Bezpečnost a lidský faktor v automatizovaných systémech

O bezpečnosti výrobních procesů se často začne mluvit, až když se stane nehoda. Nezřídka stojí za haváriemi člověk. Je-li člověk převážně tím chybujícím článkem, proč ho úplně nevyloučit z procesu řízení? Je patrné, že oblast bezpečnosti výrobních procesů vyvolává mnoho otázek. Abychom se dověděli, jak se tyto otázky řeší v praxi, požádali jsme o stanoviska odborníky z několika firem. Díky jejich ochotě podělit se o své zkušenosti můžeme předložit čtenářům tento polemický příspěvek.

Jak se podle vašich zkušeností staví provozovatelé výrobních procesů k bezpečnosti? Považují za nutné pouze splnit příslušné normy, nebo mají skutečný zájem o bezpečnost pracovníků?

Luděk Barták (Panasonic Electric Works):

Pevně věřím ve snahu chránit zdraví a životy pracovníků v průmyslových provozech i nad rámec příslušných bezpečnostních norem. Naproti tomu je bohužel v současné době přibližně polovina provozů zabezpečena nedostatečně – záměrně, z nedbalosti či z neznalosti legislativy. Bezpečnost stojí finanční prostředky, a tak je to stále oblast, kde ke změnám dochází velmi pomalu.

Luděk Barták, manažer marketingu společnosti Panasonic Electric Works Czech

„Bezpečnost stojí finanční prostředky, a tak je to stále oblast, kde ke změnám dochází velmi pomalu.“

Antonín Zajíček (Schneider Electric CZ):

Myslím si, že provozovatelé strojního zařízení jsou všeobecně málo informováni o aktuálních normách a nařízeních. Z toho plyne, že naprostá většina pouze splní to, co musí. Existují však i světlé výjimky, tedy podniky, které se pro bezpečnost svých zaměstnanců snaží dělat maximum.

Zdeněk Švihálek (B+R automatizace):

Výrobci strojů a zařízení se snaží především za co nejnižších nákladů splnit to, co jim ukládá zákon. Když už to však musí udělat, snaží se používat bezpečnostní systémy, které jim samým nebo konečnému uživateli přinesou něco navíc. Například co nejrychlejší opětovný náběh stroje po nebezpečné události, malé rozměry stroje a vyšší produktivitu díky rychlé reakci bezpečnostního systému nebo zkrácení vývoje díky distribuci na sběrnici a modularitě. Cílem je uvést zařízení do bezpečného stavu tak, aby se nepoškodilo a bylo možné je co nejrychleji znovu rozběhnout.

Filip Pelikán (Sick):

Podle mé zkušenosti urazila Česká republika od roku 2002, odkdy se tímto oborem zabývám, velký kus cesty směrem ke zlepšení bezpečnosti. Všeobecně platí, že čím větší firma, tím větší je kladen důraz na bezpečnost. Naproti tomu se ale často jedná pouze o zabezpečení pomocí osobních ochranných pomůcek (OOP), bezpečných chodníků nebo o požární bezpečnost. I to je důležité, ale je smutné, že jsou provozy, kde všichni nosí OOP, používají bezpečné chodníky, ale samotné stroje jsou zabezpečeny nedostatečně, nebo nejsou zabezpečeny vůbec!

Petr Pekárek (Elmep):

Podle mých zkušeností se v posledních deseti letech rozmáhá používání systémů bezpečnosti procesu téměř v celém odvětví zpracovatelského průmyslu. Zpočátku to byla výsada lídrů oboru, ale postupně se téma bezpečnosti přeneslo i do menších výrobních celků. Majitelé provozů si uvědomují, že v jejich zařízení je akumulováno obrovské množství energie, jejíž nekontrolovatelné uvolnění by ohrozilo životy, majetek a životní prostředí uvnitř i vně závodu. Nicméně mnohdy je odradí, jak finančně náročné je zavedení systému řízení rizik a bezpečnosti. Ale jen do té doby, než se stane havárie. Bezpečnostní systémy sice znamenají pro provozovatele nikdy nekončící výdaje na jejich provoz a údržbu, ale také v dlouhodobém výhledu významně přispívají k účinnému snížení rizik a efektivnímu vynakládání finančních prostředků do nejproblematičtějších částí výroby.

