ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

TECHNICKÁ FAKULTA

KATEDRA TECHNOLOGICKÝCH ZAŘÍZENÍ STAVEB

INTEGRACE OCHRANNÝCH SYSTÉMŮ V RÁMCI PROJEKTU „INTELIGENTNÍ BUDOVY“

INTEGRATION OF PROTECTIVE SYSTEMS WITHIN INTELLIGENT BUILDING SYSTEMS

Doktorská disertační práce

Doktorský studijní program:	Zemědělské inženýrství
Obor:	Technika výrobních procesů
Doktorand:	**Ing. Zdeněk VOTRUBA**
Školitel:	**doc. Ing. Miroslav Přikryl, CSc.**

Praha 2014

Prohlášení

„Prohlašuji, že jsem tuto disertační práci na téma "INTEGRACE OCHRANNÝCH SYSTÉMŮ V RÁMCI PROJEKTU 'INTELIGENTNÍ BUDOVY'" vypracoval samostatně pod vedením školitele a uvedl jsem veškerou použitou literaturu.

Tištěná a elektronická verze práce se doslovně shodují"

V Praze dne **9.9.2014**

. . . . . .

Ing. Zdeněk Votruba

Poděkování

Děkuji především své rodině za trpělivost s mojí osobou po dobu zpracování této práce. Dále děkuji svému vedoucímu práce doc. Ing. M. Přikrylovi CSc. a doc. Ing. P. Vaculíkovi Ph.D. za pomoc a podporu při zpracování práce.

Klíčová slova:
poplachový systém, inteligentní budova, integrace, neuronová síť, sběrnice inteligentních budov, zabezpečovací systém

Anotace:

Práce je zaměřena na problematiku integrace poplachových systémů v rámci informačních systémů inteligentních budov. V první části práce jsou definována základní technická a legislativní pravidla, nezbytná pro korektní fungování poplachových systémů v systémech inteligentních budov. Druhá část analyzuje nejčastěji používané technologie pro komerční integraci a poukazuje na jejich úskalí při integraci poplachových systémů. Klíčovou částí práce je porovnání možností nasazení různých technologií pro integraci.

Podrobně a dlouhodobě je testován především způsob integrace pomocí programových výstupů zabezpečovacích ústředen (PGM). Na základě několikaletého testování je prokázáno a statisticky doloženo, že integrace nemění míru spolehlivosti uvedených systémů. Na úrovni integrace menších a středně velkých systémů se jedná o optimální řešení z hlediska technologické spolehlivosti a ceny, s jistou výhradou přehlednosti řešení.

Testování distribuované sběrnice KNX/EIB bylo realizováno pouze v úvodní fázi, neboť již při prvních testech se jednoznačně prokázal základní vážný nedostatek tohoto řešení. Jedná se především o problém s napájením sběrnice a uzlů, zásadní však je problém se spolehlivostí doručování telegramu (kolize paketů) a s kompatibilitou produktů různých výrobců. Proto bylo toto řešení z možných integračních nástrojů vyloučeno.

Využití sběrnice CIB českého výrobce TECO a.s. prokázalo oprávněnost použití pro integrace zvláště středních a větších systémů. Na návrh autora v současné době výrobce modifikuje přístup k napájení a parciálnímu programování, což evidentně zvýší aplikační potenciál. Spolehlivost a odolnost celého řešení pomocí CIB sběrnice je velice uspokojivá.

Autorem bylo dále navrženo vlastní původní řešení integrace pomocí tzv. neuronového klíče. Princip tohoto řešení spočívá ve schopnosti neuronové sítě „naučit“ se strukturu komunikace jednoho z integrovaných systémů a potřebné stavy předávat v libovolně jiné struktuře jinému z integrovaných podsystémů. Na základě několika matematických modelů byl tento princip otestován a zjištěné výsledky potvrdily reálnost použití. Uvedený princip je v tuto chvíli podán s návrhem na patentovou ochranu.

Druhým původním řešením je návrh na integraci pomocí standardizovaného protokolu SIA DC-09. Tento princip integrace nebyl v rámci této práce prakticky testován, pouze rozpracován po teoretické stránce jako možné řešení. Rovněž v tuto chvíli je podán návrh na jeho patentovou ochranu.

Celkově výsledky této práce prokázaly, že problematika integrace poplachových systémů v kontextu inteligentních budov je otázka poměrně rozporuplná. Většina v současné době komerčně používaných řešení neodpovídá požadavkům na integraci.

Keywords:
alarm system; smart building; integration; neural network; bus; smart building bus, security system.

Abstract:

Presented work is focused on the integration of alarm systems into the information systems of smart buildings. Basic technical and legislative rules which are necessary for the proper function of alarm system within the frame of smart building system are defined in the first part.

Frequently used technologies are analyzed from both the commercial and integration process points of view. Important stumbling blocks of the integration of alarm systems are discussed. A key part of this work is the comparison of different technological approaches to achieve really efficient integration.

An approach to the process of integration based on search of respective security programmable control units (PGM) outputs was tested in detail for considerably long time. Several years long testing proved and statistically documented that well done integration on this principle does not alter the degree of reliability of these systems. At the level of small and medium-sized systems integration it certainly is the optimum solution in terms of technological reliability and price, subject to the lack of clarity of such solution.

Testing of distributed KNX / EIB bus was realized in the initial stage only, since it was clearly demonstrated during initial tests that this approach owes a serious drawbacks. It's a problem with the power supply of bus and nodes, but above all a fundamental problem with the reliability of the telegrams delivery (packet collisions) compatibility of the products from different manufacturers. Therefore this solution of respective integration was cancelled.

Detailed analyze of CIB bus of the Czech manufacturer Tesco justified that the use of this approach to the integration is advantageous especially for medium and large systems. Manufacturer at the suggestion of the author currently modifies his approach to the power supply as well as to partial programming, which obviously could increase the application potential. Reliability and robustness of this solution as a whole using the CIB bus is very satisfactory.

The author has also designed its own original solution of the integration via the so-called “Neuronal key”. The principle of this solution lies in the ability of neural

networks to "learn" the structure of one of the communication systems being integrated and consequently to pass required states in any other form, which can be quite different from the first one, to the second subsystem. This principle was tested on the basis of several mathematical models and the results confirmed the feasibility of its real use. This principle is at this moment in the phase of patent pending.

Another original solution of the author is a proposal to integrate system using a standardized SIA DC-09 protocol. This principle of integration was not in this work practically tested, just theoretically elaborated as a feasible solution. Also this principle is at this time in the phase of patent pending.

Overall, the results of this work have shown that the issue of integration of alarm systems within the frame of intelligent building is rather controversial one. Most of currently used commercial solution does not satisfy the integration needs.

Obsah

1 ÚVOD

Předložená disertační práce si klade za cíl posoudit technické, technologické, bezpečnostní a komerční možnosti integrace bezpečnostních systémů (tj. zejména zabezpečovacích systémů, kamerových systémů, protipožárních a přístupových systémů) do vnitřních informačních systémů tzv. inteligentních budov. Cílem práce není detailní a komplexní popsání obvyklých systémů, vybavení, technologií a technik v tomto oboru, klade si však za úkol definovat základní využívané systémy a zhodnotit je z pohledu možné integrace se zohledněním především bezpečnostních a legislativních rizik. Úvodní kapitoly práce tak poskytují obecný přehled na současnou situaci v integrační problematice. Navazující kapitoly pak definují a zdůvodňují vlastní navržená řešení a porovnávají jej s výsledky testovaných alternativních technologií.

Na základě získaných poznatků, provedených měření a testů je v rámci této práce představeno původní řešení možné integrace bezpečnostních systémů a prvků. Posouzeny jsou faktory limitující integraci bezpečnostních systémů v různých typech objektů, vliv tohoto začlenění na spolehlivost celého integrovaného systému budovy a možný přínos komerční, technologický a především bezpečnostní. Dílčí úlohou, nezbytnou pro celkové řešení práce se stalo především vyřešení kompatibility decentralizovaných řídících systémů. Na základě teoretických výpočtů, experimentálního měření a modelování uvedených v této práci (jak v laboratorních podmínkách, tak i v běžných provozních podmínkách), jsou formulovány základní premisy, z nichž vychází soubor požadavků na vlastnosti dílčích systémů a jejich možnou integraci. Tyto předpoklady jsou diskutovány ve vztahu s legislativní a normativní základnou platnou v ČR i v Evropské Unii. Tento aspekt se v konečném součtu ukázal jako nejkritičtější a nejobtížnější část práce. Konečným výstupem pak je vytvoření návrhu technologie na bezpečnou a modulární integraci bezpečnostních systémů a to včetně řešení ověřeného na matematickém modelu.

V úvodní části práce je provedeno shrnutí základních pojmů, o které se práce opírá, rovněž jsou zde definována klíčová paradigmata, která jsou stěžejní pro výslednou realizaci navrhovaného řešení a to včetně nezbytných základních historických konsekvencí (nezbytných především z normativního a legislativního hlediska).

1.1 Inteligentní budova

Pojmy jako inteligentní dům či inteligentní budova (*smart building*) jsou v dnešní době velice populární a lze se s nimi setkat ve velkém množství článků, diskusí i odborných publikací. Inteligentní budovy (dále jen IB) jsou i oblastí výzkumu a testování, kterému se věnuje celá řada nejenom výzkumných a vzdělávacích institucí, ale i komerčních firem a firemních sdružení. Je proto logické, že tento pojem, resp. jeho aspekty, jsou dnes oblastí zájmu nejenom architektů, projektantů, technologů, ale i informatiků a v neposlední řadě i specialistů na bezpečnostní otázky a technologie.

Pod pojmem inteligentní budova je dnes většinou vnímána rozsáhlejší stavba typu komerční či užitkové budovy (školy, kancelářské budovy, budovy firem). Inteligentní dům pak naopak představuje stavbu relativně rozměrově malou, obvykle rodinný dům. Za účelem této práce nebudou tyto dva pojmy rozlišovány kromě části, kde bude diskutována návratnost investic do inteligentní budovy (domu).

Základní obtíž je v tom, že pojem inteligentní budova (dále IB) je v současnosti používán velmi volně[101]. Tímto pojmem bývají často označovány triviálně integrované objekty, kde jsou pouze propojeny například bezpečnostní systémy (PZTS) s kamerovým systémem (CCTV) a strukturované kabelové rozvody (SKS) pro počítačovou síť, až po rozsáhlé objekty, jejichž integrované systémy se „umí učit“ a přizpůsobovat vnitřní prostředí pro požadavky konkrétního uživatele.

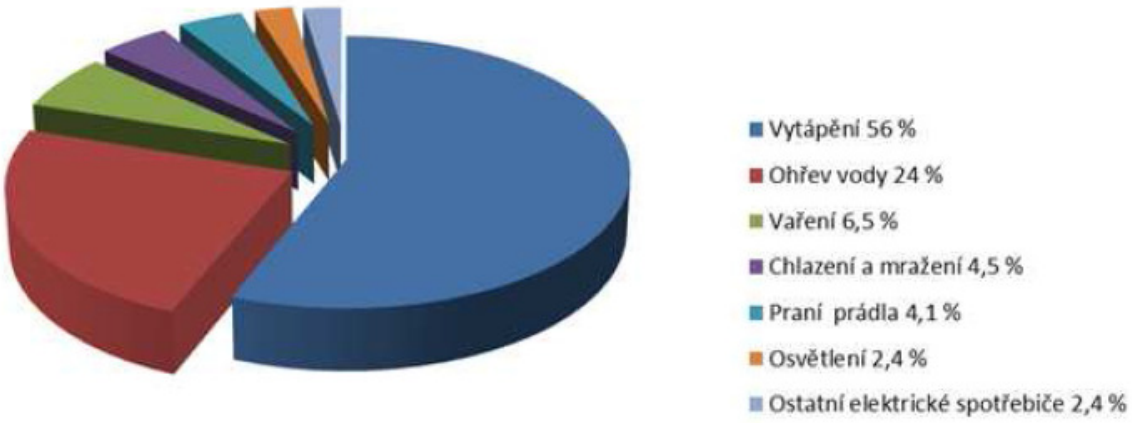
Současné tržní prostředí, spolu se stále rostoucím tlakem na automatizaci, spolehlivost a především na bezpečnost osob, objektů i technologií, staví obvyklý pohled na projektování budov stále většímu tlaku na nezbytnou a zásadní změnu. V dnešní době je již zcela běžné, že v rámci objektu jsou paralelně instalovány **informační systémy** (počítačové sítě, telefonní sítě, rozvody zvuku a obrazu), **bezpečnostní systémy** (poplachové systémy, kamerové systémy, přístupové systémy, protipožární systémy, systémy protivýbuchové, systémy proti zaplavení a další) i rozsáhlé **technologické systémy** (klimatizace, větrání, topení, výtahy, technologické linky). Následkem toho je ze strany uživatele objektu stále větší tlak na centralizaci správy instalovaných systémů, jejich propojování a v konečné instanci pak i na jejich vzájemné ovlivňování a automatickou optimalizaci provozu a autodiagnostiku.

Tento trend se projevuje již desítky let, výsledky však nejsou nijak výrazné. Integrace většiny vnitřních systémů je v řadě případů sice technicky možná, vzhledem ke

spolehlivosti, bezpečnosti a z pohledu platných norem, však i značně problematická. Vzhledem k tomuto 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.

Jedním z hlavních cílů inteligentního domu (a prvním argumentem pro jeho zavedení) je snížení spotřeby energií. Jde samozřejmě jak o finanční úspory, tak o ochranu životního prostředí. V následujícím grafu je znázorněna statistika rozdělení spotřeby průměrné české domácnosti[101]. V další části práce však bude demonstrováno, že finanční aspekt rozhodně nemá univerzální platnost a jeho význam je značně diskutabilní.

Obr. 1 *Spotřeba energie v české domácnosti*



Zdroj: [101]

První „**inteligentní dům**“ byl v 60. letech 20. století prezentován v Japonsku [37] . Tak, jak bylo v té době moderní, veškeré technologie a funkce řídila centrální jednotka, dnes bychom ji označili jako PLC počítač. Tyto úvodní praktické pokusy se však nesetkaly s velkým zájmem technologů ani stavebníků a nebyly tedy výrazněji uplatněny v praxi. Zhruba o 10 let později, počátkem 70. let minulého století zapříčinila energetická krize a prudký nárůst cen ropy opětovné vzkříšení zájmu o tento projekt. Především proto, že tato myšlenka by mohla vést k výraznému a globálnímu snížení spotřeby elektrické energie při vytápění budov, osvětlení, klimatizaci a to při celkovém zvýšení uživatelského komfortu. Poměrně rychle bylo dosaženo prvních úspěchů – řada především německých výrobců

začala nabízet nejenom kvalitnější otopné a další systémy, ale především nově koncipované, navzájem spolupracující elektrické instalace.

V té době se přístup ke snižování energetické náročnosti objektu rozdělil v podstatě na dvě části. První směr se věnoval rozvoji konstrukcí a materiálu budov tak, aby budovy spotřebovávaly méně energie na úpravu vnitřního prostředí. Díky tomu začala postupně vznikat představa domu, který dnes označujeme za nízkoenergetický. Tato výstavba byla úspěšně ověřena v praxi v 80. letech [54]. Druhý směr vývoje se věnoval především měření spotřeby energií a jejich vyhodnocování a zpětného řízení. Z tohoto směru vznikl trend dnes označovaný jako automatizovaný systém, jehož úkolem je zefektivnit vynakládání energií v objektu a zabránit tak zbytečnému plýtvání. Rozvoj výpočetní techniky umožnil nasazení centrálních řídicích počítačů, které vycházely z první generace osobních počítačů. Vysoké investiční náklady těchto systémů nedovolily nasazení do běžné praxe řadových domů a menších budov, ale pouze do objektů, ve kterých bylo možno dosáhnout vysokých energetických úspor. Těmito objekty byly především školy, zdravotnická zařízení a budovy státní správy. Zde bylo možné stanovit harmonogram provozu jednotlivých místností v průběhu dne, týdne a případně celého roku. Proto bylo možné naprogramovat vytápění tak, aby udržovalo provozní teplotu v místnostech jen v době, kdy jsou skutečně využívány a v ostatní době se výrazně snížila dodávka energií. Prakticky bylo ověřeno, že díky tomu se snížila energie na vytápění v průměru o 30%. Bylo tedy zřejmé, že tyto technologie mají smysl, ovšem za předpokladu výrazně vyšší technické vybavenosti elektrických instalací. Projevily se však i první nedostatky centrálně řízeného systému. Základním problémem byla bezpečnost a spolehlivost celého systému. Především proto, že v případě poruchy centrálního řídícího prvku došlo ke kolapsu celého systému. Rovněž topologie sítě rozvodů byla při tomto přístupu poměrně složitá (nezbytnost kabeláže od centrální jednotky ke každému sensoru a aktoru) [64].

Za počátek zrodu jednotné koncepce inteligentní elektroinstalační techniky lze považovat rok 1987, v němž založily firmy Berker, Gira, Merten a Siemens společnost **Instabus Gemeinschaft** . Jejich cílem bylo vyvinout systém pro měření, řízení, regulaci a sledování provozních stavů v budovách. [37], [38]

Následně začala vznikat celá řada nástrojů a protokolů umožňující propojení jednotlivých systémů. Je pravda, že v současné době stále není jednoznačná definice toho, co to IB vlastně je a jak jí lze specifikovat. Pro korektní řešení uvažovaného problému a

nalezení odpovídajícího řešení je však nezbytné základní definici stanovit, přinejmenším s ohledem na provázanost na vnitřní bezpečnostní systémy. Proto jsou zde uvedeny některé z nejčastějších definicí IB, každá z nich však řeší IB z pohledu konkrétního uživatele (projektant, architekt, technolog, informatik,…).

I. **European Smart House Standards Group** uvádí tuto definici:

„Inteligentní dům vytváří prostředí, jež umožní zajištění a zvýšení kvality života všech obyvatel domu a bytu integrací technologií a služeb za účelem ekologického využití všech zdrojů, zjednodušení obsluhy, zvýšení ochrany a bezpečnosti, komfortu a komunikace“ [12].

Definice se orientuje na spokojenost jejích uživatelů, které je dosaženo pomocí integrace technologií a služeb. Budova samotná, její konstrukce, materiály a uspořádání, v definici není obsažena.

II. **Japan Intelligent Building Institute** uvádí tuto definici:

„Budova je vybavena komunikačními službami s automatizovaným provozem a je vhodná pro inteligentní aktivity“ [37].

Podle této definice by IB byla většina moderních budov, které mají řízené vytápění, PZTS a počítačovou síť. Je zřejmé, že tato definice je sice poměrně volná, ale zároveň i zcela bezobsažná.

III. Definice uvedená na **Mezinárodním symposiu v Torontu 1985**:

„Inteligentní budova představuje kombinaci inovace a techniky s kompetentním řízením s cílem maximalizovat návratnost investice.“ [12]

Definice je sestavena z pohledu technologií a efektivnosti, není tedy zaměřena na komplexnost řešení. Jedná se tedy pouze o částečné řešení skutečných funkcí IB.

IV. **Intelligent Building Institute of USA (IBI)** definuje IB takto.

„Inteligentní budova je taková, která vytváří produktivní a úsporné prostředí pomocí optimalizace čtyř základních prvků - struktury, systému, služeb a managementu - a vzájemných vztahů mezi nimi.“ [101]

Tato definice je velice obecná, jednoznačně preferuje provázání různých řešení a systémů. Zahrnuje pohled projektanta, technologa i informatika uvedeného systému IB. Její nevýhodou je přílišná všeobecnost a nekonkrétnost.

V. **European Intelligent Building Group (EIBG)** uvádí tuto definici:

„Inteligentní budova je taková, která obsahuje nejlepší dostupné koncepce, materiály, systémy a technologie navzájem propojené tak, že budova splňuje nebo překračuje výkonnostní požadavky zainteresovaných stran, k nimž patří vlastníci, správci a uživatelé, stejně jako lokální a globální komunity.“ [101]

Zcela komplexní definice, která asi nejlépe vystihuje nutnost provázání architektonické, technologické a systémové stránky komplexní IB.

Z pohledu systémového integrátora systémů IB se zaměřením na bezpečnostní systémy lze považovat definici **European Smart House Standards Group** (*definice I.*) doplněnou o konkretizaci **EIBG** (*definice V.*) jako nejvhodnější a při následujícím popisu a návrhu bude z této definice vycházeno.

Nejednoznačná definice IB je dnes celosvětově poměrně velký problém, neboť velká část komerčních investorů produkuje pod názvem „inteligentní budova“ či „smart budova“ objekt, který je spíše pouze automatizovanou budovou se zvýšeným uživatelským komfortem a sníženou spotřebou energií[12]. Znamená to tedy, že budova i nevýrazných kvalit (velké tepelné ztráty, špatná orientace ke světovým stranám, nevhodné materiály,…) vybavená technologiemi a moderním systémem řízení, je také inteligentní budovou? Je smutné, že řada velkých firem, developerů a systémových integrátorů stále více toto tvrzení, zjevně pod komerčním tlakem, podporuje a uvádějí tak do provozu budovy, které se skutečně IB nemají téměř nic společného.

Pokud se jedná o malé instalace, jako jsou rodinné domy či menší objekty s jednoduchým provozem, je možné zmíněných požadavku dosáhnout pomocí nabízených řešení, za předpokladu, že návrh a realizace systému je provedena s ohledem na všechny souvislosti. Je však samozřejmé, že ani v tomto případě se nebude jednat o IB, ale pouze o budovu automatizovanou[16].

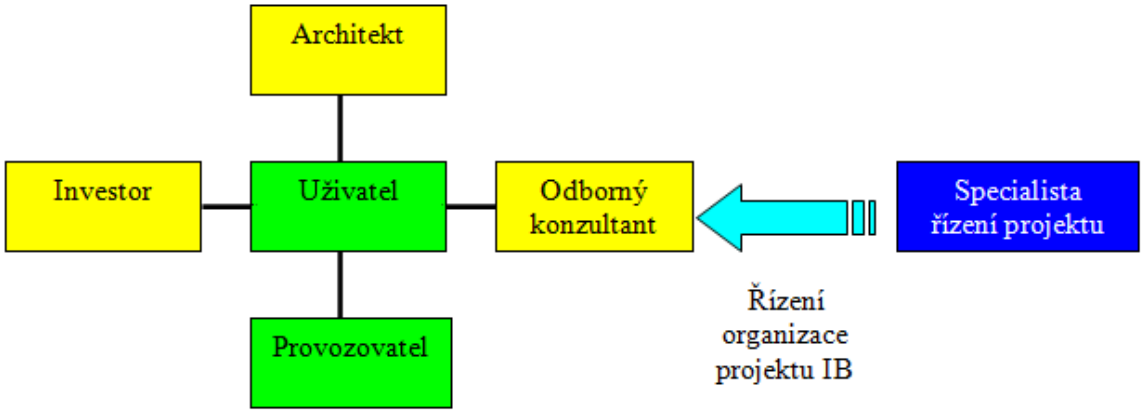
U větších objektů a rozsáhlých instalací je situace ještě nepřehlednější. Dodavatelů schopných dodat rozsáhlé instalace je omezené množství a samotná schopnost dodat takto rozsáhlý systém neznamená, že dojde ke snížení energií v budově a ke zvýšení komfortu. Je bohužel často faktem, že nasazení této technologie přinese naopak nejenom zvýšení pořizovacích nákladů, ale i nákladů provozních[16]. A uživatelský komfort je pak spíše iluzí, resp. vyžaduje opravdu dobře zaškoleného uživatele objektu (uživatelé jsou

obtěžováni neustálým rozsvěcením a zhasínáním světel a pohybem žaluzií, které reagují na světelné podmínky či na rychlost větru). Rovněž se stává, že nesprávně navržené systémy (či chybně odladěné systémy) zároveň chladí i topí v jednom objektu (či dokonce jedné části objektu) [1].

Tyto problémy jsou způsobeny především tím, že dodavatelé se při realizaci IB neřídí žádnou definicí IB a používají tento termín zcela volně, spíše jako marketingový, reklamní pojem. Dalším vážným problémem je, že celý proces realizace IB (tzn. zadání projektu, návrh řešení a zpracování dokumentace, realizace stavby, uvedení do provozu a užívání stavby) není kompetentně řízen a hlavně popsán. Při realizaci IB, je důležité znát body, ve kterých musí být učiněna domluva účastníku realizace IB, aby nedocházelo k zásadním chybám, které způsobí, že nebudou naplněny cíle projektu. Musí být jasně stanoven způsob komunikace a informačních toků v rámci přípravy projektu a po celou dobu její realizace.

Minimálně po dobu **přípravy projektu** musí být jasná komunikace dle následujícího schématu:

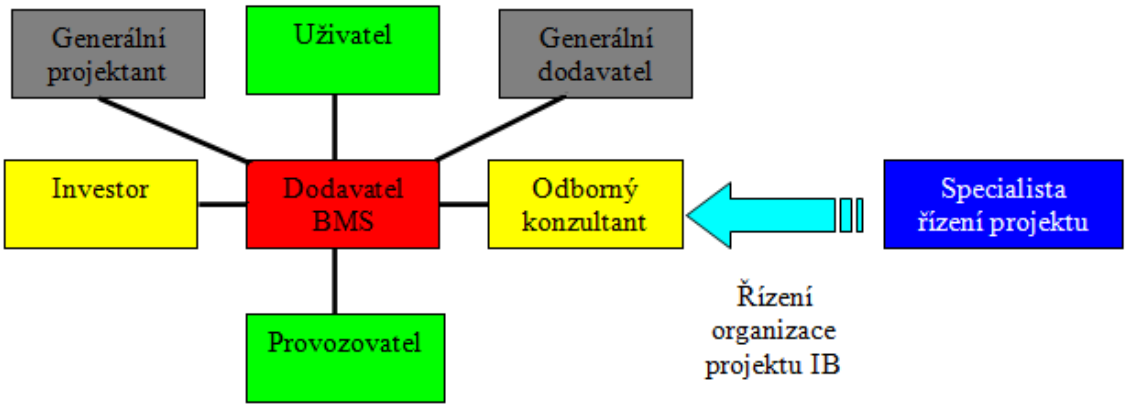
Obr. 2 *Schéma vztahů při návrhu projektu IB*



Zdroj:upraveno dle [52],[53],[101]

V okamžiku realizace projektu je potřeba koordinace a spolupráce mnohem vyšší, minimálně podle následujícího schématu.

Obr. 3 *Schéma vztahů při přípravě technické dokumentace projektu IB*



Zdroj: upraveno dle [52],[53],[101]

Na základě těchto informací a komunikace pak může skutečně vzniknout IB, jejímž přínosem bude především usnadnění a zpříjemnění obývání domu jeho uživatelům, a to za současného snížení energetické náročnosti a výrazného snížení ekologické zátěže.

Problematické tak tedy není překvapivě vlastní technické řešení konkrétní integrace jednotlivých systému IB, ale její korektnost a dlouhodobá spolehlivost a funkčnost. A to jsou právě největší problémy, na které se naráží při pokusu o integraci poplachových systémů do informačních systémů IB, tedy snaha integrovat zabezpečovací systémy (PZTS), kamerové systémy (CCTV) přístupové systémy (ACC), protipožární systémy (EPS), asistivní systémy (SMA) a další[11]. Problém ve funkcionalitě a především legislativě a normách je pak téměř neřešitelný.

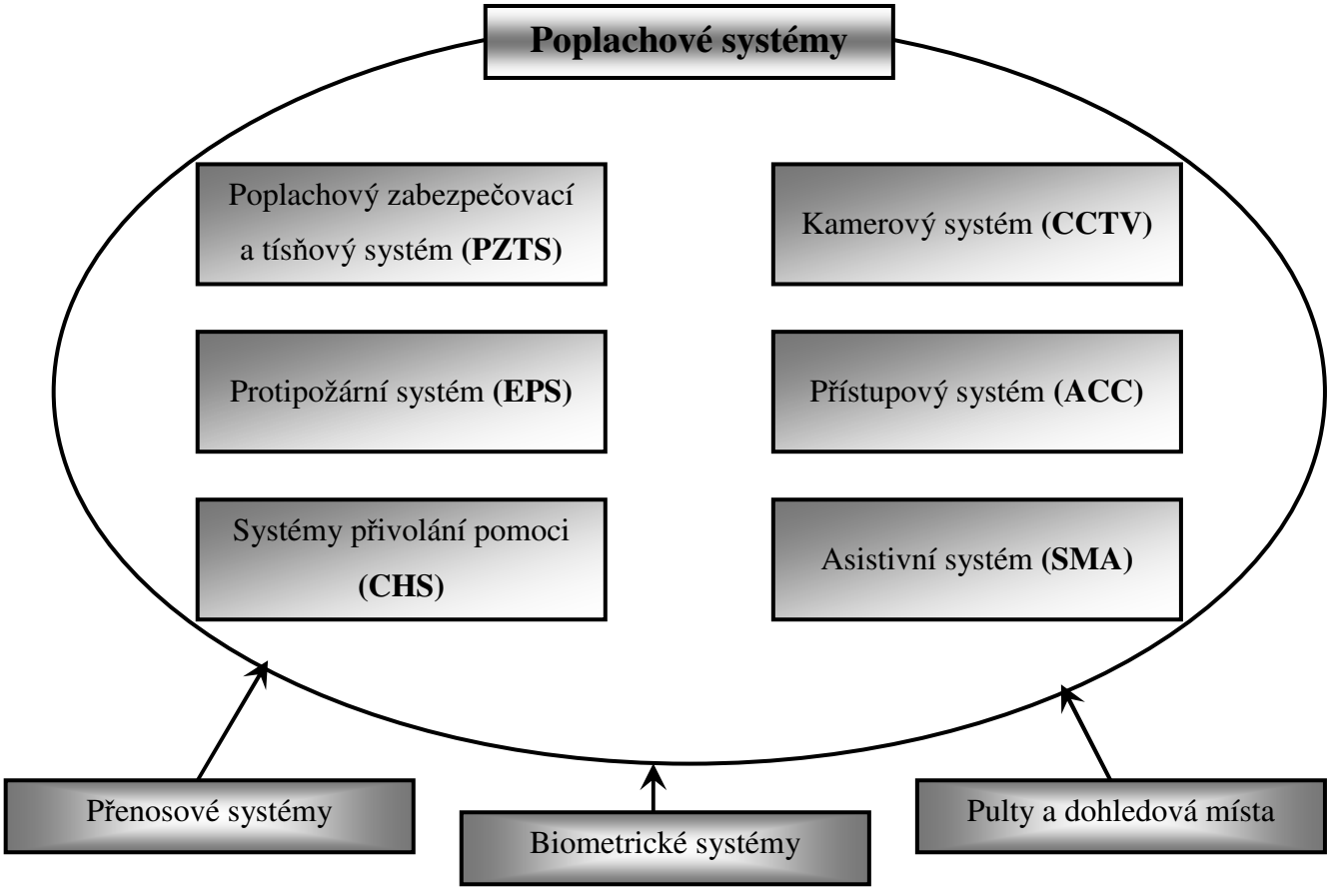
1.2 Poplachové systémy

Na tomto místě je potřeba zdůraznit, že terminologie v oblasti bezpečnostních systémů (či obecněji poplachových systémů) se jednak poměrně rychle mění, jednak je různými autory různě vykládána. Pro přehlednost bude užívána nejčastěji používaná terminologie vycházející z historicky původního definování pojmů, byť v některých případech neodpovídá zcela normativními názvosloví.

Především pojem poplachové systémy je sice normou předepsaný, ale poměrně nepřesný[48]. Řada systémů, které patří do této kategorie poplachových systémů,

poplachové události negeneruje. Je osobním názorem autora, že dříve používaný pojem bezpečnostní systémy byl mnohem přesnější a odpovídal i spíše původnímu anglickému výrazu. Do této kategorie systémů tedy patří všechny systémy, které se přímým způsobem podílí na zajištění bezpečí a vnitřní pohody jedince užívající daný objekt. Vychází tedy z klasického zabezpečovacího systému (dnes označovaného pojmem poplachový zabezpečovací a tísňový systém), kdy postupem času a použitím se právě vlivem automatizace bezpečnostních činností vyvinuly další samostatné systémy – viz následující schéma.

Obr. 4 *Poplachové systémy a související prvky*



Zdroj: [113]

Základních šest systémů je tedy spojeno pod jedním pojmem (Poplachové systémy) s tím, že další pomocné systémy mohou podporovat činnost každého z uvedených systémů. V posledních několika let se k těmto doplňujícím systémům někdy připojuje i systém tak

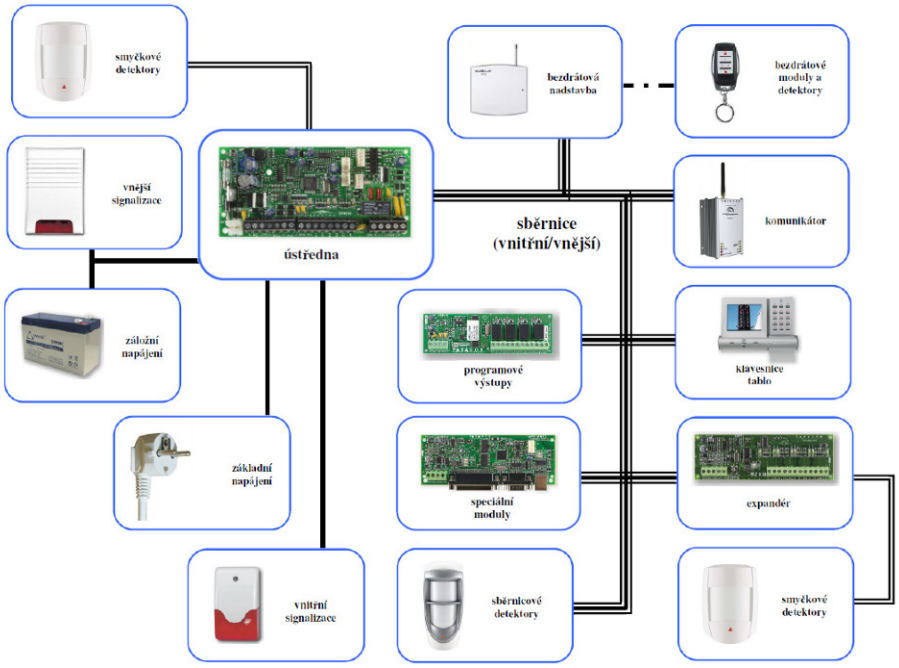
zvané telemedicíny, její zaměření a použití však dle autorova názoru stojí zcela mimo poplachové (či bezpečnostní) systémy.

Při rozboru PZTS (jako klíčového a nezbytného prvku poplachových systémů) je potřeba analyzovat jeho vývoj.

Základy pro moderní **zabezpečovací systémy** byly položeny v roce 1853, kdy Augustu Pope patentoval první elektrický zabezpečovací systém, který v roce 1857 prodal E.T. Holmesovi. [33], [49] Tento skvělý vizionář v oblasti zabezpečovacích systémů přispěl nejenom k modernizaci a rozvoji zabezpečovacích systémů, ale svou osvětovou činností podpořil i výrazné rozšíření znalostí o jejich funkci a rozvoj. Pod jeho vedením vznikla např. v Bostonu a později i v New Yorku první síť propojující jednotlivé zabezpečené objekty, tedy při použití dnešní terminologie pulty centrální ochrany (PCO). Zajímavé je, že na těchto rozvodech o pět let později testoval Graham Bell možnost přenosu lidského hlasu a úspěšně tak otestoval funkci telefonního přístroje[49] . Až do 50. let 20. století byly zabezpečovací ústředny (a vlastně i detektory) zásadně postaveny na reléových obvodech. Rozvoj elektroniky v období druhé světové války se výrazně a především velice rychle projevil i v zabezpečovacích systémech, a to jak na straně čidel, tak i ústředen. Objevují se nové typy detektorů (VKV prostorová čidla, posléze známé PIR detektory a infrabariéry, mikrovlnné detektory, optické závory), ústředny se stávají plně elektronizovány, byť logika přenosu poplachové informace se nemění[49].

S rozvojem bezdrátového přenosu se tato technologie postupně zavádí i do přenosových tras zabezpečovacích systémů i když aplikační důsledky nejsou vždy pozitivní[107], [108].V dnešní době je již celkem přesně definována a legislativně stanovena činnost a funkce zabezpečovacích systémů (dříve označovaných jako EZS, nyní PTZS) [65] i protipožárních a hasicích systémů (EPS a SHZ), bouřlivým vývojem a normalizací v současnosti prochází oblast kamerových systémů (především IP kamer, ale i CCTV). Jednotliví výrobci i specializované společnosti se pokoušejí o jistý stupeň propojování systémů, narážejí však na významné technické, technologické a především legislativní (a bohužel i pádné komerční) problémy[11]. V následujících kapitolách je právě tento klíčový problém rozpracován podrobněji, neboť je zcela rozhodující pro řešení problému popsané v této práci.

Obr. 5 *Blokové schéma typického zabezpečovacího systému*



Zdroj: [109]

1.3 Technologické systémy

Automatizace objektu, ať se již jedná o topení, větrání, stínící techniku, nebo o technologie výrobní (technologické linky) se objevují již s prvním objevem regulačních členů (viz použití korčáku v mlýnici – 15. století či například novější využití Wattova regulátoru - r.1765)[16]. Masivního rozšíření se však dočkala až s nástupem polovodičových prvků. (r.1947 – první tranzistor, r.1958 – první integrovaný obvod). Zvláště v období konce 20. století řada společností (Siemens, Bosch a další) prezentuje a zavádí do běžné výroby technologické linky s plně automatizovaným řízením [67], [54], [100]. Drtivá většina těchto koncepcí je však založena na principu centrálního počítače a lokální sítě. To s sebou nese dva základní problémy:

a) nedostatečnou spolehlivost a robustnost řešení,
b) problém s integrací nových prvků a komponent do systému.

Proto je v dnešní době výrazný ústup od centralizovaného systému řízení směrem k systémům distribuovaným. To, při jednoznačně definovaném rozhraní (interface), v praxi

přináší především možnost téměř neomezeného propojování různých systémů a částí, na druhé straně to však přináší mnohem větší nároky na kvalitu provedení především v projektové části[63]. I z tohoto důvodu řada (především větších) společností stále ještě nabízí řízení technologií centrálním počítačem. V současné době, kdy dochází k trvalému rozšiřování a modernizaci informačních systémů budov, se však již jedná o technologii výrazně zastaralou a své uplatnění nalezne spíše u menších objektů, rodinných domů či nenáročných kancelářských objektů. Centralistický přístup při řešení informačních systémů IB je v řadě významných indikátorů (např. flexibilita) pro většinu aplikací nevhodný a v mnoha případech i legislativně neprůchozí[72][101] .

Výsledky této disertační práce tak mohou být využity i pro doporučení konstruktérům, servisním a provozním technikům, především však projektantům a pracovníkům v legislativě a normotvorbě.

2 PŘEHLED SOUČASNÉHO STAVU PROBLEMATIKY INTEGRACE BEZPEČNOSTNÍCH SYSTÉMŮ

Je zřejmé, že snaha o integraci bezpečnostních systémů či alespoň jejich prvků je klíčová pro reálné a plnohodnotné vytvoření informačního systému budovy, který lze dle výše uvedených definic označit jako systém inteligentní budovy. Současná situace je však poměrně nepřehledná – existuje velká nabídka technologií i praktických řešení, existují alespoň základní legislativní a normalizační předpisy a začíná již fungovat i poměrně velké množství budov označovaných jako tzv. „inteligentní". Je ale bohužel stále výraznější, že legislativa, normy a použitá technická řešení stojí velice často zcela proti sobě. Což samozřejmě u bezpečnostních systémů nelze dopustit[16]. Je tedy nejdříve nezbytné na tomto místě definovat kritická místa pro integraci bezpečnostních systémů – tedy stanovit kritické performační indikátory pro zavedení uvažovaných systémů[63].

2.1 Inteligentní budova

Jak je uvedeno v Kap. 1, přesná a obecná definice pojmu inteligentní budova je poměrně problematická. Pro závěry této práce byla využita modifikovaná definice **European Smart House Standards Group** (*definice I.*) doplněna o konkretizaci **EIBG** (*definice V.*). Pro konkrétní potřeby této práce postačí, když problematika IB bude zjednodušena pouze na hledisko architektonické, automatizační a komunikační.

Z **architektonického hlediska** se jedná o budovu, která svým řešením zajišťuje maximální energetickou úspornost. Je samozřejmě celá řada způsobů jak tohoto dosáhnout. Od základního umístění budovy, přes jeho orientaci, použité materiály, zvolené stavební technologie, až po svědomité a precizní provedení práce. Tato definice není sama o sobě pro problematiku informačních systémů podstatná, důležitý je však její důsledek. ***Již od počátku projektu musí být zřejmé, že se bude jednat o stavbu inteligentní budovy***. Pokusy implementovat pokročilou integraci vnitřních systémů do stávajících běžných budov se sice poměrně často realizují, výsledky jsou však spojeny s mnoha problémy a značnými finančními náklady.

Z pohledu **vnitřních systémů** je termín „inteligentní budova" vyhrazen pro takový objekt, kde soubor všech (většiny) instalovaných systémů (PZTS, CCTV, ACC, EPS, klimatizace, vytápění, stínící technika, multimedia, počítačové a komunikační systémy) je propojen do jednoho ovládacího prvku (toto samozřejmě nedefinuje vlastní pojem

inteligentní budovy, specifikuje to však uživatelský dopad takového projektu). Tím lze nejen ušetřit určité náklady na samostatnou instalaci jednotlivých systémů, ale také výrazně eliminovat redundantní ovládací prvky[72], [78]. Tímto sloučením lze dosáhnout značného zjednodušení ovládání a zpravidla se výrazně zvýší i funkcionalita a design vnitřních prostor objektu.

To však nejsou jediné důvody pro zavedení integrace těchto systémů. Pro budoucího majitele objektu je především důležitá (byť i částečná) **úspora energií**. Inteligentní termostaty mohou například regulovat teplotu v celém domě podle potřeby (osvit sluncem, přítomnost osob, vliv dalších zdrojů tepla) v konkrétních, právě užívaných místnostech. U soukromých objektů je například zajímavé, pokud lze ohřívat teplou užitkovou vodu pouze, pokud je někdo v domácnosti; lze odpojit vyhřívání radiátorů v místnostech, kde je otevřené okno (zdroje dat z bezpečnostních systémů). Systémové instalace jsou stále ve větší míře nasazovány nejen k řízení osvětlení, žaluzií, vytápění, klimatizace, ventilace (a podobných funkcí budov), ale spolupracují s celou škálou dalších funkcionalit, jakými jsou sluneční kolektory nebo fotovoltaické články. Kooperují také se systémy PZTS a EPS, přičemž tyto funkce mohou zajišťovat bez nutnosti používání nezávislých bezpečnostních systémů. Stále běžnější je spolupráce i s moderními audio a videosystémy. Budoucností systémových instalací je zvládnutí všech funkcí, které jsou vytvořeny pro komplexní činnost budovy a jejího okolí. Současné představy zacházejí dokonce do situací, kdy takto pojatá instalace bude samostatně rozhodovat („myslet“) - bude bezprostředně reagovat na chování, jednání a pocity uživatelů objektu. Teprve tehdy bude skutečně pravdivý doposud snad neoprávněně používaný termín „inteligentní instalace“. První pokusy v této oblasti se již v dnešní době vyskytují – za připomenutí stojí např. systém **STAY-D** kanadské firmy Paradox Ltd. [102]. V tomto systému, v závislosti na chování uživatele objektu, se upravuje nastavení chování bezpečnostního systému. Tento systém není nutné obvyklým způsobem zapínat a vypínat, do jisté míry předpovídá požadavky na zabezpečení objektu pouze podle pohybu (chování) osob v objektu[82].

I když projekty inteligentních budov (IB) jsou již v dnešní době poměrně populární, jejímu masivnímu rozšíření brání některé překážky. Nejpodstatnější je zřejmě v oblasti technologie řízení inteligentního systému[11]. Principiálně existují dva způsoby řízení systému IB.

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 informačního systému (IS) s centrální správou. Kritické jsou však obtíže při rozšiřování systému, jeho modernizaci a při integraci nových modulů. Zásadní problém je pak při rozboru spolehlivost celého centrálního systému. Situace v tomto případě lze připodobnit pokusu o globální řízení toku dat na Internetu pomocí jednoho centrálního počítače (i za předpokladu odpovídající propustnosti). 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. Tento způsob má celou řadu výhod především z perspektivy rozvoje – lze bez problému doplňovat nové moduly (se standardní sběrnicí), projektant, ani následně uživatel objektu, není vázán na dané konkrétní řešení konkrétního výrobce, lze poměrně snadno definovat závady a „úzká“ místa systému. Základní nevýhodou je nutnost důsledné předběžné analýzy informačního systému daného objektu, kvalitně navržená a realizovaná instalace a dobře zaškolená obsluha. Běžně i cena tohoto řešení bývá výrazně vyšší, než centrální systém řízení budovy.

Centralizovaný systém[52] tedy obsahuje centrální řídící 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, nepříznivě ovlivněná spolehlivostí centrální jednotky a nezálohovanou architekturou.

Decentralizovaný systém[52] obsahuje jednotlivé prvky propojené komunikační sběrnicí, 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.

2.1.1 Porovnání klasické elektroinstalace a inteligentní sběrnice řízeni IB

Klasická elektroinstalace patří v ČR i ve světě jednoznačně k nejpoužívanějším. Je realizována za pomocí silového vedení, které zároveň slouží i jako zdroj elektrické energie a neumožňuje měnit funkce systému bez zásahu do zapojení. Tímto řešením lze přenášet ve většině případů pouze základní stavové informace (např. informaci typu zapnuto/vypnuto).

Funkce každého jednotlivého spínače (tlačítka) je pevně dána tím, k jakému zařízení je připojen (jak jsou položeny kabely). Pro přenos jiného typu informace je potřeba instalovat další vedení pouze pro tuto konkrétní situaci. Jakákoliv změna znamená zásah do instalace (vložení dalšího kabelu) nebo do budovy (stavební úpravy, sekání omítek, lištové či podparapetní rozvody). Při návrhu je elektroinstalace navrhována pro jednotlivé zařízení s jedním účelem. Systémy nejsou kompatibilní a většinou mezi sebou nekomunikují, což vede ke snížení komfortu uživatele[52] [93].

Celkové shrnutí:

Nevýhoda:

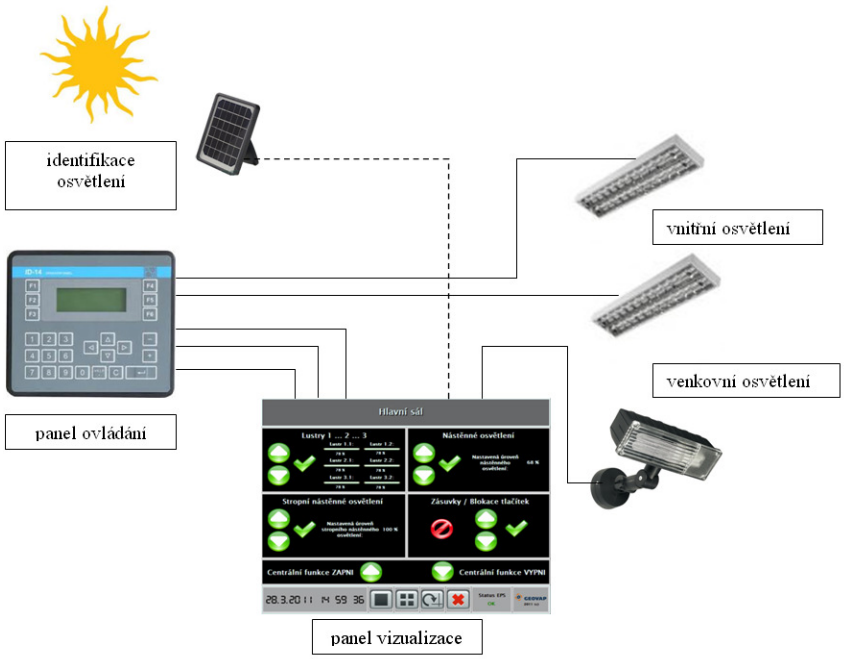
- nelze měnit bez nutnosti stavebních prací, každý nový prvek znamená samostatné vedení kabeláže,
- není možné požadovat žádné další rozšiřující funkce,
- je velice problematicky možný dálkový dohled a řízení systémů.

Výhoda:

- je možná kombinace s novými prvky z oblasti inteligentní elektroinstalace,
- je možné propojovat systémy podporující obnovitelné zdroje energie (tepelná čerpadla, solární panely, domácí větrné elektrárny).

Celkově je tedy tento systém vhodný pro tradiční budovy bez požadavků na úsporu energií s komfortem obsluhy spíše pro méně náročné uživatele.

Obr. 6 *Princip klasické elektroinstalace*



Zdroj: upraveno dle [52][100][101]

Rozvody **inteligentních instalací** jsou založeny na principu datové sběrnice, pomocí které jednotlivé moduly mezi sebou komunikují a mohou se navzájem ovlivňovat. Uživatel pak ovládá pouze jeden systém (uživatelský interface), pomocí kterého řídí všechny ostatní systémy. Jedná se o otevřený kompatibilní systém, který umožňuje i podstatné změny bez zásahu do stavební části či systému. Navíc v řadě případů mohou jednotlivé prvky komunikovat bezdrátově, čímž odpadá nezbytnost klasické drátové kabeláže, byť za cenu zvýšených nákladů na realizaci[66]. V tuto chvíli je úmyslně pominuta problematika datových komunikací po silovém vedení (např. KNX/PL), tato část je podrobně rozpracována v kapitole 2.2.1 až 2.2.4.

