

Školicí středisko pro systém ASSET

A Training Centre for the ASSET System

Bc. Martin Buňka



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Martin Buňka**
Osobní číslo: **A13342**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Školící pracoviště pro systém ASSET**
Téma anglicky: **A Training Centre for the ASSET System**

Zásady pro vypracování:

1. Provedte rešerši podobných školících pracovišť.
2. Popište systém ASSET.
3. Navrhněte školící pracoviště pro systém ASSET.
4. Vytvořte výukový materiál pro jednotlivé etapy školení.
5. Navrhněte jednotlivé úlohy školení a jejich hodnocení.
6. Navrhněte závěrečné testy a certifikát o úspěšném absolvování kurzu.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. ŠPAČKOVÁ, Alena. Umění dialogu: jak si s lidmi opravdu porozumět. 1. vyd. Praha: Grada, 2011, 196 s. ISBN 978-80-247-3810-9.
2. SIDHU, Inder. Cisco umí obojí: jak dnes vydělávat a zároveň zajistit budoucí růst. Vyd. 1. Brno: Computer Press, 2011, 248 s. ISBN 978-80-251-3537-2.
3. CHROMÝ, Jan. Komunikace, média, vzdělávání, kultura. Vyd. 1. Praha: Extrasystem Praha, 2014, 201 s. ISBN 978-80-87570-19-7.
4. VALOUCH, Jan. Projektování integrovaných systémů. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj (152 s.). ISBN 978-80-7454-296-1.
5. TRADE FIDES, a.s. Asset Client: Manuál správce systému. Brno, 2015. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/16-asset-client.html>
6. TRADE FIDES, a.s. Asset Config: Manuál technika systému. Brno, 2015. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/31-asset-config.html>
7. TRADE FIDES, a.s. Asset Console: Manuál správce systému. Brno, 2015. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/69-asset-console.html>
8. TRADE FIDES, a.s. Asset Server: Manuál správce systému. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/44-asset-server.html>

Vedoucí diplomové práce:

Ing. Rudolf Drga, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

12. ledna 2015

Termín odevzdání diplomové práce:

15. května 2015

Ve Zlíně dne 6. února 2015

doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu


Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 20.5.2015



podpis diplomanta

ABSTRAKT

Tato diplomová práce se zabývá vytvořením školicího pracoviště, jako nástroje pro efektivní zaučení techniků pracujících s integrovaným zabezpečovacím systémem Asset. Práci tvoří literární rešerše školicích pracovišť z oblasti technického vzdělávání a popis systému Asset. V praktické části jsou vypracovány školicí materiály pro jednotlivé etapy výuky a systém ověřování získaných znalostí na základě testů a praktických úloh.

Klíčová slova: Asset, školení, PZTS, integrované poplachové systémy

ABSTRACT

This thesis deals with establishing a training centre aimed at effective training of technicians working with the integrated security system Asset. It consists of literary researches by training institutes of technical education and the description of Asset system. The practical part includes training materials prepared for particular stages of tuition and the verification system of acquired knowledge based on tests and practical exercises.

Keywords: Asset, training centre, I&HAS, integrated alarm systems

Děkuji Ing. Rudolfu Drgovi, který vedl mou diplomovou práci. Poděkování dále patří firmě Trade FIDES, a.s. jmenovitě Ing. Václavu Lukášovi a Robertu Exnerovi za odborné připomínky a poskytnutí podkladů včetně hardwarových a softwarových komponent. Poděkování patří také Mgr. Romaně Šilhavé Ph.D. a Mgr. Jaroslavě Nesetové za poskytnutí konzultací týkajících se jazykové části práce. V neposlední řadě děkuji rodině za podporu během studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD.....	10
I TEORETICKÁ ČÁST.....	11
1 INTEGROVANÝ ZABEZPEČOVACÍ SYSTÉM ASSET.....	12
1.1 KONCEPCE SYSTÉMU	12
1.1.1 Hardwarová vrstva	12
1.1.2 Vrstva nadstavbového software	12
1.2 HARDWARE	13
1.2.1 Řídící jednotka	14
1.2.1.1 Asset 801Z, 804Z.....	14
1.2.1.2 Asset 804,808,812.....	15
1.2.2 Ovládací panely.....	15
1.2.2.1 KMU-4.....	15
1.2.2.2 KMU-6.....	16
1.2.2.3 KMU-7.....	16
1.2.3 Dveřní jednotky.....	17
1.2.4 Vstupně-výstupní moduly	18
1.2.4.1 LML-8.....	18
1.2.4.2 Octopus	18
1.2.5 Komunikační moduly.....	19
1.2.5.1 PZL	19
1.2.5.2 Ademco Contact ID	19
1.2.6 Klíčové trezory KWAD	20
1.3 SOFTWARE	21
1.3.1 Asset Config.....	22
1.3.2 Asset Server	23
1.3.3 Asset Console.....	23
1.3.4 Asset Client	23
1.3.5 Asset Client - Mobile	24
1.3.6 Asset Control.....	25
1.3.7 Asset Control-Mobile.....	25
1.3.8 Fides Device Configurator	25
1.3.9 Asset Guestbook.....	26
1.3.10 Asset Monitor.....	26
1.3.11 Asset Web Interface	26
1.3.12 Autorizační portál.....	26
1.3.13 Fides Software Storage	26
2 PŘEHLED ŠKOLICÍCH STŘEDISEK.....	27
2.1 VÝZNAM ŠKOLICÍCH STŘEDISEK V PKB	27
2.2 ÚČEL ŠKOLENÍ.....	28
2.2.1 Bezpečnost a ochrana zdraví při práci.....	28
2.2.2 Obchodní školení	28
2.2.3 Technické školení.....	28
2.2.4 Uživatelské školení	29
2.2.5 Aktualizační školení.....	29

2.3	FORMA ŠKOLENÍ.....	29
2.3.1	Teoretická forma	29
2.3.2	Kombinovaná forma.....	29
2.4	ŠKOLICÍ STŘEDISKA A ŠKOLENÍ V PRAXI.....	30
2.4.1	KNX	30
2.4.2	Jablotron.....	30
2.4.3	Variant.....	31
2.4.4	Axis	31
2.4.5	CCNA Exploration.....	31
2.4.6	RipEX.....	32
2.4.7	Abbas.....	32
2.4.8	Acti	33
2.4.9	Moxa	33
2.4.10	Stávající systém školení Asset	33
2.4.11	Dílčí závěry	34
II	PRAKTICKÁ ČÁST	35
3	ŠKOLENÍ.....	36
3.1	SOUČASNÝ STAV	36
3.1.1	Výhody současného stavu	36
3.1.2	Slabé stránky současného stavu	37
3.1.3	Dílčí závěr	37
3.2	KONCEPCE NOVÉHO ŠKOLICÍHO STŘEDISKA	37
3.2.1	Vstupní testy.....	38
3.2.1.1	Počítačové sítě	38
3.2.1.2	Elektrotechnika	38
3.2.1.3	Operační systém Windows a databáze.....	39
3.2.1.4	Zpětná vazba na otázky vstupního testu	39
3.2.2	Struktura lekcí	40
3.2.2.1	Přednáška	41
3.2.2.2	Cvičení	42
3.2.2.3	Zpětná vazba	42
3.2.3	První lekce.....	43
3.2.3.1	Přednáška	43
3.2.3.2	Cvičení	43
3.2.4	Druhá lekce	43
3.2.4.1	Přednáška	43
3.2.4.2	Cvičení	43
3.2.5	Třetí lekce.....	44
3.2.5.1	Přednáška	44
3.2.5.2	Cvičení	44
3.2.6	Čtvrtá lekce	44
3.2.6.1	Přednáška	44
3.2.6.2	Cvičení	44
3.2.7	Pátá lekce	45
3.2.7.1	Přednáška	45
3.2.7.2	Cvičení	45
3.2.8	Šestá lekce	45
3.2.8.1	Přednáška	45

3.2.8.2	Cvičení	45
3.2.9	Sedmá lekce	46
3.2.9.1	Přednáška	46
3.2.9.2	Cvičení	46
3.2.10	Osmá lekce	46
3.2.10.1	Přednáška	46
3.2.10.2	Cvičení	47
3.2.11	Devátá lekce	47
3.2.11.1	Přednáška	47
3.2.11.2	Cvičení	47
3.3	ZÁVĚREČNÁ ZKOUŠKA	47
3.3.1	Teoretická část	48
3.3.2	Praktická část	48
3.4	CERTIFIKÁT	48
ZÁVĚR		50
CONCLUSIONS		51
SEZNAM POUŽITÉ LITERATURY		53
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		57
SEZNAM OBRÁZKŮ		59
SEZNAM TABULEK		60
SEZNAM PŘÍLOH		61

ÚVOD

Montáž a zprovoznění komplexních integrovaných poplachových zabezpečovacích systémů je velmi složitou záležitostí vyžadující velké množství znalostí. Potřebné znalosti je možné získat prostřednictvím samostudia s vlastním odvozováním mnohdy mylných závěrů nebo s využitím školicích středisek se zaměřením na konkrétní technologie pod vedením specialistů.

Integrovaný zabezpečovací systém Asset, který je východiskem této diplomové práce, nabízí nepřehledné množství konfigurovatelných funkcí. Asset zahrnuje poplachový zabezpečovací a tísňový systém, systém kontroly vstupu, systém měření a regulace a možnost připojení kamerových systémů. Poskytuje možnosti softwarových vazeb, skrze které se tyto jinak samostatné systémy příznivě ovlivňují. Neproškolený technik je ale schopen využít pouze zlomkové množství těchto funkcí. Nezajistí tak spokojenost zákazníka ani plnou funkčnost systému. Místo toho z množství variant, které integrované systémy nabízejí, vytváří špatná a neúplná řešení.

Pojišťovny vyžadují pro pojištění objektu zabezpečení systémem, který byl instalován certifikovaným technikem montážní společnosti. Pokud je instalace prováděna technikem, který systém zná pouze díky samostudiu a nedisponuje certifikátem, jenž by znalosti potvrdil, bude pojištění objektu pravděpodobně finančně nákladnější nebo dokonce neproveditelné. Mnoho výrobních firem poskytuje záruku správné funkčnosti pouze v případě, že bylo zařízení správně nainstalováno a nakonfigurováno. Tato skutečnost je předpokládána na základě montáže zařízení certifikovaným montážním technikem.

Dobře provedené školení techniků se může stát marketingovou strategií výrobní společnosti, neboť odběratelská montážní společnost bude častěji odebírat zařízení, která jejich technici dovedou optimálně nainstalovat díky znalostem ze školení a to jak z pohledu kvality, tak času. Výrobní společnost poskytující bezplatnou technickou podporu produktů může dobře zvládnutým školením techniků tuto podporu a s ní související náklady minimalizovat. Vhodně proškolení technici totiž budou mít minimum reálných důvodů se na výše zmíněnou technickou podporu obracet. Stejně tak montážní společnost by měla v rámci zkvalitňování vlastní image mít zaměstnance proškolené na montáž nejrozumnějších technologií.

I. TEORETICKÁ ČÁST

1 INTEGROVANÝ ZABEZPEČOVACÍ SYSTÉM ASSET

Asset je integrovaný zabezpečovací systém českého výrobce, který je certifikován pro IV. stupeň zabezpečení – vysoké riziko. Systém Asset je souhrn:

- a) vyhodnocovací řídicí jednotka
- b) periferie pro získávání údajů ze svého okolí a zařizující zpětnou odezvu
- c) nadstavbové konfigurační a ovládací software

1.1 Koncepce systému

Systém Asset je koncipován pro zabezpečení nejvyšší úrovně se současným důrazem na uživatelský komfort a vysokou přidanou hodnotu. Aby byl systém schopen plnit tyto požadavky bez negativních bezpečnostních dopadů, je členěn na dvě samostatné vrstvy a to vrstvu hardwarovou a vrstvu nadstavbového software.

Integrovaní poplachových zabezpečovacích systémů s nepoplachovými systémy prezentuje maximální využití moderních prvků informačních technologií. Zmíněné aplikace lze integrovat navzájem a tím zajistit efektivní provedení samočinných procesů v obytných i výrobních prostorech. Trendy v integrování poplachových systémů reagují na vyšší bezpečnostní požadavky zákazníků spojené s uživatelským komfortem a snahou o snížení ceny.[1]

1.1.1 Hardwarová vrstva

Úkolem hardwarové vrstvy je integrace poplachového zabezpečovacího a tísňového systémů (PZTS), systému kontroly vstupu (SKV) a systému jednoduchého měření a regulace (MaR). Výše zmíněnou integraci řídí ŘJ, která k zisku informací a řízení využívá moduly připojené přes sběrnici RS 485. Na sběrnici RS 485 je možno umístit až 30 modulů. Ústředna je v systému nazývána řídicí jednotkou (dále ŘJ). Samostatnost hardwarové vrstvy zaručuje odolnost vůči chybám, které by případně vznikly na úrovni složitého nadstavbového software.

