

Principy komunikace a diagnostika sítí Profinet

Tento článek si klade za cíl poskytnout základní informace o tom, jak Profinet funguje, jaké jsou principy komunikace a jak probíhá zpracování diagnostiky. Velká pozornost je věnována identifikaci a adresaci zařízení, protože zde je velký rozdíl ve srovnání se způsobem adresace v tradičních průmyslových sítích. Článek se také věnuje topologii sítě a zdůrazňuje hlavní výhody, které znalost topologie v daném automatizačním provozu poskytuje.

Profinet je komunikační systém podporovaný mezinárodní organizací Profibus & Profinet International a standardizovaný jako mezinárodní otevřený standard IEC 61158, který patří k nejrozšířenějším komunikačním systémům založeným na průmyslovém Ethernetu. Ke konci roku 2012 již bylo v provozu po celém světě instalováno téměř šest milionů zařízení Profinet.

Principy komunikace

Profinet využívá jako přenosovou vrstvu Ethernet, jak je popsán ve standardu IEEE 802.3. Jako prvky síťové infrastruktury jsou využity síťové přepínače neboli switche (označovány též jako komunikační mosty – *bridges*), které jsou definovány ve standardu IEEE 802.1D. Přepínač pracuje na úrovni druhé vrstvy komunikačního modelu ISO/OSI a pro koncová zařízení v síti je transparentní. Znamená to, že každý přepínač plní funkci předávání zpráv ve vstupním portu na výstupní port a že koncová zařízení o přítomnosti přepínačů „nemají ponětí“. Funkci přepínače ilustruje obr. 1, kde se předpokládá, že celá síťová infrastruktura je postavena pouze na přepínačích. Modré subsítě, ke kterým jsou připojeny koncové stanice, tedy představují část sítě alespoň s jedním přepínačem. Uprostřed sítě je explicitně znázorněn čtyřportový přepínač. Zde je nutné upozornit, že slovo „subsítě“ je zde myšleno jako část sítě, která obsahuje navzájem propojené koncové stanice na úrovni druhé, tedy spojovací vrstvy protokolu, a nemá v tomto smyslu nic společného s protokolem IP a IP-subnet. Z důvodu přehlednosti bude v tomto smyslu místo subsítě používáno slovo segment.

Předpokládáme tedy, že stanice v levé horní části obrázku, která je označena jako WAGO:01-02-03, chce poslat zprávu stanici Intel:01-02-03, umístěné v pravé horní části obrázku. Zpráva dorazí na port 1 přepínače uprostřed, který podle své interní tabulky adres zjistí, že koncová stanice je dostupná na portu 2. Z pohledu přepínače je pro tuto přenášenou zprávu port 1 vstupním portem a port 2 výstupním portem. Přepínač tedy přijme zprávu na vstupním portu, uloží ji do paměti a odešle na výstupní port. Není důležité, zda je stanice Intel:01-02-03 připojena přímo na výstupní portu, nebo je mezi výstupním portem přepínače a touto konco-

vou stanicí další přepínač. V uváděném případě zcela určitě alespoň jeden přepínač připojen být musí, protože segment sítě, ke kterému vede port 2 přepínače uprostřed, obsahuje dvě koncové stanice.

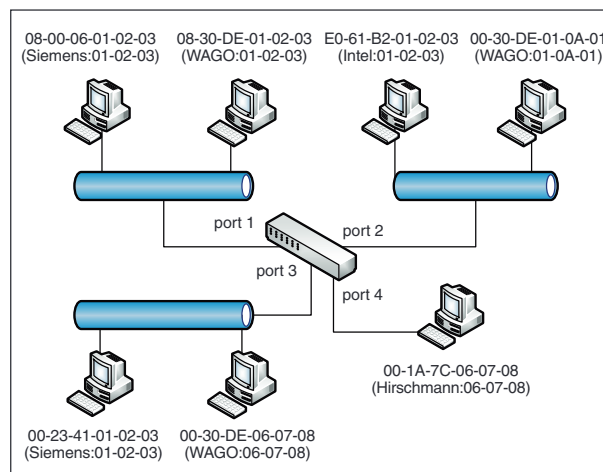
Použití přepínačů jako prvků síťové infrastruktury vede k odstranění kolizí na síti

