Základem interoperability bezpečnostního protokolu OpenSafety s libovolným přenosovým protokolem je bezezbytku uplatněný princip tzv. černého komunikačního kanálu (*black channel*). Pro činnost bezpečnostního protokolu tudíž není důležité, jaký přenosový protokol je použit k přenosu bezpečnostních rámců, protože všechny mechanismy spjaté s bezpečností (dvojité posílání telegramů, kontrolní součty atd.) se nacházejí výhradně v aplikační vrstvě protokolu, a jejich činnost tady není závislá na transportní vrstvě nacházející se vespod (*obr. 2*). Protokol OpenSafety neustále sleduje veškerý přenášený datový obsah co do jeho celistvosti, správného pořadí při přenosu a dodržení doby trvání přenosu. Protože veškeré chyby zjištěné při přenosu jsou okamžitě registrovány, lze ve funkci základního komunikačního prostředí použít bez jakýchkoliv omezení jak komunikační systémy specifické pro určitá odvětví, tak dokonce i jednokanálové přenosové sítě bez jakýchkoliv bezpečnostních prvků. Nicméně použití v sítích s menší šíří přenosového pásma, než mají sítě průmyslového Ethernetu, může vést ke snížení dosažitelné úrovně SIL. Ale i tak je použití protokolu

OpenSafety myslitelné nejen ve spojení s protokoly průmyslového Ethernetu, ale např. i v sítích využívajících jako fyzickou vrstvu RS-485 nebo CAN.

Vlastnosti protokolu OpenSafety

Protokol OpenSafety má tři význačné technické vlastnosti: v mimořádně širokých mezích proměnný formát telegramu určující způsob přenosu dat, integrované služby pro nastavování i automatickou distribuci hodnot parametrů a zejména komunikační strukturu využívající k dosažení optimální produktivity přímou křižnou komunikaci mezi stanicemi (*cross traffic*). To znamená, že bezpečnostní informace se od jednoho účastníka ke druhému dostává přímo, nehledě na to, jakou roli účastníci hrají v rámci bezpečnostního systému nebo základního běžného řídicího systému. Pro interakci bezpečnostního modulu v pohonu a světelné závory v případě jejího porušení není nutný zásah určitého nadřazeného modulu (s funkcí *master*). Z toho plynoucí krátké reakční doby jsou stěžejní pro efektivitu řešení celého systému.

Všeobecné přednosti systému OpenSafety shrnuje text v rámečku na předchozí stránce.

EPSG podporuje uživatele

Organizace EPSG aktivně podporuje použití protokolu OpenSafety v kombinaci s libovolným přenosovým protokolem a nabízí svou pomoc např. při ověřování shody a certifikaci. Protokol OpenSafety je otevřený po stránce technické i právní a lze ho zdarma stáhnout jako software s otevřeným zdrojovým kódem (*open source*). To platí pro zdrojový kód zásobníku (*stack*) jak pro podřízené (*slave*) komponenty, tak i pro řídicí (*master*) komponenty. Licence BSD spolu s možností použít protokol OpenSafety s jakýmkoliv typem komunikační sběrnice zaručují všem uživatelům této metody nejvyšší možnou bezpečnost jejich investice a umožňují dodavatelům automatizační techniky i provozovatelům výrobních závodů významně snížit náklady na vývoj (*obr. 3*).

Potenciální uživatelé protokolu Open Safety se mohou opřít o jistotu, kterou jim poskytuje skutečnost, že protokol je používán v praxi již od roku 2008 a počet zařízení, která s ním pracují, již přesáhl čtyřciferné číslo. A reakce představitelů význačných výrobců komponent z poslední doby, stejně tak jako výroky velkých koncových uživatelů a významných výrobců strojů a zařízení dávají tušit, že protokol OpenSafety je vhodným řešením problémů naznačených v úvodu a nabízí to, co je titulkem článku – bezpečí pro všechny: výrobce bezpečnostních komponent, projektanty a integrátory řídicích a bezpečnostních systémů a výrobce strojů a strojních zařízení i jejich koncové uživatele.

Karel Bílek,
Bernecker + Rainer
Industrie-Elektronik Ges. m. b. H.