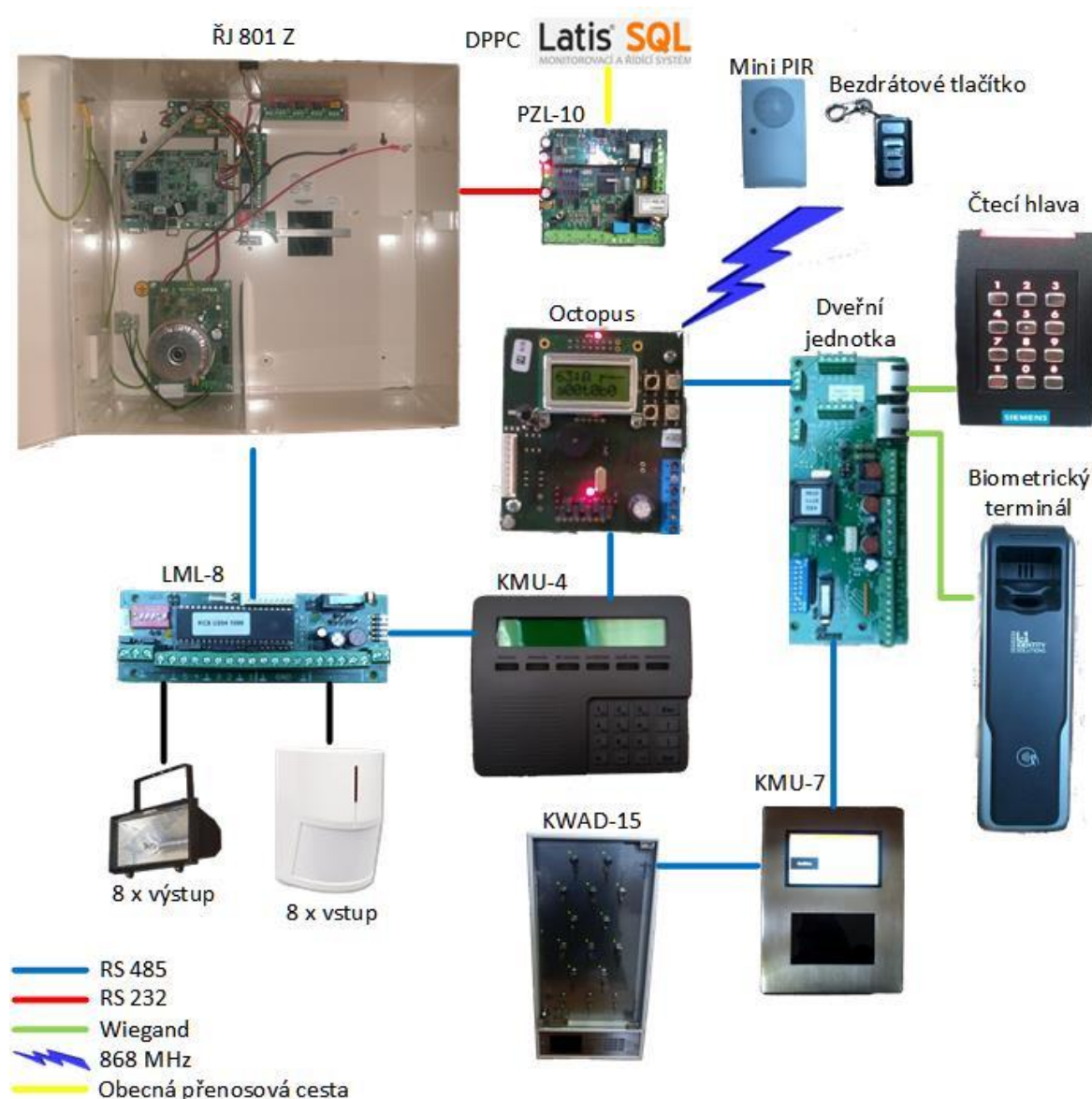
1.1.2 Vrstva nadstavbového software

Vrstva nadstavbového software má za úkol provádět softwarovou integraci a maximálně usnadňovat ovládání a správu celého systému. Základním prvkem vrstvy nadstavbového software je Asset Server (ASVR) zajišťující vazby na kamerové systémy, personální systémy (PeS), systémy docházky nebo připojení operátorského software. K tomuto serveru se následně připojují další grafické aplikace, které jsou konzumentem událostí serveru. Toto oddělení výkonné a zobrazovací části je známé například z odolných serverových operačních

systemů Unixového typu, kdy jsou od sebe jádro systému a uživatelská nastavba odděleny z důvodu vyšší odolnosti vůči chybám. Vrstva nadstavbového software je určena pro operační systém Windows a základní operační systémy mobilních telefonů.

1.2 Hardware

Systém Asset je vystavěn na hardwarové struktuře, která je schopna velmi náročné bezpečnostní činnosti po dlouhou dobu bez odstávky.



Obr. 1: Hardwarová struktura

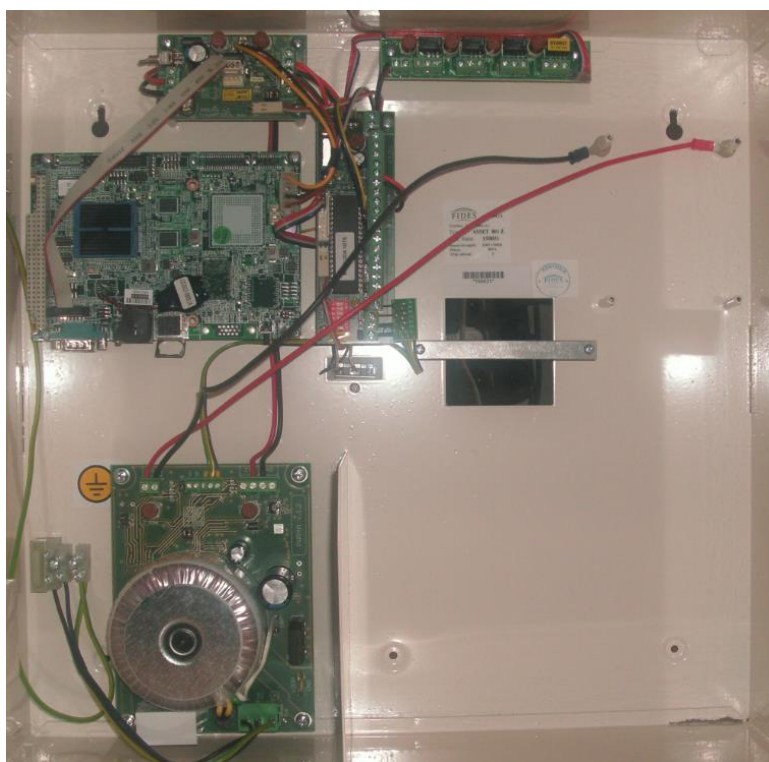
1.2.1 Řídicí jednotka

Zabezpečovací ústředna je v systému Asset je srdcem celého systému. Jedná se o průmyslový počítač s operačním systémem Linux, napájecí měnič pro desku počítače a linkový modul řešící základní údaje spojené s během systému.

Součástí ŘJ mohou být také až 3 expandéry, což jsou zásuvné moduly, které mohou každý řídit až 4 linky RS 485 a rozšiřovat tak počet připojitelných linek na 12. Mezi volitelné varianty připojitelných zařízení a modulů, které jsou součástí ŘJ, patří také modul Asset Depo řešící přebírání linek v redundantním režimu ŘJ, napájecí zdroj 12V, komunikátory na dohledová přijímací poplachová centra (DPPC), modul fólie vyhodnocující pokus o vytvoření otvoru do skříně ŘJ nebo modul regulující teplotu v ŘJ.

1.2.1.1 Asset 801Z, 804Z

Asset 801Z je nejmenší variantou ŘJ, která umožňuje vyvedení linky RS 485 přímo z měniče napětí pro desku počítače bez nutnosti použití expandéru. Tato jednotka je v nové verzi rozšiřitelná na variantu Asset 804Z zasunutím modulu expandéru pro 4 linky RS 485 do měniče. V takovém případě získáme ŘJ s možností připojení 4 x 30 modulů.[2]



Obr. 2: Asset 801 Z

ŘJ typu 801Z a 804Z jsou vybaveny 12V napájecím zdrojem PWR4A, který poskytuje dostatečný výkon pro nabíjení zálohovací baterie, napájení ŘJ a napájení modulů na linkách.[2]

1.2.1.2 Asset 804,808,812

Větší varianta ŘJ Asset, která je vybavena oproti variantám Asset 801Z a 804Z výkonnější deskou průmyslového počítače a deskou expander base (EB) pro zasunutí až třech expanderů. Právě počtem zasunutých expanderů se liší typ ŘJ a počet použitelných linek RS 485.

ŘJ 804 až 812 neobsahuje napájecí zdroj, který bývá řešen u této varianty externí formou. K použití externího zdroje jsou dva důvody a to použití většího a výkonnějšího zdroje PWR533, který zabírá více místa a také z důvodu instalace EB do skříně ŘJ.[3]

1.2.2 Ovládací panely

Ovládací panely jsou moduly připojitelné na linku RS 485, které umožňují ovládání systému bez použití nadstavbové části a poskytují informace o stavu systému. K ovládacím panelům je možno připojit čtečku karet a s použitím vstupů a výstupů řídit stav dveří.

1.2.2.1 KMU-4

Nejpoužívanějším typem ovládacích panelů je klávesnice KMU-4, která vychází z dnes již nevyráběné varianty KMU-3. Ovládací panel KMU-4 umožňuje ovládání systému prostřednictvím tlačítek numerické klávesnice a dvouřádkového informačního displeje. Ke každé instalaci Asset musí být připojen alespoň jeden ovládací panel umožňující lokální zobrazení poplachů. V aktuální nabídce modulů Asset toto splňuje pouze KMU-4[4]



Obr. 3: Elektronika KMU-4

Ovládací panel KMU-4 umožňuje po přihlášení uživatele v závislosti na právech tohoto uživatele měnit stav zastřežení podsystému, rušit poplachy, vytvářet uživatele, měnit režim topení nebo prohlížet historii systému. Po přihlášení v režimu „Technik“ pak umožňuje například korektní vypnutí ŘJ nebo základní diagnostiku systému, změna konfigurace prostřednictvím ovládacích panelů není z důvodu komplexnosti systému možná. [4,5]

1.2.2.2 KMU-6

Ovládací panel KMU-6 je varianta docházkového terminálu, která umožňuje vkládání docházkových událostí do systému Asset. Výhodou této varianty docházkového terminálu je nízká cena. Od této varianty je však ustupováno z důvodu zastaralé konstrukce a je nahrazována moderním řešením KMU-7[6]

1.2.2.3 KMU-7

Ovládací panel KMU-7 je zařízení sloužící jako docházkový terminál systému Asset. Prostřednictvím barevného dotykového displeje a bezkontaktní čtečky karet je možno do systému zadávat docházkové události, například příchod do zaměstnání nebo plánovat dovolenou. Tyto docházkové události lze následně exportovat do profesionálních docházkových systémů. KMU-7 mimo zaznamenávání docházkových událostí umožňuje také jednoduché ovládání systému spouštěním aktivit. [7]



Obr. 4:KMU-7

Jádro docházkového terminálu KMU-7 je řešeno mikropočítačem s vyměnitelným firmwarem, a tak je velmi snadno možné budoucí rozšiřování ovládacího terminálu o nové funkce. V závislosti na použité verzi firmware se KMU-7 chová jako terminál připojitelný na linku s řízením činnosti ŘJ, nebo je použitelný jako autonomní jednotka, kdy prostřednictvím počítačové sítě odesílá data do nadstavbového software a ŘJ tak vůbec nepotřebuje. [7]

1.2.3 Dveřní jednotky

Dveřní jednotky systému Asset jsou moduly připojitelné na linku RS 485. Jejich hlavním úkolem je spínání zámků dveří a monitorování stavů dveří. Ke dveřním jednotkám se připojují čtecí hlavy, jejichž výběr je velmi široký z důvodu nezávislosti na konkrétním typu čtecích hlav nebo na výrobci. Jediným požadavkem je, aby čtečka komunikovala prostřednictvím rozhraní Wiegand. To umožňuje připojení nejen čteček v klasickém pojetí, ale také například biometrických terminálů, které jsou schopny údaje odesílat rozhraním Wiegand. V závislosti na typu čtečky je možno připojit také některé čtečky komunikující přes RS 232. U připojovaných čteček je umožněno použití algoritmů pro hardwarové dešifrování karet soukromého i státního sektoru.[8]



Obr. 5:Dveřní jednotka Asset-20

Dveřní jednotky jsou vyráběny ve variantě pro připojení jedné čtecí hlavy a jedné dveří nebo ve variantě pro připojení dvou čtecích hlav a jedné dveří. Toto umožňuje řízení vstupu na režimových pracovištích s počítáním osob v zónách. Vstupní svorky dveřních jednotek umožňují připojení tlačítka pro povolení vstupu návštěvy, výstupu cizího PZTS nebo ovládání vlastní PZTS v kombinaci s přiložením karty. [8,9]

1.2.4 Vstupně-výstupní moduly

Vstupně-výstupní moduly systému Asset jsou zařízení, která ŘJ prostřednictvím RS 485 poskytují informace o okolním prostředí a umožňují zpětně prostředí ovlivňovat.