priority se používá políčko VLAN, které je definováno ve standardu IEEE 802.1Q. Nelze tedy přesně zaručit, za jak dlouho projde zpráva celou sítí a dorazí na místo určení. V síti Profinet jsou zprávy s vyšší prioritou označovány jako RTC1 (*real-time class 1*) a zprávy s nízkou prioritou jako NRT (*non real time*).

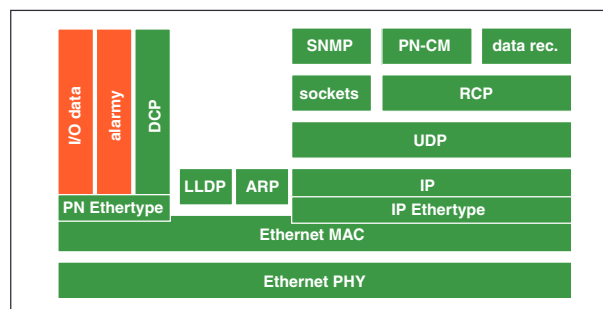
Na obr. 1 je také ilustrován formát adres, které se na této úrovni komunikace používají. Jde o tzv. adresy MAC, jež jsou jednoznačnou identifikací stanice, protože jsou celosvětově unikátní. Horní polovina adresy představuje

identifikaci výrobce, dolní polovina adresy je zařízení přiřazena výrobcem. Použití adres MAC je důsledkem toho, že veškerá komunikace probíhá na úrovni spojovací vrstvy a přenášená data jsou obsažena v ethernetovém rámci.

Podrobnější pohled na jednotlivé komunikační vrstvy poskytuje obr. 2, ze kterého je zřejmá jedna z velkých výhod Profinetu, a to současně využití síťové infrastruktury několika protokoly současně. To je možné díky skutečnosti, že všechny protokoly využívají stejnou spojovací vrstvu, tedy v popisovaném případě vrstvu Ethernet. Jinými slovy, veškerá data jsou v síti „zabalena“ do ethernetových rámců (úroveň spojovací vrstvy), které jsou prostřednictvím jednotlivých přepínačů předávány na základě cílové adresy od odesílatele k příjemci při současném zohlednění priority zpráv (rozlišení priorit RTC1 a NRT).



Obr. 1. Funkce síťového přepínače (switche)



Obr. 2. Vrstvový model komunikace Profinet

a činí komunikaci víceméně deterministickou. Je totiž třeba mít na paměti, že přepínač při příchodu dvou zpráv, které jsou určeny pro stejný výstupní port, musí jednu z nich pozdržet a druhé dát přednost. To, která zpráva bude pozdržena, může být dáno např. tím, která zpráva dorazí dřív nebo která zpráva má vyšší prioritu. Profinet využívá oba principy. Zprávy, které přenášejí provozní data, mají vyšší prioritu (tzv. real-time zprávy) a přepínač jejich předání na výstupní port upřednostní proti ostatním zprávám (např. zprávám, které přenášejí data TCP/IP). Pro posouzení

Pro úlohy, které vyžadují přísně deterministickou komunikaci, nabízí Profinet další typ komunikace, a to RTC3 (*real-time class 3*), označovanou také IRT (*isochronous real time*). Pro tyto zprávy je v rámci komunikačního cyklu vyhrazeno zvláštní pásmo, které typicky bývá 15 až 50 % z celkové délky cyklu a v němž není dovoleno posílat zprávy typu RTC1 ani NRT. Veškerá komunikace RTC3 je navíc dopředu naplánována, a proto není možné, aby se některá zpráva RTC3 na své cestě sítě od odesílatele k příjemci zdržela. Lze tedy s mikrosekundovou přesností pře-

dem spočítat, jak dlouho bude trvat doručení každé zprávy. Část komunikačního cyklu je pro RTC3 vyhrazena jako časový slot, a proto každý přepínač, který zprávy RTC3 přenáší, musí vědět, kdy vyhrazené pásmo začíná. Všechny přepínače v síti proto mají synchronizované hodiny. Rozdělení různých druhů komunikace v komunikačním cyklu ukazuje obr. 3.