Celkové shrnutí:

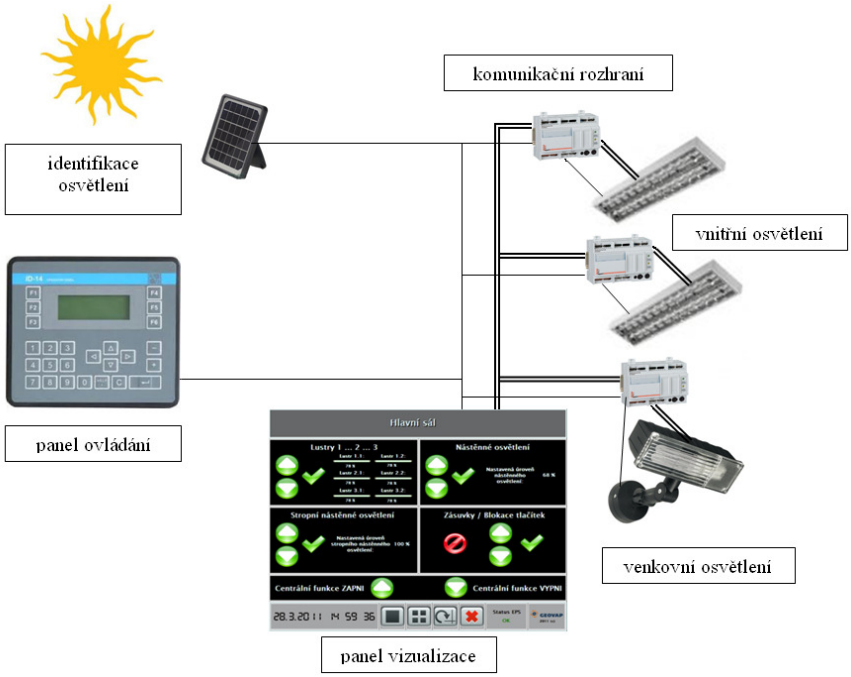
Nevýhoda:

- dražší než klasická instalace.

Výhoda:

- jednodušší instalace,
- je možné propojovat systémy podporující obnovitelné zdroje energie (tepelná čerpadla, solární panely, domácí větrné elektrárny) s přímou návazností na ovládání dalších systémů,
- lze přehledně konfigurovat pomocí uživatelského programu,
- podpora bezdrátového přenosu informace,
- rozměrově menší prvky,
- spřažení více funkcí na jednom prvku.

Obr. 7 *Princip inteligentní elektroinstalace*



Zdroj: upraveno dle [52][100][101]

2.1.2 Typy budov dle návrhu koncepce IB

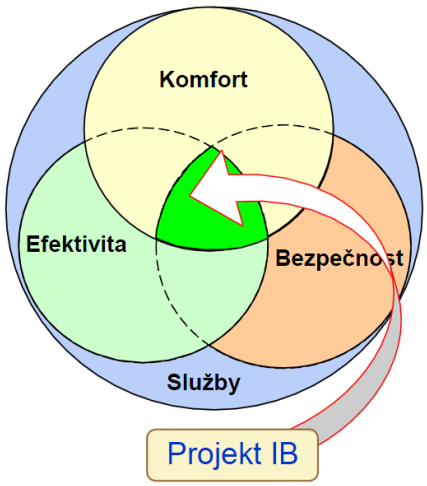
Z výše uvedených faktů jasně vyplývá, že při návrhu koncepce struktury informačního systému inteligentní budovy (ISIB), lze využít celou řadu možností (technologií), z nichž každá má své výhody. Je tedy vždy potřeba zohlednit jednotlivá kriteria při rozhodování tak, aby byl vybrán optimální model. V praxi se velice často využívá výběr technologie podle následujícího modelu[66].

Při návrhu typu systému IB se zohledňují tří základní požadavky [67]:

- komfort prostředí,
- energetická efektivnost a ekologičnost provozu,
- bezpečnost.

Tyto požadavky se zpravidla znázorňují grafem, ve kterém se určí primární kriteria. Následně je pak identifikovatelný typ vhodného systému pro konkrétní užití budovy.

Obr. 8 *Výběr vhodné technologie systémů IB*

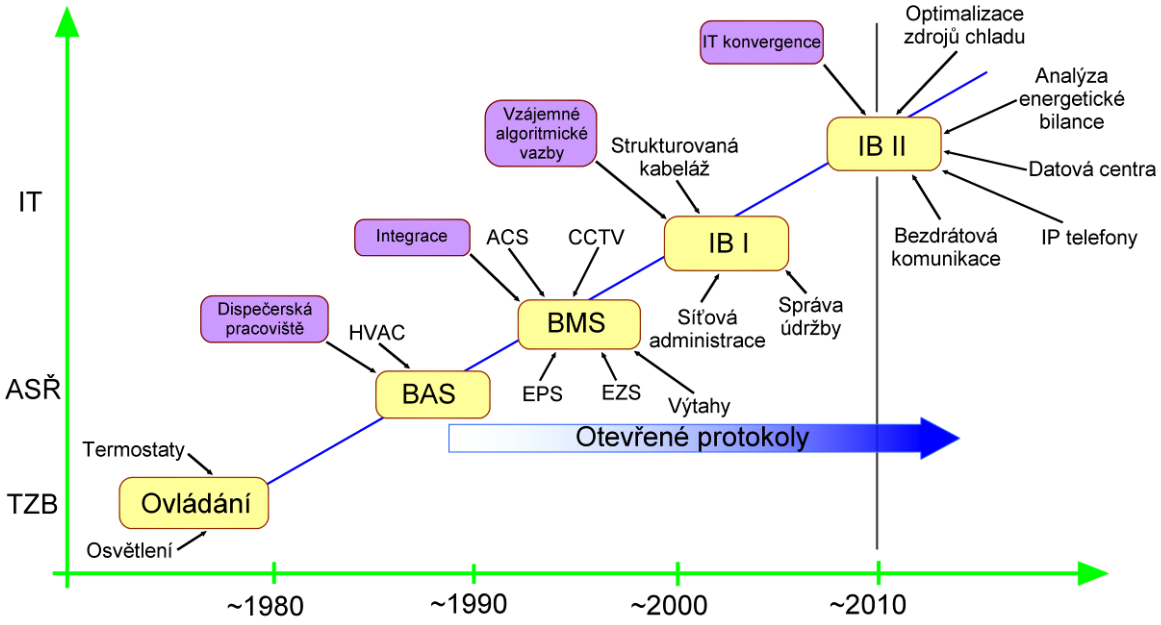


Zdroj: [67]

Je logické, že při instalaci systému např. do kancelářských budov se zohlední především kriterium efektivity, při instalaci do výrobních a chráněných budov spíše kriterium bezpečnosti a při instalaci do rodinných domů a konferenčních budov spíše kriterium komfortu. Tím je zároveň v podstatě definován jak druh, tak i topologie předpokládaného systému. S postupným vývojem technologií a moderních konstrukčních prvků, se vyvíjí i jednotlivé „šablony“ využívané v projektu systémů IB.

Stále více se projevuje probíhající konvergence jednotlivých technologií, což demonstruje následující graf.

Obr. 9 *Konvergence technologií v projektech IB*



Zdroj:[16]

2.1.3 Sběrnice pro systémy IB

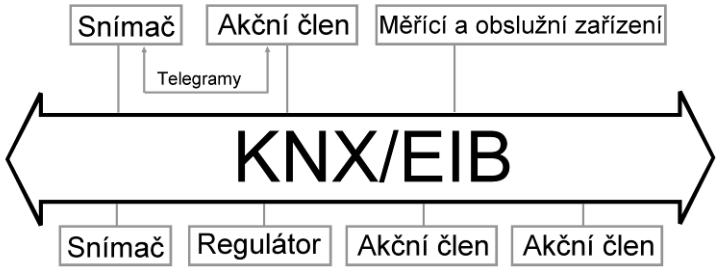
Aktuálně se využívá několik různých řešení, která jsou vázána na konkrétního výrobce či skupinu výrobců a i když je v řadě případů deklarována kompatibilita dle daného standardu, v reálné praxi je tento problém velice často poměrně vážný (což potvrzují i výsledky měření použitá v této práci). Některá komerčně nabízená řešení jsou přitom z uživatelského pohledu v podstatě identická. Po technické stránce se liší většinou pouze počtem využitelných prvků a jejich propojením [63].

2.1.3.1 Sběrnice KNX/EIB

Evropská sběrnice KNX/EIB je průmyslový komunikační systém, který se v systémové technice budov používá pro síťové informatické spojení zařízení (snímačů, akčních členů, regulačních a řídících zařízení, obslužných a měřících zařízení). Implementace KNX/EIB je přizpůsobena elektrotechnické instalaci, čímž jsou zajištěny funkce a automatizované procesy v budově[98]. Výměna informací probíhá mezi jednotlivými systémy přímo. Data jsou vkládána do datového telegramu a digitálně

přenášena pomocí sběrnice (viz Obr.10). Každý prvek má jedinečnou fyzickou adresu sloužící k identifikaci. Komunikace probíhá pomocí telegramu obsahující instrukce pro daný prvek. Tento telegram je konfigurovatelný programem. Sběrnice může být jakékoliv topologie s podmínkou, že délka jedné větve nebo linie je do 1km s maximálním počtem prvků 64. Tento systém je určený pro budovy komerčního využití nebo do velkých a luxusních staveb obytného charakteru. [64] [33]

Obr. 10 *Princip telegramu sběrnice KNX/EIB*



Zdroj: [64]

Sběrnice mohou být:

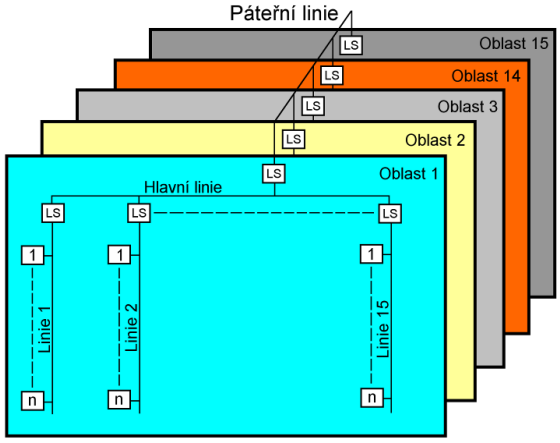
- **KNX/TP** kabel – Twisted Pair (kroucený pár metalických vodičů). Nejpoužívanější provedení KNX sběrnice. Jde o kroucený metalický pár vodičů. Rychlost komunikace na sběrnici tohoto typu je 9 600 bps,
- **KNX/PL** – Power line (silové vedení). Vedení je realizováno pomocí silového vedení 230 V. Rychlost přenosu dat po tomto typu sběrnice je 1 200 bps,
- **KNX/RF** – rádiové spojení. Bezdrátová komunikace mezi prvky probíhá na frekvenci 868 MHz. Výhodou je že odpadá instalace kabeláže. Rychlost komunikace je 16 000 bps,
- **KNX/IP** – Ethernet, KNX telegramy mohou být vysílány jako součást IP telegramů, z čehož vyplývá, že k jejich přenosu je možné využít sítě LAN nebo Internet. Proto je možné použít IP routery jako alternativu k USB převodníkům, případně je možné páteřní TP linii nahradit rychlejší ethernetovou linkou,
- **KNX/FG** - Optická vlákna.

Do nových staveb se většinou instaluje typ KNX/TP. Další dvě sběrnice KNX/PL a KNX/RF se využívají při dodatečné instalaci například při rekonstrukci budov. Přístroje, které komunikují pomocí KNX/EIB se obvykle rozdělují na dvě skupiny – sensory (vysílače) a aktory (přijímače).

Systémová technika s KNX/EIB klade mnohem menší nároky na kabeláž než klasické rozvody. V současnosti již prakticky pro každé technologické zařízení budov existuje varianta, která je normalizovaná s KNX/EIB. Tato zařízení jsou sice poněkud dražší, mají však lepší hospodárnost, lepší návaznost mezi s sebou a jsou zejména vhodná, pokud je nutné uvažovat o dynamickém přizpůsobení a zapojení (změna topologie, počtu uzlů a jejich typ).

Páteřní linie je složena z jednotlivých oblastí. Oblasti jsou složeny z hlavních linií a dalších příslušných vedení. Např. jedno patro rodinného domu lze pak považovat za jednu oblast systému. Všechny přístroje v každé místnosti na daném podlaží jsou potom postupně připojeny na hlavní linii oblasti. Propojení všech podlaží je páteřní linií. [1] [67]

Obr. 11 *Topologie sítě KNX/EIB*



Zdroj:upraveno dle [67]

Klasickým příkladem využití této sběrnice je automatizace v oblasti osvětlení a stínící techniky, kdy při vhodné implementaci lze dosáhnout až 60% úspory elektrické energie v závislosti na denním světle. V ČR (i ve světě) tento způsob integrace prodávají především společnosti, které jsou součástí ABB Group. [67] [33] [99] [100]

Hlavní výhody sběrnice KNX/EIB jsou:

- kompatibilita výrobků různých firem,
- jednoznačná certifikace,
- jednotné uvedení do provozu.

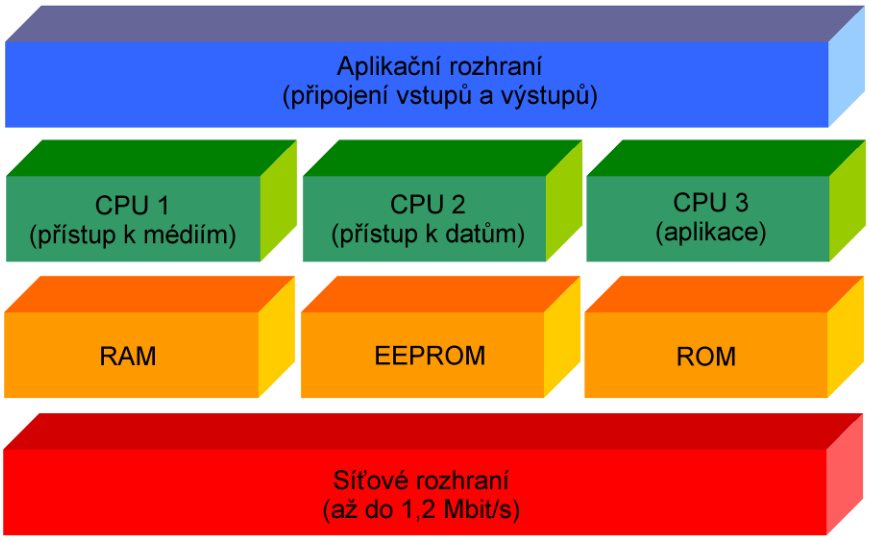
2.1.3.2 Sběrnice LONWORKS

Americkým přínosem do oblasti inteligentních komunikačních decentralizovaných sběrnic je standard **LON** (Local Operating Network). Byl vytvořen společností Echelon[69] počátkem 90. let minulého století jako univerzální a levné komunikační spojení pro různá technická vybavení budovy na nejnižší automatizační úrovni. Cílem pak byla výroba čipu s názvem ***Neuron***, obsahujícího všechny potřebné funkce. Použitý protokol se nazývá **LonTalk** a celá technika se označuje souborně jako **LonWorks**[43]. Topologie je odvozena z teorie počítačových sítí, stejně tak jako pravidla přenosu telegramu v těchto sběrnicích. V Evropě se tento systém rozšířil právě jako komunikační sběrnice v IB. Jeho použití je však výrazně širší, známé jsou např. aplikace pro řízení vlakové dopravy realizované nad touto sběrnicí. [37] [93]

Základní výhoda tohoto systému je v tom, že zařízení, která jsou v systému použita, mají vlastní „inteligenci“ a jsou napojena na běžnou počítačovou síť. Díky tomu je možné, i když sběrnice LONWORKS je striktně sběrnicová (dle standardu EN 14908), využít „klasickou“ počítačovou stromovou strukturu, což výrazně zjednoduší (=zlevní) vlastní instalaci i následné oživení systému. Protože základem této technologie je zmíněný chip “Neuron“, lze použít téměř jakékoli přenosové médium bez nutnosti určení komunikačního protokolu mezi komponenty. Čipy jsou již při výrobě vybaveny protokolem LONTALK, který popisuje, jak mezi sebou jednotlivá zařízení komunikují a jakým způsobem se dají programovat. Tento protokol zajišťuje univerzálnost a tak lze propojovat i zařízení od jiných výrobců, pokud rovněž splňují podmínku kompatibility s protokolem LONTALK.

Z pohledu technického provedení je síť LON přísně strukturovaná. Základní jednotkou sítě je uzel (node), se svou základní jednotkou – čipem. Pokud zařízení sítě LON (např. výkonný modul DDC) obsahuje více čipů, pak každý jednotlivý vestavěný čip představuje samostatný uzel sítě.

Obr. 12 *Vnitřní struktura čipu LON*



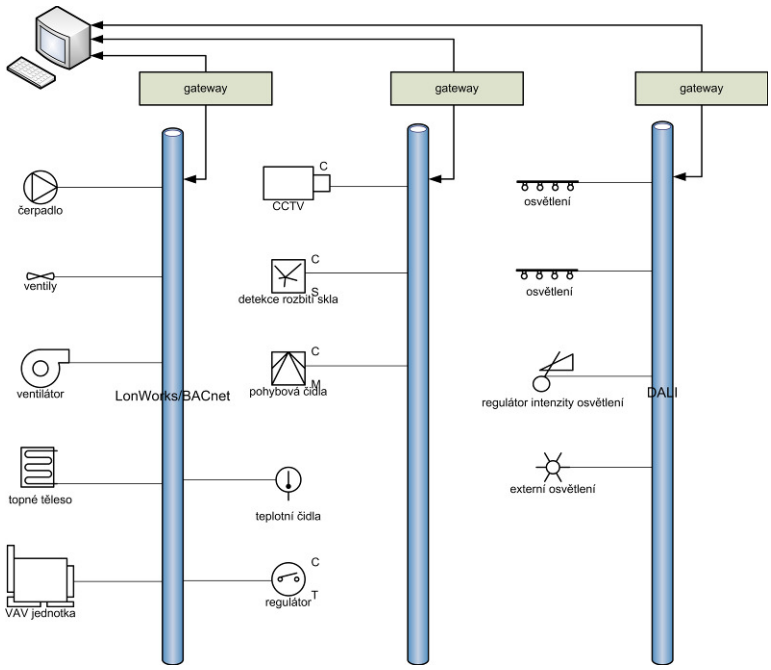
Zdroj: upraveno dle [8]

Podobně jako je tomu u počítačových sítí, tak i u sběrnice LONWORKS si lze vybrat požadovanou topologii, která by nejvhodněji splňovala požadavky zákazníka (či spíše projektanta). Pokud je kladen důraz na maximální potřebnou délku sběrnice, je vhodné použít topologii sběrnicovou. V tomto případě lze zrealizovat vedení o délce až 2700 m v závislosti na použitém vodiči. Stejně jako v počítačové sběrnicové topologii se i zde musí vedení zakončit tzv. terminátory, které zabraňují zpětnému odrazu signálů do sítě. V rozsáhlejších automatizacích budov se více používají hvězdicové nebo kruhové topologie. Zde je maximální délka sítě výrazně nižší než u sběrnicové topologie (cca 500 m), přičemž maximální délka vedení mezi jednotlivými uzly nesmí být delší než 320 m. Tyto topologie nacházejí uplatnění nejvíce v objektech, kde se postupně instalují další komponenty infrastruktury. U kruhových a hvězdicových LON sítí je potřeba věnovat pozornost na dodržení správné polarity, aby nedošlo ke zkratu rozvodů. [33]

Komunikace v sítích typu LON probíhá pomocí komunikačních proměnných (Network Variables). Síťové proměnné se musí správně definovat (v lepším případě i s jednotkami) aby nedocházelo ke kolizím. Správné definice síťových proměnných se určují podle oblasti použití, struktury proměnných, celkové délky datového telegramu, a rozsahu hodnot. Příkladem použití může být např. průtok vody, nebo nastavená teplota pro vytápění či klimatizaci.

V praxi se sběrnice LON s výhodou využívá v aplikacích, kde je kladen nárok na délku sběrnice (nikoliv na rychlost přenosu dat). Základní využití sběrnice je v případě propojování různých systémů (vytápění, CCTV, přístupové systémy, řízení spotřeby energií, apod.). Pro připojení sběrnice LON do PC je nutné použít vhodný adaptér. Adaptérem jsou data transformována ze sběrnice do příslušného vizualizačního systému, který data zobrazuje[72].

Obr. 13 *Celkové schéma implementace LON v projektu*



Zdroj: [18]

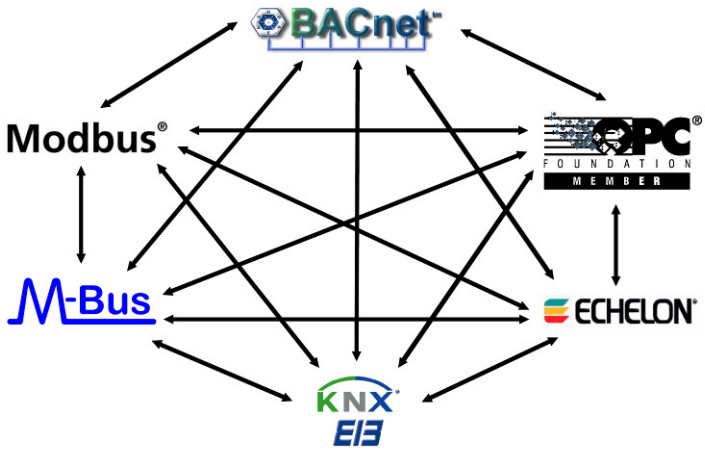
2.1.3.3 Komunikační protokol BACnet

Označení BACnet (Building Automation and Control Network) se využívá pro identifikaci standardizovaného komunikačního protokolu využívaného pro automatizační a řídící systémy budov, ve kterém si zařízení a systémy mohou vzájemně vyměňovat informace. Tento komunikační protokol byl vyvinut společností American Society of Heating, refrigeration and Air - Conditioning Engineers a v roce 1995 byl standardizován[70]. Společný jazyk BACnet se rozšířil v mnoha aplikacích po celém světě a od 1.8. 2004 byl normalizován i v ČR jako ČSN EN ISO 16484-5[10].

Celý protokol a veškerá komunikace je založena na objektovém přístupu. Komponenty jsou reprezentovány objekty, které mají svoje vlastnosti a služby. Výhodou

tohoto protokolu je nezávislost na komunikačním prostředí. Z Obr.14 je zřejmé, že tento protokol je možné využít s jakýmkoliv jiným protokolem pro systémy řízení budov [18] [72][33].

Obr. 14 *Možné propojení komunikačních protokolů*



Zdroj: upraveno dle [67]

Jelikož se jedná o otevřený protokol, umožňuje rozsáhlou kompatibilitu mezi jednotlivými zařízeními na datové sběrnici v systémech ovládání budov. Zákazník tak není vázán na konkrétního výrobce (jak tomu bylo dříve), ale může volit z celé řady nabízených produktů podporující tento protokol. Tím se mimo jiné výrazně snižuje i cena a spolehlivost používaných komponent. Nejčastěji používanou komunikační sběrnicí je ARCNET, případně LONTALK. Informace, které protokol přenáší, mohou obsahovat např. analogové nebo digitální hodnoty vstupů a výstupů, vypočtené vstupní i výstupní hodnoty (analogové i digitální), funkce signalizace atd. BACnet je založen na modelu ISO/OSI a proto také obsahuje vrstvy síťového rozhraní, síťové, transportní a prezentační vrstvy. Z úsporných důvodů na HW i SW jsou funkce prezentační, transportní a relační vrstvy zahrnuty do vrstvy aplikační (viz struktura protokolu TCP/IP). [38] [82]

Vlastní přenos zpráv protokolem BACnet lze realizovat pomocí rozvodů:

- Ethernet – nejvýkonnější volba,
- RS485 – sériová linka, typ protokolu Master – Slave (jeden nebo více master uzlů, které mezi sebou spolupracují; slave uzel nemůže poslat zprávu, dokud není vyzván masterem),
- LonTalk – protokol LonTalk je použit jen k přenosu dat mezi jedním a druhým zařízením.

2.1.3.4 Další komunikační protokoly

Kromě uvedených existují i další komunikační protokoly. Jedním z nich je např. **Modbus**. Tento protokol se nejčastěji využívá k přenosu dat v průmyslových aplikacích. Stejně jako BACnet umožňuje rovněž komunikaci různých zařízení po různých typech sběrnic. V automatizaci budov však nemá takové uplatnění, vyjma případů centralizace průmyslových zařízení do automatizace budov[67].

Další ještě nezmíněné protokoly jsou např. **SNMP** a **C-bus** [64] [72]. Jejich využití je však vzhledem ke standardům KNX/EIB, LONWORKS a BACnetu minimální a jsou většinou spíše vhodné pro individuální řešení.

Velice zajímavou myšlenkou je systém **ENOCEAN**[98]. Jedná se o čistě bezdrátový systém s distribuovanou inteligencí. Nejčastěji je využíván jako subsystém nadřazeného systému pro řízení budov, lze jej však využít i samostatně. Celý systém se snaží absolutně minimalizovat spotřebu elektrické energie, proto se většinou napájí z alternativních zdrojů. Jako zdroj se využívá převodníků dostupné energie (mechanická, světelná, tepelná a další). Např. při stisknutí tlačítka se energie vynaložená na stisknutí využije k danému úkolu. Komunikace se realizuje na přenosové frekvenci 868 MHz. Signál je následně kódován, čímž se omezuje možnost vzájemného ovlivňování s dalšími přístroji. Dosah v budově je cca 30 m, v případě přímého dohledu až 300 m. Základem je modulární řešení kombinující řídicí jednotku se vstupními a výstupními moduly, které jsou propojeny pomocí sběrnice [21] [40].

2.2 Možnosti inteligentních instalací budov

Jak je již naznačeno v Kap. 2.1, v současné době nelze ani odhadnout, jaké možnosti instalace informačních systémů v IB vlastně nabízí. Již v dnešní době realizované projekty však jednoznačně ukazují, že se jedná o cestu vedoucí jednoznačně k úspoře energií, zvýšení uživatelského komfortu a při vhodné integraci i k výraznému zvýšení celkové bezpečnosti objektu, uživatelů i technologií. Je samozřejmé, že jiné možnosti a uplatnění najdou tyto systémy v komerčních objektech, jiná budou hlediska pro integraci do objektů obytných a zcela jiné požadavky budou kladeny na objekty technologické.

Nasazení **v komerčních** (a částečně technologických) **objektech** je charakteristické snahou navrhnout a následně realizovat ***adaptabilní*** systém, který umožní na úkor vyšších pořizovacích nákladů minimalizovat náklady na pozdější rekonstrukci a modernizaci objektu. Například v kancelářských budovách, kde dochází k častým prostorovým změnám, postačí přeprogramovat inteligentní moduly, díky kterým není nutné provádět zásadní změny elektrické a datové instalace. To ušetří čas na rekonstrukci a zároveň s tím spojené finanční prostředky. Takto jednoduše lze změnit např. místo, odkud bude ovládáno osvětlení, žaluzie či klimatizace. Klasické použití je ve velkých komerčních budovách pronajímaných jako kancelářské prostory, hotelech, ubytovnách, kolejích a především výrobních halách.

Úspora energií v těchto objektech je poměrně výrazná. Náklady na automatizační techniku, využívanou pro automatickou regulaci a kontrolu vytápění, klimatizace a vzduchotechniky činí 1,0 % až 1,5% celkových investičních nákladů. Možnosti potenciálu úspory energií nasazením automatizace se podle konzervativních odhadů dají vyčíslit podílem 10 % z celkových provozních nákladů. Z této úvahy vyplývá, že doba návratnosti investice do automatizační techniky činí cca 6 – 8 let. [72][75]. Z pohledu této práce je především zajímavé, že lze integrovat společně se zabezpečovacím a kamerovým systémem též systémy evidence přístupu a docházky, které podávají snadný přehled např. o zaměstnancích, jejich časech příchodu a odchodu nebo jejich momentální pozici. Celý souhrn pak lze snadno exportovat do textových (případně tabulkových) souborů, nebo jej následně zpracovat jako podklad pro zpracování mezd. Lze jej tedy využít jako další zdroj možné úspory provozních nákladů a celkového zjednodušení řízení systému[91]. Ještě podstatnější je pak dopad do situací krizového řízení[1].

Poněkud odlišná je situace instalace inteligentních informačních systémů **v obytných objektech**. V těchto případech se zavádí integrované systémy především proto, aby se zvýšil komfort uživatelů objektu. Současné technologie dovolují ovládat vytápění, větrání, osvětlení, či audiovizuální techniku jen pomocí mobilního telefonu. Uživatel může sledovat film, upravovat si jeho hlasitost a současně s tím může stejným ovladačem zvýšit nebo snížit teplotu v místnosti, nebo např. intenzitu světla.

Instalace v soukromých obytných objektech je v porovnání s celkovou cenou objektu značně vysoká a proto se prozatím provádí spíše výjimečně. Běžným standardem jsou dnes rozvody antén a UTP kabelů do všech místností, popř. vedení pro audiovizuální techniku. Proto lze výrazně omezit množství rozvodů (= potenciálního zdroje závad), navíc kromě estetického hlediska je výhodou i snadné připojení přístrojů.

Inteligentní domy se dnes také často spojují s pojmy nízkorozpočtový, nebo také ekologický dům. Svou „inteligencí“ šetří jak náklady jeho majitele, tak i životní prostředí. Zejména se jedná např. o použití solárních článků, které v případě pasivity domu dodávají elektrickou energii zpět do sítě a tím se fakticky stávají méně závislými na dodávkách elektřiny. Nespornou výhodou pro obyvatele inteligentních rodinných domů je také příjemný design interiéru. Tím, že jsou veškeré prvky integrovány do multifunkčních zařízení, lze termostaty, regulátory a další řídící prvky nahradit jedním (mnohdy designově zajímavým) ovládacím panelem.

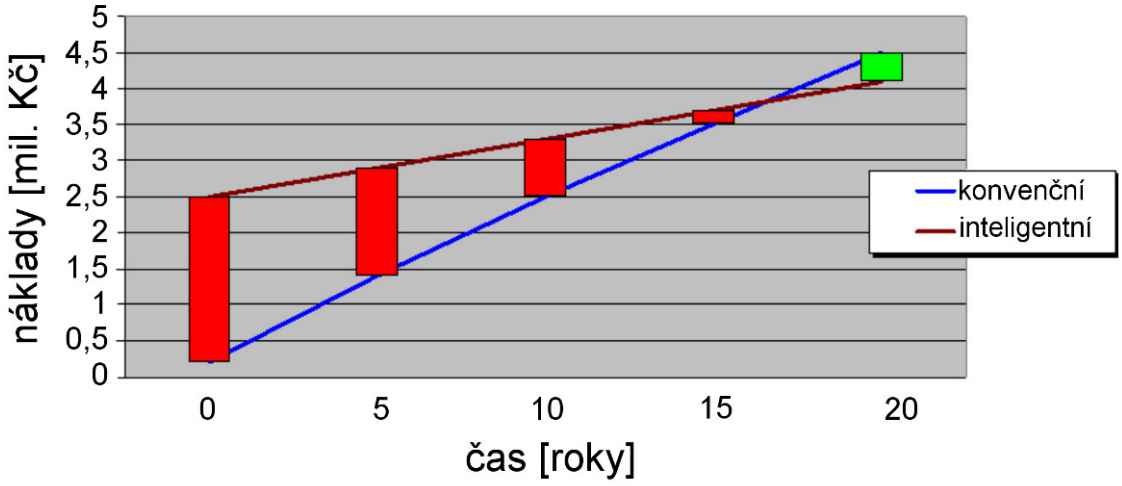
Celková úspora energií činí opět přibližně 10 % oproti běžné instalaci. Pokud se však vezme v úvahu suma pořizovacích nákladů na takovouto investici, je zřejmé, že návratnost v tomto případě bude sporná. Zásadní roli tedy bude spíše hrát úspora energie, nejistota v cenách surovin a energií a především nadstandardní komfort a zvýšený pocitu bezpečí.

2.2.1 Ekonomické zhodnocení

Z výše uvedených důvodů je potřebné ekonomické zhodnocení návratnosti investic do projektu inteligentního domu posuzovat odděleně pro jednotlivé typy objektů. Navíc, jak bylo zdůrazněno v předchozí kapitole, význam IB není pouze v ekonomické návratnosti či ekologické vyrovnanosti, ale zvláště u komerčních budov ve zvýšené bezpečnosti systému jako celku a v případě obytných domů ve zvýšení komfortu pro uživatele. Samozřejmě, i tak je ekonomický dopad a jeho návratnost podstatný argument[57].

V případě obvyklého komerčního objektu předpokládáme z výše uvedených důvodů (viz kap.2.3) celkové navýšení investic do inteligentních rozvodů oproti klasickým o cca 2 500 000 Kč. V těchto objektech bývá předpoklad ročních nákladů na energii cca 750 000 Kč při cca 20% úspoře energie v případě použití inteligentních systémů[3] [73] [75]. Pokud pomineme běžné provozní náklady, opravy a servis, lze návratnost graficky vystihnout následujícím způsobem.

Obr. 15 *Návratnost rozdílu investic u komerčních budov*



Zdroj: [107][110]

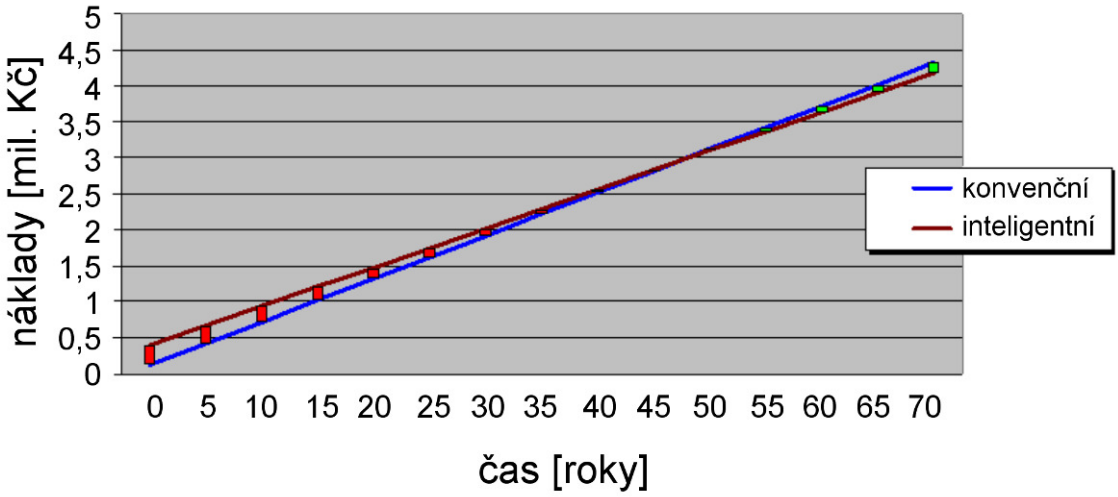
Z grafu na Obr.15 vyplývá, že v případě komerčních budov je již dnes možné očekávat návratnost zvýšené investice kolem 17. roku provozu, což je významné. Některé firmy realizující inteligentní systémy budov uvádějí v řadě případů návratnost dokonce 4 – 5 let, to ale neodpovídá zjištěným datům ani odhadům odborníků.

Zcela jiná je situace při využití inteligentních systémů řízení budov v případě soukromých obytných budov. Nejedná-li se např. o provoz hotelového typu (který spadá svoji charakteristikou spíše do komerční budovy), jde u obvyklého rodinného domu o investice do výstavby klasických inženýrských sítí řádově v částkách kolem 120 000 Kč.

Pokud se stejný objekt navrhne dle výše uvedených zásad a technologií „inteligentní“ instalace, jedná se o částku minimálně 350 000 Kč, která se může výrazně zvýšit při rozsáhlejší integraci a požadavku na komfort. Obvyklá investice je v tomto

případě kolem 400 000 Kč. Vzhledem ke kvalitní izolaci a obvyklém provozním režimu budovy jsou rozdíly za energii ve vytápění a osvětlení maximálně kolem 10%. Výsledek nejlépe charakterizuje Obr. 16, ze kterého je zřejmé, že k návratnosti investic bude docházet dlouho po očekávané životnosti stavby, což je z ekonomického hlediska zcela nezajímavé. Výrazněji se situace začne měnit, pokud začleníme do systému další zdroje energií (solární panely, teplotní čerpadla, malé větrné elektrárny). V tomto případě je návratnost v intervalu 20 – 30 let. To je sice stále příliš mnoho na ekonomickou rentabilitu, udává to však zřejmý směr, kudy se dále ubírat[1]. A to zvláště za poněkud nejistých cen za energii do budoucna.

Obr. 16 *Návratnost rozdílu investic u obytných budov*



Zdroj: [107][110]

Výše uvedený graf je potřeba analyzovat velice diferencovaně – v této kategorii budov se návratnost investic z již popsaných důvodů pohybuje od cca 20 let až do 50 let – zpravidla mimo jiné i v závislosti na způsobu integrace jednotlivých systémů a uživatelském komfortu[53]. Pro výpočet byly proto použity obvyklé hodnoty a průměrné ceny integrace nejčastěji integrovaných inteligentních systémů.

2.3 Legislativní a standardizační předpoklady

Pro zpracování této práce je detailní rozbor legislativních resp. standardizačních požadavků kladených především na zabezpečovací systémy zcela zásadní. Ve své podstatě se na řešení zpracovávaného problému nabízí celá řada možných technických i technologických řešení (podstatné jsou popsány v kapitole 2.1). Problém však vyvstal v okamžiku, kdy je snaha tyto technologie „zapouzdřit" do stávajících norem a legislativního rámce platného pro poplachové systémy. V této oblasti je stále zřejmý jistý tradicionalismus, který způsobuje, že prakticky veškeré moderní komunikační systémy lze jen velice obtížně použít na vyšším stupni zabezpečení objektu. Což na druhou stranu ukazuje i na podstatný problém těchto moderních komunikačních technologií – k přenosu informací využíváme technologie, které nemají dostatečný stupeň spolehlivosti a odolnosti proti úmyslnému napadení[2]. ***Důsledek je pak podobný tomu, čeho jsme v dnešní době svědky na Internetu.***

Samozřejmě, pokud je využívána zmíněná počítačová síť obvyklým způsobem, je běžnému uživateli poměrně lhostejné, zda na síti dochází, např. vlivem technologie, ke ztrátě dat za přenosu (kolize – ztrátovost paketů). Nastavené služby na aktivních prvcích sítě **zpravidla** dokážou tuto ztrátu zjistit a ve většině případů kompenzovat (opakováním přenosu). Přesto je však zjevně nemyslitelné, aby byl pro přenos signálů s vysokými požadavky na bezpečnost a spolehlivost používány přenosové technologie, které jsou již ze svého principu nespolehlivé a jak praxe ukazuje, velice snadno napadnutelné. To je logický důvod, proč normy bezpečnostních systémů stále nezavádějí moderní komunikační technologie (přenos Ethernet) jako primárně akceptovatelná přenosová prostředí[2].

Jaká je tedy legislativní situace v oblasti bezpečnostních systémů?

Pro zjednodušení a zkrácení bude shrnuta pouze situace ve třech základních bezpečnostních systémech (podrobněji viz. Příloha 3 či teze této práce):

- Protipožární systémy a SHZ,
- PZTS (dříve EZS),
- CCTV.

V případě, kdy je předpokládána integrace poplachových systémů do IB, jedná se vždy minimálně o integraci těchto tří základních systémů (zpravidla bývá integrován i ACC, není to však vždy pravidlem). Skutečně „inteligentní" instalace domu totiž vyžaduje

řadu čidel uvedených systémů jako senzorů pro rozhodování a naopak velká část prvků těchto systémů se velice často stává aktory (viz kap. 2.1.1 až 2.1.4) [58].

2.3.1 Technická legislativa v EU a v ČR

V Evropských společenstvích spadá zabezpečovací technika (zařízení používané v poplachových systémech) pod působnost **směrnic Evropského společenství**.

V ČR jsou technické směrnice EC přejímány formou nařízení vlády České republiky. S ohledem na to, že ČR je od roku 2004 plnoprávným členem EU, kopíruje linie základních legislativních požadavků na výrobky pravidla obvyklá v ostatních zemích EU. Základní legislativní rámec je tvořen Zákonem č. 22/97Sb. o technických požadavcích na výrobky. Tento zákon je průběžně novelizován.

Důležitou roli zde rovněž hrají dvě technické komise, jednak tzv. **TC79/**CENELEC, jednak **TC72/**CENELEC. Obě dvě tyto technické komise pracují při Evropském výboru pro normalizaci v elektrotechnice. Jejich působnost je velice široká. Zjednodušeně lze říci, že komise TC79 zpracovává otázku zabezpečovacích a kamerových systémů, komise TC72 pak problematiku elektrické požární signalizace.

Podrobnější rozklad viz. Příloha č.3

2.3.2 Legislativa protipožárních systémů a SHZ

Je třeba zdůraznit, že ač legislativní otázka v této oblasti jistě není zcela ideální (zvláště z pohledu vlastní realizace systémů), je rozhodně nejpropracovanější ze všech poplachových systémů. Je to dáno jistě tradicí, ale i aktivní prací celá řady státních, soukromých i zájmových organizací, které dovedly současný stav platných norem do situace, kdy více - méně detailně popisuje technické a technologické požadavky na jednotlivé prvky protipožárního systému, na systém jako celek i na organizační realizaci nezbytnou ke korektnímu fungování systému.

Legislativní rámec pro projektování a zřizování systémů EPS tvoří **zákon č. 67/2001 Sb**. o požární ochraně a z řady vyhlášek především **vyhláška č. 246/2001 Sb**. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru a stavební zákon (**č. 183/2006 Sb**.). Normativním základem pro obor EPS jsou normy řady **EN 54,** především **ČSN EN 54 132**.

Další důležité zákony, nařízení vlády, vyhlášky a normy související s diskutovanou problematikou jsou uvedeny v Příloze č. 3 této práce.

Z výše uvedeného soupisu norem, zákonů a vyhlášek je pro realizaci a integraci v rámci inteligentních systémů podstatná především již zmíněná vyhláška č. 246 Ministerstva vnitra ze dne 29.6.2001, především § 1d a navazující. Díky této vyhlášce lze definovat zda, případně za jakých podmínek, lze v daném konkrétním případě uvažovat o integraci v rámci inteligentních budov. Velice zjednodušeně a nepřesně lze předběžně předpokládat, že protipožární systém, splňující předpoklady dané výše uvedenou vyhláškou a uvedenými předpisy, lze integrovat do systému inteligentních budov za předpokladu, že rozvody a signalizace splňují výše uvedené předpisy. **To v praxi znamená, že celý systém EPS musí být v podstatě zcela autonomní a nezávislý na ostatních rozvodech, další systémy mu tedy nesmí být nadřízeny.**

V terminologii informačních systémů IB musí být tedy prvky systému EPS senzory, nikoli však aktory. To je důvod toho, proč se v praxi využívá výhradně výstupů definovaných na ústředně EPS k řízení jiných částí systémů IB (SHZ, ACC, výtahy, klimatizace atd.).

Bohužel však ani tato zásada není legislativně zcela striktně dodržována. V základním dnes platném legislativním předpisu – vyhlášce č. **23/2008 Sb** o technických podmínkách požární ochrany staveb se v celém dokumentu striktně hovoří buď o autonomních hlásičích požáru, případně o protipožárním systému (EPS, tam kde je předepsán). A přitom v tom samém dokumentu se v závěru na straně 496 v příloze č. 5 jasně definuje:

Autonomní detekce a signalizace

Zařízením autonomní detekce a signalizace se rozumí:

a) *autonomní hlásič kouře dle české technické normy ČSN EN 14 604, nebo*
b) *hlásič požáru dle české technické normy řady ČSN EN 54 „Elektrická požární signalizace“ a to například část 5, část 7 a část10; tyto hlásiče jsou použity například v lince elektrických zabezpečovacích systémů v souladu s českými technickými normami ČSN EN 50 131 „Poplachové systémy – Elektrické zabezpečovací systémy*“

(citace Vyhlášky č. 23/2008Sb, příloha 5)

Důsledek těchto dvou bodů je zcela zásadní. Oproti vyznění celé předchozí vyhlášky, oproti znění stavebního zákona (183/2006 Sb.) i proti znění normy ČSN EN 50132 dává najednou tato příloha možnost integrovat protipožární a zabezpečovací systémy (za splnění certifikace použitých detektorů dle ČSN EN 50 132).

2.3.3 Legislativa poplachových zabezpečovacích a tísňových systémů

V oblasti poplachových tísňových a zabezpečovacích systémů (PZTS, dříve EZS – elektrické zabezpečovací systémy) je situace poněkud jiná než v oblasti EPS. Základní normativní rámce a legislativa jsou již v podstatě definovány, alespoň co se týče základních technických parametrů celého systému i jednotlivých prvků. Základní problém je spíše v koordinaci technického rozvoje s poměrně zdlouhavou normotvorbou a přenosem norem EU do našich předpisů (= harmonizace norem).
V současné době jsou platné normy:

ČSN EN 50130-4:2012 Poplachové systémy – Část 4: Elektromagnetická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci.
Tato norma stanovuje požadavky na odolnost komponentů poplachových systémů, určených pro použití uvnitř a v okolí budov, v prostředích obytných, obchodních, lehkého průmyslu a průmyslových:

- Elektrické zabezpečovací systémy (EZS),
- Elektrická požární signalizace (EPS),
- Uzavřené televizní okruhy pro zabezpečovací účely (CCTV),
- Systémy kontroly vstupů (ACC),
- Systémy přivolání pomoci,
- Systémy tísňové,
- Systémy přenosové (doplněny změnou A1:1998),

Norma uvádí zkušební postupy provádění zkoušek a stanovuje stupně přísnosti na zařízení používaná pro vnitřní a venkovní aplikace, pro pevná, pohyblivá a přenosná zařízení. Norma se nezabývá elektromagnetickým vyzařováním.

ČSN EN 50131 Poplachové systémy - elektrické zabezpečovací systémy uvnitř a vně budov.

Tato norma je českou verzí evropské normy EN 50131-1:2006. Evropská norma EN 50131-1:2007 má status české technické normy. EN 50131. Norma specifikuje požadavky na provedení nainstalovaných PZTS, ale neobsahuje požadavky pro návrh, projekci, instalaci, provoz a údržbu. Tyto požadavky se týkají systémů mající společné prostředky detekce, vzájemného propojování, ovládání, komunikace a napájecích zdrojů s jinými systémy. Provoz daného poplachového systému nesmí být nepříznivě ovlivněn jinými systémy. V normě jsou specifikovány požadavky pro komponenty příslušné klasifikace prostředí a stupně zabezpečení. **Stupeň zabezpečení 4 je nejpřísnější** (opačně než u ČSN 334590). Norma specifikuje požadavky na provedení nainstalovaných zabezpečovacích systémů. Požadavky pro návrh, projekci, instalaci, provoz a údržbu obsahuje ČSN EN 50131-7. Tato část normy je z pohledu zpracování této práce zcela stěžejní.

Vzhledem k vlastní práci člena normalizační komise TNK 124 při ÚNMZ může autor potvrdit, že změny norem v této oblasti probíhají v podstatě neustále. TNK 124 má v tuto chvíli 3 subkomise, z nichž každá se věnuje jedné z klíčových otázek normalizace bezpečnostních systémů a subkomise pracují v podstatě bez přerušení. Pro rok 2014 se předpokládá dokončení kompletní revize celé normy ČSN EN 50 131, která byla zahájena v minulém roce, pracuje se na změnách v definici normy ČSN EN 50 136 a především, což považuje autor i za svůj přínos, bude v tomto roce zahájena práce na aktualizaci normy ČSN EN 50 398:2009.

Jako podstatné pro celý bezpečnostní průmysl a stěžejní i pro zpracování této práce se pak jeví schválení **TNI 33 4592** (prosinec 2013). Tato TNI dává zcela nové možnosti využití přenosu informace jak v rámci bezpečnostního systému, tak i mimo něj – bude dále diskutováno v práci jako jedno z možných řešení integrovaných bezpečnostních systémů.

Další důležité zákony, nařízení vlády, vyhlášky a normy související s diskutovanou problematikou jsou uvedeny v Příloze č. 5 této práce.

Z pohledu dopadu této práce je klíčový především výklad normy **ČSN EN 50131-1**, která definuje bezpečnostní kategorie a podmínky na systémy příslušející do příslušných bezpečnostních kategorií. V součinnosti s **ČSN EN 50136-1-2** a **TNI 33 4592** je pak zřejmé, jaké komunikační cesty lze využít, resp. které použít nelze. Právě zde je definován klíčový rozpor pro integraci poplachových systémů a jejich provázání do systémů IB. Podrobněji je tato otázka rozebíraná v praktické části této práce.

2.3.4 Legislativa kamerových systémů

V oblasti kamerových systémů je situace v oblasti legislativy a norem zřejmě nejhorší, resp. nejméně definovaná. Teprve před 2 roky byly vydány základní normy popisující kamerové systémy z technického hlediska. Bylo provedeno základní bezpečnostní rozdělení kamerových systémů podobně jako pro oblast zabezpečovacích systémů a do jisté míry se tak sjednotil postup pro návrh a vlastní realizaci kamerových systémů. Přesto však praxe ukazuje, že v této oblasti je potřeba provést ještě celou řadu inovací nejenom norem, ale i legislativy. [39]

Nejdůležitější právní normou, která upravuje provozování kamerových systémů, je **Zákon č. 101/2000 Sb., o ochraně osobních údajů**. Tato norma se však zabývá kamerovými systémy **pouze v případě, že dochází k pořizování a ukládání nahrávek** (ať už obrazových nebo zvukových). Provozování kamerového systému se ale může řídit i dalšími právními normami, jako např. občanským zákoníkem upravujícím podmínky ochrany osobnosti. Podstatným je rovněž tzv. **Zákon o elektronické komunikaci č. 127/205Sb.** ve znění pozdějších předpisů definující náležitosti přenosu obrazového záznamu. Protože však stále chybí zásadní legislativní rámec, nahrazují jej tzv. **Stanoviska Úřadu pro ochranu osobních údajů**, která se v tomto případě považují za směrodatná, i když nejsou přímo soudně vymahatelná[60]. Technická oblast kamerových systémů je v poměrně obecné formě definována v **ČSN EN 50132** Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích. CCTV jsou pojaty v EN jako doplňková zařízení poplachových systémů a nejsou pro ně stanovena kritéria na stupně zabezpečení jako na EZS (ale i tato změna se připravuje).