1.2.4.1 LML-8

Vstupně-výstupní linkový modul obsahuje 8 vstupů s vyvážením DEOL použitelných pro připojení smyček PZTS, SKV a MaR, těchto 8 vstupů je možno přepnout do režimu proudových smyček s měřením analogových veličin. Linkový modul je vybaven také dvěma vstupy pro připojení datově komunikujících analogových čidel MaR. Své okolí může Asset ovlivňovat prostřednictvím 8 tranzistorových výstupů linkového modulu. [10]



Obr. 6: Modul LML-8

Pro vyšší zatížitelnost výstupů je možnost doplnění o relé moduly. Tyto relé moduly pro připojení na linkový modul jsou dodávány v provedení lišty obsahující 1, 4 nebo 8 relé se zatížitelností do 1 A a v provedení lišty s 8 relé se zatížitelností do 10 A. [11]

1.2.4.2 Octopus

Bezdrátový linkový modul Octopus slouží pro připojení detektorů systému Octopus společnosti 3S Sedlák, které komunikují na frekvenci 868MHz. Bezdrátový systém Octopus je certifikovaný pro III. stupeň zabezpečení a nabízí mimo klasické detektory PZTS, jako jsou detektory pohybu a detektory tříštění skla, také pro veřejnost méně obvyklé detektory pro předmětovou ochranu jako jsou podstavce pod předměty, závěsné detektory nebo kapacitní detektor pro hlídání přítomnosti plátna obrazu. Mimo detektory patří do systému Octopus také tísňová a ovládací tlačítka, které umožňují přivolání pomoci nebo například odstřežení objektu. [12]

1.2.5 Komunikační moduly

Pro komunikaci na DPPC Asset mimo vlastní ethernetové rozhraní používá komunikační moduly připojitelné na sériový port desky průmyslového počítače řídicí jednotky. Komunikační moduly bývají osazeny jako součást řídicí jednotky.

1.2.5.1 PZL

Zařízení PZL slouží k přenosu dat na DPPC Latis s využitím protokolu FXP. Veškerá komunikace může být zálohována prostřednictvím až 3 záložních kanálů v závislosti na použitém komunikačním režimu. Ve variantě PZL-10 je možné k přenosu využít ethernet, GPRS, SMS nebo jednotnou telefonní síť (JTS). Varianta PZL-11 nahrazuje využití GSM sítě prostřednictvím připojení na rádiovou síť Morse. [13]



Obr. 7:PZL-10

1.2.5.2 Ademco Contact ID

Přenosový modul Ademco Contact ID (CID) slouží jako varianta přenosu na DPPC cizích výrobců skrze JTS bez záložní přenosové trasy. Nevýhodou využití CID je potřeba údržby aktuálních konfiguračních tabulek na straně DPPC, kdy nedochází k přenosu kompletní informace, ale pouze k číselnému vyjádření události.[14]

1.2.6 Klíčové trezory KWAD

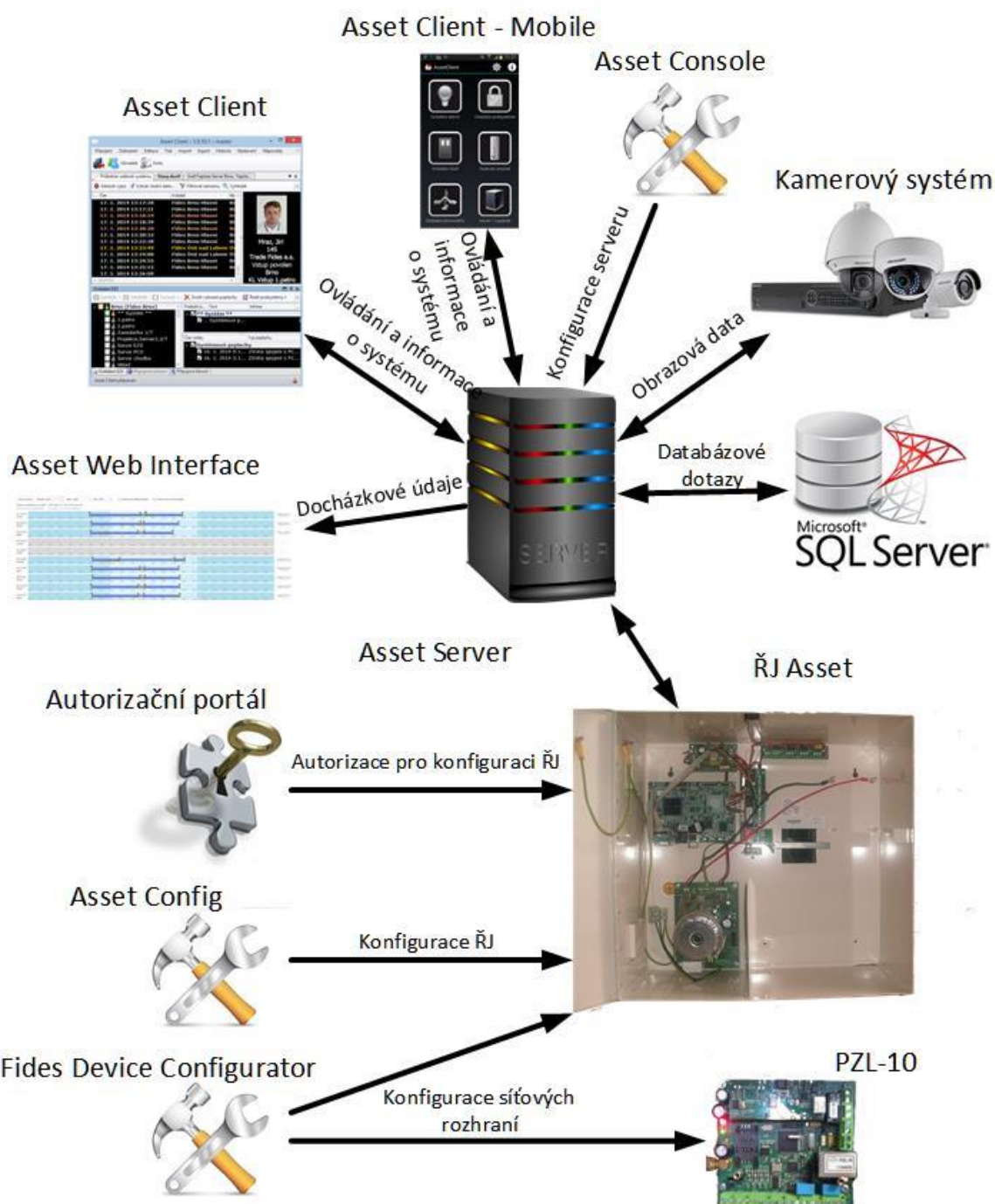
Klíčový trezor KWAD je zařízení, které je v systému použitelné jako náhrada nebo doplnění SKV s elektromagnetickými zámky. Klíčové trezory v závislosti na oprávnění uživatele uvolní po přiložení karty klíč a událost zaznamenají do paměti. Klíčové trezory KWAD jsou vyráběny ve variantě pro připojení na linku RS 485 ŘJ nebo jako autonomní zařízení pro připojení po počítačové síti k ASVR.[15]



Obr. 8:KWAD-15

1.3 Software

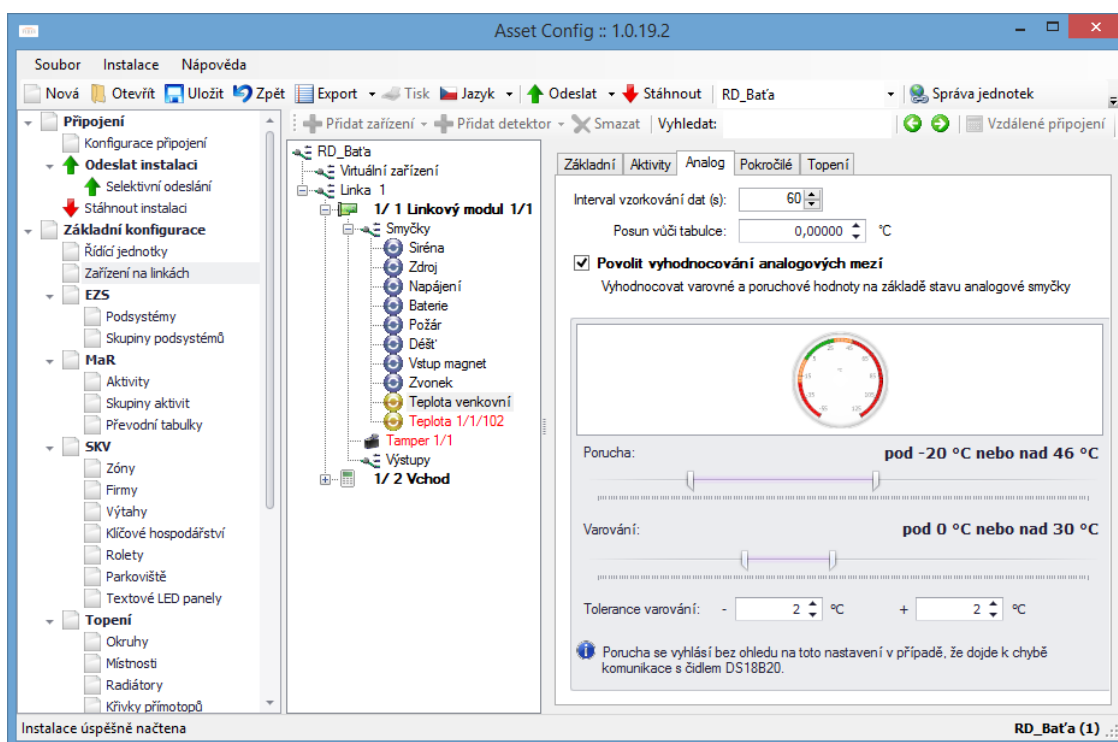
Nadstavbová softwarová úroveň je prezentována velkým množstvím softwarů, sloužících k softwarové integraci a k usnadnění práce techniků a uživatelů. Softwary jsou určeny pro operační systém Windows a operační systémy Android, Windows Mobile a iOS mobilních telefonů.



Obr. 9: Softwarová struktura

1.3.1 Asset Config

Konfigurační software Asset Config (ACFG) slouží k nastavení struktury, vazeb a vlastností systému Asset. Konfigurace systému skrze klávesnici kvůli komplexnosti systému není možná. V aplikaci se mimo jiné nastavuje typ řídicí jednotky, adresy jednotlivých modulů a jejich chování, způsob připojení na DPPC, připojení na ASVR, vazby mezi událostmi v systému, připojení do sítě BACnet nebo pravidla pro SKV. Vytváření konfigurace zařízení probíhá bez připojení k ŘJ a hotová konfigurace je pak jednorázově odeslána do ŘJ po počítačové síti. Tímto způsobem lze provádět ve fungujícím systému změny za běhu, aniž by uživatel pocítil jakékoliv omezení. Konfigurační software připojitelný k systému prostřednictvím počítačové sítě umožňuje také provádění změn v systému bez nutnosti fyzické přítomnosti technika v objektu. [16]



Obr. 10: Asset Config [17]

Asset Config obsahuje nástroje pro online diagnostiku systému zobrazením stavu modulů a jejich vstupů, spuštěním vizualizované klávesnice systému nebo stažením historie událostí z řídicí jednotky. V software je možno generovat tabulky pro CID nebo textovou zprávu o konfiguraci systému, pro předání uživateli systému jako součást předávacího protokolu. [16]

1.3.2 Asset Server

Asset Server je základní služba softwarové vrstvy, ke které se připojují ŘJ systému Asset, docházkové terminály nebo cizí zařízení a aplikace, nad kterými ASVR provádí softwarovou integraci. ASVR veškerá přijatá data ukládá do databáze MS SQL a tyto pak dále distribuuje uživatelům, zařízením nebo cizím aplikacím.[18]

Služba ASVR umožňuje automatické rozesílání e-mailů dle skriptů, připojení s PeS institucí, odesílání dat do docházkových systémů nebo automatické logování auditu změn v systému. Mezi připojitelná cizí zařízení patří čtečky otisků prstů Bioscrypt 4G V-flex, kamerové systémy Avigilon, HikVison, Geutebrück, Dedicated Micros nebo kamery podporující protokol ONVIF. Tato zařízení, mimo kamer s protokolem ONVIF, jsou připojována prostřednictvím SDK jednotlivých výrobců a ASVR je tak dále rozšiřitelným softwarem.[18]

