Ing. Jan VIDIM
Domat Control System s.r.o.

Síťové komunikace u systémů VVK – přínosy a rizika

Net Communications at Heating, Ventilating, Instalation Systems – Contributions and Hazards

Recenzent
doc. Ing. Jiří Bašta, Ph.D.

Příspěvek popisuje komunikační možnosti současných regulačních komponent, dostupných na trhu a propojení sítí Ethernet. Ukazuje, jakými způsoby se dá řešit vazba technologické sítě na rozvody v budově a na několika příkladech je ilustruje. Jsou popsány přínosy a rizika u jednotlivých modelů a to jak z hlediska uživatele, tak realizačních a servisních firem, především pokud jde o bezpečnost, funkce systému a investiční a provozní náklady. V příspěvku nechybí ani zkušenosti z realizovaných akcí.
Klíčová slova: řízení, komunikace, sítě

The article describes the communication possibilities of the present regulation components accessible on the market and Ethernet nets connection. It indicates what kinds of ways enable to solve the technology net accouplement to distribution frames in the building and it illustrates these ways on some examples. The contributions and hazards of individual models are described namely both from the point of view of the user and from the point of view of implementation and service firms, first of all as far as concerns safety, system function and investment and operation costs. Not even experience from implemented actions is missing in the article.
***Key words:** control, communication, nets*

Přenos dat po sítích typu Ethernet se začal u komponent a systémů pro měření a regulaci objevovat již před více než deseti lety. Teprve s prudkým rozvojem síťových infrastruktur a s tím spojeným poklesem cen začala být síťová komunikace masivněji využívána. Dnes již pozorujeme, jak rychle vytlačuje především u dálkových přístupů vytáčenou telefonní linku. Pro místní komunikaci je zase velkou výhodou vysoká propustnost sítě a široce rozšířené znalosti pro její instalaci. Po roce 2000 začaly sítě konvergovat: vzniká společná platforma pro přenos hlasu, obrazu a dat při využití standardních protokolů, což dále snižuje investiční i provozní náklady. Co tedy výrobci systémů měření a regulace nabízejí a na co si musíme při výběru systému dát pozor?

DODAVATEL TECHNOLOGIE

Především je třeba porozumět řeči katalogových listů a letáků. V nich obvykle stojí, že příslušné rozhraní komunikuje po rozhraní Ethernet protokolem TCP/IP, což ovšem znamená pouze definici linkové, resp. přenosové vrstvy a nikoli popis vrstvy aplikační, tedy např. zda na „druhém konci" má být webový prohlížeč nebo klient v ceně tisíců euro. Dodavatel systému by měl vždy nabízet celý řetězec, případně u otevřených systémů přesně definovat, jaké rozhraní na druhé straně očekává.

To platí hlavně v případech, kdy dodavatel technologie (VZT, kotle, ...) zastřešuje dodávku řídicího systému, jenž pak má být integrován do řídicího systému budovy (building management system, BMS). V lepších případech je do projektu zapojen systémový integrátor, který tyto vazby koordinuje a již ve fázi nabídek vyloučí řešení, která by nebyla úspěšně realizovatelná. Jinak dochází k situacím, kdy technologové přenesou neúplné zadání investora na své subdodavatele, za jejichž řešení posléze nesou zodpovědnost. Subdodávka řídicího systému pochopitelně obsahuje pouze věci striktně požadované v zadání, aby byla cenově konkurenceschopná, ovšem při koordinačních jednáních se přijde například na to, že chlazení nebo kaskáda kotlů mají umožňovat přenos hodnot do systému měření a regulace (MaR) po datové lince, nikoli řadou kontaktů. Rozhraní – modul s komunikační kartou – v dodávce kotlů ovšem chybí. Výsledkem je snížení buď technického standardu budovy, nebo marže zúčastněných firem.