Je ironií, že právě nedokonalost norem a judikatury umožňuje kamerovým systémům poměrně dobrou provázanost směrem k centrálním informačním systémům, aniž

by bylo nutné splnit poměrně přísné normativní požadavky na integrační prvky. To je zřejmě i jeden z důvodů, proč se kamerové systémy, v podstatě živelně, v posledních několika letech rozvíjejí. [50]

2.3.5 Legislativní shrnutí

Pro projekt inteligentní budovy je klíčovou integrací především začlenění systémů PZTS, resp. systémů PZS. Normy poměrně jasně definují zásady pro interface (tedy integrační prvky). Zjednodušeně řečeno – např. zabezpečovací systém, který je dle normy definován v bezpečnostním stupni 2 (tedy nízké až střední riziko - což je velká většina instalací), musí obsahovat komponenty, které mají certifikaci minimálně pro tento bezpečnostní stupeň. Jakmile se tedy připojí stávající systém PTZS prostřednictvím interface, které žádný atest nemá k dalšímu systému, ztrácí celek systému bezpečnostní certifikát třídy 2, což se okamžitě projeví např. při jednání s pojišťovnou a finanční i právní důsledky mohou být velmi nepříznivé. I proto je z pohledu těchto systémů výrazný odpor k využití jiných technologií přenosu poplachové informace než těch definovaných normou. Je bohužel pravdou, že se vzrůstajícím tlakem výrobců i prodejců se bude projevovat snaha o zapojení IT technologií do těchto systémů. Je však nezbytné k této snaze přistupovat velice uvážlivě, neboť spolehlivost resp. zabezpečení běžného IT přenosu je významově i technicky na výrazně nižší úrovni než stávající konvenční přenosy poplachových systémů – což dokumentují i výsledky této práce. Přesto již v dnešní době několik společností realizuje takto integrované systémy, byť za cenu toho, že mlčky ignoruje platné normy a doporučení pojišťoven. Je zřejmé, že k vyřešení tohoto problému dojít musí, je však otázkou, jaké technické řešení zvolit[8]. **Je právě klíčovým cílem této práce nalézt odpovídající technické řešení, které bude splňovat legislativní a normalizační požadavky, resp. navrhne případné legislativní změny.**

Z pohledu zpracování této práce se z počátku zdálo, že bude vhodné striktně dodržovat odpovídající předmětné normy řady ČSN EN 50 –xxx a na jejím základě se pokusit definovat vhodný integrační přístup. Při vlastní praktické realizaci se však velice rychle prokázalo, že v plném znění příslušných norem není v podstatě tento problém prakticky realizovatelný a muselo být použito další hledisko. Proto byla využita norma **ČSN CLC/TS 50398:2009 – Kombinované a integrované systémy**.

Tato norma je sama o sobě v podstatě velice nekonkrétní, přesto však za určitých podmínek umožňuje integraci poplachových systémů v IB a to dokonce na takové úrovni (a stupni), že je to z pohledu projektanta poplachových systémů zcela neakceptovatelné. V podstatě totiž definuje 3 třídy kombinovaných systémů lišících se v míře vzájemného ovlivňování jednotlivých integrovaných systémů mezi sebou.

Z těchto důvodů autor inicializoval vznik subkomise na úrovni komise TNK124 při ÚNMZ, která se bude zabývat právě aktualizací a modernizací této normy, čímž budou legislativně splněny všechny nezbytné předpoklady dále definované a využívané v této práci.

2.4 Aktuální stav integrace poplachových systémů ve světě i v ČR

Pro analýzu aktuálního stavu integrace poplachových a bezpečnostních systémů v rámci IB bylo nutné nejdříve definovat předpoklady akceptovatelné integrace bezpečnostních systémů do informačních systémů IB. Po několika pokusech začalo být zřejmé, že optimální bude vycházet z normy ČSN EN 50131-1 a normy ČSN CLC/TS 50398. Tím byly okamžitě vyřazeny integrační nástroje většiny velkých výrobců a možné řešení se omezilo na pouze několik málo používaných řešení, z nichž některé obsahují použitelné základy pro odpovídající integraci bezpečnostních systémů[8]. Již v tuto chvíli však bylo jasné, že zcela legislativně a normativně „čisté“ řešení na trhu ani u nás, ani ve světě reálně neexistuje. A zřejmé také je, že to není zastaralostí norem či jejich pomalého zavádění do praxe, ale spíše skutečně **vážnými pochybnostmi nad technickými a bezpečnostními problémy modernějších integračních technologií.** Tento rys je zřejmý v řadě klíčových publikací renomovaných světových autorů i v materiálech mnoha velkých firem[34]. Na druhou stranu je nutné přiznat, že řada autorů nehodnotí výše popsaný rozpor tak zásadně[32][34][35] a považuje jej za spíše marginální. Jedná se ale velice často za autory spojené s některou z velkých firem věnující se integračním technologiím, což je v současné době jeden z nejvíce rostoucích ekonomických a vývojových oblastí trhu[5].

Z těchto důvodů bylo výrazně omezeno studium reálných moderních instalací tzv. inteligentních budov u nás i ve světě, neboť buď stávající řešení odporuje platné legislativě, nebo (častěji) se jedná pouze o parciální řešení integrující několik málo systému (zaměřeno především na energetickou úspornost). V zásadě lze o relativně „čisté“ a úplné instalaci (pokud se omezíme na ČR) v případě velkých komerčních budov mluvit o

budově Národní technické knihovny v Praze – Dejvicích a sídle společnosti Skanska v Praze – Opatově[5]. Přesto, že lze mít jisté výhrady k některým integračním koncepcím (především bezpečnostních prvků), jedná se o budovy, které ukazují zřejmý směr pro budoucí vývoj v oblasti integrování systémů budov.

Obr. 17 *Sídlo společnosti Skanska v Praze – moderní IB*

Zdroj:[101]

Integrace automatizačních a poplachových aplikací je ve většině případů v reálné praxi řešena několika málo technickými principy. V zásadě existují tři základní způsoby řešení[3]:

- Integrace propojením vstupů a výstupů – vhodná pro přenášení relativně omezeného množství stavových údajů (při reálném ověřování se podařilo pracovat s 256 stavy – viz dále v praktické části)
- Systémové instalace (SIE) – k automatizačnímu systému se může pomocí integračního prvku SIE připojit autonomní poplachový či bezpečnostní systém[8]. Tento způsob integrace je poměrně častý, nejvíce však naráží na legislativní předpisy a především normy řady ČSN 50 xxx.
- Softwarový způsob integrace – propojení individuálních aplikací (jednotlivých samostatných částí informačních systémů IB) zajišťuje komunikační sběrnice. Správu a uživatelský přístup zajišťují programy instalované na počítači (PLC) nebo na řídící centrále.

Systémová integrace jako taková není prosté sloučení několika systémů, jedná se o propojení na několika úrovních. A právě míra integrace systémů je dána kvalitou (způsobem) integrace těchto částí [8] Podrobněji v následující tabulce.

Tab 1. Způsoby integrace informačních systémů

Provedení integrace	Aplikace
Technologická integrace	Sjednocení PZTS, CCTV, ACC, EPS, osvětlení, vytápění, další technologie
Funkční integrace	Sjednocení funkčnosti prvků jednotlivých systémů (např. přístupové karty, biometrické scany, bezdrátové klíčenky)
Integrace uživatelského interface	Založeno na kombinovaném ovládání jednotlivých poplachových i nepoplachových systémů identickým prvkem (dotyková obrazovka, mobil, tablet, dálkový ovladač)
Datová integrace	Sestavení databázového modelu informačního systému tak, aby byl akceptovatelný pro integrované systémy (např. identifikace osob, přístup na pracoviště, evidence docházky, výpočet mzdy)
Metodická integrace	Způsob integrace uváděný u některých především zahraničních autorů obsahující především registraci pohybu osob a vozidel v objektu, evidence jejich doprovodu a obsahující nástroje k omezení jejich pohybu. ***Dle názoru autora se jedná spíše o implementaci kvalitní Datové a Funkční integrace***

3 CÍL PRÁCE

Cílem disertační práce **INTEGRACE OCHRANNÝCH SYSTÉMŮ V RÁMCI PROJEKTU „INTELIGENTNÍ BUDOVY“** je navrhnout technické, technologické a legislativně akceptovatelné řešení, na jehož základě bude možné realizovat integraci bezpečnostních systémů v rámci informačních systémů budov, především tzv. inteligentních budov.

Na základě získaných poznatků, provedených měření a testů bude předložen návrh vlastního řešení v diskutovaných oblastech. Vzhledem k výsledku provedených výpočtů a realizovaných praktických testů (které jsou prováděny jak v laboratorních, tak i v běžných provozních podmínkách), bude snaha formulovat základní premisy pro specifikaci vlastností dílčích systémů na jejich integraci. Tyto závěry pak budou zpětně porovnány s legislativní a normativní základnou platnou v ČR a v EU.

Konečným výstupem práce bude návrh technologie bezpečné a modulární integrace bezpečnostních systémů, a to pokud možno včetně poloprovozního řešení či modulární simulace takového řešení.

Z předchozích kapitol vyplývá, že z technického hlediska nic principiálně nebrání integraci bezpečnostních systémů do systémů IB. Dokonce lze říci, že bez integrace právě prvků bezpečnostních systémů nelze v podstatě plnohodnotnou „inteligentní“ instalaci uskutečnit. Systém musí mít pro své rozhodování informace. Ty lze získat kupříkladu z detektorů PZTS a ACC (přítomnost osob), z detektorů EPS (teplota a její změna), ze systémů OAT (o stavu technologií).

A právě to je největším problémem integrace. Již zmíněná dilemata ve vztahu k platné legislativě a normám striktně omezují možné okruhy technického řešení a výrazně omezují možnosti praktického výzkumu. Z pohledu výše uvedené analýzy norem a legislativy je zřejmé, že pro daný objekt je předepsán (navržen) bezpečnostní systém odpovídající danému bezpečnostnímu zatížení. Jednotlivé bezpečnostní systémy jsou tedy navrženy tak, aby splnily odpovídající bezpečnostní stupně vyžadované pro konkrétní objekt. To ale znamená, že se použijí samostatné uzavřené systémy, mající odpovídající bezpečnostní certifikace (*tedy v podstatě na integraci rezignujeme*), nebo pro integraci použijeme integrační komponenty mající příslušnou certifikaci (*takové ale neexistují!)*.

Znamená to, že pokud je požadováno splnění všech platných zákonů, norem a předpisů (včetně předpisu ČAP), není v současnosti možné integraci na úrovni distribuovaného IS aplikovat. Dokonce, i když použijeme centrální systém s řídícím PC, který řídí všechny podřízené systémy, není takové řešení legislativně přijatelné.

Cíle disertační práce lze tedy na základě těchto poznatků rozpracovat do následujících bodů:

- vypracovat metodiku tvorby legislativních podmínek pro začlenění bezpečnostních systémů do stávající IS budov,
- analyzovat stávající technologie přenosu informace používané v IS budov z pohledu bezpečnosti, spolehlivosti a legislativy,
- vyhodnotit vlastní měření a testy a porovnat je s poznatky z vědecké, odborné a technické literatury
- ověřit získané hodnoty ze zkušebního provozu navržené technologie s provozem v reálné instalaci,
- zhodnotit získané výsledky a navrhnout možnosti jejich poloprovozního využití v praxi,
- formulovat technologické principy možného způsobu integrace poplachových systémů na základě vlastního navrženého řešení.

4 METODY ZPRACOVÁNÍ PRÁCE

Stanovení metodiky zpracování práce a postup praktického ověřování předpokladů vychází z předchozí části práce. V tomto případě se nemůže jednat o pouze technické hodnocení a posouzení navrženého řešení, ale minimálně stejně důležité je i zohlednění legislativního a normativního základu a to nejenom vzhledem ke stávajícímu stavu, ale (a to především) k předpokládanému vývoji v tomto směru. Vzhledem k práci autora v **Technicko-normalizační komisi TNK124** (Poplachové a bezpečnostní systémy) při **Úřadu pro normalizaci a měření** má řešitel práce ideální přístup nejenom k aktuálnímu stavu norem a legislativy, ale zároveň se účastní i prací nad návrhy nových norem. Prostřednictvím práce v **Hospodářské komoře** se pak autor do jisté míry spolupodílí na tvorbě příslušných zákonů a legislativních předpisů v oblasti bezpečnostních systémů a komerční bezpečnosti. Z tohoto úhlu pohledu je práce autora nad tímto tématem poměrně zjednodušena plnohodnotným a trvalým přístupem ke korektním a aktuálním informacím, na druhé straně závěry v této práci obsažené mohou být autorem bezprostředně promítnuty do jeho působení v těchto organizacích.

Předpokládaný postup praktické části práce je tedy následující:

a) stanovení legislativních a normativních identifikátorů pro realizaci integrovaného systému obsahující bezpečnostní (či poplachové) systémy

b) praktické ověření integrace bezpečnostních systémů s dalšími systémy, pomocí programovatelných výstupů bezpečnostních ústředen (PGM) – ústředna PZTS se pak vlastně stává centrální jednotkou integrovaného distribuovaného systému,

c) praktické ověření využití inteligentní sběrnice pro integraci jednotlivých systémů inteligentní budovy – principiálně decentralizovaný systém bez centrálního uzlu jednotlivých podsystémů,

d) matematické a simulační ověření realizovatelnosti integračního prvku založeného na principu neuronové sítě – řešení dosud nikde nepoužité otvírající nové aspekty globální integrace libovolných systémů, problematická je spíše spolehlivost řešení, které bude nezbytné ověřit simulací,

e) využití univerzálního komunikačního prostředku (TCP/IP) pro komunikaci a vzájemné ovlivnění jednotlivých (v podstatě nezávislých) systémů – toto řešení vyplynulo při jednání nad normalizací protokolu SIA-09 (jednání TNK 124 konec roku 2012 – listopad 2013) a dle názoru autora nabízí velice zajímavé možnosti pro distribuovanou integraci (vyšší úroveň decentralizované centralizace, podrobněji v kap. 5).

K vypracování rešeršní a analytické části disertační práce byla využita dostupná literatura českých i zahraničních autorů včetně internetových zdrojů. Vlastní výzkum probíhá v laboratoři Katedry technologických zařízení staveb ČZU v Praze, v praktickém provozu (reálné instalace bezpečnostních systémů), simulace a matematické modelování v oblasti neuronových sítí probíhalo částečně na dopravní fakultě ČVUT. Postupy řešení a potřebné přístrojové vybavení jsou popsány v následujících kapitolách.

4.1 Legislativní rámec

Již v kap. 2.3, je označena legislativní a normalizační situace v oblasti integrace bezpečnostních systémů jako poměrně problematická a nejednoznačná. Díky tomu vzniká celá řada řešení, která jsou koncipována zcela proti obsahu uvedených zákonů, nařízení a norem, nebo je výrazným způsobem obchází. Vzhledem k tomu, že se však jedná o systémy, které mohou výrazně ovlivnit míru ohrožení života a zdraví uživatelů objektu, je naopak nezbytný jasný, vyhraněný a zcela nekompromisní přístup v této integrační oblasti.

Z dosavadní analýzy je zřejmé, že legislativně „čistá“ jsou v zásadě dvě řešení, obě však přinášejí své specifické problémy.

První varianta („centrální“) je založena na topologii serverového řešení (či lépe varianta s centrálním PLC), které v rámci tohoto serveru integruje veškeré diskutované integrované služby (systémy). Příkladem může být například systém společnosti VariantPlus, systém VARNET Integrál[102]. Toto řešení však předpokládá, že je možné realizovat takové serverové a komunikační řešení, které bude schopné získat atest bezpečnostní kategorie min. 2 (dle TrezorTest a NBU). Je otázkou dalších výpočtů a modelování tuto záležitost potvrdit či vyvrátit (není obsahem této práce). V současné době prakticky veškeré výsledky modelování ukazují, že toto řešení je za obvyklých finančních nákladů v podstatě nerealizovatelné. Pokud je definována spolehlivost celého systému rovnou současné spolehlivosti jednotlivých dílčích bezpečnostních systémů, lze dovodit, že

spolehlivost celého integrovaného řešení se musí pohybovat kolem 99,9%, přitom nelze dopustit to, aby chyba jednoho systému se projevila chybou (či poruchou) systému druhého, integrovaného v jeden celek[28].

Druhá varianta („distribuovaná“) má výraznou výhodu v moderní koncepci, z pohledu legislativy je však v podstatě nepřijatelná. V rámci této práce je vytvořeno několik praktických modelů a tyto otestovány se snahou k možné a nekompromisní legislativní „únosnosti“ tohoto řešení. Dosud však (jak je diskutováno v úvodu kapitoly 2.3) není takové řešení známé v odborné (české ani zahraniční) literatuře. Proto musí být navržené řešení originální.

Shrnutí klíčových legislativních a normativních faktorů, které budou ovlivňovat návrh integrovaného řešení, lze poměrně jednoduše definovat v několika bodech:

- jednotlivé normy příslušných poplachových systémů definují, že k poplachovému systému lze připojit komponenty, které mají odpovídající bezpečnostní certifikaci (atest) s výjimkou definovaných rozhraní (programové výstupy, tiskové a zálohovací interface, komunikační rozhraní),
- pokud dojde k připojení komponenty, která nemá odpovídající certifikaci, ztrácí celý systém bezpečnostní certifikaci jako celek (problém s pojišťovnami, odpovědnost za škody, rozpor se zákonem – v extremním případě trestní odpovědnost),
- certifikace je proces jednak poměrně časově náročný, velice drahý a především je potřeba jej každých 5 let opakovat,
- norma ČSN EN 50398 je v podstatě bezobsažná kromě toho, že povoluje vzájemné ovlivňování integrovaných systémů (definuje 3 třídy vzájemného možného ovlivňování), navíc sama v úvodu definuje nadřazenou platnost norem řady 5013x, čili tím sama sebe v podstatě ruší.

Je asi zbytečné na tomto místě rozebírat podrobněji legislativní a normativní předpisy pro tuto oblast, v zásadě se každý další rozbor vždy vrací k výše uvedeným bodům (s výjimkou předpisů pro protipožární systémy, které určitým způsobem umožňují integraci i náhradu systémy PZTS, pouze však v určitých případech).

Z tohoto výčtu jasně vyplývá, že v případě pokusu o integraci např. systému PZTS je nutné použít povolené rozhraní, tedy především PGM a komunikační rozhraní. Proto je první část práce zaměřena primárně na toto rozhraní, byť vlivem tlaku trhu řada především velkých firem a výrobců volí cestu integrace prostřednictvím napojení konkrétního interface zpravidla pro konkrétní typ bezpečnostního systému a daného výrobce[36]. Logicky to však znamená, že pro splnění podmínek stávající legislativy (viz. výše uvedené body) by bylo nutné každý jednotlivý interface certifikovat. Navíc, a tuto okolnost je nutné považovat za zvláště důležitou, je potřeba získat od výrobce bezpečnostního systému povolení k zásahu do vlastního zařízení bezpečnostního systému a to samozřejmě zaplatit. Někteří výrobci toto řeší vlastními SDK, které prodávají řešitelům integrace, neřeší to však otázku legislativní. Navíc se ve většině případů jedná pouze o výrobce v oblasti kamerových systémů[3].

Předkládaná řešení se tedy nadále (až na několik málo pokusů a ověření předpokladů) budou věnovat pouze interface, které je možné použít bez ztráty certifikace, tedy:

- programové výstupy
- tiskové a integrační moduly
- komunikátory

Je všeobecnou mylnou představou (šířenou především v ČR zástupci spol. Jablotron a.s., v zahraničí pak především společností Siemens ltd), že ke vstupu dat do ústředny lze použít libovolné smyčky, pokud tyto nebudou nastaveny pro hlídací režim (na smyčce je necertifikované zařízení) a nedojte tím ke ztrátě bezpečnostní certifikace systému. Nesmyslnost tohoto tvrzení je zřejmá po přečtení ČSN EN 50 131-2, proto se autor tohoto způsobu přenosu dat pokusí dále v práci vyvarovat, přesto, že je mezi komerčními integrátory velice oblíbené.

4.2 Integrace prostřednictvím programových výstupů ústředny PZTS

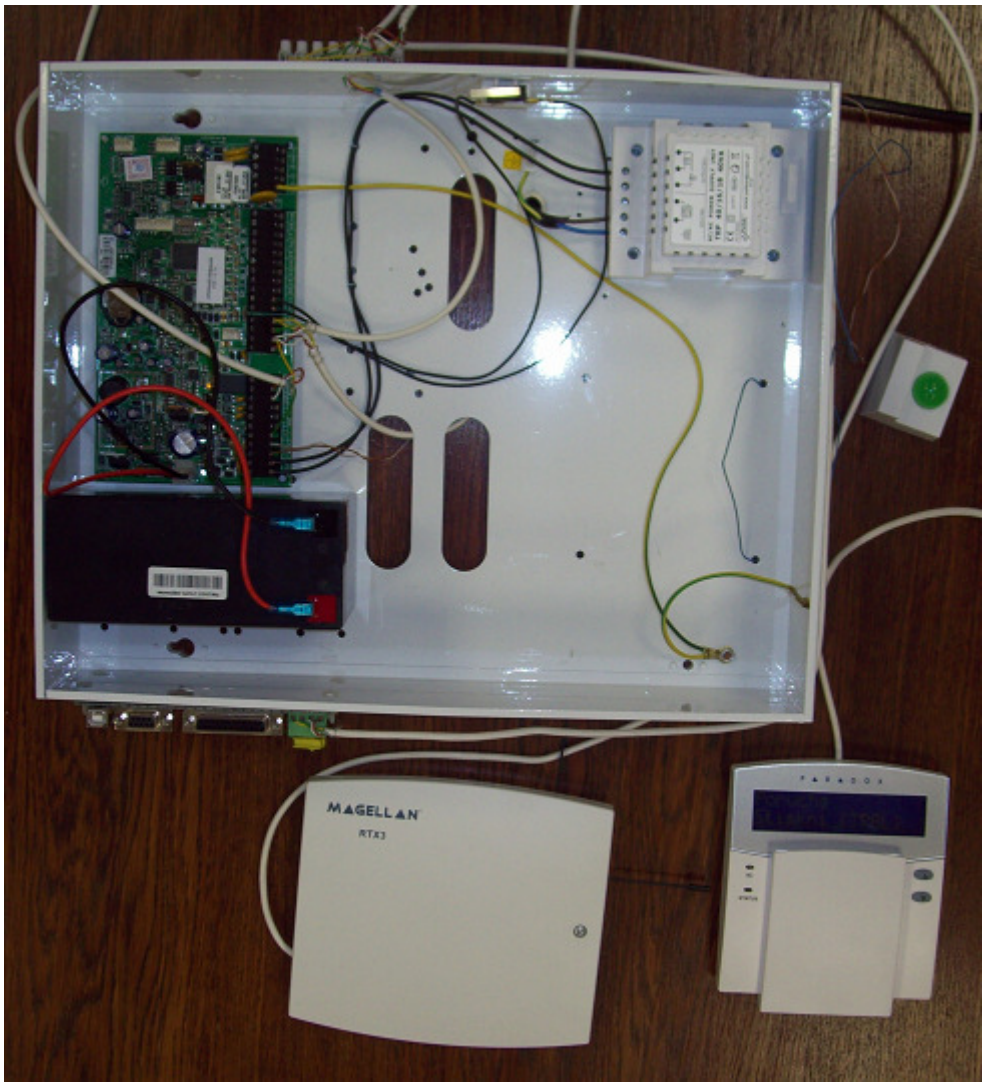
Sami výrobci zabezpečovacích ústředen a poplachových systémů předpokládají využití programových výstupů (tzv. PGM) pro jednoduchou automatizaci objektu. Ve

většině případů (s výjimkou společnosti Honeywell International Inc.) však velcí producenti neuvažují o využití těchto PGM pro rozsáhlejší integraci.

Ve své podstatě se jedná o relativně jednoduché řešení. Ústředna zabezpečovacího systému (v příslušné bezpečnostní třídě) je vlastně integrační ústřednou propojující a ovládající jednotlivé další systémy, ať již poplachové či technologické. Vzhledem k tomu, že se jedná pouze o přenos jednoho bitu (sepnutí/rozepnutí relé) je složitější programování poněkud náročné a i když spojité ovládání je principiálně možné, je lépe se mu pokud možno vyhnout. Je logické, že tento způsob komunikace je pouze jednosměrný, proto se pro přenos informací (stavů) do ústředny jeví jako možný přenos pomocí poplachových zón (což již bylo v předchozí části důrazně nedoporučováno z legislativních důvodů), nebo využití pomocí komunikačních interface pro tisk (USB port, RS232 port). Při vlastních testech tohoto způsobu integrace se však ve většině praktických řešení ověřilo, že zpětná komunikace není principiálně nezbytná, resp. je využívána pouze v kritických situacích. V souvislosti s vlastní komerční činností autora bylo možné instalovat a dlouhodobě provozovat několik takovýchto instalací, takže výsledky získané z měření a testů jsou jednak dlouhodobé, jednak z reálného provozu a výrazně tak doplnily laboratorní testy. Výsledky a závěr jsou demonstrovány v kapitole 5.

Pro laboratorní testy byla použita ústředna Digiplex Evo 48 s expandérem pro PGM a s komunikačním a tiskovým modulem. Technické řešení je podle provedených analýz a experimentů plně funkční. Provedená měření a testy dle předpokladu plně potvrdily možnost integrace poplachových systému pomocí PGM a to jak mezi sebou tak i s dalšími systémy IB. Rovněž tak byla potvrzena možnost využít PGM PZTS k dlouhodobému řízení integrovaných systémů, což se dosud považovalo jako největší překážka takového způsobu integrace.

Obr. 18 *Celkový pohled na testovanou soustavu Digiplex Evo*



Zdroj: [110]

Uvedená ústředna umožňuje aktivaci při běžné konfiguraci 5 programových výstupů, proto je možné definovat příliš malé množství stavů a to i v případě, že je použit multiplexor (za použití multiplexoru lze definovat **31 stavů**). Protože však lze ústřednu doplnit dalšími programovými výstupy, bylo testováno chování systému při doplnění ústředny na celkový počet 20 programových výstupů (PGM). V tomto případě bylo za použití multiplexoru možné na výstupu rozeznat až **1 048 575 stavů.** Tento počet nepochybně zcela postačí pro běžné řízení i poměrně rozsáhlého systému, včetně případné potřeby spojitého řízení konkrétních veličin. Při dlouhodobé zátěží (168 hodin

programového ovládání výstupů PGM) nebyla zjištěna jediná chyba a to dokonce i při neplánovaném výpadku el. energie [108] [107].

Protože systém Digiplex lze osadit až 250 PGM výstupy, je tato možnost propojení a řízení poměrně široká. Zásadní nevýhodou je poměrně složitá integrace, která v tomto případě je vždy zcela jedinečná pro každou další instalaci. Navíc potřeba spojitého řízení musí být převedena na řízení diskrétní.

Z výše uvedených důvodů byly hledány jiné možnosti využití ústředny PZTS k řízení externích systémů. Prakticky se ověřilo několik variant:

a) **Ovládání prostřednictvím expandéru**: tato možnost se zpočátku jevila jako velice zajímavá a perspektivní. V podstatě jakýkoli stav externího systému by byl v rámci ústředny vyhodnocen jako stav detektoru a v závislosti na předepsané funkci by aktivoval příslušné výstupy PGM. Jedná se o bezpečné, levné a přehledné řešení, které má zásadní nevýhodu v omezeném množství vstupů (max. 128 binárních vstupů, bylo by možné vyřešit demultiplexorem). Klíčovým nedostatkem tohoto řešení je však nemožnost obousměrné komunikace tohoto způsobu přenosu informace.

b) **Ovládání prostřednictvím IP modulu**: je řešení, při kterém se využívá komunikace ústředny PTZS a tzv. internetového modulu. Internetový modul je v podstatě síťová karta připojená na sběrnici ústředny a umožňující komunikaci mimo systém prostřednictvím TCP/IP protokolu (RJ45 konektor). Na tomto modulu je instalován jednoduchý web server, na který se lze pomocí prohlížeče přihlásit a lze nejenom zobrazovat stavy systému, ale jej i ovládat. Výhodou tohoto řešení je tedy především možnost obousměrné komunikace, rychlost a jednoduchost řešení. Zásadní nevýhodou je však otevřenost a bezpečnostní riziko takového řešení. Po ověření možností tohoto řešení a zvláště jeho rizik bylo toto řešení zavrženo.

c) **Ovládání prostřednictvím tiskového a komunikačního modulu**: toto řešení se dlouhodobě jevilo jako optimální. Pomocí modulu připojeného na sběrnici ústředny je možné provádět obousměrnou komunikaci, ovládat libovolný externí systém a to dokonce i ve spojitém (lineárním)

řízení. Zásadní problém je však v tom, že komunikace s tímto modulem je šifrována a k jejímu plnému použití je potřeba prolomit tuto šifru či získat od výrobce povolení k jejímu zrušení a odpovídající přístupové kódy. Vzhledem k tomu, že výrobce odmítl možnost spolupráce v této oblasti a rovněž odmítl zapůjčit přístupová práva, je reálně možná pouze varianta prolomení šifrování silou. Tím však samozřejmě dojde k narušení autorských práv výrobce. Přesto, že někteří integrátoři zvolili tuto cestu, bylo toto řešení rovněž zavrženo.

Výsledky a testy popsané v bodech a) – c) byly shrnuty v rámci grantu IGA **31170/1312/3136**, začátkem roku 2011 obhájeny a opublikovány [33],[108] (**Integrace systémů PZTS v návaznosti na technologický dohled komerčních budov**, Security Magazín 2/2011 ISSN 1210-8723, str. 47 – 53; **Elektrotechnické a telekomunikační instalace** ISBN 80-86897-06-0 kapitola 11/3 – 11/3.5 Rozvody bezpečnostních elektrických systémů).

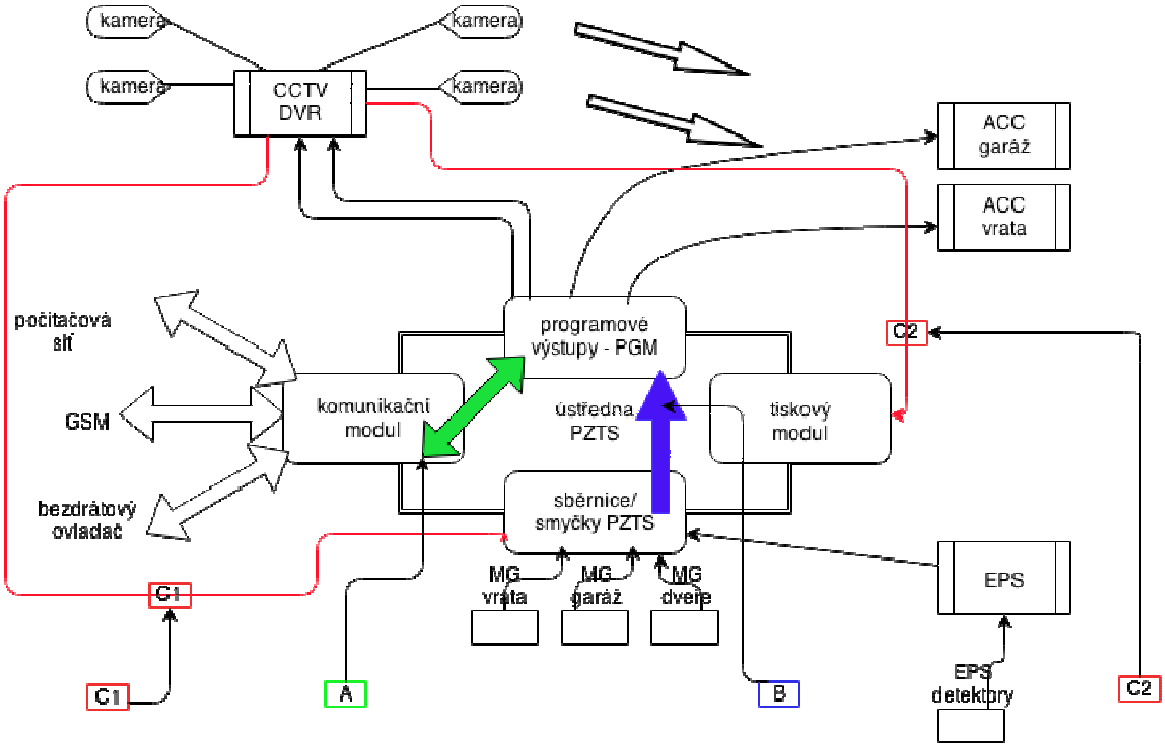
Obr. 19 *Detail testovacího zařízení – pohled na modul IP100 a komunikační modul PRTX3*

Zdroj: [108]

Z předchozích odstavců i z provedených experimentů a měření je zřejmé, že skutečně jednoduchý, spolehlivý a bezpečný integrační prvek, který by byl zároveň i dostatečně univerzální, není v současné době k dispozici. A to se týká jak integrace pomocí centrálního uzlu, tak i integrace decentralizované.

Proto bylo rozhodnuto uvedené řešení ověřit dlouhodobě v praxi. Do reálného provozu byly instalovány bezpečnostní systémy integrující výše popsaným způsobem systém PZTS, systém EPS, systém ACC a systém CCTV, tedy čtyři nejčastěji používané poplachové systémy. Vzhledem k tomu, že tento způsob integrace se v experimentálních testech jevil jako optimální pro menší a střední instalace, byla vybrána instalace do několika soukromých rodinných domů. Blokové schéma navrženého systému je následující:

Obr. 20 *Detail blokového schématu předpokládaného PGM systému*



Zdroj:[112]

Princip činnosti je zřejmý ze schématu. Pro zjednodušení jsou uvedeny pouze moduly přímo se podílející na integraci.

Funkční popis systému je následující (výchozí stav – systém ve stavu hlídání, objekt prázdný):

1. dálkovým ovladačem PZTS, mobilem či počítačovou sítí se otvírají vjezdová vrata na pozemek (zelená šipka A),
2. ústředna PZTS na základě reakce otevření MG vrata aktivuje PGM1 které aktivuje vstup na DVR kamerového systému na základě toho se kamera sledující vjezd na pozemek přepíná do snímání max. rozlišení a DVR odesílá fotografii z kamery e-mailem či MMS (nastavitelný počet) (modrá šipka B),
3. dálkovým ovladačem PZTS, mobilem či počítačovou sítí se otvírají vrata do garáže (zelená šipka A), podsystém garáž se vypíná z hlídání (alternativně celý objekt),
4. ústředna PZTS na základě reakce otevření MG garáž aktivuje PGM2 které aktivuje vstup na DVR kamerového systému na základě toho se kamera umístěná v garáži nastaví do polohy „garáž-vjezd“ a přepíná do snímání max. rozlišení a DVR volitelně odesílá fotografii z kamery e-mailem či MMS (nastavitelný počet); zároveň je aktivováno automaticky PGM1, čímž dojde k zavření vjezdových vrat na pozemek (modrá šipka B),
5. dálkovým ovladačem PZTS, mobilem či počítačovou sítí se zavírají vrata do garáže (zelená šipka A), podsystém garáž lze alternativně nastavit do hlídání, vypíná se hlídání objektu dům, ve většině případů bylo aktorem v tomto případě pevné nástěnné tlačítko v garáži přímo propojené v ústřednou PZTS (keyswitch),
6. alternativně byl systém v jednom případě vybaven IR kamerou s algoritmem detekce konkrétní osoby. V tomto případě došlo k vypnutí systému z ostrahy na základě pozitivní identifikace.

Poměrně problematické bylo v tomto případě otestování a ověření vlastních parametrů přenosu signálů a především ověření dlouhodobé funkčnosti a stability navrženého řešení. U poplachových systémů jsou relativně vysoké požadavky nejenom na běžnou spolehlivost systému, ale i na odolnost vlivu prostředí, chyby uživatele a případné systémové chyby.

Posuzování funkčnosti a spolehlivosti bezpečnostních systémů (a v tomto případě tedy i systémů s nimi integrovanými) se dle normy provádí pomocí 4 kriterií:

- pravděpodobnost detekce (Pd)
- četnost planých poplachů (NaR)
- četnost falešných poplachů (FaR)
- pravděpodobnost překonání (Vd)

Pravděpodobnost detekce (***probability of detection***): Jedná se o pravděpodobnost zjištění přítomnosti nebo pohybu narušitele v rámci oblasti střežené příslušným detektorem eventuálně detekčním systémem (detekční zóna). Tato pravděpodobnost může být různě vysoká. Obecně však platí, že při jejím zvyšování roste četnost planých poplachů a za splnění určitých podmínek roste i četnost falešných poplachů. Udává se v intervalu od 0 do 1. Jelikož jde o relativní veličinu, musí být vždy určeny podmínky, za nichž platí. Například typ narušitele, způsob a rychlost jeho pohybu.

Četnost planých poplachů (***nuissance alarm***): Jedná se o četnost neplatných poplachů způsobených příčinami, které je možné považovat za nerizikové a na které je detektor z principu své činnosti citlivý (např. povětrnostní podmínky, pohyb zvěře nebo vegetace, atd.). Udává se jako počet poplachů v jedné detekční zóně za určitou jednotku času.
Aby byl detekční systém důvěryhodný, tak by četnost planých poplachů neměla přesáhnout ***jeden poplach za týden***.

Četnost falešných poplachů (***false alarm***): Jde o četnost neplatných poplachů vyvolaných bez patrné vnější příčiny, nejčastěji způsobené vlivem šumu obvodů, vadou elektronické součástky nebo jinou poruchou detektoru. Typicky se udává jako počet poplachů v jedné detekční zóně za určitou jednotku času.
Za přijatelnou hodnotu četnosti falešných poplachů můžeme ***považovat jeden poplach za 1 – 2 roky (podle třídy bezpečnosti)***.

Pravděpodobnost překonání: Jedná se o pravděpodobnost, s jakou může pachatel překonat detekční technologii, aniž by způsobil poplach. A to nejčastěji buď prostřednictvím překonáním detekční zóny např. jejím přelezením, podhrabáním či

přemostěním nebo využitím technických limitů jednotlivých detekčních technologií. Zkušený tým narušitelů může také detekční systém překonat degradací vyhodnocovací a zásahové složky zabezpečení. Vyšší počet poplachů vyvolaných na různých místech obvodu objektu v krátkém čase bude mít za následek narušení metodiky vyhodnocování poplachů a umožní tak v době uměle vyvolaného chaosu úspěšné vniknutí do lokality. Proto je výhodné, aby monitorovací část systému zaznamenávala poplachy podle toho, jak jsou vyvolané a to i v době poplachu a zásahu.

Provedené měření, testy a jejich výsledky popsaného systému jsou za dobu až pěti let provozu systému popsány v kapitole 5.1

4.3 Integrace prostřednictvím průmyslových sběrnic

Jak je popsáno v předchozích kapitolách (především Kap. 2.1) je použití průmyslových sběrnic pro integraci bezpečnostních systémů v rámci inteligentních budov legislativně sice problematické, koncepčně a technologicky se však jedná o velice zajímavé řešení a stále větší množství velkých výrobců (Siemens, Honywell, Echelon, v ČR např. TECO a.s.) je prosazuje. Bohužel občas i na úkor platné legislativy a platných norem. Principiálně však toto řešení není (po odpovídající změně legislativy) z provozního ani bezpečnostního hlediska kritické a je rozhodně vhodné tomuto řešení věnovat odpovídající pozornost. Vzhledem k cenám modulů se jedná o řešení vhodné spíše pro větší systémy a budovy (na rozdíl od předchozího řešení demonstrovaného v Kap. 4.2).

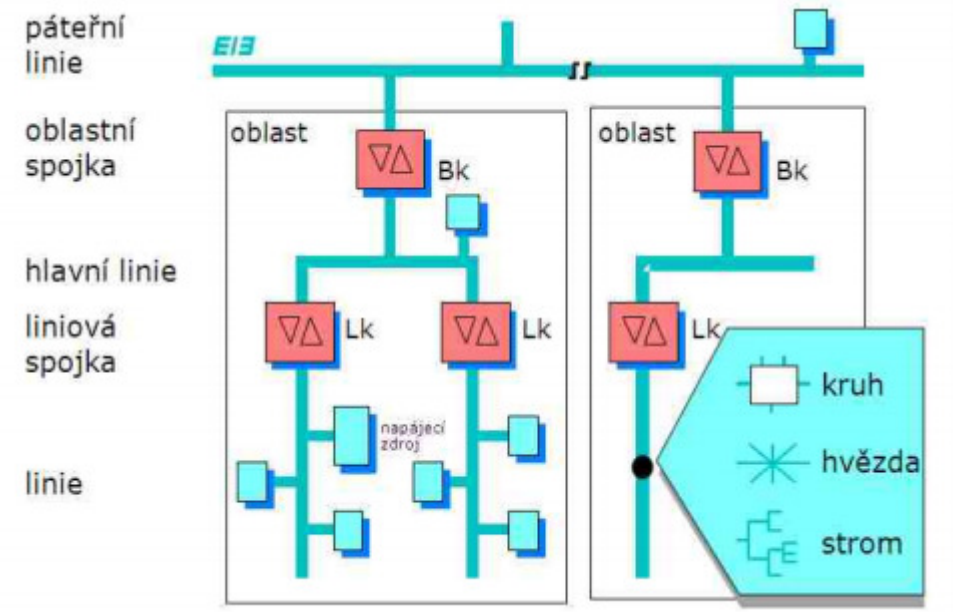
V České republice se zpravidla setkáváme se sběrnicí založené na standardu KNX/EIB (podrobněji popsána v kapitole 2.1.3.1) a sběrnicí CIB společnosti TECO a.s. Proto bylo ověřování funkčnosti integrace bezpečnostních systémů prostřednictvím distribuovaných sběrnic zaměřeno především na tato dvě řešení.

4.3.1 Metodika testování sběrnice KNX

Testování možného použití sběrnice KNX bylo metodicky poměrně jednoduché. KNX je plně decentralizovaný systém, ve kterém může vzájemně komunikovat až 65 536 zařízení /uzlů pomocí 16-ti bitového adresování. Celá síť se skládá ze tří úrovní. Nejvyšší úroveň je centrální nebo též páteřní linie (backbone line) s 15 hlavními liniemi (main line - střední úroveň) a na každou z nich může být napojeno dalších 15 linií (spodní úroveň -

podsítě). Struktura podsítě umožňuje připojit až 256 zařízení na jednu linku, které mohou být spolu s hlavní linií a částí páteřní sběrnice zahrnuty do jedné skupiny zvané zóna (oblast) 1 až 15 (area 1 až 15) [46]. Tato 3úrovňová struktura sítě však vyžaduje oddělovače zón (area coupler) a linií (line coupler) – viz Obr. 21. Bez nich je struktura sítě omezena jen na jednu linii (páteřní) s maximálně 256 připojenými jednotkami. KNX volitelně umožňuje i integraci podsítě přes IP[4] [46] [47].

Obr. 21 *Tři úrovně sběrnice KNX za použití coupleru*



Zdroj:[79]

Prostřednictvím oblastních spojek lze rozšířit hlavní linii o 15 oblastí. Tak jako každá linie, musí mít i každá oblast svůj zdroj napájení. Na hlavní a oblastní linii se nesmí nacházet liniový zesilovač. Tento liniový zesilovač může být osazen pouze v liniích, pokud nestačí její maximální kapacita 64 účastníků. V rámci jedné oblasti (zóny) může být osazeno až 15 x 64 = 960 účastníků v základním (nerozšířeném) provedení sběrnice[4].

Používaná fyzická adresa slouží pochopitelně pro jednoznačnou identifikaci účastníka. Z fyzické adresy lze rozpoznat i přesnou polohu zařízení v rámci topologie sběrnice. Fyzická adresa má podobu Oblast x Linie x Účastník a pohybuje se v rozmezí od 0.0.1 do 15.15.255.

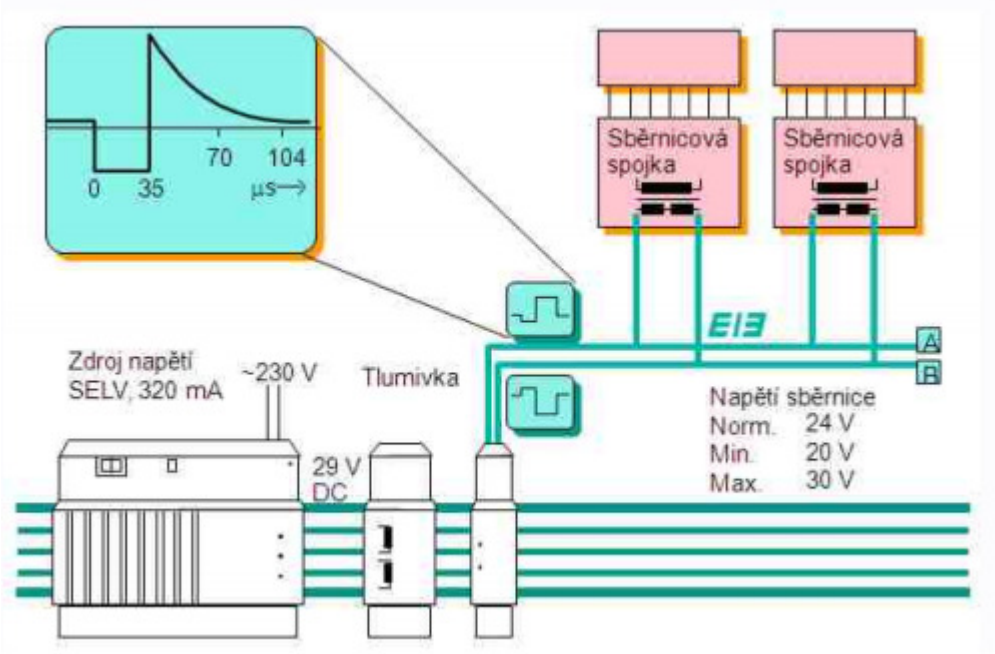
Fyzická adresa je přidělována jednotlivým účastníkům v rámci programování systému. Přijetí fyzické adresy účastníkem se provádí během programování po stlačení

programovacího tlačítka. Během tohoto procesu svítí programovací LED dioda. Pro normální provoz není znalost fyzické adresy důležitá. Po úspěšné konfiguraci systému je nezbytná znalost konkrétní fyzické adresy pouze pro tyto případy:

- diagnóza a hledání chyb,
- výměna zařízení za jiné,
- pro potřebu programování prostřednictvím sběrnicové spojky jiného zařízení[4].

Pro testování byla použita minimální (tzv. TP1) komunikace. Skládá se ze zdroje 24 V DC, modulu pro zapojení senzoru, aktoru a sběrnicového kabelu (viz. Obr. 22) [77]:

Obr. 22 *Základní schéma zapojení testování KNX sběrnice*

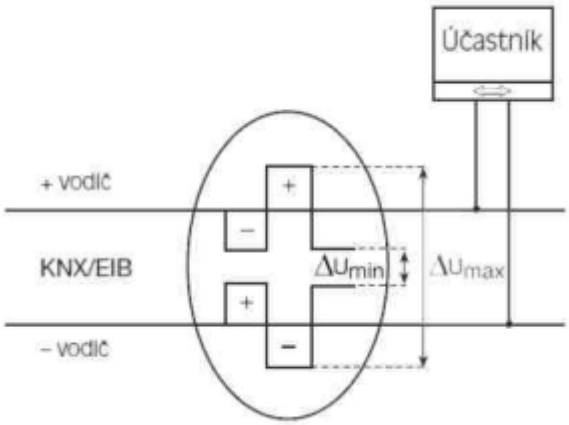


Zdroj:[79]

Vlastní data jsou ve sběrnici posílána pomocí telegramu, který se provádí změnou stavů napětí – napětí přítomno / napětí nulové. Přenos jednotlivých signálů je symetrický, to znamená, že záporný potenciál na plusovém vodiči (+) má svůj protějšek v kladném potenciálu na minusovém vodiči (-)[77]. Takto vzniká minimální napětí dUmin až 14 V. V opačném případě při kladném potenciálu na plusovém vodiči (+) vzniká na minusovém

vodiči (-) stejně velký, ale záporný potenciál. Takto vznikne u odesilatele napětí dUmax až 34 V[19] [20] [59].

Obr. 23 *Identifikace signálu na sběrnici KNX dle napěťových úrovní*



Zdroj:[4][78]

Vlastní sběrnicové spojky reagují pouze na rozdíl potenciálů mezi vodiči sběrnice, nikoli na jejich napětí vůči jiným potenciálům, např. ochrannému vodiči. To umožňuje poměrně velkou odolnost vůči rušení z prostředí[59].
Vlastní struktura telegramu je následující:

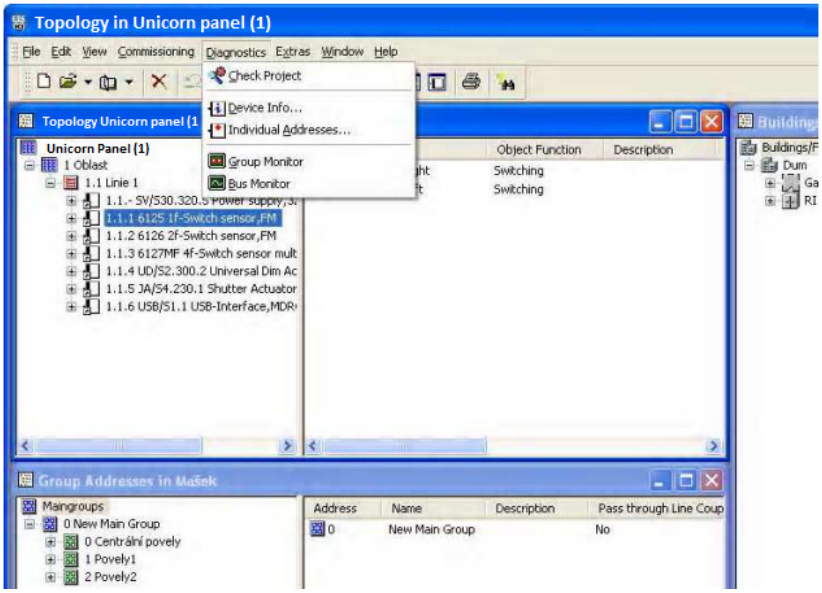
Obr. 24 *Schéma telegramu na KNX*

Telegram TP1						
8 bitů	16	16+1	3	4	až 16x8 bitů	8 bitů
Kontrolní pole	Kontrolní pole	Kontrolní pole	Routingový čítač	Délka (už. inf.)	Užitečná informace	Ověřovací Byte

Zdroj: [79][20]

Programování základní komunikace bylo provedeno pomocí veřejně dostupného programu ETS3 (později ve verzi 4).

