Proč je v průmyslu kromě bezpečnosti stále důležitější i zabezpečení dat?

V moderní automatizaci se stále častěji používají otevřené systémy. To je užitečné z hlediska jejich vzájemné spolupráce, ale nese to s sebou velká rizika z hlediska zabezpečení dat a komunikace. Otevřené systémy jsou také náchylnější k sabotážím nebo průmyslové špionáži. Komunikační infrastruktura výrobních podniků a všechny komponenty jejich řídicích systémů by proto měly být certifikovány nezávislou certifikační institucí. To platí zejména pro bezpečnostně relevantní systémy.

Bezpečnostně relevantní systémy jsou stále častěji realizovány prostřednictvím softwarových komponent. Příkladem mohou být řídicí systémy v automobilech. Výrobci automatizační techniky hlásí rekordní nárůsty objemu výroby komunikačních prvků pro systémy zajišťující funkční bezpečnost. Jak dosáhnout dostatečného zabezpečení dat a komunikace, současně i velkého stupně integrace a komunikačního propojení systémů, a přitom neomezit funkční bezpečnost?

Zvyšující se možnost výměny dat mezi výrobními systémy přináší větší flexibilitu a nižší výrobní náklady. Omezuje se zmetkovitost, šetří se čas, materiál i energie. Není to začátek procesu integrace výrobních systémů, ale již jeho průběh: není náhodou, že tématem loňského veletrhu Hannover Messe byla „integrovaná výroba“. Komponenty, které dříve komunikovaly prostřednictvím vyhrazených protokolů, jsou nyní vybavovány rozhraními pro komunikaci prostřednictvím otevřených sítí.

Ochrana otevřených a uzavřených systémů

Na rozdíl od uzavřených systémů, založených na specifikacích jednotlivých výrobců, obsahují otevřené systémy standardizované hardwarové i softwarové prvky, jejichž specifikace jsou všeobecně známy. V automatizaci a informační technice otevřenost pomáhá při integraci nových komponent, koncoví uživatelé mohou díky otevřeným systémům snáze a rychleji reagovat na nové požadavky zákazníků a inovace výrobních postupů, ale současně tento postup usnadňuje přístup nepovolaným účastníkům komunikace. Ovšem ani uzavřené systémy dnes nejsou nepřekonatelnou překážkou. Je to jen otázka času a úsilí, které jsou narušitelé ochotni proniknutí do těchto systémů věnovat.

Riziko narušení bezpečnosti a integrity dat roste s mírou propojení komponent v řídicích systémech. Stuxnet, průmyslový virus určený k sabotáži, nebo průmyslový špionážní malware Flame posunují otázku zabezpečení dat do centra zájmu odborníků. Neplatí to jen pro podnikání v oblasti bezpečnostně kritické infrastruktury, jako jsou elektrárny a rozvodné nebo vodárenské sítě, ale i pro průmyslovou výrobu, zvláště pro potravinářský, chemický a farmaceutický průmysl. Téma zabezpečení dat se tu náhle setkává s tématem bezpečnosti výroby. Například v chemii a petrochemii mohou chyby ve výrobních procesech vést ke katastrofě spojené s velkými materiálními škodami a obětmi na životech. V těchto oborech je zabezpečení dat a komunikace nutné nejen pro zajištění bezpečnosti výroby a ochrany zdraví pracovníků, ale i pro ochranu životního prostředí a ochranu zdraví obyvatel v okolí výrobního závodu.

Dr. Kai Strübbe

Bezpečnost a zabezpečení dat patří k sobě

Bezpečnost i zabezpečení dat jsou úzce spojeny s prvky, které se používají v průmyslových řídicích systémech a komunikační infrastruktuře výrobních závodů. To, jak jsou technické komponenty ve skutečnosti bezpečné, závisí na jejich funkci, oblasti použití a kvalitě. Zvláště je důležité brát ohled na to, k jakému účelu je prvek použit. Jestliže řídicí systém ovládá např. osvětlení ve výrobní hale, není jeho selhání tak nebezpečné, jako když řídí výrobu např. průmyslových hnojiv, kde se používají výbušné vstupní suroviny. Jestliže mají řídicí systémy i bezpečnostní funkce, musí být vyloučena manipulace s jejich daty a případná sabotáž.