Pro komunikaci RTC3 jsou tedy nutné speciální přepínače, které kromě funkcí podle IEEE 802.1D a IEEE 802.1Q navíc podporují synchronizaci a rozlišují část komunikačního cyklu, ve které lze přenášet pouze zprávy RTC3. Tato část je také označována jako „červený interval“ a zbývající část komunikačního cyklu, určená pro zprávy RTC1 a NRT přenášené ve standardním režimu přepínačů, je označována jako „zelený interval“ (obr. 3).

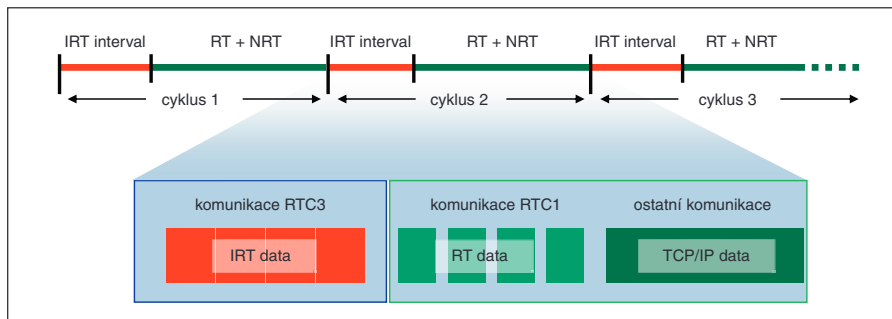
Výčet protokolů, které obsahuje obr. 2, není úplný, ale ty, které zde jsou zobrazeny, představují základ pro komunikaci Profinet a autor se na ně bude odkazovat v dalším textu. Protokoly označené oranžovou barvou jsou určeny pro komunikaci v reálném čase (RTC1 nebo RTC3 pro I/O data a RTC1 pro alarmy) a spolu s protokolem DCP jsou přímo nad vrstvou Ethernetu (pole Ethernetu v ethernetovém rámci označuje protokol Profinet). Další protokoly LLDP a ARP mají vlastní Ethernetu (v obr. 2 pro jednoduchost není naznačen) a jde o běžné protokoly známé ze světa informační a komunikační techniky. Protokol SNMP, také běžný v komunikační technice, využívá, jak je zřejmé z obr. 2, komunikaci UDP a IP. Blok označený PN-CM (*Profinet Context Management*) představuje sadu zpráv, které jsou využívány při navázání komunikace mezi stanicemi *PN IO Controller* a *PN IO Device*, jak bude uvedeno dále. Blok označený „data rec.“, *data records*, představuje zprávy, které jsou využívány pro čtení a zápis hodnot parametrů či jiných dat ze zařízení a budou rovněž zmíněny dále.

Zařízení v síti Profinet

Na rozdíl od komunikačních sítí typu Profibus, kde jsou zařízení rozdělena na nadřazená a podřazená (*master, slave*), jak to odpovídá řízení přístupu na sběrnici, na Profinetu jsou role zařízení rovnocenné. Přístup k síti totiž není třeba řídit, protože bezkolizní komunikace, ať už NRT, RTC1 nebo RTC3, je dána použitím přepínačů. Standard Profinet definuje tři role zařízení, a to *Profinet IO Device*, *Profinet IO Controller* a *Profinet Supervisor* (dále označovány jako PN IO-C, PN IO-D a PN S). Základní komunikační vazby mezi nimi naznačuje obr. 4. PN IO-C je typicky řídicí počítač nebo PLC, jehož hlavním úkolem je zajišťovat cyklickou výměnu provozních dat (vstupů a výstupů). Aby tato výměna dat mohla začít, musí PN IO-C nejdříve vytvořit aplikační relaci (AR), která za-

střešuje veškerou další komunikaci mezi ním a periferií, což je PN IO-D. Do této komunikace dále spadá přenos alarmů (acyklická komunikace RTC1) a přenos parametrů (tzv. datové záznamy – *data records*), které jsou přenášeny rovněž acyklicky, ale s využitím protokolu RPC (resp. UDP a IP; viz obr. 2).