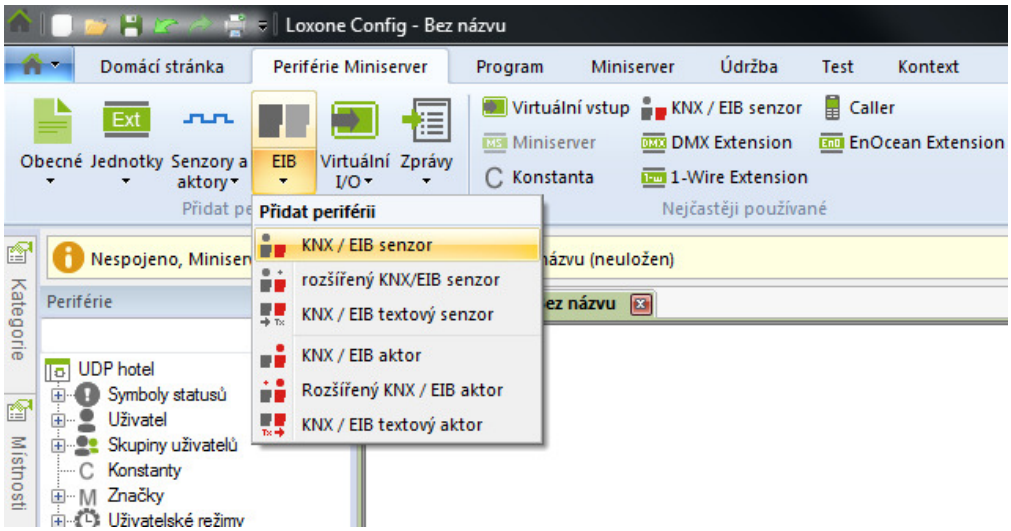
Obr. 25 *Ukázka základního nastavení pomocí programu ETS*



Zdroj: [113]

Původně bylo předpokládáno propojení bezpečnostních relé ABB BT50 s interface na LAN, na které budou umístěny dva routery s možností monitoringu přenášených dat (paketů) [55] [76]. Tím bude možné získat hodnověrnou statistiku spolehlivosti komunikace, byť do jisté míry ovlivněnou vlastním routováním a Ethernet konvertorem[76]. Během prvních pokusů však byla k dispozici nová verze produktu firmy LOXONE, která nejenom že velice pohodlně umožní vlastní programování členů, ale provádí i testování a ověření činnosti jak prvků, tak i celého systému. Tím se celý proces velice zjednodušil.

Obr. 26 *Ukázka základního nastavení v programu LOXONE*



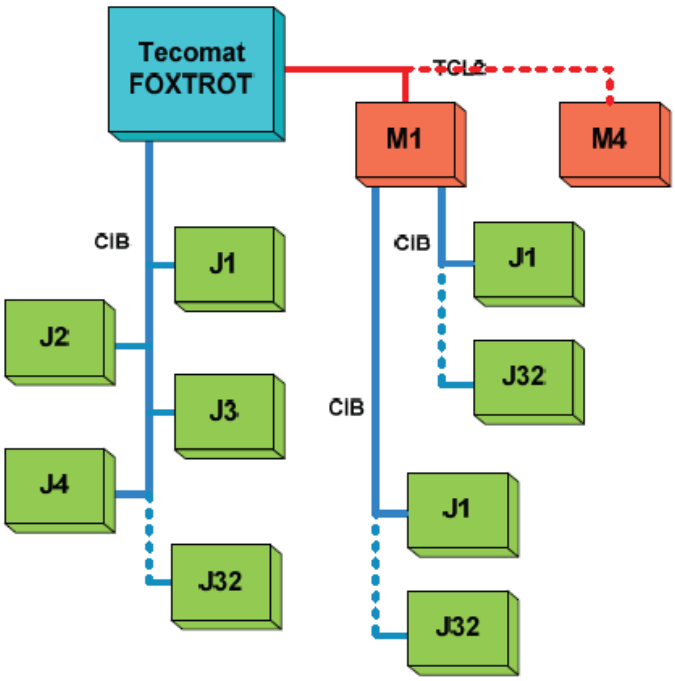
Zdroj: [113]

4.3.2 Metodika testování sběrnice CIB

Obdobným způsobem jako testování KNX bylo provedeno i testování CIB sběrnice společnosti TECO a.s. CIB sběrnice není v pravém slova smyslu distribuovanou sběrnicí, jedná se spíše o sběrnici s PLC prvkem s částečně distribuovanou „inteligencí“ prvků. Jedná se o dvouvodičovou sběrnici, která umožňuje napojené prvky zároveň napájet. Vlastní komunikace na sběrnici probíhá v režimu „master – slave“ a je namodulována na stejnosměrném napájecím napětí. Způsob zapojení sběrnice (topologie) není jednoznačně definována, může být tedy v zásadě libovolná (s výjimkou kruhové topologie, stejně jako v případě sběrnice KNX).

Sběrnice může obsahovat max. 32 prvků na každé větvi s tím, že je potřeba dodržet maximální možný proudový odběr na jedné větvi (max. 1 A za použití oddělovače, jinak 0,1 A). Maximální vzdálenost mezi centrální jednotkou a modulem je 300 m v případě metalického rozvodu a 1.7 km při použití optického vlákna. Vhodným větvením lze tedy výrazně rozšířit jak dosah, tak počet prvků[80].

Obr. 27 *Příklad možného propojení prvků sběrnici CIB*



Zdroj:[45]

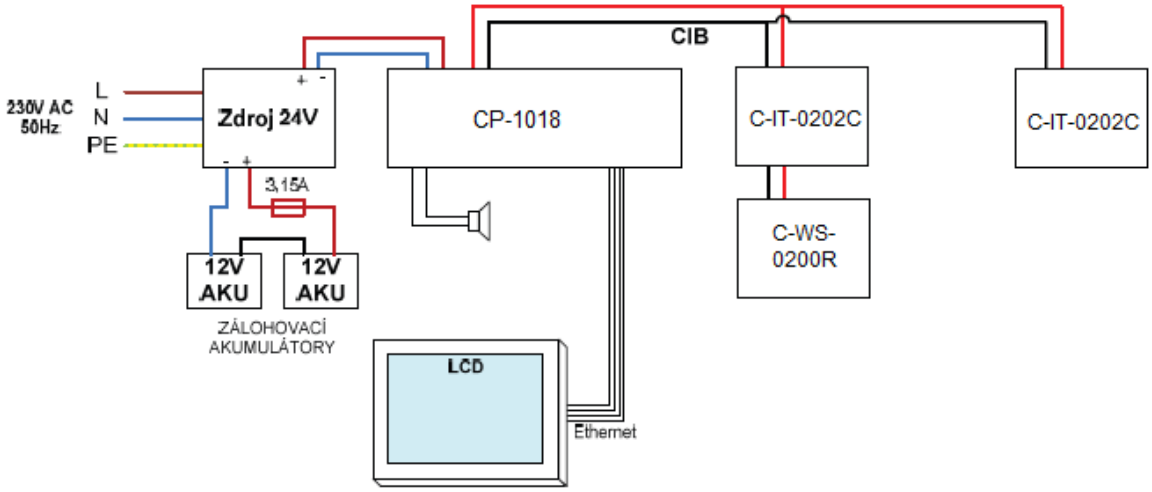
Sběrnice je napájena 24 V s doporučením využít 27 V pro trvalé dobíjení zálohovacích akumulátorů. Díky tomu je celý systém poměrně stabilní a nezávislý na externím napájení. V případě výpadku napájení sice nebudou fungovat spotřebiče 230V, ale systém jako takový včetně přenosu komunikace mezi zálohovanými bezpečnostními systémy bude zcela funkční. Adresace je řešena pevnou šestnáctibitovou adresou vyjádřenou čtyřmi hexadecimálními číslicemi (na štítku modulu) [32].

Tab. 2 Limity sběrnice CIB[29][44][45]

Název	Hodnota	Tolerance
Jmenovité napětí napájení sběrnice se zálohováním	27,2 V	+10 % -25 %
Jmenovité napětí napájení sběrnice bez zálohování	24 V	+25 % -15 %
Topologie	libovolná kromě kruhu	
Max. vzdálenost PLC od rozšiřujícího modulu CIB	300 m (metalika) 1700 m (optika)	
Max. vzdálenost periferní jednotky od nejbližšího mastera	500 m	(orientačně)
Rychlost přenosu dat	19,2 kbit/s	

Pro testování byl použit modul CP-1018 (PLC), PS2-60 (zdroj), ID-28 (grafická klávesnice), C-WS-0200R (vypínač) a dva kusy C-IT-0202C dle Obr. 28[42].

Obr. 28 *Konkrétní schéma zapojení testované sestavy CIB*



Zdroj: upraveno dle [29][45]

Společnost TECO dodává další moduly vhodné přímo pro integraci do prvků zabezpečovacích systémů (detektorů) či pro připojení celých systémů (Paradox, Jablotron, Galaxy) [42]. Tyto moduly však již byly testovány z pohledu možného využití v rámci několika diplomových prací pod autorovým vedením[32] [45], je tedy zbytečné je na tomto místě opět testovat. Navíc uvedené moduly spíše řeší možnost přímo vytvoření zabezpečovacího systému pomocí CIB sběrnice, což je za současných legislativních podmínek nereálné.

Programování bylo provedeno v prostředí Mosaic dodávaného výrobcem[81]. Tento nástroj obsahuje i podrobné nástroje pro testování komunikace, proto měření bylo poměrně jednoduché a přesné[32].

Ověření komunikace v obou případech testů (jak KNX tak i CIB) bylo zaměřeno především na spolehlivost a rychlost přenosu a dále na jeho soulad se standardem. Výsledky měření a jejich závěr jsou dokumentovány v kapitole 5.2.

4.4 Integrace prostřednictvím „neuronového klíče“

Po několika testech a ověřování funkčnosti průmyslové sběrnice LON a KNX bylo zřejmé, že je nezbytné a krajně vhodné ověřit a otestovat zcela jinou, původní technologii.

Byla nazvána metodikou **„neuronového klíče“** (odvozeno od neuronových sítí, nikoli od sítí LON).

Předpokládá se, že celý proces bude fungovat tak, že celý, již instalovaný, oživený a plně funkční poplachový systém se připojí k tomuto „neuronovému klíči“, který se automaticky „naučí“ šifrovaný způsob komunikace uvedeného systému. Proces učení je založen na principu neuronové sítě. V okamžiku, kdy dojde k odpovídající úrovni rozeznání komunikace (nikoli k prolomení šifry, nedochází tedy k poškození autorských práv ani ke snížení bezpečnosti celého systému), je možné na tento „neuronový klíč“ připojit již běžné komunikační rozhraní dalších systémů (či obdobné neuronové moduly) a systémy pak mezi sebou plnohodnotně komunikují na úrovni předem definovaných stavů[97] [117].

Univerzálnost tohoto řešení, jeho bezpečnostní a legislativní „čistota“ jsou důvodem, proč následně bylo rozhodnuto pro vlastní řešení integrace systému zvolit právě tento postup, i když je ze všech popsaných postupů nejobtížnější. Vzhledem k jeho novosti lze očekávat i určité realizační obtíže. Z výše uvedených důvodů bylo testování dalších sběrnic a jejich rozbor ukončeno až do okamžiku potvrzení či zamítnutí reálnosti uvedeného řešení minimálně na úrovni matematického modelu. Po konzultacích s pracovišti ČVUT a UK byl zvolen dále navržený postup.

4.4.1 Výběr vhodného neuronového modelu

Informační technologie založené na použití neuronových sítí se staly již pevnou součástí nástrojů moderní informatiky. Neuronová síť je jedním z výpočetních a simulačních modelů používaných v umělé inteligenci[41]. Jejím vzorem je chování odpovídající chování biologických struktur. Umělá neuronová síť je tedy nástroj určený pro distribuované paralelní zpracování dat. Tato síť se skládá z umělých (nebo také formálních) neuronů vytvořených podle vzoru biologického neuronu[68]. Formální neurony jsou vzájemně propojeny a navzájem si předávají signály a transformují je pomocí určitých přenosových funkcí. Neuron má libovolný počet vstupů, ale vždy pouze jeden výstup[24] [26].

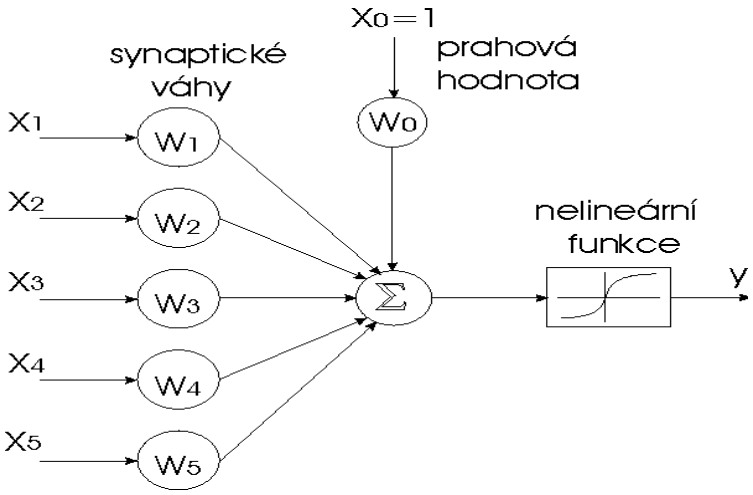
Použití neuronových sítí je v poslední době velice široké – od rozeznávání obrazu, přes predikci časových řad až po simulování chování biologických organizmů. Právě využití neuronových sítí v simulaci biologických (i jiných dějů, které nedokážeme přesně

popsat) je oblastí, která se v několika posledních letech velice rozšířila a spolu s tím vznikla i celá řada modelů neuronů a přenosových funkcí[23].

Obecně řečeno, se za umělou neuronovou síť považuje struktura pro distribuované paralelní zpracování dat, která se skládá (zpravidla) z velkého množství vzájemně propojených výkonných prvků. Základní vlastnost neuronových sítí udává jejich tzv. paradigmata (tedy nejenom topologii, ale i postup učení a vybavování).

Vzhledem k tomu, že principy fungování a matematický aparát neuronových sítí byl detailně popsán již v tezích této práce a existuje poměrně velké množství odborné literatury, nebude na tomto místě uváděn celý matematický postup využitý pro neuronový model. Uvedena je pouze základní definice matematického modelu umělého neuronu, ze které vychází další odvozené aplikace a využití[24].

Obr. 29 *Matematický model umělého neuronu*



Zdroj:[95]

V tomto přiblížení lze v zásadě definovat, že synaptické váhy definují (vyjadřují) uložení zkušeností do neuronu se zachováním schopnosti adaptace na zkušenosti získané prostřednictvím učení. Somatické operace (agregace, prahování a nelineární zobrazení) pak slouží především k převodu na skalární signál[95].

Klíčovým kriteriem pro výběr daného typu neuronové sítě je rovněž (možná primárně) volba vhodné architektury této sítě. Zvolená architektura se projevuje nejenom v možnosti modelovat určitý reálný děj, ale rovněž v schopnosti učení daného typu. Podle způsobu propojení neuronů a podle jejich přenosových funkcí se rozdělují neuronové sítě

na celou řadu architektur. Nejznámější, nejpoužívanější a v tomto konkrétním případě pravděpodobně nejvhodnější budou architektury[25]:

- **Perceptron:** nejjednodušší model neuronové sítě. V základním pojetí lze použít pouze na lineárně separovatelné množiny. V základní variantě perceptron je jednovrstvá neuronová síť s dopředním šířením a učením s učitelem. Existují i mnohavrstvé perceptrony i jiné strategie učení sítě[26]. Je otázkou, zda pro toto konkrétní řešení bude perceptron vhodným nástrojem, pokud ano, celá situace se výrazně zjednoduší.

- **Vrstevnatá neuronová síť**: někdy označovaná jako dopředná síť, což reprezentuje způsob šíření signálu v síti, tj. od vstupu k výstupu, resp. od vstupní vrstvy k výstupní vrstvě. Tyto sítě mají neurony rozmístěny do tzv. vrstev. Vzájemné propojení všech neuronů je realizováno pouze mezi vrstvami. Tj. výstupy neuronů dané vrstvy jsou propojeny se vstupem každého neuronu ve vrstvě následující. Podle informací z odborné literatury[7][26][27][30][31][71] a i podle prvních testů je toto typ sítě, který by měl být optimální pro uvažované modelování.

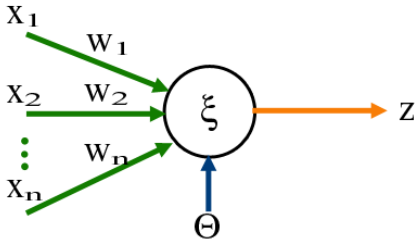
- **Rekurentní neuronová síť**: omezení dopředných sítí (limitované možnosti zpracování časového kontextu vstupních dat spolu s nutností doplnění „externí" pamětí sítě („okénková metoda") vedlo ke snaze tyto nedostatky odstranit. Řešením je zavedení dalších vazeb do modelu sítě, které umožní zpětnou vazbu na předchozí neurony. Tím se sníží celkový počet neuronů (vrstev) v síti a výrazně se posílí „samoučící" schopnosti této architektury[95].

- **Kohonenova mapa**[61]: patří mezi specifickou skupinu samoorganizujících se sítí. V tomto případě se jedná o jednovrstvou síť. Pracuje na principu shlukování neuronů. Síť se snaží napodobit lidský mozek, který si uchovává informace pomocí vnitřní prostorové reprezentace dat. Na rozdíl od Hopfieldovy sítě, kde jsou

neurony propojeny každý s každým, jsou v Kohonenově síti pospojovány jen nejbližší sousední neurony. Neuron také nemá předem specifikovanou přenosovou funkci, pouze počítá vzdálenosti mezi vzorem zakódovaným ve vahách a vzorem vstupním - $d_j = \sum_{i=0}^{N-1} [x_i(t) - \omega_{ij}(t)]^2$ [30]. Použití v tomto konkrétním případě bude poměrně obtížné, tento typ sítí má problém s delším učícím procesem a je oprávněný předpoklad, že by mohlo dojít k „přeučení“ tohoto modelu. Bude tedy nezbytné tuto variantu podrobně otestovat. V případě, že ji bude možné použít, bude se jednat zřejmě o jednu z nejrychleji učících se variant.

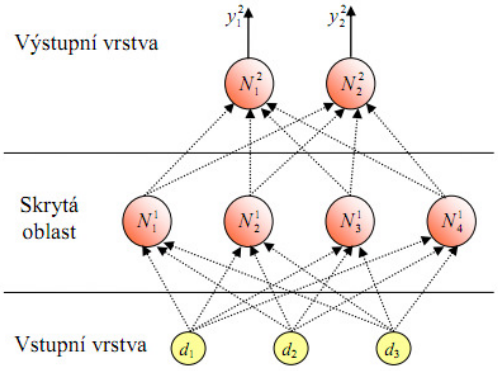
- **<u>Modulární neuronová síť</u>**[61]: Biologické studie ukazují, že lidský mozek nepracuje jako jediná masivní síť, ale jako soubor malých sítí. Tento výzkum dal zrod konceptu modulárních neuronových sítí, ve kterých několik malých sítí spolupracuje nebo soutěží, aby vyřešily daný problém. Komise (výbor) strojů (Committee of Machines; CoM) je soubor různých neuronových sítí, které dohromady "hlasují" pro daný příklad. To obvykle dává mnohem lepší výsledky ve srovnání s dalšími modely neuronových sítí. CoM směřuje ke stabilizaci výsledku. V případě zvažovaného nasazení nemá tento přístup zjevně velký význam a nebude prozatím uvažován.

Obr. 30 *Jednoduchý jednovrstevný perceptron*



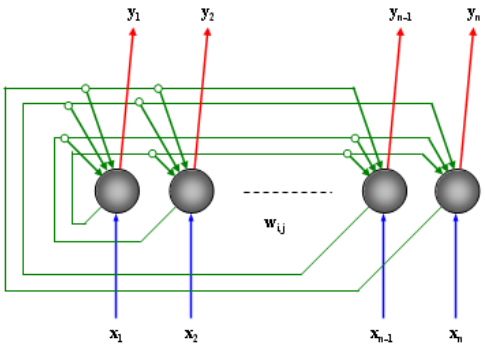
Zdroj: [94]

Obr. 31 *Vrstvená neuronová síť s šesti neurony*



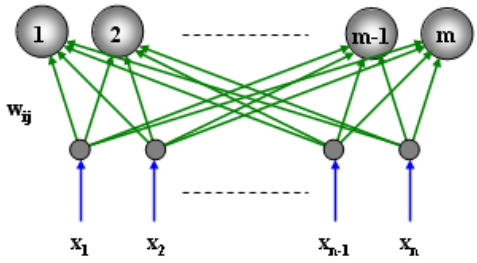
Zdroj: upraveno dle [62]

Obr. 32 *Topologie rekurentní Hopfieldovy sítě*



Zdroj: [95]

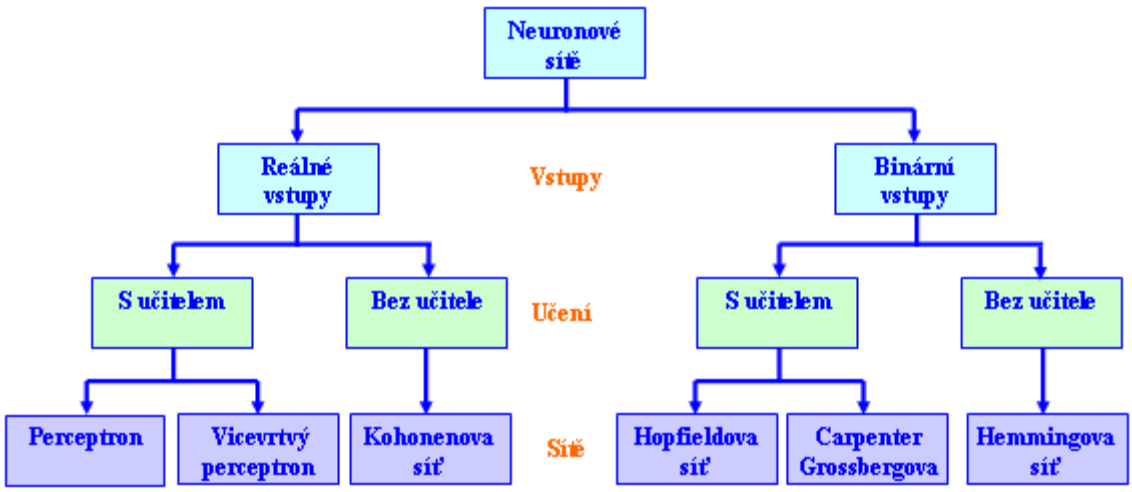
Obr. 33 *Zjednodušený model Kohenovy mapy*



Zdroj:[95]

Souhrnně lze tedy neuronové sítě rozdělit podle celé řady kriterií (viz Obr. 34), z nichž podstatné typy jsou v předchozí části zběžně popsány včetně definice jejich možného použití. A to je právě rozhodující pro volbu v konkrétním případě jako integračního nástroje informačních systémů a to nejenom poplachových.

Obr. 34 *Základní rozdělení umělých neuronových sítí s vyznačením kriterií*



Zdroj: [94]

Zcela je prozatím opominuta problematika učení těchto sítí s tím, že tento klíčový aspekt bude posouzen až následně po provedených testech jednotlivých architektur. V tuto

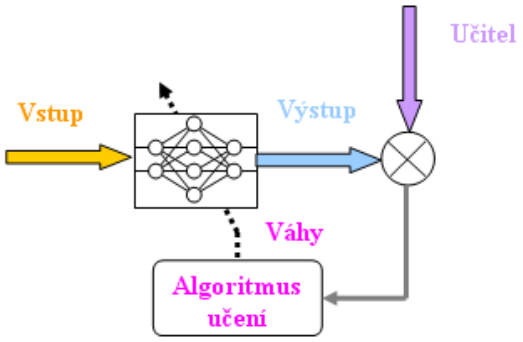
chvíli lze předběžně definovat obecně platné základní předpoklady týkající se procesu učení neuronových sítí.

Cíl učení je proces, kdy probíhá nastavení váhy spojení mezi neurony tak, aby síť generovala požadovanou správnou výstupní hodnotu na vstupní signál[74].

Učení s učitelem (supervised learning): srovnává se aktuální výstup ze sítě s požadovaným výstupem (učitelem). Změnou vah se minimalizuje rozdíl mezi tímto výstupem a učitelem[71].

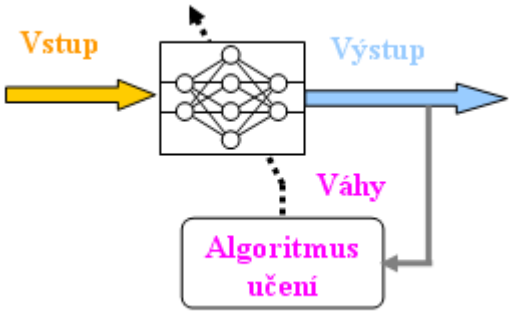
Učení bez učitele (unsupervised learning): změnou vah je třeba docílit konzistentní výstup, tj. aby síť poskytovala při stejných vstupních (nebo alespoň podobných) hodnotách, stejné hodnoty výstupní. [71]

Obr. 35 *Učení s učitelem*



Zdroj: [94]

Obr. 36 *Učení bez učitele*



Zdroj: [94]

Používání umělých neuronových sítí se skládá ze dvou základních kroků. Prvním z nich je tzv. "trénink", druhým pak "předpovídání" neboli predikce. Trénink se skládá nejdříve z definice vstupních a výstupních hodnot. Obvykle je nezbytné vkládaná data vhodně upravit a normalizovat tak, aby je byla síť schopna pojmout. Tato data poté tvoří tzv. "tréninkovy set". V této fázi jsou hledány optimální struktury a váhové koeficienty pro dané informace[71]. Trénink je považován za kompletní, jakmile neuronové sítě dosáhnou

požadované statistické přesnosti a produkují vhodné výstupy vůči vstupním datům. [7][27] [30].

Vhodné kritérium pro nalezení správné síťové struktury a tudíž zastavení tréninkového procesu, je minimalizace střední hodnoty kvadrátu chyby (root mean square error = RMS) [88].

$$RMS = \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(x_{ij} - y_{ij})^2}{NxM}} \qquad (1)$$

kde x_{ij} je prvkem matice N x M pro tréninkový set

y_{ij} je prvkem matice N x M pro výstupní matici

N je počet proměnných v matici

M je počet vzorků

Ve spojitosti s vícevrstvými neuronovými sítěmi je nutné podrobněji analyzovat i nejčastěji používaný algoritmus učení v tomto typu sítí. Všeobecně se použití této metody učení odhaduje na 80% všech aplikací neuronových sítí. Uvedený algoritmus (**Back-propagation of error**) je postup, kdy je chyba na výstupu zpětně šířena do skrytých vrstev neuronů a podle ní jsou upravovány hodnoty váhových propojení jednotlivých neuronů.

Celý postup je zpravidla pro snazší implementaci rozdělován do 3 samostatných kroků:

- dopředné šíření signálu
- zpětné šíření chyby
- aktualizace váhových spojení

V prvním kroku je šířen vstupní signál z tréninkové množiny skrze neurony $\mathbf{x_k}$ vstupní vrstvy do sítě. Za tuto trénovací množinu lze považovat vzory, které jsou definovány jako dvojice následujícím způsobem:

$$T = \left\{(x_k, t_k) \middle| x_k \in \{0,1\}^n, t_k \in \{0,1\}^m, k = 1,...q\right\} \qquad (2)$$

kde :

$\boldsymbol{q}$ počet vzorů v trénovací množině,

$\boldsymbol{x_k}$ vektor excitací vstupní vrstvy tvořené $\boldsymbol{n}$ neurony,

y_k vektor excitací výstupní vrstvy tvořené m neurony.

Následně každý neuron vypočítá svou aktivaci dle vlastní aktivační funkce. Poté jsou srovnávány takto vypočítané hodnoty s definovanými hodnotami výstupu neuronů y_m pro každý vzor z trénovací množiny. Na základě tohoto porovnání vzniká chyba sítě $E(w)$, kterou lze definovat následujícím vzorcem:

$$E(w) = \sum_{l=1}^{q} E_l(w) \tag{3}$$

Jedná se tedy o součet jednotlivých chyb vzhledem ke vzorům v trénovací množině. Tyto jednotlivé chyby lze vypočítat pomocí vzorce:

$$E_l(w) = \frac{1}{2} \sum_{k \in Y} (y_k - t_k)^2 \tag{4}$$

Je to v podstatě součet druhých mocnin odchylek výstupu sítě skutečných a požadovaných hodnot pro l-trénovací vzor. Závislost celkové chyby na počtu cyklů sítě popisuje chybová funkce. Jelikož je cílem minimalizovat tuto chybu, je tedy hledáno globální minimum v této chybové funkci.

Z výše uvedených poznatků lze očekávat, že optimální zřejmě bude využití vícevrstvého perceptronu s učením s učitelem, případně použití Kohonenovy mapy s učením bez učitele. Dokud však neproběhne modelování všech předložených variant, není možné jednoznačně rozhodnout o definitivním řešení (např. Hopfieldova síť dává rovněž slušnou pravděpodobnost ke korektnímu řešení, lze zde však spíše očekávat technické problémy při vlastním procesu učení [61][62][86]).

4.4.2 Výběr vhodného prostředí pro modelování sítí

Po prvních testech je zřejmé, že většina simulací a modelování proběhne v prostředí **Matlab** verze R2011a. V tomto prostředí se využívá programovací jazyk, který se vyvinul z původního jazyka Fortran a je tedy pro tyto výpočty a modelování obecně

vhodný. Ukazuje se však nezbytným doplnit základní systém Matlabu o některé Tolboxy, především **Matlab Neural Network Toolbox**. [14][15][17] Tato knihovna mohla být zatím otestována pouze velice zběžně, byla zapůjčena i s PC z fakulty dopravní ČVUT, pro další práci bude potřeba ji zakoupit či dlouhodobě zapůjčit. Další komponentou, která bude nezbytná pro posouzení vhodnosti nasazené architektury je **Statistica Neural Network**. Tato komponenta je již zakoupena na ČZU, bude možné ji tedy využívat k práci. Jako poslední nástroj, který se při vlastním režimu modelování ukázal jako velice zajímavý a snadno použitelný je nástroj **NeuroSolution *7*** od společnosti NeuroDimension Ltd. Nejen, že je uvedený nástroj poměrně snadno ovladatelný, ale jeho výsledky i na méně výkonném HW jsou velice uspokojivé. Zásadní nevýhodou je však omezení pro freewarevou licenci. Díky tomu bylo nutné některé zablokované postupy obcházet jinými nástroji.

Na trhu se vyskytuje velké množství konkurentů produktu MATLAB. Z komerčních nástrojů to jsou například **Mathematica**, **Maple**, **IDL** od společnosti ITT Visual Information Solutions nebo také **Metlynx**. Existují také open source alternativy k systému MATLAB, jako je GNU **Octave**, **FreeMat** a **Scilab**, které jsou jazyku MATLABu relativně blízké, ovšem kvality prostředí MATLAB zdaleka nedosahují. Také se používají různé knihovny, které přidávají podobnou funkčnost jako má MATLAB do jiných již existujících jazyků. Takovýmito knihovnami jsou například **IT++** pro C++, **Perl Data Language** pro Perl nebo **SciPy** společně s **NumPy** a **Matplotlip** pro Python. Vzhledem k prováděným testů však bylo primárně využito právě programu MATLAB s tím, že pokud to bude možné, jsou výsledky porovnány s výsledky získanými v programu NeuroSolution a případně v programu Mathematica, se kterým jsou v tomto případě rovněž dobré zkušenosti. [13][14][15]

4.4.3 Vyhodnocení vybraných modelů

Vzhledem k tomu, že při testování vhodného modelu neuronové sítě bude klíčovým kriteriem spolehlivost rozeznání příslušného stavu na sběrnici, bude vyhodnocení významnosti řešení probíhat obvyklými statistickými nástroji, který je ve většině uvedených programů již přímo implementován. Kromě spolehlivosti rozeznání však bude muset být zohledněna i doba učení, rychlost jeho konvergence a případně technická náročnost. [15][17]

Podle zkušeností z literatury[26][27][30][31][64] i podle zkušeností z testů realizovaných modelů, je obecně možnost integrace bezpečnostních systémů s využitím neuronových sítí realizovatelná. Navrhovaná metoda neuronového klíče je původní a využití těchto principů při řešení zvažovaného problému nebylo dosud popsáno v žádné literatuře.

4.4.4 Získání dat k modelování

Je samozřejmě možné pro modelování a testování neuronového klíče použít v podstatě libovolná data a přiřadit jim jednotlivé stavy ústředny PZTS které je potřeba vyhodnotit. Protože se však předpokládá přímé praktické nasazení modulu, bylo rozhodnuto v tomto případě pracovat přímo s konkrétními daty (stavy) ústředny. A to s sebou samozřejmě přineslo určité problémy.

Především, pokusit se číst přímo komunikaci na sběrnici ústředny je po úvodních drobných problémech poměrně jednoduché, je však třeba si uvědomit, že data jsou v šifrované podobě a pokusit se je dešifrovat by bylo porušení autorských práv (zmíněno již v Kap.3.2). Navíc by tím padl i hlavní argument pro tento způsob integrace – modul musí být schopen detekovat stavy libovolného systému s libovolným šifrováním (podmínkou je určitá časová setrvačnost šifry nezbytná pro samoučící schopnost modulu, alternativně učící se schopnost s učitelem).

Proto byly zvoleny dva přístupy. Pro první testování byla data z ústředny získávána prostřednictvím výrobcem PZTS ústředny dodávaného komunikačního rozhraní (v tomto případě modulu PRT3 – viz. Obr.19). To má výhodu jednak v jednoduchosti zapojení, jednak v tom, že bylo možné rychle a snadno ověřit stavy, které se zrovna generovaly na sběrnici. Navíc modul umožňuje přímé ukládání dat do ASCII souboru, což opět výrazně zjednodušilo testování.

Komponentu PRT3 je možné použít pro tisk prostřednictvím tiskárny připojené na paralelní port modulu. Dále je možné pomocí sériového portu či portu USB připojit modul na PC a sledovat stavy a události, které vznikají na celém systému. Mimo samotné načítání těchto informací lze ale prostřednictvím modulu i systém ovládat. Slouží k tomu příkazy, pomocí nichž je možné systém uvést do střežení a následně zase vypnout. Dále je k dispozici příkaz, který na ústředně vyvolá Panik poplach, a nakonec dotazy, pomocí nichž lze získat aktuální informace o dění na konkrétní zóně či podsystému. Následující tabulky Tab.3 a Tab. 4) popisují posloupnosti znaků u vybraných dotazů a příkazů, jimiž lze ústřednu ovládat, a možné odezvy přijímané zpět z ústředny. [102]

Tab. 3 Řídící sekvence ústředny PZTS

Dotaz na stav zóny											
byte	1	2	3	4	5	6	7	8	9	10	11
	R	Z	0	X	X	<cr>					
Obdržená informace											
byte	1	2	3	4	5	6	7	8	9	10	11
	R	Z	0	X	X	byte 6	byte 7	byte 8	byte 9	byte 10	<cr>
byte 6		byte 7		byte 8		byte 9		byte 10		**pozn. X = číslo zóny**	
C-zavřena O-otevřena		A-v poplachu		F-požár		S-porucha dohledu		L-slabá baterie			
T-tamper F-porucha		O-OK		O-OK		O-OK		O-OK			

Tab. 4 Struktura řídícího paketu

byte	1	2	3	4	5	6	7	8	9	10	11	12	13
	A	A	0	0	X	byte 6	byte 7	byte 8	byte 9	byte 10	byte 11	byte 12	<cr>
byte 6	byte 7		byte 8		byte 9		byte 10		byte 11		byte 12		
A-běžné F-force S-stay I-stay bez zp.	uživatelský kód číslo 1		uživatelský kód číslo 2		uživatelský kód číslo 3		uživatelský kód číslo 4		uživatelský kód číslo 5		uživatelský kód číslo 6		
pozn. X = číslo podsystému													

Celkový počet všech možných stavů, které se mohou objevit na výstupu tiskového modulu, je 22 564. Tyto stavy jsou však reprezentovány sekvencí ASCII kódu ve formátu uvedeném v následující tabulce.

Tab. 5 Formát dat na sběrnici (modul PRT3)

Událost													
Byte	1	2	3	4	5	6	7	8	9	10	11	12	13
Data	**G**	x	x	x	**N**	y	y	y	**A**	z	Z	z	

V této struktuře platí:

xxx – skupina událostí

yyy – událost

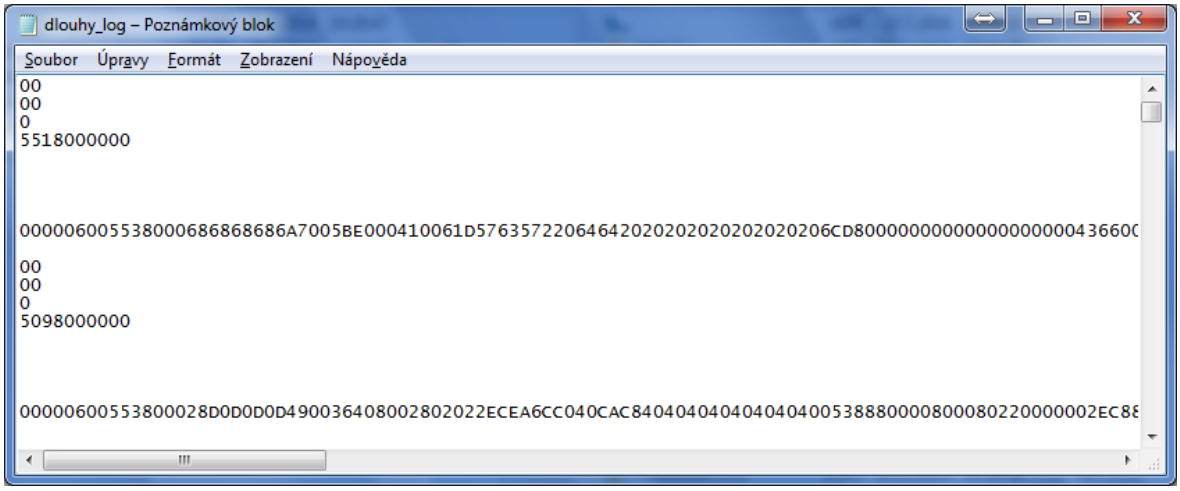
zzz – číslo (vyplývá z charakteru událostí – číslo zóny, uživatele atd.)

Z modulu PRT3 jsou tedy výstupní data ve výše uvedené struktuře. Pro zpracování neuronovou sítí se však tato struktura dat příliš nehodí, proto byl vytvořen krátký program (viz. Příloha 8), který z uvedeného textového souboru vybere pouze konkrétní data, tato převede do binární podoby a uloží je ve struktuře dat vhodné pro import do programu

Matlab (binární soubor, data uloženy ve sloupcích). Tato data pak byla následně testována na několika typech sítí (viz. Kap.5).

Jak bylo řečeno v úvodu této kapitoly, tento způsob získávání dat je sice jednoduchý a praktický pro ladění, není však příliš podobný očekávanému reálnému provozu neuronového klíče. Proto bylo v druhé etapě využito řešení, které nabízí na svých webových stránkách Martin Harazinov *(http://harizanov.com/2013/05/interfacing-with-paradox-home-security-system/ cit. 2.3.2014*). Úmyslně na tomto místě nebude použitý postup získání dat na zmíněných stránkách komentován, je důvodný předpoklad, že autor na svých stránkách jde výrazně za hranu autorských práv. V postupu řešeném v této práci však nedochází k dekódování stavů či pokusům o dekódování komunikace na sběrnici, pouze o získání její binární podoby. Protože se však jedná o potenciálně poměrně snadno zneužitelný postup, nebude zde ani na hardwarové, ani na logické vrstvě popisován. V každém případě je výsledkem řada bitů organizovaných do paketů, které nelze přiřadit ke konkrétním stavům poplachového systému. *Na tomto místě bych velice rád poděkoval Ing. Janu Kuchařovi za pomoc při načítání reálných dat na sběrnicích systémů PZTS.*

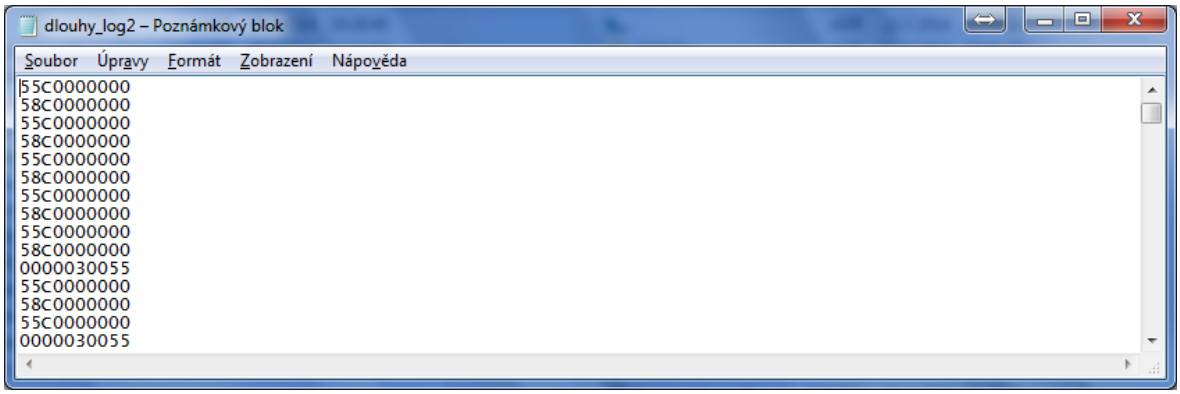
Obr. 37 *Nezpracovaná struktura dat*



Zdroj: [112][51]

Automatickou úpravou dat dle vlastního programu byla získána data v následující struktuře:

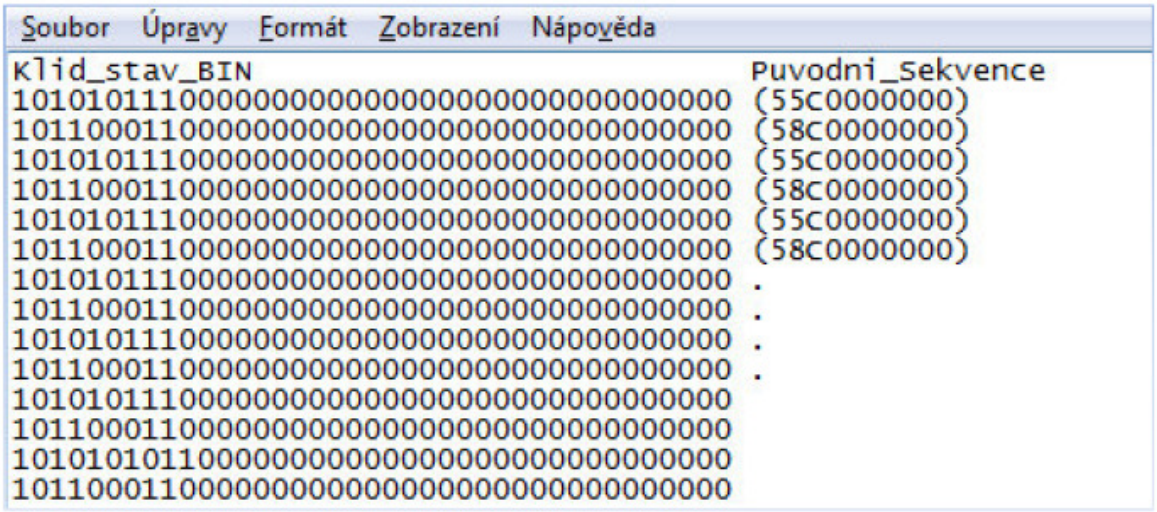
Obr. 38 *Parsování dat a filtrování*



Zdroj: [112][51]

Následně bylo potřeba data konvertovat podobně jako v případě použití modulu PRT3 (převézt do binární podoby, hodnoty uloženy ve sloupcích a ne v řádcích):

Obr. 39 *Změna struktury dat vhodná pro neuronové zpracování*



Zdroj: [112][51]

Data byla konvertována a připravena ke zpracování v programu Matlab a NeroSolution obdobným programem jako v případě konverze dat z modulu PRT3 (viz.

Příloha 6). V tuto chvíli bylo již možné začít s vytvořením modelu, jeho učením a ověřením funkce celého neuronového klíče – viz. Kap. 5.

4.5 Integrace prostřednictvím protokolu SIA09

Jak již bylo předesláno v kapitole 4., při činnosti autora této práce v Technicko normalizační komisi TNK 124 byl projednáván z pohledu integrace velice zajímavý dokument – technicko normalizační informace SIA DC-09 s označením **TNI 33 4592**. Tento protokol je nejmodernějším protokolem pro komunikaci po datových sítích. Vznikl z iniciativy Asociace pro požární ochranu v USA a Kanadě ve spolupráci s dalšími významnými institucemi SIA, FIPS, NIST. Převzalo jej více než 60 předních světových firem (např. Honeywell, ASIS, Bosch, Siemens atd.)[75]. Zavádí nové a velmi silné možnosti šifrování zpráv (AES 192 pro objekty zvláštní důležitosti). Uvnitř svého formátu může přenášet všechny známé komunikační formáty objektových zařízení. Rovněž obsahuje rozsáhlé možnosti verifikace událostí vzniklých ve střeženém objektu. Přední světoví výrobci tento protokol již běžně používají ve svých zařízeních (např. Technoalarm, Texecom atd.). V ČR tento protokol zatím neměl oporu v normě a proto jej většina prodejců a tvůrců ústředen a PCO na českém trhu neimplementovala.

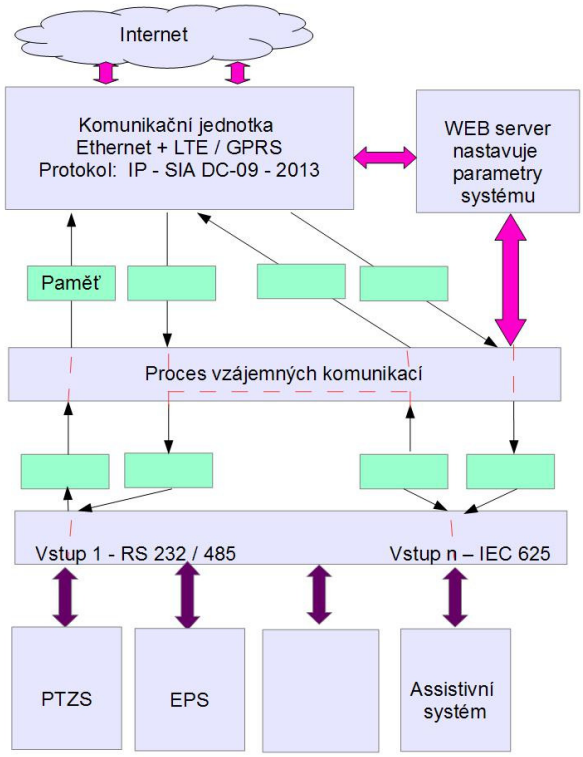
Z pohledu integrátora je standart protokolu SIA09 zajímavý především v tom, že umožňuje definovat v podstatě libovolná data do přenášeného paketu bezpečnostní komunikace a to bez ztráty zabezpečení související s nárůstem délky paketu (což je většinou významný problém). Samotná definice protokolu je poměrně náročná (21 stran normy), nebude tedy na tomto místě popisována. Podstatnější jsou však praktické dopady zavedení protokolu. Ve své podstatě protokol umožňuje bezpečným způsobem, s minimálními požadavky na přenosové pásmo a přenosovou rychlost nejenom přenášet konkrétní data mezi dvěma uzly sítě (typicky PCO a PZTS), ale lze alternativně zvolit, že některá z přenášených dat budou (současně a verifikovaně) přenesena na jiný uzel (např. přímo zásahové vozidlo), aniž by se musel realizovat jiný (problematicky zabezpečený) přenos. Významné je tedy především to, že je k dispozici konečně protokol, který v komunikaci DPPC zavádí[114]:

- synchronizaci času v celé síti,
- sjednocuje komunikaci PZTS, EPS, CCTV a další,
- zavádí časové razítko u každé přenášené zprávy i potvrzovací zprávy,

- zavádí obousměrnou komunikaci mezi PCO a ústřednou,
- zavádí další metody kódování zpráv pro každý objekt,
- zavádí vícenásobnou identifikaci zdrojů (MAC, ID, Dev. no, IP),
- zavádí povinnost starat se o šířku přenášeného pásma,
- umožňuje ovládat technologie objektu bez možnosti zneužití,
- komunikace se řídí mezinárodně platnými předpisy pro datové sítě (RFC).

Zavedení tohoto nástroje je konečně krokem správným směrem v oblasti bezpečnostní komunikace. Autor této práce je však přesvědčen, že tento nástroj je i ideálním pro vlastní integraci bezpečnostních systémů. Již předkladatel této normy v ČR p. B. Vrbovec naznačoval možné využití dle následujícího schématu.

Obr. 40 *Možné použití protokolu SIA09 pro integraci bezpečnostních systémů*



Zdroj: [114] nepopsané bloky nemají význam pro předpokládané užití

Tento návrh je jistě dobré potenciální řešení integrace, lze jej však posunout ještě o něco dále. Návrh a možná řešení realizace je předloženo v Kap.5.4.

5 VÝSLEDKY

Vzhledem k tomu, jaké cíle práce byly definovány v kapitole 3, bylo nutné průběžně s probíhajícím měřením a zpracováním jejich výsledků upravovat jednak metodiky navazujících testů, jednak jejich vyhodnocení. To především z toho důvodu, že se tato práce pokouší porovnat několik možných integračních nástrojů, které jsou založeny na různých technických i technologických řešení. A protože bylo snahou získat výsledky alespoň na základní úrovni srovnatelné, bylo nutné některé z testů provádět výrazně podrobněji, než bylo původně zamýšleno a v některých případech bylo nutné provádět i doplňkové měření a vyhodnocení, přesto, že v počátku práce a měření se toto nepředpokládalo. Týká se to především testů integrace bezpečnostních systémů prostřednictvím programových výstupů, které byly následně definovány jako porovnávací a proto bylo nutné provézt testování v dostatečně dlouhém časovém intervalu a podrobněji je statisticky zpracovat.

