SCADA QNX 2012
SYNCHRONIZACE A MĚŘENÍ ČASU

V pracovní skupině složené z pracovníků FIT VUT v Brně O.Ryšavého (16h/m) a J. Pacnera (50h/m) bylo v roce 2012 rozpracováno téma měření času ve SCADA systémech. Toto téma se vzhledem ke kapacitě řešitelů a rozsahu potřebných prací bude řešit i v první polovině roku 2013. Výsledkem bude analýza dosažitelné a potřebné přesnosti časové informace v typických SCADA aplikacích.

Popis problému

V rámci tématu je sestaveno testovací prostředí, ve kterém se vyhodnocují různé metody pro synchronizaci času za účelem stanovení maximální dosažitelné přesnosti hodin v distribuovaném SCADA systému založeném na operačním systému QNX. Dále je pak provedeno měření parametrů komunikace pro různé technologie a podmínky. V rámci projektu bude nutná portace protokolu PTP do prostředí OS QNX.

Cíl řešení

Vyhodnocení požadavků na RT vlastnosti komuniukace a synchronizaci času v SCADA QNX.

Plánované výstupy:

- Stanovit dosažitelnou přesnost pro získávání a přiřazování časových údajů k zaznamenávaným datům za použití různých technik synchronizace času.
- Dále pak vytvoření demonstračních úloh, které budou ukazovat, jak lze časové údaje z různých zdrojů používat v systémech QNX.
- Vytvoření návrhu komunikační architektury a definice jednotlivých klíčových komponent, například server, PTPD switch, ...

Postup řešení:

1. Seznámit se detailně se systémem QNX OS s ohledem na dostupné prostředky pro synchronizaci času v distribuovaných systémech (NTP, PTP, GPS). Termín 08/2012.
2. Vytvořit testovací a měřící prostředí pro vyhodnocení přesnosti pro různé metody synchronizace času. Implementace/portace PTPd v QNX. Termín 12/2012.
3. Provést experimenty s různými vybranými metodami synchronizace času. Termín 02/2013.
4. Naměřené výsledky vyhodnoit a diskutovat jejich význam z pohledu prostředí řídících systémů. Termín 04/2013.
5. Vytvořit demonstrační aplikace pro použití různých metod synchronizace. Termín 06/2013.

Studijní literatura

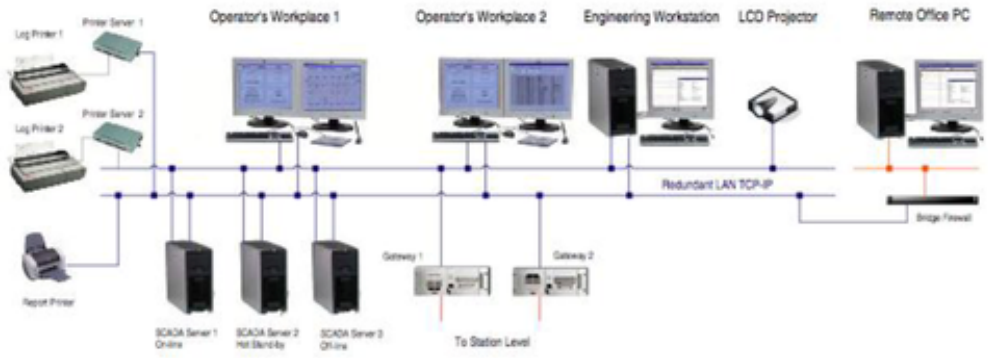
- F. Zezulka and O. Hyncica, "Synchronizace v distribuovaných řídicích systémech: Precision Time Protocol podle IEEE 1588," AUTOMA, vol. 2, pp. 17-19, 2010.

- V. Smotlacha, "Time Issues in One-way Delay Measurement," Czech Technical University in Prague, 2005.

- V. Igure, S. Laughter, and R. Williams, "Security issues in SCADA networks," Computers & Security, vol. 25, no. 7, pp. 498-506, Oct. 2006.

Úvod

Architektura SCADA systémů je vzhledem k povaze těchto systémů nutně distribuovaná. Jednotlivé uzly spolu často komunikují různými protokoly. V současné době se stále více používá pro přenosy koperátorské stanici klasické TCP/IP sítě postavené nad Ethernetem. Výhodou je jednoduchá a levná instalace, nevýhodou může být vzhledem k povaze této sítě nepředvídatelné zpoždění a rozptyl (jitter) přenášených dat.



