Informační bezpečnost jako součást funkční bezpečnosti řídicích systémů

Příspěvek volně navazuje na článek [1] věnovaný zajišťování funkční bezpečnosti produktů společnosti ZAT, a. s., i produktů od jiných výrobců používaných v automatizovaných systémech řízení, které tato společnost dodává. Společnost ZAT v rámci svého systému řízení jakosti vytvořila a dále rozvíjí vlastní systém zajištění funkční bezpečnosti tzv. přístrojových systémů spjatých s bezpečností (bezpečnostní přístrojové systémy, *Safety Instrumented System* – SIS), jehož úkolem je garantovat odpovídající funkční bezpečnost dodávaných automatizovaných systémů řízení. Uvedený vnitropodnikový systém zajištění funkční bezpečnosti produktů společnosti ZAT (dále *systém funkční bezpečnosti ZAT*) určuje pro společnost ZAT, jakožto výrobce a dodavatele řídicích systémů typu DCS pro velké energetické celky, optimální zajištění funkční bezpečnosti v rozsahu norem ČSN EN 61508-1 až 7, částečně ČSN EN 61511-1, 2, 3, ČSN IEC 61513, ČSN EN 1050, ČSN IEC 300-3-9 a IEC 12207.

Aspekty zajišťování funkční bezpečnosti

Systém funkční bezpečnosti ZAT jednoznačně definuje systém managementu funkční bezpečnosti, tj. systém, jakým je organizována dokumentace životního cyklu bezpečnosti, činnosti a dokumenty požadované při tvorbě plánů funkční bezpečnosti pro jednotlivé zakázky, cíle a požadavky jednotlivých fází životního cyklu bezpečnosti, způsoby jejich verifikace i proces odhadu a potvrzení výsledné funkční bezpečnosti.

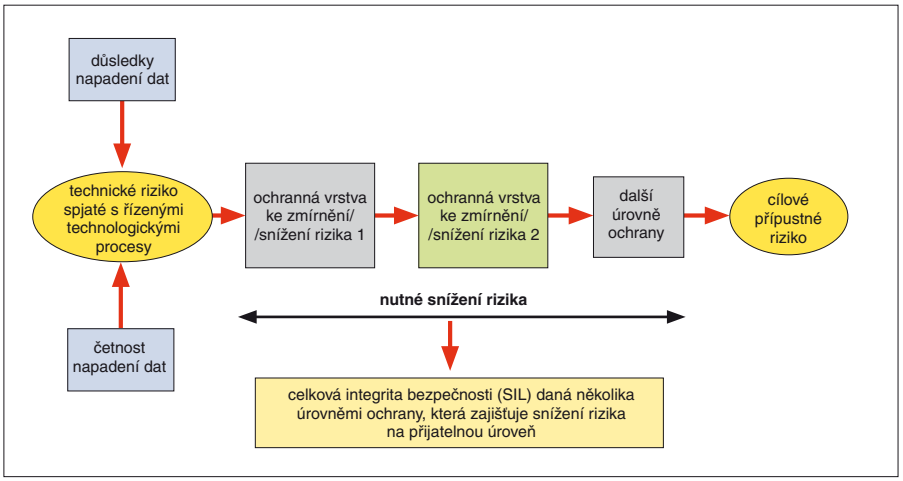
Uvedený systém managementu funkční bezpečnosti zasahuje také do oblasti řídicích systémů, kde pokrývá relevantní činnosti, postupy a dokumenty tvořící systému managementu bezpečnosti informací, který je předmětem norem ČSN ISO 27001 a ČSN ISO 17799.

Součástí systému funkční bezpečnosti ZAT jsou rovněž návody a metodické postupy k činnostem tvořícím náplň patrně nejdůležitější a nejnáročnější fáze zajištění funkční i informační bezpečnosti. Těmito činnostmi jsou zejména analýzy nebezpečí a rizika, tvorba modelů spolehlivosti, výpočty spolehlivosti a výběr technik a opatření ke zvýšení spolehlivosti systémů a snížení rizika vzniku nebezpečných událostí plynoucích z poruch a vad systémů nebo vlivu lidského činitele. Důraz je přitom kladen na to, aby veškeré zaváděné návody, metodiky a postupy byly použitelné v technické praxi.

Kvantifikace funkční bezpečnosti a nutné snížení rizika

Mají-li se stanovovat požadavky na prostředky, které zajistí požadovanou úroveň funkční (i informační) bezpečnosti, tedy nutné snížení rizika, je třeba pro každé nebezpečí provést odhad rizika a následně určit požadovanou míru bezpečnosti a zjistit, při jakých vlastnostech ochranných prostředků jí lze dosáhnout.

