



Chytré domy a bezpečnost

krátká úvaha nad problematikou bezpečnostních systémů v
„inteligentních“ budovách

aneb

Co se za rok změnilo ?

Ing. Zdeněk VOTRUBA

Ing. Petr VACULÍK, Ph.D.





„Chytrá“ budova ?

Je zbytečné v tuto chvíli diskutovat o tom, **co to inteligentní budova je** (i když jednoznačná definice je stále poněkud problematická).

Spíše se podívejme na to, **co od takové budovy očekáváme:**

- optimalizace řízení – finanční návratnost
- sdružení ovládacích prvků
- vysoký uživatelský komfort
- **zvýšená bezpečnost a odolnost**





Možná technická řešení

Snahou **projektanta i uživatele** je tedy stále větší tlak na **centralizaci správy instalovaných systémů**, jejich propojování a v konečné instanci pak i jejich **vzájemné ovlivňování** a automatickou optimalizaci provozu a autodiagnostiku.

Tento trend se projevuje již desítky let, výsledky však nejsou nijak výrazné. Integrace celé řady vnitřních systémů je v řadě případů sice **technicky možná**, vzhledem ke spolehlivosti, bezpečnosti i z pohledu platných norem však **značně problematická**.



Možná technická řešení

Vzhledem k výše uvedenému faktu je tedy nejdříve nezbytné definovat **parametry systémů** (***performační indikátory***), využívaných v různých typech objektů a následně pak definovat jejich vhodnost pro případnou integraci.

Teprve poté je možné určit způsoby integrace a to s ohledem na zachování nezbytných **provozních, technologických** a především **bezpečnostních** podmínek.



Možná technická řešení

Historicky starší (a stále nejvíce používaný) je systém s **centrální jednotkou**. Tento způsob má své výhody především v jednoduchosti implementace informačního systému - lze použít obvyklé nástroje pro vytvoření IS s centrální správou. Narážíme zde však na zásadní obtíže při rozšiřování systému, jeho modernizaci a při integraci nových modulů. Zásadní problém je pak při pohledu na spolehlivost celého centrálního systému. **Je to v podstatě podobné, jako bychom např. Internet založili na centrálním řídicím uzlu (serveru).**

Centralizovaný systém tedy obsahuje centrální řídicí jednotku, která je propojená pomocí sběrnice s ostatními prvky. Informace ze senzorů jsou posílány do centrální jednotky, kde jsou zpracovány a výsledné informace jsou posílány do aktorů.

Výhoda:

- levné senzory a aktory

Nevýhoda:

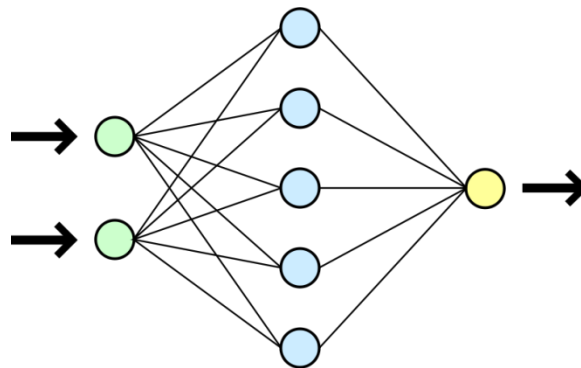
- složitější funkčnost centrální jednotky
- nutnost propojení centrální jednotky se všemi ostatními prvky systému
- celková nižší spolehlivost systému daná spolehlivostí centrální jednotky





Možná technická řešení

Modernější a nepochybně koncepčnější technologie řízení systému IB je založena na **distribuovaném systému řízení**, tedy bez centrální jednotky, resp. s centrální jednotkou jednotlivých modulů, komunikujících na inteligentní sběrnici mezi sebou. Přesun informace mezi moduly je pak řešen speciálním protokolem.





Možná technická řešení

Decentralizovaný systém obsahuje jednotlivé prvky propojené komunikační sběrnici, po které si navzájem posílají nebo přijímají informace. Není zde žádný centrální prvek, což znamená, že všechny prvky jsou si rovnocenné.

Výhoda:

- jednodušší a levnější propojení mezi prvky,
- variabilita systému,
- při poruše nedojde k výpadku systému,

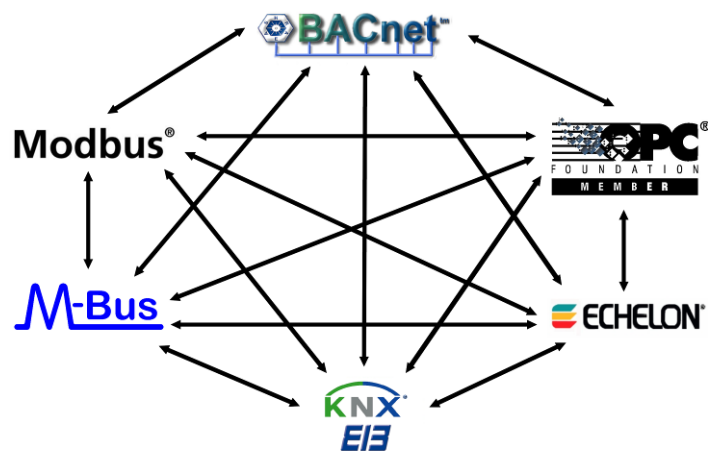
Nevýhoda:

- vyšší cena prvků z důvodu inteligence jednotlivých prvků.