Jsou normy pro bezpečnost strojů a strojních zařízení, funkční bezpečnost a prevenci závažných havárií ve vašem oboru vyhovující? Odpovídají současnému stavu techniky?

Filip Pelikán (Sick):

Normy vždy pokulhávají za technickým vývojem, protože jejich vytvoření trvá řádově i roky. Velkým problémem dnešní legislativy, která se týká bezpečnosti, je existence tří norem, které řeší stejný problém – úroveň bezpečnosti řídicího systému stroje. Mám na mysli EN 954-1, ČSN EN ISO 13849-1/2 a ČSN EN 62061. Dalším velkým problémem je nařízení vlády č. 378/2003, Sb., které má zásadní nedostatky a chybí v něm důležité části originální směrnice EU.

Antonín Zajíček (Schneider Electric CZ):

Nehledejme problém v normách, ty nikdy nepostihnou 100 % možných rizik. Téměř vždy je příčinou nehod člověk. A proto je důležité vzdělávání. Uvědomí-li si každý rizika spojená se svou prací a upozorní na ně zaměstnavatele, jistě se najdou i cesty k odstranění těchto rizik. Kde ale není vůle, ani ta nejkvalitnější norma nepomůže. Na dodržování všech platných pravidel a norem by měly zaměstnavatele důsledně upozorňovat příslušné kontrolní orgány.

Antonín Zajíček, produktový manažer: ovládání, detekce a bezpečnost, Schneider Electric CZ, s. r. o.

„Pouhá instalace sebekvalitnějšího bezpečnostního prvku může totiž ztroskotat na typicky českém přístupu ‚vždycky se to dá nějak obejít‘.“

Při zavádění automatizace bývá jedním z hlavních cílů vyloučit nespolehlivého člověka. Je vždy výhodné vyhnout se zásahům lidského operátora? Kdy je naopak lepší zachovat lidskou obsluhu?

Petr Pekárek (Elmep):

Ve výrobních provozech se spolehlivost zásahu operátora snižuje s dobou potřebnou k jeho správné reakci. Proto má aplikace automatizovaných bezpečnostních funkcí smysl pouze tam, kde operátor potřebuje na zjištění problému, správné rozhodnutí a nápravné akce delší dobu než čas, který uplyne od vychýlení procesu z mezních hodnot do vzniku havarijní události.

Zdeněk Švihálek (B+R automatizace):

Zde bych rozlišil procesní a strojní automatizaci. V rozsáhlých provozech procesní výroby hrají operátoři procesu ve velínu významnou roli. Automatický provoz významně sníží rizika i požadavky na operátory během nebezpečné události, ale operátor by vždy měl mít možnost do procesu nějak zasáhnout. Ve strojní automatizaci a především tam, kde se používají pohony (elektromotory, hydraulika), většinou nelze po nebezpečné událos-

ti jakýkoliv zásah operátora vůbec připustit. Takt strojů je velmi rychlý a i reakce na nebezpečnou událost vyžaduje rychlost, která je mimo možnosti člověka.

Filip Pelikán (Sick):
Člověk je tvor chybující, ale zároveň myslící. Proto záleží na druhu provozu, zda je zásah operátora nutný, ať už pro obsluhu stroje nebo jeho kontrolu. Dobře zkonstruovaný automatický stroj oprostí člověka od těžké, ne-

Filip Pelikán, divize bezpečnostních systémů, Sick spol. s r. o.
„Problémem dnešní bezpečnostní legislativy je existence tří norem, EN 954-1, ČSN EN ISO 13849-1/2 a ČSN EN 62061, které řeší stejný problém – úroveň bezpečnosti řídicího systému stroje. Dalším velkým problémem je nařízení vlády č. 378/2003 Sb., které má zásadní nedostatky a chybí v něm důležité části originální směrnice EU.“

ergonomické, monotónní práce. Stroj může být kompletně zakrytý, a tím i velice bezpečný. Lidskou obsluhu si v budoucnu dovedu představit jenom tam, kde je nutné při práci myslet, použít fantazii, zkušenosti, což stroje dosud neumějí. Jednoduché monotónní zakládaní polotovarů do stroje a jejich vyjímání vedou pouze ke ztrátě pozornosti, a tím je i riziko úrazu mnohonásobně vyšší.

