Problematika zavádění konceptu Industry 4.0 – díl III. – Jak na průmyslové komunikační sítě při integraci ve stávajících výrobních podnicích

Ve druhém článku našeho seriálu o problematice Industry 4.0 v tuzemském průmyslu (Automa 11/2017, str. 14 až 15) jsme se zaměřili na úlohu integrace z pohledu různých typů automatizačních úloh. V článku jsme vycházeli z předpokladu, že síťová infrastruktura je již vybudována. Jednotlivé typy automatizačních úloh jsme tak mohli rozdělit na tři, podle našich zkušeností typické úlohy. Šlo o integraci řídicích systémů pro spojité řízení, integraci systémů pro diskrétní řízení a integraci výrobních strojů (obráběcí stroje a výrobní stanoviště). Pro každou z těchto úloh jsme popsali typické požadavky, se kterými býváme v případě integrace konfrontováni, tj. co z technického pohledu znamená danou integraci realizovat a jaká technická úskalí nás přitom čekají.

Další příspěvek věnujeme problematice vlastní komunikační sítě, resp. metodice, jak jedno každé zařízení opravdu připojit.

Naším cílem je, aby každé instalované zařízení vybavené řídicím systémem bylo připojeno do komunikační sítě. V intencích většiny odborných publikací o Industry 4.0 by veškerá zařízení měla být na jedné úrovni sítě. Toto napojení by mělo nahradit všechny doposud existující komunikační standardy a vše sjednotit do jedné komunikační platformy bez ohledu na to, zda jde o přenos vstupů a výstupů (dříve realizovaný sítěmi kategorie např. Profibus nebo Profinet), nebo o přenos dat z PLC do HMI, nebo z HMI do MIS/MES (realizovaný sítí Ethernet), a nebo jiné datové přenosy.

Jak se však postavit k reálné situaci, kdy chceme na jedné straně sbírat data z řídicích systémů původně do sítí nezapojených nebo vlastními komunikačními sítěmi oddělených a vše *de facto* propojit a na druhé straně maximální možnou měrou zamezit „možným nepovolaným“ manipulacím a velmi často vyhovět i různým požadavkům korporátních oddělení IT?

V naší realizační praxi se při integraci řídicích systémů v podstatě setkáváme se třemi různými přístupy, od striktně konzervativního přístupu až po novátorský podle Industry 4.0.

Konzervativní přístup plně oddělených sítí

Nejvíce konzervativní přístup při připojení řídicích systémů pro sběr (popř. zápis) dat je úplné oddělení na úrovni fyzické vrstvy. V praxi se to uskutečňuje instalací separátního sběrného PLC (nebo jiného výpočetního systému), který je na jedné straně připojen k vlastnímu řídicímu systému prostřednictvím vstupů a výstupů nebo libovolné komunikační sítě (sériové linky, provozních sběrnic Profibus, DeviceNet apod.), na straně druhé je připojen do sítě sběru dat. Tím je dosaženo vlastního fyzického oddělení, i když je přitom nutné respektovat případnou možnost routování u nejnovějších PLC, kterou je nutné v nastavení zakázat. Touto metodou sice dokonce při propojení digitálními signály dosáhneme úplného oddělení řídicích systémů od sítě pro sběr dat, ale okrádáme se o možnost na dálku sledovat a programovat vlastní řídicí systém, popř. modifikovat rozsah komunikovaných dat pro účely nadřazeného systému. Dosáhneme tak v tomto případě 100% oddělení a ochráníme program řídicího systému před případným zneužitím či kopírováním unikátního *know-how*, výhody, které nám takovéto propojení s komunikační sítí přinese, jsou ale značně omezené.

Instalace separátního komunikačního procesoru

Druhou metodou je instalace separátního komunikačního procesoru do řídicího systému a vytvoření samostatné sítě propojující pouze komunikační procesory určené pro sběr dat. Touto metodou vytvoříme oddělenou speciální síť určenou pouze pro sběr dat, se svým vlastním adresním prostorem. Vytvoříme tak sice oddělenou zabezpečenou strukturu, ale i tento přístup má svá negativa. Jde zejména o nutnost rozšířit existující řídicí systém novým komunikačním procesorem, pro což je nezbytné, aby existoval potřebný volný slot pro instalaci. Neopomenutelná je také finanční stránka celé instalace, neboť běžné ceny komunikačních procesorů standardních PLC se pohybují v relaci 500 až 2 000 eur, což velmi často v případě linek či hal s desítkami řídicích systémů představuje neakceptovatelný náklad. Další otázkou je, jak nastavit vlastní nově instalovaný procesor pro sběr dat, zda povolit, či nepovolit přístupy do CPU apod.

