Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Analýza možností nasazení systému Fibaro jako potenciálně certifikované PZTS

diplomová práce

Vedoucí diplomové práce:

Ing. Zdeněk Votruba, Ph.D.

Autor diplomové práce:

Bc. Jan Kadeřábek

Praha 2016

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jan Kadeřábek

Informační a řídící technika v agropotravinářském komplexu

Název práce

Analýza možností nasazení systému Fibaro jako potenciálně certifikované PZTS

Název anglicky

Analysis of options to deploy the system as potentially Fibaro certified I&HS

Cíle práce

Analyzovat současné integrační nástroje, jejich posouzení a zhodnocení. Rozbor systému Fibaro pro integraci menších a středních objektů. Ověření funkčnosti a definování provozních parametrů. Doporučení pro další provoz.

Metodika

1. Popis současného stavu integračních nástrojů, způsoby integrace v rámci IB.
2. Normy a legislativa vztahující se k integraci poplachových systémů v IB
3. Popis a možnosti systému Fibaro
4. Praktická realizace v typickém objektu
5. Ověření reálné funkce a parametry provozu
6. Zpracování a vyhodnocení výsledků
7. Doporučení a finanční zhodnocení

Doporučený rozsah práce

50 – 60 stran textu včetně příloh

Klíčová slova

integrace, PZTS, inteligentní budova, Fibaro

Doporučené zdroje informací

BEBČÁK, P.: Požárně bezpečnostní zařízení, 2004, SPBI, 226 s. ISBN 80-86634-34-5.
časopisy Automa, Elektro a Security Magazín
firemní literatura a manuály
HEŘMAN, J., TRINKEWITZ, Z., et al.: Elektrotechnické a telekomunikační instalace, 2006, Verlag Dashofer, ISBN 80-86897-06-0.
KOCÁBEK, P.; KONÍČEK, T.: Bezpečné bydlení. ERA 2003, Brno
KŘEČEK, S.: Příručka zabezpečovací techniky. 2002, Critetus, 313 s. ISBN 80-902938-2-4.
související normy a zákony, především ČSN CLC/TS 50131:2007, ČSN EN 50132, ČSN EN 50134, ČSN EN 50133, ČSN EN 50136, ČSN CLC/TS 50 398:2009, zákon č. 101/2000 Sb., zákon č. 67/2001 Sb. včetně především vyhlášky č. 246/2001 Sb

---

Předběžný termín obhajoby

2015/16 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 20. 1. 2015

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 4. 2015

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 28. 03. 2016

Prohlášení:

Prohlašuji, že jsem diplomovou práci na téma: „Analýza možností nasazení systému Fibaro jako potenciálně certifikované PZTS“ vypracoval samostatně a použil pouze pramenů, které cituji a uvádím v seznamu použité literatury.

V Příbrami dne 31. března 2016

……

Bc. Jan Kadeřábek

Poděkování:

Rád bych poděkoval v první řadě panu Ing. Zdeňku Votrubovi, Ph.D. za obětavý přístup a velkou pomoc s prací. Dále pak celé společnosti Yatun s.r.o. za propůjčení všech zařízení k účelům této práce, především pak Jakubovi Ježkovi za vstřícnou a profesionální pomoc z pozice technické podpory této společnosti. V neposlední řadě děkuji za pomoc své přítelkyni a rodině.

V Příbrami dne 31. března 2016

……

Bc. Jan Kadeřábek

Abstrakt:

Cílem této práce je nastínit čtenáři problematiku integrace poplachových zabezpečovacích a tísňových systémů v rámci projektu „inteligentní budovy“, přinést typové rozdělení možných integračních řešení s uvedením několika příkladných systémů a stanovit kritické aspekty při navrhování takového projektu. Součástí této diplomové práce je uvedení normativní a legislativní literatury vztahující se k problematice. Dále je proveden podrobný rozbor zapůjčeného systému domácí automatizace Fibaro a ověřena jeho praktická funkce, tedy užití toho systému jako PTZS, sestavením realizačního modelu a porovnáním tohoto modelu s alternativními modely z hlediska praktické, legislativní a finanční stránky. Dále jsou za pomoci sestaveného testovacího zařízení provedeny funkční zkoušky. Vyhodnocuje se schopnost řídící jednotky Fibaro správně reagovat na uměle vyvolané detekční stavy přenášené bezdrátově po síti Z-Wave. Na základě porovnání realizačních modelů a výsledků funkčních zkoušek jsou stanoveny závěry a předána doporučení.

Klíčová slova: integrace, PZTS, inteligentní budova, Fibaro

Abstract:

The aim of this thesis is to delineate the issue of Intrusion and Hold-up Alarm System integration in terms of the project „intelligent building“, bring a clasification of the potential integration solutions with induction of some exemplary systems and define crticial aspects during desining projects. Part of this thesis is an introduction of normative and legislative literature related to this issue. Further there is detailed analysis of home automatization system Fibaro and verification of practical function therefore utilization this system as an I&HAS by the assembling of implementation model and comparising this model with alternatives models from practical, legislative and financially aspects. Functional examinations are executed by the compiled testing device. Then is evaluated the ability of controll unit Fibaro to react correctly on artificially induced detecting states transmitted wirelessly over Z-Wave network. Finally there are established conclusions based on comparison of implementation models and the results of functional examinations.

Keywords: integration, I&HAS, intelligent building, Fibaro

Obsah

1 Úvod

Automatizační systémy jsou již dnes několik let běžně užívány nejen k jejich primárnímu účelu, tedy pro průmysl, vědní obory a lékařství, ale staly se již běžně také součástí technologického vybavení soukromých budov. Takovými systémy jsou například technologie řízení klimatických podmínek v objektu (HVAC), zabezpečovací a protipožární systémy, systémy pro řízení osvětlení, systémy měření spotřeby a mnohé další. Lidé již berou jako samozřejmost využívat tyto technologie, které jim přináší bezpečí, komfort a v neposlední řadě také finanční úspory, které velice blízko souvisejí s ekologičností provozu objektu. S větším počtem technologií v objektu se stává jeho správa nepřehledná. Logickou potřebou uživatelů i projektantů nových staveb je provázání těchto technologií takovým způsobem, aby na sebe dokázaly reagovat, komunikovat spolu a mohly být následně co nejkomplexněji pomocí centralizované správy nebo samočinně využívány ve prospěch člověka. Vyvíjejí se **sběrnice** sloužící k propojení jednotlivých systémů, vytvářejí se **protokoly** stanovující pravidla datového přenosu, formulují se **standardy** určené k rozšiřování služeb pomocí komunikace po datových sítích, stanovují se **normy** pro předepsání požadovaných vlastností systémů k zajištění bezpečnosti atd. Problematice integrace bude věnován rozbor v první části práce, kde bude nastíněno možné využití těchto technologií pro projekt „inteligentní budovy“.

S postupem času se integrované technologie stále vyvíjejí a přitom zlevňují natolik, že se již běžně používají i v obytných objektech. Vzniká velké množství výrobců, kteří se zaměřují na vývoj těchto systémů domácí automatizace, často pak komerčně prodávané jako systémy „chytré domácnosti“ či „inteligentní budovy“. Jedním z takových systémů je systém polského výrobce Fibaro Group S. A. Fibaro, kterému bude věnován detailní rozbor v další části práce. Pro účely této práce je tento systém propůjčen jeho českým distributorem Yatun s.r.o.

Jednou ze stěžejních technologií využívaných obecně v budovách je poplachový zabezpečovací a tísňový systém (PZTS). Ten bývá instalován za účelem ochrany majetku a zdraví, navození pozitivního psychologického pocitu nebo také z důvodu potřeby splnění podmínek pro uzavření pojistné smlouvy pro daný objekt. Propůjčený systém Fibaro ve svém principu přináší možnost sestavení PTZS ze svých komponent, avšak dosud bez náležité certifikace vázané k těmto systémům. Je cílem sestavit PTZS z komponent systému Fibaro a porovnat ho s obvyklým PTZS s ohledem na cenu celé realizace. Dalším cílem je otestovat spolehlivost bezdrátové komunikace sítě Z-Wave, po které systém Fibaro realizuje svoji komunikaci. Dle těchto výsledků bude systém Fibaro zhodnocen pro případnou vhodnost k iniciaci certifikačního procesu.[1,3,4,15]

2 Popis současného stavu integračních nástrojů, způsoby integrace v rámci IB

Prve zde bude rozebrána terminologie pojmů „inteligentní budovy“ a integrace, poté popsán postup návrhu takových systémů a uvedeny některé příklady integračních řešení.

2.1 Historie inteligentních budov

O prvním „inteligentním domě“ bylo zmíněno již v 60. letech 20. století v Japonsku, kdy byl prezentován projekt budovy řízené centrální jednotkou podobnou dnešnímu PLC. Primárním aspektem k uplatnění takové technologie bylo snížení spotřeby elektrické energie při vytápění budov, osvětlení, klimatizaci a to za celkového zvýšení uživatelského komfortu.

O tento projekt se nejdříve nejevil zájem, avšak po energetické krizi v 70. letech, díky uvědomění si všeobecně nadměrného plýtvání energií v budovách, začala řada především německých výrobců nabízet kvalitnější otopné a další systémy, nově koncipované jako navzájem spolupracující elektrické instalace.

Díky rozvoji konstrukcí a materiálu začali vznikat v 80. letech první nízkoenergetické domy. Paralelně s nízkoenergetickými domy se dále rozvíjely technologie měření spotřeby energií, jejich vyhodnocování a zpětného řízení - automatizovaného systému. Tyto technologie vycházely z první generace osobních počítačů. Vysoké investiční náklady systémů však nedovolily nasazení do běžné praxe v řadových domech a menších budovách, ale pouze do objektů, ve kterých bylo možno dosáhnout vysokých energetických úspor a zajistit tak zpětnou úsporu nákladů z provozu budov.

Teprve vývoj mikroprocesorové techniky umožnil masivní rozšíření technologií, které se v dnešní době využívají v tzv. „inteligentních budovách“. Dnes již běžně bývají do objektů paralelně instalovány informační, bezpečnostní i technologické systémy. Ze strany uživatele je snahou tyto oborově odlišné systémy propojovat a umožnit jim centralizovanou správu, pomocí níž by bylo možné automatizovaně či vnějšími zásahy řídit veškeré napojené technologie v objektu (budově). [1,15]

2.2 Inteligentní budova

Pojem inteligentní budova je již několik let a stále častěji skloňovaným termínem v odborných kruzích architektů, projektantů, stavebních firem, elektroinstalačních firem nebo pracovníků tzv. facility managementu, ale také v kruzích běžných spotřebitelů, kteří se touto problematikou zabývají především z důvodu jak učinit život ve svých domácnostech více bezpečný, komfortní, ekonomičtější nebo ekologičtější.

Z architektonického hlediska se jedná o budovu, která se nikterak nemusí lišit od klasických budov, avšak myslí dopředu svým konstrukčním řešením na maximální energetickou úspornost a umožňuje integraci potřebné techniky. Každá taková budova je postavena za použití jistých materiálů a stejně jako na každé budově lze i na té „inteligentní“ rozeznat šest základních konstrukčních elementů - základy, svislé nosné konstrukce, vodorovné nosné konstrukce, schodiště, komunikační prostory a střechu. Energetické úspory lze dosáhnout kromě instalované techniky právě samotným umístěním budovy, její orientací, použitými materiály či zvolenou stavební technologií.

Co se týče technického vybavení, již běžně bývají souběžně instalovány v budovách rozsáhlé **technologické systémy** (klimatizace, větrání, topení, výtahy), **bezpečnostní systémy** (poplachové systémy, tísňové systémy, kamerové systémy, přístupové systémy, protipožární systémy, systémy protivýbuchové, systémy proti zaplavení a další) a v neposlední řadě **informační systémy** (počítačové sítě, telefonní sítě, rozvody zvuku a obrazu). Takový výčet technologií však stále z těchto dobře technicky vybavených budov nečiní budovy „inteligentní“.

Problémem je, že termín „inteligentní budova“ je používán velmi volně. Využívá se spíše více jako marketingový pojem, už z principu, že jakékoliv zařízení nebo systém, který je slovně prezentován s přívlastkem „inteligentní“, nabývá v komerční sféře prodejní hodnoty**.**

Pro pojem inteligentní budova (IB) bylo vytvořeno několik definic, například:

„*IB 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.*“

Zdroj: [European Smart House Standards Group]

„*IB 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.*“

Zdroj: [European Intelligent Building Group]

„*IB je taková, jejíž integrované systémy se „umí učit“ a přizpůsobovat vnitřní prostředí pro požadavky konkrétního uživatele.*“

Zdroj: [http://www.inteligentni-budovy.cz/]

„*IB je vybavena komunikačními službami s automatizovaným provozem a je vhodná pro inteligentní aktivity*.“

Zdroj: [Japan Intelligent Building Institut]

„*IB je budovou plně pronajatou*.“

Zdroj: [http://www.inteligentni-budovy.cz/]

Definic IB je daleko víc a každá na problém nahlíží trochu z jiného úhlu pohledu. Například první dvě zmíněné definice se vzhledem ke komplexnosti pojmenování blíží tomu, co by ve skutečnosti termín IB měl znamenat. Neexistuje standard, který by přesně normou vymezil co pojem „inteligentní budova“ znamená a jak ho používat. To nahrává prodejcům systémů, kteří jsou schopni za projekt IB označit i naprosto triviální instalaci, v níž jsou například obsaženy systémy PZTS, ACC a CCTV nikterak inteligentně nepropojené a na sobě jen minimálně závislé. Skutečností je, že **termín „inteligentní budova/inteligentní instalace“ bude skutečně pravdivý až tehdy, kdy takto pojatá kompletní instalace bude samostatně rozhodovat - „myslet“** tzn., bude bezprostředně reagovat na chování, jednání a pocity uživatelů objektu a bude zpětně ovlivňovat původní optimalizační algoritmy tak, aby do systému byly zahrnuty individuální podmínky konkrétní stavby. Teprve poté bude ve výsledku produkován „učící se systém“ – „inteligentní systém/instalace/budova“. [1,3,15]

Optimální propojení informačních systémů v moderní tzv. „inteligentní budově“:

Stavba s optimálními architektonickými vlastnostmi (pozice dle světových stran, rozměry, konstrukce budovy, stavební materiál atd.) s přístupem ke všem potřebným energetickým zdrojům, zdrojům pitné vody s odvodem kanalizace a v neposlední řadě dnes již nepostradatelným zdrojům z informační sítě. Budova je vybavena technologiemi PZTS, CCTV, ACC, EPS, HVAC, stínícími technikou, multimédii, streamovými přenosy hlasu a videa, rozpoznáváním SPZ a dalšími technologiemi dle koncepce. Tyto technologie jsou propojeny do jednoho řídicího systému umožňujícího jednotlivé subsystémy monitorovat, ovlivňovat a řídit jako jediný celek z jednoho místa či vzdáleně z několika kvalitně zabezpečených zařízení. Infrastruktura sítě je zálohována sítí redundantní (např. metalická síť je zálohována sítí bezdrátovou). O řízení budovy se pak starají samotní obyvatelé domácnosti, odpovědný proškolený personál či najatá společnost provádějící facility management v podobě outsourcingu, samozřejmě dle koncepce.

S větší obsáhlostí technologických systémů v budovách se stává technická situace složitější. Snaha uživatelů o propojování systémů, centralizaci správy a umožnění vzájemného ovlivňování systémů je přirozeným požadavkem. Uveďme si několik vzorových situací, které by mohly být přínosné díky centralizaci a možnému vzájemnému ovlivňování systémů:

- při zastřežení dojde k aktivaci detektorů, simulaci přítomnosti, zamčení všech dveří, stažení rolet, žaluzií, vypnutí el. proudu, uzavření plynu,
- PIR čidla zabezpečovacího systému (PTZS) mohou zjistit teplotní výkyv indikující vznik drobného požáru i tam, kde protipožární systém nemá své detektory,
- možnost detekce přítomnost kysličníků uhlíku v klimatizačním systému dříve, než tuto skutečnost zjistí detektory kouře v protipožárním systému,
- získání kontroly o pohybu osob v budově pomocí přístupových systémů s návazností na mzdový systém,
- v interakci s citlivým návrhem přístup, ovládání a pobyt i osobám se sníženou pohyblivostí (např. ovládání zámků či vypínačů hlasem),
- při narušení objektu může být nastavena vazba na kamerový systém, který odešle snímek nebo videosekvenci z kamery v narušené zóně na tablet nebo telefon,
- infra kamerou lze dohlédnout do neosvětlených míst např. garáží a monitorovat prostor jinými systémy označený za podezřelý. [1,15]

2.3 Integrace systémů IB

V rámci inteligentní budovy je nezbytně nutná a podstatná vzájemná komunikační vazba mezi jednotlivými systémy. Tato vazba se realizuje pomocí integrace.

Pod pojmem integrace se všeobecně rozumí proces spojování různých (heterogenních) subsystémů v jeden fungující celek - v našem případě inteligentní budovu. Pod těmito subsystémy si můžeme představit výčet softwarových a hardwarových komponent (technických prostředků) tvořící budoucí inteligentní budovu (společně s jejími dalšími náležitostmi – architektonická realizace). Integrace je postup s cílem synergie subsystémů, tedy zvyšování účinnosti (stávajících či nových) subsystémů. Tento postup provádí tzv. systémový integrátor. **Je cílem právě systémového integrátora jednotlivé subsystémy propojit v jeden požadovaný funkční celek splňující všechna relevantní nařízení a předpisy.** Je však třeba zdůraznit, že integrace by neměla být chápána jako produkt, ale spíše jako dodávka služeb (konzultace, bezpečnostní posouzení, projektování, implementace, instalace, školení a servis).

Kvalitně řešená integrace pak uživatelům budovy přináší několik cíleně pozitivních vlastností:

- optimalizace řízení (finanční návratnost investice),
- sdružení ovládacích prvků,
- vysoký uživatelský komfort,
- zvýšená bezpečnost a odolnost (řešení krizových situací).

Ač je centralizace (integrace) poslední desítky let stále více rozvíjejícím se trendem, v mnoha projektech nebývají výsledné instalace nikterak uspokojující. Integrace je v řadě případů sice technicky možná, ovšem z pohledu platných norem, a z toho vyplývající spolehlivosti a bezpečnosti, značně problematická. Poté záleží na systémovém integrátorovi, jak se s konkrétním projektem dokáže vypořádat.

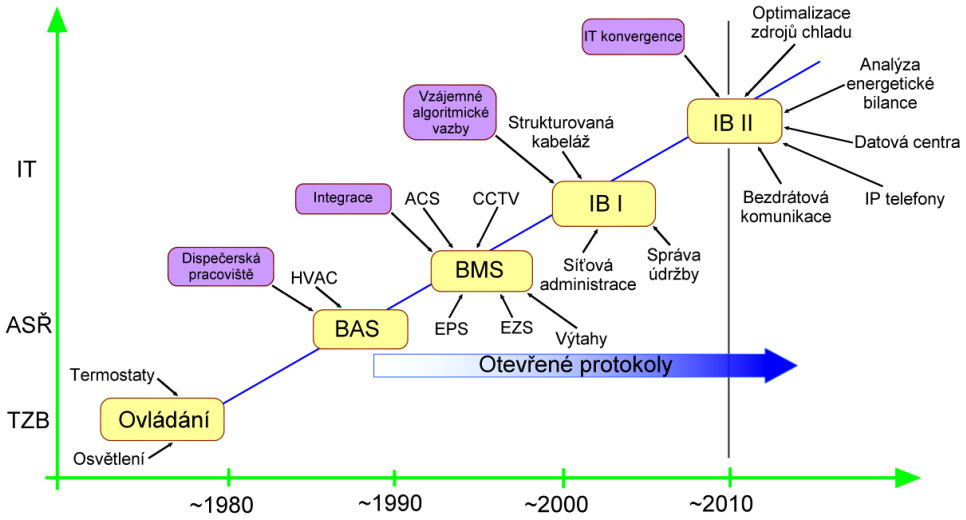
Prioritami a základní charakteristikou kvalitního integračního systému, nejen poplachových systémů, je především:

- spolehlivost přenosu dat,
- bezpečnost přenášených dat,
- vyloučení vzájemného negativního ovlivnění integrovaných systémů,
- univerzálnost řešení,
- možnost snadné konfigurace a modifikace,
- ověřitelnost přenesených dat (časové známky, logy atd.), [1,16,17]

2.4 Vývoj a bezpečnost integračních systémů

Při vývoji technologií inteligentních budov se v průběhu času stále více projevuje konvergence jednotlivých technologií, což demonstruje graf níže. Je z něj patrné, že se v současné době nacházíme v období, kdy se pro integraci využívají především principy komunikace skrze IT technologie.

Obr. 1 - Konvergence technologií integračních systémů; Zdroj: [14]



V budoucnu se pravděpodobně bude projevovat snaha výrobců i prodejců o zahrnutí IT technologií do poplachových a tísňových systémů (PTZS). 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. Přesto již v dnešní době několik společností realizuje takto integrované systémy, byť za cenu toho, že mlčky ignorují platné normy a doporučení pojišťoven.

Pokud odhlédneme od problematiky norem a zaměříme se na problematiku komunikace, je způsob integrace bezpečnostních systémů prostřednictvím počítačových sítí (TCP/IP nad sítí Ethernet) a částečně i integrace s pomocí automatizačních systémů chybnou. Kvůli diskutabilní spolehlivosti jednotlivých prvků (především serverů a PLC) v takto navržených systémech, s sebou nese tento způsob integrace značná rizika spolehlivosti celého systému. Ta jsou řádově vyšší než u nikterak neintegrovaného modulárního systému. Pro opodstatnění tohoto tvrzení uvádím ke kategorii integrace s využitím počítačových sítí všeobecný **problém se zahlcováním sítí**, u integrace s pomocí automatizační techniky pak šest let aktuální **problém s virem Stuxnet** (červ schopný přeprogramovávat PLC). [1,7]

2.5 Rozdělení typů IB

Laicky se termín „inteligentní budova“ používá plošně pro všechny typy staveb. V podstatě jde ale pouze o názvosloví užívané v marketingu. Můžeme se setkat s pojmem „inteligentní dům“, který se využívá pro objekty typu rodinného domu nebo s pojmem „inteligentní byt“, který je určen pro objekty typu bytové jednotky. Obecný termín „inteligentní budova“ je z technického pohledu vhodné rozlišovat:

dle užití:

- komerční objekty,
- technologické objekty,
- obytné objekty,

dle velikosti:

- velké objekty,
- středně velké objekty,
- malé objekty,

dle míry integrace:

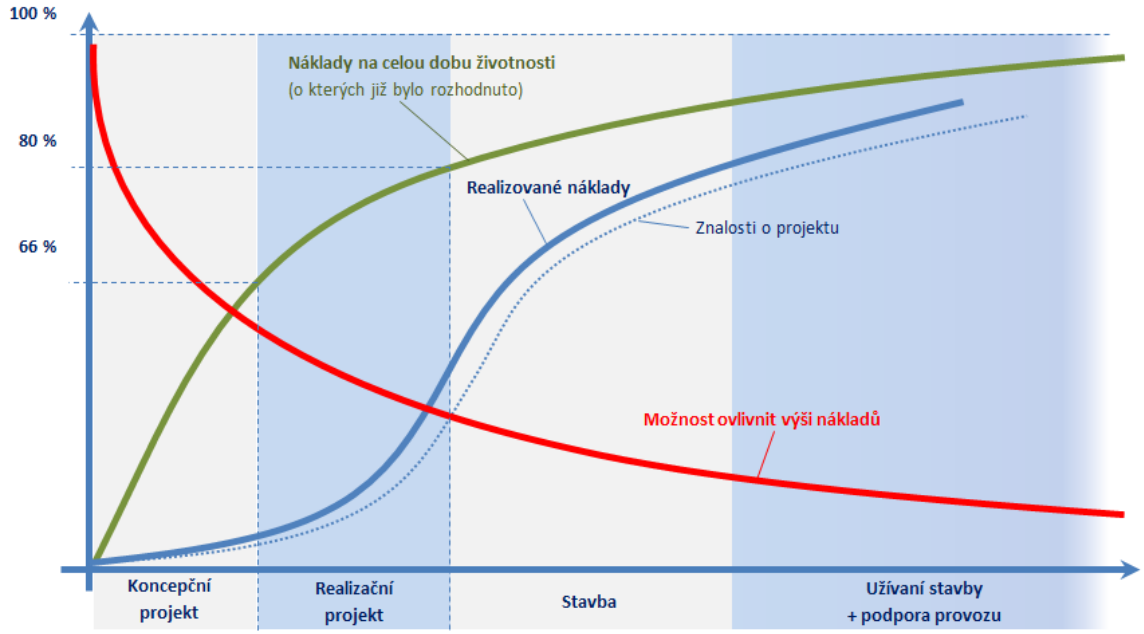
- komerční objekty (základní úroveň interakce – tlačítkové ovladače),
- rezidenční objekty (vyšší úroveň interakce – grafický interface),
- městské systémy (integrace integrovaných budov).