Antonín Zajíček (Schneider Electric CZ):
Člověk je nepochybně příčinou mnoha poruch a havárií, nicméně stoprocentně ho z žádného procesu vyloučit nemůžeme. Za prvé dodnes neexistuje žádný inteligentnější systém, který by mohl člověka ve výrobních procesech nahradit, a za druhé zase jenom člověk může různým druhům poruchy díky své inteligenci zabránit. Ano, maximalizujme bezpečnostní prvky, minimalizujme potřebu člověka v procesu, ale zachovejme jistou míru jeho supervize. A tady jsme opět u vzdělávání a upozorňování na možná potenciální rizika.

Má v případě havárie řídit proces operátor, nebo řídicí systém?

Petr Pekárek (Elmep):
V případě havárie je podle mého názoru lepší nechat automatický bezpečností systém odstavit provoz, než se spoléhat na člověka, který si ve stresových a nestandardních situacích může počínat neefektivně, má-li řešit více závažných problémů vyskytujících se najednou.

Setkáváte se s tím, že se přeceňují technické prostředky pro zajištění bezpečnosti výroby a nedoceňuje se lidský faktor a organizační opatření?

Antonín Zajíček (Schneider Electric CZ):
S přeceňováním technických prostředků jsem se setkal nesčetněkrát. Pouhá instalace sebekvalitnějšího bezpečnostního prvku může totiž ztroskotat na typicky českém přístupu „vždycky se to dá nějak obejít“. Zaráží mě proto stálé podceňování organizačních opatření. Ta mohou zabránit mnoha chybám vedoucím k poruchám a haváriím. Příčinu často vidím v managementu, který je řízen ekonomickými ukazateli a snahou zlevnit a zrychlit výrobu. Neuvědomuje si, že malou investicí do organizačních opatření může zabránit škodám značného rozsahu.

Zdeněk Švihálek (B+R automatizace):
Já také pokládám organizační opatření za velmi efektivní. Riziko nelze nikdy úplně vyloučit a i jeho snížení na přijatelnou míru pomocí technických prostředků (i těch elektronických) může být velmi drahé. Naproti tomu organizační opatření bývají často velmi levná. Je jistě levnější nařídit nošení přílby než veškeré části konstrukce, kde by mohlo dojít k úrazu hlavy, opatřovat výstražnými světly.

Filip Pelikán (Sick):
Já se setkávám s jiným přístupem. Bezpečnost se zajišťuje tak, že obsluha podepíše, že „někam“ nebude vstupovat, sahat atd. Častým a primárním požadavkem provozovatelů strojů totiž bývá produktivita, takže výrobci vědomě nedodržují základní požadavky nařízení vlády č. 176/2008 Sb. a při konstrukci stroje na bezpečnost vůbec nehledí.

Petr Pekárek (Elmep):
V dynamických procesech je ale pro zajištění bezpečnosti často nutný automatizační systém. Na organizační opatření se lze spolehnout pouze tehdy, je-li jejich realizace pravidelně prověřována a nacvičována. Jsou nedílnou součástí politiky řízení rizik a v případě selhání všech bezpečnostních mechanismů i poslední možností, jak zmírnit následky havarijní události.

Lidská obsluha je spíše přeceňována než podceňována. Podle mých zkušeností jsou možnosti člověka při zajištění bezpečnosti výroby omezené a lidský operátor je daleko méně spolehlivý než automatický bezpečnostní systém, který je správně navržen, provozován a udržován v souladu s příslušnými normami (pro výrobce ČSN EN 61508, pro provozovatele průmyslových procesů ČSN EN 61511).