5.1 Výsledky měření integrace prostřednictvím programových výstupů ústředny PZTS a jejich základní zpracování

Metodika měření tohoto způsobu integrace byla již popsána v Kapitole 4.2. Realizovalo se testování dlouhodobé funkčnosti a spolehlivosti propojení poplachových systémů mezi sebou prostřednictvím programových výstupů PGM (relé aktivované událostmi bezpečnostního systému). Původní testy prováděné na testovací aparatuře Digiplex Evo 48 s PGM expandérem sice ověřily funkčnost tohoto řešení, ale i při dlouhodobém testování v laboratoři nebylo možné získat zpracovatelné výsledky, neboť systém v laboratorním prostředí fungoval zcela bez závad a to i při pokusu o jeho rušení, simulaci výpadku napájení a podobně. Jediným zajímavým výsledkem mající relevanci k tématu práce bylo zjištění propojení obvodu dobíjení záložního akumulátoru s napětím na výstupu programových výstupů (PGM), což způsobovalo zcela nahodilou chybu při aktivaci/deaktivaci PGM. Po několika seriích měření byl zjištěn důvod a prostřednictvím dodavatele kontaktován výrobce. Chyba byla opravena v nové verzi firmware 2.15. Bezdrátové PGM uvedené problémy pochopitelně neobsahují. Na základě těchto

zkušeností bylo sestaveno několik reálně komerčně použitelných sestav, které byly instalovány do běžného provozu. Vzhledem k tomu, že jako koncesovaná osoba a revizní technik s oprávněním na tato zařízení mohl autor této práce uvedené systémy nejen komerčně instalovat, ale i dlouhodobě provádět předepsané revize, podařilo se získat poměrně zajímavé výsledky, které jsou již zpracovatelné pro obsah této práce a mají i další přínos pro instalační firmy i výrobce a prodejce poplachových systémů.

5.1.1 Popis sestav a jejich testování

Podle zadání nebyl předen definován typ objektů pro předpokládanou integraci, byly proto zvoleny takové sestavy, aby byla postižena co nejširší oblast možného nasazení. Na druhou stranu, jak je již popsáno v kapitole 4.2, je způsob integrace pomocí PGM vhodný především pro menší a střední objekty spíše bytového či kancelářského provozu. Proto byly vybrány (i vzhledem k požadavkům klientů) pro testování následující sestavy:

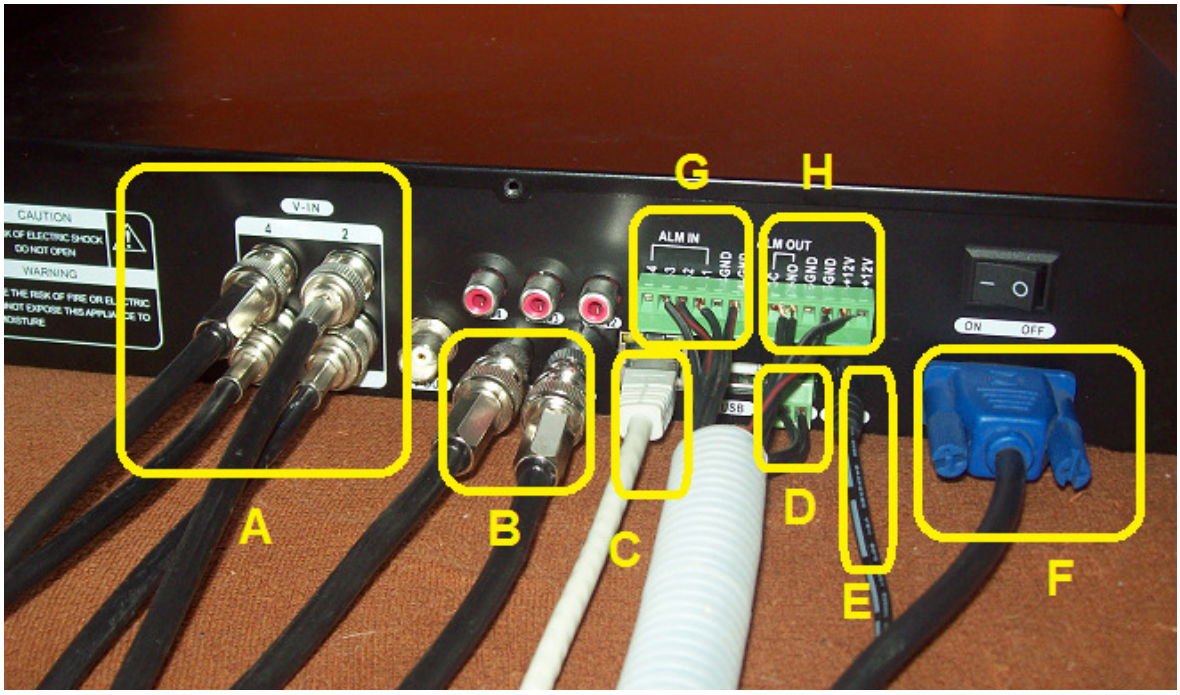
1. **sestava**: hybridní systém Magellan 5050 s převážně bezdrátovými rozvody, celkem 13 detektorů (z čehož 2 drátové), jedna klávesnice drátová, druhá bezdrátová, vnitřní a venkovní siréna, komunikace přes GSM bránu (VT20) a počítačovou síť (IP100). Pomocí PGM byla propojen přístupový systém (vjezdová vrata na pozemek, vrata do garáže, později branka), kamerový systém (3 analogové kamery pevné, jedna kamera s PTZ) a protipožární systém (2 autonomní kouřové hlásiče s možností připojení na PZTS a jeden teplotně diferenciální detektor rovněž připojitelný na PZTS). V závěrečné etapě testování došlo k integraci se systémem vytápění (elektrický kotel Protherm Rejnok 12K). Integrace i provoz proběhl bez problémů, nejedná se však o integraci dvou poplachových systémů, takže jsem toto dále nezapracovával do výsledků. Instalace proběhla v rodinném domě střední velikosti na Praze – západ, uživateli objektu je jedna rodina (2 dospělí + jedno dítě). Doba sledování systému v tomto objektu byla **1938 dnů**.
2. **sestava**: hybridní systém Magellan 5050 s převážně drátovými rozvody, celkem 21 detektorů (z čehož 6 bezdrátových), jedna klávesnice drátová, druhá bezdrátová, vnitřní a venkovní siréna, komunikace přes GSM komunikátor (PCS200) a počítačovou síť (IP100). Integrace byla provedena s již stávajícím analogovým kamerovým systémem (3 kamery), zhruba po roce sledování byla provedena integrace s plynovým topením (DAKON P 30 LUX HL) a integrace systému PZTS se stávajícími autonomními detektory zemního plynu a CO. Instalace proběhla v rodinném domě střední velikosti

na Praze Lysolajích, uživateli objektu jsou dvě rodiny (rodiče a jejich dcera s manželem a vnučkou). Doba sledování systému v tomto objektu byla **780 dnů**.

3. **sestava**: sběrnicový systém Digiplex Evo 48 s převážně drátovými rozvody (použití expandérů). V roce 2014 se systém rozšiřoval a bylo využito několik bezdrátových detektorů. Celkem 11 detektorů (3 bezdrátové), 1 drátová klávesnice, vnitřní siréna, komunikace přes GSM komunikátor (PCS250) a počítačovou síť (IP100). Integrace byla provedena se současně budovaným kamerovým IP systémem, který se v roce 2014 rozšířil o další IP kameru. K systému jsou připojeny 1 ks snímače kouře a 1 teplotně-diferenciální detektor. Rovněž se PZTS využívá pro zajištění příchodu a odchodu z objektu - přístupový systém (vstupní dveře trvale zamčeny, odemyká je pohybový detektor uvnitř objektu). Instalace proběhla v kancelářských prostorách v blízkosti Václavského náměstí. Doba sledování systému je **920 dnů.**
4. **systém**: sběrnicový systém GalaxyDimension 264 s čistě drátovým řešením rozvodu. V systému je pomocí expandéru připojeno 32 detektorů, 11 požárních hlásičů a signalizace havárie (detekce zemního plynu, CO, únik vody). Systém je integrován se současně budovaným kamerovým systémem (5 kamer vnitřních, 2 kamery vnější). V systému je pouze jedna klávesnice, vnitřní a venkovní siréna, GSM komunikátor (GxySmart) a IP komunikátor (E080-4). Uvedený systém je instalován v ubytovacím středisku v jižních Čechách. Doba sledování systému **64 dnů** (systém je v testovacím provozu).

Vzhledem k tomu, že vlastní integrace je ve většině případů technicky poměrně triviální záležitost – viz např. schéma Obr. 20 v Kap. 4.2., není při dobré přípravě a kvalitním projektu realizace vlastní integrace problém. Je pouze potřeba, aby byl integrující technik poměrně detailně seznámen se všemi integrujícími systémy. Vzhledem k parametrům provozu byl zvolen jako standard integraci sestavy č. 1 (nejvíce integračních prvků, nejdelší doba sledování). V tomto případě to znamená propojit PGM ústředny se vstupem DVR kamerového systému, poplachový výstup DVR (detekce pohybu, identifikace/negativní osoby) s poplachovou smyčkou PZTS a následně propojit výstupy sběrnice RS485 s ovládání PTZ konkrétní kamery. Příklad zapojení je na následujícím obrázku Obr. 41 (na straně DVR, kde je zřejmě nejobtížnější zapojení).

Obr. 41 *Schéma propojeni DVR a PZTS*



Zdroj: [111]

Legenda k obrázku: *(DVR Qihan QH-D21104B-A*)

A: vstupy kamer (koax)

B: zvukový vstup a výstup pro kameru 1 (s PTZ)

C: datová síť (UTP)

D: ovládaní PTZ přes RS232

E: napájení DVR

F: výstup na monitor (VGA)

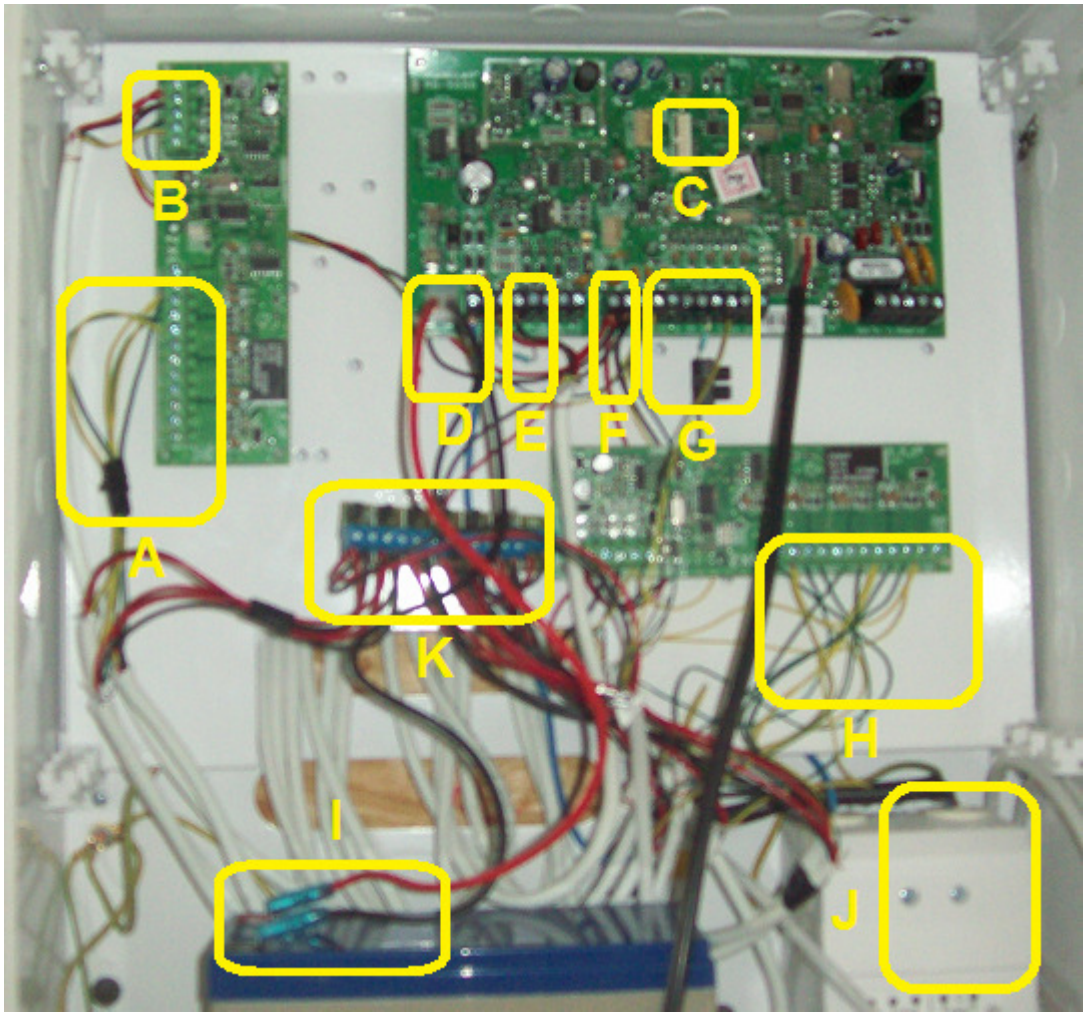
G: poplachové vstupy (aktivace typu záznamu a automatizace PTZ)

H: poplachové výstupy (detekce pohybu + identifikace osoby)

Na straně ústředny PZTS je zapojení ještě jednodušší, opět bude demonstrováno na konkrétní instalaci systému č.1. Po několika nepříjemných zkušenostech s komerčními instalacemi především středně velkých a větších projektů, bylo rozhodnuto upustit od zapojování detektorů pomoci vyvažovací smyčky (dva detektory na jedné smyčce) a raději volit instalaci jeden detektor na smyčce s kontrolou napadení vedení (jmenovitý odpor na

detektoru). Proto je v konečném projektu zvoleno použití expandérů, byť je to o něco dražší řešení, právě při integraci však dává výrazně větší možnosti (každý expandér obsahuje 1 – 2 další PGM) – viz. Obr. 42.

Obr. 42 *Schéma zapojení ústředny PZTS s DVR*



Zdroj:[111]

Legenda k obrázku: *(MG5050 + 2x ZX8SP)*

A: smyčky expandéru 1 (detektory)

B: napájení + PGM expandéru 1

C: připojení GSM komunikátoru

D: připojení záložního akumulátoru

E: PGM ústředny

F: sběrnice ústředny (klávesnice a sběrnicové moduly)

G: smyčkové vstupy detektorů režimu NC

H: smyčky expandéru 2 (detektory)

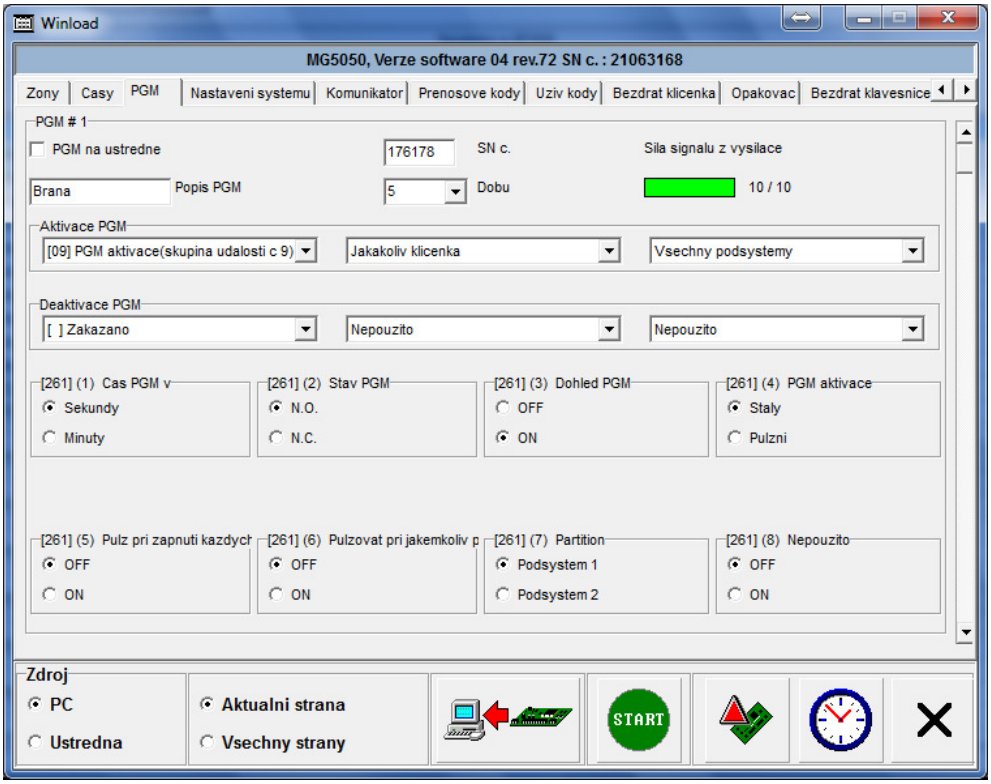
I: záložní akumulátor

J: primární zdroj el. energie

Tímto způsobem bylo provedeno zapojení dle výše popsaných metod integrace (systém 1 – systém 4). K plné funkčnosti propojení systému bylo nezbytné nastavit vhodné aktivační události PGM (na ústředně PZTS) resp. PGM (na DVR CCTV) a propojit je způsobem popsaným v popisu činnosti jednotlivých systémů (pro systém č. 1 např. dle Obr. 20).

Velice častý problém, který nastával při integraci různých systémů spočívá v tom, že některé systémy pro svoji aktivaci vyžadují různé délky sepnutí aktivačního vstupu, resp. je potřeba aktivační vstup nastavit po celou dobu aktivace sepnutý (klasicky některé pohony garážových vrat Hörmann Supramatic). Proto je důležité uzpůsobit této okolnosti i chování příslušného PGM výstupu. Zde například nastavení aktivace a chování bezdrátového PGM systému 1 používaného k otevírání pojezdových vrat pro vjezd na pozemek:

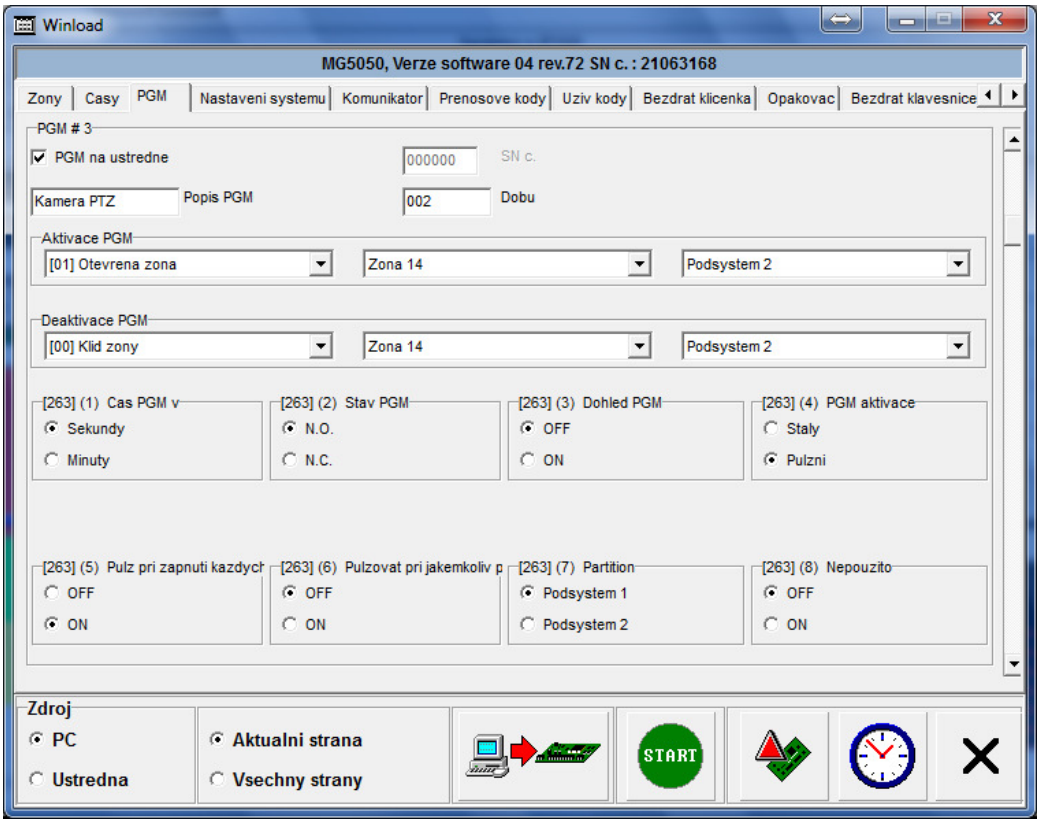
Obr. 43 *Nastavení ústředny PGM pro propojení s ACC*



Zdroj: [111]

Naopak nastavení a natočení PTZ kamery při otevření garážových vrat směrem na garážová vrata a sejmutí plné sekvence videodat je možné aktivovat následujícím nastavením PGM:

Obr. 44 *Aktivace natočení kamery PTZ pomocí PGM v ústředně*



Zdroj: [111]

5.1.2 Měření a základní vyhodnocení

Problém v integraci tímto způsobem tedy není ve velké náročnosti na technické vybavení či rozsáhlost dalších nezbytných komponent. Naopak, zvolený způsob se po celou dobu testování jevil jako velice nenáročný po technické stránce po celou dobu instalace i provozu. Klade však výrazně větší nároky na projekčního technika než jiné (dále popsané) metody. Co se však v průběhu testování uvedených systémů jevilo jako potenciální problém, byla nejistota, zda dlouhodobý provoz takto integrovaných systémů nezvyšuje celkovou poruchovost a chybovost celého integrovaného systému jako celku a případně i jednotlivých dílčích částí[6]. Tento názor poměrně často citován v české i zahraniční literatuře. Bylo tedy v prvé řadě potřeba ověřit spolehlivost celého systému před integrací a následně po integraci a vyhodnotit případné zvýšení pravděpodobnosti poruchy, eventuálně míru ovlivnění poruchy jednoho systému systémem jiným, s ním integrovaným.

Pro toto ověření sloužila data z ústředen PZTS (historie logu událostí), která byla pravidelně (zpravidla jednou za měsíc) prostřednictvím datové sítě z ústředen stahována a průběžně vyhodnocována. Protože některé systémy byly provozovány řadu let, je předpoklad, že případné navýšení poruchovosti po integraci se poměrně průkazně projeví.

V testu byly sledovány následující parametry:

a) počet planých poplachů
b) počet falešných poplachů
c) počet poruch systému degradující celkovou funkci systému (např. porucha komunikátoru, porucha zvukové signalizace, porucha rozvodů)
d) chyba uživatele způsobující buď poruchu systému či vyvolání planého poplachu
e) počet pokusů o proniknutí do systému (vloupání či neoprávněný přístup) detekované systémem
f) počet pokusů o proniknutí do systému (vloupání či neoprávněný přístup) nedetekovaný systémem

V následujících tabulkách jsou uvedena celková data pro jednotlivé sledované sestavy.

V první tabulce jsou uvedena data pro období bez integrace, v další tabulce pak data po integraci výše popsaných systémů.

Tab. 6 Struktura stavů systému od okamžiku instalace do integrace s dalšími poplachovými systémy

	Systém 1	Systém 2	Systém 3	Systém 4
Počet dnů provozu (do integrace)	557	420	889	0
Počet planých poplachů	7	24	30	0
Počet falešných poplachů	4	3	2	0
Počet kritických poruch systému	6	1	11	0
Počet kritických chyb uživatele	19	35	82	0
Počet pokusů o proniknutí do systému	2	0	1 ?	0
Počet úspěšných průniků do systému	0	0	0	0

Tab. 7 Struktura stavů systému od okamžiku integrace s dalšími systémy

	Systém 1	Systém 2	Systém 3	Systém 4
Počet dnů provozu (od integrace)	1379	299	31	64
Počet planých poplachů	30	14	3	2
Počet falešných poplachů	2	3	1	0
Počet kritických poruch systému	15	0	0	1
Počet kritických chyb uživatele	8	20	1	15
Počet pokusů o proniknutí do systému	1	0	0	2
Počet úspěšných průniků do systému	0	0	0	0

Po statistickém zpracování[6] (počet událostí na jeden den vyjádřeno v procentech), byly získány následující výsledky:

Tab. 8 Přepočtené kritické události

	Systém 1		Systém 2		Systém 3		Systém 4	
	před	po	před	po	před	po	před	po
Počet dnů provozu (od integrace)	557	1379	420	299	889	31	0	64
Poměr planých poplachů	1,2%	2,1%	5,7%	4.7%	3,3%	9.6%	null	3,1%
Poměr falešných poplachů	0.7%	0.1%	0.7%	1 %	0.2%	3.2%	null	0 %
Poměr kritických poruch systému	1 %	1 %	0.2%	0 %	1.2%	0 %	null	1.5%
Poměr kritických chyb uživatele	3.4%	0.6%	8.3%	6.7%	9.2%	3.2%	null	23%

Poznámka: *označení „**před**“ znamená provoz před termínem integrace, „**po**“ znamená provoz po datu integrace (platí i nadále v tabulkách)*

Před tím, než je možné vyhodnotit získaná a výše uvedená sumarizovaná data, bude vhodné ověřit, že uvedené sestavy odpovídají doporučeným hodnotám pro plané a falešné poplachy bezpečnostních tříd dle ČSN EN 50 131 – 7. Dle této normy a doporučení AGA z roku 2013 platí, že množství planých poplachů u systémů třídy 1 a 2 je maximálně 1 poplach za týden, u systémů třídy 3 a 4 maximálně 1 poplach za dva týdny. Množství falešných poplachů u systémů s bezpečnostní certifikací 1 a 2 je 1 za rok, u třídy 3 jednou za dva roky a u třídy 4 nesmí vůbec nastat. V testovaných sestavách v případě sestavy 1 a 2 jsou certifikovány v bezpečnostní třídě 2 a pro tu i předány do použití vstupní revizí, sestavy 3 a 4 jsou certifikovány v bezpečnostní třídě 3, vstupní revizí však byly předány do použití pro bezpečnostní třídu 2. Lze tedy na všechny 4 sestavy z tohoto pohledu nahlížet shodně.

Výsledky jsou shrnuty v následující tabulce (jako poměr k požadované hodnotě):

Tab. 9 Počet kritických událostí v poměru k platné normě

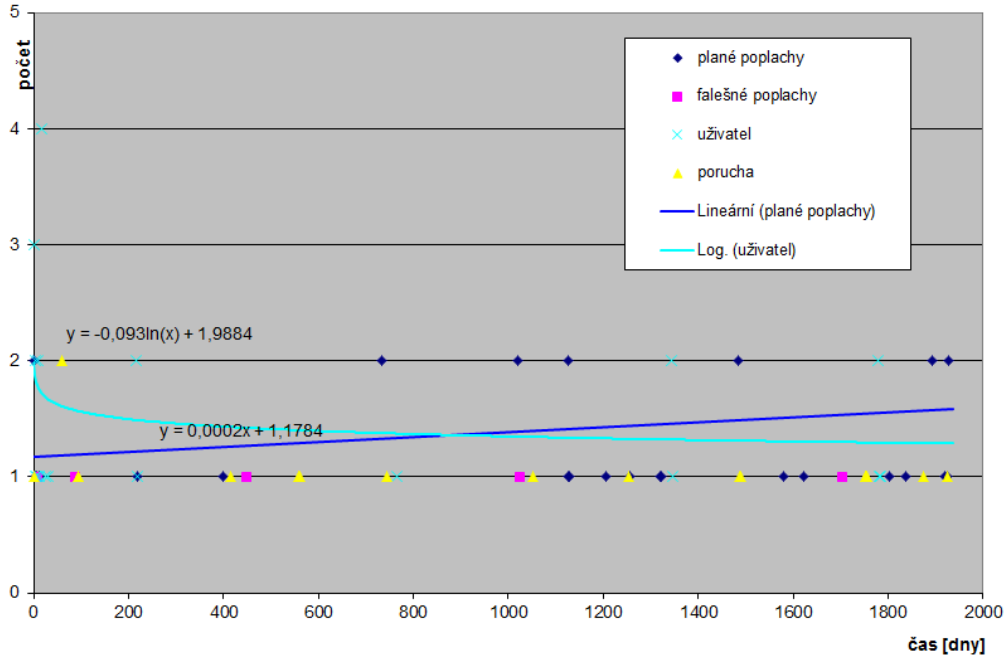
	Systém 1		Systém 2		Systém 3		Systém 4	
	před	po	před	po	před	po	před	po
Počet dnů provozu (od integrace)	557	1379	420	299	889	31	0	64
Poměr planých poplachů	0,09	0,15	0,4	0,33	0,23	0,68	0	0,22
Poměr falešných poplachů	2,6	0,52	2,6	3,4	0,83	12,5	0	0

Přepočty v této tabulce jsou zvoleny tak, aby poměr planých poplachů a poměr falešných poplachů vždy odpovídaly jedné, pokud je výše uvedená norma a doporučení splněno. Nižší hodnoty než 1 znamenají, že systém je odolnější vůči nekritickým poplachům, hodnoty nad 1 ukazují na větší citlivost k těmto poplachům.

Závěr z uvedené tabulky je zřejmý – všechny sestavy splňují požadavek limitu planých poplachů. Restrikce falešných poplachů je překračována (kromě sestavy 4) nezávisle na tom, zda je sledována dobu před integrací nebo po ní. **Toto je tedy první předpoklad toho, že uvedený způsob integrace neovlivňuje spolehlivost systému jako celku ani jednotlivých částí integrovaného systému.**

Grafické vyjádření tohoto názoru lze potvrdit v následujících grafech (zde graf pro sestavu 1, grafy ostatních sestav jsou uvedeny v příloze). Pokus vyjádřit konkrétní matematickou závislost četnosti uživatelských chyb při ovládání systému a definovat vztah pro vyjádření planých poplachů nebylo možné dokončit vzhledem k velice malému počtu případů na časové ose. Výsledek je tak poměrně neprůkazný, takže jej nemá cenu dále zpracovávat. Podstatné je však to, že četnosti se v okamžiku integrace prokazatelně nemění, což bude potřeba dále prokázat.

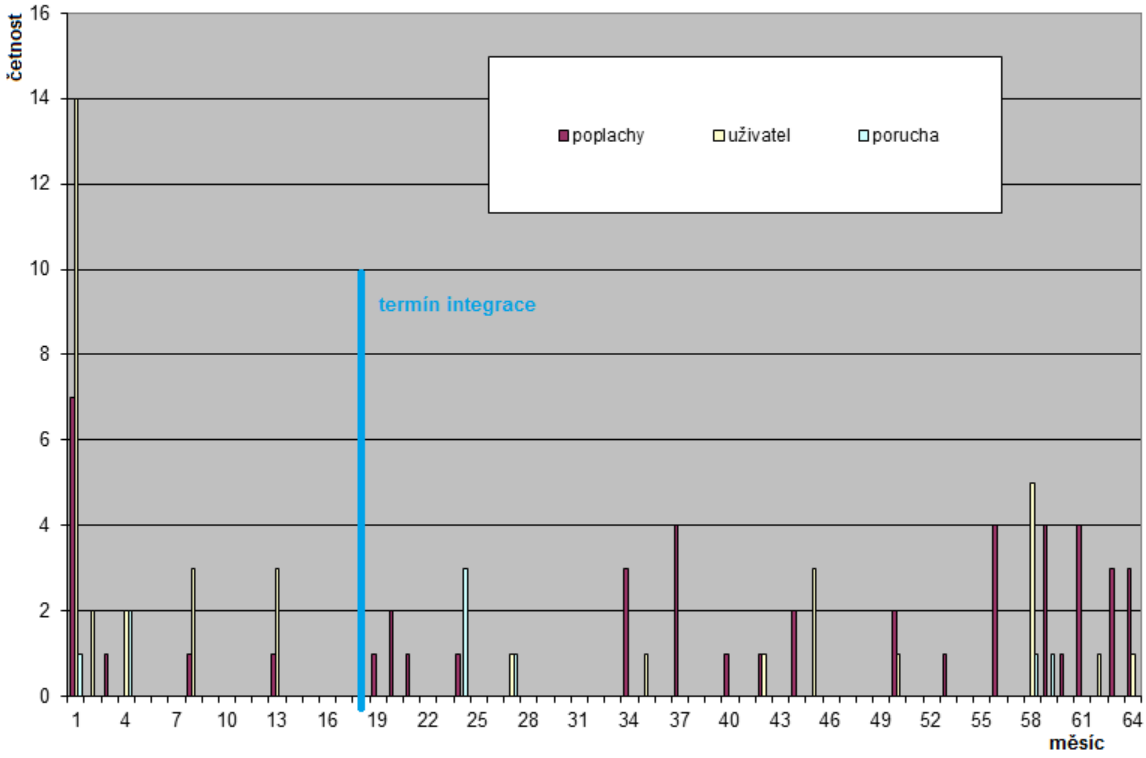
Obr. 45 *Graf četnosti jednotlivých typů poplachů (na ose x je vynášen graf ve dnech, na ose y je uveden počet poplachů)*



Zdroj: [113]

Pokud se provede rozdělení celé doby testování (zde sestava 1) po jednotlivých měsících a zpracují se ve sloupcovém grafu, je zřejmé, že sice lokálně dochází k nárůstu četnosti událostí, ale bez zjevného vztahu k realizované integraci (vyznačena modře).

Obr. 46 *Četnosti událostí zabezpečovacího systému*



Zdroj:[113]

Zajímavý je spíše poměrně výrazný nárůst souhrnného počtu planých a falešných poplachů od 56. měsíce dál. Není to sice náplní této práce, ale v zásadě by to potvrzovalo zatím spíše empiricky získanou zkušenost tradovanou v oblasti bezpečnostních systémů, že každých 5 – 6 let je potřeba provézt rozsáhlejší revizi a modernizaci systému, jinak prudce klesá celková spolehlivost a funkčnost těchto systémů.

5.1.3 Statistické zpracování, dílčí závěr

K definitivnímu určení zda jsou oba soubory dat statisticky shodné či nikoli postačí použít parametrický Studentův t-test, resp. jeho variantu dvojvýběrového t-testu. Tento test

je vhodný pro hodnocení experimentů, kde není známa střední hodnotu základního souboru, a porovnávají se pouze 2 soubory výběrových dat. Tato data mohou být představována buď dvěma měřeními provedenými opakovaně u jedné skupiny jedinců (typicky měření před aplikací pokusného zásahu a po aplikaci – tzv. „párový pokus“ neboli „závislé výběry“) nebo dvěma nezávislými skupinami měření („nepárový pokus“ neboli „nezávislé výběry“), což je tento případ.

V případě dvojvýběrového t-testu je testována nulová hypotézu:

$$H_0 : \mu_1 = \mu_2$$

Vzhledem k charakteristice měření a požadavku na testování byl použit tzv. „nepárový t-test“. Výpočet testu vychází z odhadů parametrů obou srovnávaných populací, tj. aritmetického průměru a výběrového rozptylu u pokusného a kontrolního výběru:

U výběrových souborů byl proveden výpočet výběrové charakteristiky:

1. výběrový soubor (počet členů n_1) : $\bar{x}_1$, S_1
2. výběrový soubor (počet členů n_2) : $\bar{x}_2$, S_2

Protože testované soubory mohou pocházet ze skupin, které mají stejný nebo naopak různý rozptyl hodnot sledované veličiny, je nejprve nutno otestovat rozdíl rozptylů obou souborů (nulovou hypotézu H_0: $\sigma_1^2 = \sigma_2^2$) pomocí F-testu.

F = větší z rozptylů (S_1^2, S_2^2) / menší z rozptylů (S_1^2, S_2^2)

kde výběrové rozptyly:

$$S_1^2 = \frac{\sum x_i^2 - \frac{(\sum x_i)^2}{n_1}}{n_1 - 1} \qquad (5) \qquad\qquad S_2^2 = \frac{\sum x_i^2 - \frac{(\sum x_i)^2}{n_2}}{n_2 - 1} \qquad (6)$$

Pro vyhledání tabulkové kritické hodnoty pro F-test je nutno stanovit stupně volnosti pro čitatele většího i menšího rozptylu.

Je-li $F \leq F_{0,975}$, tzn. že platí H0: $\sigma_1^2 = \sigma_2^2$ (oba výběry tedy pocházejí z populací se shodným rozptylem), pro testování rozdílu středních hodnot je použit nepárový t-test pro shodné rozptyly:

$$t = \frac{\left|\overline{x_1} - \overline{x_2}\right|}{\sqrt{\frac{(n_1 - 1) \times S_1^2 + (n_2 - 1) \times S_2^2}{n_2 + n_1 - 2} \times \frac{n_1 + n_2}{n_1 \times n_2}}} \qquad (7)$$

Je-li F > $F_{0,975}$, tzn. že neplatí platí H0: $\sigma_1^2 = \sigma_2^2$ (oba výběry tedy pocházejí z populací s různým rozptylem), pro testování rozdílu středních hodnot je nutné použít nepárový t-test pro různé rozptyly:

$$t = \frac{\left|\overline{x_1} - \overline{x_2}\right|}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^1}{n_2}}} \qquad (8)$$

Vypočtená statistika ***t*** se porovná s tabulkovou kritickou hodnotou nalezenou podle daného stupně volnosti a zvolené hladiny významnosti α (0,05 nebo 0,01).

Pro uvedené výpočty byla využita funkce v programu Excel (funkce F.TEST a T.TEST).

Tab. 10 Výsledek testování hypotéz

	Systém 1		Systém 2		Systém 3		Systém 4	
	před	po	před	po	před	po	před	po
průměr	0,0647	0,0398	0,1030	0,15	0,1406	0,1613	null	0,2812
směrodatná odchylka	0,3879	0,2538	0,7739	0,4195	0,6567	0,4469	null	1,1383
rozptyl	0,1504	0,0644	0,5989	0,1759	0,4312	0,1997	null	1,2957
F test významnost	5E-36 p <0.05		1,28E-30 p <0.05		0,0150 p <0.05		bez testu	
t test významnost	0,1635 p >0.05		0,3052 p >0.05		0,8096 p >0.05		bez testu	
Závěr	na dané hladině významnosti je potvrzena H_0		na dané hladině významnosti je potvrzena H_0		na dané hladině významnosti je potvrzena H_0		nelze otestovat	

Z provedených měření a statistického zpracování je zřejmé, že integrace způsobem realizovaným pomocí programových výstupů / vstupů poplachových systémů je bez vlivu na snížení spolehlivosti a jednotlivé systémy se statisticky významně neovlivňují. Četnost poplachů (planých i falešných), chyby obsluhy i kritické poruchy zařízení nemají

prokázány žádné rozdíly mezi situací před integrací a po ní. Lze do jisté míry vyvodit určité závislosti vztahující se k četnosti falešných poplachů v časové závislosti, stejně tak jako lze ze získaných dat odvodit funkce definující chybové jednání uživatelů. Vzhledem k tomu, že se toto však netýká tématu zpracovávané práce, nebyla tato okolnost dále rozpracovávána, bylo by však vhodné se k tomuto později vrátit v dalším navazujícím výzkumu.

Celkově lze předpokládat, že v případě přímé integrace několika poplachových (i dalších) systémů, které jsou tímto způsobem integrovatelné, se jedná o vhodné řešení z pohledu spolehlivostního, legislativního a především finančního. Vzhledem k určité obtížnosti procesu vlastní integrace (nelze použít žádné partikulární řešení) je nezbytná kvalitní příprava projektu, definice logických stavů a především výstupní revize postihující všechny reálné stavy integrovaného systému i jednotlivých částí. V žádném případě nelze toto řešení doporučit začínajícím integračním technikům či dokonce firmám zabývající se prostou instalací poplachových systémů. Pro odborníky se však jedná o optimální a spolehlivé řešení pro menší a střední integrace. Své místo nalezne především v rodinných domech, středně velkých kancelářských prostorách a především v menších technologických centrech (revize technologií).

5.2 Integrace pomocí průmyslových sběrnic

Tento způsob integrace byl již v úvodu práce na základě literární rešerše považován za jeden z nejperspektivnějších. Teoreticky totiž slučuje relativně snadnou instalaci spolu s vysokou spolehlivostí a relativně nízkou cenou.

5.2.1 Testování sběrnice KNX/EIB

Vzhledem k tomu, aby výsledky testů sběrnice KNX byly alespoň částečně srovnatelné s předchozím (a následným) testováním, bylo nutné výzkum a zhodnocení použití sběrnice KNX v bezpečnostních systémech směřovat poněkud jinak, než se běžně KNX sběrnice testuje. Po několika vlastních testech a rozsáhlých konzultacích bylo rozhodnuto o jedné z následujících variant testování[9]:

a) Testování prostřednictvím libovolného KNX rozhraní. V tomto případě možné použít jakékoli zařízení s vhodným software, které je schopno komunikace RS232 (komunikuje protokolem KNX PEI) či přes USB

(komunikace rovněž pomocí KNX PEI, na straně PC je USB dostupné jako generické HID zařízení) případně pro IP (využívá KonnexNet). Všechna tato rozhraní reprezentují KNX provoz způsobem, který je opět standardizován (jako cEMI zprávy).

b) Sledování signálu na fyzické úrovni. Tento způsob je logicky nejpřesnější a zatížen nejmenším množstvím chyb, je však rovněž poměrně obtížný na přístrojové vybavení a vlastní měření. Metoda vyžaduje osciloskop (v našem případě použit datalogger), pro rutinní čtení dat je nevhodná.

c) Pomocí zařízení s částečnou podporu hardware. V současnosti pro KNX existují tři druhy hotových hardware řešení, pomocí kterých lze externí programy připojit. OEM moduly s BCU jsou připraveny pro okamžité nasazení (BCU je kompletní KNX zařízení včetně KNX operačního systému), jejich použitím lze získat např. KNX rozhraní. Druhý OEM způsob připojení, BIM, je více modulární a dovoluje např. vystavět vlastní zařízení bez fyzické vrstvy (tu reprezentuje modul BIM). Lze však sestavit až řešení, které je ekvivalentní BCU. Třetí a nejelegantnější metodou je použití modulu ASIC TP-UART (Siemens), který po doplnění pasivních součástek realizuje fyzickou vrstvu a také kompletní vrstvu linkovou. Jeho vnější rozhraní je sériové. TP-UART je oblíbený ve všech experimentálních zařízeních, neboť již dovoluje koncentraci zájmu na logické (programové) části KNX bez nutnosti řešení technických vazeb. TP-UART se rovněž typicky používá v zařízeních, která mají mikroprocesor se sériovým portem.

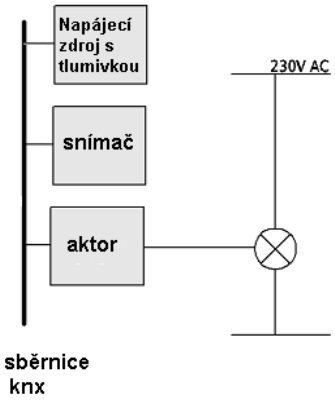
Při volbě a testování jednotlivých variant byla jako první vyloučena varianta a). Při jejím použití hraje nepřiměřeně velkou roli vlastní komunikační interface (RS232 či USB). Modul s IP komunikací nebyl bohužel v době testování k dispozici (relativní novinka). Vlastní testování pro formulování závěrů bylo tedy provedeno podle metodiky b) a c).

5.2.1.1 Testování KNX/EIB dle metodiky b)

Před vlastním testováním bylo nutné definovat kritické oblasti komunikačního protokolu. Veškerý přenos informace je založen čistě na principu decentralizace, nevyžaduje tedy žádnou řídící jednotku. Proto každý účastník na sběrnici je vybaven

vlastní mikroprocesorovou jednotkou. Snímače odpovídají za detekování změn a potřebných činností sledovaných parametrů a odesílají telegramy akčním členům, které vykonají příkazy obsažené v těchto telegramech. Je tedy zřejmé, že kritická z pohledu komunikace bude spolehlivost a rychlost přenosu konkrétního telegramu do cílového aktoru.

Obr. 47 *Elementární zapojení KNX dle vybrané metodiky*



Zdroj:[6]

Dalším kritickým místem se jeví napájení celého systému. Každá linie je opatřena napájecím zdrojem (nezapočítává se do počtu modulů na sběrnici – podobně jako další pomocné prvky – viz. Kap.2.1.3. a Kap.4.2.1). Napájecí zdroj není stabilizovaný, má pouze vestavěnou elektronickou ochranu proti přetížení a zkratům. Velikost filtračního kondenzátoru je taková, aby zvládla „udržet“ výstupní napětí v dostatečné toleranci i po dobu krátkodobých výpadků síťového napětí, ke kterým poměrně často dochází. Automatické vratné přepěťové ochrany fungují dle definice standartu (a dle výrobce) nejdéle do 200 ms (odpojení/připojení) při praktických testech však zvláště hodnota připojení byla zpravidla výrazně překročena. Pro bezpečný provoz je potřebné napájecí napětí alespoň 21 V DC, přičemž odběr jednoho aktivního přístroje smí dosahovat nejvýše 150 mW, v případě že je modul vybaven indikačními LED může být spotřeba až 200 mW. Zdroj je vybaven filtrační tlumivkou – viz. Obr.48 . Je zřejmé, že celý systém napájení a zálohování napájení je dalším kritickým místem celého systému KNX/EIB.

Obr. 48 *Napájecí zdroj KNX sběrnice firmy ABB*

Zdroj:[22]

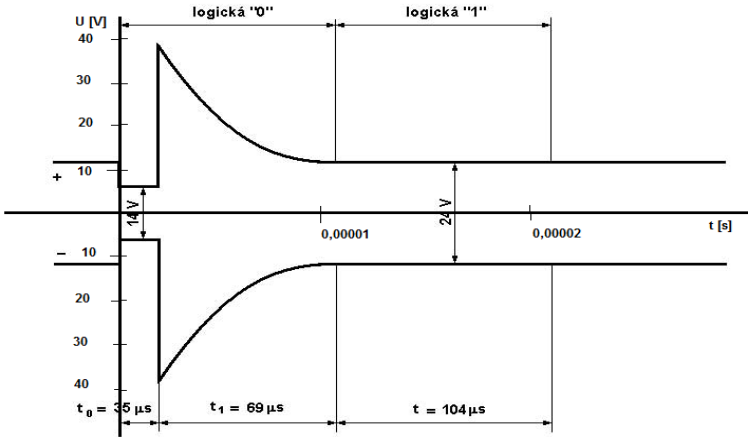
Přenášené telegramy jsou založeny na přenosu informace s přenosovou rychlostí 9600 bit.s^{-1}. Potřebná doba pro přenos jednoho bitu je dána vztahem, který je odvozen od přenosové rychlosti 9600 bit.s^{-1}.

$$t_{1bit} = \frac{1}{9600} = 104\mu s \qquad (9)$$

Typická doba přenosu telegramu je 20-40 ms v závislosti na počtu přenášených informací. Obecně lze tedy říct, že lze přenést až 40 telegramů za vteřinu, což je v rámci domácího prostředí zcela dostačující. Zpoždění v rámci sběrnice je i v případě kolize rovno maximálně stovkám milisekund. Zcela jiná situace ale nastává v případě zatížení sítě – prudký nárůst počtu telegramů způsobí větší prostoje při čekání na odbavení telegramu, častěji nedojde zpětné potvrzení, které se musí opakovat (maximálně 3x) a spolehlivost přenosu výrazně klesá. Navíc délky telegramů jsou různé, takže výše uvedené hodnoty jsou spíše orientační a platné v optimálním případě.

Průběh napětí a logických stavů na napájecích (datových) vodičích je zřejmý z Obr. 49.

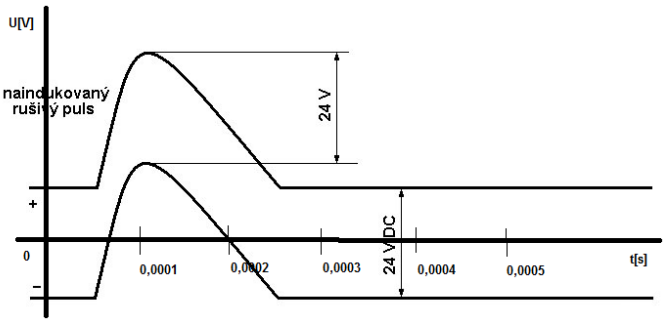
Obr. 49 *Průběh napětí a logických stavů na vodičích KNX*



Zdroj:vlastní, [34]

Je logické, že použití rozdílového transformátoru pro přenos datových signálů zvyšuje odolnost proti poruchám. Při příjmu signálu se na sekundárním vinutí transformátoru v přenosovém modulu sběrnicové spojky sečtou signály z obou primárních vinutí, takže na řídicí obvody sběrnicové spojky jsou přiváděny příslušné pulsy binárního telegramu. Vyskytne-li se na sběrnici poruchový signál (např. elektromagnetickou indukcí), na obou vodičích sběrnice bude jeho průběh např. podle Obr. 50. Pulsy na obou vodičích se v rozdílovém transformátoru odečtou – v ideálním případě bude výsledkem nulový puls. Rozdílový transformátor na vstupech sběrnicových spojek tedy výrazně zvyšuje odolnost systému proti poruchovým signálům.

Obr. 50 *Odolnost KNX proti elektromagnetické indukci*

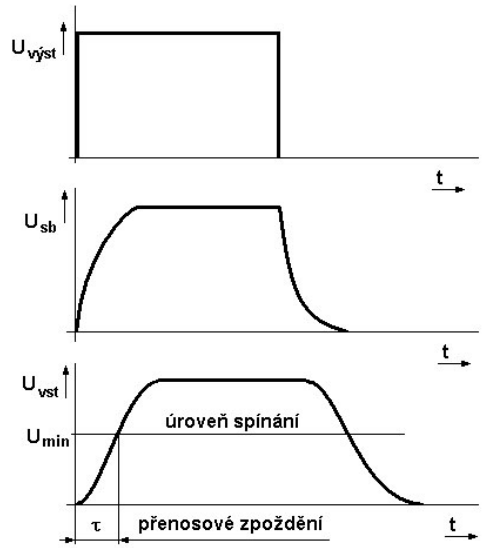


Zdroj:vlastní, [34]

Původně pravoúhlé impulsy jsou deformovány vlivem parazitních kapacit vedení sběrnice a indukčnosti transformátorů ve vstupních částech sběrnicových spojek (a tlumivky v napájecím obvodu) a dochází i k určitému přenosovému zpoždění. Ve sběrnicových spojkách jsou impulsy generovány jako pulsy o špičkovém napětí 5V a jako takové převedeny na stejnosměrné sběrnicové napětí o jmenovité velikosti 24 V.