2.6 Kritéria návrhu projektu IB

Návrh projektu IB je velice složitý proces, předpokládající uplatnění širokého spektra znalostí ze vztahujících se technických oborů. Do projektu je třeba zahrnout účastníky celého díla (architekt, projektant, specialista řízení projektu, investor, budoucí majitel či provozovatel) a zajistit jim co nejprospěšnější diskuzi vedoucí ke spolupráci na naplnění všech cílů, a to jak v době návrhu, tak především během samotné realizace projektu IB.

Podstatným aspektem je časové hledisko momentu, kdy je o projektu IB uvažováno. Obecně platí, že je vhodné jeho začlenění do počátečních fází projektu budoucí nové budovy. To zvláště z důvodu do té doby možného přizpůsobení architektonické realizace projektované budovy podmínkám IB. Při úvaze o začlenění projektu IB v pozdějších fázích stavebního projektování se možnost ovlivnit „stupeň inteligence“ budoucí budovy stává čím dál více problematickou kvůli nákladnému zásahu a technickým obstrukcím do již uzavřeného koncepčního či realizačního projektu. To přehledně znázorňuje graf (viz níže).

Obr. 2 - Časové hledisko implementace "inteligentních" technologií do projektu; Zdroj: [upraveno dle 15]



Teoreticky může být projekt IB implementován do libovolného již existujícího objektu. Zde je však třeba důsledně zvážit vhodnost konkrétní implementace, a to především z pohledu ekonomické rentability, přijatelnosti stavebně-technických úprav a možnosti docílení předpokládaného „stupně inteligence“ budovy. **Systémem, který by mohl být přijatelnější, co se týče možnosti pozdější implementace, je díky bezdrátové koncepci právě testovaný systém Fibaro** (detailněji viz níže).

Projekt IB nezahrnuje pouze vybavení integrovanými technologiemi. Musíme zde připočíst i parametry architektonické realizace budovy samotné. Důrazně je třeba zmínit, že integrační systém by neměl být projektován pouze dle prvoplánových požadavků realizace, ale i s ohledem na běžné a krizové podmínky budoucího provozu. [1,15]

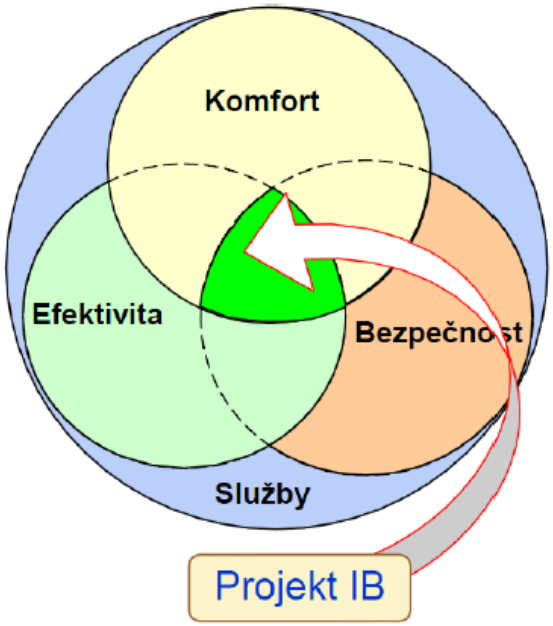
Při návrhu integrace je vhodné vycházet z následujícího modelu postupu:

Určení parametrů systémů (performačních indikátorů) -> zvážení vhodnosti objektu pro případnou integraci -> určení způsobu integrace (s ohledem na zachování nezbytných provozních, technologických a především bezpečnostních podmínek).

Při hledání performačních indikátorů, a také při následném určování technického způsobu integrace, je vhodné hodnotit technologie budoucí integrace podle těchto třech základních kritérií:

- kritérium komfortu v objektu,
- kritérium energetické efektivnosti (ekologičnosti) provozu objektu,
- kritérium bezpečnosti objektu.

Obr. 3 - Vhodná kritéria při návrhu performačních indikátorů; Zdroj [16]



Váhy kritérií budou ohodnocovány odlišně v závislosti na typu užití objektu (komerční, technologický či obytný). Požadavek na kvalitní inteligentní budovu by se měl nalézat v prostoru, kde dochází k průniku těchto kritérií. [1]

2.7 Možnosti integrace poplachových systémů v IB

Integrace technologických a poplachových aplikací je ve většině případů fyzicky řešena třemi základními technickými principy:

- **pomocí výstupů PGM** – Přenos relativně omezeného množství stavových údajů z ústředny zabezpečovacího systému. Z hlediska legislativních a normativních předpisů se jedná se o bezproblémový způsob integrace. Tento typ integrace je vhodný především pro malé objekty.
- **pomocí datové sběrnice** – Je možné prakticky libovolné ovlivňování systémů nad možnostmi konkrétní sběrnice. Jejich komunikace je řízena za pomocí protokolu. Tento způsob integrace je poměrně častý, většinou se však neshoduje s legislativními předpisy a to především normou řady ČSN 50 xxx (podrobněji viz níže). Je vhodný pro středně velké a velké objekty.
- **pomocí bezdrátového přenosu** – Budoucnost technologií „internetu věcí“ a cloudových systémů. Zatím spíše teoretická myšlenka, téměř splnitelná technickou stránkou věci, avšak prozatím velice problematická z hlediska legislativy. Bude zde zapotřebí brát zřetel na zabezpečení přenosu (k tomu směřuje například standart SIA DC-09, ten je však určen pro přenos objemnějších dat).

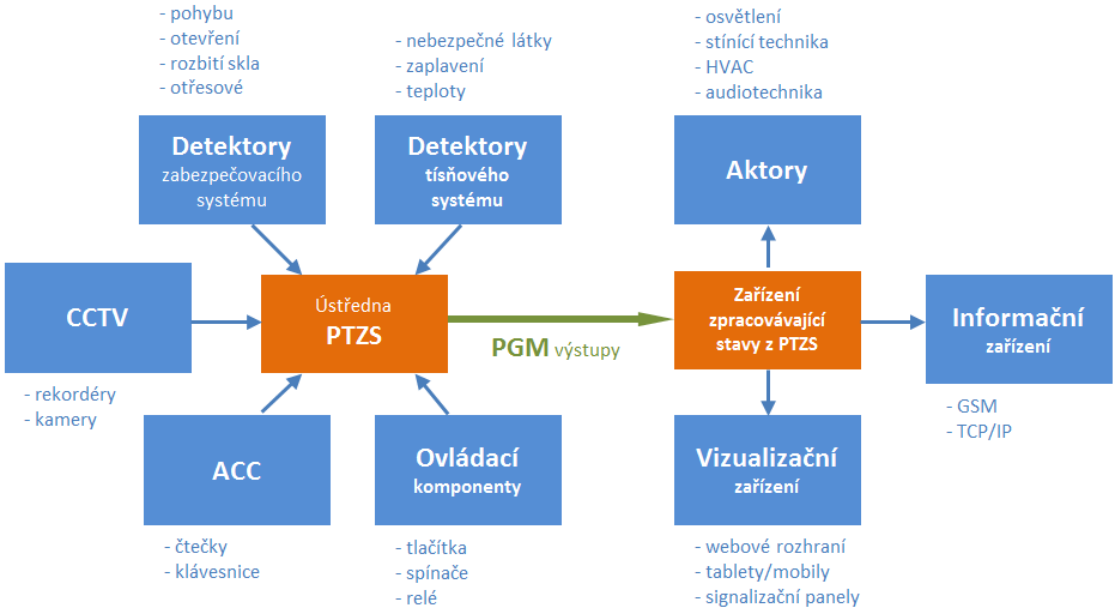
Dále je relevantní rozdělení integrovaných systémů dle topologie:

- centralizované systémy,
- decentralizované systémy,
- cloudové systémy. [1,5]

2.8 Integrace pomocí výstupů PGM

Jedná se o vzájemné propojení systémů prostřednictvím jejich výstupů ze zabezpečovací ústředny (PGM) a vstupů ostatních systémů. Ke kladům patří možnost v systému použít komponenty bez ohledu na výrobce a komunikační protokoly. Zjednodušeně se dá říct, že může být použito každé zařízení, které využívá logiky přepínání mezi otevřeným a uzavřeným okruhem. Je prakticky ideálním a levným řešením v případě požití cca max. 15 přenášených stavů (z aktorů/sensorů). Při větším množství ovšem výrazně stoupá složitost zapojení a logika celého systému. Provedení této integrace přináší vysokou spolehlivost i životnost a prakticky 100 % odolnost vůči vzájemnému negativnímu ovlivňování systémů mezi sebou.

Obr. 4 - Blokové schéma integrace pomocí výstupů PGM; Zdroj: [upraveno dle 17]



Z blokového schématu viz výše je zřejmé, že takovýto typ provedené integrace má pouze jednosměrný tok dat. To znamená, že zařízení zpracovávající stavy PGM výstupů (zařízení čtecí binární stavy + PLC/PC/sběrnice) nemůže zpětně ovlivňovat PTZS. Teoreticky je možné při větším rozlišení komunikace (navýšením počtu PGM výstupů ústředny) konkretizovat změnu stavu na každém vstupním prvku. Toto zapojení nemá problém s reálným řešením z hlediska norem. [1,5]

Tab. 1 - Stručné zhodnocení integrace pomocí výstupů PGM; Zdroj: [1]

Výhody:	Nevýhody:
• cena • jednoduchost • spolehlivost • univerzálnost	• pouze pro menší systémy • problematická rozšiřitelnost • nižší uživatelský komfort

2.9 Centralizované systémy

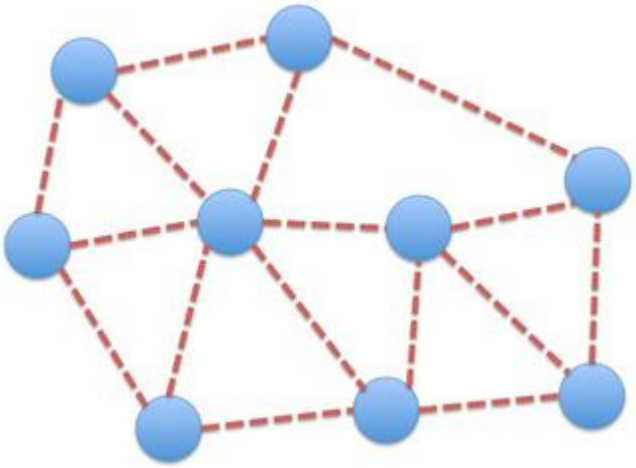
Jedná se o typ topologie systému s jedním řídícím uzlem v rámci celé sítě - centrální jednotkou. Ta je propojená pomocí sběrnice s ostatními prvky sítě. Informace ze senzorů jsou posílány do centrální jednotky, kde jsou zpracovány a výsledné informace směřují do aktorů. Výhodou tohoto způsobu je nízká pořizovací cena senzorů a aktorů a především jednoduchost implementace informačního systému. Nevýhodou je naopak složitější funkčnost centrální jednotky, nutnost propojení centrální jednotky se všemi ostatními prvky systému a celková nižší spolehlivost systému daná spolehlivostí centrální jednotky. [1,10]

2.9.1 Fibaro

Tento systém je předmětem praktické části této práce a bude mu věnován podrobnější rozbor v dalších kapitolách, nejdříve však ve zkratce o topologii tohoto systému:

Systém automatizace domácnosti/budov Fibaro je systém využívající technologii bezdrátového rádiového přenosu v bezlicenčním pásmu za pomocí protokolu Z-Wave. Komunikace v této síti probíhá pomocí topologie typu „mash“. Systém využívá funkci tzv. retranslace (provázání a přesměrovávání komunikace modulů mezi sebou a z toho plynoucí navýšení dosahu celé sítě) a funkci tzv. asociace (vytvoření přímé vazby mezi moduly bez účasti řídicí jednotky).

Obr. 5 - Topologie typu „mash“; Zdroj: [18]

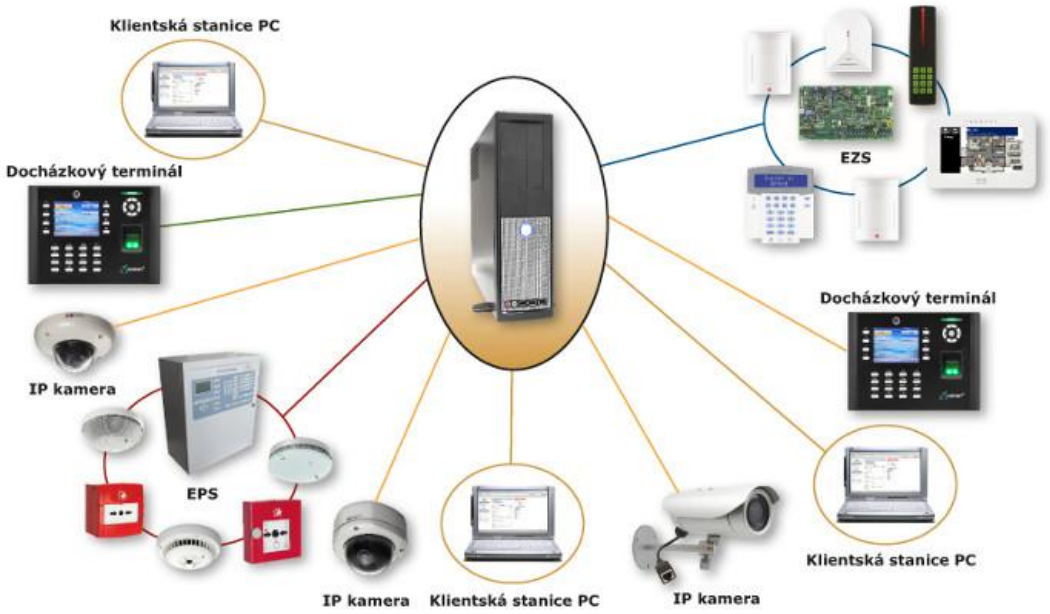


Přes možnost využití asociativního ovládání patří systém Fibaro do kategorie centralizovaných systémů, jelikož systém ke své plné funkci využívá jako řídící člen jednu řídící jednotku, která slouží jako centrální bod tohoto systému. Ta zpracovává převážnou většinu složitějších funkcí, jako jsou scény, ovládání ze vzdáleného zařízení, management spotřeby energií, zabezpečovací systém (podstatný pro tuto práci) atd. [24,28]

2.9.2 *Var-net Integral*

Var-net Iintegral je systém pro centrální sledování, správu a vyhodnocování elektronických systémů budov. Je navržen jako ucelené řešení složené ze vzájemně provázaných modulů. Var-net Iintegral využívá architekturu typu klient-server a pracuje nad TCP/IP protokolem. Jako interface zde slouží webový klient. Je nutné, aby na serveru, kde bude instalováno integrační řešení Var-net Iintegral, byl přítomen OS verze alespoň Windows Web Server 2008 SP1. Do sítě celého systému výrobce uvádí možné zařazení zabezpečovací ústředny DIGIPLEX EVO, kamerových systémů IP kamery ACTi, IP kamery Canon nebo DVR Micro Digital, elektronické požární signalizace JOB detectomat a docházkové a přístupové terminály VAR-NET. Je určen pro malé a středně velké objekty. [19]

Obr. 6 - Schéma realizace centralizovaného systému Var-net Integral; Zdroj: [19]



Tab. 2 - Stručné zhodnocení integračního řešení Var-net Integral; Zdroj: [vlastní]

Výhody:	Nevýhody:
• dostupnost v ČR pro malé a středně velké objekty • cena	• serverové řešení • omezený výběr subsystémů integrace

2.9.3 Tecomat Foxtrot

Tecomat Foxtrot (CP – 10xx) je modulární PLC ze skupiny Tecomat programovatelný v prostředí Mosaic (LD, FBD, ST a IL). Umožňuje připojit až 288 jednotek na sběrnici CIB. Je kompatibilní s normou IEC 61131-3. Jednodušší alternativou k této centrální jednotce je jednotka CU2-01M, s možným rozsahem až 192 jednotek na sběrnici CIB, parametrizovatelná pomocí programu IDM.

Sběrnice CIB je dvouvodičová modulární sběrnice s libovolným větvením (vyjma topologie kruhu). Napájecí napětí a data jsou vedena společně po těchto dvou vodičích. **Komunikace probíhá v modelu master−slave. Celý systém je pak řízen centrální jednotkou na bázi PLC (Tecomat Foxtrot nebo CU2-01M), proto je zařazena do centralizovaných systémů**. Každá jednotka má svoji vlastní unikátní šestnáctibitovou adresu vyjádřenou čtyřmi hexadecimálními číslicemi, která je uvedena na krytu každé jednotky. Master lze umístit až do vzdálenosti 300 m od řídicí jednotky při připojení metalickým kabelem nebo až 1,7 km při připojení optickým kabelem, a to bez snížení rychlosti odezvy (do 150 ms). Garantovaná přenosová rychlost sběrnice CIB je 19,2 kb/s. V případě potřeby více větví je možno síť rozšířit pomocí externích master modulů. Sběrnice je napájena napětím 24 V DC (doporučováno 27 V DC). Pro schopnost vykonávat zabezpečovací a komunikační funkce v případě výpadku sítě je možné připojení akumulátorů 2 × 12 V. Obsahuje v sobě prostředky pro správu skrze vlastní webserver. Řešení je určeno pro středně velké a velké objekty. [9]

Tab. 3 - Stručné zhodnocení integračního řešení Tecomat Foxtrot; Zdroj: [1]

Výhody:	Nevýhody:
• rozšířenost v ČR a kompatibilita s jinými řešeními • proprietární příprava na integraci PTZS • rozsáhlé systémy • přehledné programování	• vyšší cena • serverové řešení • nedořešené zamykání modulů • nedostatečně řešené napájení

2.10 Decentralizované systémy

Modernější a nepochybně koncepčnější technologie řízení systému IB je založena na distribuovaném systému řízení jednotlivých modulů (aktory, senzory, prostředky pro vizualizaci, zdroje). Tyto moduly mají vlastní „inteligenci“ a jsou schopny společného řízení celého systému. Není zde žádný centrální prvek, což znamená, že všechny prvky jsou rovnocenné. Komunikace probíhá vždy po sběrnici nebo bezdrátově za pomoci speciálního protokolu.

Výhodami jsou jednodušší a levnější propojení mezi prvky, variabilita systému, absence výpadku systému při poruše. Nevýhodami jsou hlavně vyšší pořizovací cena z důvodu inteligence jednotlivých prvků (modulů) a větší nároky na realizaci.[1,10]

2.10.1 Sběrnice

Sběrnice má za účel zajistit přenos dat a řídících povelů mezi dvěma a více elektronickými zařízeními. Níže je uvedeno několik příkladů sběrníc užívaných jako integrační prostředek.

2.10.1.1 KNX / EIB

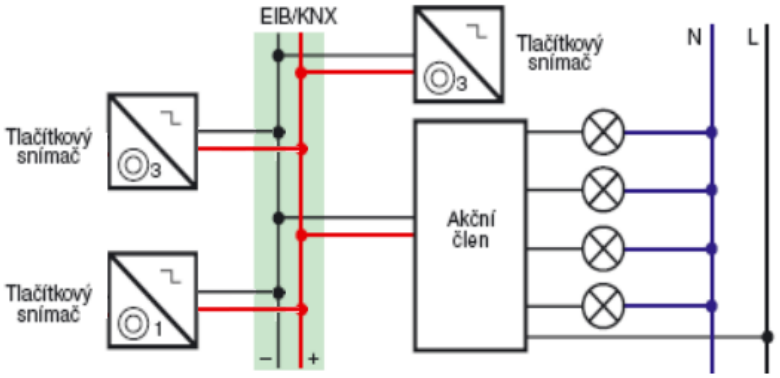
Byla vytvořena sdružením European Instalation Bus Association (EIBA) společně s velkými světovými výrobci (např. Siemens, ABB) ze základu původní starší sběrnice EIB a z ní teprve vznikla zpětně kompatibilní sběrnice KNX. KNX sběrnice je používaná v Evropě a často se s ní můžeme setkat v České republice.

Jde o decentralizovaný instalační řídicí systém pro automatizaci budov. Je určena ke komunikaci všech prvků (snímače, akční členy, řídící prvky atd.) po jedné sběrnici v budově nebo i více budovách. Ta je vedena paralelně s vedením 230 V. Výměna informací mezi jednotlivými systémy probíhá přímo. Data jsou vkládána do datových telegramů a jsou digitálně přenášena sběrnicí. Každý prvek má jedinečnou fyzickou adresu sloužící k identifikaci. Sběrnice může být jakékoliv topologie s podmínkou, že délka jedné větve nebo linie je do 1 km s maximálním počtem prvků 64. Existuje několik alternativ přenosového média KNX/EIB:

- KNX/TP kabel – twisted pair (kroucený pár metalických vodičů). Je nejpoužívanějším provedením KNX sběrnice. Rychlost komunikace na sběrnici tohoto typu je 9 600 b/s.
- KNX/PL – power line (silové vedení). Vedení je realizováno přímo pomocí silového vedení 230 V. Rychlost přenosu dat po tomto typu sběrnice je 1 200 b/s.

- KNX/RF – rádiové spojení. Bezdrátová komunikace mezi prvky probíhá v bezlicenčním pásmu. Odpadá instalace kabeláže. Rychlost komunikace je 16 000 b/s.
- KNX/IP – k jejich přenosu je možné využít sítě LAN nebo Internet. KNX telegramy jsou vysílány jako součást IP telegramů.
- KNX/FG - optická vlákna.

Obr. 7 - Blokové schéma decentralizovaného užití KNX/EIB; Zdroj: [upraveno dle 20]



Pro sběrnici KNX je potřeba speciální KNX / EIB napájecí zdroj (24 VDC). Pro programování jednotlivých zařízení a celého systému EIB lze využít zpoplatněného nezávislého programovacího softwaru Engineering Tool Software (ETS) a IP brány instalované na DIN lištu, například Loxone Miniserver nebo ABB i-bus® IPS/S 2.1.

Se sběrnicí KNX je možno také propojit například ústřednu Satel Integra pomocí převodníku sběrnic INT-KNX nebo INT-KNX-2. Ústředna tak může ovládat aktory připojené ke sběrnici KNX a zařízení na sběrnici mohou ovládat zabezpečovací systém. KNX/EIB je určen spíše pro středně velké a velké objekty průmyslového nebo komerčního charakteru. [9]

Tab. 4 - Stručné zhodnocení integračního řešení KNX/EIB; Zdroj: [1]

Výhody:	Nevýhody:
• rozšířenost • používají velcí výrobci • rozsáhlé systémy • distribuované řešení	• vyšší cena • neúplná kompatibilita • chybovost přenosu (kolize) • nedostatečně řešené napájení • problematická změna konfigurace a programování

2.10.1.2 LonWorks

Standard Local Operating Network (LON) byl zřízen roku 1992 firmou Echelon ve spolupráci s firmami Toshiba a Motorola pro univerzální a levná technická použití na nejnižší automatizační úrovni. Protokol se nazývá LonTalk a celé technické řešení se označuje souborně jako LonWorks. V Evropě se tento systém rozšířil právě jako komunikační sběrnice IB. Jeho použití je však výrazně širší, známé jsou například aplikace pro řízení vlakové dopravy realizované nad touto sběrnicí.