nahrazena v dalším komunikačním cyklu. Počet tolerovaných ztracených zpráv je parametrem při vytváření AR a typicky má hodnotu tři. Stav poskytovatele a konzumenta je součástí přenášených dat, a tak je každý účastník komunikační relace v každém intervalu informován o stavu svého protějšku.



Obr. 3. Struktura komunikačního cyklu

Bez vytvoření aplikační relace není možné, aby začala nějaká další komunikace. Proto je vytvoření aplikační relace nezbytné pro přenos dat jak mezi PN IO-C a PN IO-D, tak také mezi PN S a PN IO-D. PN S je zařízení, které jednak uvádí síť do provozu (přřazení jmen stanicím), jednak zapisuje parametry, popř. zjišťuje diagnostické informace; jde tedy o konfigurační a diagnostické zařízení.

Přenos dat na Profinetu je tedy cyklický a acyklický. Cyklická neboli provozní (procesní) data jsou přenášena v předem nastavených intervalech, kterým se říká interval aktualizace dat. Tím, že jsou zařízení PN IO-C i PN IO-D rovnocenná, je perioda aktualizace dat postačující údaj pro to, aby zařízení mohla cyklicky posílat svá data. To probíhá v rámci komunikační relace (CR – *communication relation*), která je součástí vytvořené aplikační relace. Každá komunikační relace má poskytovatele dat (odesílatel) a kon-

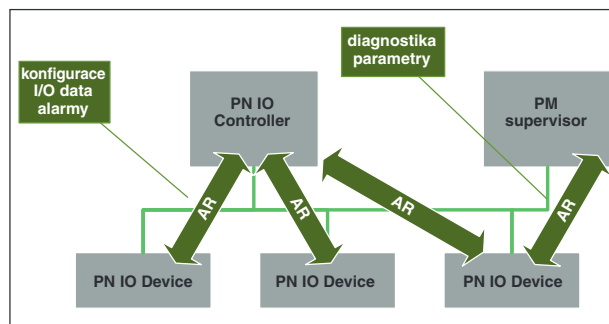
Acyklická data představují alarmy a datové záznamy a na rozdíl od cyklicky přenášených zpráv jsou tyto zprávy potvrzovány explicitním potvrzením.

Identifikace zařízení v síti

Jednoznačnou identifikací zařízení na Ethernetu je adresa MAC, která je pro každé zařízení celosvětově unikátní. Profinet však zavádí koncept tzv. jmen zařízení (*Name of Station*), která jsou doplňkem k adrese MAC a jejichž použití s sebou nese mnoho výhod, mezi něž patří:

- jméno zařízení je snadno zapamatovatelné,
- podle jména zařízení je typicky možné zařízení lokalizovat,
- při výměně poškozeného zařízení za nové není třeba měnit projekt s konfigurací sítě.

Musí tedy existovat jednoznačné přiřazení mezi adresou MAC a jménem pro každé zařízení. Při uvádění síť Profinet do provozu přiděluje jména zařízení PN Supervisor na základě adresy MAC prostřednictvím protokolu DCP (*Discovery Configuration Protocol*), který, jak ukazuje obr. 2, je přímo nad vrstvou Ethernetu. Sekvenci identifikace zařízení v síti, která předchází každému navazování komunikace mezi PN IO-C a PN IO-D, ukazuje obr. 5. Po připojení se PN