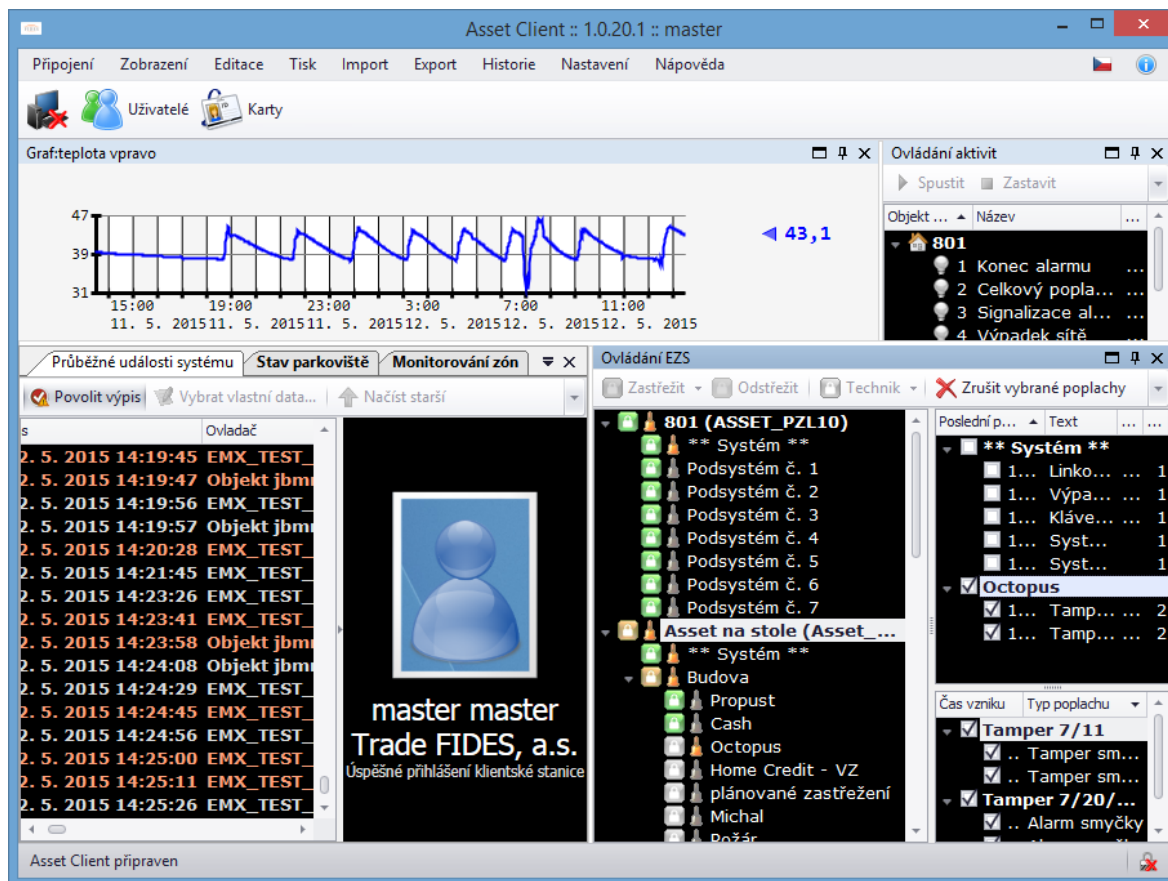
1.3.3 Asset Console

Správcovská aplikace Asset Console (ACNS) se společným instalátorem jako Asset Client (ACLT) slouží k nastavení ASVR. V programu se nastavuje databáze, ke které se server připojuje včetně souvisejících parametrů, jako je počet pokusů o připojení k databázi před vyhlášením chyby nebo četnost tvorby databázových záloh a způsob údržby databáze. Dále v aplikaci probíhá nastavení pravidel pro připojování jednotlivých zařízení jako například nastavení TCP portu, na kterém server naslouchá příchozím spojením, konfigurace ovladačů zařízení, skrze které se tato zařízení připojují, nebo dokonce plná konfigurace menších zařízení, jako jsou například autonomní KMU-7 nebo biometrické terminály. V ACLT jsou již existujícím uživatelům přidělována práva přihlášení do aplikací nadstavbové části a práva pro přístup k jednotlivým modulům ACLT.[19]

1.3.4 Asset Client

Jedná se o základní operátorskou a správcovskou aplikaci pro ovládání systému v nadstavbové části. Tato aplikace je pouhým zobrazovačem a ovladačem, který data neukládá, ale načítá je ze serveru při každém připojení. Při průniku neoprávněné osoby do počítače s aplikací ACLT tak nehrozí žádné odcizení dat uložených v systému Asset. V aplikaci je možno ovládat stavy střežení podsystémů a přemostění smyček, rušit poplachy, ovládat aktivity a tím výstupy zařízení nebo nastavovat a přepínat režimy topení. V softwaru ACLT probíhá správa systémových uživatelů, jejich přístupových práv z pohledu SKV a PZTS nebo správa otisků prstů pro biometrická zařízení. Jako nástroje pro kontrolu poskytuje ACLT prohlížení

průběžných událostí, zobrazení obrazu z kamer, výpis stavu připojených ŘJ včetně jejich aktuálního vytížení, zobrazení stavu dveří nebo například nahlédnutí do logu systémového auditu s uživatelskými změnami a jejich autory. [20]



Obr. 11: Asset Client[21]

1.3.5 Asset Client - Mobile

Tenká verze software ACLT pro mobilní zařízení s operačním systémem Android 4.0 a vyšším slouží pro základní vzdálenou správu systému. Z pohledu PZTS umožňuje ovládání podsystémů, přemostění smyček, rušení poplachů a sledování historie. Dále je umožněno v souvislosti s MaR sledovat historii analogových smyček a ovládat výstupy prostřednictvím aktivit. Z pohledu SKV Client zobrazuje stavy dveří a umožňuje spínání elektromagnetických zámků. Posledním prvkem, který mobilní aplikace Asset Client Mobile nabízí je virtuální klávesnice KMU – 4, skrze kterou lze provádět stejné operace jako z klávesnice, která je hardwarově připojena k ŘJ. Možností aplikace je vytvářet widgety na ploše, skrze které lze rychle ovládat konkrétní prvky výše zmíněných kategorií.[22]

1.3.6 Asset Control

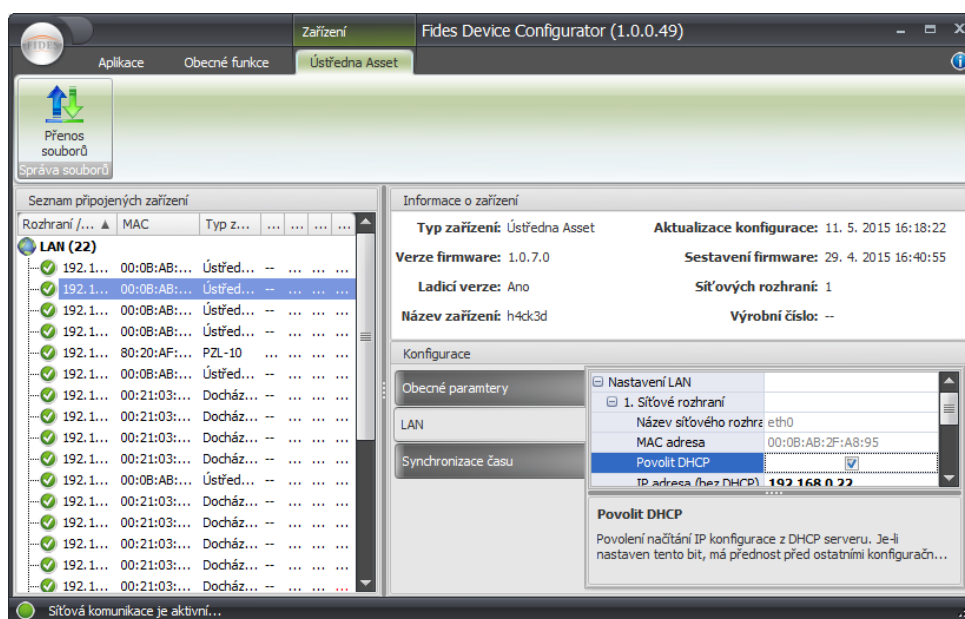
Asset Control je jednoúčelový software pro operační systém Windows, který na hlavní panel obrazovky umožní přidat ikonu, prostřednictvím které dojde například k sepnutí zámku konkrétních dveří. Tato aplikace je hojně využívána k otevření dveří návštěvě aniž by se pracovník v kanceláři musel zvednout a dveře ručně otevřít.[23]

1.3.7 Asset Control-Mobile

Varianta aplikace Asset Control pro mobilní zařízení s operačními systémy Android, Windows a iOS slouží jako jednoduchý softwarový otevřáček, který uživatelům umožňuje otevřít si dveře s elektromagnetickým zámekem. Díky tomuto software není nutné, aby uživatel vlastnil RFID kartu, veškeré ovládání dveří může probíhat prostřednictvím telefonu.[24]

1.3.8 Fides Device Configurator

Fides Device Configurator (FDC) slouží ke konfiguraci síťových rozhraní produktů společnosti Trade Fides a k nastavení všech parametrů zařízení PZL. Nastavením síťových rozhraní se rozumí nastavení IP adresy, masky, výchozí brány a DNS v síti LAN, do které jsou zařízení připojena prostřednictvím ethernetu. Na zařízení PZL je tento parametr rozšířen na nastavení konektivity na DPPC prostřednictvím LAN, GSM, rádiové sítě Morse a JTS a na nastavení zjednodušené osmismýčkové interní PZTS.[25]



Obr. 12: Fides Device Configurator[26]

1.3.9 Asset Guestbook

Asset Guestbook je aplikace pro zadávání návštěvníků do systému Asset, přidělování návštěvnických RFID karet a správu tras čteček, které jsou jednotlivým návštěvníkům zpřístupněny. Tato aplikace bývá doplněna o OCR čtečku dokladů, která v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů načte patřičné údaje o návštěvě bez nutnosti manuálního vyplňování.[27]

1.3.10 Asset Monitor

Jde o pomocnou aplikaci pro strážného v objektu s velkým pohybem stálých zaměstnanců, která umožňuje zobrazovat na obrazovce fotografie majitelů karet, které jsou přikládány k definovaným čtečkám. Strážný pak již pouze vizuálně na základě podobnosti kontroluje, zdali osoba zobrazená na fotografii je totožná s osobou, která přiložila ke čtečce kartu.[28]

1.3.11 Asset Web Interface

Asset Web Interface (AWI) je aplikace, jejímiž prostřednictvím je možno kontrolovat nebo v případě dostatečných oprávnění upravovat docházku integrovanou v systému Asset. Aplikace běží jako serverová aplikace na IIS operačního systému Windows a je zpřístupňována prostřednictvím webových prohlížečů, což uživatelům umožňuje zpřístupnění dat bez nutnosti instalace speciální softwarů.[29]

1.3.12 Autorizační portál

Autorizační portál je serverová aplikace fungující na IIS operačního systému Windows, která umožňuje zákazníkům rozsáhlých systémů řídit přístup techniků servisních firem ke konfiguraci ŘJ připojených do počítačové sítě. Autorizační portál povoluje přístup do konfigurace na principu generování časového tokenu šifrovaného asymetrickou kryptografií.[30]

1.3.13 Fides Software Storage

Fides Software Storage je souhrn aplikací pro správu automatických aktualizací softwarů společnosti Trade Fides bez nutnosti kopírování instalačních balíčků. Souhrn aplikací zahrnuje správcovské rozhraní pro přidávání aktualizací do databáze a rozhraní, které zajišťuje dostupnost aktualizací ze strany aplikací a uživatelů.[31,32]

2 PŘEHLED ŠKOLICÍCH STŘEDISEK

V praxi je používáno velké množství školení a školicích středisek, které se liší způsobem provedení a obsahem. V následujících kapitolách bude rozebráno, jaké důvody pro školení existují, jaké formy školení jsou používány a na několika příkladech budou v praxi realizovaná školicí střediska popsána a systemizována.

2.1 Význam školicích středisek v PKB

Školením zaměstnanců v průmyslu komerční bezpečnosti (PKB) dochází k navýšení přidané hodnoty, kterou je zaměstnanec schopen svému zaměstnavateli poskytnout. Zaměstnanec, který je pravidelně školen, je schopen přemýšlet a odvádět práci na vysoké odborné úrovni. Takoví zaměstnanci jsou na trhu práce velmi žádaní.[33]

Školení v oboru montáže bezpečnostních technologií není v současné době vyžadováno žádným zákonem, vyhláškou nebo normou. Jedinou výjimku tvoří montáže EPS, pro které norma ČSN EN 54 a potažmo vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb v úpravě vyhláškou 268/2011 Sb. nařizuje montáže proškolenými certifikovanými technikami.