Sběrnice LON je otevřený decentralizovaný sběrnicový systém využívající sériového přenosu zpráv. Sestává se z uzlů a zařízení na sběrnici, které si mezi sebou vyměňují informace. Každé zařízení vlastní univerzální čip „Neuron“ obsahující všechny potřebné funkce protokolu LonTalk. Ten popisuje způsob komunikace a přístup k programování. Zařízení mohou být napojena na téměř jakékoli přenosové médium (běžnou počítačovou síť, RS-485, síťový rozvod 230 V, rozvod kabelové televize). Topologie je odvozena od TCP/IP sítí (stromová struktura), stejně tak jako pravidla přenosu telegramu v těchto sběrnicích. V praxi se sběrnice LON využívá v aplikacích, kde je kladen nárok na délku sběrnice a nikoliv na rychlost přenosu dat. [6,31]

Tab. 5 - Stručné zhodnocení integračního řešení LonWorks; Zdroj: [vlastní]

Výhody:	Nevýhody:
• variabilita fyzické vrstvy • distribuované řešení	• vyšší cena

2.10.2 Síťové protokoly

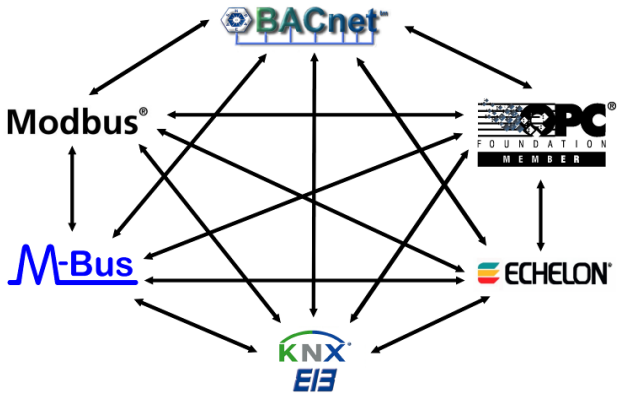
Obecně je protokol soubor pravidel (specifikací) mezi dvěma nebo více uzly sítě (systémy, moduly, regulátory). Protokoly tedy stanovují způsob komunikace uzlů mezi sebou. Kromě definování formátu fyzického přenosu určují například i to, jakými nástroji bude přenos zabezpečen či jakými bude kontrolována správnost přenesených dat.

2.10.2.1 BACnet

Building Automation and Control Network (BACnet) se využívá pro identifikaci standardizovaného komunikačního protokolu využívaného pro automatizační a řídící systémy budov. Tento komunikační protokol byl vyvinut společností American Society of Heating, refrigeration and Air - Conditioning Engineers v roce 1995. Jedná se o otevřený protokol. Přináší značnou kompatibilitu zařízení komunikujících po datové sběrnici, kde si zařízení a systémy mohou vzájemně vyměňovat informace. Jeho nejčastěji používanou komunikační sběrnicí je Arcnet nebo Lon, případně lze využít i Ethernet nebo sériovou linku RS-485.

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. Je založen na modelu ISO/OSI, sestává se ze specifikace struktury BACnet objektu, služeb pracujících s objekty, protokolu síťové vrstvy definující přenos a směrování zpráv a fyzické síťové přenosové technologie. Aplikační programy se vytvářejí pomocí programovacího kompletu PG5 Controls-Suite. Společný jazyk BACnet se rozšířil v mnoha aplikacích po celém světě a od 1. 8. 2004 je normalizován i v ČR jako ČSN EN ISO 16484-5. [14]

Obr. 8 - Možné propojení komunikačních protokolů; Zdroj: [upraveno dle 16]



2.10.2.2 ZigBee

ZigBee je komerční označení standardizovaného protokolu IEEE 802.15.4 pro bezdrátové osobní místní sítě (WPAN). Tento bezdrátový síťový protokol je zaměřen na oblast automatizace a vzdáleného řízení, u jehož zrodu stály společnosti ZigBee Aliance a IEEE (Institute of Electrical and Electronics Engineers). Jeho charakteristickými vlastnostmi jsou malá přenosová rychlost, nízká spotřeba a nízká cena komponent. Protokol ZigBee lze využít u zařízení napájených z baterií, která nepotřebují vysoké přenosové rychlosti. Právě kvůli nízké spotřebě mohou zařízení pracovat z bateriového napájení několik měsíců až let. Kvůli snižování spotřeby využívá režimu spánku - systém se probouzí periodicky ve zvolených intervalech, kdy probíhá komunikace. Jeho přenosová rychlost se odlišuje dle použité modulace signálu (O-QPSK, BPSK) a distribučního regionu: 250 kbps na 2,4 GHz (celosvětově), 40 kbps na 915 MHz (Amerika) a 20 kbps na 868 MHz (Evropa). Dosah zařízení ZigBee se přibližně pohybuje mezi 10-75 metry v závislosti na použitých anténách a vyzářeném výkonu. Je určen pro malé a středně velké objekty. [18]

2.10.2.3 Z-Wave

Jde o bezdrátový síťový protokol, který je zaměřen na oblast automatizace a vzdáleného řízení. Používá obousměrnou, potvrzovanou rádiovou komunikaci a automatické vytváření optimální přenosové trasy s retranslací. Z-Wave protokol používá pro komerční účely přenos po několika rádiových frekvencích ISM pásma odlišných dle regionu distribuce: Evropa - 868,4 a 869,9 MHz; Spojené státy - 908,4 a 916 MHz; Austrálie/Nový Zéland - 921,4 a 919,8 MHz; Rusko - 869,2 MHz. Data jsou přenášena v 8-bit blocích rychlostí 40 Kb/s, starší verze umožňovaly rychlost 9 600 b/s. Obě tyto verze jsou kompatibilní. Každá vytvořená síť Z-Wave má svůj jedinečný identifikátor HOME ID a každé k ní připojené zařízení (uzel) obdrží svůj vlastní identifikátor NODE ID. V rámci jedné konkrétní sítě je pak HOME ID stejné pro všechna zařízení, zatímco NODE ID uzlu je unikátní pro daný uzel.

Kompatibilita zařízení garantovaná společenstvím výrobců Z-Wave Alliance umožňuje velkému množství firem vyrábět širokou škálu praktických prvků, snímačů, čidel a dalších doplňků. Tato otevřenost zajišťuje rozvoj systému a velký výběr periferií pro všechny aplikace. Je určen především pro malé a středně velké objekty.[1,10]

2.10.2.4 IQRF

Jedná se o modulární systém navržený pro bezdrátovou komunikaci topologií „mash“ sítě (IQMASH) za pomoci protokolu DPA (Direct Peripheral Adressing). Systém IQRF pracuje v bezlicenčním pásmu (Evropa - 868 MHz, Spojené státy - 916 MHz). Jeho základem jsou miniaturní „TR moduly“ o velikosti formátu SIM karty. Díky modulaci tzv. klíčováním frekvenčního posuvu (FSK) a malé přenosové rychlosti (v nastavitelném rozsahu 1,2 – 115 KB/s) se moduly vyznačují velmi malým odběrem (35 μA v příjem, 14 – 24 mA vysílání) a zároveň velkým dosahem signálu (udává se až 700 m). Díky retranslaci jde vzdálenost celé sítě podstatně navýšit.

Systém IQRF je možné použít všude tam, kde je třeba zabezpečit komunikaci mezi dvěma a více zařízeními (TF moduly). Každý modul má v sobě zabudován jednoduchý operační systém, který zajištuje komunikaci protokolem DPA. Samotné programování je soustředěno pouze na vytváření uživatelských událostí a přenos obstarávají TR moduly samostatně. Moduly se programují programovacím jazykem C rozšířeným o knihovnu funkcí IQRF platformy. Jsou nabízeny i speciální vývojové kity (CK-USB-04, DK-EVAL-04), pomocí kterých je možné snadno vytvářet vlastní aplikace postavené na volitelném TR modulu (TR-52B, TR-54D). K systému lze také přistupovat pomocí speciálních bran (GW-ETH-01, GW-USB-04) USB nebo Ethernet rozhraním. K dispozici jsou také dotyková grafická rozhraní (VCP-0x).[29,30]

Tab. 6 - Přehled základních parametrů protokolů užívaných pro bezdrátový přenos; Zdroj: [vlastní]

	Wi-Fi	Bluetooth	ZigBee	Z-Wave	IQRF
Standard	802.11x	802.15.1	802.15.4	-	-
Modulace	OFDM, DSSS	pi/4-DQPSK	OPQSK, BPSK	GFSK	FSK
Frekvence	2,4 / 5 GHz	2,4 GHz	2,4 GHz, ISM	ISM	ISM
Rychlost	< 54 Mb/s	1 Mb/s	250 kb/s	9,6; 40 kb/s	9,6 – 920 kb/s
Odběr při vysílání	> 400 mA	40 mA	35 mA	23 mA	14 – 24 mA
Odběr při „STAND-BY“	20 mA	200 µA	3 µA	2,5 µA	35 µA
Dosah vysílání	1 km	3 m	10 m	30 - 50 m	až 700 m
Aplikace	Propojení počítačů, přístupové body	Přenos středně objemných dat, náhrada za kabelové spojení	Domácí automatizace, vzdálený přístup	Domácí automatizace, vzdálený přístup	Domácí automatizace, jakékoliv regulační aplikace
Topologie	Poin to multi-point	Poin to multi-point	Strom	Strom	Point to point / mash

2.10.2.5 Standard SIA DC-09

Tyto moderní protokoly jsou přímo určeny pro další rozšiřování poskytovaných služeb pomocí komunikace po datových sítích nad IP komunikačními prostředky. Jedná se o otevřený standard vyvinutý v roce 2007 americkými výrobci alarmové techniky. Standardizovanému protokolu (nyní poslední verze ANSI/SIA DC-09-2013) stačí pouze jedno přijímací centrum (DPPC) pro všechny výrobce techniky instalované v objektu. Unikátnost a bezpečnost komunikace se zajišťuje použitím šifrovacího klíče (16 nebo více náhodných znaků), který může být pro každý objekt jiný a je kdykoli vyměnitelný. K předávání zpráv se využívají komunikační formáty objektových zařízení, například DOM-XML.

Ač je z pohledu bezpečnosti a spolehlivosti přenos dat nad IP nevhodné integrační řešení, tento protokol zavádí robustní a bezpečnou opakovanou komunikaci a dokonce je takřka ideálním protokolem pro přenos rozsáhlejších bezpečnostních informací veřejnou sítí. Standard SIA DC-09 také zavádí nové a velmi silné šifrování zpráv nad IP (AES 192 pro objekty zvláštní důležitosti). **Je novinkou několika posledních let a s největší pravděpodobností se jedná o optimální řešení především pro integraci velkých systémů na rozsáhlé oblasti.** Standard již nyní využívá mnoho předních světových firem (např. Honeywell, ASIS, Bosch, Siemens atd.). Tento standard se pak jeví jako zajímavý možný prostředník budoucího vývoje integračních technologií, a to především pro cloudová řešení nebo dokonce „internet věcí“, kde je ovšem otázkou objemnost dat zasílaná po tomto protokolu.

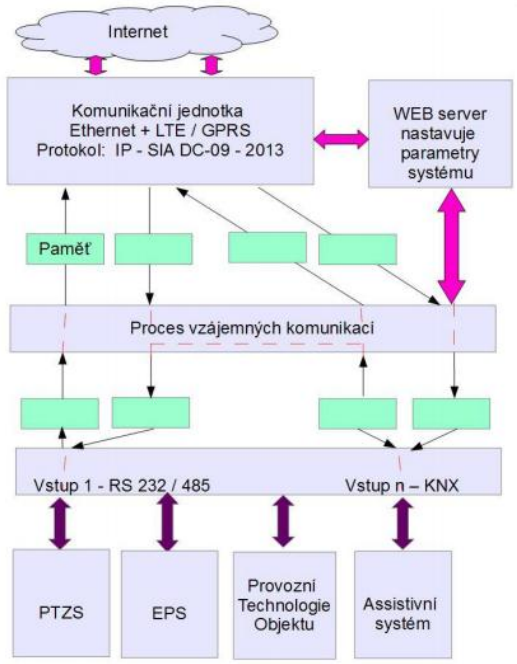
Protokol se řídí několika principy:

- ke komunikaci s dohledovými centry je vždy využito současně dvou internetových připojení (x DSL a GPRS/LTE),
- dochází k synchronizaci času v celé síti,
- sjednocuje komunikaci PZTS, EPS, CCTV a dalších systémů,
- zavádí časové razítko u každé přenášené zprávy i potvrzovací zprávy,
- protokol podporuje verifikaci vzniklých událostí pomocí kamerových systémů, jednotlivých obrázků či přenosů zvuků (hlasu) z objektu,
- protokol umožňuje posílat zpětné povely do objektů a ovládat různá zařízení,
- jsou dána pevná pravidla pro sestavení hlavní části kódu,
- každé vysílací zařízení může využívat svůj vlastní šifrovací klíč (šifrovací metoda CBC-AES),
- jsou zde rozsáhlé možnosti verifikace událostí vzniklých ve střeženém objektu,
- všechny vstupy a výstupy se řídí mezinárodními normami (ANSI/SIA)

- na výstupu jsou dokumenty typu DOM-XML,
- dokumenty typu DOM-XML jsou snadno zpracovatelné a **mohou sloužit například k informování zásahových jednotek o krizové situaci on-line (například pomocí tabletu).**

Standard byl schválen jako americká národní norma Radou bezpečnosti průmyslových standardů (SISC) roku 2013. Jedná se o následovníka protokolu SIA DC-07-2001 vydaného též Security Industry Association (SIA). V České republice byla dobrovolná norma TNI 33 4592 schválena Úřadem pro technickou normalizaci (ÚNMZ) dne 1. 3. 2014 a je nadále rozvíjena jako norma pro komunikaci ústředen PZTS a EPS s DPPC pomocí internetu. [12,27]

Obr. 9 - Vnitřní komunikace integrovaného systému pomocí SIA DC-09; Zdroj: [21]



Tab. 7 - Stručné zhodnocení integračního řešení SIA DC-09; Zdroj: [1]

Výhody:	Nevýhody:
• univerzálnost • bezpečnost • kompatibilita s většinou současných používaných poplachových systémů a PCO	• nutný další vývoj a testování pro integraci PTZS

2.10.3 Cloudové systémy

Cloudový způsob integrace je spíše technologií budoucnosti. Je to další odbočka ve vývoji stále aktuálnější technologie IoT – Internet of Things, česky „internetu věcí“. Ta je založena na propojení jednotlivých zařízení prostřednictvím internetu bez aktivní účasti uživatele a je předpoklad jejího masivního rozšíření v budoucích několika letech. Existují odhady, že k této síti bude koncem roku 2015 připojeno 4,9 mld. zařízení a do roku 2020 se počet zařízení odhaduje na více než 20 mld. Možnosti nasazení této technologie jsou globálního charakteru a velice široké. Počítá se, že k „internetu věcí“ bude možno připojit prakticky jakékoliv zařízení (senzory, aktory, termostaty, zařízení pro odečty energií, bílou techniku, náramkové hodinky, automobily), také se hovoří o možnosti nasazení v průmyslu. Tato technologie má potenciál býti prostředníkem k vytvoření tzv. „chytrých měst“.

Celá síť běží, tak jako v mnoha bezdrátových technologiích, v bezlicenčním pásmu (ČR – 868 MHz). Nyní v ČR síť buduje například společnost T-Mobile spolu se společností SimpleCell Networks. K jejímu pokrytí bude vyžadováno 400 – 500 stanic s dosahem signálu předpokládaných

120 km při přímé viditelnosti. Dalším zprostředkovatelem v ČR je společnost České Radiokomunikace. Prostředkem k připojení do nové sítě T-Mobile a SimpleCell Networks bude čip společnosti Sigfox, pro České Radiokomunikace to bude pravděpodobně několik zařízení vyvíjených uskupením firem a výrobců LoRa.

„Internet věcí“ je umožněn mimo jiné díky miniaturizaci, snižování spotřeby a ceny čipů a bezdrátových technologií, které se tak mohou obejít bez velké baterie a komunikují spolu s velmi malou spotřebou. Principem je, že každé zařízení (detektor, aktor, nástroj pro vizualizaci atd.) má vlastní čip umožňující připojení do sítě „internetu věcí“. Čipy mohou odeslat jen několik málo bytových zpráv denně, čímž je dosáhnuto extrémně nízkých hodnot odběru čipů a mohou být napájeny bateriově. Řízení celého systému je pak přítomno kdesi ve virtuálním světě internetu (na cloudu) – systém je řízen tzv. Cloud Computingem (poskytování služeb či programů uložených na serverech). Celý výpočetní výkon je tedy umístěn na síti „internetu věcí“ a hostuje ho konkrétní společnost. Konečný uživatel by pak k celému systému obchodně přistupoval jako k službě Iaas.

„Internet věcí“ je dalším možným technologickým řešením „inteligentní budovy“, nutno dodat, že patrně opravdu revolučním. Bude však velmi záviset na konkrétních řešení, zda bude moci být takový systém uveden do provozu. Například zřízení zabezpečovacího systému na této technologii dle stávajících norem je nyní naprosto nemyslitelné. [11]

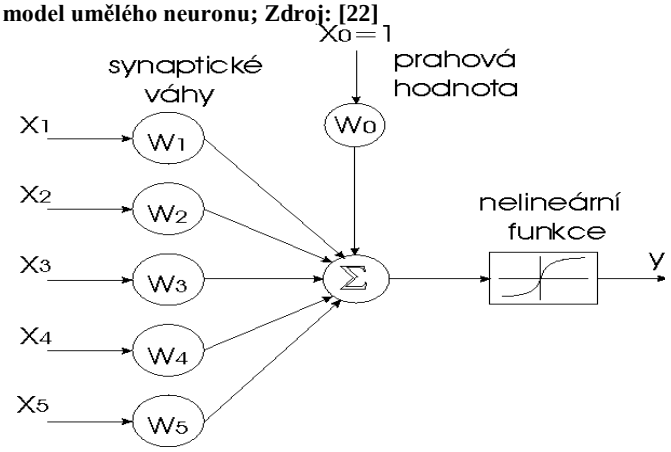
Tab. 8 - Stručné zhodnocení cloudového řešení integrace; Zdroj: [vlastní]

Výhody:	Nevýhody:
• globální nasazení technologie • integrace se „všemi věcmi“ • cloudové řízení	• bezpečnostní rizika • otázka řešení nasazení pro PTZS • malá četnost komunikace (nevhodné pro PTZS)

2.11 Využití neuronového klíče

Použití neuronových sítí je v poslední době velice široké (rozeznávání obrazu, predikce časových řad, simulování chování biologických organizmů atd.). Jedním ze skutečných předpokladů užití neuronových sítí je ten, že se může jednat o univerzální integrační nástroj, který je založen na procesu učení se komunikace právě díky matematickému modelu neuronových sítí.

Obr. 10 - Matematický model umělého neuronu; Zdroj: [22]



Předpoklad fungování procesu je, že celý, již instalovaný, oživený a plně funkční poplachový systém se připojí k „neuronovému klíči“, který se automaticky „naučí“ šifrovaný způsob komunikace uvedeného systému. 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). Systémy pak mezi sebou plnohodnotně komunikují na úrovni předem definovaných stavů. Nároky na instalaci a servis by poté byly v podstatě nulové. [1,13]

Tab. 9 - Stručné zhodnocení integračního řešení pomocí neuronového klíče; Zdroj: [1]

Výhody:	Nevýhody:
• uživatelsky a systémově jednoduché • cenově příznivé • přiměřeně spolehlivé • zcela univerzální	• původní v praxi nevyzkoušené řešení • potencionálně bezpečnostní riziko • vhodné pro menší a středně velké systémy

2.12 Open Source

Mnoho lidí si snaží vytvářet svá integrační řešení pomocí Open Source platforem. Platformy toho typu mohou plnit funkci nástroje pro vyvíjení hardwarového/softwarového mezičlánku jednotlivých subsystémů. Na rozdíl od proprietárního řešení closed source umožňuje Open Source otevřenost kódu a tím udává potenciál k nalezení technického řešení vzájemné kompatibility subsystémů široké veřejnosti. Existují skutečné případy technicky velmi kvalitně zpracovaných systémů, jejichž úvahu o komerčním prodeji (po překonání problému přenositelnosti a po opomenutí velkých obtíží v konkurenčním prostředí) zpravidla ukončí potřebná certifikace. Pro získání certifikace by bylo nutné nalezení určitého rovnováhy mezi technickými, ale také legislativními požadavky, které musí výsledná integrace plnit. Otevřenost kódu s sebou totiž nese výrazná rizika bezpečnosti, která musí být omezena legislativními předpisy (zákony, vyhláškami, normami).

3 Normy a legislativa vztahující se k integraci PTZS v IB

Z hlediska integrace PTZS do inteligentních budov jsou relevantní tyto normy:

- ČSN CLC/TS 50 130 Poplachové systémy,
- ČSN EN 50 131 Poplachové zabezpečovací a tísňové systémy,
- ČSN EN 50 132 CCTV sledovací systémy pro použití v bezp. aplikacích,
- ČSN EN 50 133 Systémy kontroly vstupů pro použití v bezp. aplikacích,
- ČSN CLC/TS 50 398 Kombinované a integrované systémy.

Dále je vhodné zmínit zákony týkající se problematiky:

- zákon č. 101/2000 Sb., o ochraně osobních údajů (u kamerových systémů)
- zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)

3.1 ČSN CLC/TS 50 131 - Poplachové zabezpečovací a tísňové systémy

Norma ČSN CLC/TS 50 131 se vztahuje k poplachovým zabezpečovacím a tísňovým systémům (PZTS) nebo systémy obsahující pouze zabezpečovací, nebo pouze tísňové prostředky. Byla schválena sdružením CENELEC 4. 4. 2006. Členové CELENEC jsou povinni splnit interní podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy. **Smyslem této normy je pomoci pojistitelům, instalačním firmám, uživatelům či policii zpracovávat celkovou a přesnou specifikaci ochrany vyžadované v jednotlivých prostorách,** ale nespecifikuje typ technologie, rozsah nebo stupeň detekce. Nezabývá se ani žádnými požadavky k instalaci. Norma říká, že účelem PZTS je zvýšení bezpečnosti střeženého prostoru. Pro dosažení maximálního možného zabezpečení by měl být systém kombinován s prvky a postupy fyzického zabezpečení, nejvíce je toto nutné u PZTS vyšších stupňů zabezpečení. Komponenty PZTS musí být v rámci systému vzájemně kompatibilní a musí se volit v souladu se stupněm zabezpečení a náležitou třídou prostředí. **Prvky jiných systémů mohou být integrovány do PZTS, ale pouze tehdy, pokud nedojde k negativnímu ovlivňování systému**.

PZTS představují komplexní soubor technických prostředků, jejichž prostřednictvím je řešena ochrana proti neoprávněnému vstupu do objektu. V ČR norma ČSN CLC/TS 50131-1 definuje čtyři stupně zabezpečení. Každému konkrétnímu PTZS v objektu je přiřazen konkrétní stupeň zabezpečení určující jeho provedení:

Stupeň	Míra rizika	Předpokládaný narušitel
1	nízké	Vetřelec nebo lupič má malou znalost I&HAS a má k dispozici omezený sortiment snadno dostupných nástrojů
2	nízké až střední	Vetřelec nebo lupič má omezené znalosti o I&HAS a používá běžného nářadí
3	střední až vysoké	Vetřelec nebo lupič je obeznámen s I&HAS a má rozsáhlý sortiment nástrojů a elektrických zařízení
4	vysoké	Používá se, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič je schopen zpracovat podrobný plán vniknutí a má kompletní sortiment zařízení

Stupeň zabezpečení se zařízení přiděluje certifikací konkrétní zkušebny, která vykonala potřebný proces stanovený normou ČSN CLC/TS 50 131-1. Norma také stanovuje, že stupeň bezpečnosti systému je roven komponentě s nejnižším stupněm zabezpečení v něm obsaženým. **Pokud je systém dělen do subsystémů, stupeň zabezpečení subsystému odpovídá komponentě s nejnižším stupněm zabezpečení.**

K vytvoření jakéhokoliv zabezpečovacího systému je vždy nutné propojit několik základních prvků tak, aby z nich byl sestaven korektní zabezpečovací systém. Každá část tohoto systému má předem stanovenou roli a pouze správným výběrem, funkčností a umístěním lze dosáhnout plně fungujícího systému. [25]

* norma ČSN CLC/TS 50131 používá anglické označení I&HAS jako synonymum za PTZS

3.2 ČSN CLC/TS 50 398 - Kombinované a integrované systémy

Norma uvádí všeobecné požadavky a typy struktur kombinovaných a integrovaných poplachových systémů. Norma má zajistit integraci jedné nebo více aplikací do jednoho integrovaného systému. Tento dokument poskytuje další informace týkající se prvotního návrhu (projektu) systému, plánování, instalace, předávání, provozu a údržby (servisu) kombinovaného a integrovaného systému. Tato norma specifikuje požadavky na poplachové systémy, které

jsou kombinovány nebo integrovány s jinými systémy, které mohou a nemusí být poplachovými systémy. Definuje požadavky týkající se pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasnit případné rozpory. [10]

V Normě ČSN CLC/TS 50 398 jsou uvedeny 3 konfigurační typy integrovaných poplachových signálů:

- **typ 1** – kombinace a integrace jednoúčelových poplachových systémů a jednoúčelových nepoplachových systémů,
- **typ 2A** – kombinace a integrace poplachových systémů a nepoplachových systémů, které používají společné přenosové trasy a společná zařízení. Porucha v jakékoli aplikaci nemá žádný negativní vliv na jakoukoli další poplachovou aplikaci, čehož se dosahuje redundancí neboli nadbytečností,
- **typ 2B** - kombinace a integrace poplachových systémů a nepoplachových systémů, které používají společné přenosové trasy a společná zařízení. Porucha v jedné aplikaci může mít negativní účinek na jinou aplikaci v systému.