Luděk Barták (Panasonic Electric Works):
Člověk bude vždy patřit k nejslabším článkům výrobních procesů. Jakékoliv rozhodování, které lze svěřit do „rukou“ bezpečnostních řídicích systémů, povede k zefektivnění výroby.

Jak se bezpečnostní systémy vyrovnávají s rostoucí složitostí strojů, strojních zařízení a řízených technologických procesů?

Luděk Barták (Panasonic Electric Works):
Možná právě rostoucí složitost strojů a strojních zařízení a řízených procesů stojí za přísnějšími bezpečnostními normami. Výrobní linky většinou nelze jen vypnout, znovu zapnout a vyrábět dál. Okamžité vypnutí celé výroby může vést ke škodám na polotovarech či strojích a opětovné spuštění a náběh výroby zaberou čas a vyžadují také většinou zásah pracovníků údržby. To vše finančně zatíží výrobu. Bezpečnostní systémy jsou schopny zaregistrovat různé úrovně nebezpečí na konkrétních místech. Podle předem určených pravidel tedy stačí zpomalovat či vypínat jen dílčí úseky výroby. Po odstranění problému bezpečnostní automatizační systém daný úsek opět rozjíždí a synchronizuje s celou výrobou. Vše proběhne s přesností, kterou by lidský operátor naprosto nemohl zajistit.

Filip Pelikán (Sick):
Před několika lety bylo nemyslitelné, aby bezpečnost byla řízena elektronickými nebo bezdrátovými prvky, např. EN 954-1 to ani neumí postihnout. Dnes je běžné, že stroj je řízen bezpečnostním PLC a veškeré komponenty jsou zapojeny do bezpečnostní sítě. Takto lze bezpečně řídit i složité a obsáhlé strojní zařízení.

Zdeněk Švihálek (B+R automatizace):
Souhlasím, vždyť na trhu jsou již běžně dostupné elektronické programovatelné

Zdeněk Švihálek, vedoucí vývoje aplikací, B+R automatizace, spol. s r. o.
„Nástup moderních programovatelných a distribuovaných bezpečnostních systémů byl odstartován zavedením nových norem a rozšířením průmyslového Ethernetu v automatizaci.“

bezpečnostní systémy, které lze distribuovat po průmyslových sběrnicích a integrovat do klasického řídicího systému. Tyto systémy inteligentně reagují na nebezpečnou událost během několika málo milisekund. Lze do nich integrovat i bezpečnostní pohony a realizovat tak i složité funkce jako bezpečné zastavení, bezpečnou rychlost, bezpečný směr otáčení apod. Ve srovnání s pevně zapojenými bezpečnostními systémy s bezpečnostními relé jsou tyto moderní systémy mnohem přizpůsobivější (umožňují například i zabezpečení modulárních strojů), a dokonce i rychlejší. Legislativně byl nástup moderních programovatelných a distribuovaných bezpečnostních systémů odstartován právě zavedením nových norem, technicky rozšířením průmyslového Ethernetu v automatizaci.

Antonín Zajíček (Schneider Electric CZ):
I já si myslím, že odpovědí na rostoucí složitost řízených provozů jsou bezpečnostní PLC určené do bezpečnostních částí řídicích systémů. Řídí tak nejenom jednotlivé bezpečnostní komponenty, ale i celé technologické procesy. Rostoucí složitost strojů a procesů rozhodně nesmí být důvodem ke snížení jejich bezpečnosti.