V rámci SCADA systému je nutné, aby každá událost měla přiřazeno časové razítko označující okamžik jejího výskytu. S tím v distribuovaném systému souvisí nutnost synchronizovat hodiny reálného času všech relevantních uzlů. Pro dosažení přesnosti časových razítek, které jsou událostem v distribuovaném řídícím systému přiřazovány je nutné, aby jednotlivá zařízení pracovala se synchronizovaným fyzickým časem s dostatečnou přesností. Běžně používané jsou metody synchronizace založené na použití NTP nebo PTP protokolech a synchronizace vzhledem k časovým informacím nesených GPS signálem.

Pro určení vhodné metody synchronizace času vzhledem k ceně a technické náročnosti implementace je potřebné určit charakteristiku komunikační sítě a požadavků aplikace. Z implementačního hlediska je nejsnazší nasazení protokolu NTP, který však z uvedených metod poskytuje nejmenší přesnost. Tato přesnost je však dostatečná pro některé typy SCADA aplikací, které monitorují pomalé procesy, například XX.

Tato práce se zabývá měřením:

- vlastností různých datových sítí, zejména zpoždění přenosu a rozptyl zpoždění,

- přesnosti vybraných synchronizačních metod fyzického času,

a specifikací tříd SCADA aplikací vzhledem k požadavku na přesnost časových razítek a RT vlastnosti komunikace.

Synchronizace fyzického času

Existuje několik metod pro synchronizaci hodin reálného času v počítačových sítích. Zde uvedeme a v rpojektu budeme uvažovat pouze tři nejpoužívanější. Seřazeny dle míry přesnosti a složitosti se jedná o protokol NTP, PTP a metodu přímé synchronizace vzhledem k informacím v GPS signálů.

NTP

Je protokol pro synchronizaci hodin reálného času na pracovních stanicích v IP sítích. Pracuje na principu Marzullova algoritmu. Jeho přesnost závisí na vzdálenosti zdroje přesného času a uzlu požadující synchronizaci. Pro synchronizaci v Internetu se dosahuje přesnosti v řádu desítek milisekund. V lokálních sítích je možné přiblížit se s přesností na jednotky milisekund. Použitý algoritmus umožnuje klientovi určit round-trip delay (RTD) a offset vzhledem ke zdroji přesného času pomocí jednoduchého výpočtu ze 4 časových údajů připojených ke dvěm NTP zprávám. Klient provádí sérii výpočtů a použije offset, který patří k měření ve kterém je nejmenší RTD. Vzhledem ke způsobu výpočtu offsetu, přesnost synchronizace závisí na symetričnosti přenososvé cesty. Systematická odchylka je rovna jedné polovině rozdílu mezi časem přenosu od klienta ke serveru a obráceně. Impementace tohoto protokolu je dostupná ve většině operačních systémů, včetně QNX a nevyžaduje žádné přídavné HW prostředky.

PTP

Je protokol pro snychronizaci hodin reálného času, který vzhledem ke své přesnosti je vhodný pro RT řídící a měřící distribuované aplikace. Tento protokol je definován standardem IEEE1588-2008. Jeho návrh byl motivován požadavkem doplnit existující metody synchronizace, založené na NTP, který je méně přesný a GPS, který je velmi přesný, ale vyžaduje použití GPS přijímače a hlavně možnost přijímat GPS signál.

Architektura PTP systému je hierarchická typu master-slave. Oblastí synchronizace je síťový segment, neboť PTP logicky pracuje na linkové vrstvě. Grandmaster je uzel, jehož hodiny jsou považovány za přesné v rámci segmentu a ke kterému jsou ostaní hodiny synchronizovány. Tato synchronizace je šířena prostřednictvím relay hodiny, zvaných boundary clocks.

V cílovém operačním systému QNX tento protokol není standardně implementován. Existuje komerční implementace protokolu od společnosti Real-Time Systems GmbH. K dispozici je open source implementace PTPd[1] , která je v rámci projektu portována do prostředí QNX.

GPS

Metoda synchronizace času pomocí GPS přijímače je založena na přijímání GPS zpráv, které obsahují časová razítka s přesností v nanosekundách. GPS přijímač dosahuje vysoké přesnosti svých hodin pomocí periodické synchronizace těchto hodin vzhledem k přijímaných časovým údajům pomocí Phase Locked Loops (PPL) a Frequency Locked Loops (FLL).