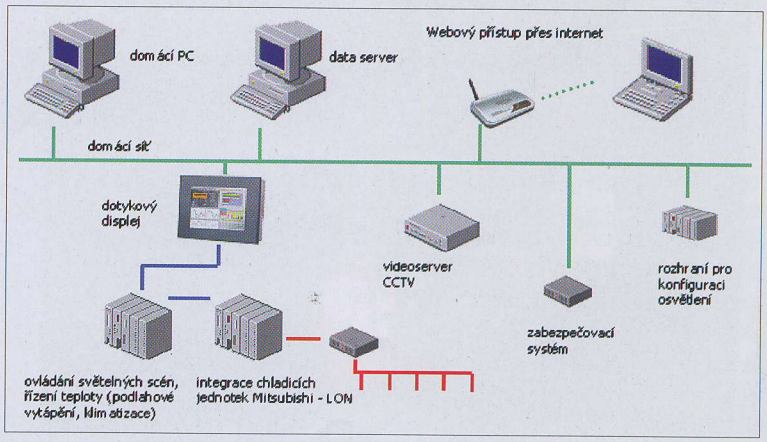
V poslední době se dokonce objevují případy, že zástupce investora problémy schválně neřeší a nechává je až na poslední chvíli, aby měl další nástroj na snižování ceny dodávek a penalizace za nesplnění zadání. Proto je velmi vhodné pozici systémového integrátora zavést. Otázkou ovšem zůstává, kdo jej bude financovat. Nejčastěji je to profese MaR, která tuto úlohu ve vlastním zájmu přebírá jakožto dodavatel BMS a garant systémového řešení.

PŘÍKLAD REZIDENČNÍHO OBJEKTU

Projektant MaR také specifikuje technologickou síť, v níž jsou jednotlivá rozhraní zapojena. I zde je nutná koordinace, a to i u nejmenších akcí, jak vidíme na příkladu rekreační vily v Ste. Maxime, Francie.

V síti jsou zde zapojeny následující prvky:

- ❑ podstanice s dotykovým displejem pro ovládání vytápění, světelných scén a klimatizace, s webovým přístupem a přístupem pro servis



Obr. 1 Topologie vily v Ste. Maxime

- videoserver pro kamery ze systému CCTV, s webovým přístupem pro přehrávání záznamů i pro servis
- rozhraní zabezpečovacího systému s komunikací na ovládací program
- rozhraní pro konfiguraci osvětlení s přístupem pro servis
- data server, na němž běží ovládací program pro zabezpečovací systém
- domácí PC v pracovně majitele
- ADSL router s veřejnou adresou, který umožňuje bezdrátový přístup z notebooků, propojuje vnitřní síť s internetem a zajišťuje konektivitu uživatelů do internetu, dálkový přístup pro ovládání MaR (uživatelsky) a přístup pro servis vybraných technologií.

I u systému rozsahem tak malého (cca. 150 datových bodů) bylo nutné řešit prakticky všechny aspekty síťové koordinace a bezpečnosti. Číslovací plán sítě, konfiguraci routeru a zabezpečení WiFi i dálkového přístupu zařizovala profese MaR, instalaci kabeláže a pasivních prvků pak dodavatel slaboproudých systémů.

FIREMNÍ SÍTĚ

Dalším případem je propojení řídicích systémů do firemní sítě zákazníka, který využívá data ze systému při řízení výroby (sledování teploty a vlhkosti ve výrobních prostorech, centrální řízení klimatizace a vytápění). Tomuto řešení se často bránily především zahraniční firmy s přísnými požadavky na zabezpečení svých intranetů.

Ve většině případů pomůže řada jednání s vedením IT oddělení za účasti technologa zákazníka. Vždy je ovšem třeba dodat podrobné technické informace k použitým rozhraním včetně předpokládaného zatížení sítě, požadavky na routování (některé protokoly, jako například BACnet, vyžadují pro přenos mezi sítěmi zvláštní podmínky), citlivost na zpoždění paketů (latenci), požadovaný počet síťových adres a plán rozmístění přípojek v areálu atd.