Dále norma uvádí tři stupně integrace, které charakterizují úroveň kompletnosti a míru homogenizace systému:

- **integrační stupeň 1** - jedná se o základní stupeň integrace, která je provedena v rámci jednoho bezpečnostního systému. Příkladem může být systém kontroly vstupu, ve kterém jsou čtečky karet, klávesnice, monitorovací prvky, systém výdeje karet a správy uživatelských dat integrovány do jednoho systému.
- **integrační stupeň 2** - jde o vyšší stupeň integrace v rámci několika bezpečnostních systémů. Příkladem může být integrace systému kontroly vstupu se zabezpečovací signalizací a kamerovým systémem do společného uživatelského rozhraní. Existuje zde vazba mezi systémy.
- **integrační stupeň 3** - představuje nejvyšší stupeň integrace bezpečnostních a IT technologií. Například integrace systému kontroly vstupu s vnitřní komunikací s dalšími aplikacemi jako je mzdový systém pro výpočet mzdy dle odpracovaných hodin.

Norma je velice obecná, přesto však v bodě 4.2. jasně říká: „**U integrovaných poplachových systémů musí být pro každou aplikaci systému použity její příslušné normy.“** [5,10,26]

3.3 Zákon č. 455/1991 Sb.

Tento zákon pojednává o živnostenském podnikání (živnostenský zákon). Dle toho zákona je instalace bezpečnostních systémů koncesovanou živností. Pro získání koncese k provozování živnosti č. 314 - Technické služby k ochraně majetku a osob je potřeba splnit některé zásadní předpoklady. **Bezpečnostní systémy nesmí instalovat osoba bez odpovídající koncese a certifikátu opravňující instalovat konkrétní bezpečnostní systém.** Důsledkem tohoto zákonného vymezení je, že jakýkoliv projekt či instalaci provádí pouze koncesované firmy s certifikátem.

3.4 Certifikace

Certifikace je postup, kterým třetí strana poskytuje písemná ubezpečení, že výrobek, proces nebo služba je ve shodě se **specifikovanými požadavky**. Postup získání certifikátu se nazývá certifikační systém. Ten má vlastní pravidla postupu řízení pro provádění certifikace shody. Aby byla certifikace konkrétní technologie uznána, je zapotřebí vycházet z předpokladu, že objekt certifikace vyhovuje předem určeným specifikovaným požadavkům. Ty se uvádějí v **normách nebo některých dalších technických dokumentech**. Po splnění předpokládaných požadavků si kontaktovaná certifikační laboratoř vyžádá určitý počet potřebných komponent a po jejich dodání může být spuštěn proces nutných zkoušek stanovených normou pro získání certifikátu. Teprve na základě pozitivního absolvování všech zkoušek certifikační orgán vydá **dokument ubezpečující o platnosti shody výrobku**. Od doby platnosti tohoto dokumentu může být výrobek označován například dle normy ČSN CLC/TS 50 131 příslušným stupněm bezpečnosti.

V České republice jsou všechny platné technické normy zakomponovány do certifikačního postupu Národního bezpečnostního úřadu (NBÚ). Certifikace se provádí ve zkušebnách akreditovaných tímto úřadem. Pokud má být certifikát platný v zemích sdružení CELENEC, je třeba provést všechny zkoušky dle norem tohoto sdružení. Ceny certifikátů nejsou předem stanoveny podle ceníků.[6]

4 Popis a možnosti systému Fibaro

V této kapiole bude věnován prostor podrobnému rozboru systému Fibaro.

4.1 Obecný popis

Moderní systém automatizace budov/domácností Fibaro integruje jednotlivá modulární zařízení pro zajištění komfortu, bezpečí, úspor času, energií a v neposlední řadě financí. Díky bezdrátové koncepci, je instalace systému možná bez nutnosti náročných stavebních úprav interiéru. Umožňuje připojení až 230 bezdrátových prvků (modulů Z-Wave), mezi kterými lze vytvářet scény v závislosti na uživatelem definovaných proměnných. Komfort přináší hlavně vzdálený přístup přes web, mobilní telefon nebo tablet, kde je možné systém spravovat v uživatelsky přívětivé aplikaci (uživatelem vlastnícím příslušná práva).

Funkce, kterými systém Fibaro disponuje:

- ovládání světel (relé, stmívač, RGBW),
- komfortní a automatizovaná regulace teploty v místnostech,
- ovládání střídavých motorů (rolety, žaluzie, markýzy, vrata, brány atd.),
- dohled nad havarijními stavy (požár, zaplavení),
- jednoduché zabezpečení objektu,
- měření spotřeby energií (okamžitá, celková, peněžní),
- video interkom s IP kamerou,
- SMS upozornění,
- geolokalizace (sledování rodinných příslušníků),
- a další.[24,28]

4.2 Popis komunikace systému Fibaro

Fibaro je bezdrátový systém využívající technologii rádiové sítě Z-Wave. Tato síť pracuje na frekvencích ISM pásma 868,4 až 921,4 MHz odlišných dle distribučního regionu. **Přenos informací mezi moduly probíhá po obousměrné (příjem/vysílání) potvrzované (kontrola spojení) retranslační (zvýšení kvality pokrytí) bezdrátové rádiové síti s automatickým vytvářením její optimální přenosové trasy skrze protokol Z-Wave.**

Každý použitý prvek (modul) v síti zvyšuje kvalitu pokrytí tím, že může přenášet informace prvkům, které jsou vzdáleny nebo v místech se silným tlumením rádiového pole. V důsledku toho síť není závislá pouze na kvalitě signálu antény řídící jednotky (HC-2, HCLite) – tato funkce se nazývá retranslace rádiového signálu. Po zapnutí je vždy automaticky aktualizována pozice jednot-

livých prvků a v reálném čase je v mřížové topologii ověřena a sestavena optimální komunikace (přenosová trasa) se všemi prvky. Síť rovněž periodicky kontroluje spojení s jednotlivými prvky.

Moduly systému Fibaro dokáží pracovat v režimech tzv. asociace, jejíž princip spočívá ve vytvoření přímé vazby mezi moduly. Umožňuje tak přímý přenos povelů mezi moduly bez účasti řídicí jednotky. Je nutno dodat, že se jedná o omezené množství základních povelů (akcí), ty složitější pak musí obstarávat sama řídící jednotka. Jako praktickou stránkou této funkce se jeví možnost redundantní komunikace prvků, které by byly mezi sebou takto asociovány a fungovali by jako záložní primitivní systém na úrovni asociace při případném výpadku řídící jednotky.

Technické parametry komunikace jsou blíže specifikovány v kapitole výše (viz kapitola 2.10.2.3). [24,28]

4.3 Řídící jednotky Fibaro

V této podkapitole budou popsány dvě z nabízených řídících jednotek systému Fibaro.

4.3.1 FGHC2 - Home Center 2

Home Center 2 (HC-2) je jedna ze dvou variant řídících jednotek systému domácí automatizace, které jsou dosud výrobcem nabízeny. Jedná se o elektronické zařízení, které bezdrátově za pomocí protokolu Z-Wave spravuje veškeré moduly v dané instalaci a umožňuje uživatelsky přívětivým rozhraním vizualizaci jejich stavů a ovlivnění systému člověkem. Přístup do rozhraní je prováděn buď přímým připojením k jednotce lokální sítí formou aplikace webového prohlížeče, nebo je k dispozici vzdálený přístup do jednotky, opět aplikací webového prohlížeče nebo speciální aplikací pro mobilní zařízení. Vzdálený přístup je podmíněný připojením jednotky k internetu a její následnou registrací k zabezpečenému serveru. K jednotce Fibaro HC-2 je možno připojit pomocí Z-Wave až 230 zařízení (modulů). Dále jednotka umožňuje zpracovávat například data z video zařízení nebo GPS systémů geolokalizace.[23,24,28]

Obr. 11 - Řídící jednotka Fibaro HC-2; Zdroj: [23]

Ke zpracování dat jednotka využívá poměrně výkonný procesor Intel Atom 1,6 Ghz a k ukládání dat SSD o kapacitě 2 GB. Dále každá jednotka HC2 obsahuje další jeden disk o kapacitě 4 GB na SSD, který je určený k možnému obnovování instalací ze zálohy. Pro připojení do LAN sítě je určen standardní ethernetový konektor RJ-45. Jednotka umí pracovat s DHCP nebo ji je možno pro identifikaci přiřadit statickou IP adresu. K připojení antény, díky níž je umožněna komunikace se všemi moduly v objektu, je určen standardní SMA konektor. Rozměry hliníkového šasi jednotky jsou 43 x 225 x 185 mm.[24,28]

4.3.2 FGHCL - Home Center Lite

Druhá nabízená řídící jednotka systému Fibaro Home Center Lite (HC Lite) firmy FIBARO je menší a ekonomičtější alternativa k jednotce HC-2. Umožňuje řešit většinu nejčastěji požadovaných funkcí jako model HC-2, avšak s několika omezeními:

- není vybavena programovacím interpretem Lua,
- nepodporuje hlasové ovládání Lili,
- nepodporuje VoIP,
- nepodporuje integraci zabezpečovacího systému Satel,
- nelze použít jako Master controller pro další jednotky ,
- doporučený počet připojovaných prvků je cca 150.

V jednotce zpracovává data úsporný procesor Cortex A8. Jednotka může být použita jako podřízená Slave jednotka k jednotce HC2 pro zvýšení pokrytí signálem Z-Wave. Plášť o rozměrech 90 x 90 x 33 mm je uzpůsoben k uchycení na DIN lištu. Na webu distributora se lze dočíst, že jsou pro tuto jednotku v přípravě moduly zálohovací baterie a připojení GSM komunikátoru.[24,28]

Obr. 12 - Řídící jednotka Fibaro HC Lite; Zdroj: [vlastní]

4.3.3 Moduly Fibaro

Jak již bylo řečeno, sytém domácí automatizace Fibaro pracuje na principu bezdrátové komunikace s pomocí protokolu Z-Wave. Firma Fibaro vyrábí několik svých vlastních modulů pro senzoriku a řízení akčních veličin. Díky otevřenosti protokolu Z-Wave však do systému Fibaro mohou být zařazena zařízení jiných výrobců splňující standardy této sítě (Z-Wave).

Moduly jsou většinou koncipovány tak, aby se vešly například do instalační krabice pod vypínač (Ø ≥ 50 mm) či jiného esteticky nerušivého místa. Některé moduly jsou navrženy s velice sympatickým „prodejným“ designem. Jsou koncipovány jako zařízení s minimální spotřebou, u většiny zařízení je odběr uváděn v desetinách W. Díky tomu je potřeba u bateriově napájených modulů měnit baterii (je doporučeno) při správném nastavení každé 2 roky. Moduly umožňují přeposílat informaci o stavu baterie. Životnost baterie zkracují některé podněty, které lze omezit nastavením modulu, například: pokud je nastaven krátký interval periody probouzení, pokud jsou zprávy o teplotě a intenzitě světla posílány příliš často nebo při opakovaných pokusech detektoru spojit se z již odpojenými zařízeními (v rámci asociace).

Funkčnost jednotlivých modulů lze dále ovlivnit přizpůsobením nastavovacích parametrů v řídící jednotce. Lze například ovlivnit a přizpůsobit podmínky prostředí za jakých bude vyvolána poplachová událost (citlivost detektoru pohybu, počítadlo detekcí k vyvolání poplachu, doba neaktivity detektoru po detekci, perioda probouzení detektoru).

Délka antény je optimalizována pro vlnovou délku používanou rádiovou sítí Z-Wave. Dosah bezdrátového přenosu zařízení je uváděn až 30/50 m (interiér/otevřený terén). Je ovšem závislý na umístění, například velké kovové předměty v blízkosti modulu (kovové instalační krabice, rámy dveří atd.) mohou být příčinou zhoršeného příjmu. Dále se pro bezproblémový přenos nedoporučuje s modulem pohybovat během jeho činnosti.[24,28]

4.3.4 FGS-221/ FGS-211 - Fibaro spínací modul 2x1,5kW / 1x3kW

Výrobce Fibaro nabízí dva druhy reléových spínacích modulů, se dvěma nebo jedním výstupním kontaktem. Moduly FIB-FGS-221 / FIB-FGS-211 jsou určeny pro montáž pod vypínač nebo kamkoliv, kde je zapotřebí spínat odporovou zátěž až do 2 x 1,5 kW / 3 kW. Moduly je možno ovládat rádiovou sítí Z-Wave nebo tlačítky připojenými na vstupní kontakty S1 a S2. Maximální spínaný proud kontaktu AC / 230 V i DC / 30 V se uvádí u modulu FIB-FGS-221 8 A a u modulu FIB-FGS-211 16 A. Jako ochrana proti přehřátí je přítomna funkce odpojení zátěže při překročení teploty 105 °C. Zařízení je v souladu s normami EN 55015 (rušení rádiovými vlnami) a EN 60669-2-1 (provozní bezpečnost). Modul FIB-FGS-221 může být použit jako modul pro komunikaci

s externím GSM komunikátorem pro případné napojení na pult centrální ochrany (jedno z náležitých opatření ke splnění certifikace dle ČSN CLC/TS 50 131). Výstupním prvkem modulů je galvanicky izolovaný spínací kontakt.[24,28]

4.3.5 FGWPE-101 - Fibaro spínaná zásuvka s měřením, 2,5 kW

Zařízení FIB-FGWPE-101 je univerzální reléový spínač ve formě mezičlánku zásuvky, který je podobný klasickým spínaným zásuvkám. Dálkově prostřednictvím protokolu Z-Wave nebo přímo tlačítkem na těle zásuvky je možno připojovat a odpojovat odporové zátěže do příkonu až 2 500 W (u ostatních typů zátěží je nutno počítat s účiníkem cos φ dle charakteru zátěže). Zásuvka je vybavena ochranou proti zkratu a také funkcí automatického odpojení zátěže v případě, že je překročena maximální nastavená hodnota (touto funkcí však není vhodné suplovat funkci předpisového jištění elektrického okruhu). Maximální možné zatížení je udáváno 8 A / 1 500 W. Modul je dále vybaven obvodem pro měření celkové spotřeby elektrické energie a aktuálního odběru zátěže. Ten je vizualizován měnící se barvou svítícího lemu na čelní straně zásuvky. Připojení zásuvky je kompatibilní s ostatními EU zásuvkami dle normy IEC 60083, na vstupu s typem E/F a na výstupu s typem CEE 7/16 nebo CEE 7/17. Zařízení je v souladu s normami EN 55015 (rušení rádiovými vlnami) a EN 60669-2-1 (provozní bezpečnost). Výstupním prvkem modulu je galvanicky izolovaný spínací kontakt.[24,28]

4.3.6 FGD-211 - Fibaro stmívač

Zápustný univerzální stmívač FGD-211 je určený pro bezdrátové stmívání a přepínání světel. Může být zapojen s nulovým vodičem i bez nulového vodiče (bez zapojení nulového vodiče pak plní pouze funkci přepínacího kontaktu do 500 W). Stmívač automaticky identifikuje typ připojené zátěže. Je jím možno ovládat zátěž o výkonu 25 až 500 W. S použitím bypassu (FGB-001) zapojeného paralelně se zátěží je pak možno stmívat svítidla s minimálním odběrem. Díky nastavitelnému prahu minimální úrovně jasu je možno zcela stmívat LED svítidla. Funkcí stmívače lze ovládat například klasické žárovky 230V, halogenové žárovky 230V, halogenové žárovky 12V (se stmívatelnými předřadníky - spínanými zdroji) nebo stmívatelné LED. Modul je vybaven ochranou proti přetížení. Jeho výstupním prvkem je triak.[24,28]

4.3.7 FGRM-222 - Fibaro žaluziový modul

Žaluziový modul Fibaro FGRM-222 je určený pro bezdrátové ovládání rolet, žaluzií, markýz, vrat, bran a libovolných dalších zařízení poháněných jednofázovým střídavým motorem. Modul je možno ovládat řídící jednotkou v síti Z-Wave nebo tlačítky připojenými na vstupní kontakty S1 a S2. Ke vstupním kontaktům mohou být připojena mžiková nebo dvoupolohová tlačítka, které

ovládají připojený motor na výstupních svorkách O1 a O2 (maximální udávaný výkon motoru je 1 kW / 230 V). Rovněž je možné vzájemné logické propojení a následné skupinové ovládání více modulů jako jednoho. Modul je schopen přizpůsobit se danému zařízení díky procesu kalibrace, kdy si modul zjišťuje pozici koncových poloh a charakteristiku připojeného motoru. Po kalibraci je umožněno plné polohovatelnosti systému a monitorování aktuální pozice. Modul je vybaven měřením aktuálního odběru a celkové spotřeby elektrické energie. Výstupním prvkem modulu jsou spínací kontakty.[24,28]

4.3.8 FGRGBWM-441 - Fibaro modul pro řízení LED, RGBW

Modul FIB-FGRGBWM-441 má několik variabilních funkcí a jistě najde širší využití při integraci do sítě Z-Wave. Modul obsluhuje 4 vstupní (IN1 až IN4) a 4 výstupní (R, G, B a W) kanály, které je možno konfigurovat jako na sobě závislé či nezávislé. Výstupy jsou primárně určeny pro ovládání LED/halogenových svítidel, je na ně však možno připojit například ventilátory či jiná zařízení o nízkém výkonu závislém na dodaném napájecím napětí (dle zátěže 12 nebo 24 V DC). Regulace výstupů probíhá pomocí PWM modulace při frekvenci 244 Hz Při připojení dlouhých RGBW / RGB / onecolor LED pásků na výstup modulu, může docházet k úbytku napětí, což má za následek snížení jasu na vzdálených koncích pásků. Pro eliminaci tohoto jevu je doporučeno místo jednoho dlouhého pásku použít několik kratších pásků připojených paralelně. Jmenovitý výstupní příkon je uváděn pro součet všech výstupních svorek 12 A, pro jednotlivý kanál 6 A a maximální možné zatížení se uvádí 144 W / 12 V DC a 288 W / 24 V DC.

Vstupní kontakty jsou určeny pro řízení binární logikou pomocí kolébkových či mžikových spínačů, také však mohou být nakonfigurovány jako analogové vstupy s logikou 0 - 10 V. Analogové vstupy tak umožňují připojení externích snímačů (teplotní čidla, čidla vlhkosti, čidla kvality vzduchu, senzory okolního osvětlení, potenciometry pro ovládání atd.), které jsou svým výstupem kompatibilní s logikou 0 - 10 V. Čtení signálu z těchto snímačů probíhá na principu měření a diskrétního vyhodnocování hodnoty napětí na konkrétní svorce v rozmezí 0 - 10 V. Modul je schopen vyhodnotit změnu napětí ve většinové časti rozsahu s minimálním vzorkem cca 0,1 V ± 0,04. Vyhodnocování této hodnoty probíhá s nejmenší nastavitelnou periodou měření 1 s, kdy je vždy předán signál modulem do sítě Z-Wave. Zařízení je ve shodě s certifikacemi EMC 2004/108/EC a R&TTE 199/5/WE. Výstupním prvkem modulu jsou tranzistory.[24,28]

4.3.9 FGFS-101 - Fibaro detektor zaplavení

Detektor zaplavení FIB-FGFS-101 je univerzální snímač zaplavení, teploty a náklonu, který bezdrátově komunikuje pomocí protokolu Z-Wave a zároveň může signalizovat detekované stavy otevřením výstupních bezpotenciálových kontaktů ALARM NC a TAMP NC. Ty jsou určeny přímo pro připojení k zabezpečovací ústředně. Výrobce udává maximální přípustné proudové zatížení 25 mA a maximální napětí 40 V (AC nebo DC) na jednotlivý kontakt.

Detektor zaplavení je možno umístit na podlahu nebo na zeď (s použitím externí sondy zaplavení připojené kabelem ke kontaktům SENS1 a SENS2). Detektor má dále vestavěný snímač teploty snímající teplotu okolí/podlahy, výrobce udává přesnost jeho měření s tolerancí ±0,5 °C (v rozsahu 0 – 40 °C). Detektor je dále vybaven snímačem náklonu, který slouží nejen jako senzor přírůstku hladiny pod detektorem, ale i jako ochrana proti krádeži a přemístění modulu. Pro správnou funkci se detektor instaluje na nejnižší místo podlahy, kde se uvažuje o pravděpodobném stoku vody. Modul je navržen tak, že při významném zvýšení hladiny vody plave, a tudíž je eliminováno přerušení signalizace při havarijním zaplavení nebo poškození modulu. Detektor dokáže indikovat stav vestavěnou LED diodou ve třech barvách nebo akusticky miniaturní piezosirénou. Detektor může být napájen externím zdrojem 12 / 24 V DC nebo baterií (CR123A 3 V DC), při napájení z externího zdroje slouží baterie jako záložní zdroj (emergency mode). Je přítomna funkce automatické bezdrátové aktualizace softwaru. Zařízení je v souladu s EU normami EMC 2004/108/EC a R&TTE 199/5/WE. Výstupním prvkem modulu je bezpotenciálový rozpínací kontakt. [24,28]

4.3.10 FGSS-001/FGSD-002 - Fibaro detektor kouře

Fibaro FGSD-002 je univerzální optický detektor kouře s rádiovou komunikací Z-Wave. Optický princip detekce kouře zajišťuje citlivost na detekci raných stádií požáru, kdy ještě nedochází ke vzniku plamenů a nárůstu teploty, ale pouze k doutnání se vznikem kouře. Detektor je vybaven snímačem teploty s rozsahem měřených teplot -20 až 100 °C a přesností měření o toleranci ±0,5 °C (v rozsahu 0 – 55 °C), který může signalizovat překročení nastavených prahových hodnot teploty a slouží tak jako druhý jistící způsob detekce. Dále je též vybaven, jak tomu bývá u většiny podobných detektorů, ochranným kontaktem otevření krytu detektoru. Signalizace poplachu při zachycení kouře je předávána vestavěnou sirénou, indikační LED a přenosem poplachu sítí Z-Wave. Modul disponuje vestavěnou pamětí naměřených hodnot intenzity kouře a teplot pro budoucí možnou diagnostiku a analýzu, je napájen z baterie (CR123A 3 V DC) a je certifikován dle ČN EN 14604:2005 jako autonomní hlásič kouře vyhovující normě pro instalaci v obytných prostorách a rodinných domech pro tři úrovně citlivosti na kouř:

- 1. úroveň – 1,20 ± 0.5 % útlum / 0,25 m,

- 2. úroveň – 1,80 ± 0.5 % útlum / 0,25 m,
- 3. úroveň – 2,80 ± 0.5 % útlum / 0,25 m.

Pro správnou funkci se detektor instaluje na strop (či zeď) mimo rohy místností a mimo blízkosti nábytku, záclon či jiných předmětů. Již z podstaty principu optické detekce kouře je třeba detektor instalovat v prostředí bez prachu, kouře a kondenzující vodní páry.