Vzhledem k dosažené přesnosti časové informace v rámci GPS přijímače se problémeme stává přenos této informace do PC. Levné GPS přijímače používají RS232 nebo USB připojení, čímž vzniká vysoká latence při přenosu této informace a tudíž ztráta přesnosti. Vyšší přesnosti se doahuje použitím GPS modulů s rozhraním PCI nebo PCIex.[2]

---

[1] http://ptpd.sourceforge.net

[2] http://www.lammertbies.nl/comm/info/GPS-time.html

Měření doby přenosu

Důležitou charakteristikou komunikačních sítí vzhledem k Real-time požadavkům je zejména zpoždění přenosu a rozptyl vzhledem aktuální zátěži na síti. V této práci uvažujeme paketově přepínané sítě, které na rozdíl od TDMA, FDMA či podobných technik negarantují dobu přenosu dat. Určení aktuálního zpoždění a rozptylu závisí na aktuální zátěži sítě.

- Packet Transit Delay - označuje zpoždění paketu při přenosu v síti, vlivem zpoždění přenosu datového signálu, zpoždění zpracování dat při přijetí a odeslání v aktivních prvcích a době, kdy je paket uložen ve vyrovnávacích pamětech.

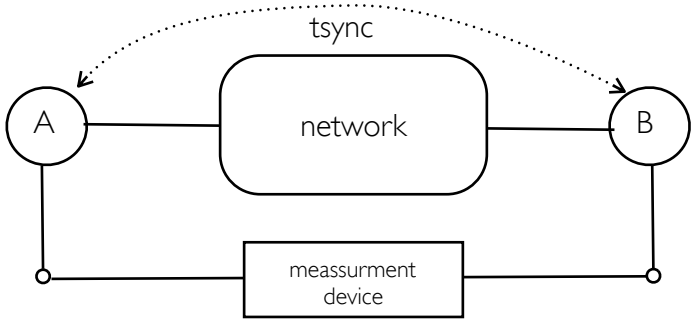
- Packet Delay Variation - označuje rozdíl PDT jednotlivých paketů. Kolísání PDT má negativní vliv nejen na RT aplikace, ale i na samotné metody synchronizace času, realizované protokoly NTP a PTP.

- Network Load - zátěž sítě má přímí vliv na PDT a PDV. Měření zátěže a odpovídajích hodnot PDT a PDV nám tak umožňuje definovat funkční závislost pro kontrétní síť a stanovit tak její časově-přenosovou charakteristiku.

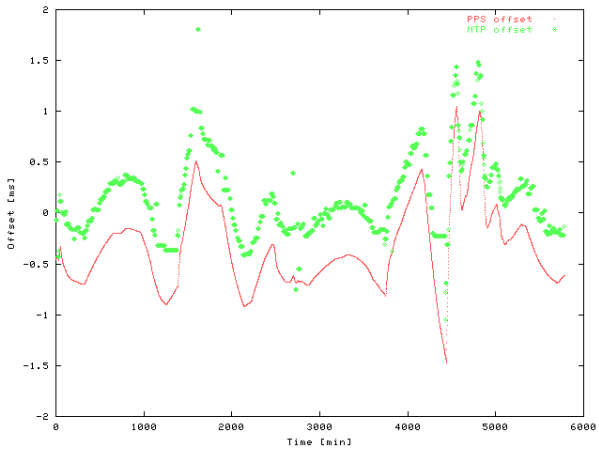
V rámci práce se tedy zaměřujeme na měření PDT, PDV a NL pro různé druhy a topologie paketových sítí. Cílem je získat parametrizované funkce PDT a PDV na NL. Uvažujeme různé síťové topologie (lokalní hvězda, sdílená sběrnice, komplexnější architektury) a použité přenososvé technologie (Ethernet, DSL, modem).

Měření přesnosti synchronizace

V rámci tohoto experimentu bude měřena přesnost synchronizace fyzických hodin jednotlivých metod. Základní prostředí se skládá ze dvou stanic. Jedna stanice je master a druhá je slave. Obě stanice vystavují měřitelný výstup na kterém je připojeno měřicí zařízení, které sleduje a měří rozdíl vystavených hran.