U zařízení se servisní smlouvou na dálkovou správu musíme zajistit, aby k nim byl přístup z dispečinku nebo sídla servisní firmy. Telefonní vytáčená linka je čím dál více vytlačována přístupem přes síť, a to z těchto důvodů:

- telefonní modemy mají řádově nižší přenosovou rychlost než sítě;
- zákazník nemá v místě, kde je instalována technologie, přivedenou telefonní linku, zatímco síťová přípojka tam bývá nebo je jednoduché ji zřídit;
- zákazník se obává provozních nákladů, spojených s vytáčeným připojením (odchozí spojení)
- internet pro připojení dispečera nebo servisního technika „je všude", a to i doma nebo přes GPRS za fixní náklady;
- pevná IP adresa bývá k dispozici u zákazníka v rámci platby za jeho připojení, navíc lze využít směrování portů nebo VPN – viz dále;
- je možné sestavit trvalé připojení např. pro záznam historických dat nebo nepřetržitou kontrolu funkce technologie.

GPRS/EDGE

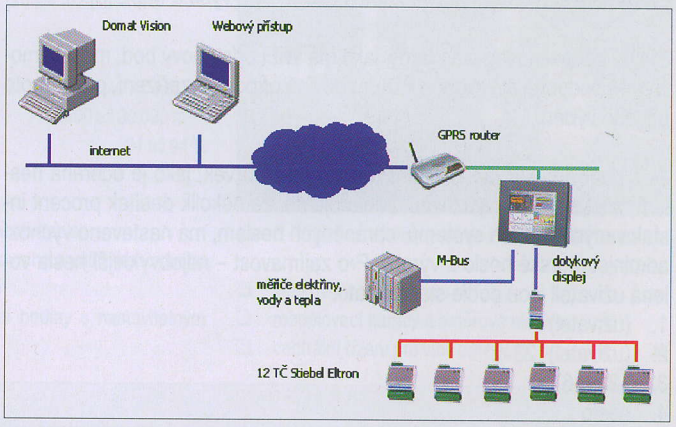
V případech, kde pevné síťové připojení není k dispozici, můžeme využít například GPRS/EDGE routerů, tedy „převodníků" ze sítě Ethernet na síť GPRS nebo EDGE. U nich se nabízí několik možností, jak konektivitu zřídit:

- neveřejná proměnná IP adresa, vhodná pouze pro odchozí spojení (v zásadě na ni „není vidět z internetu") nebo pro příchozí spojení přes speciální služeby (VPN) a hardware (router s podporou funkce VPN klient);
- veřejná pevná IP adresa, která znamená měsíční poplatky vyšší o cca. 150 Kč, je „viditelná zvenku" a se zařízením tak můžeme přímo navazovat spojení z internetu;
- neveřejné APN (Access Point Name) – řešení, kdy v rámci GPRS sítě operátora vznikne uzavřený adresový prostor, nepřístupný z jiné sítě ani z internetu [1]. Adresy v prostoru mezi sebou mohou neomezeně komunikovat. Toto je asi nejvhodnější (i cenově) řešení pro připojení většího množství distribuovaných systémů, které je třeba spravovat z jednoho nebo více definovaných míst (každý, kdo se chce do sítě připojit, musí mít SIM kartu s nastaveným oprávněním).

Při objednávání služby u operátora musíme přesně určit, o jakou službu máme zájem, a zvolit optimální datový tarif. Praxe ukázala, že s výjimkou telemetrie (sběr dat z měřičů) je snad vždy výhodnější objednat tarif s neomezeným množstvím dat. Je vhodné kontaktovat přímo oddělení pro datové služby operátora, s běžnou linkou zákaznické podpory nebývá snadné se dorozumět.

Pokud zákazník neumožní příchozí spojení do své sítě přes veřejnou IP adresu a přesto potřebujeme sledovat měřené hodnoty, případně ovládat zařízení na dálku, můžeme využít řešení, kdy systém navazuje odchozí spojení standardním protokolem zevnitř sítě na server dostupný na internetu a na něj data ukládá. Hodnoty jsou pak dostupné po autorizaci odkudkoli. Server může navíc odesílat varovné SMS nebo e-maily [2].

Příkladem spojení přes GPRS router může být dálková správa regulace tepelných čerpadel v Liberci (realizovala fa. Atax CZ). Webový přístup zde slouží uživateli pro kontrolu funkce, spotřebu energií a nastavování požadovaných hodnot (teplota TUV), dále je zde připojení přes firemní protokol SoftPLC na centrálu servisu s vizualizací a záznamem historických dat.