Petr Pekárek (Elmep):
Programovatelné bezpečnostní systémy skutečně nemají z hlediska složitosti řízeného provozu žádná omezení. Složitost technologických procesů dělá spíše problém lidem, kteří samotný bezpečnostní systém projektují. Je důležité uplatňovat zásady procesní bezpečnosti od samého začátku, již při návrhu výrobního celku. Pro jednotlivé identifikované nebezpečné situace je třeba stanovit nezávislé ochranné vrstvy (mechanické – např. pojistné ventily; automatizované – např. přístrojové vybavení, organizační opatření). Pro automatizovaný systém následně specifikovat bezpečnostní přístrojové funkce, zhodnotit jejich kritičnost (stanovit úroveň SIL), navrhnout jejich konfiguraci (MooN[1)]) a stanovit strategii preventivní údržby.

Petr Pekárek, Elmep, s. r. o.
„Možnosti člověka při zajištění bezpečnosti výroby jsou omezené a lidský operátor je daleko méně spolehlivý než automatický bezpečnostní systém, který je správně navržen, provozován a udržován v souladu s příslušnými normami.“

Zabezpečení strojů a strojních zařízení proti následkům poruchy jejich vlastního řídicího systému řeší norma ČSN EN ISO 13849-1/2008, o bezpečnostních částech řídicích systémů. Přechodné období ukončování platnosti staré normy EN 954-1 skončí 31. 12. 2011. Jak se uplatňování této normy projeví v návrhu řídicích systémů?

Zdeněk Švihálek (B+R automatizace):
Norma EN 954-1 se vůbec nezabývala elektronickými programovatelnými systémy a u bezpečnostního systému definovala pouze jeho strukturu, tzv. kategorii. Nové normy ISO 13849-1 a IEC 62061 se už zabývají i elektronickými programovatelnými systémy a kromě struktury bezpečnostního systému posuzují i jeho kvalitu. K dosažení určité úrovně bezpečnosti (PL) tedy již nestačí pouze například dvoukanálový systém (kategorie podle EN 954), ale musí se posoudit i parametry ($MTTF_d$, *DC*, kategorie atd.) jeho jednotlivých prvků (tlačítka, spínače, zámky, stykače, světelné závěsy, měniče frekvence apod.), včetně samotného bezpečnostního PLC. Nové normy přesně určují, jak by měl vypadat a jakým způsobem by měl být vyvíjen bezpečnostní aplikační software. Výrobci strojů u nás většinou postupují podle ISO 13849-1, která neřeší jen elektroniku, ale celý bezpečnostní systém stroje, včetně například mechanických a hydraulických prvků. Navíc má tato norma oproti IEC 62061 poněkud „mírnější“ požadavky.

Výrobci bezpečnostních PLC musí postupovat podle normy IEC 61508, ze které obě již zmíněné normy vycházejí a která klade velmi přísné požadavky na konstrukci elektroniky a firmwaru. Tato norma definuje nyní často používaný pojem SIL.

Filip Pelikán (Sick):
Norma ČSN EN ISO 13849-1/2 je na první pohled velmi komplikovaná a ke správnému výsledku se dochází velmi složitě oproti zažité normě EN 954-1. Na druhý pohled ale ČSN EN ISO 13849-1/2 umožňuje širokou flexibilitu. Požadované úrovně vlastností PL lze dosáhnout s použitím široké palety komponent a způsobů zapojení. Osobně považuji prodloužení platnosti EN 954-1 za chybu.

Antonín Zajíček (Schneider Electric CZ):
Mnoho konstruktérů a projektantů se s novou normou ještě neszilo – považují ji za příliš složitou. Naštěstí existuje několik vhodných softwarových nástrojů, které konstruktérům práci usnadní. V mnoha případech je přímo navedou k bezpečnějšímu řešení. Velkou roli zde samozřejmě hraje ochota výrobců komponent vůbec někomu sdělit hodnoty potřebné pro výpočet SIL/PL.

Není velký důraz na bezpečnost výroby v EU konkurenční nevýhodou pro evropské výrobce ve srovnání se zeměmi, kde se na bezpečnost tolik nehledí?