Možná technická řešení

Postupem času vznikla celá řada sběrnic vhodných pro instalaci do „inteligentních budov“ (centralizovaných i decentralizovaných):



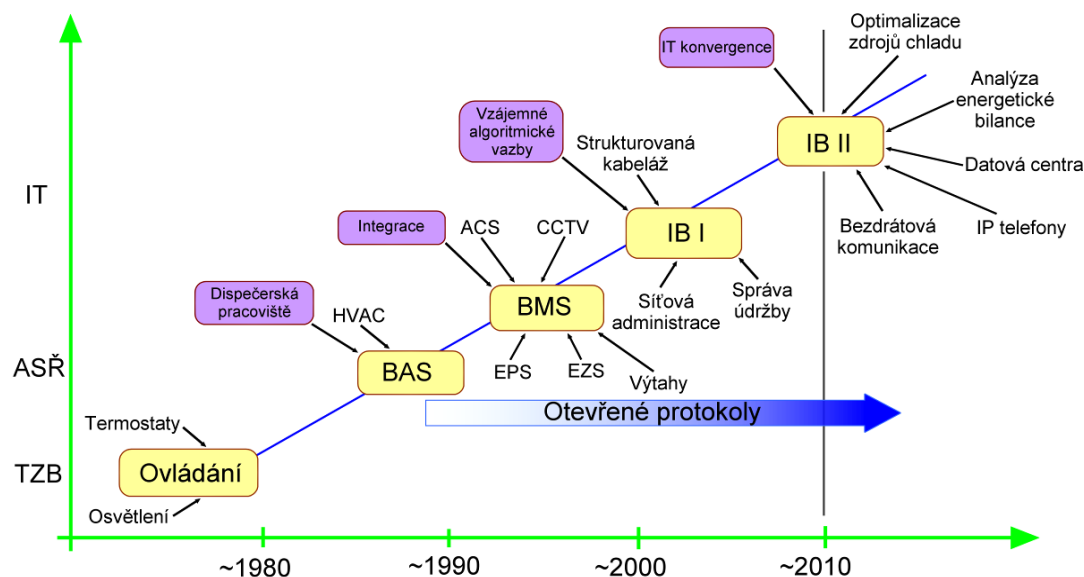
- Sběrnice **KNX/EIB**
- Sběrnice **LONWORKS**
- Protokol **BACNET**
- Protokol **MODBUS**
- Protokol **SNMP**
- Protokol **C-BUS**
- Protokol **ENOCLEAN**
- Sběrnice **TECOMAT/Foxtrot**





Možná technická řešení

Při rozhodování o volbě konkrétního způsobu integrace systémů je samozřejmě rovněž potřeba zvážit **míru a úroveň technologií** a jejich integrovatelnost. Velice dobře je tento vývoj popsán v následujícím grafu:





Možná technická řešení

Výše uvedený graf je pro další argumentaci zcela zásadní. Z grafu je zřejmé, že se v současné době nacházíme v období, kdy se pro integraci využívají **především principy počítačové komunikace.**

Tento postup je samozřejmě optimální z hlediska ceny a snadné systémové integrovatelnosti, je však zcela tragický z pohledu integrace bezpečnostních systémů.



Možná technická řešení

Zdůvodnění předchozího tvrzení lze doložit např. článkem:

- doc. Ing. Antonín Mykiska, CSc: ***Zabezpečení spolehlivosti technických systémů v období návrhu*** (Automa, 11/2001),
- doc. Ing. Mirko Novák, DrSc: ***Obecná hlediska spolehlivosti a bezpečnosti technických systémů*** (Výzkumná zpráva č. LSS 100/01).



Možná technická řešení

Důsledkem je tedy fakt, že pokud vezmeme za výchozí pro další předpoklady způsob komunikace převažujících počítačových sítí (TCP/IP nad sítí Ethernet), vezmeme v potaz spolehlivost běžných síťových prvků, serverů včetně PLC, lze dovodit, že **předpokládaná spolehlivost takto integrovaných bezpečnostních systémů bude řádově nižší než je stávající neintegrováný modulární systém.**

To samozřejmě nelze v rámci bezpečnostních systémů akceptovat !