Nejvyšší míry bezpečnosti lze dosáhnout jedině tehdy, když jsou brány v úvahu nejen komponenty samotné, ale celá infrastruktura, v níž pracují, a to po celou dobu jejich životního cyklu: od návrhu, přes uvedení do provozu a provoz až po update jejich softwaru, modernizaci, popř. jejich výměnu. Z hlediska bezpečnosti to např. znamená navrhnout řídicí systém z komponent odolných proti poruše, s redundancí a velkou mírou diverzity. Konkrétní požadavky

Co je třeba pro zabezpečení dat a komunikace v průmyslu?

Používat komponenty jen z autorizovaných zdrojů (nejlépe přímo od výrobce).

Používat výhradně programy s digitálním podpisem a zakódované na ochranu proti reverznímu inženýrinku.

Zajistit, aby v zařízení bylo možné spustit jen určené programy (využití digitálních certifikátů).

Zaručit důvěryhodnost zdrojů dat (používat autentizaci a šifrovanou komunikaci).

Pro komponenty infrastruktury v provozu používat bezpečnostní hesla; tato hesla chránit (neposílat elektronicky).

Zavést systém přístupových práv (hesla pro vývojové inženýry, výrobní techniky atd.).

Udělat taková opatření, aby při průniku slabým místem do chráněného systému nebylo možné získat přístup do celého systému a ovládnout jej.

Tab. 1. Základní rozdíly mezi bezpečností a zabezpečením dat

Zabezpečení (*security*):	Bezpečnost (*safety*):
– zabezpečení systémů před neoprávněným přístupem zvnějšku, – ochrana důvěrnosti komunikace a konzistence dat, – zabezpečení systémů před výpadkem.	– provozní bezpečnost systémů: zajištění bezpečnosti a ochrany zdraví pracovníků i okolních obyvatel a ochrana životního prostředí, – zajištění dostupnosti systémů pro uživatele.

vycházejí z důkladné kvalitativní i kvantitativní analýzy rizik.

Z hlediska zabezpečení dat a komunikace je třeba pro utajení bezpečnostně relevantních dat používat šifrování a dostatečně odolné mechanismy autentizace. To se týká přístupu prostřednictvím veřejně otevřených komunikačních kanálů i ochrany komunikačních systémů před přetížením. Proto je doporučováno sledovat otázku zabezpečení dat a komunikace již v počátku vývoje, do řídicího systému zavádět potřebné bezpečnostní funkce, testovat je a realizovat penetrační testy.

Bezpečnost a zabezpečení prostřednictvím standardizace a certifikace

Pro oblast bezpečnosti existuje mnoho osvědčených norem, podle nichž je možné vyvíjet a certifikovat jednotlivé komponenty, komunikační infrastrukturu a celé systémy. Příkladem může být norma ČSN IEC 61508 *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností*. Po splnění požadavků této normy je riziko spojené se škodami na zdraví a životech, na životním prostředí a na výrobním zařízení omezeno na přípustnou míru.

Ale jak je tomu v oblasti zabezpečení dat a komunikace? Zatímco pro oblast běžných „kancelářských“ informačních systémů příslušné normy existují, v oblasti průmyslových informačních a řídicích systémů jsou teprve vyvíjeny. Přestože pro tuto oblast momentálně není k dispozici žádná norma, jsou některé, jež lze částečně použít. Odborníci ze společnosti TÜV Süd Embedded Systems např. berou jako základ pro testování normu IEC 62443 *Industrial communication networks – Network and system security*. Na základě této normy vyvinuli plán testů, který zahrnuje zkoušky systémů ve fázi vývoje, postupy pro testování implementovaných zabezpečovacích funkcí a rozsáhlý soubor penetračních testů. V oblasti bezpečnosti tento postup vychází z normy IEC 61508, která je základní normou pro funkční bezpečnost.

TÜV SÜD Embedded Systems

Společnost byla založena v roce 2011. V roce 2012 otevřela zkušební a testovací laboratoř v Mnichově. Následovala její akreditace podle UCA (*Utilities Communication Architecture*) a akreditace jako kompetenčního centra pro IEC 61850. Na veletrhu SPS IPC Drives představila program certifikace IEC 61850 Conformance. TÜV Süd Embedded Systems je součástí mezinárodní společnosti TÜV Süd, která působí v oblasti certifikace v průmyslu a dopravě. Klíčové kompetence jsou poradenství, testování, certifikace a vzdělávání. Více než 17 000 zaměstnanců pracuje v 800 kancelářích v Evropě, Americe, Asii a Africe.