Mírou funkční bezpečnosti je podle ČSN EN 61508 tzv. *integrita bezpečnosti* (*safety integrity*) neboli pravděpodobnost, s jakou bude bezpečnostní (nebo řídicí) systém uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu.



Obr. 1. Snížení rizika na přípustnou úroveň použitím několika vrstev ochranných opatření

Rozměrem (jednotkou) integrity bezpečnosti je *úroveň integrity bezpečnosti* (*Safety Integrity Level* – SIL) jako diskrétní hodnota (jedna ze čtyř možných – SIL 1 až SIL 4) umožňující kvantitativně stanovit požadavky na integritu bezpečnosti bezpečnostních funkcí přiřazených bezpečnostním přístrojovým systémům (SIS), kde SIL 4 znamená nejvyšší a SIL 1 nejnižší úroveň integrity bezpečnosti.

Způsob, jakým se dosáhne přípustného nebo přijatelného rizika v případě ochrany dat v závislosti na požadované úrovni integrity bezpečnosti, je naznačen na *obr. 1*.

Riziko se označuje jako *přípustné* v případech, kdy je jeho další snížení buď neproveditelné, nebo náklady na jeho snížení jsou ve velkém nepoměru k dosaženému zlepšení. Naproti tomu *přijatelné* riziko takové, jehož velikost se považuje za tak malou a bezvýznamnou, že se nepožaduje její další zmenšení.

Vliv funkční bezpečnosti na řídicí a bezpečnostní systémy

Požadavky na funkční bezpečnost stanovené analýzou mají významný vliv na způsob realizace i používání řídicích a bezpečnostních systémů.

Ve fázi projektování vedou požadavky na dosažení funkční bezpečnosti, v závislosti na žádané úrovni integrity bezpečnosti, především k používání několikakanálových struktur v konfiguraci bezpečnostních systémů, na diverzitu hardwarových a softwarových komponent bezpečnostních systémů a jejich diagnostické pokrytí, k zabezpečení napájení a k zajištění informační bezpečnosti komunikačních kanálů a monitorovacích a ovládacích komponent a systémů. Strukturované aplikační programy se vytvářejí s použitím řádně testovaných a ověřených softwarových modulů.

Ve fázi instalace a uvádění do provozu je třeba dbát zejména na oddělené a zabezpečené soustavy pro napájení bezpečnostních systémů, oddělené vedení a patřičné označení kabeláže, oddělené snímače a měřicí kanály, oddělené samostatné skříně systémů umístěné v prostředí, pro které byl systém testován, a na další opatření zabraňující poruchám se společnou příčinou.

Pro fázi provozování bezpečnostních systémů se požadavky spjaté s funkční bezpečností uplatňují převážně prostřednictvím provozních předpisů určujících způsoby školení a požadovanou kvalifikaci pracovníků obsluhy, operátorů i údržbářů, úkony při profylaktické i ostatních druzích údržby, včetně periodických kontrolních zkoušek zařízení, činnost operátora při potvrzování výstražných hlášení týkajících se bezpečnosti technologického zařízení a následné činnosti a činnost operátora při monitorování bezpečnostních funkcí, jejich záměrném vyřazení z činnosti nebo při jejich poruše.

Zajištění funkční bezpečnosti řízeného zařízení (*Equipment Under Control* – EUC) a řídicích a bezpečnostních systémů se tak stalo záležitostí nejen výrobce a dodavatele řídicích a bezpečnostních systémů, ale podílejí se na něm všichni účastníci životního cyklu bezpečnosti zařízení, jako např. generální dodavatel, investor a konečný uživatel.

Řídicí systémy a informační bezpečnost

Ze zmíněných opatření reflektujících požadavky na funkční bezpečnost ve fázích realizace a provozování řídicích a bezpečnostních systémů se s problematikou informační bezpečnosti prolínají především vícekanálové struktury komunikačních kanálů, redundantní zabezpečené napájení, zabezpečení dat v komunikačních kanálech a zabezpečení monitorovacích a ovládacích systémů.

V oblasti informační bezpečnosti řídicích systémů se významně uplatňuje vliv lidského činitele.

Specifikum datových sítí řídicích systémů samo o sobě do jisté míry omezuje bezpečnostní rizika, kterým jsou vystaveny veřejné nebo privátní datové sítě a zařízení umožňující dosahovat mocenského nebo ekonomického zisku. V rámci funkční (i informační) bezpečnosti jsou přesto předmětem analýzy rizika i metody umožňující omezit vliv lidského činitele a jiných nebezpečí na data v komunikačních kanálech řídicích systémů a jejich koncových zařízení. V řídicích systémech se, podobně jako v informační technice (IT), používají různá ochranná opatření, a to v závislosti na požadované úrovni integrity bezpečnosti.