Novější verze detektoru FGSD-002 nese od starší verze FGSS-001 několik odlišností:

- v modulu již není přítomna svorkovnice kontaktů
  - modul již nemá možnost napájení z externího zdroje (12/24 V DC)
  - modul již není schopen předávat signalizační stavy pomocí kontaktů relé (SMOKE NC a TAMP NC)
- automatický test detektoru je nyní prováděn s periodou 10 s (dříve 5 s)
- rozsah pracovní teploty modulu je rozšířený na 0 až 55 °C (dříve 0 až 40 °C)
- nově je uváděna pracovní vlhkost 0 až 93 %
- intenzita zvuku SPL (Sound pressure level) signalizace poplachu vestavěnou sirénou je nyní 85 dB / 3 m [24,28]

4.3.11 FGMS-001 - Fibaro detektor pohybu

Detektor pohybu FGMS-001 je vícefunkčním bateriovým detektorem/senzorem. Zastává funkci klasické PIR a také další senzorické funkce, jimiž jsou: měření teploty, měření intenzity jasu a měření otřesu. O detekovaných stavech, měřených veličinách a dalších stavech informuje modul řídící jednotku skrze Z-Wave protokol, kde se jeví jako 4 zařízení (PIR / senzor teploty / senzor intenzity světla / měření otřesu). Signalizace detekce pohybu a teploty je vizualizována barvou a svitem indikační LED diody. Vestavěný akcelerometr supluje funkci ochrany krytu detektorem otřesů při pokusu o sabotáž či odcizení. Při zachycení otřesů posílá modul zprávu řídící jednotce. Teoreticky jej lze využít i jako detektor otřesů půdy (zemětřesení).

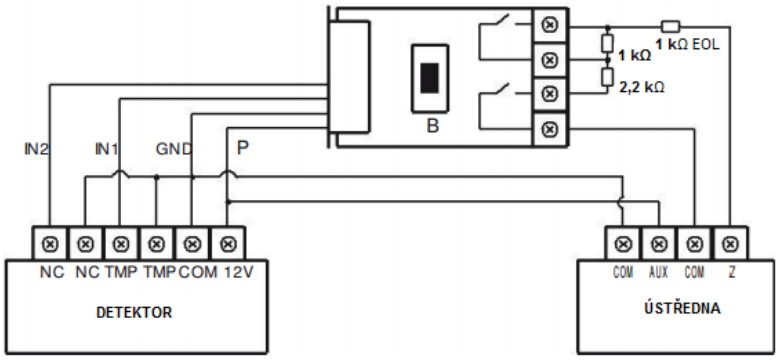
Pro správnou funkci, předejetí negativního ovlivnění dosahu detektoru či výskytu falešných poplachů se na tento PIR senzor váží stejná pravidla při jeho instalaci jako pro všechny ostatní detektory tohoto typu. Detektor pohybu musí být instalován osou detekční charakteristiky kolmo na směr předpokládaného pohybu osob (kolmo na směr průchodu dveřmi) dle udávaných prostorových detekčních charakteristik výrobcem (viz níže). Doporučená instalační výška je 2,4 m. Díky dodávanému držáku a kulatému tvaru detektoru je docíleno maximální variability nastavení detekčního zorného pole. Instalace je jednoduchá jedním šroubem na zeď, strop nebo na jakýkoliv povrch. [24,28]

Modul je napájen pouze bateriově (CR123A). Rozsah měřených teplot je udáván -20 až 100 °C s tolerancí vyhodnocování ±0,5 °C (v rozsahu 0 – 40 °C). Rozsah měření intenzity světla 0-32000 Lux. Podporuje také funkci dálkové aktualizace software. Zařízení je ve shodě s normami LVD 2006/95/WE, EMC 2004/108/WE, R&TTE 1999/5/WE, RoHS II. [24,28]

4.3.12 FGBS-001 - Univerzální binární senzor

Univerzální binární senzor je modul, jenž umožňuje připojení libovolného zařízení s bezpotenciálovým výstupem (tlačítka, spínače, detektory, relé atd.) na jeden ze svých dvou vstupů (IN1 a IN2). Zasílá informaci o změně stavu na vstupním kontaktu rádiovým protokolem Z-Wave a zároveň ji okamžitě předává v linii dál na své výstupní kontakty (OUT1 a OUT2). Modul má miniaturní rozměry, díky kterým je možno jej nainstalovat přímo do některého z krytů detektorů/snímačů pracujících na kontaktní logice a může tak být elegantně řešena jedna z forem integrace (tabulka několika typů konkrétních detektorů, do kterých je tento modul možné aplikovat viz Příloha 1). Nastavit jednotkou lze pak typy detekce NO/NC/MONOSTABLE/BISTABLE a přizpůsobit typu detektoru GENERIC/SMOKE/CO/CO2/HEAT/WATER. Dle obrázku níže je možné vřazení modulu do vyvážených smyček PTZS. **Takto provedené zapojení splňuje zachování normativních požadavků (dle normy ČSN CLC/TS 50 131) pro stupeň zabezpečení č. 2.**

Obr. 13 - Návrh zapojení detektoru a modulu Fibaro FGBS-001 pro účely integrace PTZS; Zdroj: [upraveno dle 24]



Modul umožňuje kromě snímání stavu dvou bezpotenciálových kontaktů také připojení až čtyř teplotních snímačů DS18B20 protokolem 1-Wire. Teploměry DS18B20 mají měřící rozsah -55 až 126 °C a mohou díky své digitální koncepci komunikovat po třech vodičích do uváděné vzdálenosti až 30 m. Připojují se ke svorkám TP (napájení), TD (data) a GND (zem). Modulu je určeno napájení 9 - 30 V DC ±10 % pomocí svorek (P a GND). Výstupním prvkem zařízení jsou bezpotenciálové kontakty (max. 150 mA, 36 V DC/24 V AC). [4,24,28]

4.3.13 FGK-101 až 107 - Magnetický kontakt

Tento modul je vyráběn jako bateriový detektor otevření dveří/oken/rolet/garážových vrat, plní však následně i další funkce. V modulu se nalézá klasický jazýčkový magnetický kontakt, který je otevírán oddálením magnetu od kontaktu, načež je odesílána poplachová informace. Magnet je dodáván v balení s tímto modulem. Modul se upevňuje pomocí šroubků vždy na statickou část průchodu, magnet stejným způsobem na pohyblivou část. Tyto dvě části smí být vzdáleny od sebe maximálně 5 mm.

Další možností modulu je připojit mezi jeho bezpotenciálové kontakty (IN a GND) libovolný externí spínač, kterým může být zvonkové tlačítko nebo jiný magnetický kontakt. Tento externí kontakt je připojen k internímu magnetickému kontaktu paralelně, z toho důvodu je ke správné funkci doporučeno používat jen jeden z těchto dvou kontaktů (při NC plní logickou funkci AND). Třetí možností je připojení číslicového teploměru (výhradně DS18B20) pomocí protokolu 1-Wire a doplnit funkci o měření teploty. Teploměr je pak při použití vhodného krytu možno instalovat všude, kde je vyžadováno přesné měření teploty, a to i v nestandartních podmínkách, například ve vlhkém prostředí, pod vodou či zalit v betonu. Připojuje se tří-žilovým kabelem o délce maximálně 30 m ke sběrnici 1-Wire (svorkám) modulu TP (napájení), TD (data) a GND (zem).

Na spodní straně modulu se nalézá tlačítko tamperu (TMP), které zároveň plní funkci B tlačítka pro přihlašování k jednotce. Na přední straně je kontrolka LED, která blikne pokaždé, když snímač detekuje změnu v přítomnosti magnetu. Modul používá baterii typu ER14250(1/2AA) o napětí 3,6 V. Modul je nabízen v několika barevných variantách krytu. [24,28]

5 Praktická realizace v typickém objektu

Pro názornou ukázku byly sestaveny tři modely instalací poplachového zabezpečovacího a tísňového systému (PTZS). Vzorovým objektem pro všechny tři případy se stal menší jednopatrový rodinný dům o ploše zástavby cca 100 m^2. Všechny tři verze jsou sestaveny bez ohledu na případnou certifikaci, jde pouze o funkční návrh realizace. Jsou navrženy tři modely realizací:

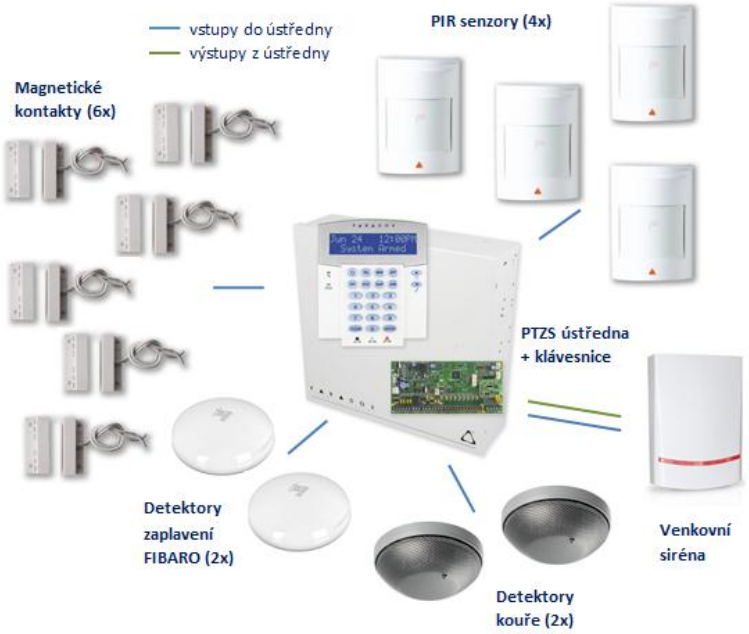
- standardní instalace PTZS,
- systém Fibaro s jeho vlastními detektory,
- standardní instalace PTZS s integrací do systému Fibaro.

5.1 Standardní instalace PTZS

Základ této realizace je postaven na smyčkové ústředně série Spectra, která je součástí setu nabízeného dodavatelem elektronických systémů budov Variant. Součástí tohoto balíku je i přístupová klávesnice s dvouřádkovým LCD displejem (schopna programování ústředny) a plechový ochranný box. Součástí ústředny je telefonní a IP komunikátor. Všechny detektory jsou k ústředně připojeny drátově logikou NC s ATZ a EOL odporem (viz Příloha 9). Model realizace se skládá z těchto komponent:

- set ústředny, boxu a klávesnice – SP6000/R + BOX S-40 + K32LCD,
  - 2 x 8 zón, 4 x PGM výstup, telefonní komunikátor,
  - klávesnice s LCD displejem,
- venkovní zálohovaná siréna – BLADE 01,
- 4x pohybový detektor – PARADOX PRO PLUS 476,
- 6x magnetický kontakt – FM-106,
- 2x detektor zaplavení – Fibaro FGFS-101 (umožňuje drátové připojení k PTZS),
- 2x detektor kouře – CT-3001O.

Obr. 14 - Návrh standardní instalace PTZS; Zdroj: [vlastní]



5.2 Systém Fibaro s jeho vlastními detektory

Tento model je sestaven na základě systému domácí automatizace Fibaro dodávaného distributorem Yatun s.r.o. Tento systém nabízí kromě mnoha užitečných funkcí i možnost vytvoření zabezpečovacího systému pomocí vlastních detektorů (viz kapitola 4.3.3). Roli ústředny může zajistit jedna ze dvou řídících jednotek Fibaro, v tomto případě je vybrána ekonomičtější varianta Fibaro HC Lite. Detektory jsou k řídící jednotce (zabezpečovací ústředně) připojeny bezdrátově protokolem Z-Wave (spolehlivost tohoto přenosu je řešena v následující kapitole). Navržený model realizace se skládá se z těchto komponent:

- řídící jednotka – Fibaro HC Lite,
- ochranný plechový kryt – BOX M,
- zálohovaný zdroj napětí – BP12-18,
- venkovní zálohovaná siréna – BLADE 01,
- 4x pohybový detektor – Fibaro FGMS-001,
- 6x magnetický kontakt – Fibaro FIB-FGK-101,
- 2x detektor zaplavení – Fibaro FIB-FGFS-101,
- 2x detektor kouře – Fibaro FGSD-002,
- GSM komunikátor – David GD-04,
- „inteligentní“ klávesnice – Entry E KR11,
- 2x univerzální binární modul – FIB-FGBS-001.

Obr. 15 - Systém Fibaro s jeho vlastními detektory; Zdroj: [vlastní]

Řídící jednotka Fibaro HC Lite (stejně jako její alternativa HC2) dokáže posílat bezplatné SMS zprávy přes internet. Tato funkce by teoreticky mohla plnit funkci připojení k pultu centralizované ochrany (PCO) vyžadovaného normou, avšak je zde otázkou možné funkční splnění těchto norem. Jako bezpečné připojení k PCO je distributorem doporučováno řešení připojením externího GSM komunikátoru DAVID GD-04 některým z kontaktních výstupů (například pomocí reléového spínacího modulu FGS-221). GSM komunikátor je i s modulem umístěn v plechovém boxu o dostatečných rozměrech, který je vybaven ochranou proti sabotáži (tamperem). Tato ochrana je připojena na další Univerzální binární modul, který se nachází také v ochranném boxu. Pro zesílení signálu je nutné vyvést obě antény (Z-Wave vysílače a GSM komunikátoru) ven z tohoto boxu.

Venkovní siréna požadovaná normou je k systému napojena skrze stejný modul (FGS221) jako je připojen komunikátor. Při poplachové události vyvolané systémem Fibaro bude siréna reagovat na rozepnutí výstupního bezpotenciálového kontaktu modulu umístěného v plášti sirény. Zároveň je na detekci sabotáže sirény společně se signalizací nízkého stavu její záložní baterie připojen Univerzální binární modul informující systém Fibaro o těchto změnách.

K řízení přístupu je zvolena Klávesnice Entry E KE11. Tu je možno připojit taktéž skrze Univerzální binární modul na jeden z výstupů klávesnice (NC). Je ovšem nutné tento binární senzor vyřadit z alarmu, protože systém Fibaro automaticky zahrnuje všechny takto napojené moduly jako součást svého bezpečnostního systému. K modulům pro připojení GSM komunikátoru, sirény a klávesnice je nutné omezit přístup uživatelům dle příslušné úrovně (ČSN CLC/TS 50 131-1).

Záložní napájení (baterie) potřebné k udělení certifikace (jak o něm hovoří norma ČSN CLC/TS 50 131-6) není distributorem doposud nabízeno. U jednotky HC-Lite je uveden modul zálohovací baterie v přípravě (společně s modulem vlastního GSM komunikátoru). Řídící jednotku Fibaro HC Lite je třeba napájet 12 V / 1 A, k čemu postačí napájecí zdroj BP12-18 splňující tyto požadované certifikace. Kapacita záložní baterie tohoto zdroje je uváděna 7 – 26 Ah. Záložní zdroj je nutné opatřit výstupním konektorem pro malá napětí o rozměrech 5,5 / 2,1 mm.

5.3 Standardní instalace PTZS s integrací do systému Fibaro

Třetí model realizace vychází z prvního navrženého řešení (se základem postaveným na smyčkové ústředně série Spectra) s tím rozdílem, že funkci zabezpečovacího systému plní výhradně systém PTZS Spectra a systém Fibaro slouží jako podřízený systém vykonávající funkce automatizace domácnosti – „inteligentní domácnosti“.

Realizace je tvořena z těchto zařízení:

- set ústředny, boxu a klávesnice – SP6000/R + BOX S-40 + K32LCD,
  - 2 x 8 zón, 4 x PGM výstup, telefonní komunikátor,
  - klávesnice s LCD displejem,
- venkovní zálohovaná siréna – BLADE 01,
- 4x pohybový detektor – PARADOX PRO PLUS 476,
- 6x magnetický kontakt – FM-106,
- 2x detektor zaplavení – Fibaro FGFS-101 (umožňuje drátové připojení k PTZS),
- 2x detektor kouře – CT-3001O,
- řídící jednotka Fibaro HC Lite,
- 11x univerzální binární modul - FIB-FGBS-001.

Obr. 16 - Standardní instalace PTZS s integrací do systému Fibaro; Zdroj: [vlastní]

Na informační vedení jsou mezi jednotlivé detektory a ústřednu vřazeny speciální moduly (Univerzální binární modul) umožňující vyhodnocování změn stavů na tomto vedení a jejich následný přenos po Z-Wave. O změnách stavů na detektorech je tedy informována ústředna PTZS a zároveň jednotka systému Fibaro. Univerzální binární modul může být díky svým rozměrům instalován do mnoha detektorů PTZS, v čemž spočívá elegantní princip integrace těchto dvou systémů. Umístěním modulu do pláště detektoru s ochranou proti sabotáži (tamper) se přenese ochrana i na tento modul. Moduly jsou k ústředně připojeny smyčkami NC s ATZ a EOL odporem (viz Příloha 9).

O změnách stavů PTZS Spectra bude systém Fibaro informován PGM výstupy a též prostřednictvím Univerzálních binárních senzorů. Jelikož PGM ústředna Spectra SP6000/R disponuje čtyřmi binárními výstupy, z čehož byl jeden výstup vyhrazen pro sirénu, nabízí se přenositelnost až 8 volitelných informací (zastřežení, poplach na určité zóně, odstřežení konkrétním uživatelem atd.).

Součástí balíku nabízené firmou Variant s.r.o. je přístupová klávesnice (schopna programování ústředny) a plechový ochranný box. Ústředny v sobě zahrnuje telefonní a IP komunikátor. Vybraný box je dostatečně rozměrný pro umístění řídící jednotky Fibaro HC Lite přímo do jeho prostor, je však nutné vyvést anténu ven z boxu pro zvýšení signálu sítě Z-Wave.

Co se týče zde zvolených PIR senzorů a detektorů kouře, jsou moduly systému Fibaro vloženy přímo do plášťů detektorů. Odlišná je situace u magnetických kontaktů, kam není možno, kvůli rozměrům jejich pláště, moduly instalovat. Modul bude muset být instalován do zvláštního krytu mimo detektor.

Siréna je zapojena standardně na jeden z PGM výstupů ústředny skrze Univerzální binární modul a EOL odpor. Ochranné výstupy ze sirény (detekce sabotáže sirény a signalizace nízkého stavu záložní baterie sirény) jsou připojeny na vstupní smyčku ústředny skrze jeden Univerzální binární modul, který je umístěn uvnitř pláště venkovní sirény zapojením NC s ATZ a EOL odporem.

5.4 Cenová kalkulace

Pro tři modely realizací je sestavena cenová kalkulace do tabulek. Ceny uvedené v kalkulaci vycházejí z cen uvedených na webových katalozích k datu 24. 3. 2016. Především se jedná o tyto katalogy:

- https://www.yatun.cz/produkty/smarthome-fibaro/,
- http://www.variant.cz/dokumenty/obor-ezs/.

Následně je pak připočtena aktuální daň z přidané hodnoty (21 %) a posléze je naceněna konkrétní realizace s ohledem na množství jednotlivých komponent. Tato cena nezahrnuje cenu za práci instalace, oživení systému ani marži instalační firmy.

Tab. 10 - Finanční kalkulace standardní instalace PTZS; Zdroj: [vlastní]

Název	Množství [ks]	Cena za kus bez DPH [Kč]	Cena celkem bez DPH [Kč]	**Cena celkem s DPH [Kč]**
SP6000/R + BOX S-40 + K32LCD (set ústředny, boxu a klávesnice)	1	5 885,00	5 885,00	**7 120,85**
BLADE 01 (venkovní zálohovaná siréna)	1	1 380,00	1 380,00	**1 669,80**
PARADOX PRO PLUS 476 (PIR detektor)	4	327,00	1 308,00	**1 582,68**
FM-106 (dveřní kontakt)	6	71,00	426,00	**515,46**
Fibaro FGFS-101 (detektor zaplavení)	2	1 364,00	2 728,00	**3 300,88**
CT-3001O (detektor kouře)	2	1 667,00	3 334,00	**4 034,14**
VL 04-4x0,22/100 (kabeláž 100 m)	1	1 008,00	1 008,00	**1 219,68**
	Cena celkem:	11 702,00	16 069,00	**19 443,49**

Tab. 11 - Finanční kalkulace instalace systému Fibaro s jeho vlastními detektory; Zdroj: [vlastní]

Název	Množství [ks]	Cena za kus bez DPH [Kč]	Cena celkem bez DPH [Kč]	**Cena celkem s DPH [Kč]**
Fibaro HC Lite (řídící jednotka/ústředna)	1	6 347,00	6 347,00	**7 679,87**
BOX M (ochranný plechový box)	1	499,00	499,00	**603,79**
BP12-18 (zálohovaný zdroj napětí)	1	1 042,00	1 042,00	**1 260,82**
BLADE 01 (venkovní zálohovaná siréna)	1	1 380,00	1 380,00	**1 669,80**
Fibaro FGMS-001 (PIR detektor)	4	1 322,00	5 288,00	**6 398,48**
Fibaro FIB-FGK-101 (dveřní kontakt)	6	1 140,00	6 840,00	**8 276,40**
Fibaro FGFS-101 (detektor zaplavení)	2	1 364,00	2 728,00	**3 300,88**
Fibaro FGSD-002 (detektor kouře)	2	1 479,00	2 958,00	**3 579,18**
David GD-04 (GSM komunikátor)	1	2 582,00	2 582,00	**3 124,22**
Entry E KR11 (přístupová klávesnice)	1	3 018,00	3 018,00	**3 651,78**
Fibaro FGS-221 (releyový modul)	2	1 364,00	2 728,00	**3 300,88**
Fibaro FGBS-001 (univerzální binární modul)	3	909,00	2 727,00	**3 299,67**
	Cena celkem:	22 446,00	38 137,00	**46 145,77**

Tab. 12 - Finanční kalkulace standardní instalace PTZS s integrací do systému Fibaro; Zdroj: [vlastní]

Název	Množství [ks]	Cena za kus bez DPH [Kč]	Cena celkem bez DPH [Kč]	**Cena celkem s DPH [Kč]**
SP6000/R + BOX S-40 + K32LCD (set ústředny, boxu a klávesnice)	1	5 885,00	5 885,00	**7 120,85**
BLADE 01 (venkovní zálohovaná siréna)	1	1 380,00	1 380,00	**1 669,80**
PARADOX PRO PLUS 476 (PIR detektor)	4	327,00	1 308,00	**1 582,68**
FM-106 (dveřní kontakt)	6	71,00	426,00	**515,46**
Fibaro FGFS-101 (detektor zaplavení)	2	1 364,00	2 728,00	**3 300,88**
CT-3001O (detektor kouře)	2	1 667,00	3 334,00	**4 034,14**
Fibaro HC Lite (řídící jednotka/ústředna)	1	6 347,00	6 347,00	**7 679,87**
Fibaro FGBS-001 (univerzální binární modul)	12	909,00	10 908,00	**13 198,68**
VL 04-4x0,22/100 (kabeláž 100 m)	1	1 008,00	1 008,00	**1 219,68**
	Cena celkem:	18 958,00	33 324,00	**40 322,04**

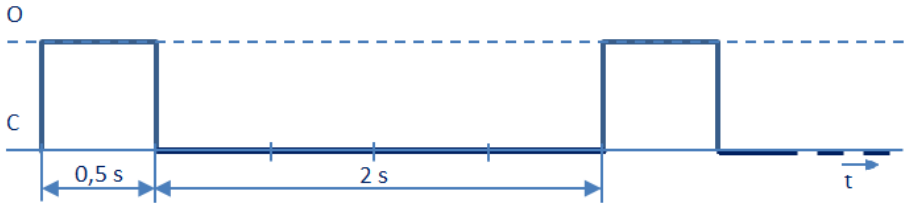
6 Ověření reálné funkce a parametry provozu

V podkapitolách normy ČSN CLC/TS 50 131 (viz Příloha 8) jsou podrobně vypsány jednotlivé náležitosti potřebné ke splnění certifikace PTZS příslušného stupně. Pro ověření reálné funkce a parametrů provozu je podstatná část ČSN CLC/TS 50 131-3 (ústředny), kde je uvedena tzv. funkční zkouška. Ta se skládá z vysílání signálů nebo zpráv (tísňových, o narušení, sabotážních) na vstup ústředny a z monitorování, zda byly tyto signály zpracovány během požadované doby a zda aktivovaly správné hlášení.