Obr. 4. Zařízení v síti Profinet

zumenta dat (příjemce). Komunikační relace je vždy jednosměrná, je tedy vždy nutné vytvořit v rámci jedné aplikační relace dvě komunikační relace, tam a zpět. Příjemců může být několik a v tom případě jde o tzv. *multicast* komunikační relaci. Vzhledem k tomu, že data jsou posílána cyklicky, není nutné, aby příjemce posílal explicitní potvrzovací zprávu, protože při ztrátě zprávy budou data

IO-C dotazuje na přítomnost zařízení v síti odesláním dotazu DCP.Ident, který je odeslán jako multicast ethernetový rámec se skupinovou adresou Profinet. Každé zařízení Profinet jej tedy přijme a podle jména stanice, které je přenášeno v datech dotazu, se rozhodne, zda má na dotaz reagovat. Na obr. 5 PN IO-D na první dva dotazy nereaguje, protože zatím žádné jméno nemá. Jméno získá

až poté, co mu je přiřadí PN Supervisor prostřednictvím zprávy DCP.Set, a tak může zareagovat na následující dotaz od PN IO-C. V situaci na obrázku se rovněž předpokládá, že PN IO-D nemá žádnou IP adresu, což sdělí v odpovědi na DCP.Ident. PN IO-C následně prostřednictvím DCP.Set přiřadí zařízení IP adresu na základě nastavené konfigurace projektu. Následující dotaz ARP odesílá PN IO-C, aby se přesvědčil o tom, zda v síti nejsou dvě zařízení s duplicitní IP adresou.

Poté, co má zařízení přidělenou IP adresu, může PN IO-C vytvořit aplikační relaci a následně začít přenos cyklických dat.

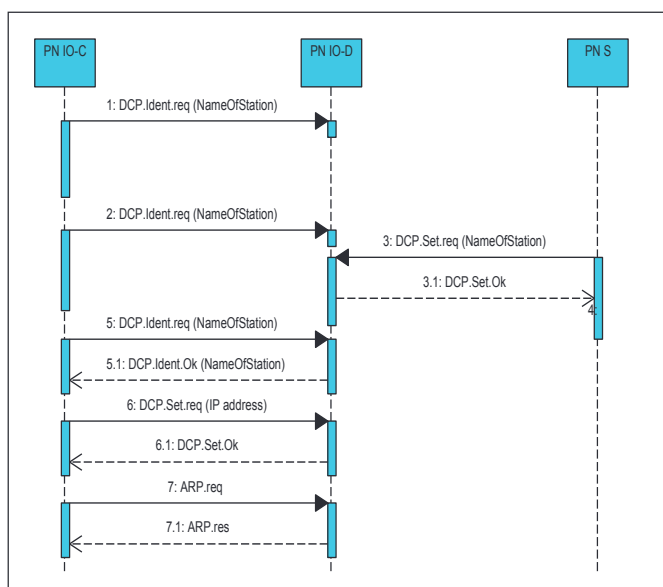
Topologie sítě a její detekce

Díky použití přepínačů lze ve Profinetu navrhnout topologii sítě velmi flexibilně a ve většině případů se v praxi objevují kombinace různých základních topologií. Hvězda, tradiční zapojení z kancelářského prostředí, využívá víceportový přepínač, aby se do jednoho místa připojilo několik zařízení. Výhodou hvězdy je možnost nechat na přepínači volné porty, které lze následně využít k připojení dalších zařízení podle potřeby. Naopak v průmyslovém prostředí je typické zapojení zařízení za sebou, k čemuž je využívána liniová topologie. Je třeba si uvědomit, že na rozdíl od sběrnice topologie je liniová topologie vždy propojením dvou zařízení prostřednictvím portů přepínače. Každé

zařízení tedy musí obsahovat alespoň dvouportový přepínač, aby jej bylo možné zařadit v liniové topologii doprostřed. Kombinací hvězdy a liniové topologie vzniká strom, který kombinuje vlastnosti obou. Důležitou topologií je kruh, který lze využít pro zajištění redundance a dostupnosti komunikace: je-li jedna z cest přerušena, může komunikace probíhat druhou redundantní cestou. Na Profinetu se používá protokol MRP (*Media Redundancy Protocol*), který provádí rekonfiguraci kruhu, jestliže byl přerušen spoj mezi dvěma stanicemi nebo došlo k výpadku stanice. Rekonfigurace kruhu v tomto případě proběhne do 200 ms. Je-li třeba beznárazově přepnutí cest v kruhu, tzn. aby nenastalo žádné, byť krátkodobé přerušení komunikace, lze využít redundanci MRPD (*Media Redundancy for Planned Duplication*).