Obr. 2 Dálkový přístup k tepelným čerpadlům Liberec

BEZPEČNOST

Jakékoli síťové připojení je třeba zabezpečit proti neoprávněnému přístupu. Zařízení ale není buď zabezpečeno nebo nezabezpečeno, neboť síťová bezpečnost je spojitý proces a čím více bezpečnostních mechanismů použijeme, tím nižší bude riziko napadení útočníkem. Zásadou je „povolit jen to, co je nutné, vše ostatní zakázat".

Prvním pravidlem – pokud je to možné – je povolit přístup jen z určitých IP adres. To můžeme splnit například v případě, kdy se na technologii připojuje pouze dispečink ve firmě, která má pevné připojení do internetu. U přístupu z mobilních sítí by se musela objednat pevná adresa nebo by se na firewallu u technologie musel nastavit rozsah adres, což opět bezpečnost snižuje.

Dále je vhodné zablokovat všechny nepotřebné služby a nechat otevřené jen ty síťové porty, za nimiž běží naše aplikace. U regulátoru s webovým

přístupem to může být například web server pro uživatelský přístup a připojení firemním protokolem na proces pro servis a dálkový dozor z dispečinku (změna parametrů, příp. úprava softwaru). Používání neobvyklých čísel portů naproti tomu žádné bezpečnostní opatření není.

Velmi dobrý postup je připojovat se prostřednictvím virtuální privátní sítě (VPN), která vytvoří mezi oběma stranami šifrovaný tunel, v němž pak probíhá komunikace, která je pro pozorovatele „zvenčí" zcela nepřístupná. To ale vyžaduje na obou stranách zvláštní software nebo hardware a zvlášť u dálkového přístupu k rezidenčním budovám je VPN pro uživatele někdy stěží přijatelná: na každém stroji, z nějž se uživatel připojuje, musí být nainstalován VPN klient, což je například u firemních sítí nebo kapesních počítačů (PDA) někdy problém. Pak se doporučuje alespoň šifrovaný webový přístup (https), i když ten v podstatě chrání jen proti odposlechu komunikace cizí stranou, a VPN pro servisní firmu.

V lepším případě je vstup do sítě navíc chráněn firewallem, který kontroluje mj. stav spojení a použité protokoly. U pokročilých modelů jsou pak implementovány i funkce pro odhalení virů a útoků jako je skenování portů atd.

Zvláštní pozornost si zaslouží bezdrátové sítě (WiFi). Jejich obliba v posledních pěti letech silně vzrostla: technologie je cenově velmi dostupná a uvedení do provozu poměrně snadné. Problém je v tom, že jsou velmi snadno napadnutelné, protože útočníkovi stačí být v blízkosti objektu zasíťovaného technologií WiFi.

Opět platí, že musíme vyžadovat zabezpečení na několika úrovních:
- ❑ přístupový seznam MAC adres (MAC access list),
- ❑ šifrování alespoň standardem WPA (raději WPA2),
- ❑ silný WPA klíč (ne řada číslic za sebou jdoucích atd.),
- ❑ a dále standardní síťová zabezpečení – viz výše a např. [3].

Stejné bezpečnostní standardy, jako má WiFi přístupový bod, musí samozřejmě podporovat i klient – PDA nebo jiné připojené zařízení, pozor proto při jeho výběru.

Je s podivem, jak tak základní bezpečnostní prvek, jako je ochrana heslem, zůstává málo využíván. Odhaduje se, že několik desítek procent instalovaných řídicích systémů, chráněných heslem, má nastaveno výchozí administrátorské heslo z výroby. Pro zajímavost – nejobvyklejší hesla volená uživateli jsou podle statistik tato:
1. (uživatel)
2. (uživatel)123
3. 123456
4. heslo
5. 1234
6. 12345
7. password
8. 123
9. test
10. admin

Správné by bylo používat tzv. silná hesla, tedy dostatečně dlouhé řetězce obsahující písmena velká i malá, číslice a někdy i zvláštní znaky (_@&#/%...), pokud to systém dovoluje. Praxe však ukazuje, že čím je heslo silnější a čím se častěji mění, tím je větší riziko, že si je uživatel nakonec napíše na žlutý lístek a nalepí na monitor. Příkladem pravidel pro tvorbu silného hesla může být výňatek z pokynů poskytovatele obchodní aplikace:
POUŽÍVAT
- heslo sestavené ze směsi velkých a malých písmen abecedy,
- heslo obsahující kombinaci abecedních, neabecedních (symboly – povoleny jsou pouze „." a „_" a číselných znaků,
- hesla o délce minimálně 8 znaků,
- různá hesla pro různé účty a identifikace.