Možná technická řešení

A to je klíčový problém integrace bezpečnostních systémů do současného modelu projektů inteligentních budov! I když odhlédneme od problematiky norem, je cesta integrace prostřednictvím TCP/IP a PC serverů (částečně i PLC) zcela chybnou a v dlouhodobé perspektivě bychom se dostali do podobných problémů, jako řeší síť Internetu např. s QOS a obdobných. Bohužel s tím rozdílem, že v případě bezpečnostních systémů jde již o výrazně více než o načtení webové stránky či emailu!



Takže neintegrovat ?

Již z principu funkce IB je potřeba integrovat minimálně některé prvky bezpečnostních systémů pro plnou a korektní funkci IB:

- detektory **PZTS** (PIR, magnetické kontakty),
- **ACC** (přístupové terminály),
- požární detektory systémů **EPS**,
- případně záznamy z kamer **CCTV** systému



***Všechny tyto zdroje informací využíváme tedy jako
senzory pro IB (pro aktory)***



ANO, ale...

A právě v tomto okamžiku narážíme na legislativní a normalizační hranice bezpečnostních systémů:

- objekty mající předepsanou třídu bezpečnosti, či je z pohledu spolupráce s pojišťovnou třídu bezpečnosti nutné dodržet, musí mít **PZTS** dle **ČSN CLC/TS 50131:2007** !





ANO, ale...

- objekty mající za povinnost instalaci systému **EPS** či **SKS** musí splňovat pro tyto systémy normy řady **EN 54** a samozřejmě zákon č. **67/2001 Sb.** včetně především vyhlášky č. **246/2001 Sb**



- pokud je v objektu využit kamerový systém **CCTV** musí tento splňovat normu **ČSN EN 50132** a samozřejmě další zákony, především zákon č. **101/2000 Sb.**



ANO, ale...

Obdobně by bylo možné pokračovat **systemy** **přivolání pomoci (ČSN EN 50134)**, přístupovým systémem **(ČSN EN 50133)**, **poplachových** **přenosových systémů (ČSN EN 50136)** atd.

Kde však je zmíněný problém?



Problém 1

V podstatě libovolný ze zmíněných bezpečnostních systémů přesně definuje, jaké komponenty a za jakých podmínek lze použít pro jeho realizaci.

Pokud si za příklad vezmeme např. **PZTS** (situace v EPS je ještě mnohem přísnější), máme všechny použitelné komponenty definovány do 4 bezpečnostních tříd (přiřazeno NBÚ či TestAlarm).





Problém 1

Platí jednoduchá zásada:

Bezpečnostní třída celého zabezpečovacího systému je dána třídou prvku s nejnižší bezpečností!



Pokud realizuji integraci zabezpečovacího systému do systému IB, kde je předepsána třída bezpečnosti např. 3 a pro propojení použiji prvky bez bezpečnostní certifikace – je celý zabezpečovací systém v bezpečnostní třídě 0 a nejsou splněny požadavky (zákoné, investora, pojišťovny).



Problém 1

Jakou bezpečnostní třídu dle NBU či TA má dle ČSN 50 131 např. modul KNX či Bacnet ?

**- bez certifikace –
tedy třída 0 !**

→ máme problém ..





Námitka !

Samozřejmě lze s tímto tvrzením polemizovat. Většinu těchto polemik lze shrnout ve dvou námitkách:

- **normy, vyhlášky a legislativa je zastaralá**
- **existuje norma ČSN CLC/TS 50 398:2009**



Námitka !

Normy, vyhlášky a legislativa je zastaralá!

Samozřejmě nelze polemizovat - na druhou stranu současně používaná struktura je již více jak 150 let prověřená a osvědčená.

Rozhodně by tedy nebylo vhodné nahrazovat jasná pravidla např. využitím univerzálního komunikačního protokolu TCP/IP – cesta do pekel – velký tlak ze strany výrobců a integrátorů.

Námitka !

Existuje norma ČSN CLC/TS 50 398:2009!

Norma je velice obecná, přesto však v bodě 4.2. jasně říká:

„U integrovaných poplachových systémů musí být pro každou aplikaci systému použity její příslušné normy.“

Tím se vracíme k původně definovanému problému. Norma sice definuje 3 typy konfigurace integrovaného systému, rozděluje je však podle vzájemného ovlivňování a samostatnosti jednotlivých podsystémů (Typ1, Typ 2A, Typ 2B).



Osobní poznámka

Na tomto místě si dovolím jednu velice osobní poznámku – stávající podoba normy **ČSN CLC/TS 50 398:2009** je tak „příšerná“, že si vůbec nedovedu představit, jak mohla „projít“ přes TNK 124 a osobně velice doufám (a pokusím se), aby zde tato norma byla výrazně revidována a uvedena do logického vztahu s normami ostatních bezpečnostních systémů.