Profinet rovněž stanovuje způsob, jak lze topologii detekovat. Mezi protokoly, kte-

ré ukazuje obr. 2, je protokol LLDP (*Link Layer Discovery Protocol*), definován jako IEEE 802.1AB, a protokol SNMP (*Simple Network Management Protocol*). LLDP se používá jako základní mechanismus pro detekci sousedních stanic, který umožní zjistit, jaké zařízení a na jakém portu je připojeno jako partner. Tato informace je uložena v datových záznamech zařízení a dostupná prostřednictvím komunikace pro přenos datových záznamů Profinetu (*data records*) nebo je uschována ve struktuře označované jako MIB (*Management Information Base*). K získávání informací ze struktury MIB se potom používá právě protokol SNMP. V souvislosti s topologií se používají struktury LLDP-MIB včetně rozšíření PNIO a MIB-II. Z umístění obou zmíněných protokolů v obr. 2 lze také vyvodit, že LLDP pracuje na úrovni spojovací vrstvy, zatímco protokol SNMP je na úrovni aplikační vrstvy nad transportní vrstvou UDP, tzn. že jsou k adresaci využívány IP adresy.



Obr. 5. Sekvence zpráv pro identifikaci zařízení v síti

Je tedy možné do sítě umístit zařízení, které bude skenovat topologii čtením příslušných datových struktur MIB z každého zařízení a ukládat informace do své paměti. Předpokladem je, aby každé skenované zařízení mělo IP adresu, což na Profinetu platí pro všechna zařízení PN IO-C i PN IO-D. Otázkou zůstávají síťové komponenty, tj. přepínače. Z pohledu Profinetu lze totiž použít úplně základní přepínače, které nepodporují žádné rozšířené funkce, jako je např. protokol LLDP. Takové přepínače ale není možné v topologii detekovat, a proto skenováním topologie nelze vytvořit skutečný obraz toho, jak je síť zapojena. Lze tudíž jednoznačně doporučit, aby všechny síťové komponenty detekci topologie podporovaly.

Souhrn vlastností, které mají zařízení a síťové komponenty podporovat, je vyjádřen tzv. třídami konformity (*Conformance Classes*). Základní třída je CC-A, podle níž musí

každé zařízení podporovat protokol LLDP. Podle třídy CC-B musí zařízení navíc podporovat protokol SNMP, a tak umožnit čtení informací o svých sousedech, které jsou uloženy ve strukturách MIB. V CC-B je také požadavek na podporu protokolu MRP. Poslední třída, CC-C, obsahuje požadavek na podporu MRPD, přičemž tento typ redundance vyžaduje komunikaci IRT, aby bylo možné zprávy zdvojit a přenášet je oběma směry v kruhu.

Diagnostika v síti Profinet

Profinet definuje diagnostický model, kde se PN IO-C prostřednictvím přenosu alarmů dozví o události, která nastala na straně PN IO-D. Veškeré události jsou vztaženy k modulům v zařízení, a tak lze snadno a rychle lokalizovat místo, kde k události došlo. Jestliže tedy např. nastane zkrat na výstupním modulu, je tato informace přenesena do PN IO-C alarmovou zprávou včetně čísla a pozice modulu v zařízení, kde ke zkratu došlo. Stejný mechanismus platí pro události typu vytažení nebo zasunutí modulu nebo také např. pro události typu změna topologie.

Informace o změně topologie může být velmi užitečná, protože se díky tomu zjistí, že někdo se sítí manipuloval, připojil nové zařízení nebo existující zařízení zapojil na jiné místo. Je však nutné, aby topologie byla předem zkonfigurována, jinými slovy je nutné, aby se topologie stala součástí projektu PN IO-C, který tuto informaci v rámci vytvoření aplikační relace přeneše do každého zařízení PN IO-D.