Propojit všechno se vším

Poslední, nejjednodušší a nejlevnější variantou je propojení všech zařízení, která se v dané lokalitě nacházejí, do jedné společné komunikační sítě. Z pohledu hardwarového vybavení jde o využití nebo dovybavení ethernetovými komunikačními rozhraními. Taková architektura však v okamžiku implementace vytvoří z původně oddělených sítí síť jedinou. S vytvořením jedné jediné sítě, která bude obsahovat všechny komponenty jak ze světa „řízení technologie“, tak i ze světa „ekonomických informačních systémů“, se objevují všechny výhody, jež komunikační technika přináší. Lze přenášet data do centrálního serveru, je možné všechny řídicí systémy na dálku monitorovat a programovat, je možné přistoupit třeba i ze snímačů na internet a opačně, ale objeví se i opačný problém: jak takovouto síť zabezpečit, resp. jak danou strukturu sítě navrhnout, aby splňovala alespoň základní bezpečnostní standardy.

Pojďme se nyní krátce podívat na správný postup při vypracovávání návrhu komunikačního prostředí pro řízení technologických zařízení na bázi průmyslového Ethernetu.

Každý, kdo navrhuje jednotnou komunikační infrastrukturu, si musí, a to dávno před tím, než vezme do ruky tužku a papír a začne s vlastním návrhem komunikační sítě, položit několik základních otázek. V mnoha projektech se ale tento krok opomine a důsledky takovéhoto opomenutí se pak zkoumají a řeší až v okamžiku oživení díla. To bývá už pozdě, neboť na rozdíl od řádků kódu v PLC nebo PC obvykle nelze již instalované kabeláže a zejména optické trasy jen tak rychle změnit.

A nyní ony základní otázky. Lze je rozdělit do tří skupin. Tou první je oblast fyzického rozmístění prvků (topologie), druhou pohled na fyzické zabezpečení a třetí zabezpečení systému.

Topologie

Mezi základní otázky pro návrh topologie patří:

- jaká je základní konstrukce sítě (fyzická topologie – kruh, hvězda, kombinace apod.),
- mechanicko-elektrické požadavky – standardy pro rozváděče s infrastrukturou, konstrukce lávek páteřních sítí a podsítí, konektory, zámky apod.,
- požadavky na redundanci – napájení, záložní cesty, odolnost proti více chybám,
- očekávaná koncová zařízení a z toho plynoucí potřeby služeb sítě (distribuce zpráv, řízení toků skupinových komunikací, kon-

cová zařízení s konstantním výstupním datovým tokem apod.),
– rychlostní parametry páteřních a nepáteřních linek,
– logický model komunikace z pohledu očekávaných zátěží a objemů datových toků,
– dohled nad celým systémem a řešení tohoto dohledu (přičemž dohledem není čekání na poslední chybu, proti které je systém ještě odolný),
– požadavky na zpracování dokumentace (zejména realizační a následně i skutečného provedení) – neboť i toto je součástí dále zmíněného bezpečnostního pohledu na sítě, protože když uživatel infrastruktury netuší, jak infrastruktura vypadá a jaké služby poskytuje, bude velmi obtížné požadavkům zabezpečeného systému vyhovět.

Zabezpečení přístupu

Zastavme se nyní u již zmíněného bezpečnostního pohledu. Tady nás bude nejdříve zajímat zabezpečení fyzické. V této kategorii je hlavní otázkou bezpečnostní pohled od okamžiku přístupu do objektu k fyzickému přístupu k zařízení, tj. dostupnost klíčů k místnostem a rozváděčům, zajištění před neoprávněným vstupem a manipulací atd. Fyzické zabezpečení není třeba detailněji rozebírat, jde spíše o úlohu zabezpečení objektu a stanovení pravidel vstupu.

Při řešení zabezpečení systémů je zapotřebí stanovit a nastavit soubor opatření týkajících se konektivity jedné sítě na sítě jiné, v našem případě na sítě nadřazených systémů (např. na interní IT infrastrukturu jednotlivých podnikových subsystémů včetně ekonomických agend, sítě pro zajištění správy na dálku, sítě pro připojení a zabezpečení bezpečného provozu samostatných méně odolných zařízení – např. robotů, zajištění filtrace nechtěných komunikací, zajištění omezení provozu pro zařízení se speciálními režimy přenosu aj.).