Studium nového oboru SKŘ na SPŠE v Ječné v Praze

Střední průmyslová škola elektrotechnická v Praze 2, Ječná 30, zavádí od školního roku 2011/12 vzdělávací program *elektronické a informační systémy pro jadernou techniku.* Škola tím pružně reaguje na poptávku po odbornících s uceleným středoškolským vzděláním v oblasti automatizovaných systémů kontroly a řízení (SKŘ) českých elektráren, především jaderných. Potřeba středoškolských odborníků vzroste nejen s výstavbou dalších jaderných bloků, ale i v důsledku generačního problému, který toto odvětví očekává.

Zavedením studia oboru SKŘ se zaměřením na jadernou energetiku škola nejen obnovuje historickou tradici výuky v oboru jaderné techniky ze 70. let minulého století, později utlumené. Současně tím také rozšiřuje svou nabídku vzdělání v oboru automatizace, zatím reprezentovanou vzdělávacím programem *aplikace počítačů v automatizaci a robotice*. V něm především podporuje samostatnou práci studentů se zařízeními běžně používanými v průmyslu, v technice budov atd. a vychovává odborníky, kteří se bez problémů okamžitě uplatňují v praxi (*obr. 1*).

Nový obor k tomuto komornějšímu pojetí automatizace přidává problematiku velkých řídicích systémů používaných v jaderné energetice, klasické energetice i v jiných odvětvích průmyslu, a tím dále rozšiřuje možnosti celoživotního uplatnění absolventů.

Obr. 1. Studenti při práci s PLC v laboratoři systémů Tecomat od firmy Teco; obdobně se studenti seznamují také se systémy od firem Amit a Panasonic (foto: autor)

Cílem studia v novém oboru je seznámit studenty s principy a činností jaderné elektrárny a vybavit je potřebnými znalostmi funkcí a skladby SKŘ jednotlivých technologických celků primárního a sekundárního okruhu. Dále se studenti v obecné rovině seznámí také s architekturou bezpečnostních systémů SKŘ a jejich funkcemi a požadavky, které jsou na ně kladeny z hlediska jaderné bezpečnosti. Protože jde o digitálně řízené systémy, studenti se mimo jiné seznámí s průmyslovými výpočetními, komunikačními a informačními systémy. Škola po pečlivých analýzách volila strukturu a věcnou náplň jednotlivých předmětů tak, aby absolventi, kteří nebudou dál pokračovat ve vysokoškolském studiu, měli co nejširší možnosti uplatnění nejen v jaderných elektrárnách, ale zároveň i v klasických elektrárnách a teplárnách, v chemickém a petrochemickém průmyslu atd., v podstatě všude tam, kde se v průmyslu využívají automatizované řídicí systémy (*tab. 1*). Po úspěšném složení maturitní zkoušky může absolvent po absolvování kurzu a složení zkoušky získat kvalifikaci ve smyslu § 5 vyhlášky ČBÚ 50/1978 Sb. Skutečnost, že škola otevírá nový studijní obor, je velkou výzvou nejen pro firmy, které SKŘ dodávají, ale zejména pro firmy, které na těchto systémech při odstávkách technologických zařízení apod. vykonávají servisní činnosti.

Při zavádění nového vzdělávacího programu se škola samozřejmě neobejde bez podpory z „vnějšku“, ať už jde o studijní materiály, učební pomůcky, možnost odborných stáží, ale také připomínky ke struktuře a věcné náplni učebních osnov ze strany zainteresovaných firem a organizací. Další informace lze získat na www.spsejecna.cz, popř. přímo u autora.

Ing. Zdeněk Vondra, SPŠE, Praha 2, Ječná 30
(vondra@spsejecna.cz)

Tab. 1. Vyučovací předměty studijního oboru elektronické a informační systémy pro jadernou techniku na SPŠE v Praze 2, Ječná 30 (návrh na šk. r. 2011/12)

Všeobecně vzdělávací předměty	Odborné předměty
český jazyk a literatura	strojírenská technologie a zařízení
cizí jazyk (angličtina, němčina)	elektrotechnika a elektrotechnologie
dějepis, občanská nauka	digitální technika a řízení
matematika	elektronika jaderných zařízení
fyzika	silnoproudá zařízení
jaderná chemie a ekologie	jaderná a aplikovaná fyzika
informační a komunikační technologie	jaderné reaktory a zařízení
tělesná výchova	měření v jaderné technice
ekonomika	praktická cvičení