Konfigurace topologie také usnadňuje výměnu vadného zařízení za nové. Každé zařízení před prvním navázáním komunikace musí dostat jméno stanice. Některá zařízení obsahují paměťovou kartu, na které je jméno stanice uloženo, takže při výměně zařízení dostane nové zařízení paměťovou kartu z toho původního, a tím získá správné jméno stanice. Má-li ale síť nakonfigurována topologii a zařízení odpovídá CC-B, získá jméno stanice pouze na základě svého umístění v topologii a výměna paměťové karty již není nutná. Jestliže je tedy nové zařízení umístěno v topologii na přesně stejné místo jako zařízení staré, naváže PN IO-C s novým zařízením komunikaci automaticky.

Velkou výhodou sítě postavené na přepínačích je kromě současně probíhající komunikace na několika linkách také snadná lokalizace chyb na úrovni fyzické vrstvy, které se projevují jako chybný kontrolní kód CRC v přenášeném rámci. Ty mohou být způsobeny odrazy na kabelu nebo přítomností zdroje vnějšího rušení, často jde o kombinaci obou. Ve sběrnicových systémech typu Profibus lze podobné chyby lokalizovat velmi obtížně, protože např. externí zdroj rušení, který se objevuje náhodně, může poškozovat komunikaci pokaždé mezi jinými zařízeními, a tím bude i k vý-

padkům zařízení docházet náhodně. V případě Profinetu ale chyby CRC detekuje každý přepínač pro každý příchozí port, a protože je vždy realizováno spojení mezi dvěma porty, jde vždy o chybu způsobenou na jednom konkrétním spoji. Sledováním statistik portů lze tedy sledovat zhoršení komunikace na jednotlivých linkách, a tím předvídat případné výpadky v komunikaci.

Závěr

Profinet je komplexní komunikační systém, který kombinuje komunikaci v reálném čase s komunikací běžnou ve světě informačních systémů. Na světě je v současné době instalováno přibližně šest milionů zařízení Profinet a tento počet se každým rokem zvětšuje zhruba o 1 až 1,5 milionu. Tomu odpovídá

narůstající podpora výrobců čipů, kteří nabízejí jednočipová řešení přímo s integrovaným protokolem Profinet, a také podpora významných firem z oboru automatizace; stále více jich integruje Profinet do svých řídicích systémů a periferií.

Pavel Burget, FEL ČVUT v Praze, Energoklastr, Profibus CZ

Průmyslové ethernetové sítě optimalizované pro propojování automatizovaných systémů

K průmyslové revoluci došlo proto, že si výrobci uvědomili, že spolupracující řemeslníci pracují efektivněji, než když každý z nich pracuje samostatně. Toto průlomové zjištění je základem moderní průmyslové výroby. V současné době si provozovatelé průmyslových automatizovaných systémů uvědomují, že integrací správy dat, řízení procesů, zabezpečení, videodohledu a dalších automatizačních úloh je možné dosáhnout vyšší efektivity, bezpečnosti a kvality. Spolupráce původně samostatných, vzájemně nekomunikujících automatizačních systémů je podstatou nové průmyslové revoluce.

Sjednocoování podsystémů je základem nové revoluce v průmyslové automatizaci. Podstatou je připojení automatizačních podsystémů k jednotné průmyslové ethernetové infrastruktuře místo použití několika oddělených průmyslových sběrnic. Komplexní nabídka firmy Moxa pro průmyslový Ethernet je klíčovým stavebním kamenem pro propojování podsystémů v průmyslu a zajišťuje jejich bezproblémovou konektivitu a spolupráci. Místo dělení pozornosti mezi několik komunikačních systémů se mohou provozovatelé průmyslové automatizace zaměřit na jedno univerzální komunikační rozhraní. Taková konvergence umožňuje různorodým podsystémům sdílet data a optimálně využívat svůj výkon.