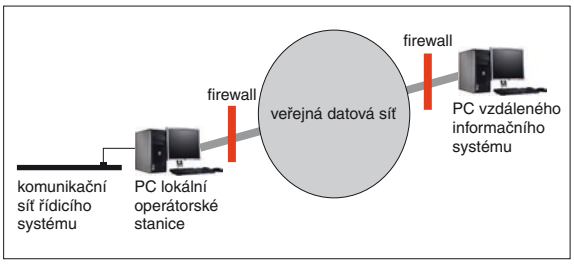
Jaká jsou tedy u řídicích systémů možná nebezpečí a rizika spojená s přenosem dat v systémových sítích na jedné a ochranná opatření použitelná ke snížení rizik na druhé straně?

Nejčastějším bezpečnostním rizikem zařízení pracujících s daty je výpadek napájení, poměrně časté je poškození konzistence dat vlivem náhodné poruchy nebo elektromagnetického rušení a nejmenší četnost má poškození, ztráta nebo zcizení dat v důsledku lidské činnosti.

Ke snížení uvedených rizik se standardně používají tyto metody ochrany dat:

- zálohované napájení s okamžitým záskokem na všech úrovních a použití zdrojů nepřerušovaného napájení (UPS),
- redundantní systémové přenosové kanály se zabezpečením konzistence dat kontrolním součtem,
- důsledné oddělení administrativní a technologické systémové sítě,
- použití hardwarových klíčů pro přístup do softwarového pracovního prostředí monitorovacího, ovládacího nebo servisního zařízení,
- autorizace přístupu k monitorovacím a ovládacím systémů,
- základní ochrana před ztrátou dat zálohováním obsahu paměti operátorských stanic (monitorovací a ovládací systém) a zálohováním dat na archivačním serveru.

Účinnost těchto opatření není pro všechna rizika vždy dostačující. Zatímco ochrana zálohováním napájení a zálohováním dat na serveru je sama o sobě dostačující i pro vyšší úroveň integrity bezpečnosti, k dosažení stupně ochrany konzistence a věrohodnosti dat odpovídajícího vyšší úrovni integrity bezpečnosti je třeba používat systémové komunikační kanály s fyzickou bezpečnostní vrstvou se zvýšeným zabezpečením dat (např. profil Profisafe komunikačních systémů Profibus a Profinet od společnosti Siemens).



Obr. 2. Dálkový přenos technologických dat prostřednictvím veřejné datové sítě

Účinnost ochrany dat na základě přístupových úrovní (autorizace) je velmi dobrá, jde-li o náhodný pokus o přístup. Pro vyšší úroveň integrity bezpečnosti je ovšem nedostatečná. Každý uživatel se sice musí při vstupu do svého pracovního prostředí na monitorovacím a ovládacím nebo servisním zařízení přihlásit uživatelským jménem a heslem a přístup na úrovně umožňující poškození, ztrátu nebo zcizení dat mají většinou pouze administrátor (pracovník dodavatele zařízení) nebo systémový inženýr (pracovník uživatele). Systém převážně dokumentuje okamžitý stav, historii aktivit uživatelů i pokus o prolomení přístupových práv. Přesto s sebou použití přístupových úrovní nese poměrně velké riziko selhání. K průniku v tomto případě dochází většinou zevnitř, nežádoucí aktivitou pracovníků konečného uživatele. Dalšího snížení rizika je pak dosahováno především fyzickým omezením možného kontaktu se zařízením.

Informační bezpečnost a dálkový přenos dat v řídicích systémech

Donedávna se pro dálkový přenos dat v řídicích systémech, a to nejen z důvodu informační bezpečnosti, výhradně používaly pronajaté pevné linky (metalické nebo optické) nebo rádiové spojení na pronajatých frekvencích. Tato pojítka jsou co do možnosti ovlivnění dat stejně bezpečná jako lokální systémové komunikační sítě a pro ochranu dat jsou u nich používány i stejné prostředky (viz předchozí odstavec).