Této zkoušce byl podroben zapůjčený systém Fibaro. Konkrétně byla ověřena spolehlivost přenosu mezi detektorem (Univerzální binární modul) a ústřednou (řídící jednotka HC2). Byl vysílán stanovený počet signálů (změn stavů na detektoru) a následně byla vyhodnocena schopnost ústředny patřičně vyhodnotit tento přenos. Zkouška byla provedena s pomocí sestaveného zařízení (viz Příloha 3) pro testování spolehlivosti přenosu binárních zpráv po síti Z-Wave.

Zařízení pomocí relé řízeného mikrokontrolerem ATmega (Arduino) simulovalo periodické rozepínání a spínání bezpotenciálového kontaktu jednoho ze vstupů Univerzálního binárního modulu (NC vůči zemi). Počet cyklů (otevření/zavření kontaktu) byl u každého měření stanoven na 100 – celkem tedy 200 změn stavu. Jeden cyklus (viz Obr. 17) znamená periodickou událost, kdy je bezpotenciálový kontakt vždy 0,5 s otevřen (signál detekce narušení) a další 2 s uzavřen (klidový stav).

Obr. 17 - Průběh jednoho cyklu (periody) vysílaného signálu při testování; Zdroj: [vlastní]

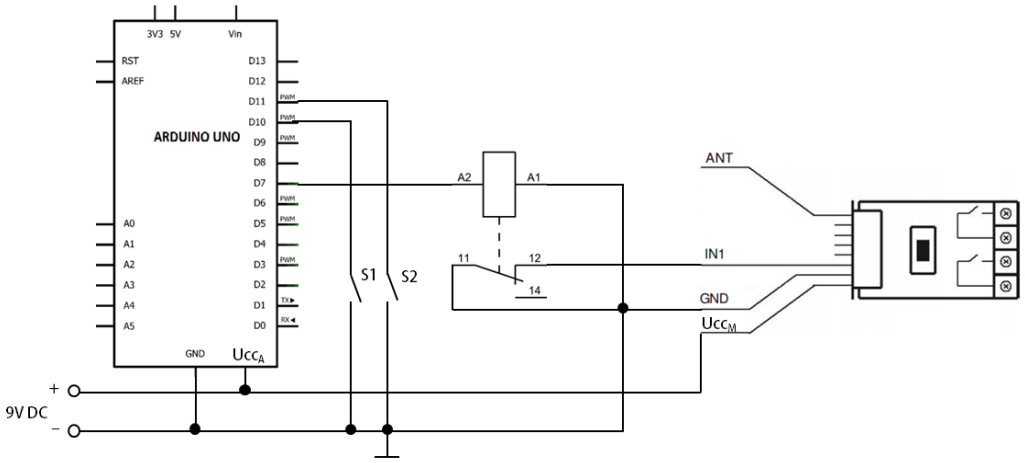


Zařízení se skládá z těchto součástí:

- vývojová deska Arduino Uno,
- Fibaro Univerzální binární senzor,
- relé SRD-05VCD-SL-C,
- 2x spínací kontakt (pro ovládání spouštění cyklu),
- vstup pro stabilizované napětí 9 V.

Všechny tyto součásti jsou propojeny pomocí nepájivého pole a pevně uchyceny společně s deskou Arduino do jednoho celku tak, aby mohly plnit funkci bezdrátového testovacího zařízení. Prve bylo zařízení koncipováno jako zcela bezdrátové (k napájení byla určena 9 V baterie), avšak pro zajištění spolehlivosti překlápění relé bylo k napájení užito stejnosměrného stabilizovaného zdroje napětí ze sítě. Zapojení testovacího zařízení je znázorněno v obrázku níže.

Obr. 18 - Schéma zapojení testovacího zařízení; Zdroje: [vlastní]



Testovací zařízení pracuje tak, že nahraný jednoduchý program (viz Příloha 4), vytvořený jazykem Wiring v Arduino IDE, čte ve smyčce dıgıtalnı hodnotu na portech D11 a D12, kde jsou umístěna tlačítka. Po příchodu náběžné hrany na vstupu D11 (propojení se zemí stisknutím tlačítka S1) se rozepne relé do okamžiku, než je tlačítko na tomto portu uvolněno. Toto tlačítko tak slouží pouze pro ozkoušení funkce testovacího zařízení. Po propojení portu D12 se zemí (stiskem tlačítka S2) se spustí testovací sekvence o 100 cyklech (tak, jak je popsáno výše). Průběh této sekvence lze kdykoliv přerušit opětovným stisknutím a podržením tlačítka S2 cca na 2 sekundy.

6.1 Parametry funkční zkoušky

Měření do 10 m bylo prováděno ve vnitřních prostorách Technické fakulty ČZU při standardních pokojových podmínkách. Byly zde prováděny zkoušky přenosu o těchto vzdálenostech:

- 2 m,
- 10 m.

U tohoto prostředí se testovaly také různé typy ovlivnění přenosu:

- přímý dohled,
- skrz dřevěné dveře,
- skrz cihlovou zeď.

V těchto vnitřních prostorách byla navíc provedena zkouška spolehlivosti přenosu na vzdálenost 10 m s přímým dohledem, avšak ovlivňovaného vytvářením umělého elektromagnetického ruchu pomocí RF klíčenky (dálkový ovladač otevírání dveří automobilu – Škoda Yeti). RF klíčenka byla umístěna aktivní mezi trasu přenosu obou antén.

Dále byla vykonána zkouška ve venkovních prostorách před Technickou fakultou ČZU při teplotě 9 °C, nulových srážkách a vlhkosti vzduchu 63 %. Uskutečnilo se zde pouze měření při přímé viditelnosti obou antén a to o vzdálenostech:

- 10 m,
- 20 m,
- 30 m.

Kvůli nedostačujícímu prostoru potřebného pro vykonání zkoušky (dle návodu zařízení je uváděn dosah zařízení do 50 m ve venkovních prostorách) a předpokládané zvýšené přítomnosti elektromagnetického ruchu před prostorami Technické fakulty ČZU, byla navíc provedena zkouška v náhradním venkovním prostředí. Náhradní zkouška byla provedena na fotbalovém hřišti na okraji obce Podlesí ve Středočeském kraji, kde byl k dispozici vhodnější prostor a předpokládán minimální výskyt elektromagnetického ruchu. Měření probíhalo o teplotě vzduchu 16 °C, nulových srážkách a vlhkosti vzduchu 39 %. Měřilo se opět pouze při přímé viditelnosti obou zařízení při těchto vzdálenostech:

- 30 m,
- 40 m,
- 50 m.

6.2 Postup funkční zkoušky

Každé měření začíná promazáním logu událostí v uživatelském rozhraní Fibaro (viz Příloha 7). Dále jsou překontrolovány podmínky přenosu a stav obou zařízení a poté je spuštěn tester, který vyšle jednotce jednu sekvenci cyklů. Přenos jedné této sekvence trvá déle než 4 min. Po vyslání celé testovací sekvence jsou všechny události zaregistrované jednotkou zaznamenány v logu událostí do řádků. Řádky odpovídající době měření je nutné překopírovat do připravené excelové tabulky, jejíž součástí je připravené makro, které automaticky přeformátuje vložený log událostí na protokol o prováděném měření do nového listu excelového sešitu s příslušným názvem. Součástí protokolu je údaj o počtu událostí (změnách stavů na kontaktu) logovaných jednotkou. Tento údaj je stěžejní pro zhodnocení výsledků funkční zkoušky.

6.3 Výsledky funkční zkoušky

Z makrem vygenerovaných výsledků v protokolech byla sestavena tabulka shromažďující všechny naměřené hodnoty. Tabulka je logicky uspořádána tak, jak bylo definováno v kapitole viz výše. Pro každou definovanou zkoušku udává 3 výsledky z měření tak, jak byly prováděny po sobě. Ty udávají počet signálů vyhodnocených jednotkou jako potenciální události hodnocené jako poplach. V posledním sloupci je vypočten poměr správně vyhodnocených signálů jednotkou, tedy údaj vypovídající o spolehlivosti přenosu informace při daném měření.

Tab. 13 - Výsledky funkční zkoučky; Zdroj: [vlastní]

	Vzdálenost [m]	Popis zkoušky	Počet signálu zaznamenaných jednotkou [-]			Poměr správně vyhodnocených signálu [%]
			č. 1	č. 2	č. 3	
Vnitřní prostor (uvnitř TF ČZU)	**2**	Přímý dohled	200	200	200	**100,0**
		Skrze dřevěné dveře	200	200	200	**100,0**
		Skrze zeď	192	186	196	**95,7**
	10	Přímý dohled	200	200	200	**100,0**
		Skrze dřevěné dveře	196	200	200	**99,3**
		Skrze zeď	200	200	200	**100,0**
Venkovní prostor (před TF ČZU)	**10**	Přímý dohled	200	194	200	**99,0**
	20	Přímý dohled	198	200	200	**99,7**
	30	Přímý dohled	184	198	198	**96,7**
Venkovní prostor (fotbalové hřiště)	**30**	Přímý dohled	200	200	200	**100,0**
	40	Přímý dohled	200	200	200	**100,0**
	50	Přímý dohled	200	198	198	**99,3**
Vnitřní prostor (uvnitř TF ČZU)	**10**	Přímý dohled, zarušováno RF klíčenkou	176	44	59	**46,5**

6.4 Parametry provozu

Byly zkoumány i další parametry důležité pro užití systému Fibaro jako potenciální PTZS. Těmito parametry jsou:

- pokud přenos proběhl, byla doba reakce na všechny události vyslané testovacím zařízením do 0,5 s,
- na každou událost hodnocenou jako událost detekce narušení je možné navázat poplachový stav systému, ta pak může reagovat spuštěním scény aktivací signalizačních zařízení,
- paměť záznamů v logu událostí Fibaro je větší než 250 událostí s datem trvanlivosti delším jak 30 dní,
- dostupnost propojení bezdrátových detektorů je periodicky kontrolována.

7 Zpracování a vyhodnocení výsledků

V této kapitole bude zhodnocena praktická realizace a vyhodnocena funkční zkouška.

7.1 Zhodnocení praktické realizace

Pro praktickou realizaci byly sestaveny tři modely pro potenciální instalace PTZS do rodinného domu. Cenové kalkulace jsou shrnuty v kapitole výše.

V prvním případě se jednalo o model standardní instalace PTZS, kde bylo užito zabezpečovací ústředny řady Spectra a detektorů spolu s náležitostmi PTZS připojených drátově do smyček. Tato realizace při dodržení náležitých instalačních postupů dosahuje certifikace stupně zabezpečení 2. Jako velice pozitivní je zde hodnoceno hledisko ceny a ověřená spolehlivost této realizace. Jedná se však o systém minimálně schopný interakce s dalšími zařízeními (integrace). Je možné využít pouze 3 volné PGM výstupy ústředny a informace z přítomného telefonního/IP komunikátoru.

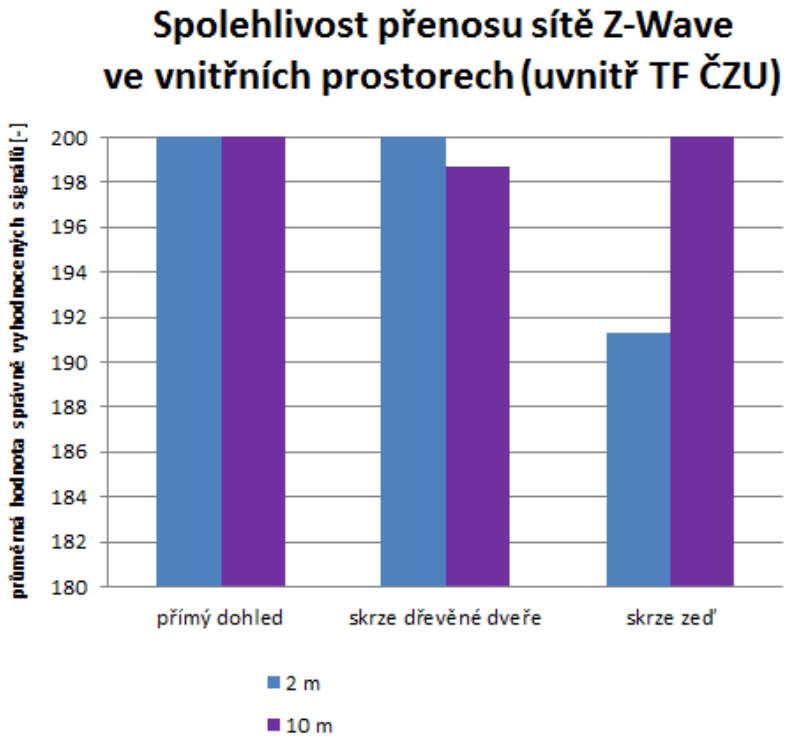
Ve druhém případě šlo o model realizace s použitím systému Fibaro (Fibaro HC Lite) jako ústředny s jeho vlastními detektory. Ty jsou všechny k jednotce připojeny bezdrátově pomocí protokolu Z-Wave (jehož spolehlivost přenosu bude hodnocena níže). Jedná se dosud o necertifikovaný systém (stupeň bezpečnosti je roven nule), tudíž případné požadavky ke splnění podmínek pro uzavření pojistky v tomto systému najít nelze. Cena tohoto systému oproti první variantě je více jak dvojnásobná. To je dáno především bezdrátovou koncepcí detektorů, které i v konvenčních PTZS navyšují cenu celkové realizace. Jako výhoda tohoto systému se jeví zakomponování takto vytvořeného PTZS do systému „chytré domácnosti“, se kterým lze u daného objektu velice navýšit hodnoty komfortu a ekonomičnosti (ekologičnosti). To však bohužel na úkor bezpečnostního hlediska. Jako další pozitivní přínos tohoto řešení hodnotím jednoduchost instalace detektorů, avšak s nutností připojení dalších periferií pro splnění funkce PTZS (přístupová klávesnice, siréna a GSM komunikátor) pomocí speciálních modulů.

Třetí varianta modelu je založena na klasické smyčkové ústředně řady Spectra, která spadá svou certifikací do stupně zabezpečení 2 (nízké až střední). Jedná se o stejnou ústřednu jako v případě prvního modelu se stejnými užitými detektory. Rozdíl je v tom, že celá realizace je obohacena o integraci PTZS se systémem Fibaro pomocí modulů (Univerzální binární senzor). Ty jsou připojovány na jednotlivé smyčky k detektorům (ideálně přímo do krytů pro zahrnutí ochrany proti sabotáži), výsledkem čehož je umožněna informační vazba s přítomnou řídící jednotkou Fibaro o změnách stavů na takto připojených detektorech. Celý systém tak může využívat všechny komfortní a spořící funkce přinášející systém Fibaro, stejně jako v druhém modelu realizace, a zároveň je objekt zastřežen PTZS, stejně jako v prvním modelu. Navíc systém Fibaro může čerpat doplňující

informace z ústředny Spectra skrze PGM výstupy. Pokud jde o cenu, tato realizace vychází dokonce o několik tisíc korun levněji oproti druhému modelu (není uvedena cena za práci, jedná se o cenu za komponent v daném množství). Jako negativum tohoto modelu hodnotím nemožnost využít vyvažovacích odporů instalovaných před Univerzální binární modul z důvodu neschopnosti tohoto modulu číst jeho vstupy analogové hodnoty. Tento problém lze obejít umístěním těchto modulů do krytů detektorů pod tamper, čímž se zabezpečí celý tento modul i část vedení mezi jím a detektorem. Jiná situace je u instalace magnetického kontaktu, kam se tento modul ve většině případů nevejde a je nutné pro něj připravit speciální kryt s ochranou proti sabotáži. Další negativní stránkou tohoto modelu je dosavadní absence certifikace tohoto modulu a větší nároky na technické zpracování této realizace.

7.2 Výsledky funkčních zkoušek

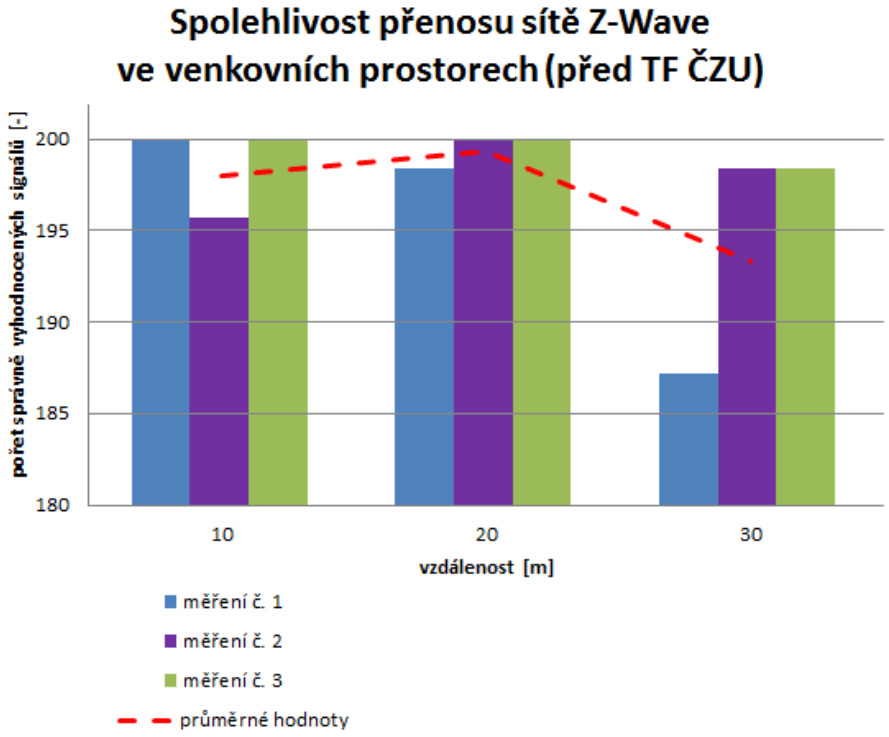
Naměřené výsledky funkčních zkoušek byly zpracovány dle tabulky (viz Tab. 13) pro tři prostředí. Pro přehlednost výsledků byl použit sloupcový typ grafu. Svislá osa všech grafů byla oříznuta na minimum 180 správně vyhodnocených signálů pro lepší zřetelnost výsledků. U prvního grafu byl na svislou osu vynesen aritmetický průměr z jednotlivých šesti zkoušek a sloupce byly rozděleny do skupin dle typu ovlivnění přenosu.



Obr. 19 - Spolehlivost přenosu sítě Z-Wave ve vnitřních prostorech (uvnitř ČZU TF); Zdroj: [vlastní]

Z tohoto grafu je jasně patrné, že zkoušky spolehlivosti přenosu skrze zeď proběhly za nestejných podmínek měření (odlišný materiál zdi). Přesto je viditelná další nuance, patrná ze skutečnosti, že zkouška přenosu skrze dřevěné dveře měla horší výsledek než zkouška přenosu na stejnou vzdálenost (10 m) skrze zeď. Tato skutečnost je odůvodněna odlišností místa provádění zkoušky v budově, kde byl pravděpodobně v odlišné míře přítomen další element ovlivňující výsledky zkoušek (zvýšený výskyt elektromagnetického rušení).

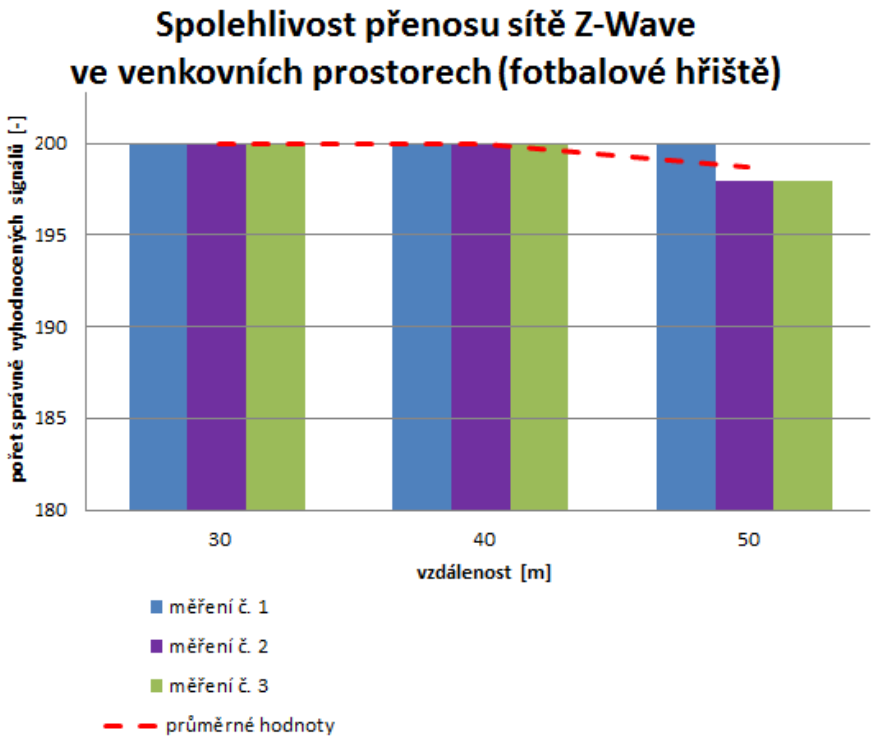
Do grafů z venkovních prostor jsou vyneseny naměřené hodnoty dle tabulky (viz Tab. 13) ve sloupcích, vždy po skupinách třech měření z jedné prováděné zkoušky v daném prostředí a vzdálenosti. O regresivním průběhu těchto prováděných zkoušek pak hovoří červená přerušovaná křivka. Ta je sestrojena z průměrných hodnot zkoušek závislých na vzdálenosti prováděného měření.



Obr. 20 – Spolehlivost přenosu sítě Z-Wave ve venkovních prostorech (před ČZU TF); Zdroj: [vlastní]

Při prováděné zkoušce na 10 m se u druhého měření nepodařilo řídící jednotce správně zachytit celou sekvenci signálů. Měření prokázalo 4 nepřenesené stavy. To se promítá na degradaci průměrné spolehlivosti této zkoušky na 99 %. U zkoušky na 20 m se projevila chyba dvou nepřenesených stavů hned v prvním měření, což má za následek průměrnou spolehlivost 99,7 %. Zkouška spolehlivosti na 30 m se projevila nejhůře, a to celkem 20 nepřenesenými stavy a z toho vyplívající spolehlivosti 96,7 %. Červená regresní křivka v grafu vystihuje nekorelující vztah průměrné hodnoty spolehlivosti přenosu s rostoucí vzdáleností přenosu, jak by bylo logicky předpokládáno. Tento

diskutabilní výsledek zkoušek je opět přisuzován výskytu elektromagnetického ruchu v okolí TF ČZU.



Obr. 21 - Spolehlivost přenosu sítě Z-Wave ve venkovních prostorech (fotbalové hřiště); Zdroj: [vlastní]

Zkoušky prováděné mimo území TF ČZU přinesly pro systém Fibaro pozitivnější výsledky, jelikož byly prováděny v místě s evidentně nižším výskytem elektromagnetického ruchu. Zkoušky na 30 m a 40 m proběhly se 100 % úspěšností, tedy vyhodnocením všech signálů zaslaných řídící jednotce pomocí testovacího zařízení s nulovou chybou. U zkoušky na 50 m se však vyskytla celková chyba čtyř neúspěšně přijatých signálů jednotkou, z čehož vychází 99,3 % spolehlivost přenosu systému Fibaro na tuto vzdálenost. V dodávaných návodech u zařízení se uvádí jejich dosah až do 50 m, což přibližně odpovídá tomuto měření, avšak pro užití systému Fibaro jako potenciální PTZS (použitím řídící jednotky Fibaro HC2 jako ústředny PTZS) i taková míra spolehlivosti je nepřípustná.

V posledním řádku tabulky (viz Tab. 13) jsou přítomny výsledky doplňujícího měření o spolehlivosti přenosu při vytváření umělého elektromagnetického rušení (úmyslném zarušováním trasy přenosu RF klíčenkou). Ty hovoří o jasném vlivu elektromagnetického ruchu na spolehlivost komunikace zařízení Fibaro.

8 Doporučení a finanční zhodnocení

Tři modely realizací PTZS jsou přehledně shrnuty spolu s finanční kalkulací výše (viz kapitola 5.4). Nejlevněji a z hlediska norem bez problémů vyšel první model, avšak s minimální integrační schopností. Ta je omezena schopností komunikace jednotky pouze na výstupy tři PGM (8 možných přenositelných stavů. Tento model byl uveden záměrně pro porovnání s dalšími řešeními.