Antonín Zajíček (Schneider Electric CZ):
Evropští výrobci strojů, kteří uplatňují své výrobky ve státech EU, jsou v oblasti bezpečnosti strojů vázáni stejnými pravidly, která platí i pro importéry z tzv. třetích zemí. Zde tedy pes zakopán není. Hlavní problém vidím u provozovatelů strojních zařízení (výrobců zboží). Stává se totiž, že náklady na nezbytné dovybavení strojů o bezpečnostní prvky prodraží výrobu. Tyto dodatečné náklady jsou výrobci nuceni promítnout do konečné ceny výrobků, a často tak ztrácejí konkurenceschopnost k levnému dovezenému zboží.

Zdeněk Švihálek (B+R automatizace):
Pro výrobce strojů to jistě nevýhodou je. Nicméně moderní bezpečnostní technika chrání nejen obsluhu, ale také stroj. Navíc dokáže na jakoukoliv nebezpečnou událost reagovat inteligentně, takže stroj může po takové události velice rychle opět najet na plný výkon.

Luděk Barták (Panasonic Electric Works):
Přizpůsobení a udržování všech procesů výroby v souladu s aktuálními bezpečnostními normami se logicky promítnou do ceny výrobku. Jestliže pořizujeme nové zařízení, rozhoduje při výběru více faktorů. Kromě ceny je to kvalita výrobku, technická podpora, záruka atd. Proč nezohlednit, za jakých bezpečnostních podmínek byl produkt vyroben? Pojďme najít mechanismus značení a kontroly tohoto faktoru.

Filip Pelikán (Sick):
Rozumný provozovatel strojního zařízení by měl uvažovat takto: Zranění vyškoleného zaměstnance a následné zaškolení nového mu přinese finanční ztrátu, která mnohdy řádově převyšuje cenu bezpečnostních komponent. Dobře zabezpečené strojní zařízení přináší plynulost, produktivitu i kvalitu výroby, a tím i vysokou konkurenceschopnost.

Petr Pekárek (Elmep):
Pohled na seznam katastrof v průmyslových provozech za posledních 40 let naznačuje, že investice do bezpečnosti není radno podceňovat (Flixborough 1974, Seveso 1976, Bhópál 1984, Texas 2005, Buncefield 2005). Ať už v EU nebo mimo ni, každý provozovatel průmyslového celku dojde k závěru, že je nezbytné aplikovat bezpečnostní politiku. Je nutné si uvědomit, že riziko nelze nikdy zcela eliminovat. Lze je pouze účinně řídit, tj. identifikovat a znát zdroje nebezpečí, umět ohodnotit velikost rizika a přijmout opatření na jeho snížení na akceptovatelnou míru.

V automatizaci provozů strojní výroby může být vhodné, aby lidská obsluha spolupracovala s robotickými prvky. Jaká jsou úskalí takových řešení v praxi?

Zdeněk Švihálek (B+R automatizace):
Robot je velmi nebezpečné zařízení. Robustní mechanika a silné motory mohou způsobit velmi vážná zranění. Přitom robot je vždy řízen softwarem, takže ke vzniku nebezpečné události stačí i malá chyba programátora. Vzhledem k topologii mechaniky robotu navíc i pomalý pohyb koncového bodu robotu (TCP) může způsobit velmi rychlé pohyby jednotlivých ramen a klou-

[1)] MooN značí hardwarovou robustnost bezpečnostního systému. Systém je tvořen „N“ nezávislými kanály, které jsou propojeny tak, že „M“ kanálů ještě zajistí bezpečnou funkci systému. Jsou-li např. na přívodním potrubí plynu do pece v sérii namontovány dva ventily, které mají v případě nebezpečí zavřít přívod plynu, jde o konfiguraci 1oo2. Přívod plynu se zavře, když úspěšně zafunguje alespoň jeden ze dvou ventilů, (anglicky 1 *out of* 2, zkráceně 1oo2). Toto uspořádání toleruje poruchu jednoho ventilu.

bů. Na trhu zatím není certifikovaný bezpečnostní software pro bezpečnou rychlost TCP robotu. Proto jsou robotická pracoviště většinou oplocená a obsluha vstupuje do pracovního prostoru robotu přes zabezpečené dveře nebo s robotem spolupracuje přes zabezpečený otvor v oplocení. To není příliš flexibilní, ideální je tedy spolupráci člověk-robot nahradit spoluprací robotů.