Již v tuto chvíli je s praktickým výkladem této normy poměrně velký problém a to nás skutečná integrace bezpečnostních systémů teprve čeká...



Problém 2

Z pohledu živnostenského zákona (Zákon č. **455/1991 Sb.**) je instalace bezpečnostních systémů koncesovanou živností.

Pro získání koncese k provozování živnosti č. 314 - *Technické služby k ochraně majetku a osob* je potřeba splnit některé zásadní (elementární) předpoklady.

Bezpečnostní systémy tedy **NESMÍ** instalovat osoba nemající odpovídající koncesi a certifikát opravňující instalovat konkrétní bezpečnostní systém.



Námitka 2

Námitky proti tomuto ustanovení snad nebudu ani publikovat ...

V každém případě budme rádi, že alespoň takovéto triviální omezení existuje a osobně se domnívám, že by mělo být výrazně zpřísněno!

Důsledky: projekt a instalaci provádí pouze koncesované firmy s certifikátem výrobce konkrétních komponent, dodržují se zásady definované dle ČSN 50131 a především ČSN 50136



Takže jak ???

Před rokem jsem se na tomto místě zmiňoval o několika možných komerčních řešeních, které by bylo možné za určitých předpokladů použít k integraci bezpečnostních systémů do inteligentních budov.

Jmenoval jsem řešení **Skilla** či **Charybda** (vhodné pro malá či střední řešení), zmínil jsem se o **VarnetIntegrál** (centralistické proprietární řešení) a popsal jsem i **Concept 4000** jako komplexní a drahé řešení.

Takže tak ???

Zásadním pokrokem je však trend společnosti **Teco a.s.**, která posunula (či na tom aktuálně pracuje) svoji sběrnici CIB do oblasti bezpečné (certifikované) komunikace. To by pak v tomto konkrétním případě znamenalo, že konečně budeme mít k dispozici distribuovaný systém, umožňující plnou integraci bezpečnostních systémů (a to snad dokonce systémů vytvořených přímo nad moduly společnosti Teco). Bezpečnostní systém se pak skutečně stane integračním nástrojem této sběrnice!



Takže tak ???

Dalším nesporně pozitivním pokrokem za uplynulý rok v oblasti integrace bezpečnostních systémů bylo zřízení **Pracovní skupiny pro bezpečnostní a asistivní systémy** při profesním sdružení **Českého klubu bezpečnostních služeb**. Jedním z prvořadých úkolů této pracovní skupiny je právě zhodnocení stávajících integračních technologií a doporučení o jejím využití pro členy sdružení.



A co takto...

Jako námět, jakým způsobem by se mohla ubírat bezpečná integrace, je myšlenka vzniklá při letošním přebírání technické normy datové komunikace bezpečnostních systémů **SIA DC-09-TNI 33 4592**.

Stojí za zvážení a pečlivou analýzu, zda tento protokol není právě to, co by bylo optimální použít jako komunikační protokol nejenom mezi jednotlivými systémy v rámci IB ale i přímo jako komunikační standard v rámci daného systému? (námět pro výrobce).



Soupis relevantních legislativních a normativních podkladů



- Zákon č. **101/2000 Sb.** – o ochraně osobních údajů
- Zákon č. **455/1991 Sb.** – živnostenský zákon

- **ČSN CLC/TS 50131:2007** – PZTS
- **ČSN CLC/TS 50398:2009** – Kombinované a integrované systémy
- **ČSN EN 50134-1:2003** – Systémy přivolání pomoci
- **ČSN EN 50132** – CCTV systémy
- **ČSN EN 50136 A1:2002** – Poplachové přenosové systémy
- **TNI 33 4592** – SIA DC-09

Kromě výše uvedených norem a dokumentů byly v referátu použity práce, citace a obrázky autorů:

VALEŠ, Miroslav. *Inteligentní dům*. Vyd. 2. Brno : ERA, 2008. 123 s.
ISBN 978-80-7366-137-3

MERZ, Hermann; HANSEMAN, Thomas; HÜBNER, Christof.
Automatizované systémy budov. Praha : Grada Publishing, 2008. 264
s. ISBN 978-80-247-2367-9

BURANT, Jiří., CSIRIK, Vincent., DUDÁŠ, Josef., DVOŘÁČEK,
Karel., DVOŘÁČEK, Vladimír., FENCL, František., KUNC, Josef.,
LAIFR, Jiří., MACHÁČEK, Václav., MAIXNER, Tomáš., URBAN,
Zbyněk., VOTRUBA, Zdeněk. *Elektrotechnické a telekomunikační
instalace*. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475

+ elektronické zdroje



Děkuji za pozornost !