Oba modely v sobě zahrnují integrační řešení systémem Fibaro. Rozdíl je v přístupu k realizaci PTZS tohoto modelu. Ta je u druhého modelu omezena pouze na firemní řešení Fibaro a nutné zařízení pro správnou funkci PTZS (přístupová klávesnice, venkovní siréna, komunikátor pro připojení na PCO, záložní zdroj). Tento systém vychází překvapivě nejdráž, především kvůli vysoké ceně detektorů (magnetický kontakt, PIR). Tento model nevlastní certifikaci a pravděpodobně by bylo velice nákladné ji získat, protože by bylo nutné certifikovat nejen jednu z řídících jednotek, ale i detektory a moduly potřebné k realizaci PTZS dle normy ČSN CLC/TS 50 131:2007. Jak je dokázáno provedením funkčních zkoušek (viz Tab. 13) v této diplomové práci, má tento systém velice diskutabilní spolehlivost komunikace (Z-Wave) danou ovlivnitelností vyskytujícího se elektromagnetického rušení (tak jako prakticky u všech systémů využívající pro přenos ISM pásma).

V případě realizace PTZS dle třetího modelu uvedeného v této práci (standardní instalace PTZS s integrací do systému Fibaro) není třeba uvažovat o bezpečnostních rizikách způsobených tímto jevem, protože tento model užívá pro vykonávání bezpečnostních funkcí drátové vedení a bezdrátový přenos po síti Z-Wave je používán pouze pro doplňující funkce automatizace budovy. Tuto variantu hodnotím jako velice pozitivní a to i vzhledem k finanční úspoře oproti modelu realizace PTZS pomocí systému Fibaro s jeho vlastními detektory.

Z výsledků funkčních zkoušek je patrný přímý vliv prostředí, v němž je zkouška prováděna. Konkrétní vliv je přisuzován vyskytujícímu se elektromagnetickému ruchu, který je v pásmu ISM (konkrétně 868 MHz) více přítomný v místech se zvýšeným technickým provozem, kde je užíváno bezdrátových technologií používající pro přenos stejné pásmo. Ukázkovým příkladem zvýšeného provozu takových technologií, mající za následek zahlcení tohoto pásma, je právě prostor okolí Technické fakulty České zemědělské university v Praze, kde byly některé zkoušky prováděny.

Pokud by se uvažovalo o skutečné realizaci PTZS pomocí systému Fibaro ovšem nikterak necertifikovaného systému (dle druhého modelu), bylo by vhodné ověřit přítomnost výskytu elektromagnetického ruchu v okolí objektu již během nalézaní performačních indikátorů, a to ještě před projektovou fází realizace. Přístroj, který může plnit prostředek pro ověření tohoto výskytu se nazývá spektrální analyzátor.[1,33]

9 Závěr

Integrace inteligentních systémů budov je sice často technicky možná, vzhledem k legislativním a standardizačním předpokladům však více či méně problematická. Z technického hlediska se setkáváme převážně s problémy nejednoznačnosti síťové infrastruktury, nejednotnosti původních datových modelů (kompatibility) a bezpečnosti celé sítě. Tyto problémy lze překonat navržením vhodného integračního řešení, které však musí plnit relevantní legislativní a standardizační předpoklady. To pak zvláště v otázce **stupně zabezpečení objektu při začlenění systému PZTS do projektu IB**. Zde je podstatné to, že se při integraci k přenosu informací často využívají technologie, které nemají samy o sobě dostatečný stupeň spolehlivosti a odolnosti proti úmyslnému napadení, z čehož plyne následná degradace tohoto stupně pro celý systém.

V této práci jsou nastíněny tři praktické realizace PZTS, z čehož dvě v sobě přináší funkce systému domácí automatizace – Fibaro. Jedná se o systém přinášející komfort a úsporu především malým a středně velkým obytným objektům s rezidenční úrovní integrace, avšak sám o sobě s nízkou úrovní bezpečnosti. Součástí třetího navrženého modelu realizace je popis řešení modelu, kdy je konvenční smyčkový PZTS integrován společně se systémem Fibaro, takovým způsobem kdy nedochází k degradaci stupně zabezpečení dle normy ČSN CLC/TS 50 131:2007 kategorie 2 (střední až nízké riziko). Celý systém pak splňuje funkci poplachového zabezpečovacího a tísňového systému v tomto stupni a zároveň je obohacen o funkce „inteligentního“ systému Fibaro, za poměrně příznivých vynaložených nákladů na pořízení všech komponent. Pro toto řešení autor doporučuje výrobci/distributorovi pro ČR podrobit certifikační zkoušce stěžejní prvek této integrace – Univerzální binární senzor (FGBS-001).

Výrobce uvádí spolehlivost sítě Z-Wave jako srovnatelnou se spolehlivostí komunikace drátové sběrnice. Toto tvrzení je vyvráceno funkční zkouškou v této diplomové práci, kdy je hodnocena schopnost řídící jednotky (HC2) vyhodnotit patřičný počet událostí vyslaných jedním z modulů (Univerzální binární senzor). **Negativním výsledkům této zkoušky je připsán jev výskytu elektromagnetického rušení (umělého či přirozeného).** Tento jev je všeobecným problémem u zařízení využívající přenos v ISM pásmu, tedy většiny bezdrátových systémů PTZS. Před skutečným nasazením systému Fibaro (nejlépe však v době sestavování performačních indikátorů budoucího konkrétního systému), by bylo vhodné provést zkoušku zaměřenou na výskyt tohoto jevu pomocí spektrometru a dle výsledků této zkoušky přehodnotit vhodnost nasazení tohoto systému.

10 Použitá literatura

[1] VOTRUBA, Zdeňek. *INTEGRACE OCHRANNÝCH SYSTÉMŮ V RÁMCI PROJEKTU „INTELIGENTNÍ BUDOVY“*. Praha, 2014. Doktorská disertační práce. ČZU TF. Vedoucí práce Miroslav Přikryl.

[2] BEBČÁK, Petr. *Požárně bezpečnostní zařízení*. 2. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2004. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 80-86634-34-5.

[3] HEŘMAN, Josef. *Elektrotechnické a telekomunikační instalace: komplexní zpracování problematiky elektrotechnických a telekomunikačních instalací v budovách: elektronická příručka*. Praha: Dashöfer, 2010-. ISSN 1804-5243.

[4] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. [S.l.: s.n.], 2003. ISBN 80-902938-2-4.

[5] STAŠA, Lukáš. Návrh nového zabezpečení budovy Policie. Zlín, 2013. Diplomová práce.

[6] MATĚJKA, Pavel. *Certifikace vybraných komponent spol. Teco pro realizaci zabezpečovacího systému*. Vysoké učení technické v Brně, 2014. Bakalářská práce. ČZU TF.

[7] ZOUNEK, Jiří. *K problematice konvergence informačních a komunikačních technologií a školy*. Brno, 2004(9), 111-126. ISSN 1211-6971.

[8] MULLER, Richard. *Systémová elektrická instalace ABB i-bus: KNX* [online]. Dostupné z: http://europen.cz/Proceedings/46/Richard%20Muller% [cit. 2016-03-20].

[9] *INELS jako building management system s využitím Foxtrot*. Vysoké učení technické v Brně, 2010. Diplomová práce.

[10] VOTRUBA, Zdeněk a Petr VACULÍK. *Chytré domy a bezpečnost* [online]. Dostupné z: http://docplayer.cz/15316592-Chytre-domy-a-bezpecnost.html

[11] *Internet věcí: Internet of Things* [online]. Praha: MANAGEMENTMANIA, 2015 [cit. 2016-03-20]. Dostupné z: https://managementmania.com/cs/internet-veci-internet-of-things

[12] *ANSI/SIA DC-09-2007* [online]. Praha: CKBS, 2013 [cit. 2016-03-20]. Dostupné z: http://ckbs.cz/610/

[13] *Expertní a neuronové systémy* [online]. Ostrava: geoinformatika, 2015 [cit. 2016-03-20]. Dostupné z: http://geologie.vsb.cz/geoinformatika/kap07.htm

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

[15] *Inteligentní budovy* [online]. [cit. 2016-03-20]. Dostupné z: http://www.inteligentni-budovy.cz/

[16] MOTÝL, Petr. Schneider Electric: průvodce řídicími systémy pro inteligentní budovy.*Automatizace* [online]. 2005, 48(3), 220 [cit. 2016-03-31]. ISSN 0005-125X. Dostupné z: http://www.automatizace.cz/article.php?a=602

[17] VALOUCH. *Projektování integrovaných poplachových systémů* [online]. Zlín, 2012 [cit. 2016-03-31]. UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ.

[18] *Wireless Sensor Network(WSN) using Low cost ZigBee technology* [online]. 2014 [cit. 2016-03-20]. Dostupné z: http://sanjeev4wsn.blogspot.cz/

[19] Integrace systémů budov. In: *Variant Plus* [online]. [cit. 2016-03-31]. Dostupné z: http://www.variant.cz/soubory-ve-skladu/Dokumenty/Obchod/Propagacni-materialy/ISB-letak.pdf

[20] Automation Technology / Building. In: *NF fleuren* [online]. [cit. 2016-03-20]. Dostupné z: http://www.fleuren.com/uploads/schema-gebaedeautomation-d.g

[21] *VRBOVEC, Bohumil*. Bezpečný přenos informací mezi prostředky asistivních technologií a centry pomoci. In: MPVS [online]. 2014 [cit. 2016-03-20]. Dostupné z: http://www.mpsv.cz/files/clanky/19596/BPI.pdf

[22] *TAUFER, I.; DRÁBEK, O.; SEIDL, P.* Umělé neuronové sítě – základy teorie a aplikace [online]. Dostupné z: http://www.chemagazin.cz/prehled.html

[23] HC-2: Návod pro rychlé zapojení. *Yatun*, 2014.

[24] Elektrotechnická schéma zapojení prvků FIBARO. *Yatun*, 2014.

[25] *ČSN CLC/TS 50 131: Poplachové zabezpečovací a tísňové systémy*. Praha: CLC/TS, 2007

[26] *ČSN CLC/TS 50 398 (334597):* Poplachové systémy - Kombinované a integrované systémy. Praha: CLC/TS, 2009.

[26] *OCHRANA OSOBNÍCH ÚDAJŮ*: Předpis č. 101/2000 Sb.

[27] *ANSI/SIA DC-09: SIA Digital Communication Standard*. ANSI/SIA, 2013.

[28] Manuály a dokumentace k zažízením Fibaro. *Yatun*

[29] *Přehled komponent IQRF* [online]. Dostupné z: http://www.ecom.cz/files/documents-catalogue/113.pdf

[30] *IQRF - bezdrátová technologie, která láme bariéry* [online]. 2013. Dostupné z: http://www.soselectronic.cz/?str=1342

[31] *Sběrnice LonWorks* [online]. 2005. Dostupné z: http://automatizace.hw.cz/clanek/2005040501

[32] HART, Jan a Veronika NÍDLOVÁ. *Testování pásem ISM 433 a 868 u přenosů v poplachových, zabezpečovacích a tísňových systémech* [online]. Automa. 2015. Dostupné z: http://automa.cz/res/pdf/53800.pdf

11 Seznam obrázků

12 Seznam tabulek

Příloha 1: Univerzální binární senzor

Detektory do niž se vejde Univerzální binární senzor

Kód detektoru	DRUH DETEKTORU	VÝROBCE
RXC-ST	PIR	Optex
IS 2535	PIR	Honeywell
IS 2560	PIR	Honeywell
IS 25100	PIR	Honeywell
DT 7235 duální	PIR+MW	Honeywell
DT 7435 duální	PIR+MW	Honeywell
RF360 stropní	PIR	Texecom
PREMIER360 DT stropní duální	PIR+MW	Texecom
RK 2000 stropní	PIR	Risco
FX360 stropní	PIR	Optex
SX360 stropní	PIR	Optex
Digigard 55	PIR	Paradox
Paradox Pro	PIR	Paradox

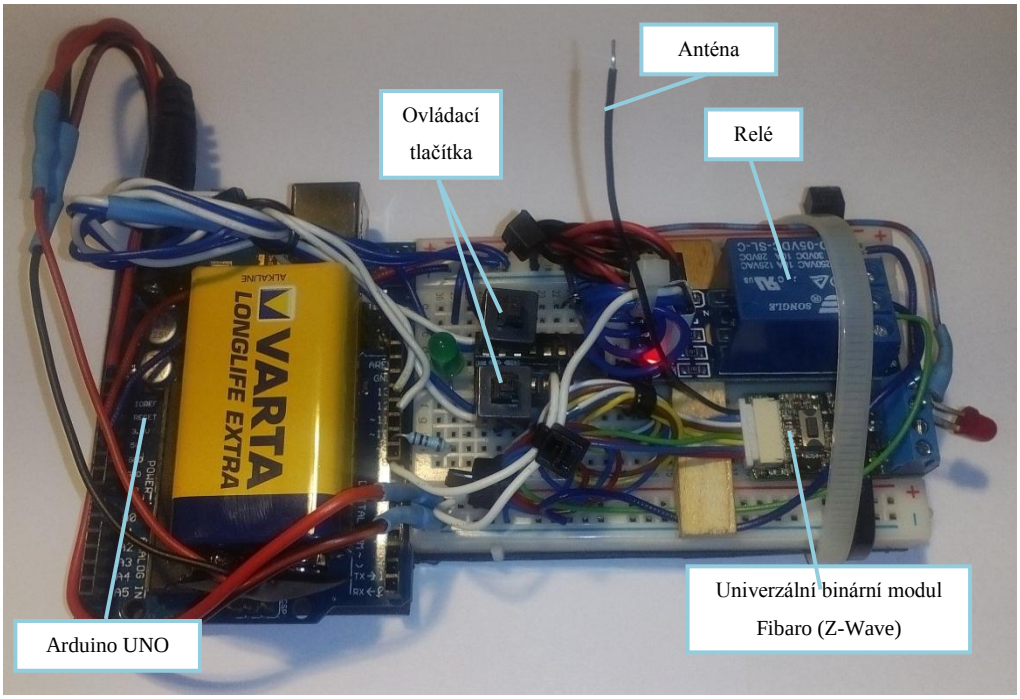
Univerzální binární modul součástí PIR Paradox PRO

Příloha 2: Přístupová klávesnice

Přístupová klávesnice/čtečka Entry E-KR11

Příloha 3: Testovací zařízení

Sestavené testovací zařízení



Toto zařízení bylo užito pro provedení funkčních zkoušek. Bylo k němu pro zajištění správnosti měření pripojené napětí z napájecího zdroje 9 V DC.

Příloha 4: Program testovacího zažízení

Program nahraný do ATMega součástí testovacího zařízení

```
#define RELEONE 7
int Tlacitko1 = 11;
int Tlacitko2 = 12;

void setup()
{
Serial.begin(9600);
pinMode(Tlacitko1, INPUT_PULLUP);
pinMode(Tlacitko2, INPUT_PULLUP);
}

void loop()
{
  int HodnotaTlacitka1=!digitalRead(Tlacitko1);
  int HodnotaTlacitka2=!digitalRead(Tlacitko2);

Serial.print(HodnotaTlacitka2);
Serial.print("\n");
Serial.print(HodnotaTlacitka1);
Serial.print("\n\n");

if(HodnotaTlacitka2 > 0)
  {
  for(int i=100; i>0; i--)
  {
  analogWrite(RELEONE,0);
  delay(500);
  analogWrite(RELEONE,255);
  delay(2000);
 HodnotaTlacitka2=!digitalRead(Tlacitko2);
  if(HodnotaTlacitka2 == 1)
  {
    i=0;
    delay(3000);
  }
  }
  }

if(HodnotaTlacitka1 > 0)
  {
  analogWrite(RELEONE,0);
  }
  else
  {analogWrite(RELEONE,255);
  }
}
```

Příloha 5: Makro pro tvorbu protokolů o měření

Makro vytvořené ve VBA pro vytváření protokolů o měření z logu událostí ve Fibaru

```
Sub mazaniImportu()
Sheets("Import").Range("A2:R2000").Select
Selection.ClearContents
End Sub


Sub filtr1()
Dim pocetUdalosti As Integer
Dim nazev As String
nazev = Range("B1").Value

On Error Resume Next
Sheets(nazev).Delete
Sheets.Add.Name = nazev
Sheets(nazev).Range("A1").Value = nazev

For i = 3 To 300
ii = (i - 2) * 8
Sheets(nazev).Range("D" & i).Value = Mid(Sheets("Import").Range("A" & ii - 3).Value, 11)
If Sheets("Import").Range("A" & ii - 4).Value = "Breached  Safe" Then
Sheets(nazev).Range("E" & i).Value = "open"
Else
Sheets(nazev).Range("E" & i).Value = "closed"
End If

Sheets(nazev).Range("A" & i).Value = Sheets("Import").Range("A" & ii - 1).Value
Sheets(nazev).Range("B" & i).Value = Mid(Sheets("Import").Range("A" & ii + 1).Value, 11)
If Sheets("Import").Range("A" & ii).Value = "Breached  Safe" Then
Sheets(nazev).Range("C" & i).Value = "open"
Else
Sheets(nazev).Range("C" & i).Value = "closed"
End If

If Sheets("Import").Range("A" & ii + 2).Value = "" Then
pocetUdalosti = (i - 2) * 2
   If Sheets("Import").Range("A" & ii - 1).Value = "" Then
   pocetUdalosti = pocetUdalosti - 1
   End If
Sheets(nazev).Range("d1").Value = "Počet událostí:"
Sheets(nazev).Range("f1").Value = pocetUdalosti
i = 300
End If

Next i
End Sub
```

Příloha 6: Ukázky protokolů

Protokol ze 100% úspěšného měření

Hřiště(40m) č.2 Počet událostí: 200

Kontakt	11:36:38	closed	11:36:38	open
Kontakt	11:36:35	closed	11:36:36	open
Kontakt	11:36:33	closed	11:36:33	open
Kontakt	11:36:30	closed	11:36:31	open
Kontakt	11:36:28	closed	11:36:28	open
Kontakt	11:36:25	closed	11:36:26	open
Kontakt	11:36:23	closed	11:36:23	open
Kontakt	11:36:20	closed	11:36:21	open
Kontakt	11:36:18	closed	11:36:18	open
Kontakt	11:36:15	closed	11:36:16	open
Kontakt	11:36:13	closed	11:36:13	open
Kontakt	11:36:10	closed	11:36:11	open
Kontakt	11:36:07	closed	11:36:08	open
Kontakt	11:36:05	closed	11:36:06	open
Kontakt	11:36:03	closed	11:36:03	open
Kontakt	11:36:00	closed	11:36:01	open
Kontakt	11:35:58	closed	11:35:58	open
Kontakt	11:35:55	closed	11:35:56	open
Kontakt	11:35:53	closed	11:35:53	open
Kontakt	11:35:50	closed	11:35:51	open
Kontakt	11:35:48	closed	11:35:48	open
Kontakt	11:35:45	closed	11:35:46	open
Kontakt	11:35:43	closed	11:35:43	open
Kontakt	11:35:40	closed	11:35:41	open
Kontakt	11:35:38	closed	11:35:38	open
Kontakt	11:35:35	closed	11:35:36	open
Kontakt	11:35:33	closed	11:35:33	open
Kontakt	11:35:30	closed	11:35:31	open
Kontakt	11:35:28	closed	11:35:28	open
Kontakt	11:35:25	closed	11:35:26	open
Kontakt	11:35:23	closed	11:35:23	open
Kontakt	11:35:20	closed	11:35:21	open
Kontakt	11:35:18	closed	11:35:18	open
Kontakt	11:35:15	closed	11:35:16	open
Kontakt	11:35:13	closed	11:35:13	open
Kontakt	11:35:10	closed	11:35:11	open
Kontakt	11:35:08	closed	11:35:08	open
Kontakt	11:35:05	closed	11:35:06	open
Kontakt	11:35:03	closed	11:35:03	open
Kontakt	11:35:00	closed	11:35:01	open
Kontakt	11:34:58	closed	11:34:58	open
Kontakt	11:34:55	closed	11:34:56	open
Kontakt	11:34:53	closed	11:34:53	open
Kontakt	11:34:50	closed	11:34:51	open
Kontakt	11:34:48	closed	11:34:48	open
Kontakt	11:34:45	closed	11:34:46	open
Kontakt	11:34:43	closed	11:34:43	open
Kontakt	11:34:40	closed	11:34:41	open
Kontakt	11:34:38	closed	11:34:38	open

Kontakt	11:34:35	closed	11:34:36	open
Kontakt	11:34:33	closed	11:34:33	open
Kontakt	11:34:30	closed	11:34:31	open
Kontakt	11:34:28	closed	11:34:28	open
Kontakt	11:34:25	closed	11:34:26	open
Kontakt	11:34:23	closed	11:34:23	open
Kontakt	11:34:20	closed	11:34:21	open
Kontakt	11:34:18	closed	11:34:18	open
Kontakt	11:34:15	closed	11:34:16	open
Kontakt	11:34:13	closed	11:34:13	open
Kontakt	11:34:10	closed	11:34:11	open
Kontakt	11:34:08	closed	11:34:08	open
Kontakt	11:34:05	closed	11:34:06	open
Kontakt	11:34:03	closed	11:34:03	open
Kontakt	11:34:00	closed	11:34:01	open
Kontakt	11:33:58	closed	11:33:58	open
Kontakt	11:33:55	closed	11:33:56	open
Kontakt	11:33:53	closed	11:33:53	open
Kontakt	11:33:50	closed	11:33:51	open
Kontakt	11:33:48	closed	11:33:48	open
Kontakt	11:33:45	closed	11:33:46	open
Kontakt	11:33:43	closed	11:33:43	open
Kontakt	11:33:40	closed	11:33:41	open
Kontakt	11:33:38	closed	11:33:38	open
Kontakt	11:33:35	closed	11:33:36	open
Kontakt	11:33:33	closed	11:33:33	open
Kontakt	11:33:30	closed	11:33:31	open
Kontakt	11:33:28	closed	11:33:28	open
Kontakt	11:33:25	closed	11:33:26	open
Kontakt	11:33:23	closed	11:33:23	open
Kontakt	11:33:20	closed	11:33:21	open
Kontakt	11:33:18	closed	11:33:18	open
Kontakt	11:33:15	closed	11:33:16	open
Kontakt	11:33:13	closed	11:33:13	open
Kontakt	11:33:10	closed	11:33:11	open
Kontakt	11:33:08	closed	11:33:08	open
Kontakt	11:33:05	closed	11:33:06	open
Kontakt	11:33:03	closed	11:33:03	open
Kontakt	11:33:00	closed	11:33:01	open
Kontakt	11:32:58	closed	11:32:58	open
Kontakt	11:32:55	closed	11:32:56	open
Kontakt	11:32:53	closed	11:32:53	open
Kontakt	11:32:50	closed	11:32:51	open
Kontakt	11:32:48	closed	11:32:48	open
Kontakt	11:32:45	closed	11:32:46	open
Kontakt	11:32:43	closed	11:32:43	open
Kontakt	11:32:40	closed	11:32:41	open
Kontakt	11:32:38	closed	11:32:38	open
Kontakt	11:32:35	closed	11:32:36	open
Kontakt	11:32:33	closed	11:32:33	open
Kontakt	11:32:30	closed	11:32:31	open