Obě dvě oblasti zabezpečení musí jít v návrhu vedle sebe rovnocenně. Nemá smysl mít dokonale systémově zabezpečenou síť, která bude komukoliv dostupná k fyzickému poškození. Jestliže tedy považujeme fyzické zabezpečení za vyřešené standardně používanými zábranami, pro zabezpečení systému používáme také standardní zařízení typu firewall či firewall s routerem jako již zcela běžnou praxi. Je třeba vždy pečlivě zvážit, která zařízení a kam budou v dané síti použita, a to z několika důvodů:
– neexistuje obecné a „geniální“ zařízení, každý typ zařízení je určen k jiné primární službě a k této službě bývá i optimálně navržen,
– v průmyslovém prostředí platí zásada, že aktivní zařízení (switche, firewally), která mají přímou vazbu na technologická zařízení, by jim měla být co nejblíže (proto také např. existují transparentní „neviditelné“ firewally, které provádějí hloubkovou inspekci provozu v rychlosti komunikační linky – *wirespeed inspection firewall*),
– stejně tak v průmyslovém prostředí platí, že počty propojení do okolního světa by měly být co nejnižší, ideálně jedno redundantní a bezpečné místo, je třeba si uvědomit, že v zásadě každý bezpečnostní prvek (až na vzácné výjimky) vnáší jisté zpoždění do komunikace, které, zejména u rozsáhlých systémů, nemusí být vhodné a může způsobit značné problémy zejména u nyní hodně prosazovaných přenosů surových (*raw*) dat bez časové známky.

Domníváme se, že podaří-li se udržet návrh komunikační infrastruktury v mezích uvedených poznámek, bude mít uživatel k dispozici komunikační systém, který splní hlavní ideu dobře navrženého systému – tedy poskytovat veškeré služby tak, aby o chodu systému při jeho regulérním provozu nikdo nevěděl. Kdyby však při vašich záměrech vznikly pochybnosti o funkci či zabezpečení komunikační infrastruktury, neváhejte se na nás jako na autory tohoto článku obrátit. Jsme připraveni vám s návrhem, instalací i provozem pomoci.

Jiří Kasner, COLSYS AUTOMATIK Kladno,
Radim Novotný, SIDAT Praha

SIDAT a Sova Digital zakládají společný podnik SIDAT Digital

Cílem vznikající společnosti SIDAT Digital je v českých a slovenských podnicích realizovat nové typy projektů s uplatněním strategie průmysl 4.0. Bude tak podporován vznik výrobních technologií, ve kterých budou propojeny fyzické výrobní systémy s digitálními technologiemi. Veřejnosti bude nová firma představena 21. března ve 13:00 na veletrhu Amper v Brně.

SIDAT, spol. s r. o.:
Ryze česká společnost SIDAT byla založen v roce 1990, má 80 kmenových zaměstnanců a dosahuje obratu čtvrt miliardy korun. Na pracovištích v Praze a v Brně zabezpečuje dodávky v oblastech komplexní automatizace, výrobní informatiky, Customer Care, průmyslu 4.0 a integračních projektů. V roce 2017 se SIDAT stal jedním ze zakládajících partnerů Národního centra Průmyslu 4.0 při CIIRC na ČVUT v Praze.

Firma SIDAT Digital hodlá dodávat systémy pro řízení digitalizované výroby v automobilkách, ve strojírenství a potravinářském průmyslu. „Přední světové firmy teď přecházejí na sledování výroby prostřednictvím online digitálních dvojčat,“ říká jednatel společnosti SIDAT Radim Novotný.

Podstatou digitálních dvojčat je vytvoření digitální kopie reálného výrobního nebo logistického procesu na základě dat z existujícího výrobního procesu. Umožňuje využít shromážděná data pro simulaci a optimalizaci výrobního procesu, pro predikci a eliminaci nežádoucích událostí a pro kvantifikaci a identifikaci úzkých a problémových míst výroby.

„Online řízení výroby má klíčový význam i pro středně velké výrobní firmy, kterým takováto řešení můžeme nabídnout za přijatelných investičních podmínek,“ uvedl Radim Novotný.

„Přesouváme se do budoucnosti, kdy softwarové digitální technologie dokáží přímo ovlivňovat a řídit výrobní linky a tím zlevnit produkci jakéhokoliv zboží a zvýšit jeho kvalitu,“ dodal Radim Novotný.

(ed)

Sova Digital a. s.:
Slovenská společnost SOVA Digital už 27 let pomáhá slovenským podnikům digitalizovat a optimalizovat výrobních procesy v souladu s Industry 4.0 a zlepšovat si tím konkurenceschopnost a produktivitu. Za řešení digitálního dvojčete získala v minulém roce ocenění Inovace roku, udělované odborníky a ministerstvem průmyslu. SOVA Digital je dodavatelem systémů PLM firmy Siemens pro slovenský trh.