System tested – pilotní projekt EUROS

Tento zkušební postup, který kombinuje hlediska bezpečnosti a zabezpečení, byl základem pro možnost udělit první certifikáty v této oblasti. Certifikát označený jako System tested představila společnost TÜV Süd loni v únoru na veletrhu Embedded World v Norimberku. V současné době probíhá certifikace v praxi na několika pilotních projektech. Je mezi nimi také mikrojádro od společnosti EUROS Embedded Systems GmbH z Norimberku. Mikrojádro je základní stavební prvek, který najde uplatnění v různých řídicích systémech, mimo jiné i v systémech určených pro procesní průmysl.

Protože některé řídicí systémy plní i bezpečnostní funkce, jsou požadavky na spolehlivost a dostupnost jejich jádra obzvlášť vysoké. Jádro nesmí být citlivé na útoky hackerů nebo pokusy o sabotáž. Podstatným předpokladem pro certifikaci bylo, aby byly zároveň zajištěny bezpečnost i zabezpečení a aby toto zajištění nemělo žádný negativní vliv na činnost jádra – např. prodloužení doby reakce v úlohách reálného času. Tento bod je zvláště důležitý, protože v průmyslu je doba reakce často kritickou veličinou. Nejvýznamnější předností nového certifikačního postupu vyvinutého společností TÜV Süd je to, že jedním postupem testuje bezpečnost i zabezpečení a v případě úspěšného završení certifikační procedury dostane zákazník jako doklad příslušný certifikát.

Riziko a investiční náklady

Stále nové druhy malwaru dokazují, že i v průmyslovém prostředí je bezpodmínečně nutné důkladné zabezpečení komunikace. Certifikace, založená na odpovídajících normách, je v této oblasti velkou šancí. Pro to, aby byla současně zajištěna funkční bezpečnost i zabezpečení komunikace proti nežádoucím přístupům, je nutné pečlivé společné vyhodnocení obou hledisek, vycházející z analýzy jednotlivých komponent. K tomu je třeba brát v úvahu i hledisko hospodárnosti. Zabezpečení automatizační techniky a infrastruktury průmyslových komunikačních systémů klade velké požadavky na odborné znalosti. Je nutné zvážit investiční náklady potřebné na certifikaci hardwaru a softwaru a poměřit je s dosaženou mírou omezení rizika. V každém případě je zapotřebí individuálně vyvážit bezpečnost a hospodárnost. Základní orientaci uživatelům strojů a zařízení poskytují platné normy a nezávislé certifikáty, udělené výrobcům jednotlivých komponent.

Dr. Kai Strübbe, TÜV SÜD AG

krátké zprávy

▶ Společnost ZAT zprovoznila tři řídicí systémy parních turbín

Příbramská společnost ZAT zprovoznila v jednom měsíci tři turbíny, v Biocelu Paskov, elektrárně Opatovice a v německém Stendalu, v celkové hodnotě 25 milionů korun. Na obnově elektrárny Opatovice, která je jednou z největších tepelných elektráren v ČR, spolupracuje ZAT dlouhodobě. Technici této firmy nechyběli ani při rekonstrukci stávající turbíny, kterou od října řídí systém SandRA Z200 nejnovější generace, navazující na světově uznávanou značku ZAT Primis. Při generální opravě turbíny společnost ZAT rekonstruovala řídicí a ochranný systém turbíny, včetně její hydraulické části (okruhy regulačních olejů).

Modernizovaná turbína pomůže v rozvoji přednímu českému výrobci viskózové buničiny Biocel Paskov. Energetické centrum Biocel Paskov provozuje dvě parní turbíny s nominálním výkonem 2× 20 MW od výrobce SGP Rakousko. V minulosti zde technici ZAT vyměnili a následně upravili řídicí systém, před šesti lety dodali řídicí systém Simatic S7-400 od společnosti Siemens. V letošním roce Biocel Paskov přistoupil k výměně technologické části parní turbíny od společnosti Siemens Brno se změnou ovládání turbíny a zásadní změnou ovládání nového rychlozávěrného okruhu. Úpravou řídicích a regulačních obvodů byla pověřena opět společnost ZAT.

ZAT dlouhodobě spolupracuje s předním výrobcem turbín – plzeňskou společností Doosan Škoda Power. Po projektech v Itálii, Bosně, Česku, Rumunsku a Maďarsku zprovoznil ZAT letos v říjnu další řídicí systém, tentokrát na nové parní turbíně Doosan Škoda Power v německém Stendalu. Byl zde použit řídicí systém na platformě Simatic PCS 7 a projekt zahrnoval i dodávky řídicího a ochranného systému turbíny Simatic S7-400 a kompletní zařízení přístrojového vybavení a kabeláže. Součástí projektu byl komunikační systém na nadřazený blokový DCS společnosti Metso.

(ev)