Tabulka č. 1: Kvalifikace montážních pracovníků v PKB[34]

	<i>Kvalifikace montážní organizace:</i>	<i>Úroveň použité techniky:</i>	<i>Specifické zařízení:</i>	<i>Cena montáže:</i>	<i>Poznámka</i>
<i>I.</i>	<ul style="list-style-type: none"> <i>Speciální znalosti</i> <i>Montáž výhradně prokazatelně proškolenými společnostmi</i> 	<i>Profesionální</i>	<i>PZTS stupeň 3-4</i> <i>EPS</i>	<i>Vysoká</i>	<i>Pojišťovny vyžadují montáž výhradně proškolenými montážními společnostmi výrobcem zařízení.</i>
<i>II.</i>	<ul style="list-style-type: none"> <i>Všeobecné znalosti</i> <i>Montáž všeobecně znalými společnostmi</i> 	<i>Standardní</i>	<i>PZTS stupeň 2-3,</i> <i>SKV,</i> <i>CCTV</i>	<i>Střední</i>	
<i>III.</i>	<ul style="list-style-type: none"> <i>Bez odborné kvalifikace</i> 	<i>Široká veřejnost</i>	<i>PZTS stupeň 1-2</i>	<i>Nízká</i>	

Výrazně odlišná situace se školeními je v segmentu soukromých bezpečnostních služeb, které se zaměřují na ostrahu majetku a osob a služby soukromých detektivů. Tento segment má povinná školení jasně specifikovaná a ve spojení s koncesovanou formou živnosti také právně vynutitelná. Tato netechnická část segmentu PKB ovšem není předmětem zpracování diplomové práce. [35]

2.2 Účel školení

Důvodů školení může být mnoho, v této podkapitole jsou zmíněny nejčastější druhy školení zaměstnanců v průmyslu komerční bezpečnosti dle účelu.

2.2.1 Bezpečnost a ochrana zdraví při práci

Zákonně povinné školení je zajišťováno zaměstnavatelem a musí být prováděno odborně způsobilou osobou. Školení má za cíl seznámit zaměstnance s riziky a přijatými opatřeními souvisejícími s výkonem práce. Při tomto druhu školení je potřeba zohledňovat předpisy k zajištění bezpečnosti a ochrany zdraví, předpisy pro bezpečnou práci s technickými zařízeními a stanovení pracovních podmínek. Provedená školení bezpečnosti práce jsou základním předpokladem pro vyjmutí z odpovědnosti za pracovní úraz zaměstnance. [36]

2.2.2 Obchodní školení

Cílem obchodního školení je seznámení posluchačů s nabízenými produkty a službami za účelem prodeje a rozšíření dobrého jména společnosti. Během těchto školení jsou posluchači seznamováni s portfoliem produktů školitele a některými parametry. Parametry zařízení a služeb, které nejsou obecně známy, bývají vysvětleny a případně porovnány s jinými zařízeními pro lepší představu posluchačů. Pro zvýšení atraktivity školení a lepší pochopení je vhodné školení doplnit praktickými ukázkami. Během obchodních školení až na výjimečné případy nedochází k seznámení s konfigurací zařízení a možnými závadami zařízení.

2.2.3 Technické školení

Technická školení jsou určena montážním technikům, servisním technikům a projektantům. Během těchto školení dochází podobně jako u obchodních školení k seznámení s produkty, ovšem technických parametrů je zdůrazněno více a jsou probrány více do hloubky včetně vazeb mezi jednotlivými částmi systémů. Během těchto školení dochází k seznamování s nastavováním produktů, které jsou předmětem školení, k upozornění na potenciální chyby nebo k simulaci reálných činností, kterých se posluchači účastní.

2.2.4 Uživatelské školení

Školení prováděná technikem seznamují koncové uživatele s provozem, signalizací a ovládáním systému. Tato školení běžně probíhají po ukončení instalace v místě, kde bude systém používán, a jsou jedním z předpokladů pro předání díla zákazníkovi. Vhodně provedené uživatelské školení společně se správně provedenou instalací umožní zákazníkovi využití všech možností, které produkt nabízí a vylepšuje tak image společnosti i produktu. Dále lze vyškolením uživatele eliminovat riziko poškození systému nesprávnou manipulací nebo plané servisní zásahy na naprosté minimum.

2.2.5 Aktualizační školení

Aktualizační školení má za úkol již vyškoleného posluchače seznámit s novými výrobky a funkcemi. Aktualizační školení bývají nejčastěji významově spojená s technickým druhem školení umožňující projektování a konfiguraci systémů dle nejnovějších trendů. Tato školení jsou mnohdy vedena neformálním stylem spojená s diskusí o zkušenostech posluchačů.

2.3 Forma školení

Pro školení jsou v závislosti na důvodech a rozsahu školení a úrovni posluchačů používány nejrůznější formy, kdy každá forma má své výhody, ale také slabé stránky. Oddělení forem školení nelze chápat striktně, neboť se mnohdy v praxi prolínají.

2.3.1 Teoretická forma

Teoretická forma školení je rychlou nízkonákladovou variantou seznámení posluchačů s potřebnými skutečnostmi. Při této formě školení jsou používány jako prostředky předání informace přednáška doplněná prezentací, případně diskuse s aktivním zapojením účastníků. Vhodným doplňkem rozšiřujícím představu posluchačů jsou pasivní ukázky a videoukázky, které zaujmou pozornost. Tato forma je vhodná zejména pro školení za obchodním účelem nebo z důvodu bezpečnosti práce. Tato forma bývá velmi často nesprávně používána pro technická školení.

2.3.2 Kombinovaná forma

Kombinovaná forma školení je sloučením formy teoretické, díky které posluchač získá potřebné znalosti, a praktického cvičení pro hluboké zažití nově získaných informací. Tato forma vychází ze všeobecně známé a uznávané Komenského metody „vysvětli, ukaž, nech

vyzkoušet“ a má velmi dobré výsledky, kdy si posluchači probíranou látku zapamatují společně se schopností uvést ji později do praxe. Nevýhodami této metody školení mohou být vyšší časová náročnost a cena.[37]

2.4 Školící střediska a školení v praxi

V této části diplomové práce jsou zmíněny příklady školení zaměřené na bezpečnostní a informační technologie, kterých jsem se osobně zúčastnil, nebo které mi byly poskytnuty prostřednictvím jiných osob včetně školicích materiálů.

2.4.1 KNX

Jedná se o zprostředkované informace o školení zaměřeném na systémové elektroinstalace. Školení na KNX je členěno na několik úrovní. V uváděných případech byla nižší úroveň školená společností ABB a vyšší úroveň společností Schneider electrics. Účastníci obou školení obdrželi velmi obsáhlé materiály kopírující obsah přednášky. Do materiálů si lze dělat vlastní poznámky a zachytávat tak informace subjektivně důležité pro každého účastníka v kontextu přednášky. Školení byla v obou případech členěna do teoretické části zaměřené na získání informací a praktické části pro reálné vyzkoušení získaných informací. Obě varianty byly zakončeny testy na vysoké úrovni obtížnosti. Některé otázky v testech však nesouvisely s technickým zaměřením a byly tak zbytečné.

2.4.2 Jablotron

Školení techniků a projektantů na zabezpečovací systémy nejprodávanějšího českého výrobce jsem se zúčastnil dvakrát osobně a to v roce 2009 a v roce 2014. Za tuto dobu nedošlo ke změně formy školení, došlo pouze ke změně technologií. Školení, ačkoliv je označováno za technické, je svým obsahem spíše obchodní a představuje formou prezentací a názorných ukázek portfolio zařízení, která společnost vyrábí a dodává. Součástí dvoudenního školení s dotací cca 10 hodin čistého času nebyla praktická činnost, při které by si posluchači prakticky vyzkoušeli předváděné systémy. Při pozdějším reálném kontaktu se systémem, který byl školen, jsem byl schopen se zařízením pracovat pouze podle manuálu, bez ohledu na absolvování školení. Informace získané na školení jsou nedostatečné pro instalaci a oživení systému. Školení společnosti Jablotron je zakončeno testem, který všichni posluchači na základě týmové spolupráce zvládnou. Díky zvládnutému testu dostanou certifikát, který společně s obvyklými požadavky, jako je platný certifikát o absolvování zkoušky dle vyhlášky 50, opravňuje k instalaci školených zařízení.

2.4.3 Variant

Společnost Variant dodává na český trh velké množství ústředen PZTS a EPS a jako podporu prodeje provádí bezplatná školení techniků na dodávané technologie. Byly mi zprostředkovány informace o technických školení PZTS Digiplex Evo, Magelan a EPS Detectomat. Struktura všech školicích lekcí byla shodná, kdy na počátku lekce byly předány teoretické informace doplněné praktickými ukázkami. Během teoretické části došlo k užitečnému zopakování známých informací, jako je výpočet úbytků napětí na vedení nebo výpočet potřebné kapacity baterie. Následně si posluchači vyzkoušeli drobné technické zásahy do systémů prostřednictvím klávesnice bez využití softwarů. Na závěr školení dostanou všichni posluchači certifikát o absolvování školení bez absolvování závěrečného testu.

2.4.4 Axis

Školení bylo pořádáno za obchodním účelem se zaměřením na kamery a kamerové systémy společnosti Axis. Ve velmi krátkém časovém úseku jednoho dopoledne bylo představeno portfolio společnosti v podobě názvů a technických parametrů, které posluchačům s teoretickými znalostmi bez praktických znalostí utvořily pouze rámcovou představu. Součástí obchodního školení mělo být praktické představení 3 kamer, z nichž se jednu nepodařilo zprovoznit vůbec a druhou s velkými obtížemi. Takovéto technické potíže mohou způsobovat nedůvěru v prezentovaný produkt, což v případě marketingového školení snižuje význam školení.

2.4.5 CCNA Exploration

Školení na profesionální řadu síťových komponentů Cisco Systems, které jsem absolvoval ve variantě CCNA Exploration, je děleno do 4 samostatných semestrů, z nichž každý je zakončen zkouškou a získáním certifikátu, který má bez ohledu na absolvování dalších semestrů již samostatný význam – další semestry jsou rozvíjením základních znalostí a znalostí o dalších technologiích. Semestr je souhrnem 12 lekcí, které na sebe vzájemně navazují. Struktura lekce je členěna na část přednáškově diskusní, během které je přednesena potřebná teorie s diskusí o bodech, které nebyly posluchačům jasné. Diskuse udržuje posluchače v pozoru a zásadně se tak liší od samostudia. Ve druhé části školicí lekce probíhá dle podrobného scénáře prohloubení získaných informací jejich vyzkoušením v simulačním software nebo na reálných zařízeních. Celému procesu je přítomen odborník s certifikací vyšší úrovně, který pomáhá v případě nejasností nebo vzniklých chyb. Každá lekce je zakončena testem,

který uživatel vyplňuje online mimo školení a ověřuje si tak, zdali si zapamatoval ze školení všechny důležité údaje. Celý semestr školení je zakončen velkým online testem, který je vyplněn technikem na poslední lekci a který zahrnuje informace získané během celého studia. Kromě testu je pro uzavření semestru potřeba předvést také praktickou ukázkou konfigurace dle scénáře, jež částečně zahrnuje všechny prostudované okruhy.

Kvalitní školicí střediska v podání společnosti Cisco jsou marketingovou strategií společnosti, kdy jsou na střední a vysoké školy v oboru informačních technologií dodána potřebná zařízení a aktuální materiály pro školení včetně prezentací, simulačních softwarů a testů. Tato školicí střediska jsou podporována školením kvalitních lektorů na vyšší úrovni. Strategie vychází z předpokladu, že student, který ukončí studium a nastoupí na pozici správce sítě, bude používat technologie, se kterými byl již dříve seznámen. Společnost Cisco pak právě těmto technikům prodává velké množství zařízení a i přes vysoké náklady na školení generuje z dlouhodobého hlediska vysoké zisky.[38]

2.4.6 RipEX

Kombinované marketingově technické školení společnosti Racom představuje v marketingové části stručně a přehledně produkty společnosti. Po tomto krátkém úvodu sloužícím k zaujetí pozornosti pracovník technické podpory provede přednáškově diskusní část školení. V dalším kroku si účastníci školení vyzkouší získané informace při konfigurování reálných zařízení. Školení bylo zvládnuto během jediného dne a bylo provedeno ve velmi rychlém tempu, kterému většina posluchačů nestačila. Vzhledem k obsáhlosti systému nebyly vyzkoušeny všechny varianty konfigurace, které zařízení RipEX nabízí a například část zaměřená na možné problémy, které mohou vznikat, byla zcela opomenuta. Při reálném nasazování produktů pak tato skutečnost způsobuje problémy. Vzhledem ke skutečnosti, že v konkrétním případě byla mezi školením a prvním nasazováním produktu velká časová prodleva, došlo k zapomenutí části informací.

2.4.7 Abbas

Technické školení společnosti Dallmeier se zaměřuje na síťová záznamová zařízení pro kamerové systémy, které tato společnost vyrábí. Toto jednodenní školení kombinované formy se proti jiným školením lišilo velmi hlubokým zaměřením na potencionální problémy při

nastavování a oživování systémů. Takto provedené školení je užitečné pro techniky při oživování a servisních pracích na zařízení a usnadňuje činnost technické podpory, která se nemusí účastnit řešení běžných závad.