Filip Pelikán (Sick):
Robot je velmi nebezpečný, a proto je důležité robotizované pracoviště adekvátně zabezpečit, speciálně v případě interakce robot-člověk. Všude tam, kde se může pohybovat obsluha a i robot, je bezpodmínečně nutné člověka optoelektronickým bezpečnostním prvkem detekovat, a tak zajistit, že se robot s člověkem nemůže střetnout. Je ovšem ideální postavit robotizované pracoviště tak, aby k interakci robot-člověk nedocházelo.

Antonín Zajíček (Schneider Electric CZ):
Hlavní úskalí vidím v nedodržení dostatečné úrovně bezpečnosti. V oborech, kde spolupracuje obsluha s robotickými prvky, je vyžadována úroveň SIL 3 podle ČSN EN 62061/2005. Bezpečnostní prvky této úrovně jsou finančně náročnější, nicméně využití připadá v úvahu v oborech, kde by taková investice neměla být problém. Navíc ekonomické důsledky způsobené zastavením výroby by byly mnohem horší.

Požadují uživatelé z průmyslu také zajištění informační bezpečnosti řídicích systémů, tzv. *cyber security*?

Antonín Zajíček (Schneider Electric CZ):
V současnosti je *cyber security* vyžadována zejména v oblasti datových center, nicméně očekávám nárůst poptávky i na trhu průmyslu.

Zdeněk Švihálek (B+R automatizace):
Informační nebo též datová bezpečnost je důležitá i pro uživatele informační techniky používané v průmyslových řídicích systémech. Nedávno jsme přece zažili napadení řídicího systému a systému SCADA výrobní technologie průmyslového podniku po internetu a představa, že by bylo možné takto zvenčí ovlivnit chod strategických nebo potenciálně nebezpečných technologií, je alarmující. Každý řídicí systém, i ve strojích, je třeba chránit před napadením po síti. Naštěstí řídicí systémy používají většinou jiné softwarové prostředky než kancelářský svět a také síťové domény bývají striktně oddělené, už pro nutnost řízení v reálném čase.

Petr Pekárek (Elmep):
Stupeň zabezpečení záleží na typu řídicího systému a na typu spojení s jeho periferiemi a vstupy a výstupy. Jiné požadavky bude mít distribuovaný řídicí systém (DCS), který se nachází v jedné chráněné výrobní lokalitě, a jiné požadavky budou na ochranu systému SCADA. Uživatelé průmyslu zatím spíše inklinují k základním a levnějším ochranným prostředkům (mechanické zabezpečení, řízení a správa uživatelských účtů) než k pokročilejším řešením *cyber security* (např. povolení a správa vzdálených přístupů, monitoring a analýza síťového provozu). S rostoucím počtem útoků na řídicí systémy do budoucna očekávám také rostoucí poptávku po komplexních řešeních a službách v této oblasti.

Kde vzít odborníky na bezpečnost? Jsou znalosti absolventů technických škol o bezpečnostních systémech dostatečné?

Zdeněk Švihálek (B+R automatizace):
Sehnat dobré techniky do automatizační branže je problém již několik let. S odborníky na bezpečnost to bude ještě horší. Díky rozmachu programovatelných bezpečnostních systémů se jedná v podstatě o nový obor, který je silně svázán normami a komplikovanými schvalovacími procesy, takže nemusí být pro studenty příliš atraktivní. Naštěstí se však již nyní systémy funkční bezpečnosti vyučují na VŠB-TU v Ostravě, VUT v Brně a ČVUT v Praze. Ve spolupráci s ČVUT už dokonce řešíme i diplomové práce, které se zabývají posouzením bezpečnosti strojů a implementací systémů funkční bezpečnosti.