Účastník, který vysílá telegram, generuje tedy pravoúhlé pulsy (viz. Obr. 51) označené jako $\mathbf{U_{výst.}}$ Během přenosu se vlivem parazitních impedancí vedení postupně deformují – viz průběh $\mathbf{U_{sb}}$. Na vstupu sběrnicové spojky, která přijímá telegram, může být průběh pulsů např**.** $\mathbf{U_{vst}}$. Řídicí obvody sběrnicové spojky však zaznamenají puls teprve při dosažení určité úrovně napětí, dané minimálním spínacím napětím $\mathbf{U_{min}}$. S ohledem na deformaci signálu během přenosu ale nastane časový posun mezi náběžnou hranou výstupního napětí a okamžikem dosažení úrovně spínání vstupního napětí. Takto vzniká přenosové zpoždění $\boldsymbol{\tau}$.

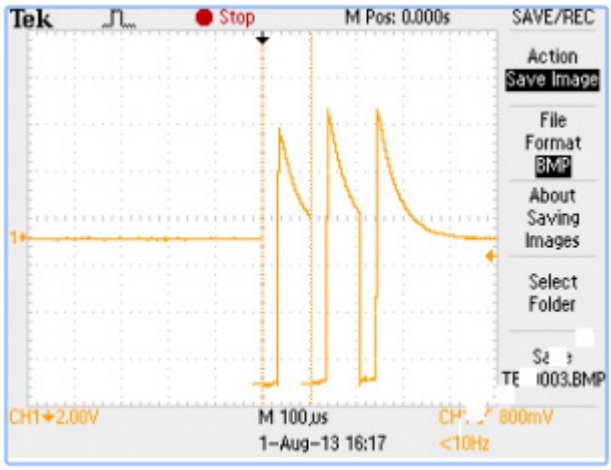
Obr. 51 *Průběh ideálního a reálného pulsu na sběrnici v okamžiku spínání*



Zdroj:vlastní, [34]

Měření potvrdilo výše uvedené předpoklady s tím, že se nepravidelně opakovala určitá „nejednoznačnost“ některých účastníků na sběrnici a to dokonce i přímo v jedné linii[56]. Podrobněji je tato situace diskutována v závěru kap. 5.2.

Obr. 52 *Průběh signálu na sběrnici*



Zdroj: [vlastní]

Časový průběh komunikace při odesílání spínacího telegramu definuje následující tabulka:

Tab. 11 KNX – časový průběh komunikace

Činnost	Trvání v dobách bitu	Trvání v µs
Čekání na volnou sběrnici	50	5 200
Vysílání telegramu	117	12 168
Pauza	13	1 352
Potvrzení	13	1 352
Celková doba	193	20 072

5.2.1.2 Testování KNX/EIB dle metodiky c)

V tomto případě, kdy je přistupováno k přenosu nikoli na fyzické, ale na aplikační vrstvě, je ověření funkčnosti uvedené sběrnice výrazně jednodušší než v předchozím testu. Jak je popsáno v Kap. 4.3.1, nabízí se poměrně výkonný nástroj pro testování komunikace na KNX/EIB sběrnici přímo v nástroji pro její návrh a programování. Nejčastěji se používá aplikace ETS3 či velice moderně pojatý nástroj Loxone. V současnosti je na trhu již verze ETS4, která je již čtvrtou verzí prostředí. Kompatibilita uložených projektů je zajištěna od verze ETS2.

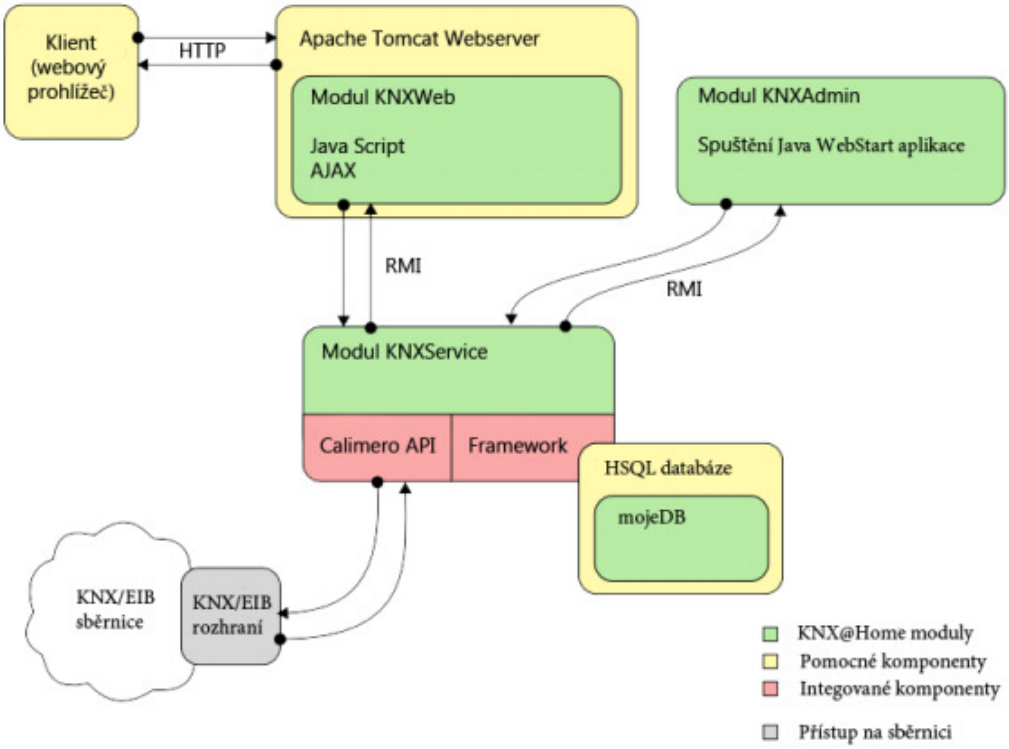
Vývojové verze jsou k dispozici pro začátečníky i velmi zkušené KNX instalační partnery:

ETS4 Demo:	bezplatná testovací verze pro velmi malé projekty
ETS4 Lite:	určeno pro malé až střední projekty
ETS4: Professional:	projekty všech rozsahů, plná funkčnost

ETS Professional je silný nástroj pro integraci automatizace. Umožňuje plánování a design projektu, uvedení systému do provozu, projektovou dokumentaci, diagnostiku a řešení vzniklých poruch a chyb. Pro vyzkoušení je možné si stáhnout ETS4 Demo zdarma z oficiálních stránek KNX asociace www.kng.org.

Velice zajímavým projektem je KNX@Home, jak se v původním názvu označuje projekt vyvinutý na německé University of Applied Sciences in Deggendorf. Jedná se o volně šiřitelný řídící server pro domácí automatizaci, založený na KNX sběrnici. Jelikož domácí systémové instalace jsou pro investory již při nákupu komponentů citelně dražší než klasické elektroinstalace, je možné díky bezplatnému KNX@Home využít přístup ke sběrnici KNX/EIB prostřednictvím IP přístupu, a to bez dalších nákladných řídících a vizualizačních aplikací. KNX@Home tedy dokáže poměrně jednoduše ovládat KNX/EIB systémovou sběrnici prostřednictvím kteréhokoliv zařízení, které je schopno přistupovat k IP sítím[9].

Obr. 53 *Schéma činnosti KNX@HOME*

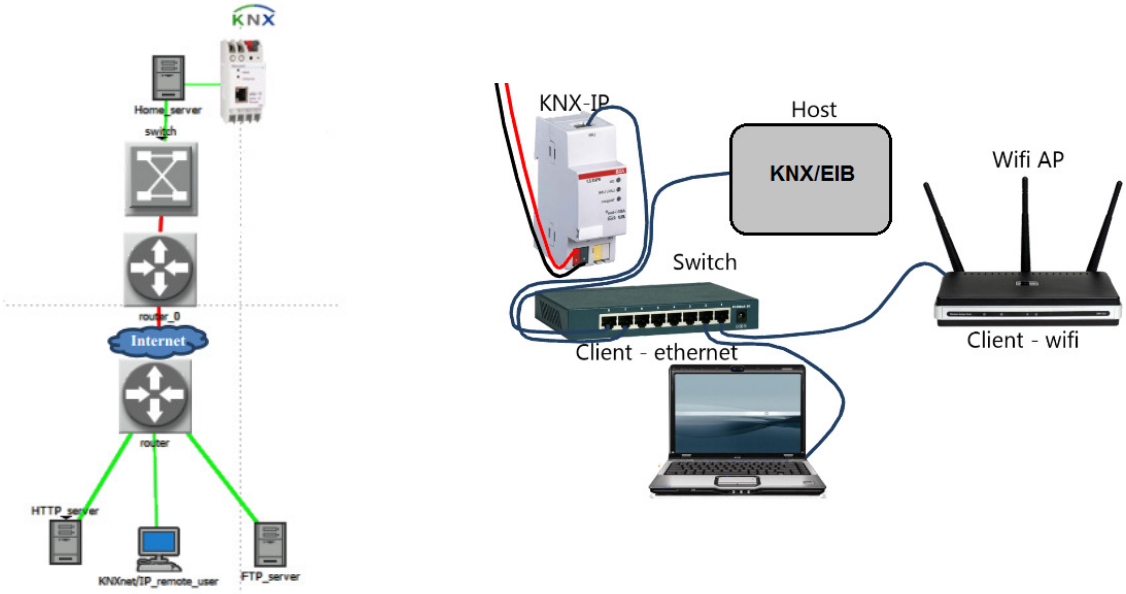


Zdroj: [4]

Toto velice zajímavé a levné řešení, by bylo vhodné dále otestovat s ohledem na bezpečnou integraci bezpečnostních systémů (již na první pohled obsahuje několik zásadních rizik), vzhledem k zaměření této práce však tato varianta KNX/EIB dále nebyla testována.

Topologie testovaného zařízení byla zvolena následující dle metodiky popsané v Kap. 4.3.1. Podrobněji demonstruje následující schéma (Obr. 54).

Obr. 54 *Objektový a fyzický model testovací soupravy*

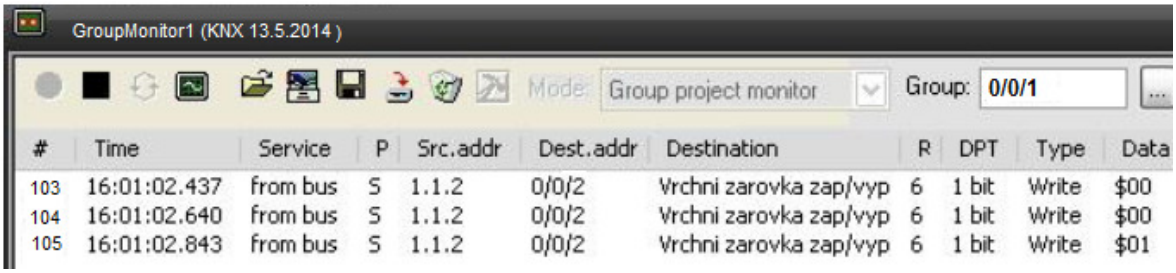


Zdroj: vlastní, upraveno dle [4][6][20]

Klientská stanice je pomocí sběrnice Ethernet připojena ke KXP/IP rozhraní ISP/S 2.1, které je dále prostřednictvím tzv. ethernetového switche připojeno k místní IP síti 10.10.0.1/24 . KNX/IP rozhraní se stará o konverzi KNX telegramů do IP sítě. KNX API a dokáže komunikovat přímo s KNX/IP rozhraním na základě požadavků předaných webserverem. Webserver je dílčí část KNX a tvoří vizualizační prostředí pro intuitivní ovládání instalace z klientských stanic, které lze libovolně připojovat do lokální sítě. Pro ověření správné komunikace a překladu telegramů do KNX sběrnice bylo využito group monitoru, jenž je součástí aplikace ETS. Komunikace byla zachytávána pomocí USB rozhraní a modulu USB/S 1.1. Schéma celé sestavy je na Obr. 54

Zachycení vysílání v programu GroupMonitor je zobrazeno na obrázku Obr. 55.

Obr. 55 *Ukázka činnosti programu GroupMonitor*

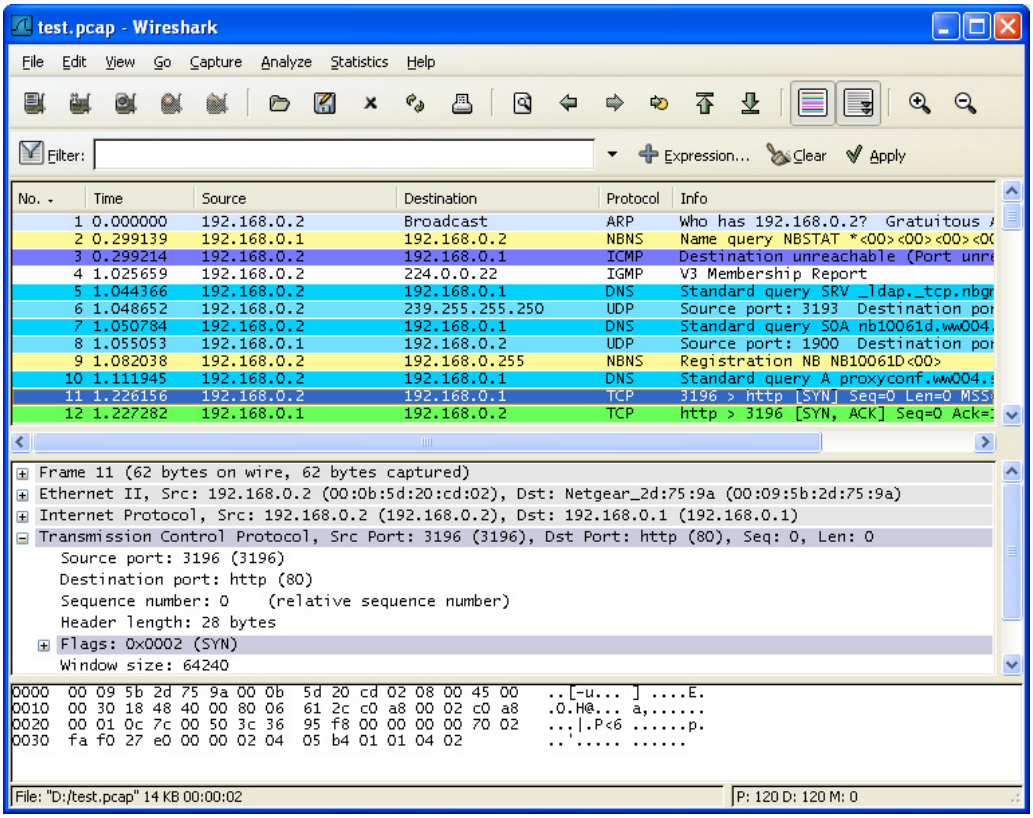


#	Time	Service	P	Src.addr	Dest.addr	Destination	R	DPT	Type	Data
103	16:01:02.437	from bus	S	1.1.2	0/0/2	Vrchni zarovka zap/vyp	6	1 bit	Write	$00
104	16:01:02.640	from bus	S	1.1.2	0/0/2	Vrchni zarovka zap/vyp	6	1 bit	Write	$00
105	16:01:02.843	from bus	S	1.1.2	0/0/2	Vrchni zarovka zap/vyp	6	1 bit	Write	$01

Zdroj:[46]

IP komunikace pak byla zachycována prostřednictvím programu Wireshark.

Obr. 56 *Ukázka činnosti programu Wireshark*



Zdroj: [112]

Tím bylo možné provádět kompletní čtení realizované komunikace a díky nástroji ETS4 a jeho rozšiřujících knihoven ověřit funkci komunikace a verifikovat ji při specifických bezpečnostních podmínkách.

5.2.1.3 Zpracování výsledků a dílčí závěr

Vzhledem k tomu, že testování bylo prováděno na zapůjčeném zařízení a tudíž některé z potenciálně rizikových testů nemohly být provedeny (riziko poškození modulů), nelze se vyjádřit zcela jednoznačně, jak by sběrnice odolávala běžným testům požadovaných na sběrnici bezpečnostních systémů. V praxi se však podařilo potvrdit následující předpoklady:

a) Komunikační sběrnice využívá metodu CSMA/CA (Carrier Sense Multiple Acces with Collision Avoidace) jako nástroj proti omezení množství kolizí na

společné sběrnici. Dojde-li k vysílání dvou účastníků ve stejný čas, dostane přednost ten telegram, u kterého jeho bitová posloupnost bude mít dříve načtenou log 0. Tento postup se využívá v komunikační technice poměrně často, má však jeden velký problém. Popsané řízení funguje pouze na úrovni liniové vrstvy. V případě, že KNX sběrnice je rozdělena na více linií (častý případ u větších instalací), tato metoda selhává a dojde ke ztrátě telegramu bez identifikace této ztráty. Pokud se účastník pokusí odeslat telegram více jak třikrát a nepodaří se mu to (vlivem zatížení komunikace či vlivem nastavené priority komunikace) může se stát (a při praktických testech se tak stalo), že účastník „odpadne“ na definovanou dobu z komunikace. Tento výpadek může trvat až několik sekund a v několika případech bylo nutné ruční restartování.

b) Systém je velice odolný vůči rušení a to jak indukcí z okolí, tak i chybami při přenosu (testováno na PLC adaptérech).

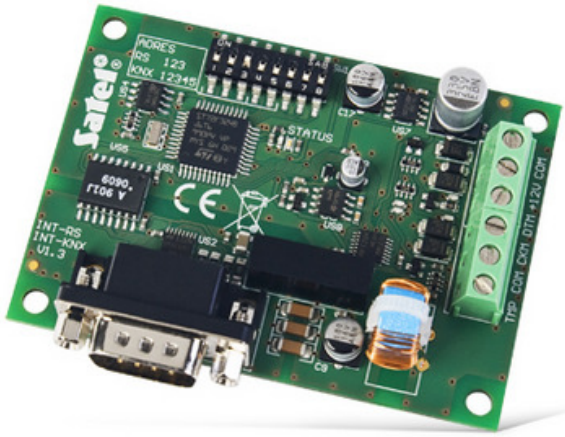
c) Velice problematická je oblast napájení sběrnice, která je přitom pro korektní provoz a přenos informace klíčová. V podobě tak jak je definována normou není možné akceptovat její realizaci do oblasti bezpečnostních systémů a to ani jako vizualizační nástroj[115].

Klíčovým problémem se tedy jeví především problematika kolize paketů a kompatibilita modulů jednotlivých výrobců s ohledem na modernizaci (stáří) produktů.

Celkově lze prozatím říci, že sběrnice KNX/EIB je nepochybně vhodným nástrojem pro integraci systémů typu osvětlení, stínící techniky, případně topení, ale pro použití v bezpečnostní oblasti k jeho principu lze mít významné výhrady (viz. výše). Je ale pravdou, že masivní zavádění tohoto standardu (a především síla velkých výrobců, kteří se výrobě komponent KNX/EIB věnují) může způsobit postupné prosazování i v oblasti bezpečnostní integrace. Příkladem může být modul INT-KNX společnosti Satel[22] (polský výrobce zabezpečovací techniky). Modul INT-KNX integruje zabezpečovací systém INTEGRA s KNX systémem, takže ústředna může ovládat aktory připojené ke sběrnici KNX a zařízení na sběrnici mohou ovládat zabezpečovací systém. Je zřejmé, že tento krok jde zcela jednoznačně proti snaze ČSN EN 50131 a norem souvisejících. Uplatnění

modulu je tedy možné pouze v případě, kdy není potřeba dodržet žádné třídy bezpečnosti ani vůči klientovi, ani vůči pojišťovně, tím spíše vůči legislativním předpisům.

Obr. 57 *Modul KNX do zabezpečovací ústředny Satel*



Zdroj:[22]

5.2.2 Testování sběrnice CIB

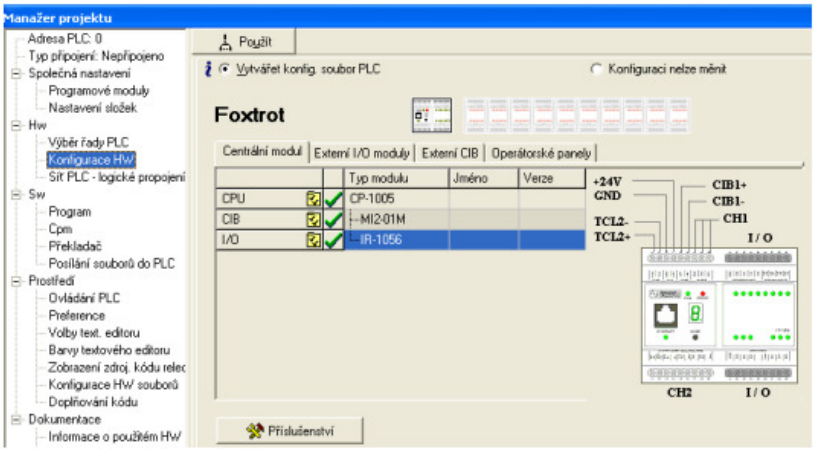
Jak bylo popsáno v kapitole 4.3.2. je sběrnice CIB sice stejně jako sběrnice KNX/EIB dvojvodičová, jedná se však o principiálně zcela jiný typ sběrnice. CIB není decentralizovanou sběrnicí podobně jako KNX, ale je řízena PLC modulem, který ovládá vlastním protokolem jednotlivé moduly připojené a napájené sběrnicí. Provoz na sběrnici řídí základní modul Foxtrot. Master se dotazuje na nové hodnoty cyklicky.

Základní modul Foxtrot „ví“ o každé události, o každé hodnotě a její změně. Má v sobě vestavěny prostředky pro jejich zobrazení přes vlastní WEB server nebo přes externí SCADA systém, data může archivovat, může poslat e-mail a SMS, může zapisovat do externích databází atd. Programátor může v Mosaicu sám napsat jakýkoliv algoritmus mezi libovolnými sensory (vstupy) a aktory(výstupy)[81]. Při potřebě změny funkce se mění pouze program v základním modulu. Všechny periferie a moduly na sběrnici zůstávají. Toto je zřejmě nejpodstatnější rozdíl CIB vůči KNX/EIB.

Zapojení dle schématu na obr. 28 bylo realizováno jednak na zařízení výrobce (spol. TECO a.s.), jednak na vlastním zařízení. Výsledky spolehlivostního testu byly v obou případech zcela srovnatelné.

Po fyzickém zapojení (které nebylo zcela bezproblémové), bylo nutné provést vlastní programování systému. Zde je opět vidět zřejmý rozdíl oproti KNX, jedná se již o skutečně programování, nikoli propojování můstků.

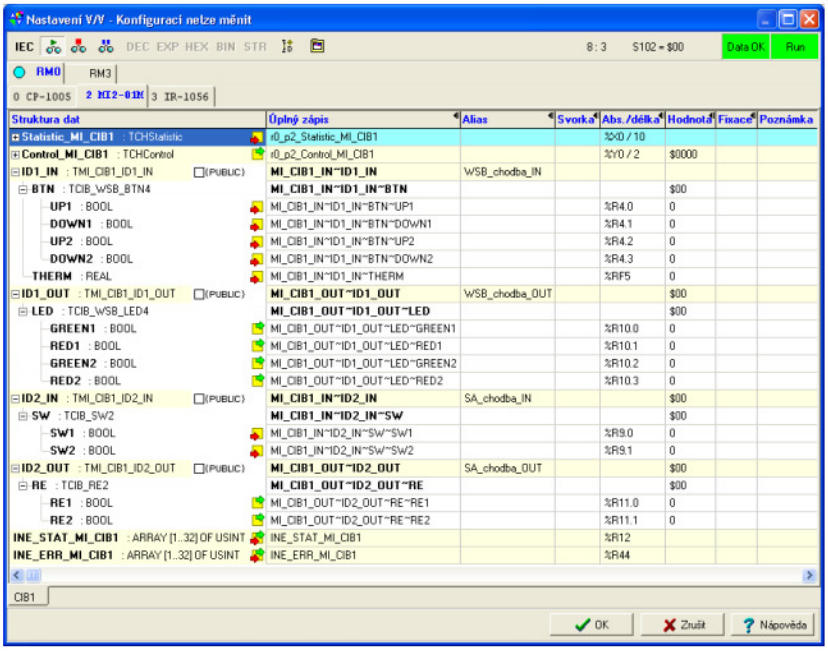
Obr. 58 *Aktivace obsluhy interního master modulu CIB*



Zdroj: vlastní dle [42][44]

Struktura přenášených dat je poměrně snadno dosažitelná přímo z konfiguračního a programovacího prostředí Mosaic. CIB master si v zápisníku CPU rezervuje datovou oblast, ve které jsou dostupná předávaná data z/do CIB jednotek, stavová a chybová zóna CIB jednotek. Struktura datové oblasti je patrná z panelu Nastavení V/V[116] .

Obr. 59 *Ukázka prostředí Mosaic*



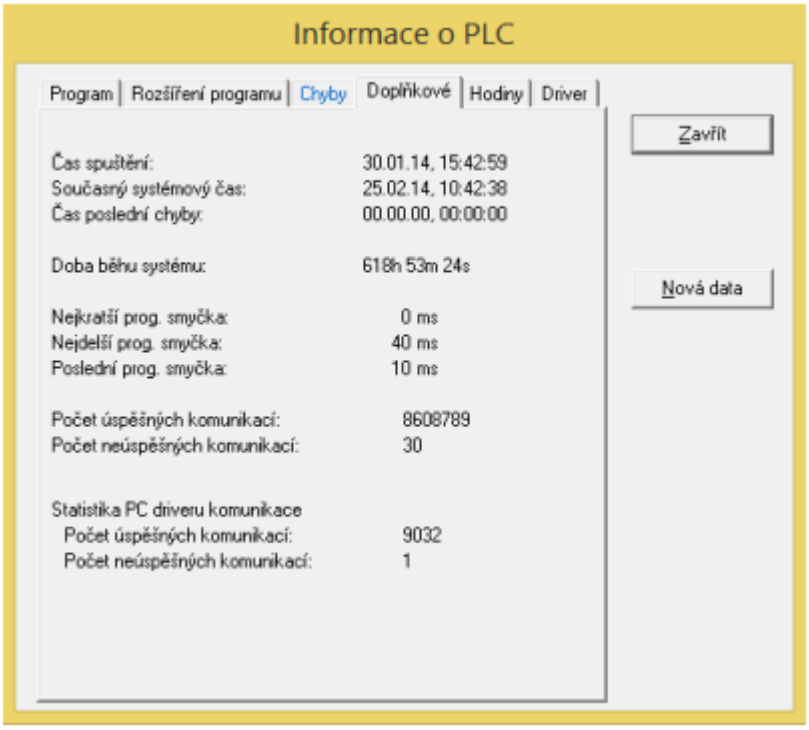
Zdroj: [115]

Na rozdíl od standartu KNX je komunikační systém odolný vůči výpadkům a poruchám napájení (i když jisté námitky lze vznést). Ačkoliv sběrnice má nominální napájecí napětí 24 V DC, doporučuje se použít napětí 27 V DC. Díky tomu je možné trvalé dobíjení připojených akumulátorů 2×12 V, které potom při výpadku sítě zajistí trvalý chod centrální jednotky včetně všech jednotek na sběrnici CIB. Samozřejmě nebudou fungovat spotřebiče napájené ze sítě 230 V, ale systém je i nadále schopen vykonávat zabezpečovací a komunikační funkce. Odezva systému je do 150ms i při plném zatížení, tj. osazení maximálního počtu jednotek na všech připojených větvích sběrnice CIB. Tato hodnota je hluboko pod 300 ms, tedy pod hodnotou, kterou člověk ještě vnímá jako okamžitou reakci. Pro regulaci tepelných procesů je to rychlost zbytečná, ale umožňuje systém bez problému využít i v osvětlovacích soustavách. Garantované rychlosti odezvy sběrnice je dosaženo přenosovou rychlostí 19,2 kb/s a optimalizovaným přenosovým protokolem (který se nepodařilo dekódovat) [96].

Vlastní měření testovacího systému spočívalo především v ověření dlouhodobé funkceschopnosti zapojeného systému. V systému se simulovala nahodilá změna hodnoty na vstupu senzoru (C-IT-0202C) s tím, že manuálně bylo nahodile aktivováno tlačítko (C-WS-0200R). Na displeji byl vždy zobrazován aktuální stav. Testování probíhalo v několika cyklech, v první etapě po dobu 618 hodin, následně 912 hodin a nakonec 105 hodin. Druhý systém byl testován po dobu 120 hodin. Úhrnná doba testu byla tedy (na obou systémech dohromady) 1755 hodin, což odpovídá cca 73 dnům trvalého provozu.

Vyhodnocení provozu je díky logice nástroje Mosaic poměrně jednoduché – PLC automat ukládá veškeré události do dataloggeru a uložená data lze vypsat přímo v prostředí Mosaic na informačním panelu – viz. Obr. 60.

Obr. 60 *Informace o stavu sběrnice v programu Mosaic*



Zdroj:[112][45][29]

Výsledky z jednotlivých cyklů měření:

Tab.12 CIB – chybovost komunikace

	I.	II.	III.	IV.
Čas spuštění	30. 1. 2014	8. 4. 2014	19. 5. 2014	14. 7. 2014
Konec spuštění	25. 2. 2014	15. 5. 2014	22. 5. 2014	18. 7. 2014
Počet chyb	0	2	0	0
Doba běhu	618h 53m 24 s	911h 42m 8s	105h 2m 51 s	120h 17m 0 s
Short loop	0 ms	0 ms	0 ms	0 ms
Long loop	40 ms	40 ms	35 ms	20 ms
Úspěšná komunikace	8 608 789	12 690 322	1 602 658	1 671 609
Neúspěšná komunikace	30	112	6	0

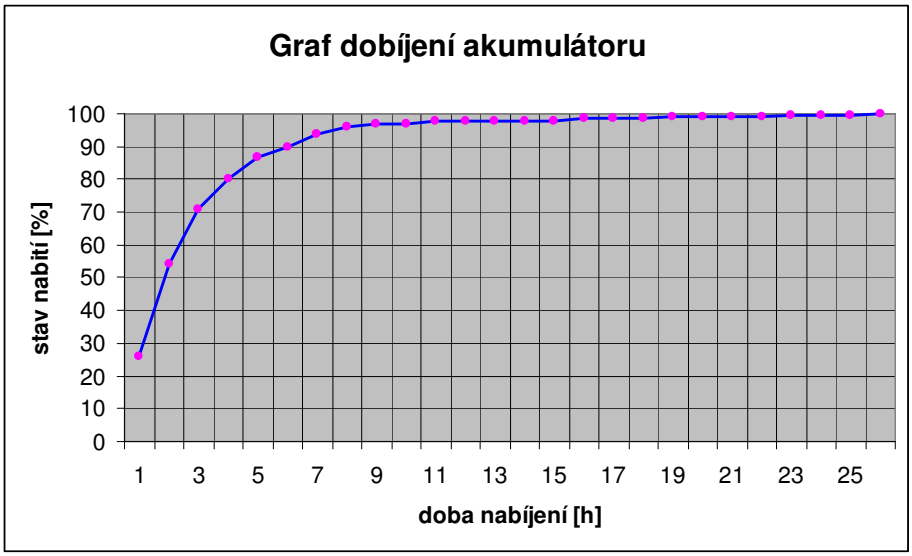
Během testování nedošlo ani v jednom případě k zastavení běhu PLC či restartování systému. Ve dvou případech bylo nutné mechanicky upravit připojení komponent, což byla spíše chyba přípravy testu než vlastní testované sběrnice. V konečném testování druhého cyklu však tato chyba zjevně způsobila výrazný nárůst celkové neúspěšné komunikace na sběrnici. Lze tedy usuzovat, že sběrnice je poměrně „citlivá“ na kvalitu provedeného zapojení.

PLC snímal nepřetržitě stav sběrnice CIB a případnou chybu zapsal do „error statusu“ a dataloggeru. V průběhu testování systém PLC upozorňoval na interní chybu E_07, která znamenala chybu při kontrole remanentní zóny se špatným kontrolním součtem. Její příčinou byla porucha v zálohování uživatelské paměti RAM na centrální jednotce. Podle nápovědy v rejstříku Mosaic se jednalo o závadu na zálohovací baterii. Pro chod ústředny a jejich komponent neměla tato chyba žádný vliv. Sběrnice CIB pracovala bezproblémově. Je však zajímavé, že se tato chyba opakovala na všech zapojení daných komponent, tedy při měření I, II i III a to i po výměně akumulátorů. Systém IV. žádné závady nedetekoval.

Napájení integrovaného systému je v této práci realizováno zdrojem PS2-60/27, který dodává 27,2 V pro zařízení na sběrnici CIB a 12 V pro případné detektory PZTS. Nabíjení baterií je realizováno pouze ustálenou hladinou napětí na 27,2 V. Zdroj neumožňuje kontrolovatelné nabíjení, tím je nemožné provádět dobíjení tak, aby bylo možné zvýšit jejich životnost. Baterie jsou připojeny přímo na výstup zdroje, tudíž nelze kontrolovat stav akumulátorů a může docházet k zahřívání při dobíjení. Jestliže pak tedy není možné zjistit stav nabití ani rozpoznat schopnost baterií napájet systém po výpadku síťového napájení, jedná se nejenom o nesoulad s normou ČSN EN 50131-6 ed.2, ale může dojít k vážnému poškození baterie či ohrožení okolí. V každém případě ale ani v jednom případě nebyl zjištěn problém se zahříváním akumulátorů použitých v systémech. Použitý zdroj poskytoval maximálně 2,3 A, z toho 0,2 A odebírala ústředna. Z ověřovacího měření bylo zjištěno, že maximální nabíjecí proud byl 2,1 A. Na 80 % kapacity se nabíjely za cca 3 hodiny a 40 minut. Křivka je zobrazena na Obr. 36. Po úplném nabití zdroj baterie udržoval na napětí 27,1 V a proudu 1,1 mA. Baterie nejsou chráněny proti hlubokému vybití. Jediná indikace nízkého napětí v systému, která nastala, bylo rozblikání stavových diod na rozšiřujícím modulu CF-1141. Na funkci systému to však nemělo vliv.

Akumulátory byly vybíjeny do 11 V, při nižším napětí by hrozilo nevratné poškození baterií.

Obr. 61 *Testování dobíjení akumulátoru v systému CIB*



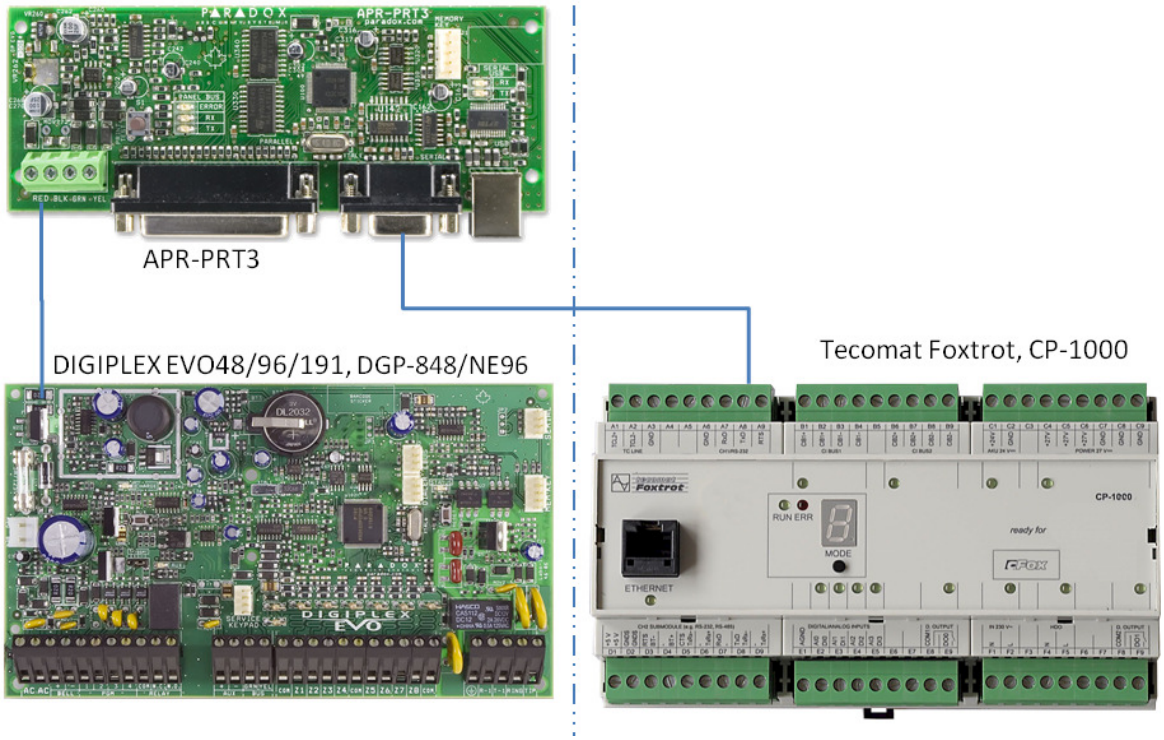
Zdroj: [111]

5.2.2.1 Zpracování výsledků a dílčí závěr

Sběrnice CIB je svým pojetím nepochybně velice zajímavým řešením, které se v současné době poměrně výrazně prosazuje na trhu inteligentních sběrnic. Svojí koncepcí stojí mezi inteligentní distribuovanou sběrnicí a klasickým PLC řídícím automatem. Při realizovaných testech byla velice pozitivně hodnocena z pohledu stability přenosu a odolnosti vůči rušení. Rovněž tak nemá logicky podobné problémy jako KNX/EIB s kompatibilitou jednotlivých modulů (v podstatě dva producenti). Zásadní problém je především ve velice diskutabilním způsobu napájení sběrnice, resp. jeho zálohováním, což se ale zdá, že je obecným problémem sběrnic pro IB. Navíc v tomto případě je poněkud problémem použité napájení 27 V, jehož použití znamená, že v případě nasazení na bezpečnostní systémy jej činí poněkud nešikovným a vyžaduje použití dalších modulů. Pro rozsáhlejší instalace je pak určitým problémem celkový max. odběr. V zásadě však je toto řešení pro využití v integraci bezpečnostních systémů až překvapivě vhodné především díky velmi vysoké spolehlivosti přenosu a velké odolnosti vůči rušení. Je však nutné dořešit některé systémové nedostatky (log. událostí, uzamčení jednotlivých částí programových modulů, doplnění kontroly a detekce dobíjení záložních akumulátorů) [29].

Podobně, jako v případě sběrnice KNX/EIB, jsou od výrobce k dispozici moduly, umožňující přímé připojení konkrétních zabezpečovacích ústředen (Jablotron, Paradox, Satel a další), které umožní stavy ústředny přenášet přímo po sběrnici CIB. Problémem opět je to, že v případě využití daného modulu, ztrácí zabezpečovací systém bezpečnostní certifikaci a lze jej tedy použít pouze tam, kde není požadován bezpečnostní systém konkrétní bezpečnostní třídy.

Obr. 62 *Princip integrace systému TECO se systémem PZTS*



Zdroj: [42]

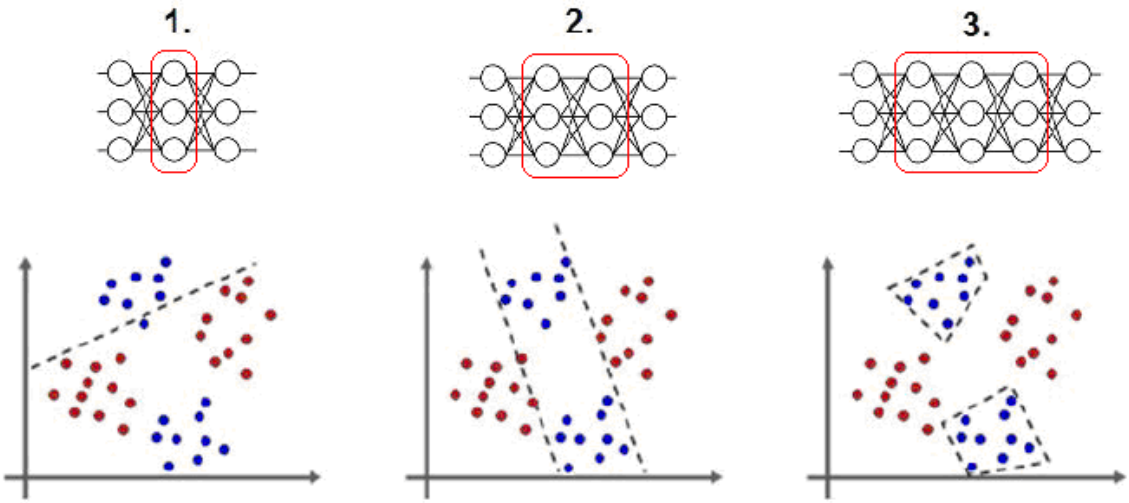
5.3 Integrace prostřednictvím „neuronového klíče“

Možnost využít neuronovou síť jako nástroj pro inteligentní a především univerzální integraci přímým propojením sběrnicí jednotlivých, jinak autonomních systémů s tím, že bude možné pouze definovat stavy (události), které se budou přenášet do integrovaných systémů je velice lákavá a dle literární rešerše nebyla tato možnost nikdy dříve testována ani v literatuře zmíněna. Náročnost na zpracování a testování se však ukazuje jako poměrně značná (v porovnání s dalšími možnostmi popsanými v této práci).

Způsob získání dat a jejich příprava pro vlastní modelování byl popsán již v Kap. 4.4., stejně tak jako diskuse nad vhodným typem neuronové sítě. Tato kapitola práce tedy rozpracovává především popis vytvoření neuronového modelu a způsob jeho testování včetně diskuse výsledků.

V první etapě bylo nezbytné rozhodnout, jaký typ modelu použít, respektive kolik vrstev sítě zvolit. V tomto případě je možné použít matematické odvození, ale vzhledem k typu použití konkrétního modelu, počtu vstupů a výstupů bylo rozhodnuto základní ověření funkčnosti metody provést maximálně na třívrstvé neuronové síti s tím, že je předpoklad, že postačující bude síť jednovrstvá či spíše dvouvrstvá[27]. Vhodnost použití modelu s daným počtem vrstev demonstruje následující schéma.

Obr. 63 *Vliv počtu vrstev neuronové sítě na schopnost klasifikace*



Zdroj:upraveno dle [31]

1. model neuronové sítě s jednou skrytou vrstvou
2. model neuronové sítě s dvěma skrytými vrstvami
3. model neuronové sítě s třemi skrytými vrstvami

Pro první testování byl zvolen model vícevrstvého perceptronu se dvěma skrytými vrstvami a zpětným šířením chyby. Tento typ neuronové sítě je vhodný ke klasifikaci, popř. kategorizaci tříd a stavů, které jsou presentovány výstupními hodnotami, např.:

- zapnout, vypnout (ON/OFF),

• model, typ,

• zdravý, nemocný a další[30].

V tomto modelu jsou očekávány dvě hlavní třídy, ve kterých jsou presentovány stavy:

• objekt narušen – not klid,

• objekt nenarušen - klid.

Jak bylo řečeno v kapitole 4.4, testování probíhalo souběžně (pro urychlení modelování a ověření výsledků) na dvou různých prostředích – v nástroji NeuroSolutions - verze 6.31 a v programu Matlab 6.5 s využitím nástroje „NNTOOL“, který byl vyvinut přímo pro práci s neuronovými sítěmi.

V rámci programu Matlab je práce s neuronovými sítěmi velice jednoduchá. Tato jednoduchost je ale vykoupena poměrně velkou časovou náročností jednotlivých výpočtů. Proto předpokládaná vstupní matice o rozměrech 31×22 564 musela být pro časovou náročnost výrazně redukována. Následně bylo testy potvrzeno, že pro ověření funkce je plné vkládání všech stavů rozhodně zbytečné.

Při vytváření sítě lze pro každou vrstvu definovat vlastní přenosovou funkci. V tomto případě byla zvolena logická sigmoida, a to z toho důvodu, že je třeba pracovat s logickými hodnotami. Dalším parametrem pro vytvoření sítě je počet neuronů v jednotlivých vrstvách. Jednotlivé počty byly navrženy v rámci optimalizace, aby síť nebyla zbytečně rozsáhlá, ale aby byla schopna naučit se všech 22 564 stavů s maximální požadovanou chybou 1%. Vstupní vrstva tak obsahuje 31 neuronů. Tento počet vychází z počtu prvků řádku matice pro jednotlivý reprezentovaný stav. Skryté vrstvy jsou celkem tři a každá obsahuje 180 neuronů. Výstupní vrstva poté obsahuje 15 neuronů. Tento počet je určen množstvím stavů, aby bylo možné všechny reprezentovat binární hodnotou (2^{15}=32 768).

Pro trénování sítě byl vybrán algoritmus Back-propagation[30]. Použití tohoto algoritmu je poměrně široké a prostředí Matlab nabízí několik variant jeho provedení. Varianty se liší v rychlosti, složitostí a stabilitou. Nabízenými typy jsou:

- traingd – Batch Gradient Descent
- traingdm – Batch Gradient Descent with Momentum
- traingdx – Gradient Descent with Variable Learning Rate

Jako nejrychlejším a nestabilnějším typem algoritmu se jeví ***traingdx***, z toho důvodu byl zvolen pro další zpracování dat. Největší výhodou tohoto algoritmu je variabilní rychlost učení odvozená z velikosti sítě a struktury učících dat množiny[92].

Posledním parametrem pro vytvoření sítě je rozsah hodnot, se kterými má síť pracovat. Tento krok je proveden pomocí příkazu ***minmax().***

Samotné vytvoření neuronové sítě se provádí pomocí příkazu ***newff***:

net=newff(minmax(w),[31,180,180,180,15],{'logsig','logsig','logsig','logsig','logsig'},'traingdx')

K vytvořené síti lze poté přistupovat jako k objektu s příslušnými vlastnostmi. Mezi základní vlastnosti sítě patří především:

- epochs – maximální počet cyklů učení (poté se učení zastaví)
- goal – požadovaná maximální kvadratická chyba
- time – maximální čas trénování v sekundách
- show – počet epoch, po kterých je cyklicky vykreslován graf
- min_grad – minimální velikost gradientu (poté se učení zastaví)
- lr – rychlost učení

V případě simulace sítě v této práci bylo nejdříve použito následující nastavení:

net.trainParam.epochs=3000

net.trainParam.goal=1e-2

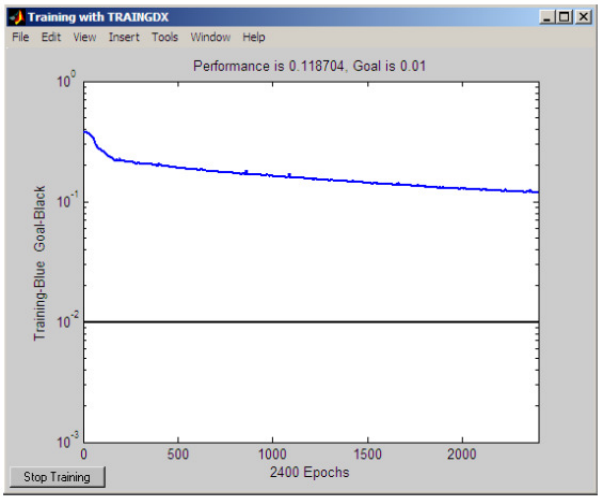
Následující příkaz slouží k naučení sítě na konkrétní vzory. Těmito vzory je myšlena matice obsahující čísla 1–22 564 v binárním kódu. Tyto hodnoty jsou voleny z důvodu jednoduchosti. V případě konkrétní aplikace a zapojení výstupů sítě do dalších systémů by bylo možné samozřejmě hodnoty změnit a přizpůsobit tak chování sítě v dané situaci[94].

[net]=train(net,w,vzor)

Jak lze vidět z níže uvedeného obrázku, požadované chybovosti 1% nebylo dosaženo. Minimální hodnota chybové funkce dosáhla hodnoty zhruba 12% při počtu 2400

učících epoch. Je to zapříčiněno zejména velkým objemem dat, pomocí kterých je celá síť učena.

Obr. 64 *Graf chybové funkce*



Zdroj: [113]

Je tedy zřejmé, že v tomto pojetí je použití neuronové sítě velice problematické, resp. chybovost rozeznání stavu je neúnosně vysoká pro konkrétní použití. Lze pokračovat dále tak, že použitím shlukové analýzy vytvoříme optimalizovanou strukturu dat, která bude mít (očekávaně) lepší charakteristiky učícího se procesu a lze očekávat extrémní snížení chybovosti. Tím se ale eliminuje základní kladná vlastnost tohoto neuronového modelu – jeho jednoduchost, univerzálnost a rychlost nasazení.

Podařilo se však nalézt ještě jednu možnost, jak zlepšit průběh chybové funkce jednoduchým způsobem – prostou redukcí vstupních dat. Je totiž zcela nesmyslné, vkládat do neuronového modelu plnou „šířku“ dat komunikační sběrnice – i když je to možné – viz. předchozí příklad. Pro účely diskutovaného modelu a pak i následně pro praktické použití postačí vkládat relativně malé množství stavů (vstupních hodnot) a detekovat na základě nich relativně malý počet potřebných událostí (při testování integrace pomocí PGM již bylo dříve doloženo, že již při počtu 3-5 událostí lze realizovat základní integraci mezi poplachovými systémy).

V druhém kroku byl tedy sestaven model, který sledoval pouze 3 základní stavy poplachového systému (klid – poplach – sabotáž) a to již při předpokládaném počtu zón 31 odpovídá 93 potřebným stavům systému. Pokud by byl uvažován větší systém, např.

obvyklý počet zón 192, odpovídalo by to 576 stavům systému (stavy obsahují informace o zónách, na kterých situace vznikla).