Podívejme se na dvě případové studie detailněji demonstrující, jak systémy s produkty Moxa plní požadavky na šířku pásma, bezpečnost a správu, což přináší schopnost plně využívat možnosti a provozní výhody propojování podsystémů v průmyslové automatizaci.

Jednotný systém SCADA a videodohledu

Při přepravě ropy a plynu jsou dálková potrubí monitorována s použitím dvou systémů: real-time I/O systémů typicky řízených prostřednictvím sys-

témů SCADA a kamerových systémů typicky spravovaných prostřednictvím odděleného systému CCTV. Při řízení provozu potrubního systému není prostor pro chyby a při reakci na kritické události, které indikují alarmy v systému SCADA, se počítá s každou sekundou. Integrace systémů SCADA a videodohledu usnadňuje operátorům propojení události v systému SCADA s příslušným videozáznamem a výrazně zvyšuje jejich informovanost o aktuální situaci na odlehklém úseku potrubí (obr. 1).

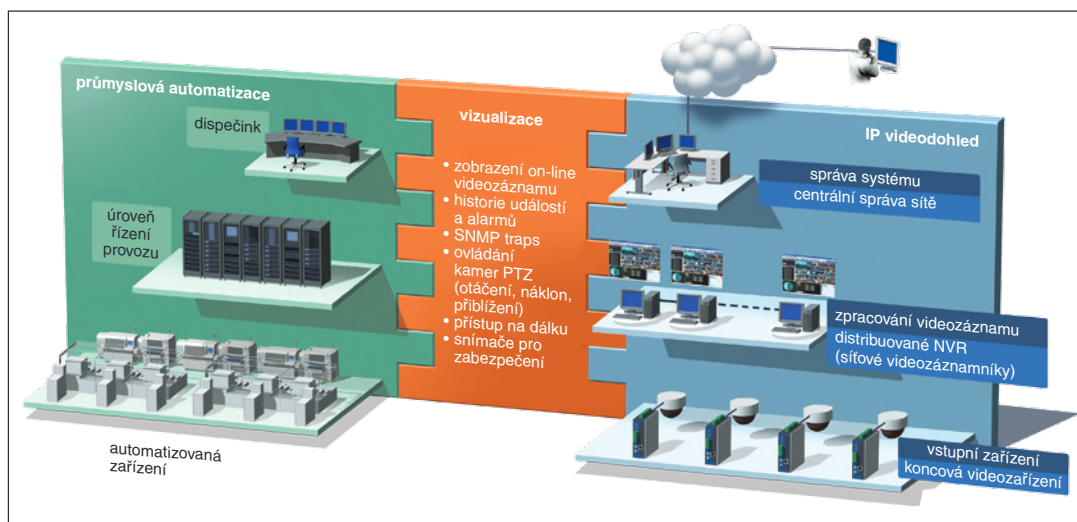
Výzvy

Sítí integrující funkce systému SCADA a videodohledu musí být dostatečně robustní,

aby obsloužila dálkový ropovod v náročných venkovních podmínkách. Samotná integrace systému musí být natolik jednoduchá, aby nevytvářela víc úkolů, než sama řeší. Oba systémy musí být integrované do takové míry, že je provozovatelé mohou používat společně bez toho, aby si to uvědomovali, a okamžitě reagovat na události v systému SCADA bez plýtvání časem na hledání příslušného videozáznamu.

Řešení

Produkty Moxa jsou pro řešení integrace systému SCADA a dohledového systému propojených robustní ethernetovou infrastrukturou vynikající. Hardwarové komponenty Moxa jsou robustní a reálně testované ve venkovním prostředí i v nejnáročnějších podmínkách. Softwarové nástroje pro vizuální dohled a softwarové komponenty OPC od firmy Moxa usnadňují integraci videodohledu do systému SCADA. Díky tomu může být přímo v obrazovce systému SCADA integrováno okno, které při příchodu alarmo-



Obr. 1. Propojení systému SCADA a videodohledu