NEPOUŽÍVAT
- své jméno ani příjmení a to ani v žádné logicky přetvořené formě (reverzní, zdvojené, proložené, velkým písmem, cyrilikou, řeckými či ruskými znaky, přesmyčkami, permutacemi apod.),
- rodinná jména (partnera, dětí, adresu),
- přezdívky nebo rodná data,
- heslo složené pouze ze stejného znaku nebo číslic,
- hesla složená z po sobě následujících sousedních znaků nebo symbolů na klávesnici,

Heslo si uživatel volí sám a systémem bude akceptováno pouze za předpokladu splnění výše uvedených požadavků.

ZÁVĚREM

Z vlastní zkušenosti víme, že více než polovina problémů u velkého zákazníka (20 supermarketů po cca. 500 datových bodech) byla vyřešena bez nutnosti výjezdu servisního technika díky možnosti dálkového přístupu přes VPN do sítě zákazníka: technik MaR na dálku z historických dat snadno zjistil, kdy k problému došlo, a pomáhal domovním technikům nebo jim upravil nastavení počítače. Jen asi 40 % závad opravdu vyžadovalo výjezd.

Na malé akci, kde bylo nutné během zkušebního provozu několik týdnů nepřetržitě monitorovat kaskádu 12 tepelných čerpadel a optimalizovat její nastavení při odběrových špičkách TUV, pak dálkové připojení přes GPRS router ušetřilo denní cestování a umožnilo parametry sledovat a nastavovat doslova z pohodlí obývacího pokoje.

Závěrem lze říci, že při dostatečné technické kompetenci dodavatele řídicího systému a včasné spolupráci s investorem je možné s použitím běžně dostupných technologií vytvořit systém pro komfortní dálkový přístup, který dokáže ušetřit značné částky na servisních zásazích.

Kontakt na autora: jan.vidim@domat.cz

Použité zdroje:

[1] www.conel.cz, např. služba Agnes
[2] VIDIM J.: Dálkový dohled chlazení webového komunikátoru, www.tzb-info.cz/t.py?t=2&i=4123
[3] THOMAS T. M.: Zabezpečení počítačových sítí bez předchozích znalostí, CP Books a.s., Brno 2005. ■□

* Kongresový palác v Paříži využívá zásobníky ledu

Stále více nabízejí dodavatelé elektřiny zvláštní tarify, akceptuje-li zákazník určité doby odstávky. Nově je u kongresového paláce v Paříži používán, kromě doby běžných tarifů proudu ze sítě i záložní (nouzový) proud. Podle dohody s dodavatelem energie (EDF) má palác atraktivní smlouvu na zvlášť nízký tarif s tím, že provozovatel bude během zimy po 21 dnů mezi 7 a 24 hodinou krýt svou potřebu z vlastního zdroje.

Aby pro klimatizační zařízení bylo k dispozici dost chladicího výkonu, jsou nabíjeny dva zásobníky ledu. První zásobník obsahu 124 m^3, nabíjený chladicím zařízením o chladicím výkonu 800 kW, je nabíjen denně ráno v době nízkého tarifu na 80 % a v zimě v době krytí spotřeby z vlastního zdroje na 100 %. Jako pojistka při krátkodobě vyšší potřebě chlazení v létě nebo při vypnutí chladicích agregátů je určen druhý zásobník obsahu 140 m^3, nabíjený dalším chladicím zařízením o chladicím výkonu 800 kW, které může v případě potřeby po celý den dodávat cca 1 MW chladu do sítě studené vody. Oba zásobníky ledu jsou schopny při výpadku chladicích agregátů dodávat do sítě chladicí vody cca 4 MW chladu po dobu 2 až 3 hodin.

CCI 11/2007 *(Ku)*