Postup pro vytvoření sítě je obdobný jako v předešlém případě, liší se pouze vstupními hodnotami, velikostí a parametry sítě:

- **v případě modelování sítě pro 93 stavů:**

net=newff(minmax(w),[14,40,40,5],{'logsig','logsig','logsig','logsig'},'traingdx')

net.trainParam.epochs=2000

net.trainParam.goal=1e-2

[net]=train(net,w,vzor)

- **v případě modelování sítě pro 576 stavů:**

net=newff(minmax(w),[14,100,100,10],{'logsig','logsig','logsig','logsig'},'traingdx')

net.trainParam.epochs=2000

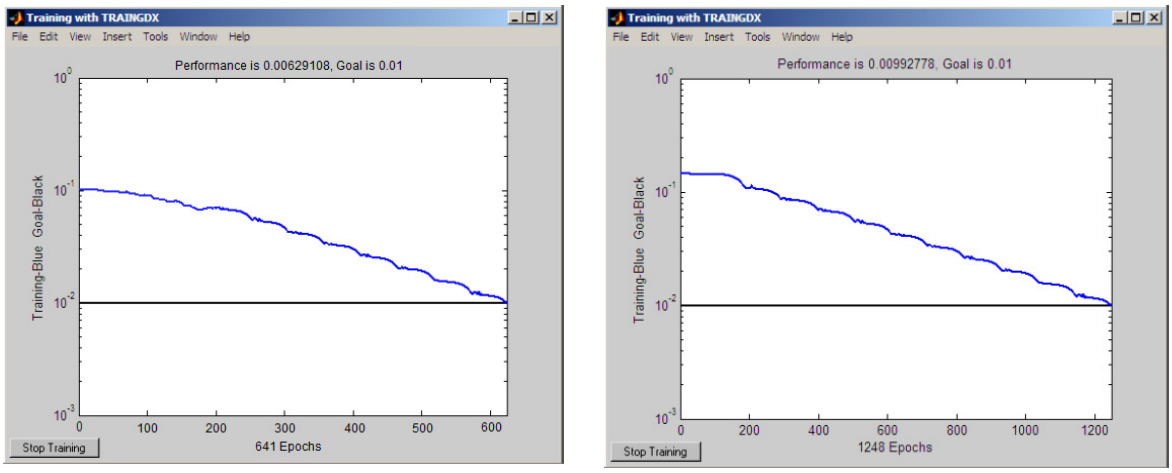
net.trainParam.goal=1e-2

[net]=train(net,w,vzor)

Výsledky testování v obou případech jsou demonstrovány v následujících grafech:

Obr. 65 *Grafy chybové funkce pro různý počet stavů*

modelování sítě pro 93 stavů: modelování sítě pro 576 stavů:



Zdroj: [113]

V tomto případě již není žádný problém síť dostatečně adaptovat a vzhledem k nižšímu objemu dat je pro chybovou funkci 1% časová náročnost výpočtu v obou

případech v podstatě zanedbatelná. Rovněž průběh učení této sítě je v podstatě identický a v obou případech bylo velice rychle dosaženo požadované chybové funkce 1%. Testováním bylo zjištěno, že pokud budeme požadovat chybovost 0.1% , bude této chybovosti dosaženo v případě modelování 93 stavů po 1728 epochách, což ještě stále je časově akceptovatelné. Při požadavcích na nižší chybovost (0.01%) však již dochází ke stavům přeučení sítě a tento postup selhává.

Korektnost a přesnost naučení neuronové sítě lze nejlépe prověřit simulací některého ze stavů naučené sítě. Následující tabulka demonstruje „odpovědi" naučené redukované neuronové sítě (pro 31 zón).

Tab. 13 Neuronový klíč – významnost predikcí naučeného perceptronu

pořadové číslo stavu	**5**				
výstup sítě	0.0000	0.0463	0.9128	0.1922	0.9844
požadovaná hodnota	0	0	1	0	1
pořadové číslo stavu	**10**				
výstup sítě	0.01836	0.8925	0.0208	0.9362	0.1108
požadovaná hodnota	0	1	0	1	0
pořadové číslo stavu	**30**				
výstup sítě	0.8736	0.9151	0.9895	0.8919	0.0087
požadovaná hodnota	1	1	1	1	0

Výše uvedená tabulka jasně demonstruje, že navržená síť je schopna se naučit patřičný počet stavů s minimální chybovostí a je tento model možné použít k dalšímu zpracovaní a technickému návrhu řešení.

Alternativně k modelu vícevrstvého perceptronu byla díky spolupráci s DF ČVUT testována možnost využití modelu neuronu vytvořeného na principu Kohonenovy sítě. Tento model je sice výrazně náročnější z pohledu HW vybavení, pro praktické použití však dává velice dobře automatizovatelné předpoklady vzhledem k samoučící schopnosti této sítě. Jedná se o jednovrstvou síť s dopředným šířením, kde vstupní vektor je definován vztahem:

$$X = [x_1,...x_N]^T, x_i \in R \qquad /6/$$

Výstupní hodnota neuronů je definována jako vzdálenost mezi vstupním a váhovým vektorem.

Pro modelování byl opět využit program Matlab. Vytvoření neuronové sítě se provádí pomocí příkazu ***nnt2som***:

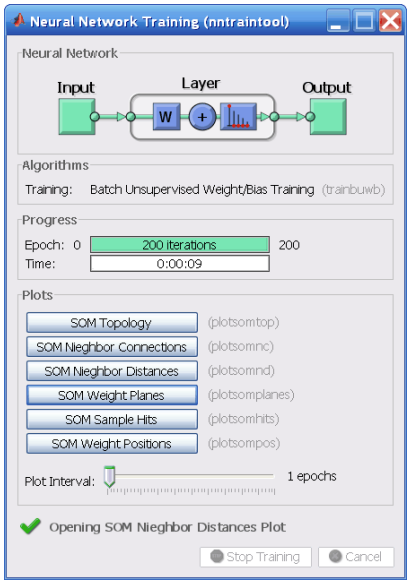
net=nnt2som(mm,w,lr,step,tlr, tnd)

Parametr net inicializuje nadefinovanou síť se stanovenými vlastnostmi:

- mm – matice tvořená hodnotami min a max vstupních hodnot
- w – matice vah
- lr – počáteční úroveň učení
- step – počet iterací
- tlr – adaptivní fáze úrovně učení
- tnd - adaptivní šíře okolí „vítěze“

Funkcí ***net=train(net,M)*** se provede spuštění vlastního trénování sítě (M je soubor s maticí vstupních vzorů). Po načtení vzorů ze souboru dat dochází k vykreslení počátečního rozložení neuronů i s jejich vazbami do mapy rozložení počátečních vzorů. Následně dojde k otevření okna **Neural Network**, kde se zobrazuje průběh vlastního trénování.

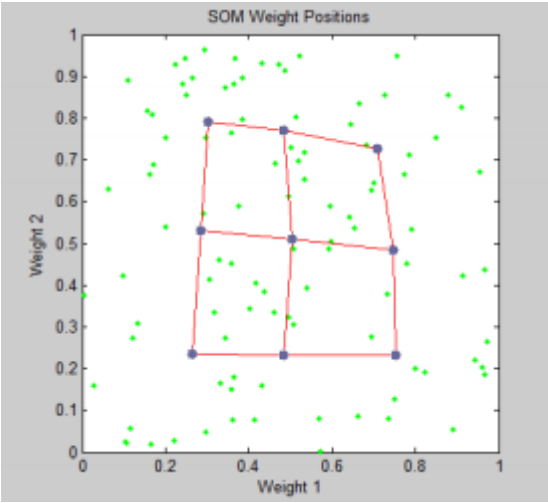
Obr. 66 *Průběh trénování Kohonenovy sítě*



Zdroj:vlastní dle [15]

Následně dojde k uložení čísel neuronů, ke kterým byl daný vstup přiřazen a k jejich grafickému znázornění příslušnými vazbami Obr. 67.

Obr. 67 *Grafické vyjádření konečného rozložení neuronů*



Zdroj:vlastní dle [15]

Tím je proces modelování ukončen. Je však potřeba provézt detailní ověření příslušných výsledků – úspěšnost přiřazení příslušných vzorů[103]. Vzhledem k pozitivním výsledkům použitím perceptronu nebude zde provedena kompletní diskuse. Ze zjištěných hodnot však plyne, že rozmezí počátečního nastavení vah nemá na konečné přiřazení vliv. Primárně úroveň nalezení shody závisí na konkrétním nastavení vah a jejich vzájemné počáteční pozici. V testování a ověření počátečních pozic v konkrétním použití je potřeba dále pokračovat. Vzorový program je uložen v Příloze 8.

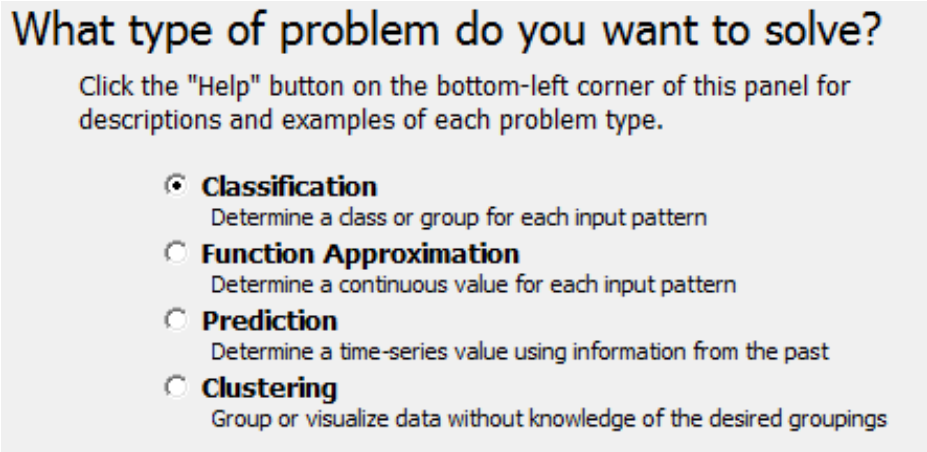
Z hlediska legislativy je nutné, aby systémy integrované tímto způsobem (model vícevrstvého perceptronu neuronové sítě) splňovaly normu ČSN CLC/TS 50 398:2009. Tato norma definuje tři základní skupiny integrovaných systémů dle jejich vzájemného ovlivňování a samostatnosti, a to do skupin 1, 2A a 2B. Díky samostatnosti navrženého modelu neuronové sítě lze navržený prvek zařadit do skupin 2A či 2B, čímž je legislativní požadavek splněn.

5.3.1 Využití nástroje NeuroSolutions

Jak již bylo zmíněno v úvodu předchozí části, pro ověření výsledků a především pro zkrácení času potřebného pro vytvoření modelu a především jeho naučení, byl souběžně s programem MathLab otestován a použit program NeuroSolutions verze 6.31. Základní výhodou tohoto systému je především to, že se výhradně věnuje problematice modelování neuronových sítí a neobsahuje tedy další moduly a knihovny s touto problematikou nesouvisející. Rovněž tak při porovnání času pro simulaci a učení je ve většině případů min. 2x rychlejší než program MathLab s odpovídajícím balíčkem. Velice příjemné je i jeho přímé propojení na vstupy a výstupy MS Excel a MS Access. Určitou nevýhodou je zcela netradiční ovládání (spíše vhodné pro méně zkušené uživatele) a především jeho cena. To je také důvod proč nebylo možné použít knihovny pro spolupráci s MS Excel a další a při modelování byla použita časově omezená volná verze. I tak je ale možné říci, že se jedná o skutečně kvalitní nástroj pro modelování pomocí neuronových sítí, což ostatně demonstruje množství významných uživatelů- MedSolutions, Lockheed Martin, Boxing, ExxonMobil, NASA, USDA,United states army - Corps of engineering a mnoho dalších[51].

Tento software nabízí široké možnosti od výběru různých typu sítí, např. vícevrstvé perceptrony, modulární, RBF sítě, SOM až po vlastní konstrukci neuronové sítě, která vyžaduje již pokročilejší znalost tvorby neuronových sítí a vnitřních nastavení. Další možností je využití průvodce, který zvolí doporučená nastavení všech komponentů neuronové sítě, které lze dodatečně dle potřeby upravovat, což je ideální právě pro začínající uživatele neuronového modelování. Je samozřejmé, že alespoň základní znalosti jsou i tak nezbytné.

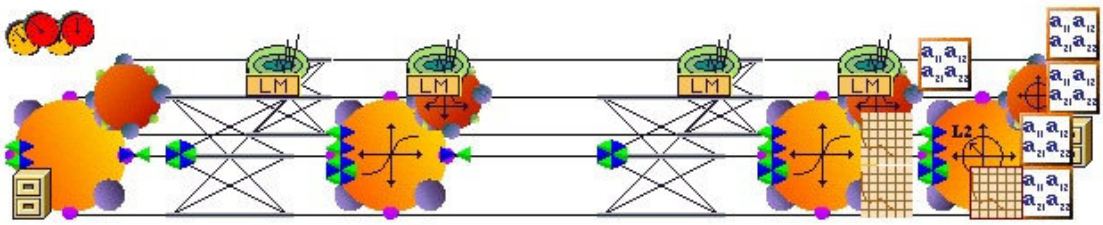
Obr. 68 *Ukázka programu NeuroSolutions – první volba typu problému*



Zdroj:[51]

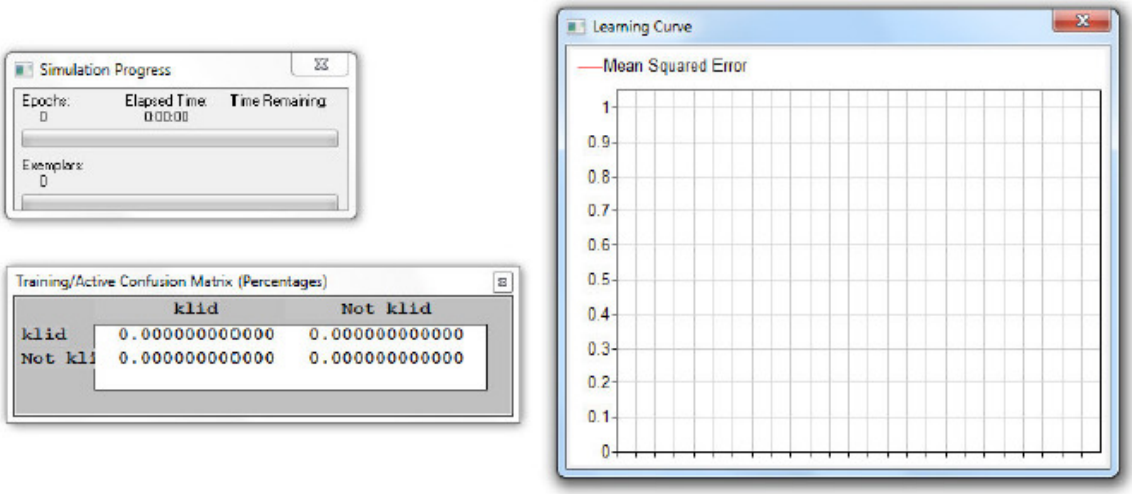
V tomto konkrétním případě byl zvolen způsob tvorby sítě s průvodcem. Byla vybrána klasifikační úloha, definován hlavní problém, umístění vstupních dat, požadovaných výstupů na disk a volba stupně komplexnosti (nižší úroveň odpovídá rychlejšímu zpracování dat a opačně). Po ukončení nastavení je automaticky sestrojena neuronová síť (viz Obr. 67 a 68).

Obr. 69 *Způsob vytváření vícevrstvého perceptronu v programu NeuroSolutions 6.31 (grafický model)*



Zdroj: [112][51]

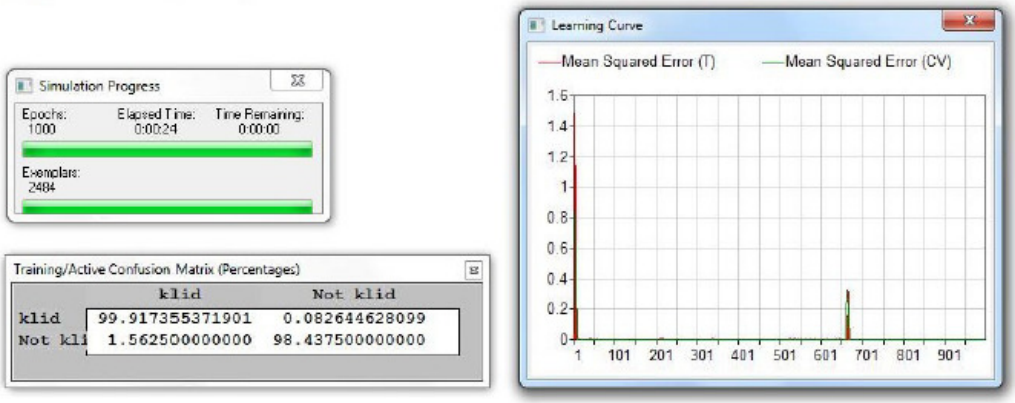
Obr. 70 *Nástroje a příslušenství v prostředí NeuroSolutions ver. 6.31- výchozí stav*



Zdroj: [112][51]

Po spuštění simulace probíhá vše automaticky dle předvoleného nastavení, kde jsou propočítávány prahovací hodnoty. Zpětným šířením chyby jsou přepočítávány hodnoty synaptických vah. Pro výpočet vah byla použita metoda Levenberg-Marquardt[88]. Učení probíhá ve zvoleném počtu opakování, resp. v počtu 1000 učících epoch, které lze dle potřeby navýšit či snížit. V průběhu učení jsou upravovány procentuální hodnoty v matici a současně je vykreslována učící křivka, která by měla mít klesající trend, resp. snižování střední kvadratické chyby (viz Obr. 69) [90].

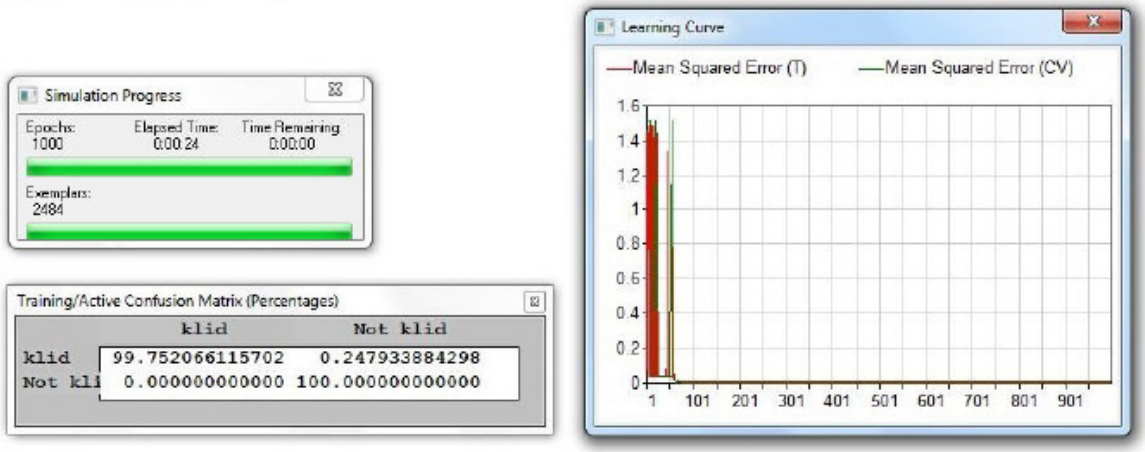
Obr. 71 *Zpřesňování učení vytvořeného perceptronu - Výstup z první simulace vícevrstvého perceptronu MLP, (klid 99,92 % a Not klid 98,44 %)*



Zdroj: [113]

Postupnou změnou výše uvedených kriterií byl nalezen optimální model, který je charakterizován následujícími parametry:

Obr. 72 *Finální vstup simulace vícevrstvého perceptronu MLP, (klid 99,75 % a Not klid 100 %)*



Zdroj: [113]

V uvedeném grafu a tabulce výpočtu je překvapivé především to, že odpovídající maximální požadované chyby bylo dosaženo již po 63 epochách. Tato hodnota je řádově lepší než hodnoty uváděné v předchozí části u programu MathLab. Bohužel, vzhledem k tomu, že nebyla k dispozici placená verze programu, nebylo možné podrobněji analyzovat průběh chybové křivky ani provézt export do externího programu (MS Excel). Ale i tak je zřejmé, že simulační nástroje v oblasti neuronových sítí jsou v programu NeuroSolutions výrazně kvalitnější než odpovídající balíček v programu MathLab.

Pomocí nástroje NeuroSolutions se tedy jednoznačně podařilo potvrdit výsledky, kterých bylo (výrazně pracněji) dosaženo pomocí programu MathLab a balíčku NeuralNetwork.

5.3.2 Shrnutí výsledků a dílčí závěr

Matematickým modelem a jeho praktickým ověřením bylo opakovaně zjištěno, že možnost použití neuronového interface pro propojování poplachových systémů mezi sebou

je nejenom možné, ale především je poměrně jednoduché a relativně spolehlivé. Z výše uvedených dat vyplývá, že při max. chybě 1% bylo nutné použít pouze kolem 60 učících epoch. O něco horšího výsledku bylo dosaženo v případě použití modelu vytvořeného programem MathLab, což ale nesnižuje realizovatelnost metody, pouze signalizuje nikoli zcela vhodný modelový nástroj.

V každém případě byl tento způsob integrace jednoznačně potvrzen a je potřeba s ním počítat jako se zcela univerzálním integračním nástrojem pro integraci nejenom poplachových systémů. Pozitivní je především vlastnost neuronového klíče dopředu určit požadované přenášené stavy a tyto se "naučit" pro přenos do druhého (dalších) systémů. Instalační a servisní pracnost je pak v podstatě nulová. To je zvláště významné například při srovnání se sběrnicemi KNX či CIB .

5.4 Integrace prostřednictvím protokolu SIA09

O standardu SIA09 (**TNI 33 4592**), resp. protokolu, který je tímto standardem aktuálně celosvětově zaváděn, bylo diskutováno již výše v kapitole 4.5. Je zde uvedeno, že tento protokol, díky své robustnosti a bezpečnosti je takřka ideálním protokolem pro přenos rozsáhlejších bezpečnostních informací veřejnou sítí. V dnešní době se používá především pro přenos informací mezi poplachovým systémem (PZTS, EPS a další) a dohledovými středisky (PCO). Rozhodující je však v tomto konkrétním případě možnost nastavit na jednotlivých uzlech propojených pomocí protokolu SIA09! Tato schopnost se v současné době používá především k tomu, aby např. objekt vysílající poplachovou informaci tímto protokolem zaslal informaci nejenom na dohledové centrum, ale současně i na přijímač aktuálně pověřeného zásahového vozidla. Výjezdová jednotka má tedy k dispozici trvale aktuální informace (stejně jako PCO) a navíc lze tyto informace propojit s dalšími externími daty v dohledovém centru (mapa objektu, struktura hořlavin, rizika pro okolí atd.). Z toho je zřejmé, že strukturu přenášených dat lze dynamicky doplňovat bez ztráty kompatibility, čitelnosti a bezpečnosti.

Pro příjem uvedeného komunikačního protokolu v potřebném čase byl experimentálně potvrzen následující hardware:

- procesor – výkonově odpovídající stávajícím procesorům v PZTS či EPS, postačující je např. jednočipový mikroprocesor AT89C51

- paměť RAM – min. 4 kB
- paměť Flash – min. 64 kB
- paměť volná – min. 64 kB
- komunikační intefrace (RJ45, USB, RS232, WiFi, PowerLine, Zigbee, GPRS,…)

To znamená, že v případě kusové výroby lze očekávat cenu řádově kolem 1200 – 1500 Kč. V případě, použití komunikačního protokolu způsobem, který je uveden na následujícím schématu, znamená to, že každý jednotlivý detektor či spínač (sensor, aktor) musí být vybaven tímto rozhraním. A tím samozřejmě výrazně stoupá cena integrovaného systému. Je otázkou, zda by v tomto případě nebylo jednodušší použít již hotové testovací jednočipové počítače (MCU) Arduino či např. Raspberry Pi. Ceny těchto jednočipových počítačů se podle výbavy a osazení pohybují od cca 800 Kč do 2 100Kč.

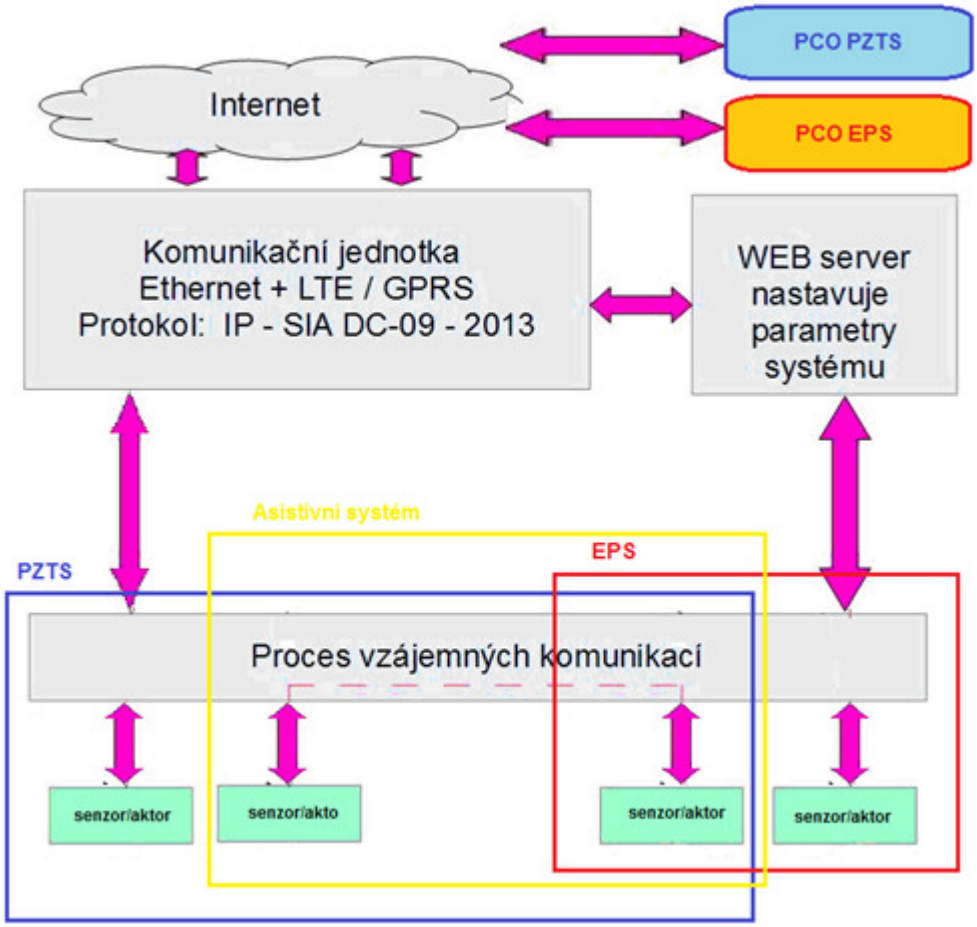
Obr. 73 *Jednočipové počítače předpokládané pro integraci*

RASPBERRY Pi Model B+ (1 490 Kč) Arduino UNO Rev3 (650 Kč)

Zdroj: [http://www.alza.cz/]

Předpokládaná integrace by dle výše popsaného principu probíhala způsobem naznačeném ve schématu Obr. 74. Každý prvek (uzel sítě), bez ohledu o jaký prvek jakého systému se jedná, by byl schopen komunikace na úrovni protokolu SIA DC-09 s libovolným dalším prvkem, s vnitřním webovým rozhraním pro konfiguraci, správu a náhled stavů.

Obr. 74 *Integrace prostřednictvím protokolu SIA09 – distribuovaný integrovaný poplachový systém*



Zdroj: [113]

V zásadě by se tedy jednalo o plně distribuovanou integrační sběrnici na libovolném přenosovém mediu (testováno na GPRS) logisticky podobnou např. sběrnici KNX/EIB či LON, ale umožňující skutečně univerzální propojování při velice administrátorsky příznivém prostředí a především již s integrovanými nástroji pro spolehlivou a bezpečnou komunikaci[104][105]. V případě této logiky by bylo možné, do jednoho např. protipožárního systému integrovat senzory či aktory ze zcela jiných objektů

s původním systémem nijak nepropojeným (podmínka konektivity). Totéž samozřejmě v případě zabezpečovacího či libovolně jiného poplachového systému. Firma mající tedy několik sídel (po celém světě) by mohla mít na jednom místě trvalé informace o všech svých detektorech ve všech objektech a podobně jako v případě tzv. „Internetu věcí“ by mohli vzniknout virtuální poplachové systémy, zcela bezpečné proti napadení a triviálním způsobem rozšiřitelné.

Podrobněji o bezpečnosti protokolu viz. Příloha 7.

5.4.1 Shrnutí výsledků a dílčí závěr

Použití bezpečnostního protokolu SIA09 dle TNI 33 4592 výše popsaným způsobem **zcela zásadně mění pohled na uzavřenost jednotlivých poplachových systémů a jejich integrovatelnost** s dalšími obvyklými systémy inteligentních budov. Pokud libovolný z prvků v systému PZTS, EPS, CCTV a řady dalších, bude schopen komunikace v plném rozsahu této TNI, je triviální na úrovni každého prvku programově určit, na jaký další prvek, se bude konkrétní informace přenášet. V podstatě se tak tento návrh podobá řešení známému z KNX/EIB (výše popsáno), ale bez nutnosti fyzického propojování a nastavování na hardwarové úrovni, ale správa těchto vlastností probíhá na úrovni aplikačního protokolu a lze tedy použít jednoduché a přitom bezpečné nástroje na správu a konfiguraci. Druhým, a možná ještě výraznějším rysem je virtuálnost celého řešení – jednotlivé systémy se stávají vlastně virtuální – fungují v jakémsi claudu a není tedy problém jeden bezpečnostní systém realizovat nad několika objekty tisíce kilometrů od sebe fyzicky vzdálených. Možnost tohoto nasazení výrazně přesahuje téma této práce a bylo by krajně vhodné se této problematice dále věnovat např. v samostatné disertační práci či soustavným výzkumem. Praktická realizace je však již nyní možná.

6 ZÁVĚRY

Tato kapitola se zabývá doporučeními a závěry, vyplývajícími s poznatků, kterých bylo v této disertační práci dosaženo. Zároveň je zde shrnut aktuální stav v problematice integrace bezpečnostních systémů právě s přihlédnutím na zjištěné závěry této práce.

Výše uvedené testy jednoznačně prokázaly nezbytnost vhodného a univerzálního integračního nástroje a to nejenom v případě integrace poplachových systémů. Jednoznačně bylo prokázáno, že nejčastěji používaná řešení nejsou v tomto případě optimální. Výraznou roli při posuzování vhodné technologie integrace hraje především rozsáhlost integrovaných systémů, množství předávaných dat mezi systémy a samozřejmě požadovaná spolehlivost. Naopak rychlost přenosu informace je při dnešních technologiích již kriteriem, které není kritické a není potřeba jej při volbě technologie integrace příliš zdůrazňovat. Po zkušenostech z provedených testů je mnohem důležitější zohlednit jednoduchost a přehlednost instalace a především správy integračního prvku včetně jeho univerzálnosti ve vztahu k systémům různých výrobců.

Prioritou a základní charakteristikou integračního systému (nejenom) poplachových systémů, bude především:

- spolehlivost přenosu dat
- bezpečnost přenášených dat
- integrované systémy se nesmí navzájem negativně ovlivňovat ve vztahu k funkčnosti a spolehlivosti jednotlivých integrovaných systémů
- možnost snadné konfigurace a modifikace
- univerzálnost řešení
- ověřitelnost přenesených dat (časové známky, logy atd.)

Z výsledků práce je zřejmé, že všechny tyto charakteristiky (kromě jediného) lépe splňují integrační systémy založené na centrálním uzlu (PC, PLC), což je ale technologicky krok zpět a nelze tento způsob integrace perspektivně doporučovat. Stejně tak je z pohledu bezpečnosti a spolehlivosti zcela neakceptovatelné jakékoli řešení, které využívá pro přenos dat klasický TCP/IP protokol. Historie průmyslového trojského viru Stuxnet se již

několikrát opakovala a jistě není vhodné zvolit technologii, která tento způsob napadení umožňuje. Provedené měření a testy opravňují k hodnocení testovaných integračních technologií a jejich posouzení ke zvažovanému nasazení. Samozřejmě, vzhledem k tomu, že se jedná o různé technologie, musely i testy být různě voleny, proto není možné prosté srovnání výsledků. Lze je však určitým způsobem kvantifikovat.

Integrace pomocí programových vstupů/výstupů (PGM) je prakticky ideálním a levným řešením v případě přenosu stavů do max. 15 přenášených stavů (aktoru/sensoru). Při větším množství však již výrazně stoupá složitost zapojení a logika celého systému. I když během testování byly realizovány integrace s větším množstvím vstupů (až do 25), změny a modifikace systému propojení musí následně provádět specializovaná firma, optimálně ta, která realizovala prvotní propojení. Testy potvrdily vysokou spolehlivost i životnost takového řešení a prakticky 100%ní odolnost vůči vzájemnému negativnímu ovlivňování systémů mezi sebou.

Využití sběrnice KNX/EIB je v současné době zřejmě nejvíce rozšířené, především v Evropě. Bohužel provedené testy jasně prokázaly, že složitost instalace a zvláště případných změn je důvodem, proč ji vždy musí provádět specializovaná firma. Navíc je systém neadekvátně drahý (a cena výrazně neklesá). Problém s napájením a spolehlivostí přenosu informace byl dostatečně diskutován v příslušných částech kapitoly 4 a 5. Největším problémem tohoto řešení (kromě ceny a spolehlivosti) je poměrně velká nekompatibilitu KNX zařízení různých výrobců a to nedává velké naděje pro budoucí integrace. Jednoznačným pozitivem řešení je však možnost propojení opravdu rozsáhlých systémů, i když za cenu relativní složitosti zapojení a konfigurace systému.

Sběrnice CIB je vzhledem ke své topologii (serverové řešení) oproštěna od většiny problémů KNX sběrnice. Navíc se jedná o českého výrobce s dobrým servisem a výbornou komunikací směrem ke klientům. V posledních několika letech podniká výrobce sám aktivní kroky k testování integrace poplachových systémů pomocí svých technologií (diskutováno v kap. 4 a 5). Bohužel největším problémem je právě centrální řešení a problém napájení sběrnice. Zamykání jednotlivých modulů kódu v tuto chvíli již výrobce řeší, stejně jako některé další nedostatky. Lze tedy očekávat, že v poměrně krátké době bude tento systém (v případě akceptace serverového řešení), připraven k případné integraci spíše středně rozsáhlých systémů.

Zcela původní technologie integrace pomocí tzv. neuronového klíče byla v rámci této práce ověřena především na matematickém modelu simulující neuronovou síť daného typu. Podstata řešení eliminuje některé negativní vlastnosti předchozích řešení (především náročnost instalace a další konfigurace). Modelováním byla ověřena teoretická funkčnost navrženého řešení. Podle výsledků získaných z modelu je oprávněné očekávat, že tento způsob integrace bude vhodný pro středně velké integrace (řádově v desítkách až stovkách stavů), bude extrémně jednoduchý pro integraci a relativně levný. Pozitivní je rovněž univerzálnost tohoto řešení. Samozřejmě jedná se o spíše serverové řešení, i když v tuto chvíli se připravuje modelování distribuované sítě navrženého modelu.

Poslední z diskutovaných řešení je metodika přenosu pomocí SIA09. Jedná se spíše o protokolární řešení (na rozdíl od většiny předchozích technologií). Zcela zásadní je zde možnost vytvoření virtuální sítě (claudu) nad v podstatě neomezeným množstvím prvků a jejich vzájemné propojení bezpečným protokolem. Toto řešení bylo v práci diskutováno pouze jako teoretická možnost a je potřeba jej prakticky blíže ověřit, ale již z provedené analýzy je jasné, že se jedná o optimální řešení především pro integraci velkých systémů na rozsáhlé oblasti (v podstatě technologicky neomezené).

Tab.14 Shrnutí výsledků v tabulkové formě

technologie integrace	klíčové pozitivní vlastností	klíčové negativní vlastnosti
PGM	• cena • jednoduchost • spolehlivost • univerzálnost	• pouze pro menší systémy • problematická rozšiřitelnost • nižší uživatelský komfort
KNX/EIB	• rozšířenost • velcí výrobci • rozsáhlé systémy • distribuované řešení	• vyšší cena • neúplná komptabilita • chybovost přenosu (kolize) • nedostatečně řešené napájení • problematická změna konfigurace a programování
CIB	• rozšířenost v ČR a kompatibilita s jiným řešením • proprietární příprava na poplachovou integraci • rozsáhlé systémy • přehledné programování	• vyšší cena • serverové řešení • nedořešené zamykání modulů • nedostatečně řešené napájení
Neuronový klíč	• uživatelsky a systémově jednoduché • cenově příznivé • přiměřeně spolehlivé • zcela univerzální	• původní v praxi nevyzkoušené řešení • potenciálně bezpečnostní riziko • vhodné pro menší a středně velké systémy
SIA09	• univerzální • zcela bezpečné • kompatibilní s většinou současných používaných poplachových systémů a PCO	• původní v praxi nevyzkoušené řešení • zatím pouze odhadovatelný způsob implementace • nejistá cenová kalkulace¨ • nutný další vývoj a testování

Na základě tohoto shrnutí byla definována míra vhodnosti nasazení daného typu integrace pro konkrétní velikost integrovaných systémů.

Tab. 15 Vhodnost nasazení technologie integrace dle rozsahu

technologie integrace	Malá integrace *(1 – 15 stavů)*	Střední integrace *(10 – 200 stavů)*	Rozsáhlá integrace *(100 a více stavů)*
PGM	80 %	20 %	0 %
KNX/EIB	2 %	8 %	90 %
CIB	5 %	15 %	80 %
Neuronový klíč	30 %	50 %	20 %
SIA09	20 % *(odhad)*	60 % *(odhad)*	20 % *(odhad)*

V současné době používané prostředky integrace poplachových systémů v tzv. „inteligentních budovách“ nejsou zcela optimální. V některých případech je jejich použití dokonce nejenom rizikové a neodpovídající platným normám, ale dokonce protiprávní (odporující platné legislativě). Proto byly v práci ověřeny nejčastěji používané technologie integrace a porovnány s vlastním původním řešením.

Praktické nasazení je samozřejmě již jinou záležitostí. Autor práce se při své další činnosti jako člen normalizační komise TNK 124 při Úřadu pro normalizaci a měření, případně při své práci v prezidiu klíčové profesní organizace (ČKBS) a v dalších poradních orgánech (např. Hospodářská komora) pokusí aktivně prosazovat takový způsob integrace, který je nejenom komerčně zajímavý, ale především koncepčně vhodný a teoreticky zdůvodnitelný.

7 PŘEDPOKLÁDANÝ DALŠÍ VÝZKUM

Autor by velice rád při své další činnosti navázal na již vytvořené kontakty a vazby, které se podařilo uzavřít během zpracování této práce. Jedná se nejenom o spolupráci v již výše jmenovaných organizacích, ale i o osobní kontakty a domluvené další projekty. V několika posledních měsících vznikl přímo na podnět Hospodářské komory (sekce komerční bezpečnosti) požadavek na ověření bezpečného a spolehlivého přenosu dat mezi poplachovými systémy a dohledovými centry. Je oprávněný předpoklad, že s rozvojem a zaváděním nového protokolu LTE (G4 sítě) dojde k výraznému snížení spolehlivosti přenosu bezpečnostních dat přes mobilní síť, což je v případě České republiky naprostá většina všech přenosových tras. Na této problematice je tedy již několik měsíců navázána spolupráce s Hospodářskou komorou a Českým telekomunikačním úřadem.

Velice zajímavým se jeví výzkum realizovaný s polskou firmou a ČKBS o.s. na integraci mobilního dohledového přístroje do perimetrického systému rozsáhlých objektů. Na ČZU již byl před několika lety podobný problém řešen (jak formou diplomových prací, tak i disertační prací). Nepodařilo se však vyřešit problém automatického dokování a přímého programování GPS mobilní jednotky ze zabezpečovacího systému a zvýšit dosah on-line přenosu. V současné době společnost MW Power dodala dron s dosahem až dva km a řeší se programová a legislativní otázka použití v ČR a v Polsku při integraci do poplachových systémů budov a objektů

Rovněž velice zajímavým, i když legislativně poměrně obtížným je testování zabezpečovacích systémů bez trvalého zdroje napájení. Opět pro ČKBS o.s probíhají testy napájení solárními panely a alternativně větrnou turbínou pro poplachový systém. Pokud budou výsledky testů příznivé (ověřování bude trvat ještě minimálně 1,5 roku), bude snaha na TNK 124 aktualizovat stávající znění normy ČSN 50 131 tak, aby bylo možné tento systém napájení využívat (řada komerčních subjektů se o toto snaží již nyní, bohužel bez hodnověrných testů).

V současnosti největším projektem, na kterém probíhá spolupráce, je řešení integrace zabezpečovacího a asistivního systému. Na řešení se spolupodílí ČKBS o.s. a Ministerstvo práce a sociálních věcí – útvar sociálního začleňování. Setkání jednotlivých řešitelů a diskuse dosažených výsledků proběhne 5. listopadu 2014 na semináři „***Promítnutí asistivních technologií do aktualizovaného NAPu***“ (Národní akční plán

podporující pozitivní stárnutí pro období let 2013 až 2017) a měl by dát jasné mantinely pro státní a komerční subjekty na tomto trhu[84] [87].

Tyto programy spolu s tématy nastíněnými v této práci (především praktická realizace a provoz neuronového klíče a implementace virtuálního řešení pomocí SIA09) dávají zřejmý předpoklad dalšího základního i aplikovaného výzkumu v integrační oblasti poplachových, zabezpečovacích i technologických systémů.

Použitá literatura

[1] ADELI, H. :Smart structures and building automation in the 21(st) century, 25th International Symposium on Automation and Robotics in Construction Location: Vilnius, LITHUANIA Date: JUN 26-29, 2008

[2] ALTHOFF, J.: Preface. In Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 5-6.

[3] ANTTIROIKO, A.-V., VALKAMA, P., BAILEY, S.J.: Smart cities in the new service economy: building platforms for smart services. AI and Society, 2013, p. 1-12, ISSN 0951-5666

[4] ASOCIACE KNX, učební materiály pro základní kurz KNX, 2013.

[5] AULICKÝ, V., et al. Inteligentní budovy a ekologické stavby. 1. vyd. Praha, Nakladatelství Dr. Josef Raabe, s.r.o, 2008. 280 s. ISBN 1803-4322

[6] BARTUŠEK, K. et al.: Měření v elektrotechnice. 2.vydání. Brno: VUT v Brně/VUTIUM, 2010. 212 s. ISBN 978-80-214-4160-6

[7] BISHOP C. M.: Neural Networks for Pattern Recognition. Oxford University Press, NewYork, 1995, 498 s., ISBN 0-38-731073-8.

[8] BOJANOVSKÝ, J.: Inteligentní budova - „Řídicí, bezpečnostní a informační systémy moderních budov“, SECURITY Magazín, listopad-prosinec 2008.

[9] BONFATTI F., MONARI P., SAMPERI U.: ‚IEC1131-3 Programming Methodology, ICS Triplex IsaGRAF Inc., 2003

[10] BUSHBY, STEVEN T.: BACnet – A Standard Communications Infrastrukture for Intelligent Buildings, Automation in Construktion, vydání 6., č.5-6, p.529-540, 1997

[11] ČANDÍK M.: Objektová bezpečnost II. Zlín: Academia centrum, 2004. 100 s. ISBN 80-7318-217-3.

[12] Definice inteligentních budov. (online) [cit. 15.11.2009]. Dostupné z: http://www.ibuilding.gr/definitions.html

[13] DOŇAR, B., ZAPLATÍLEK, K.,: MATLAB - tvorba uživatelských aplikací 2. díl, BEN - technická literatura, 2004, ISBN 80-7300-133-0.

[14] DOŇAR, B., ZAPLATÍLEK, K.,: MATLAB - začínáme se signály 3. díl, BEN - technická literatura, 2006, ISBN 80-7300-200-0.

[15] DOŇAR, B., ZAPLATÍLEK, K.,: MATLAB pro začátečníky 1. díl, BEN - technická literatura, 2003, ISBN 80-7300-175-6.

[16] DUŠEK, B.: Inteligentní budovy a jejich realizace, prezentace na konferenci „Inteligentní budovy 2010“

[17] DUŠEK, F.: MATLAB a SIMULINK – úvod do používání. Univerzita Pardubice 2000, 147 s., ISBN 80-7194-273-1.

[18] Echelon corporations: „Introdusion to the LON WORKS System“, Palo Alto, USA, 1999.

[19] EIBA Handbook Series. E.I.B.A, 3.0. vydani, Brussels, 2004.

[20] EIB-TP-UART-IC—Technical Data. Siemens, www.automation.siemens.com/et/gamma/ download/tpuart.pdf, [cit. 2009-05-20].

[21] elektrika.cz [online]. 2.7.2010 [cit. 2011-03-16]. Netradiční bezdrátový komunikační systém ENOCEAN. Dostupné z WWW: <http://elektrika.cz/data/clanky/netradicni-bezdratovy-komunikacni-system-enocean>.

[22] EZS zařízení EIB/KNX. ABB Informační portál o domovní elektroinstalaci.

[Online]. Publikováno: 2006. Dostupné z: http://www.abb.com/product/seitp329/2d9e138b8c7e35d7c125711e004b1b74.aspx. [Cit. 25. 3. 2014].
[23] FANG, H. , SI, H. , CHEN, L.: Recurrent neural network for human activity recognition in smart home, Lecture Notes in Electrical Engineering, Volume 254, 2013, p. 341-348
[24] FAUSETT, L. V.: Fundamentals of Neural Networks. Prentice-Hall, Inc., Englewood Cliffs, New Jersey 1994. ISBN 0133341860.
[25] FAUSETT, L. V.: Fundamentals of Neural Networks. Prentice-Hall, Inc.,Englewood Cliffs, New Jersey 1994.
[26] FAUSETT, L.: Fundamentals of Neural Networks. Prentice Hall, New York, 1994, 404 s., ISBN 0-13-335186-0.
[27] HAGAN, M.: Neural network design, PWS USA, 1996. 734 s. ISBN 7-111-10841-8.
[28] HARPER R., Inside the Smart Home, Springer, 2003
[29] BURDA, T. : Projekt a realizace certifikovaného zabezpečovacího systému pomocí modulů Tecomat (Foxtrot), diplomová práce TF ČZU Praha, 2013, vedoucí práce Votruba, Z.
[30] HASSOUN, M.: Fundamentals of Artificial Neural Networks. The MIT Press, Cambridge, Massachusetts, London, 1995, 506 s. , ISBN 0-262-08239-X.
[31] HAYKIN, S.: Neural Networks: A Comprehensive Foundation. Macmillan Publishing, New York, 1994, 842 s., ISBN 978-0132733502.
[32] HEJDA, K: Návrh integračního modulu pro kamerový a zabezpečovací systém, diplomová práce TF ČZU Praha, 2013, vedoucí práce Votruba, Z.
[33] HEŘMAN, J., et al.: Elektrotechnické a telekomunikační instalace. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475.
[34] HERMANN, M., HANSEMAN, T, HUBNER, Ch.: Automatizované systémy budov : Sdělovací systémy KNX/EIB, LON a BACnet. 1. vyd. Praha : Grada Publishing, a.s, 2008. 264 s. ISBN 978-80-247-2367-9
[35] HERNYCH M., Řízení funkcí rodinného domu, Automatizace, ročník 53, číslo 3-4
[36] Indect for the security of citizens [online]. Dostupné z: http://www.indect-project.eu [cit. 2013-02-24].
[37] Inteligentní budova (I). In [online]. [s.l.] : [s.n.], 4.10.2002 [cit. 2010-12-28]. Dostupné z WWW: http://www.tzb-info.cz/1143-inteligentni-budova-i .
[38] Inteligentní budovy, učební text VOŠ a SPŠ Kutná Hora, [cit. 2010-11-20]. www.edumat.cz/texty/Rizeni_budov6.pdf .
[39] JANEČKOVÁ, E., BARTÍK, V.: Kamerové systémy v praxi, Linde Praha, 2011, 238 s. ISBN 978-80-7201-850-5 .
[40] JUNQI, D., SIDONG, Z., TAO, Z.: Improved implementation and evaluation of wireless sensor networks in intelligent building. 2011, China Communications 8, 8 , pp. 64-71
[41] KASÍK, P.: Umělý mozek: IBM vytvořila počítač, který umí „programovat“ sám sebe. In: Technet [online]. Publikováno 2011-08-23] Dostupné z: < http://technet.idnes.cz/umely-mozek-ibm-vytvorila-pocitac-ktery-umiprogramovat-sam-sebe-py9-/tec_technika.aspx?c=A110819_111241_tec_technika_pka> [cit. 2014-02-25].