2.4.8 Acti

Obchodní školení prováděné společností Olympo je zaměřené na kamery Acti, jejichž je společnost Olympo distributorem. Školení bylo určeno pro obchodníky montážních firem s cílem předat dostatek informací, aby tyto kamery dále nabízeli koncovým zákazníkům. Školení kombinované formy v teoretické části představovalo kamery, kdy jejich parametry a vlastnosti pro lepší představu deklarovalo videi. Na závěr školení bylo účastníkům umožněno si za pomoci přednášejícího prezentované kamery reálně vyzkoušet a ověřit si tak pravdivost dříve prezentovaných údajů.

2.4.9 Moxa

Technické školení kombinované formy společností Elvac na bezdrátové síťové prvky Moxa, bylo atypické vysokým počtem účastníků. Na začátku školení bylo obchodně představeno portfolio dostupných produktů s následujícím přechodem k technické části vlastností a konfigurace jediného produktu. Školení bylo velmi krátké, ale tato skutečnost byla vyřešena zaměřením veškeré pozornosti technické části školení na jediný produkt. Po seznámení s tímto produktem bylo do skupin po 4 osobách předáno školené zařízení. Účastníci si následně vyzkoušeli získané znalosti v praxi skupinovým vytvořením bezdrátové sítě ze zmíněných zařízení.

2.4.10 Stávající systém školení Asset

Stávající systém školení integrovaného poplachového systému Asset je prováděn v množství variant jako obchodní i technické školení. Rozsah školení je 1-2 dny v závislosti na školené variantě, počáteční úrovni posluchačů a požadované výstupní úrovni. Školení bývá vedeno formou diskuze s praktickými ukázkami, ovšem bez možnosti osvojení naučených znalostí praktickým vyzkoušením v rámci školení. Závěrem školení je při technické variantě školení předán posluchačům certifikát o absolvování školení.

2.4.11 Dílčí závěry

Pro účastníky školení je důležité dostat vhodně strukturované informace v přiměřeném množství a rychlosti, které posluchače nepřehltí. Vhodného dávkování informací lze docílit omezením množství produktů, o nichž probíhá školení nebo natažením doby, která je školení věnována. Při natahování doby školení je důležité dbát na únavu posluchačů a školení případně rozdělit do více dní. Pro udržení získaných informací v paměti posluchačů jsou důležité ukázky systémů, v ideálním případě aktivně orientované, kdy posluchač prakticky školené činnosti provádí.

Důležitým faktorem školení, který umožňuje zapamatování si skutečností je provádění školení odborníkem z praxe, jenž látku prezentuje na skutečných příkladech. Školení, jehož předmět má zůstat v paměti posluchačů, vyžaduje samostudium spočívající v opakování informací ze školení. Motivací k tomuto samostudiu může být závěrečný test, který prověří znalosti posluchače. Ve většině zjištěných případů byl ovšem závěrečný test pouhou formalitou a neplnil skutečnou funkci.[37]

Během prezentace pro techniky a montážní pracovníky je vhodné přiznat potencionální chyby a problémy produktů a jejich možné řešení, které technikům při vzniku takové situace velmi ulehčí práci. Pro školení, které je doplněno o praktické ukázky, je důležitá důkladná příprava zamezující nechtěným chybám a omylům, jež snižují kredit zařízení i školitele. Dále je potřeba udržovat školicí materiály aktuální.

Vzhledem k vývoji technologií a k zapomínání nepoužívaných informací je důležitá dočasná platnost školení a existence obnovovacích a aktualizacních školení, které v oboru bezpečnostních technologií velmi často chybí. Další spíše výjimečnou skutečností je tvorba úrovní školení, které by od sebe oddělovalo montážní techniky se základními informacemi a techniky s hlubokou znalostí systémů.

II. PRAKTICKÁ ČÁST

3 ŠKOLENÍ

Potřeby školení pro systém Asset, veškeré znalosti a slabá místa techniků, montážníků a uživatelů vychází ze čtyřletých zkušeností na pozici specialisty technické podpory pro systém Asset společnosti Trade Fides, a.s.

3.1 Současný stav

Současný stav školení mohu posoudit dle školení montážních techniků ze dne 11. 3. 2015, které proběhlo centrále společnosti Trade Fides v Brně a kterého jsem byl účasten jako pozorovatel. Dalším východiskem pro posouzení současného stavu školení jsou problémy, se kterými se na technickou podporu obracují technici, kteří absolvovali školení a v současné době systémy montují.

Školení na systém Asset je řešeno formou technicky zaměřené teoretické neformální přednášky, během které posluchači interaktivně zasahují svými postřehy a dotazy. Přednášející na dotazy vhodně reagoval a odpovídal v rámci aktuálních znalostí.

V počáteční fázi školení byli technici seznámeni s webem společnosti Trade Fides a s dostupností aktuálních manuálů ke všem softwarům. Dle manuálu určeného pro projektanty, ve kterém je kompletní soupis veškerého dostupného hardwaru, byl během hodiny představen kompletní sortiment zařízení s upozorněním na nejružnější specifikace. Po tomto seznámení došlo ke změně předmětu školení na konfigurační software ACFG. Tato část zabrala přibližně hodinu a půl. Odpolední část školení byla věnována nadstavbové části se softwary ASVR, ACLT a ACNS.

3.1.1 Výhody současného stavu

Výhodou současného stavu je nízká časová náročnost, kdy se technici během jediného dne dozvědí v uceleném celku nezbytné informace, které jsou potřebné pro instalaci zabezpečovacího systému a jeho následné zprovoznění.

Další nespornou výhodou současného stavu je vysoká kvalifikace přednášejícího, jenž je schopen odpovídat na veškeré dotazy, které technici mají.

3.1.2 Slabé stránky současného stavu

Hlavní slabou stránkou současného stavu je, že si ze spousty informací, které jsou školeným teoreticky předány v krátkém časovém limitu v použitelném stavu, zapamatují pouze zlomkové množství.

Technici, kteří projdou tímto rychlým školením, si reálně nemohou vyzkoušet pod dohledem zkušeného školitele nabyté informace a v reálných podmínkách vytvářejí komplikovaná a neprůchodná řešení, protože nepochopili proces konfigurace.

Manuály, na které jsou technici odkazováni, jsou realizovány formou externích dokumentů, které technici nepoužijí a místo toho tvoří chyby anebo volají oddělení technické podpory. Vhodnější variantou by bylo manuály tvořit interaktivně formou kontextové nápovědy integrované v softwaru.

Další slabou stránkou je složité udržení aktuálnosti informací, které školitel technikům předává, z důvodu rychlého vývoje techniky a softwarů.

Závažným problémem při stávajícím systému školení je, že informace, které jsou školeny, nejsou testovány a certifikát za školení je tak předáván spíše za účast, než za reálně získané informace.

3.1.3 Dílčí závěr

Pro montážní pracovníky a obchodníky je tento systém školení dostačující. Pro projektanty a servisní techniky, kteří systémy uvádějí do provozu, však dostatečný není a potřebuje rozšíření na variantu, která poskytne dostatečné podklady pro pochopení systému a jeho vazeb.

3.2 Koncepce nového školicího střediska

Nové školicí středisko pro integrovaný zabezpečovací systém Asset je soustava devíti na sebe navazujících školicích lekcí doplněná o nultou lekci se vstupním testem a desátou testovací lekcí.

Pro absolvování školení je potřeba, aby školené osoby disponovaly počítačem s nainstalovaným operačním systémem Windows. Ostatní komponenty potřebné pro školení PZTS Asset, jako jsou hardwarové komponenty a softwarové vybavení, dodá provozovatel školení.

Školení je určeno pro osoby, které budou systém Asset konfigurovat a servisovat. Jedná se tedy o vyšší úroveň znalostí, než je potřeba předat například montážním pracovníkům, kteří

system pouze zapojují. Na základě očekávané vyšší výstupní úrovně je očekáván vstupní předpoklad školených osob, který bude během školení využit. Jedná se o znalosti z oblasti PZTS, SKV, OS Windows, MS SQL a počítačových sítí. Dále je po účastnících školení požadována vyhláška 50 minimálně na úrovni §5 - pracovníci znalí.

3.2.1 Vstupní testy

Před zahájením školení technika pro systém Asset je ze strany budoucího technika nutno prokázat znalosti z oblastí počítačových sítí, elektrotechniky a mírně pokročilé znalosti operačního systému Windows společně se znalostí MS SQL. Tyto znalosti nejsou součástí školení, ovšem jsou zcela nezbytnými požadavky pro plnohodnotnou instalaci a servis systému. V případě nesplnění vstupního testu ze všech samostatných částí není možno započít školení.

3.2.1.1 Počítačové sítě

První částí vstupního testu je zaměřena na počítačové sítě. Znalost počítačových sítí je důležitá z důvodu spojení řídicí jednotky s aplikačním serverem a z důvodu spojení řídicí jednotky systému s periferiemi. Testem bude ověřena základní znalost síťových protokolů souvisejících s nastavením zařízení v počítačové síti, bude požadována znalost příkazů pro ověření průchodnosti počítačové sítě a znalosti protokolů využívaných na fyzické vrstvě síťového modelu ISO/OSI. Z testu o počítačových sítích, který je přílohou diplomové práce, je nutno získat alespoň 70% bodů.

3.2.1.2 Elektrotechnika

V další části technik prakticky předvede znalosti výpočtů a měření elektrických veličin prostřednictvím multimetru, osciloskopu a dalších elektrotechnických analytických nástrojů. Tyto nástroje jsou základním diagnostickým prostředkem při odhalování chyb v systému. Jejich ovládnutí stejně jako znalost základních elektrotechnických pravidel je tak nezbytnou dovedností technika instalujícího a servisujícího systém Asset. Každému účastníkovi školení budou přiděleny dvě typové činnosti a vhodné přístroje, jejichž prostřednictvím dokáže požadovanou znalost. Zda-li je úroveň znalostí a dovedností dostatečná, určí školící pracovník na základě osobních zkušeností se systémem Asset. Příklady typových činností jsou přílohou diplomové práce.

3.2.1.3 Operační systém Windows a databáze

V poslední části technik testem prokáže, zdali je schopen uspokojivě provádět činnosti spojené s instalací, odhalováním chyb a provozem softwaru na operačním systému Windows a základní činnosti s MS SQL. Znalost těchto záležitostí je nutná, protože uživatelská a technická rozhraní jsou určena právě pro operační systém Windows a architektura nadstavbové části systému je založena na databázi MS SQL. Z testu o činnostech v operačním systému Windows, který je přílohou diplomové práce, je nutno získat alespoň 70% bodů.

3.2.1.4 Zpětná vazba na otázky vstupního testu

Na školení montážních techniků, které proběhlo 11. 3. 2015, byly výše zmíněné testy z počítačových sítí a operačních systémů zadány montážním technikům, u kterých se očekávají výrazně nižší znalosti z uvedených oblastí, protože primárním pracovním nástrojem těchto osob není počítač. Těmto lidem není nové školicí středisko primárně určeno, a proto by neměli ve většině případů test zvládnout na požadovaných 70 %. Úspěšnost odpovědí na jednotlivé otázky, která je zpracovaná v tabulkách, tato očekávání naplnila.

Tabulka č. 2: Úspěšnost montážních techniků test OS

číslo otázky OS	1	2	3	4	5	6	7	8
úspěšnost na otázce[%]	28,57	14,29	28,57	57,14	42,86	0,00	0,00	28,57
číslo otázky OS	9	10	11	12	13	14	15	
úspěšnost na otázce[%]	42,86	100,00	0,00	85,71	85,71	100,00	100,00	

Průměrná úspěšnost montážních techniků na otázkách z operačních systémů byla 47,62 %

Tabulka č. 3: Úspěšnost montážních techniků test počítačové sítě

číslo otázky sítě	1	2	3	4	5	6
úspěšnost na otázce[%]	0,00	14,29	0,00	0,00	0,00	0,00
číslo otázky sítě	7	8	9	10	11	12
úspěšnost na otázce[%]	71,43	0,00	0,00	14,29	14,29	14,29
číslo otázky sítě	13	14	15	16	17	
úspěšnost na otázce[%]	28,57	0,00	71,43	71,43	28,57	

Průměrná úspěšnost montážních techniků na otázkách z počítačových sítí byla 19,33 %

Mimo školení byly testy předloženy servisním technikům oživujícím a udržujícím systém Asset v chodu. Výsledky této skupiny v naprosté většině případů překročily požadovanou úroveň 70%, avšak odhalily jisté neznalosti, které by v případě řešení nestandardních problémů komplikovaly jejich odstranění.