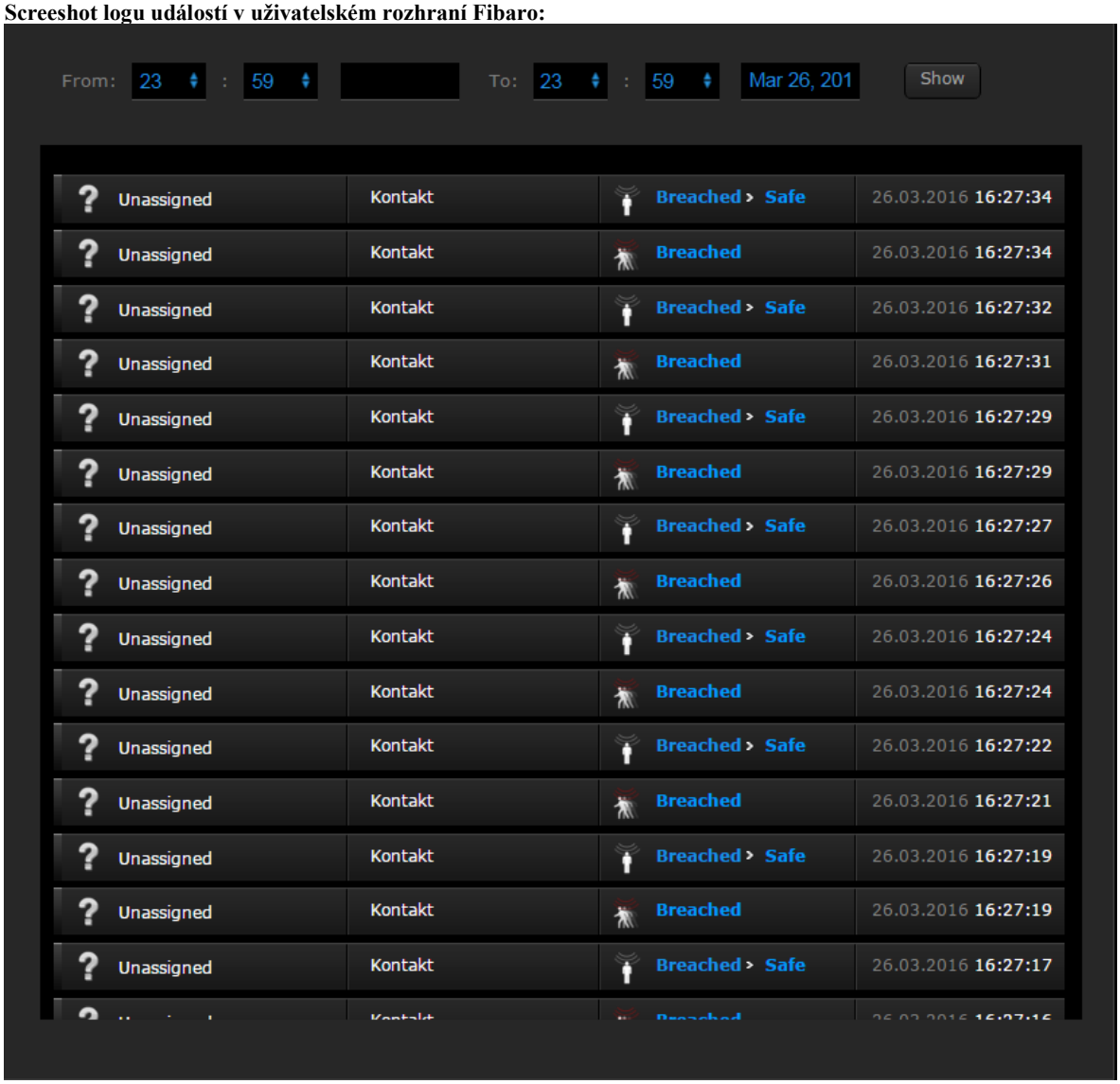
Protokol z měření s 29,5 % úspěšným měřením

Přímý dohled+klicenka (10m) č.3 Počet událostí: 59

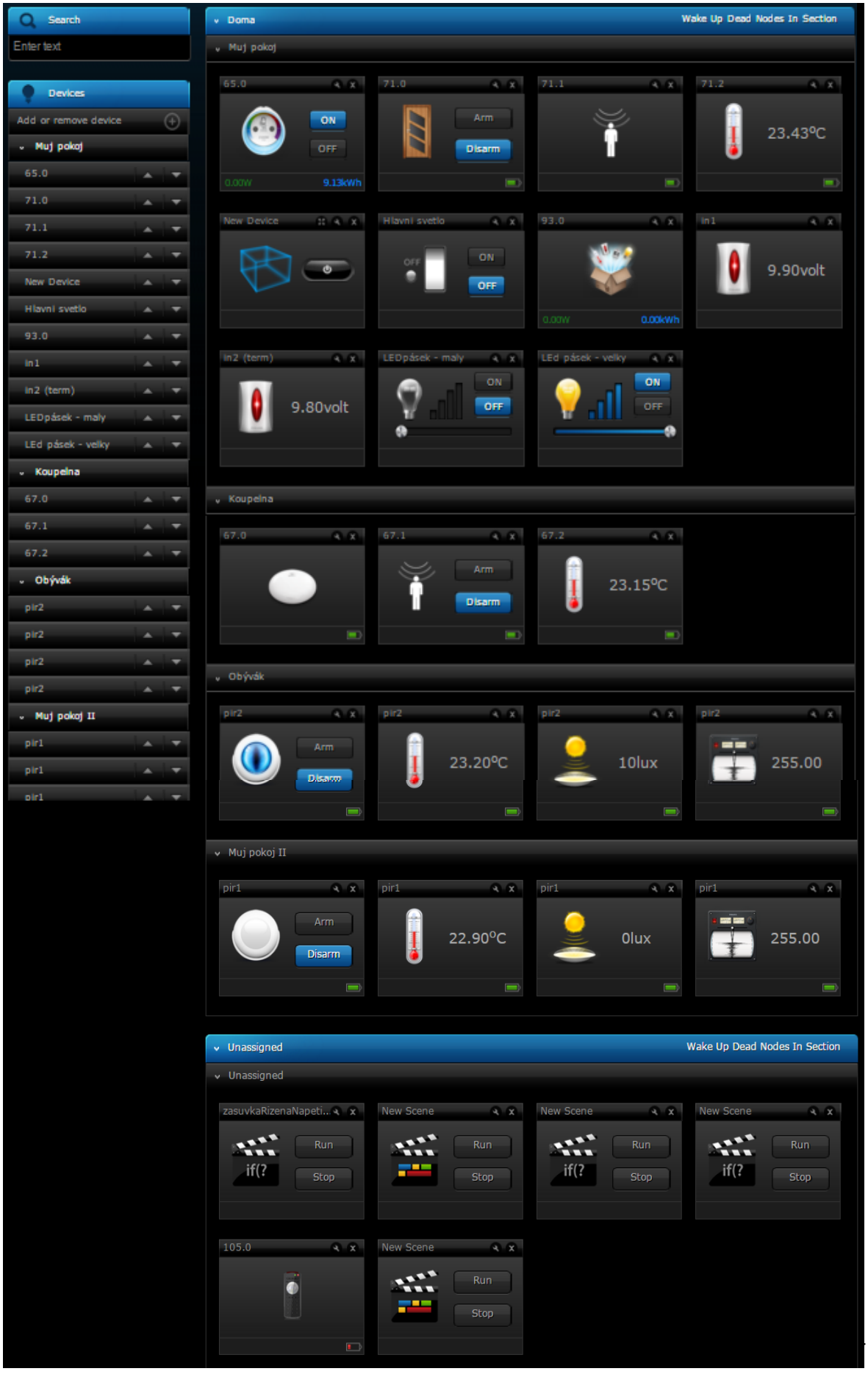
Kontakt	21:13:19	open	21:13:21	closed
Kontakt	21:13:16	open	21:13:18	closed
Kontakt	21:13:14	open	21:13:16	closed
Kontakt	21:13:12	open	21:13:14	closed
Kontakt	21:12:32	open	21:12:33	closed
Kontakt	21:12:19	open	21:12:26	closed
Kontakt	21:12:09	open	21:12:11	closed
Kontakt	21:12:07	open	21:12:09	closed
Kontakt	21:12:04	open	21:12:06	closed
Kontakt	21:12:02	open	21:12:03	closed
Kontakt	21:11:59	open	21:12:01	closed
Kontakt	21:11:56	open	21:11:58	closed
Kontakt	21:11:54	open	21:11:56	closed
Kontakt	21:11:51	open	21:11:54	closed
Kontakt	21:11:24	open	21:11:26	closed
Kontakt	21:11:12	open	21:11:14	closed
Kontakt	21:10:54	open	21:10:56	closed
Kontakt	21:10:52	open	21:10:53	closed
Kontakt	21:10:44	open	21:10:48	closed
Kontakt	21:10:32	open	21:10:39	closed
Kontakt	21:10:29	open	21:10:31	closed
Kontakt	21:10:27	open	21:10:29	closed
Kontakt	21:10:19	open	21:10:26	closed
Kontakt	21:10:17	open	21:10:19	closed
Kontakt	21:09:52	open	21:10:16	closed
Kontakt	21:09:49	open	21:09:51	closed
Kontakt	21:09:47	open	21:09:49	closed
Kontakt	21:09:34	open	21:09:36	closed
Kontakt	21:09:17	open	21:09:19	closed
		closed	21:09:14	closed

Příloha 7: Screenshoty z uživatelského rozhraní Fibaro

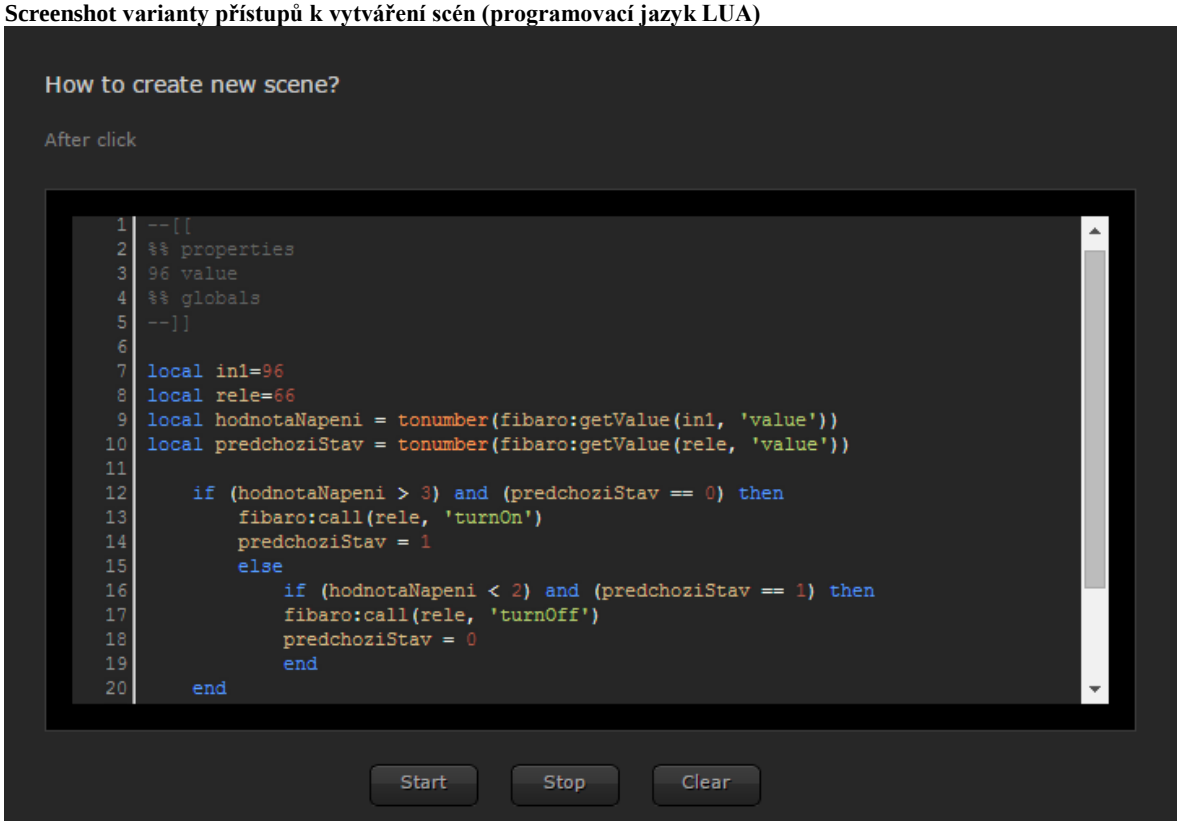
Screeshot logu událostí v uživatelském rozhraní Fibaro:



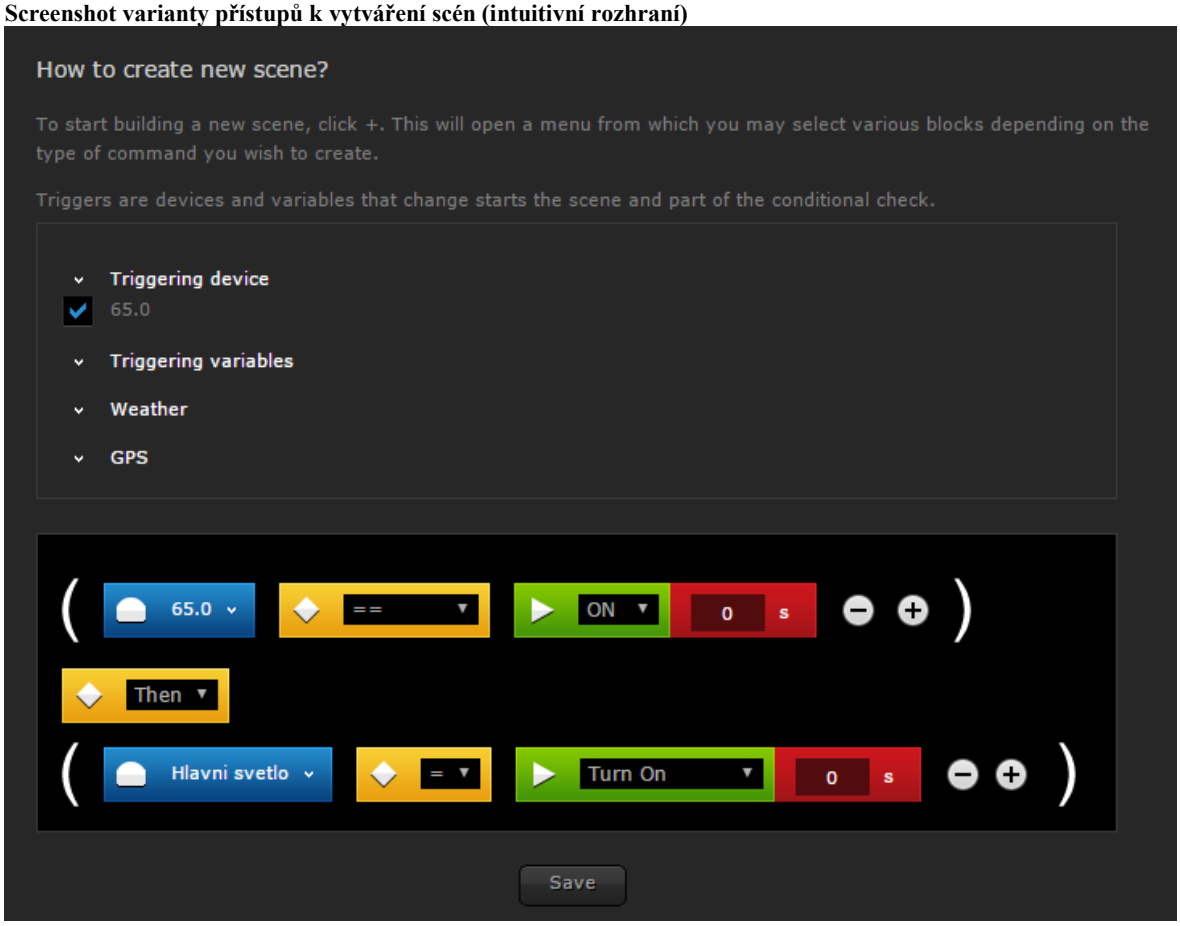
Screeshot příkladu realizace uživatelském rozhraní Fibaro



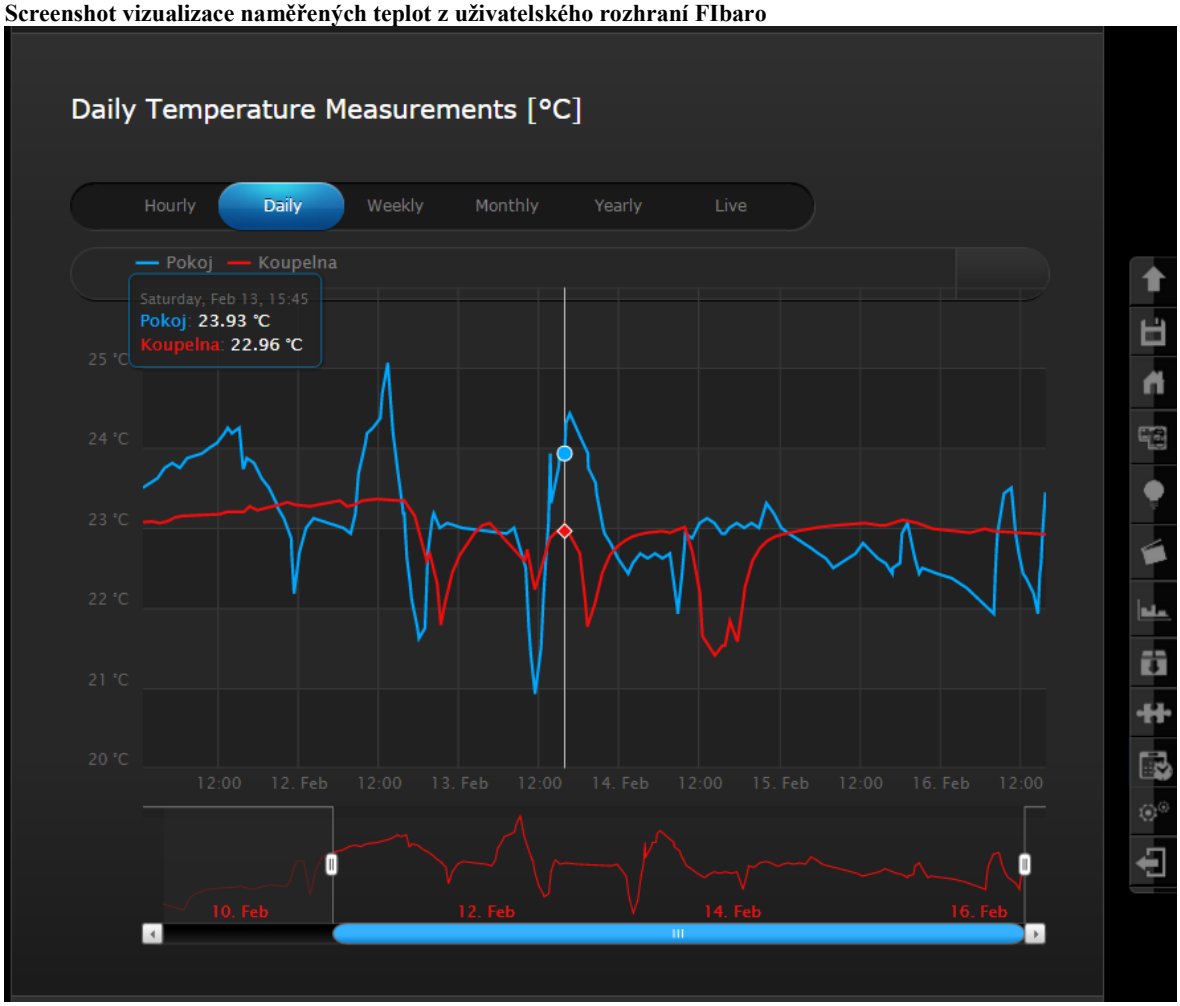
Screenshot varianty přístupů k vytváření scén (programovací jazyk LUA)



Screenshot varianty přístupů k vytváření scén (intuitivní rozhraní)



Screenshot vizualizace naměřených teplot z uživatelského rozhraní FIbaro



Příloha 8: Obsah normy ČSN CLC/TS 50 131

Obsah normy ČSN CLC/TS 50 131

Norma o poplachových zabezpečovacích a tísňových systémech se skládá z několika částí:

- ČSN CLC/TS 50 131-1 Všeobecné požadavky
- ČSN CLC/TS 50 131-2-1 Všeobecné požadavky pro detektory
- ČSN CLC/TS 50 131-2-2 Pasivní detektory
- ČSN CLC/TS 50 131-2-3 MW detektory
- ČSN CLC/TS 50 131-2-4 Kombinované detektory- pasivní/MW
- ČSN CLC/TS 50 131-2-5 Kombinovaná detektory - pasivní/UZ
- ČSN CLC/TS 50 131-2-6 Detektory otevření
- **ČSN CLC/TS 50 131-3 Ústředny**
- ČSN CLC/TS 50 131-4 Signalizační zařízení
- ČSN CLC/TS 50 131-5-1 Všeobecné požadavky pro propoj.zařízení
- ČSN CLC/TS 50 131-5-3 Prop.zař. využívající určené metalické spoje
- ČSN CLC/TS 50 131-5-5 Prop.zař. využívající určené IČ spoje
- **ČSN CLC/TS 50 131-6 Napájecí zdroje**
- ČSN CLC/TS 50 131-7 Pokyny pro aplikace

Zkoušky prováděné při certifikaci dle normy ČSN CLC/TS 50 131

Jsou uvedeny pouze relevantní zkoušky:

Zkouška ústředen ČSN CLC/TS 50 131-3

- Laboratorní podmínky
- **Funkční zkoušky**
- Přístupové úrovně
- Zkouška digitálního (logického) klíče nebo PIN kódů
- Funkční zkouška uvádění do stavu
- Zkoušky zabezpečení proti sabotáži
- Zkouška náhrady
- Zkouška monitorování propojení
- Paměť událostí
- Značení dokumentace
- Zkoušky vlivu prostředí

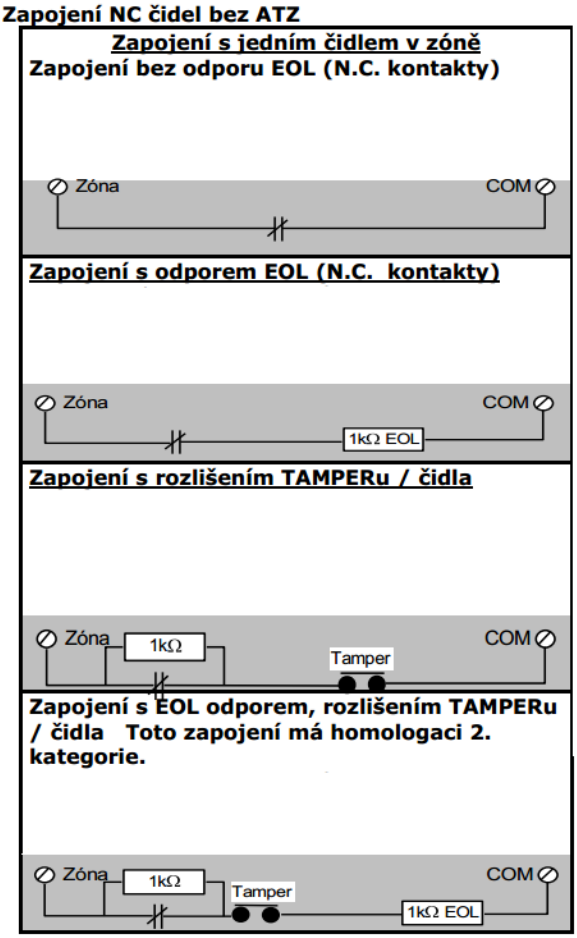
Zkouška napájecích zdrojů ČSN CLC/TS 50 131-6

- Zkrácená funkční zkouška
- Maximální zatížení napájecího zdroje
- Stabilita výstupního napětí – postupná změna zátěže
- Stabilita výstupního napětí – skoková změna zátěže
- Signalizace – výpadek vnějšího napájecího zdroje
- Signalizace – nízké napětí akumulátoru-baterie
- Signalizace – porucha akumulátoru
- Signalizace – nízké výstupní napětí
- Signalizace – porucha napájecí jednotky
- Signalizace – porucha nabíjení akumulátoru
- Dálkově řízený test
- Nabíjení akumulátoru
- Přepěťová ochrana
- Zkrat
- Přetížení
- Ochrana proti hlubokému vybití
- Automatické přepnutí na záložní napájecí zdroj
- Ochrana proti sabotáži
- Ochrana proti sabotáži – přístup dovnitř krytu
- Detekce proti sabotáži – odejmutí montážního krytu
- Detekce proti sabotáži – vniknutí dovnitř krytu
- Zkoušky vlivu prostředí a EMC
- Značení a dokumentace

Příloha 9: Možnosti smyčkových zapojení u PTZS

Zapojení detektorů PTZS pomocí smyček

Zapojení NC čidel bez ATZ



Zapojení NC čidel s ATZ