Výsledkem měření bude graf, který bude ukazovat odchylku synchronizovaných hodin od zdroje v průběhu času. Příklad naměřených hodnot v rámci projektu CESNET[3], kde byla měřena NTP synchronizace je na následujícím obrázku.Z obrázku je patrné, že s použitím NTP protokolu je možné dosáhnout přesnosti lepší než 1ms. V rámci našeho měření uvažujeme pouze laboratorní podmínky a uvedená síť se bude skládat ze zařízení dostupných v laboratoři.Uloha bude spočívat v ověření přesnosti pro protokol NTP a změření přesnosti odvchylky pro protokol PTP.



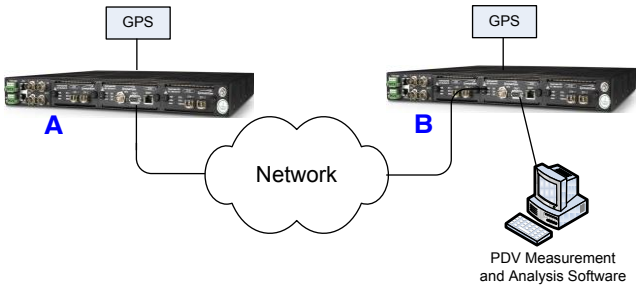
[3] roject/qosip/publications/2003/ntp-meas/result1.html

Měřící a testovací prostředí

Připravili jsme prostředí pro měření několika vlastností. Jedná se zejména o charakteristiku datové sítě, která je vyjádřena jako PDT, PDV a NL. Toto měření má za cíl získat představu o chování různých dnes běžně dostupných síťových technologií a vytvořit jejich model, který by mohl být použit při návrhu komunikační architektury SCADA aplikací. Výsledkem této úlohy jsou naměřené hodnoty a vytvořený simulační model.

Měření PTD a PDV v závislosti na NL

Tento experiment spočívá v naměření PDT mezi uzly A a B pro zůzné síťové topologie. Odesílaná data jsou opatřena časovými razítky získanými ze zdroje přesného času.



Výsledkem jsou naměřené hodnoty TA,TB a vypočten jejich rozdíl, který odpovídá PTD.

Network #	Load (%)	TA	TB	PTD

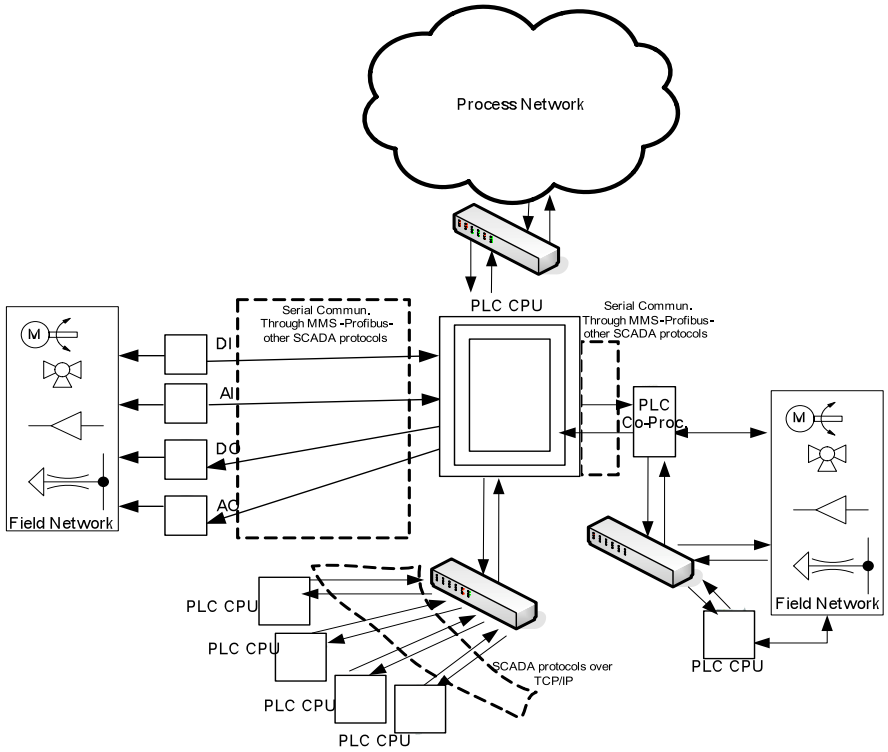
Pakcet Delay Variation je hodnota vypočtena z naměrených PDT. Vzhledem k charakteru získaných hodnot, je lepší než výpočet okamžitých hodnot počítat standardní odchylku, nebo průměrnou odchylku v čase, popřípadě využít metody TDEV pro určení časové odchylky, která lépe vypovídá o průběhů rozptylu paketů v čase. Použitá definice TDEV je následující:

$$TDEV(\tau) = \sqrt{\frac{1}{6}\left\langle \left[\frac{1}{n}\sum_{i=1}^{n} x_{i+2n} - 2\frac{1}{n}\sum_{i=1}^{n} x_{i+n} + \frac{1}{n}\sum_{i=1}^{n} x_i \right]^2 \right\rangle}$$

Měření je realizováno vždy mezi dvěma stanicemi, nicméně uvažujeme různé přenosové technologie a zařízení na cestě. Z přenosových technologií uvažujeme bežný Ethernet, Wireless, xDSL a modem. K dispozici máme různá zařízení, které je možné do cesty zapojit, například směrovač (Router), přepínač (Switch), Hub či modem. Dále pak jsou uvažovány různé kombinace těchto technologií, kdy je sledován a vyhodnocen vliv "změny technologie přenosu" na komunikační cestě. Dalším parametrem je zátěž sítě 0%-80%, v krocích po 20%. Pro generování provozu použijeme zařízení Spirent TestCenter. Toto zařízení nám umožňuje generovat libovolný provoz, který odpovídá reálnému provozu na síti. Cílem je získat dostatek informací z takto naměřených a doplněných výsledků, aby bylo možné vytvořit simulační model v prostředí diskrétního simulátoru OMNeT++.

Třídy SCADA aplikací

V rámci výsledku projektu bude také provedena klasifikace SCADA systémů do tříd vzhedem k jejich požadavkům na přesnost časových informací. Toto bude provedeno metodou rešerše dostupné publikace a konzultace s odborníky z oblasti. SCADA systémy jsou nasazovány v různých aplikačních doménách. Charakter těchto domén většinou společně s architekturou určuje požadavky na míru synchronizace a použití časových údajů. V projektu uvažujeme síťové SCADA systémy, tedy, systémy, kde je použita netriviální síťová infrastruktura pro přenos dat.



Typická architektura síťového SCADA systému

Aplikace

SCADA systémy jsou nasazoványv různých oblastech. Jedná se zejména o řízení a monitorování průmyslových procesů, přepravě, bezpečnostních systémů a systémů pro kontrolů experminetů.

Komunikační systémy a protokoly

Scada sítě používají různé přenosové technologie, například, přepínané telefonní sítě, pronajaté linky, privátní sítě (LAN/RS-485), Internet a VPN, Wireless sítě - WIFI, GSM. Ve SCADA sítích je možné se setkat s různými komunikačními protokoly, například, MODBUS, DNP, Fieldbus, CAN, Profibus, DirectNet, TCP/IP a Ethernet.

Klasifikace

Cílem klasifikace je nalézt třídy SCADA systémů na základě jejich význačných vlastností vzhledem k použití časových údajů. Tato klasifikace je ortogonální k bezpočnostní klasifikaci SCADA systémů a tvoří s ní nefuknční charakteristiku SCADA systémů. Vycházíme z obecné klasifikace RT systémů, kdy systémy dělíme podle požadavků na splnění deadline na HARD, SOFT a FIRM. Z pohledu kvantitativního, tedy jak rychlý systém musí být, jsou definovany kategorie ULTRAFAST, FAST a SLOW. Po experimentech budou určeny jednotlivé hranice pro tyto kategorie a definovány prostředky, které je možné použít pro dosažení uvedeného kritéria.

Výstupy

Následující výstupy budou dokončeny k 30.6.2012. V současné době je rozpracován port PTP a připravena měřící laboratoř.

- [SOFTWARE] Implementace/portace PTP pro QNX OS. Demo programy a konfigurace NTP, PTP pro použití ve SCADA QNX.
- [PUBLIKACE] Technická zpráva obsahující detailní informace o postupech a výsledcích experimentů.
- [PUBLIKACE] Příspěvek na konferenci prezentující výsedky projektu.