Tabulka č. 4: Úspěšnost servisních techniků test OS

číslo otázky OS	1	2	3	4	5	6	7	8
úspěšnost na otázce[%]	81,82	54,55	90,91	81,82	100,00	81,82	81,82	72,73
číslo otázky OS	9	10	11	12	13	14	15	
úspěšnost na otázce[%]	81,82	100,00	72,73	100,00	90,91	100,00	100,00	

Průměrná úspěšnost servisních techniků na otázkách z operačních systémů byla 86,06 %

Tabulka č. 5: Úspěšnost servisních techniků test počítačové sítě

číslo otázky sítě	1	2	3	4	5	6
úspěšnost na otázce[%]	90,91	36,36	90,91	100,00	81,82	27,27
číslo otázky sítě	7	8	9	10	11	12
úspěšnost na otázce[%]	100,00	90,91	81,82	63,64	81,82	63,64
číslo otázky sítě	13	14	15	16	17	
úspěšnost na otázce[%]	72,73	90,91	100,00	90,91	100,00	

Průměrná úspěšnost servisních techniků na otázkách z počítačových sítí byla 80,21 %

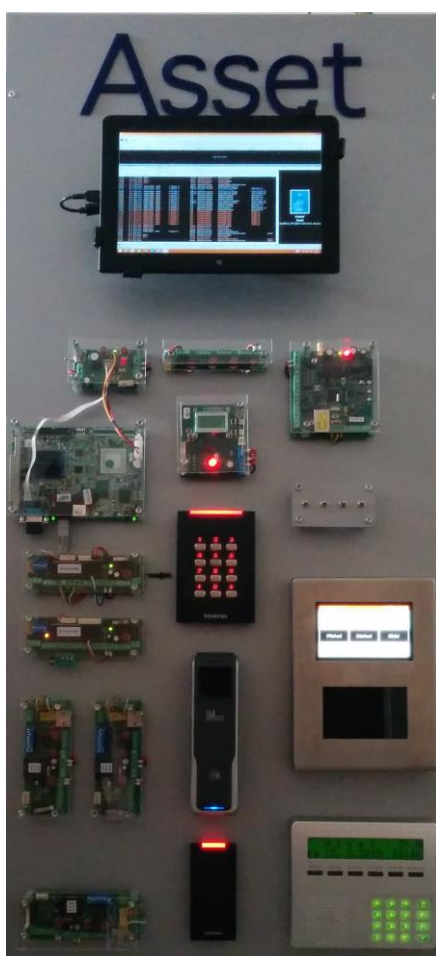
Výsledky testů naznačily, že by bylo vhodné v dalším postupu zvážit, zdali nevytvořit nultou lekci, během které by byli účastníci před začátkem samotného školení seznámeni s terminologií a pravidly operačních systémů a sítí a také s instalací a zpřístupněním MS SQL. Potřeba vytvoření této nulté lekce bude analyzována na základě zpětné vazby jednotlivých lekcí prvních realizovaných školení.

3.2.2 Struktura lekcí

Každá lekce má svoji strukturu, které je složená z přednášky a cvičení. Je důležité, aby školení vedl školitel, který má hluboké znalosti systému Asset a který je schopen odpovědět na všechny související otázky. Za vhodného školitele lze považovat pracovníka technické podpory, která je přidružena k vývojovému oddělení systému Asset. Časová dotace pro realizaci školení byla určena na 3 hodiny pro jednu školicí lekci. Rozvržení času mezi přednáškovou a cvičební částí je závislé na aktuálně probíraném tématu, schopnostech posluchačů a úrovni školitele a je určováno v průběhu jednotlivých lekcí školitelem.

3.2.2.1 Přednáška

Přednášková část se zaměřuje na předání teoretických informací posluchačům. Forma přednášky by měla být spojená s diskusí nad některými tématy s možností vysvětlení veškerých nejasností školitelem. Přednášková část je vedena prostřednictvím Power Pointových prezentací, které jsou přílohou diplomové práce. Ke tvorbě materiálu prezentací byly použity interní materiály společnosti Trade Fides zahrnující grafické ztvárnění prezentace z důvodu zachování jednotné firemní image.



Obr. 13: Přednáškové tablo

V prezentacích jsou použity pouze konkrétní údaje o zařízeních a softwarech, které jsou společností Trade Fides běžně zveřejňované. Zajímavosti, postřehy a know-how nejsou součástí prezentací a budou doplněny na komerční úrovni využití prezentací. Prezentace jsou zaměřeny na fakta a vyhýbají se tvrzením. Jako praktická pomůcka pro přednášky bylo vytvořeno přednáškové tablo, na kterém může přednášející pro názornost prakticky demonstrovat přednášené informace.

3.2.2.2 Cvičení

V praktické části školení nazývaných cvičení si technik vyzkouší vybrané nově získané teoretické informace. Cvičení budou probíhat dle připravených scénářů na školicím pracovišti složeném z hardwarových komponent a softwarů na počítačích účastníků. Scénáře záměrně uvádí pouze osnovu cvičení místo přesných kroků. Určují tak směr, kterým se má technik ubírat, ale nedávají instrukce, podle kterých by bylo možné cvičení bezmyšlenkovitě projít. Pro řešení problémů, se kterými si není technik schopen podle scénáře poradit, jsou vytvořeny manuály dostupné na stránkách společnosti Trade Fides. V případě, že se nepodaří problém vyřešit, je na školení přítomen odborník, který s řešením problému pomůže.



Obr. 14: Hardwarové komponenty cvičení

3.2.2.3 Zpětná vazba

Každé lekci je potřebné vytvářet okamžitou zpětnou vazbu formou diskuse s účastníky. Výstupy zpětné vazby je bezpodmínečně nutno uvést do písemné podoby a na základě tohoto textu upravovat strukturu jednotlivých lekcí. Důležité je tuto zpětnou vazbou kombinovat s časově posunutou zpětnou vazbou, která pomocí testů a dotazů na oddělení technické podpory exaktně dokáže účinnost školení. Tímto způsobem lze udržovat lekce maximálně účinné pro potřeby posluchačů.[39]

3.2.3 První lekce

Po úspěšném absolvování všech částí vstupního testu nebo případné nulté lekce lze předpokládat dostatečné znalosti, na které může navázat školení systému Asset. První lekce je zaměřena na pochopení hardwarové struktury.

3.2.3.1 Přednáška

Přednášková část první lekce se zabývá představením hardwarového vybavení systému Asset včetně periférií a možností jejich propojení. Dalším krokem přednášky je přehledové představení softwarových komponent systému. V posledním bodě přednášky je započato seznamování s konfiguračním softwarem ACFG.

3.2.3.2 Cvičení

V praktické části si účastníci školení vyzkouší zapojit dle právě nabytých znalostí a připraveného scénáře, který je přílohou diplomové práce, jednoduchou konfiguraci. Do tohoto zapojení následně odešlou předpřipravenou konfiguraci ze software ACFG, který si nainstalují, a správnost zapojení prostřednictvím tohoto software ověří, případně s pomocí školitele odstraní chyby. V závěru praktické části prvního školení si za pomoci osciloskopu účastníci vyzkouší, jaký vliv má na průběh signálu změna zakončovacích odporů na lince RS 485.

3.2.4 Druhá lekce

Druhá lekce je zaměřena na konfiguraci systému Asset prostřednictvím softwarů FDC a ACFG.

3.2.4.1 Přednáška

Na počátku přednáškové části je účastníkům školení představena možnost konfigurace síťového rozhraní řídicí jednotky Asset prostřednictvím FDC. Druhá část přednášky je věnována vytváření konfigurací v softwaru ACFG a základním parametrům konfigurací, které jsou součástí všech instalací systému Asset.

3.2.4.2 Cvičení

Během cvičení si účastníci vyzkouší instalaci softwaru FDC, ve kterém nastaví IP adresu zařízení tak, aby bylo možné se k zařízení připojit vzdáleně v počítačové síti. Následně bude v ACFG každým účastníkem školení vytvořena konfigurace pro zapojení realizované během

praktické části první lekce. Tato konfigurace bude rozšířená o parametry dle předpřipraveného scénáře.

3.2.5 Třetí lekce

Ve třetí lekci si technici vyzkouší připojení řídicí jednotky systému Asset do Asset Serveru. Na tuto lekci musí budoucí technik provést přípravu nainstalováním databázového systému MS SQL 2012 a se zpřístupněním přístupu po TCP/IP na portu 1433.

3.2.5.1 Přednáška

Přednáška druhé lekce je zaměřena na teoretické zvládnutí instalace serverové služby systému s následnou konfigurací. Během přednášky jsou posluchači seznámeni s širokými možnostmi nadstavbové části a s nastavováním těchto možností v programu ACNS.

3.2.5.2 Cvičení

Na cvičení si účastníci vyzkouší uvést do praxe nově nabyté zkušenosti instalací nadstavbového software ASVR a ACLT, kterého je ACNS součástí. Nově nainstalovaný server pak dle předpřipraveného scénáře v ACNS nastaví a připojí do něho instalaci, kterou v předchozích lekcích zapojovali a konfigurovali.

3.2.6 Čtvrtá lekce

S operátorským rozhraním systému Asset v podobě ACLT bude technik seznámen ve čtvrté lekci. Dokonalé ovládnutí uživatelských a operátorských rozhraní je nutné pro kvalifikované zaškolení obsluhy systému.

3.2.6.1 Přednáška

Během přednášky bude budoucí technik seznámen s operátorským rozhraním ACLT, s jeho okny a širokými možnostmi, které jsou uživatelům poskytovány.

3.2.6.2 Cvičení

Ve cvičební části si bude technik dle připraveného scénáře zkoušet standardní operátorské postupy na databázi, kterou si obnoví a jako osvěžení informací načerpaných v minulé lekci školení si do této databáze připojí řídicí jednotku nakonfigurovanou v lekci předminulé. Mezi zkoušené operátorské činnosti patří práce s okny aplikace a vytváření uživatelských účtů.

3.2.7 Pátá lekce

Pátá lekce navazuje na předchozí přípravu pro zaškolení operátorů přípravou pro zaškolení administrátorů systému. Dále se lekce zaměřuje na možnost ovládání systému bez nadstavbové části pouze prostřednictvím klávesnice KMU-4.

3.2.7.1 Přednáška

Na přednáškové části bude technik seznámen s možnostmi a pravidly vytváření systémových účtů v aplikaci ACNS a dalšími administrátorskými činnostmi. Druhá část přednášky pak bude věnována možnosti ovládání systému pouze prostřednictvím klávesnice KMU-4.

3.2.7.2 Cvičení

V praktické části si technici dle připraveného scénáře vyzkouší vytváření systémových účtů v databázi, kterou si na předchozí lekci nainportovali. Do této jednotky pak obnoví uživatele z databáze a provedou hromadné úpravy uživatelských účtů v souvislosti s touto novou jednotkou. V druhé části lekce si technici vyzkoušejí ovládání systému z klávesnice prostřednictvím několika různých úrovní uživatelů.

3.2.8 Šestá lekce

Šestá lekce je zaměřena na možnosti připojení integrovaného zabezpečovacího systému Asset na DPPC s důrazem na připojení na DPPC Latis SQL prostřednictvím PZL-10.

3.2.8.1 Přednáška

Na počátku přednášky jsou představeny všechny varianty přenosu poplachových a nepoplachových informací ze systému Asset na DPPC. Možné varianty přenosu jsou prostřednictvím modulu Contact ID, prostřednictvím ethernetového portu řídicí jednotky nebo prostřednictvím zařízení PZL – 10, potažmo variantou PZL-11. Posluchači jsou seznámeni s konfiguračními požadavky pro jednotlivé varianty přenosu a také s procesem zisku informací, které bude požadovat provozovatel DPPC. Druhá část přednášky se zaměřuje na software FDC a v tomto softwaru podrobně je podrobně rozebráno nastavování zařízení PZL-10.

3.2.8.2 Cvičení

Na cvičení technici dle připraveného scénáře připojí k řídicí jednotce Asset přenosové zařízení PZL-10. Následně provedou v software ACFG nastavení řídicí jednotky tak, aby se byl Asset schopen prostřednictvím RS 232 spojit s PZL-10. V konfiguračním software FDC

technici nastaví parametry dle scénáře a dle pokynů školitele, který bude pro potřeby školení simulovat činnosti správce DPPC Latis SQL. Každý technik si tak reálně připojí Asset prostřednictvím PZL - 10 na DPPC.

3.2.9 Sedmá lekce

Sedmá lekce se věnuje systému Octopus, který je rozhraním bezdrátových detektorů pro systém Asset.

3.2.9.1 Přednáška

Během přednášky je představen systém Octopus a jeho jednotlivé části. Jsou zopakována známá pravidla pro instalaci detektorů, které mnoho techniků ignoruje a degraduje tak hodnotu zabezpečovacího systému. Technici jsou teoreticky seznámeni s učením jednotlivých detektorů do systému Octopus a s konfigurací připojených zařízení v systému Asset.

3.2.9.2 Cvičení

V praktické části lekce technici připojí k systému Asset linkový modul Octopus, do kterého dle získaných informací a připraveného scénáře naučí detektory systému Octopus. Následně linkový modul i detektory nakonfigurují v software ACFG a přiřadí bezdrátová tlačítka a tísňe uživatelům v software ACLT. Technici na závěr odešlou změněnou konfiguraci správci DPPC, který aktualizuje tabulky a tím zabrání vzniku neznámých událostí na straně DPPC. Tímto krokem si technici zautomatizují praktické návyky, které jim byly předány na minulé lekci.