S prudkým rozvojem IT roste i komfort nabízený k použití při monitorování a ovládání řídicích systémů na dálku. Prostřednictvím veřejných datových sítí (Internet a technika ADSL) je možné technologické zařízení monitorovat nejen ve vzdálených dozornách, ale i v domácnostech vrcholových manažerů nebo prostřednictvím techniky WiFi kdekoliv. Po mobilní datové síti (např. GPRS) lze posílat jak upozornění na události v řízeném zařízení přímo do mobilního telefonu pověřených pracovníků, tak i – mobilním telefonem propojeným s notebookem – data. Zároveň se ale rozšířily možnosti, jak získat zajímavá data jako prostředek vydírání nebo data ovlivnit s úmyslem teroristického útoku.

U klasické informační techniky je problém ochrany dat prioritou číslo jedna, i když se rozlišuje míra rizika, tj. četnost a hlavně důsledek poškození, ztráty nebo zcizení dat. S převážnou většinou dat se zde pracuje při použití standardních ochranných opatření. Pro citlivá data se používají náročnější způsoby zabezpečení (zabezpečené stránky, šifrování, sledování provozu atd.) a některá data nelze vůbec veřejnými (Internet) nebo privátními (Intranet) sítěmi přenášet.

Podobná situace je i u řídicích systémů, ale kritéria pro rozlišení nebezpečí a hodnocení rizika jsou odlišná. Okamžitá ztráta dat bývá hodnocena jako přijatelné riziko, nebezpečná jsou neautorizovaná a škodlivá data. Důležitý je i směr toku dat. Konkrétně u ochranných systémů, tj. bezpečnostních systémů s úrovní integrity bezpečnosti SIL 3, paradoxně ztráta nebo poškození dat jdoucích do informačního systému nepředstavují nebezpečnou událost, neboť ochranný systém pracuje autonomně, bez zásahu operátora. Kritické je naopak riziko poškození dat nebo průniku škodlivých dat směrem do ochranného systému. Proto společnost ZAT používá pro bezpečnostní systémy s úrovní integrity bezpečnosti SIL 3 jednosměrné redundantní sériové komunikační linky principiálně vylučující průnik jakýchkoliv potenciálně nebezpečných dat do bezpečnostního systému.

Možná nebezpečí a rizika spojená s dálkovým přenosem dat veřejnými a mobilních sítěmi jsou tato:

- škodlivý kód – virus (spyware, spamy a ostatní malware jsou u řídicích systémů irelevantní),
- napadení hackerem zvenku,

– interní rizika u uživatele nebo správce sítě (neopatrnost nebo úmysl).

Největší a nejčastěji se vyskytující riziko představuje třetí z uvedených skupin.

Hlavní ochranná opatření snižující uvedená rizika jsou tato:

– antivirové systémy instalované v místě připojení systémové sítě,
– brány typu firewall,
– šifrování dat,
– uzamčení přímého přístupu do systémové technologické komunikační sítě (podmínkou je oddělení administrativní a technologické systémové sítě),
– zákaz používání poštovních klientů v systémové technologické komunikační síti (podmínkou je opět oddělení administrativní a technologické systémové sítě),
– autorizace uživatele.

Problémy s přenosem dat při monitorování a ovládání řídicích systémů na dálku prostřednictvím veřejných datových sítí (Internet přes ADSL, GPRS) řeší společnost ZAT ve spolupráci s externími firmami (poskytovateli používaných služeb) využitím outsourcingu v oblasti ICT (*Information and Communication Technology*). V závislosti na úrovni integrity bezpečnosti se většinou používají šifrované datové tunely (popř. virtuální privátní síť – VPN) s připojením ADSL v kombinaci s firewally na lokálních průmyslových PC s monitorovacím a ovládacím softwarem (produkty firmy Wonderware) u řízeného zařízení i vzdáleného (vzdálených) PC s obdobným programovým vybavením (*obr. 2*).

Závěr

Jedním z prvořadých úkolů při projektování, uvádění do provozu a provozování automatizovaných systémů je zajistit funkční a s ní související informační bezpečnost řízeného zařízení i řídicích a bezpečnostních systémů. Podílet se na tomto úkolu musí nejen výrobce a dodavatel řídicího a bezpečnostního systému, ale i ostatní účastníci životního cyklu bezpečnosti zařízení, jako např. generální dodavatel, investor a konečný uživatel. Společnost ZAT má pro tuto oblast vybudovaný vnitropodnikový systém zajištění funkční bezpečnosti produktů, které dodává. Systém vychází z aktuálních norem platných v oboru a umožňuje společnosti ZAT pokrýt všechny aspekty funkční i informační bezpečnosti, včetně přenosu řídicích dat na dálku, i velmi složitých řídicích systémů typu DCS, jichž je společnost ZAT výrobcem a dodavatelem.