[42] Katalog Teco a.s., Teco a.s., 2013
[43] KELL, A., COLEBROOK, P.: Open Systems for Homes and Buildins: Comparing LonWorks and KNX. i&i limited, 2012,
[44] KLABAN J., Inels a sběrnice CIB – moderní systém inteligentní elektroinstalace, Automa, 12/2008, p. 28 - 31
[45] KLAUDA, Z.: Realizace integrovaného zabezpečovacího systému, diplomová práce TF ČZU Praha, 2013, vedoucí práce Votruba, Z.
[46] KNX System architecture. Konnex association, 2008. Dostupne z: http://www.knx.org/_leadmin/downloads/03 - KNX Standard/KNX Standard PublicDocuments/KNX System Architecture.pdf. [cit. 2013-08-3].
[47] KNX technické informace. Dokument Schneider electric [online]. 2009. [cit. 2011-05-01]. Dostupné z: <http://www.vypinac.cz/download/vypinac.cz_knx_tech.informace.pdf>.
[48] KONÍČEK, T., KOCÁBEK, P.: Cesta k bezpečí. Praha: BEN, 2002. 256 s. ISBN 80-7300-032-6.
[49] KŘEČEK, S., et al.: Příručka zabezpečovací techniky. 3.vydání, Blatná : Cricetus, 2006. 313 s. ISBN 80-902938-2-4.
[50] KŘEČEK, S.: Ochrana majetku systémy průmyslové televize. 1. vydání. Praha: GRADA Publishning, 1997. 183 s. ISBN 80-7169-402-9.
[51] KUBÁLEK, T.: Nasazení neuronových sítí v inteligentních budovách, diplomová práce TF ČZU Praha, 2013, vedoucí práce Votruba, Z.
[52] KUNC J., Elektroinstalace krok za krokem, Praha, Grada, 2006, ISBN 978-80-247-3249-7.
[53] KUNC, J.: KNX/EIB - Inteligentní elektroinstalace. Elektroinstalatér, 2011, roč. 17, č. 1, s. 16 - 18.
[54] KUNC, J.: Krátký pohled do historie systémových instalací, 2008. (online) [cit. 15.12.2009] Dostupný z: < http://elektrika.cz/data/clanky/abb-systemove-elektricke-instalace-knx-eib-2013-2-cast/view?searchterm=knx >
[55] LANGELS, H. J.: KNX IP—using IP networks as KNX medium. Proceedings of the KNX Scientic Conference 2008, Konnex association, St. Katelijne-Waver p 812-821
[56] LECHNER, D., GRANZER,W., KASTNER,W.: Security for KNXnet/IP. Proceedings of the KNX Scientic Conference 2008, Konnex association, St. Katelijne-Waver p 911-918
[57] LI, M.: The construction and development of the green intelligent building, International Journal of Advancements in Computing Technology, 2013, Vol. 6, No. 5, p. 28-35
[58] LIAN, K., HSIAO, S., SUNG, T.: Smart home safety handwriting pattern recognition with innovative technology, Computers and Electrical Engineering, Volume 40, Issue 4, May 2014, p 1123-1142
[59] LOURDAS, V. A.: EIB/KNX as a Building Management System, diplomova prace. Universita Luneburg, Department of Automation Engineering, Luneburg, 2007. Dostupné z: http://www.lourdas.com.gr/vassilis/Files/thesis.pdf [cit. 2010-11-5].
[60] LOVEČEK, T., NAGY, P.: Kamerové bezpečnostné systémy. 1.vydání. Žilina: EDIS -vydavateĺstvo ŢU, 2008. 283 s. ISBN 978-80-8070-893-1.
[61] MAŘÍK V., ŠTĚPÁNKOVÁ O., LAŽANSKÝ J.: Umělá inteligence 4, Academia, Praha, 2003, 476 s., ISBN 80-200-1044-0.
[62] MAŘÍK, V.: Umělá inteligence, Praha : Academia, 1993. 264 s. ISBN 80-200-0496-3.

[63] MATZ, V.: Vytapeni.tzb-info [online]. 25.10.2010 [cit. 2011-03-09]. Systémy používané v "inteligentních" budovách - přehled komunikačních protokolů. Dostupné z WWW: <http://vytapeni.tzb-info.cz/mereni-a-regulace/6879-systemy-pouzivane-v-inteligentnich-budovach-prehled-komunikacnich-protokolu>.
[64] MERZ, H., HANSEMANN, T., HÜBNER, Ch.: *Automatizované systémy budov*. 1.vydání. Praha: GRADA Publishing, 2008. 264 s. ISBN 978-80-247-2377-9.
[65] MIKULA, T.: Orsec [online]. 10.11. 2010 [cit. 2011-03-15]. Konec EZS v Čechách !?!. Dostupné z WWW: <http://www.orsec.cz/cs/informacni-servis/clanky-a-komentare/konec-ezs-v-cechach_38-435/>.
[66] MILENKOVIC, M., DANG, T., HANEBUTTE, U., HUANG, Y. : Platform-integrated sensors and personalized sensing in smart buildings. SENSORNETS 2013 - Proceedings of the 2nd International Conference on Sensor Networks, p. 47-52
[67] MOTÝL, P.: Schneider Electric – průvodce řídicími systémy pro inteligentní budovy. Automatizace. Březen 2005, roč. 48, č. 3, s. 220-222. Dostupný také z WWW: <http://www.automatizace.cz/article.php?a=602>. ISSN 0005-125X.
[68] NERAD, P.: Úvod do neuronových sítí. In: Statsoft [online]. Publikováno 2013-02-05 Dostupné z: http://www.statsoft.cz/file1/PDF/newsletter/2013_02_05_StatSoft_Neuronove_site_linky.pdf [cit. 2014-01-22].
[69] Neuron Chips. Echelon, Dostupné z: http ://www.echelon.com/developers/lonworks/neuron.htm [cit. 2009-05-28].
[70] NEWMAN H. M.,: BACnet - The New Standard Protocol, Electrical Contractor, vol 9/97., p. 119-122
[71] NOVÁK, M., et al.: Umělé neuronové sítě – teorie a aplikace, C.H.Beck, 1998, Praha, 382 s., ISBN 80-7179-132-6.
[72] NÝVLT, O.: Přehled protokolů a systémů pro řízení inteligentních budov. Automatizace. Březen - duben 2010, roč. 53, č. 3-4, s. 121-124. Dostupný také z WWW: http://www.automatizace.cz/article.php?a=2782.
[73] OLEJ, V. :Modelovanie ekonomických procesov na báze výpočtovej inteligencie. Česká republika: Hradec Králové, 2003. 160 s. ISBN 80-90324-9-1.
[74] OSIČKA, P:. Umělé neuronové sítě. Univerzita Palackého v Olomouci, 2010. 29s. Elektronický text. Dostupné z: < http://phoenix.inf.upol.cz/~osicka/courses/uns/lecture4.pdf> [cit. 2010-12-20].
[75] PENYA, Y. K., BORGES, C. E., HAASE, J., et al.: Smart Buildings and the Smart Grid, IEEE Conference: 39th Annual Conference of the IEEE Industrial-Electronics-Society (IECON) Location: Vienna, AUSTRIA Date: NOV 10-14, 2013
[76] PETERKA, J.: Síťový model TCP/IP. 2011 Dostupné z: http://www.earchiv.cz/a92/a231c110.php3 [cit. 2013-02-27].
[77] PIVOŇKOVÁ, A.: Optimalizační algoritmy řídicích systémů inteligentních budov, Praha, 2005
[78] POŠVIC, P.: KNX technik [online]. 1.12.2007 [cit. 2011-03-20]. KNX/EIB. Dostupné z WWW: <http://www.knxtechnik.cz/index.html>.
[79] POŠVIC, P.: KNX technik [online]. 1.12.2007 [cit. 2014-06-8]. KNX/EIB. Dostupné z WWW: <http://www.knxtechnik.cz/index.html>.
[80] Pro projektanty. TECO Průmyslová automatizace, Inteligentní budovy, Smart Grid. [Online]. Publikováno: 16. 9. 2013. Dostupné z: http://www.tecomat.com/wpimages/other/DOCS/cze/TXV00416_01_CFoxRFoxProjektovani_cz.pdf. [Cit. 21. 10. 2013].

[81] Programování podle normy IEC 61 131-3 v prostředí Mozaic, Teco a.s., 11. vydání, 2009
[82] Promotic [online]. 2010 [cit. 2011-03-23]. Komunikace protokolem BACnet. Dostupné z WWW: <http://www.promotic.eu/cz/pmdoc/Subsystems/Comm/PLC/BACnet.htm>.
[83] Průvodce integrovanými bezpečnostními systémy. Dokument BSIA [online]. 2010, 1, [cit. 2011-04-19]. Dostupné z : <http://www.ijssecurity.cz/text/903PIBS.pdf>.
[84] RAK, R., MATYÁŠ, V., ŘÍHA, Z.: Biometrie a identita člověka. Praha, Grada, 2008. 664 s. ISBN 978-80-247-2365-5.
[85] RAY, A.K. , LENG, G. , MCGINNITY, T.M. , COLEMAN, S. , MAGUIRE, L.: Dynamically reconfigurable online self-organising fuzzy neural network with variable number of inputs for smart home application, EU FP7 Rubicon project, IEEE, vol 24(6), p.961-974
[86] ROJAS, R.: Neural Networks: A Systematic Introduction. Springer-Verlag, Berlín, Heidelberg, New York, 1996, p. 502, ISBN 3-540-60505-3.
[87] ŠČUREK, R.: Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text FBI VŠB TU Ostrava. Ostrava: VŠB TU Ostrava, 2008. 58 s.
[88] ŠÍMA J., NERUDA R.: Teoretické otázky neuronových sítí, Matfyzpress, Praha, 1996, 390 s. ISBN 80-85863-18-9.
[89] ŠÍMA, J., NERUDA, R. 18th International Conference on Artificial Neural Networks: ICANN 2008 Praha: Institute of Computer Science ASCR, 2009 . 218 s..
[90] ŠKVOR, O.: Využití neuronových sítí pro integraci PZTS do inteligentních budov, diplomová práce TF ČZU Praha, 2013, vedoucí práce Votruba, Z.
[91] ŠMEJKAL L., KLABAN J., Inteligentní budovy – luxus nebo nezbytnost?, Automatizace, ročník 52, číslo4
[92] ŠNOREK, M.: Neuronové sítě a neuropočítače. Praha: Vydavatelství ČVUT, 2002. ISBN 80-01-02549-7.
[93] Stavebnictvi3000 [online]. 2004 [cit. 2011-04-01]. CONCEPT na českém trhu. Dostupné z WWW: <http://www.stavebnictvi3000.cz/clanky/concept-na-ceskem-trhu/>.
[94] TAUFER, I.; DOLEŽAL, P.:Umělé neuronové sítě 1 – 3, přednášky VŠB-TU Ostrava, Fakulta elektrotechniky a informatiky, 2008
[95] TAUFER, I.; DRÁBEK, O.; SEIDL, P. Umělé neuronové sítě – základy teorie a aplikace (1) – (15). přednášky dostupné také na http://www.chemagazin.cz/prehled.html
[96] Teco a.s. Ceník. Ceník. Teco Advenced Automation Průmyslová automatizace, Inteligentní budovy, Smart Grid. [Online]. Publikováno: 2013Dostupné z: http://www.tecomat.com/wpimages/other/ceniky/Cenik%20Teco%202013_10_v2_CZ_LP_Foxtrot.pdf. [Cit. 30. 2. 2014].
[97] TEICH, T., ROESSLER, F., KRETZ, D., et al.: Design of a Prototype Neural Network for Smart Homes and Energy Efficiency, 24TH DAAAM INTERNATIONAL SYMPOSIUM ON INTELLIGENT MANUFACTURING AND AUTOMATION, 2013 Book Series: Procedia Engineering Volume: 69 Pages: 603-608 Published: 2014
[98] TOMAN, K.: Decentralizované sběrnicové systémy [online]. 2007 [cit. 2010-05-28]. Dostupné z WWW: <http://www.tzb-info.cz/t.py?t=2&i=4213>.
[99] Tzb-info [online]. 11.10.2002 [cit. 2011-03-09]. Inteligentní budova (II). Dostupné z WWW: <http://www.tzb-info.cz/1154-inteligentni-budova-ii>.

[100] Tzb-info [online]. 18.10.2002 [cit. 2011-03-09]. Inteligentní budova (III). Dostupné z WWW: <http://www.tzb-info.cz/1164-inteligentni-budova-iii>.
[101] VALEŠ, M.: Inteligentní dům. Vyd. 2. Brno : ERA, 2008. 123 s. ISBN 978-80-7366-137-3.
[102] Variant [online]. 2010 [cit. 2011-04-01]. VAR-NET INTEGRAL. Dostupné z WWW: <http://www.variant.cz/sekce231-var-net-integral.html>.
[103] VESELOVSKÝ, M. Lineární asociativní paměť (ART) Západočeská univerzita v Plzni, 2013. 12s. Elektronický text.
Dostupné z: http://avari.cz/uir/index.php?pg=lam [cit. 2014-2-6].
[104] VOJÁČEK, A.: Sběrnice LonWorks - 1.část - Úvod [online]. Duben 2005 [cit. 2010-04-12]. Dostupné z WWW: http://automatizace.hw.cz/mereni-a-regulace/ART151-sbernice-lonworks--1cast--uvod.html
[105] VOJÁČEK, A.: Sběrnice LonWorks - 2.část - LonTalk protokol [online]. Duben 2005 [cit.2010-04-13]. Dostupné z WWW:<http://automatizace.hw.cz/mereni-a-regulace/ART152-sbernice-lonworks--2cast--lontalk-protokol.html>.
[106] VOLNÁ, E.: Neuronové sítě I., Ostrava: Ostravská univerzita, 2008. 86s. Elektronický text. Dostupné z: < http://files.klaska.net/cvut/ns2/volna.pdf> [cit. 2012-08-09].
[107] VOTRUBA, Z., KOTEK, T., HART, J.: Integrace systémů PZTS v návaznosti na technologický dohled komerčních budov, závěrečná zpráva grant IGA 31170/1312/3136, Praha, ČZU, Technická fakulta, 2011
[108] VOTRUBA, Z., KOTEK, T., HART, J.: Univerzální propojení ochranných systémů v projektu inteligentních budov. Security magazín. 2011, č. 2, ISSN 1210-8723.
[109] VOTRUBA, Z.: obrazový archív autora, 2010
[110] VOTRUBA, Z.: obrazový archív autora, 2011
[111] VOTRUBA, Z.: obrazový archív autora, 2012
[112] VOTRUBA, Z.: obrazový archív autora, 2013
[113] VOTRUBA, Z.: obrazový archív autora, 2014
[114] VRBOVEC, B.: Předkladová zpráva a technická informace o SIA DC-09, pro TNK 124, 2013
[115] WOOD G., NEWBOROUGH M., Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design, Energy and Buildings, Volume 35, Issue 8, September 2003, Pages 821–841
[116] Začínáme v prostředí Mozaic, Teco a.s., 7. vydání, 2008
[117] ZHOU, Q., ZHANG, Z., CUI, F.: Research on the integrated control teaching system of building based on fieldbus. 2013, Applied Mechanics and Materials 278-280 , pp. 1952-1955, ISSN 1660-9336

Seznam použitých symbolů, zkratek a pojmů

ABB	Asea Brown Boveri, Švýcarsko.
ABS	Akrylonitrilbutadienstyren,
ACK	Acknowledge, potvrzení, součást komunikačních protokolů.
ACS	Access Control System, systém pro řízení přístupu, docházky.
Adaline	Adaptive Linear Neuron - typ neuronové sítě.
ANSI	American National Standards Institute.
axon	Hlavní výběžek těla buňky biologického neuronu.
BAM	Bidirectional Associative Memory (obousměrná asociativní paměť).
BAM	Bidirectional Associative Memory - typ neuronové sítě.
BCU	Bus Control Unit, připojovací člen pro KNX, obsahuje kompletní KNX komunikaci, dovoluje do sebe nahrát libovolný program.
BIM	Bus Interface Modul, připojovací člen pro KNX, podle druhu obsahuje různé připojovací části, neobsahuje program.
Bosch	Výrobce elektroniky a elektrotechniky, Německo.
bps	bits per sekond.
CAN	Rychlá sériová sběrnice, výrobce Bosch.
CANOpen	Otevřená implementace CAN pro řízení obecných realtime systémů.
CCD	Charge-Coupled Device
CCTV	Systémy uzavřených televizních okruhů
cEMI	common EIB Message Interface, formát pro přenos KNX zpráv mezi komunikační vrstvou a aplikací.
CEN	European Committee for Standardization.
CENELEC	European Committee for Electrotechnical Standardization.
CMOS	Complementary Metal-Oxide-Semiconductor (Technologie kov-oxid polovodič)
COM	Component Object Model, komponentová technologie, výrobce Microsoft.ControlWeb
CRC	Cyclic Redundancy Code nebo Cyclic Redundancy Check, kódy

	pro detekci chyb v komunikačních přenosech.
CSMA/BA	Carrier Sense Multiple Access/Bitwise Arbitration, totéž co CSMA/CR.
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance, metoda přístupu ke komunikačnímu médiu, využívá LonTalk, KNX.
CSMA/CR	Carrier Sense Multiple Access/Collision Resolution, metoda přístupu ke komunikačnímu médiu, využívá CAN.
ČSN EN	Česká technická norma (původně Československá státní norma)
DALI	Digital Addressable Lighting Interface, otevřený sběrnicový systém pro řízení osvětlení.
DCS	Door Control System, systém pro ovládání dveří, domovních telefonů, zvonků, ve větších realizacích často integrovaný s ACS.
DDC	Direct Digital Controller
dendrit	Vedlejší výběžky těla buňky biologického neuronu
DeviceNet	Otevřený komunikační protokol na bázi CAN.
DSI	Digital Signal Interface, centralizovaný systém pro řízení osvětlení, výrobce Tridonic.
E.I.B.A.	European Installation Bus Association, asociace výrobců, předchůdce Konnex Association.
Ego-N	Proprietární sběrnicový systém pro domovní elektroinstalace, ABB.
EHS	European Home Systems, sběrnicový systém pro domovní elektroinstalace, fyzické médium PLC, pohlcen KNX.
Echelon	Původní autor a výrobce LonWorks, USA.
EIB	European Installation Bus, otevřený sběrnicový systém pro domovní elektroinstalace, fyzické médium TP, RF, EibNet/IP, PLC. Pohlcen KNX, původem sběrnice Instabus (Siemens, zjednodušená verze Pro bus upravená podle OSI).
EibNet/IP	Druh přenosového média, v EIB postaven na linkovou vrstvu, přenos informací EIB pomocí IP sítě.
EIS EIB	Internetworking Standard, popis chování zařízení a přenosových formátů zajišťující v EIB/KNX kompatibilitu mezi zařízeními.

E-LTE	Easy mode, Logical Tag Extended, jeden ze způsobů adresování v KNX.
EMI	ElectroMagnetic Interference, elektromagnetické rušení.
EPS	Elektronický Protipožární Systém.
Ethernet	Typ lokální sítě, realizuje fyzickou a linkovou vrstvu.
ETS EIBTool	Software, návrhový program pro KNX.
ETSI	European Telecommunications Standards Institute.
EZS	elektrické zabezpečovací systémy (název mimo normu)
FDDI	optický datový interface
FSK	Frequency Shift Keying, přenosová modulace.
HTTP/S	HyperText Transfer Protocol/Secure, univerzální klient/server protokol pro přenos informací, 7. vrstva OSI, využívá se v IP sítích.
HVAC	Heating, Ventilating and Air Conditioning, systém pro udržování teploty a kvality vzduchu.
IAS	Poplachové a tísňové systémy
IB	inteligentní budova
IGMP	Internet Group Management Protocol, protokol pro řízení vícesměrového vysílání v IP sítích.
IP	Internet Protocol, protokol používaný v Internetu, 3. vrstva OSI.
IRC	Individual Room Control, regulace teploty a prostředí v místnosti nezávisle na ostatních místnostech.
ISO	International Organization for Standardization.
Kbps	Kilobytes per second, 1 024 bps
KNX	Otevřený sběrnicový systém pro inteligentní budovy, Konnex association, spojení EIB, BatiBUS a EHS.
kPa	kilopascal
LAM	Linear Associative Memory (lineární asociativní paměť)
LAM	Linear Associative Memory - typ neuronové sítě
LAN	Lokální počítačová síť
LonMark	Sdružení výrobců a uživatelů LonWorks, organizace udržující a

	organizující standardy spjaté s LonWorks.
LonTalk	Komunikační protokol LonWorks.
LonWorks	Otevřený sběrnicový systém pro distribuované řízení, výrobce Echelon.
LTE	viz E-LTE
m	metr
MAC	Media Access Control, součást linkových vrstev (podle modelu OSI), řízení přístupu k fyzické vrstvě.
Madaline	Multiple adaptive linear element - typ neuronové sítě
MAN	městská počítačová síť
MAU	jednotka pro připojení více stanic (kruhová topologie)
Mbps	Megabytes per second, 1 024 Kbps
MLP	Multi-Layer Perceptron (vícevrstvé perceptronové sítě)
MLP	Multilayer Perceptron - typ neuronové sítě
Modbus	jednoduchý otevřený sběrnicový protokol, výrobce Modicon.
ms	milisekunda
MS/TP	Master – Slave / Token – Passing
MSE	Mean Squared Error (střední kvadratická chyba)
MZS	Mechanické zábranné systémy
NAK	Negative Acknowledge, negativní potvrzení, součást komunikačních protokolů.
NBÚ	Národní bezpečnostní úřad
NC	Normally Close - u smyčkových systémů stav klidu
NO	Normally Open - u systémů EPS stav klidu
OCR	Optical Character Recognition (optické rozpoznávání znaků)
OEM	Original Equipment Manufacturer, výrobek vytvořený pro jiné výrobce.
OPC	OLE for Process Control, standardizovaný protokol pro výměnu procesních informací pomocí COM.
OSI	Open Systems Interconnection reference model, abstraktní model vrstvené komunikace a návrhu síťových komunikačních protokolů.
PAN	osobní datová síť

PC	Personal Computer, osobní počítač.
PCI	Peripheral Component Interconnect, sběrnice používaná v PC.
PEI	Physical External Interface, vnější rozhraní KNX BCU.
PIR detektor	Pohybový pasivní infračervený detektor
PL, PLC	Power Line Communication, druh fyzického média, silové kabely.
PLC	Programmable Logic Controller, progamovatelný automat pro (nejen) logické řízení.
PTS	Poplachové zabezpečovací systémy na detekci přepadení
PVC	Polyvinylchlorid
PZS	Poplachové zabezpečovací systémy na detekci vniknutí
PZTS	Poplachové zabezpečovací a tísňové systémy
RAD	Rapid Application Development, metodika nebo nástroj pro rychlý vývoj aplikací.
RBF	Radial Basis Function (sítě s radiálně-bazickou přechodovou f.)
RF	Radio Frequency, druh fyzického média, radiové vysílání, typicky v pásmech s generální licencí.
SAIA	Výrobce průmyslové automatizace, Švýcarsko.
Saphir	PLC pro HVAC, výrobce Siemens.
SAS	Social Alarm Systems (systémy přivolání pomoci)
SCADA	Supervisory Control And Data Acquisition, dozorové řízení a sběr dat.
Siemens	Výrobce elektronických a elektrotechnických zařízení, zakládající člen E.I.B.A., Německo.
SMS	krátká textová zpráva
SNVT	Standard Network Variable Type, standardní, předdefinovaný typ dat protokolu LonTalk.
soft-PLC	Program, který na univerzálním počítači (PC) provádí stejné úkoly jako PLC.
SOM	Self Organizing Maps (samoorganizující mapy)
SŘBD	Systém Řízení Báze Dat, také DBMS, DataBase Management System, nebo též DBS, DataBázový Systém.
synapse	Spojení dvou neuronů sloužící k předávání vzruchů

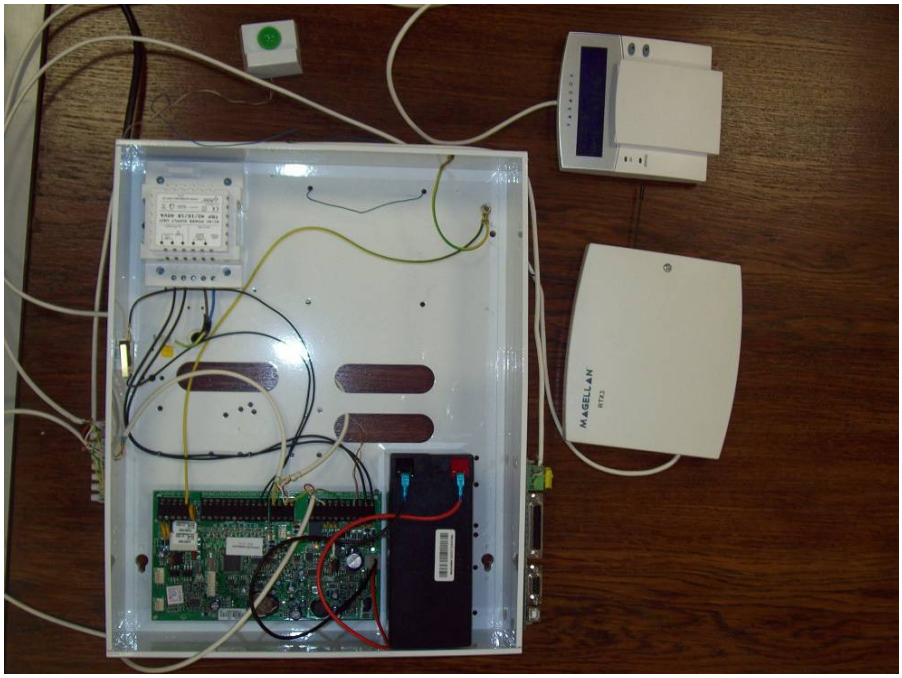
TB	Terabyte
TCP	Transmission Control Protocol, protokol pro řízení spojení, 4. vrstva OSI, využívá se v IP sítích.
TDNN	Time-Delay Neural Networks - typ neuronové sítě
TECO	Výrobce průmyslové automatizace, Česko.
TFT	Thin-Film Transistors
TIA	Telecommunications Industry Association.
TP	Twisted Pair, druh fyzického média, kroucený dvoudrát.
TP-UART	TP Universal Asynchronous Receiver/Transmitter, ASIC pro linkovou a fyzickou vrstvu KNX, výrobce Siemens.
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
USB	Universal Serial Bus, vnější sběrnice pro PC, využívá se především pro PC periférie.
UTP	Unshielded Twisted Pair (nestíněná kroucená dvoulinka)
Wago	Výrobce elektronických a elektrotechnických zařízení, Německo.
WAN	rozsáhlá počítačová síť (nepřesně internet)
Wiegand	standardní rozhraní, kterým komunikují například čtečky bezkontaktních karet
Wi-Fi	bezdrátová síť v nelicencovaném pásmu
WS	WebService, univerzální protokol pro přenos dat pomocí XML, jako nižší vrstva je použito HTTP/S.
XComfort	Proprietární sběrnicový systém pro automatizaci budov, jediná fyzická vrstva je RF, výrobce Moeller.
XOR	Logická operace, výhradní nebo. Často využitá při konstrukci kontrolních slov

Seznam obrázků

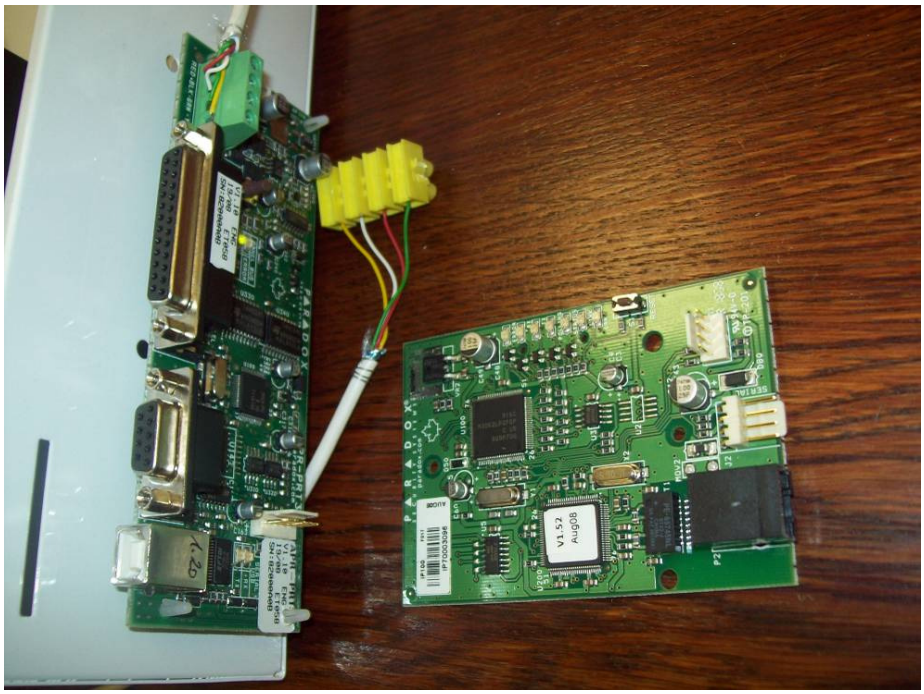
Seznam tabulek

Seznam vztahů

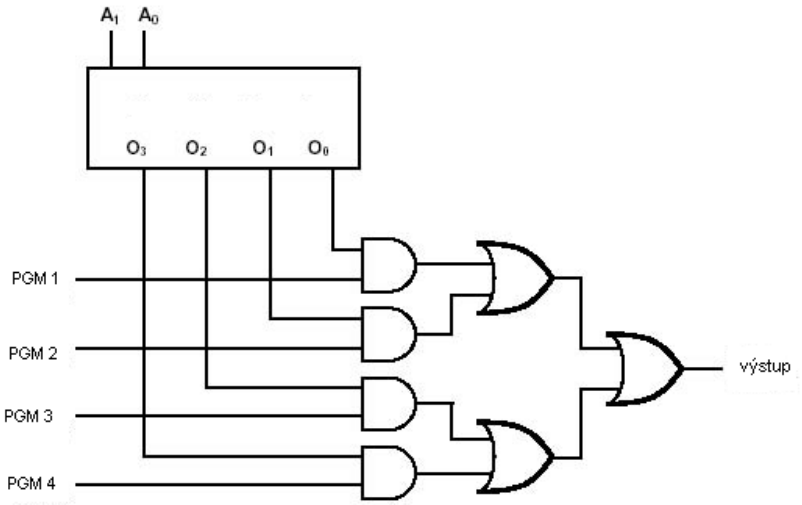
Příloha 1 *Celkový pohled na testovací zařízení PTZS*



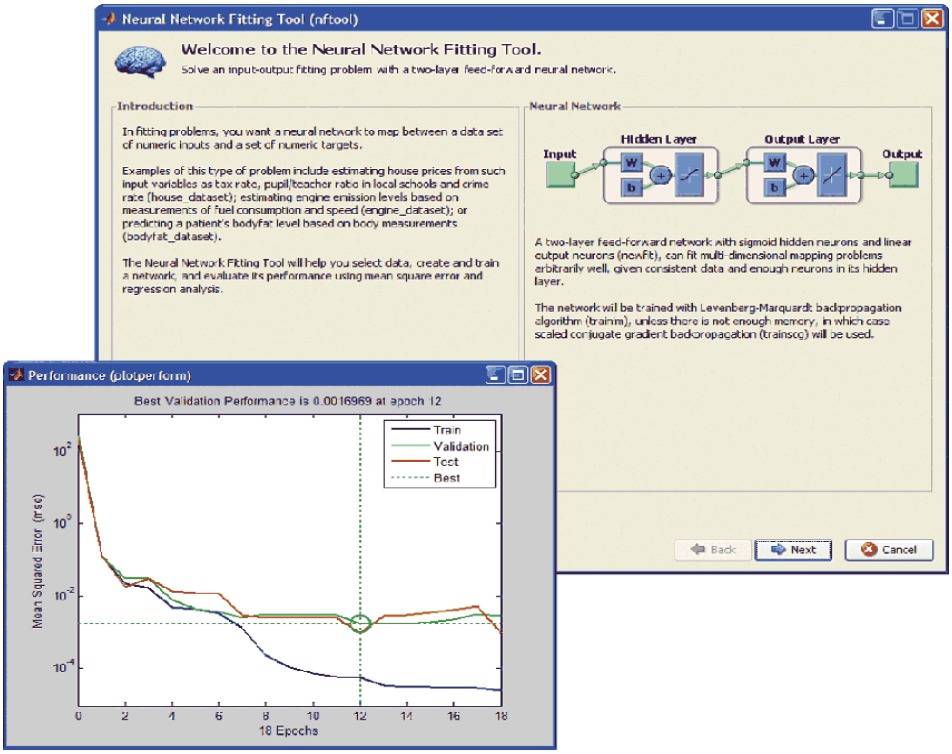
Příloha 2 *Detailní pohled na modul IP100 a PRTX3 s vyvedenou testovací sběrnicí*



Příloha 3 *Schéma multiplexoru / demultiplexoru pro napojení na PGM systému*



Příloha 4 *Využití nástroje Neural Network Toolbox*



Příloha 5 *Souhrn legislativních norem*

Směrnice Evropských společenství je typ dokumentu, který vydává Evropská komise (EC). Tento typ dokumentu stanovuje základní požadavky. Nemá přímou právní platnost v rámci členských zemí. Po jejich projednání a schválení jsou směrnice vyhlašovány v Úředním věstníku Evropských společenství (Offical Journal od European Union). Povinností členských států je zásady uvedené ve směrnicích zapracovat do národní legislativy v termínech stanovených přímo ve směrnicích. Povinnosti ze směrnic technického charakteru jsou závazné pro výrobce, dovozce a distributory této techniky spadající pod působnost příslušného národního legislativního předpisu.

Pro podporu splnění požadavků směrnic jsou vyhlašovány v Úředním věstníku EU **Evropské harmonizované normy**. Tyto normy nejsou závazné, nicméně jejich splnění je po právní stránce chápáno jako precedens splnění právních požadavků stanovených pro daný okruh výrobků. Evropské normy jsou zpracovány Evropskými normalizačními organizacemi **CEN** (Evropský výbor pro normalizaci) a **CENELEC** (Evropský výbor pro normalizaci v elektrotechnice).

Legislativa protipožárních systémů a SHZ:

Mimo legislativní podklady vydané na základě zákona o požární ochraně je nutno respektovat ještě další související předpisy navazující na konkrétní řešení příkladně u staveb, technických zařízení, nebo jednotlivých činností. Jde o soubor dokumentů, které tvoří základní právní rámec pro ochranu životů, zdraví a majetku z hlediska požární prevence. Pro požární bezpečnost staveb je možno jako nejčastěji využívané uvést:

Zákony:

- č. 40/2009 Sb., trestní zákoník, v platném znění,
- č. 360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě, v platném znění,
- č. 22/1997 Sb., o technických požadavcích na výrobky, v platném znění,
- č. 458/2000 Sb., energetický zákon, v platném znění,
- č. 102/2001 Sb., o obecné bezpečnosti výrobků,
- č. 251/2005 Sb., o inspekci práce, v platném znění,
- č. 174/1968 Sb., o státním odborném dozoru nad bezpečností práce, v platném znění,

- č. 183/2006 Sb. stavební zákon, v platném znění,
- č. 262/2006 Sb., zákoník práce, v platném znění,
- č. 309/2006 Sb., o zajištění dalších podmínek BOZP, v platném znění.

Nařízení vlády:

- č. 378/2001 Sb., kterým se stanoví bližší požadavky na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí,
- č. 11/2002., kterým se stanoví vzhled a umístění bezpečnostních značek a zavedení signálů, ve znění nařízení vlády č. 405/2004 Sb.,
- č. 17 – 27/2003 Sb., v platném znění, kterými se provádí zákon č. 22/1997 Sb., o technických požadavcích na výrobky,
- č. 406/2004 Sb., o bližších požadavcích na zajištění bezpečnosti a ochrany zdraví při práci v prostředí s nebezpečím výbuchu,
- č. 101/2005 Sb., o podrobnějších požadavcích na pracoviště a pracovní prostředí,
- č. 362/2005 Sb., o bližších požadavcích na BOZP na pracovištích s nebezpečím pádu z výšky nebo do hloubky.

Vyhlášky:

- č. 50/1978 Sb., o odborné způsobilosti v elektrotechnice,
- č. 20/1979 Sb., kterou se určují vyhrazená elektrická zařízení a stanoví některé podmínky k zajištění jejich bezpečnosti,
- č. 48/1982 Sb., kterou se stanoví základní požadavky k zajištění bezpečnosti práce a technických zařízení, v platném znění,
- č. 268/2009 Sb., o technických požadavcích na stavby,
- č. 499/2006 Sb., o dokumentaci staveb,
- č. 526/2006 Sb., kterou se provádějí některá ustanovení stavebního zákona ve věcech stavebního řádu.

Některé technické normy, které řeší "Požární bezpečnost staveb" Elektrotechnické normy související s popisovanou problematikou a požární bezpečností:

- ČSN 33 2000-4-482 Výběr ochranných opatření podle vnějších vlivů. Ochrana proti požáru v prostorách se zvláštním rizikem nebo nebezpečím,
- ČSN 33 2312 Elektrická zařízení v hořlavých látkách a na nich,
- ČSN 33 2130 ed. 2 Elektrické instalace nízkého napětí – Vnitřní elektrické rozvody,
- ČSN EN 13501-1 Požární klasifikace stavebních výrobků a konstrukcí staveb – Klasifikace podle výsledků zkoušek reakce na oheň,
- ČSN EN 1838 Světlo a osvětlení - Nouzové osvětlení,
- ČSN 33 2000-5-52 Elektrotechnické předpisy Elektrická zařízení Část 5: Výběr a stavba elektrických zařízení – Kapitola 52: Výběr soustav a stavba vedení,
- ČSN 33 2000-7-713 Zařízení jednoúčelová a ve zvláštních objektech – Nábytek,
- ČSN EN 60332-1-2 Požární bezpečnost kabelů – samozhášivé,
- sobory norem požární bezpečnosti kabelů - společné metody zkoušek ČSN EN 50266, ČSN EN 50267, ČSN EN 61034.

Požární bezpečnost staveb v normách třídy 73:

- ČSN 73 0802 Požární bezpečnost staveb. Nevýrobní objekty,
- ČSN 73 0804 Požární bezpečnost staveb. Výrobní objekty,
- ČSN 73 0810 Požární bezpečnost staveb. Společná ustanovení,
- ČSN 73 0831 Požární bezpečnost staveb. Shromažďovací prostory,
- ČSN 73 0833 Požární bezpečnost staveb. Budovy pro bydlení a ubytování,
- ČSN 73 0834 Požární bezpečnost staveb. Změny staveb,
- ČSN 73 0835 Požární bezpečnost staveb. Budovy zdravotnických zařízení,
- ČSN 73 0848 Požární bezpečnost staveb. Kabelové rozvody.

Legislativa poplachových tísňových a zabezpečovacích systémů:

ČSN EN 50131-6 Poplachové systémy-Elektrické zabezpečovací systémy. Část 6: Napájecí zdroje.

Tato evropská norma je specifikací pro napájecí zdroje elektrických zabezpečovacích systémů instalovaných v budovách. Norma také obsahuje požadavky pro napájecí zdroje instalované vně budov ve vztahu ke komponentům instalovaným v budově, které se normálně instalují na vnější plášť budovy.

ČSN EN 50134-7 Poplachové systémy-Systémy přivolání pomoci.

Norma obsahuje doporučení poskytovatelům pro efektivní a účinné řídící a organizační postupy pro instalaci, testování, obsluze a údržbě systému přivolání pomoci včetně technického vybavení a organizování pomoci.

ČSN EN 50136-1-1 Poplachové systémy-Poplachové přenosové systémy a zařízení. Část 1-1: Všeobecné požadavky na poplachové přenosové systémy.

Norma stanovuje základní požadavky na provedení, spolehlivost a charakteristické bezpečnostní znaky poplachových přenosových systémů. Zahrnuje všeobecné požadavky spojení s podmínkou signalizace mezi poplachovým systémem a poplachovým přijímacím centrem. Uvádí terminologii.

ČSN EN 50136-1-2 Poplachové systémy - Poplachové přenosové systémy a zařízení. Část 1-2: Požadavky na systémy využívající vyhrazené poplachové přenosové cesty.

Norma stanovuje požadavky na poplachové přenosové systémy využívající drátová vedení (např.stejnosměrná vedení nebo přenos modulovaného signálu po symetrickým vedení), spojení v hovorovém pásmu nebo datové linky a může obsahovat multiplexery nebo zařízení na zpracování hlášení, linky společné s jinými službami, které zahrnují účastnickou telefonní přípojku ve střežených prostorech, televizní kabelové rozvody nebo energetickou rozvodnou síť.

ČSN EN 50136-1-3 Poplachové systémy-Poplachové přenosové systémy a zařízení. Část 1-3:Požadavky na systémy s digitálními komunikátory využívající veřejnou komutovanou telefonní síť.

Norma stanovuje požadavky na komutovaná spojení , která zajišťují řízený přenos událostí mezi poplachovým systémem a vzdáleným centrem (PCO) pomocí digitalizovaných signálů.

ČSN EN 50136-1-4 Poplachové systémy- Poplachové přenosové systémy a zařízení. Část 1-4: Požadavky na systémy s hlasovými komunikátory využívající veřejnou komutovanou telefonní síť.

Norma stanovuje požadavky na spojení přenášející namluvených hlasových zpráv uložených v paměťovém mediu.

ČSN EN 50136-2-1 Poplachové systémy-Poplachové přenosové systémy a zařízení. Část 2-1: Všeobecné požadavky na poplachová přenosová zařízení.

Norma specifikuje všeobecné požadavky na poplachová přenosová zařízení, která se používají v poplachových přenosových systémech.

ČSN EN 50136-2-2 Poplachové systémy-Poplachové přenosové systémy a zařízení. Část 2-2: Požadavky na zařízení v systémech využívajících vyhrazené přenosové cesty.

Tato norma uvádí dodatečné požadavky na zařízení v systémech využívajících vyhrazené přenosové cesty k požadavkům, které jsou stanoveny v normě ČSN EN 50136-2-1. Přenosový poplachový systém může používat drátové vedení (např. stejnosměrné vedení nebo přenos modulovaného signálu po symetrickém vedení), spojení v hovorovém pásmu nebo datové linky a může obsahovat multiplexery nebo zařízení na zpracování hlášení. Normu lze také použít pro přenosové poplachové systémy, které využívají jako přenosové médium linky společné s jinými službami. Tyto služby zahrnují účastnickou telefonní přípojku ve střežených prostorech k místní ústředně, televizní kabelové rozvody nebo energetickou rozvodnou síť, jsou-li použitelné i pro jiné systémy.

ČSN EN 50136-2-3 Poplachové systémy-Poplachové přenosové systémy a zařízení. Část 2-3: Požadavky na zařízení v systémech s digitálními komunikátory využívající veřejnou komutovanou telefonní síť

Tato norma uvádí dodatečné požadavky na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť k požadavkům, které jsou stanoveny v normě ČSN EN 50136-2-1. Vzdálená centra jsou většinou poplachovými přijímacími centry. Mohou to být však i přenosová zařízení v satelitních stanicích splňující požadavky normy ČSN EN 50136-1-2.

Účelem této normy je stanovit znaky provedení na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť, k zabezpečení jejich způsobilosti pro použití a kompatibility s různými druhy poplachových systémů.

ČSN EN 50136-2-4 Poplachové systémy-Poplachové přenosové systémy a zařízení. Část 2-4: Požadavky na zařízení v systémech s hlasovými komunikátory využívajícími veřejnou komutovanou telefonní síť.

Tato norma uvádí dodatečné požadavky na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť k požadavkům, které jsou stanoveny v normě ČSN EN 50136-2-1. Vzdálená centra jsou většinou poplachovými přijímacími centry. Mohou to být však i přenosová zařízení v satelitních stanicích splňující požadavky normy ČSN EN 50136-1-2.

Účelem této normy je stanovit znaky provedení na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť, k zabezpečení jejich způsobilosti pro použití a kompatibility s různými druhy poplachových systémů.

ČSN EN 50130-5 Poplachové systémy-Zkoušky vnějších vlivů

Tato norma určuje metody zkoušek vlivu prostředí použité pro zkoušení komponentů systému následujících poplachových systémů určených pro použití uvnitř a v okolí budov:

ČSN EN 50133-1 Poplachové systémy-Systémy kontroly vstupů v bezpečnostních aplikacích.
Část 1: Systémové požadavky

Tato norma popisuje všeobecné požadavky na funkčnosti systému kontroly vstupů pro použití v zabezpečovacích aplikacích. Norma také popisuje všeobecné požadavky na komponenty z hlediska prostředí. Pokud některá část systému kontroly vstupů (například rozhraní přístupného místa) tvoří část zabezpečovacího poplachového systému, musí tato část splňovat současně i příslušné požadavky norem na zabezpečovací systémy.

ČSN EN 50133-7 Poplachové systémy-Systémy kontroly vstupů v bezpečnostních aplikacích.

Část 7: Aplikační směrnice

Tato evropská norma byla vydána jako zdroj informací pro správce a zřizovatele systémů kontroly vstupů a jako vodítko pro vyhlašování nabídek a pro montáže a údržbu. Tato norma uvádí pokyny k použití automatizovaných systémů kontroly vstupů a komponentů uvnitř a vně budov na základě norem řady ČSN EN 50133. Zahrnuje návrh systému, instalaci, předávání, provoz a údržbu systémů kontroly vstupů.

ČSN EN 50134-2-1 Poplachové systémy-Systémy přivolání pomoci.

Část 2-1: Aktivační zařízení

Tato norma specifikuje požadavky a zkoušky na ručně spouštěná aktivační zařízení tvořící část systému přivolání pomoci. Tato norma se týká pouze ručně spouštěných aktivačních zařízení, která přenášejí aktivační poplachový signál k místní nebo řídící jednotce po kabelu nebo bezdrátově radiovým přenosem, tj.:

- pevný tlačítkový spínač,
- pevný tahový spínač,
- přenosný tlačítkový spínač,
- přenosný tahový spínač.

Tato norma také poskytuje doporučení na automaticky spouštěná aktivační zařízení. U požadavků a zkoušek použitelných pro tato aktivační zařízení, jsou uvedeny příslušné odkazy na normy CEN/CENELEC pro komponenty elektrické požární signalizace, signalizace úniku plynu a elektrických zabezpečovacích systémů.

Příloha 6 *Struktura testovaných sestav (konfigurace PZTS)*

Sestava1:

Sestava 2:

Sestava 3:

U sestavy 4 nebyl poskytnut souhlas vlastníka systému

Příloha 7 *Bezpečnostní pravidla protokolu SIA 09*

Pro představu je dále popsán způsob zabezpečení protokolu SIA09 proti jednomu z velmi častých způsobů napadení - typu „playback“ – autentizací objektového zařízení.

Část zprávy označenou jako číslo přijímače je možno využít k velmi rychlému a účinnému vyhodnocení pravosti zprávy. Těchto šest znaků (R123456) se využije k identifikaci zdroje zprávy. Tyto pozice jsou určeny k upřesnění přijímače (prefix). Čísla na těchto místech jsou hexadecimální, takže nám poskytují 11 390 625 kombinací. Poskládají-li se tyto kombinace náhodným způsobem do tabulky, mohou se hodnoty z této tabulky vkládat do odesílaných zpráv. Tak se získá další skrytý „klíč“, kterým je pořadí v použité tabulce. Tento údaj znají pouze vysílací a přijímací strana.

Pokud by řazení čísel v takové tabulce chtěl „hacker“ odhalit, trvalo by to při desetiminutovém intervalu mezi kontrolními zprávami řádově 12 let. Při použití šifrování AES a časové značky, nelze úspěšně falešnou zprávu vytvořit. Z pohledu optimálních požadavků na paměť objektových zařízení a relativně malý výkon procesorových jednotek těchto zařízení, lze využít dále popsané řešení.

Vytvoří se tabulka o 4464 položkách. Tabulka se vyplní náhodně vybranými kombinacemi z množiny obsahující více než 11 milionů prvků. Při intervalu mezi kontrolními zprávami 10 minut, postačí taková tabulka objektovému zařízení na jeden měsíc. Při odpojení objektového zařízení z důvodu opravy nebo dlouhotrvající ztráty spojení, vyšle se na tomto místě zpráva o přechodu na jinou tabulku (např.: „RESET02“). To znamená, že se přechází na tabulku č.2 a začínají se používat prvky od pořadí č.1. Každá další tabulka prodlužuje dobu potřebnou pro rozkrytí pořadí čísel tabulky o jeden měsíc.

Z uvedeného formátu vyplývá možnost použití 225 tabulek, což znamená, že nedojde k opakování tabulek dříve než za 18 let. Pro 225 použitých tabulek se vyčerpá pouze 10% prvků z nabízené množiny. Číslo tabulky může pro přijímací stranu znamenat i číslo použitého šifrovacího klíče. Obsah tabulek určuje technické centrum provozovatele PCO. Stejné tabulky může používat větší množství objektových zařízení. Pořadí právě použité hodnoty z tabulky je u každého objektového zařízení jiné.

Efektivního využití s ohledem na velikost použité paměti procesoru se dosáhne tak, že se použije pouze jedna tabulka o velikosti 28 kB a další potřebné tabulky se vytvoří

např. rotací sloupců nebo řádků téže tabulky. Stejná pravidla musí platit i na přijímací straně.

Po dohodě s výrobcem zařízení, lze tabulky vložit do zařízení přímo ve výrobě. Obsah tabulek může změnit servisní technik. Výběr tabulky či její přeskupení je náhodný proces, který je signalizován přijímací straně povelem RESETu.

Pořadí	R[1]	R[2]	R[3]	R[4]	R[5]	R[6]
0001	1	B	2	C	D	E
0002	6	9	1	A	1	2
..						..
4464	F	5	D	4	A	3

Příklad použití hodnoty č. 1 z tabulky ve zprávě SIA-DCS:

003D"SIA-DCS"0001R1B2CDELF#9999[#999A|Nri01^sklad^/CL923^Novák Karel^]

Příloha 8 *Program pro testování Kohonenovy sítě v prostředí Matlab*

```
close all;
clear all;
P = load (’data.dat’);
R=5;
S=5;
Wmin=0.10;
Wmax=0.11;
w =W_min+(Wmax-Wmin) *rand(R*S,2);
w_data = w;
net = nnt2som([0 1;0 1],[R S],w,0.95,0)
net.trainFcn=’trainr’
net.adaptFcn=’trains’
net.inputWeights{1,1}.learnFcn=’learnsom’
net.layers{1}.initFcn=’initwb’
plot(P(1,:),P(2,:),’.g’,’markersize’,25)
hold on
plotsom(net.iw{1,1},net.layers{1}.distances)
hold off
net.trainParam.epochs = 100;
net = train(net,P);
a = sim(net,P);
vystup = vec2ind(a);
```

Příloha 9 *Program pro převod zdrojových dat do Matlab*

```
Attribute VB_Name = "Form1"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = False
Private Sub Command1_Click()
Open "C:\DOC\Disertačka\DATA\zv_export\upraveny_vystup\poplach_vypnuti.txt" For Input As #1
Open "C:\DOC\Disertačka\DATA\zv_export\upraveny_vystup\poplach_vypnuti2.txt" For Output As #2
Do While Not EOF(1)
Input #1, a$
b$ = Trim(a$)
If Len(b$) = 10 Then Print #2, b$
Loop
Close
End Sub
Private Sub Command2_Click()
Open "C:\DOC\Disertačka\DATA\zv_export\upraveny_vystup\dlouhy_log2.txt" For Input As #1
Open "C:\DOC\Disertačka\DATA\zv_export\upraveny_vystup\dlouhy_log3.txt" For Output As #2
Do While Not EOF(1)
Input #1, a$
b$ = Trim(a$)
If Len(b$) = 10 Then Print #2, Left(b$, 6)
Loop
Close
End Sub
```