Filip Pelikán (Sick):
Znalosti absolventů vysokých škol ohledně bezpečnosti strojních zařízení jsou podle mého názoru takřka nulové. Je to zarážející v situaci, kdy na jedné straně zákon nařizuje výrobci – konstruktérovi – aby zkonstruoval bezpečný stroj. Jiný zákon vyžaduje, aby provozovatel používal jen bezpečný stroj. Neznalost zákona sice neomlouvá, ale absolventa VŠ možná ani nenapadne se o bezpečnost vůbec zajímat, když ho škola „pouze“ naučí, jak stroj navrhnout nebo provozovat!

Antonín Zajíček (Schneider Electric CZ):
Čerstvý absolvent nemůže nikdy „vědět všechno“. Spoustu informací nasbíráte až během praxe. A právě v praxi je nutné hledat odborníky na bezpečnost. Některé věci se lze naučit, ale mnohé je nutné si prožít, abyste byli schopni tomu příště zabránit. Tím samozřejmě nechci tvrdit, že si musím nechat useknout ruku, abych poté věděl, že do jistých částí stroje ji nemám strkat. Chci tím říct, že bez znalosti rizik jim nemůžu efektivně předcházet.

diskusi vedla Eva Vaculíková

krátké zprávy

▶ Trh s bezpečnostními systémy stále roste

Význam bezpečnostních systémů SIS v oblasti procesní výroby stále sílí. Je to spojeno s rostoucím stupněm automatizace výroby: koncoví uživatelé přikládají stále větší váhu systémům, které jim pomohou předcházet všem nepříznivým událostem.

Strategická analýza evropského trhu s bezpečnostními systémy pro procesní výrobu, kterou vypracovala společnost Frost & Sullivan (www.industrialautomation.frost.com), předpokládá, že objem trhu poroste ze současných 459,3 milionu amerických dolarů na 632,4 milionu v roce 2016. Průzkum se týkal těchto oblastí průmyslu: petrochemický průmysl, chemický průmysl, farmaceutický průmysl, energetika a ostatní (v této kategorii jsou zahrnuty mj. oblasti výroby papíru, těžební průmysl, metalurgie, vodárenství a zpracování odpadních vod).

Pro zajištění bezpečnosti a spolehlivosti výroby dávají zákazníci stále více přednost integrovaným systémům před samostatnými systémy pro řízení a pro zabezpečení technologie. Na to reagují dodavatelé nabídkou systémů, které kombinují řídicí a bezpečnostní komponenty a omezují potřebu zásahů operátora, tj. i možnost lidského selhání, na minimum. Provozovatelé výrobních závodů jsou navíc pod stále větším tlakem regulatorních nařízení a předpisů a musí se vyrovnat s přísnými požadavky na bezpečnost, konstatuje analytička společnosti Frost & Sullivan Katarzyna Owczarczyková.

Globalizace výroby s sebou nese potřebu řídit distribuovanou výrobu na dálku a přitom zachovat možnost přijímat rychlá rozhodnutí. Proto jsou nutné implementace několikaúrovňových bezpečnostních systémů.

Cena zařízení je i v tomto případě jedním z rozhodujících faktorů výběru. Pro ty výrobce, kteří dodávají integrované bezpečnostní systémy SIS (*Safety Instrumented System*), je to šance dokázat zákazníkům, že takové řešení je stejně dobré, ale cenově výhodnější než klasické řešení se samostatnými systémy pro řízení a pro zabezpečení. Proto vyvíjejí značnou iniciativu na poli osvěty a vzdělání, aby zákazníkům vysvětlili přednosti moderních SIS: jsou to nejen nižší pořizovací i celkové náklady, ale také spolehlivější provoz technologie a omezení doby odstávek. To vše vede ke zkrácení doby návratnosti investic, dodává Katarzyna Owczarczyková. To, že podobné iniciativy v odborných časopisech, tištěných i internetových, a na konferencích mají smysl, dokazuje nárůst objemu trhu v oblasti SIS, který je odrazem toho, že uživatelé novou techniku stále více akceptují. *(Bk)*