Literatura:

[1] *Zajišťování funkční bezpečnosti přístrojových systémů společnosti ZAT.* Automa, 2006, roč. 12, č. 11, s. 20–21.

Ing. Oldřich Žáček,
ZAT a. s.
(oldrich.zacek@zat.cz)

Advantech má za sebou úspěšné čtvrtstoletí

Společnost Advantech, dobře známá i českým uživatelům automatizační techniky, byla založena třemi inženýry, bývalými pracovníky společnosti Hewlett-Packard, v květnu v roce 1983 v Taipehu na Tchaj-wanu. V průběhu čtvrtstoletí se z lokálního tchajwanského výrobce stala významnou firmou s globální působností. Jeden ze zakladatelů společnosti, KC Liu, je v současné době výkonným ředitelem firmy. Základní informace o historii společnosti Advantech jsou v *tab. 1*.

Advantech se neohlíží jen do minulosti, ale plánuje také budoucí rozvoj svých aktivit. V současné době prochází změnami organizační struktury směrem ke koncepci *Globally Integrated Enterprise*, jejímž cílem je upevnit pozici firmy na světových trzích a reagovat na příležitosti spojené s nástupem nových webových služeb (web 2.0).

Změna se dotkne všech úrovní struktury firmy a jejím hlavním důsledkem bude decentralizace mnoha funkcí a posílení regionálních prodejních a technických týmů. Novinkou je také zavedení tzv. *Desing to Order Services*, služeb určených pro zákazníky, kteří požadují produkty přizpůsobené přesně na míru svým požadavkům.

Pro evropské zákazníky je v rámci přechodu na *Globally Integrated Enterprise* významnou novinkou především založení evropského centra péče o zákazníky, *European Customer Care Center*. Jde o centrální kontaktní místo a komunikační bránu společnosti Advantech pro zákazníky z celé Evropy. Centrum bude poskytovat rychlou a efektivní podporu a umožní zákazníkům využívat interní znalosti a zkušenosti pracovníků společnosti Advantech po celém světě. Cílem nového centra je zjednodušit a zkvalitnit vztahy zákazníků s firmou Advantech a nacházet cesty a způsoby, jak co nejlépe uspokojit všechny jejich požadavky.

Centrum bude poskytovat všeobecné informace o cenách a dostupnosti zboží, pomáhat zákazníkům při výběru komponent ze sortimentu firmy, starat se o katalogy a literaturu, bude řešit obchodní otázky a podporovat webové služby společnosti Advantech. Bude-li to třeba, zprostředkuje kontakt na technické odborníky zaměstnané ve firmě Advantech a postará se o to, aby se dotazy, připomínky a požadavky zákazníků dostaly vždy k té správné osobě v rámci firmy. Centrum tedy bude nejen poskytovat informace a podporu zákazníkům, ale bude též vytvářet zpětnou vazbu a přenášet informace od zákazníků na správná místa ve firmě.

Zákaznické centrum, umístěné v Mnichově, lze kontaktovat několika způsoby. Od pondělí do pátku od 9 do 12 a od 13 do 17 hodin jsou k dispozici bezplatné linky 00 800 242 680 80 (ePlatform) a 00 800 242 680 81 (eAutomation). Operátoři komunikují anglicky a německy. Centrum lze kontaktovat také e-mailem na adrese customercare@advantech.eu

(Bk)

Tab. 1. Historie společnosti Advantech

květen 1983	založení společnosti Advantech (Taipeh, Tchaj-wan)
1993	společnost získala ocenění jako nejlepší tchajwanská společnost v kategorii malých a středních firem *Taiwan Top Small & Medium Enterprise Award*
1993	otevření regionálních zastoupení v Düsseldorfu (SRN) a Miláně (Itálie)
1997	otevření regionálních zastoupení v Paříži (Francie) a Milton Keynes (Velká Británie)
1999	společnost vstoupila na tchajwanskou burzu
2003	otevření výrobního závodu v Kunšanu (Čína)
2004	vznik Advantech Europe, společné centrály pro zastoupení v SRN, Francii, Velké Británii, Itálii a Beneluxu
2004	otevření kanceláře ePlatform Office ve Feldkirchenu nedaleko Mnichova (SRN)
2004	společnost se dostala do seznamu *Taiwan Top 10 Global Brand*
2006 a 2007	společnost získala tchajwanskou cenu jako společensky odpovědná firma (*Corporate Social Responsibility Award*)
2007	založení kanceláře Advantech European Head Office (Feldkirchen, SRN)
2007 a 2008	začátek transformace na *Globally Integrated Enterprise*