3.2.10 Osmá lekce

Osmá lekce je spojená s nadstandardem v oblasti elektronické kontroly vstupu. Zaměřuje se na biometrické terminály, docházkové terminály KMU-7 a instalaci uživatelského rozhraní AWI.

3.2.10.1 Přednáška

Přednáška osmé lekce se na svém počátku zaměřuje teoreticky na nastavení biometrických terminálů Bioscrypt 4G V-flex pro čtení otisků prstů v software Secure Admin tak, aby byly připojitelné k systému Asset. V návaznosti je pak představena konfigurace v ACFG a ACNS, nastavení software ACNS a učení otisků prstů do systému. Prostřední část přednášky je vě-

nována docházkovým terminálům KMU-7 ve variantě připojitelné na linku, tak variantě autonomní, způsobu konfigurace obou variant a následnému připojení. V poslední části přednášky je uživatel seznámen s nastavením AWI.

3.2.10.2 Cvičení

V praktické části si technik vyzkouší do existující databáze připojit docházkový terminál KMU-7 v autonomní verzi. Následně terminál nakonfiguruje včetně odeslání firmware, obnoví seznam uživatelů a přidá uživatelům patřičná práva. Ve druhé části cvičení si účastníci nainstalují IIS a zprovozní AWI. Dále si vyzkouší nastavení práv pro uživatele Asset Web Interface. Celý postup proběhne dle připraveného scénáře.

3.2.11 Devátá lekce

Devátá lekce se zaměřuje na pokročilé nastavení v softwarech ACFG a ACNS, na které se nedostalo v průběhu lekcí, které byly těmto softwarům věnovány.

3.2.11.1 Přednáška

Během přednáškové části jsou prezentovány pokročilé techniky systému Asset se zaměřením na ACFG a ACNS. Mezi tyto pokročilé techniky patří konfigurace redundantního režimu systému Asset, integrace kamerových systémů s možností ukládání obrazových dat nebo připojení ŘJ Asset do sítě BACnet. Po dokončení vývoje bude součástí této přednášky také aplikace Autorizační portál a její začlenění do systému. Závěrem přednášky bude představen software FSS, jeho nastavení a používání.

3.2.11.2 Cvičení

Během praktické části si technici vyzkoušejí připojit do svého serveru kamerový systém a nastavit stahování obrazových dat v případě výskytu definovaných událostí. Dále budou nainstalovány oba konce aktualizací rozhraní FSS a tento software bude odzkoušen na reálných případech.

3.3 Závěrečná zkouška

Poslední desátá lekce není lekcí vzdělávací ale má za cíl ověřit, zdali školená osoba v dostatečné míře pochopila souvztažnosti systému Asset a zdali je schopna systém dostatečně kvalitně zprovoznit. Se zachováním struktury školení prokazuje v první části technik formou

testu teoretické znalosti systému. Ve druhé části dle scénáře předvede schopnost systém zprovoznit.

3.3.1 Teoretická část

Pro teoretickou část závěrečné zkoušky je připraven test, ze kterého účastník školení musí získat minimálně 80% bodů pro úspěšné splnění. Informace, které jsou dotazovány v testu, jsou součástí přednášek předchozích lekcí a účastníci školení by je tak měli znát na úrovni, jež umožňuje zvládnutí testu s takto vysokým skóre. Přílohou diplomové práce je jedna varianta testu. Další varianty budou dopracovány na komerční úrovni a nebudou součástí diplomové práce.

3.3.2 Praktická část

V praktické části závěrečné zkoušky technik dle bodů předpřipraveného scénáře předvede nakonfigurování systému. K této části zkoušky je možno používat manuály, protože technik již prokázal znalosti v teoretické části. Jednotlivé části scénáře budou ohodnoceny body, kdy za úspěšné absolvování školení je považován minimálně zisk 80% bodů.

Scénář praktické části po technikách požaduje vytvoření konfigurace řídicí jednotky Asset a zapojení. Dále pak technik obnoví přiloženou databázi, ke které připojí nainstalovaný Asset Server. K tomuto serveru připojí výše zmíněnou řídicí jednotku a provede obnovení uživatelů ze serveru. Technik také prokáže schopnost hromadné editace práv uživatelů, schopnost vyhledávání v historii dle zadání včetně exportu dat. V neposlední řadě scénář počítá s připojením řídicí jednotky na DPPC Latis včetně všech sounáležitostí.

3.4 Certifikát

Na základě absolvování školení a úspěšného zvládnutí obou částí závěrečné zkoušky na požadované úrovni je absolventům předán certifikát, jehož vzor je přílohou diplomové práce. Certifikát by měl opravňovat techniky a tím i společnosti těchto techniků k nákupu, instalaci a provádění servisu systému Asset. Na certifikátu jsou uvedeny základní údaje o společnosti, která školení provedla, tedy Trade Fides, včetně loga, které je použito také na pozadí certifikátu. Certifikát dále obsahuje předmět certifikátu, informace o osobě, které je certifikát vydáván, základní práva a povinnosti vyplývající z certifikátu, podpisy školitele a osoby,

která je za školení prováděné společností zodpovědná a číslo certifikátu pro uložení do databáze společnosti. Číslo je složené z roku, měsíce vystavení a pořadového čísla certifikátu v daném měsíci. V neposlední řadě je na certifikátu uvedeno datum vystavení a platnost.

Platnost certifikátu je z důvodu rychlého vývoje technologií omezena na dobu dvou let. Po uplynutí této doby je v potřebné absolvovat aktualizací školení, jehož vytvoření proběhne na komerční úrovni ve společnosti Trade Fides. Toto aktualizací školení bude rozsahem odpovídat přibližně jedné lekci školicího střediska, které je předmětem této diplomové práce. Zpřístupnění aktualizací školení je podmíněno dřívějším absolvováním školení a instalací alespoň 4 kusů systému Asset v posledních dvou letech. V opačném případě je nutné absolvovat plné školení systému Asset.

ZÁVĚR

V teoretické části diplomové práce je sepsán ucelený přehled základních hardwarových a softwarových komponent systému Asset. Tento přehled dříve nebyl vytvořen a jeho absence způsobovala neznalým osobám potíže v orientaci v systému Asset. Tento přehled umožňuje rychlé vyhledání vhodného manuálu softwarové či hardwarové komponenty na webových stránkách společnosti Trade Fides, pokud osoba vyžadující manuál nezná název, ale má pouze přibližnou představu o funkcích komponenty.

Druhá polovina teoretické části diplomové práce je věnována vytvoření přehledu školicích středisek užívaných v technické rovině průmyslu komerční bezpečnosti. Pro vytvoření přehledu bylo nutné si nejdříve nadefinovat kategorie, druhy a účely školení. Ty byly následně použity pro lepší orientaci ve vybraných školicích střediscích. Zmiňovaná školicí střediska byla vybírána tak, aby pokryla celé spektrum kategorií zařízení používaných v segmentu ochrany života, zdraví a majetku. Z těchto jednotlivých školení byly odvozeny závěry vydvíhující silné a slabé stránky jednotlivých školení a tyto závěry byly použity k maximální efektivitě při vytváření koncepce nového školicího střediska.

Praktická část je věnována vytvoření nového komerčně použitelného školicího střediska systému Asset. Z výše uvedených závěrů a ze zkušenosti se systémem Asset jsem se rozhodl pro vytvoření školicího střediska děleného na 10 vzájemně navazujících vzdělávacích lekcí. Tyto lekce jsou členěny na část přednáškovou a praktickou pro maximalizaci množství zapamatovaných a prakticky použitelných informací.

Součástí diplomové práce jsou podkladové materiály, které jsou zastoupeny prezentacemi pro teoretické části lekcí a scénáři s podkladovou databází a konfigurací pro praktické části. Tyto materiály byly vytvořeny na základě osobních zkušeností z pozice specialisty technické podpory, jež zaručuje znalost systému a běžné obtíže, se kterými se technici v praxi potýkají.

Jako podmíněčnou součást školicího střediska jsem určil a vytvořil vstupní a výstupní testy. Předpokladem pro vstup do školení je vyplnění vstupního testu, které zaručuje potřebnou úroveň znalostí. Tyto testy byly vyplněny několika skupinami osob a naznačily možnost vytvoření nulté lekce, která by posluchačům potřebné znalosti doplnila. Školicí středisko je uzavřeno teoretickým testem a praktickou zkouškou, které jsou v případě úspěšného zvládnutí podkladem pro vydání certifikátu.

CONCLUSIONS

The theoretical part of the thesis contains a comprehensive overview of basic hardware and software components of Asset system. There was no such former summary and its absence caused problems with orientation within the system. This summary enables those, who need a manual but do not know particular terms and have only a rough idea about components functions, to promptly find appropriate software and hardware components on the Trade Fides website.

The second half of the theoretical part of the thesis is devoted to creating a list of training centres connected to the technical level of commercial security industry. To create the list, it was necessary to define categories, types and training purposes first. Afterwards, they were used for better orientation in selected training centres. The training centres had been chosen beforehand and carefully so that they cover the entire spectrum of categories of equipment used in the segment of life, health and property protection. Based on results from individual training sessions, conclusions highlighting strengths and weaknesses were drawn and these findings were subsequently used to enhance the efficiency of designing new training centre.

The practical part focuses on establishing a new commercially useful training centre of Asset system. From the above findings and experience with Asset system, I decided to establish a training centre divided into 10 mutually related training lessons. These lessons involve lecture and practical parts to maximize the amount of gained and practically useful information.

The thesis includes presentations for theoretical parts of lessons and scenarios related to databases and configurations for practical parts of lessons. These materials were developed on the basis of personal experience deriving from my technical support specialist position. This position guarantees the knowledge of the system and awareness of common difficulties which technical experts encounter.

As a conditional part of the training centre, input and output tests were defined and formed. The prerequisite for the admission to the training is the passing an entrance test, which ensures a required level of necessary basic knowledge. These tests were filled by several groups of people and, consequentially, the results indicate the possibility of establishing a zero lesson which might improve the basic preliminary knowledge. There is a final theoret-

ical and practical test at the end of the training, and in case of successful passing, trainees receive the certificate.

SEZNAM POUŽITÉ LITERATURY

- [1] VALOUCH, Jan. *Projektování integrovaných systémů*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj (152 s.). ISBN 978-80-7454-296-1.
- [2] TRADE FIDES, a.s. *Asset 801Z s integrovaným zdrojem PWR 4A: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/98-asset801z.html>
- [3] TRADE FIDES, a.s. *Asset 804, 808, 812: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/100-asset812.html>
- [4] TRADE FIDES, a.s. *KMU-4-ovládací panel: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/24-ovladaci-panely.html>
- [5] TRADE FIDES, a.s. *KMU-4: Manuál správce* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/81-asset-keyboard-control.html>
- [6] TRADE FIDES, a.s. *KMU-6-docházkový panel: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/24-ovladaci-panely.html>
- [7] TRADE FIDES, a.s. *KMU-7-docházkový panel: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/24-ovladaci-panely.html>
- [8] TRADE FIDES, a.s. *Asset-10-dveřní jednotka: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/49-dverni-jednotky.html>
- [9] TRADE FIDES, a.s. *Asset-20-dveřní jednotka: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/49-dverni-jednotky.html>
- [10] TRADE FIDES, a.s. *LML8-linkový modul: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/21-linkove-moduly.html>

- [11] TRADE FIDES, a.s. *RELIN 4: Základní popis* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/22-releove-moduly.html>
- [12] 3SSEDLAK, s.r.o. *Octopus* [online]. Brno, 2013. Dostupné z: <http://www.3ssedlak.com/octopus/>
- [13] TRADE FIDES, a.s. *PZL10: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/35-objektove-zarizeni-pzl-10.html>
- [14] TRADE FIDES, a.s. *CID Komunikátor: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/96-cid-com.html>
- [15] TRADE FIDES, a.s. *Klíčový trezor KWAD-15 s integrovanou ŘJ Asset 801 a zdrojem PWR 4A* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/48-klicove-trezory.html>
- [16] TRADE FIDES, a.s. *Asset Config: Manuál technika systému*. Brno, 2015. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/31-asset-config.html>
- [17] TRADE FIDES, a.s. *Asset Config 1.0.19.2*. Brno, 2015 [cit. 2015-05-12].
- [18] TRADE FIDES, a.s. *Asset Server: Manuál správce systému*. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/44-asset-server.html>
- [19] TRADE FIDES, a.s. *Asset Console: Manuál správce systému*. Brno, 2015. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/69-asset-console.html>
- [20] TRADE FIDES, a.s. *Asset Client: Manuál správce systému*. Brno, 2015. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/16-asset-client.html>
- [21] TRADE FIDES, a.s. *Asset Client 1.0.20.1*. Brno, 2015 [cit. 2015-05-12].
- [22] TRADE FIDES, a.s. *Asset Client Mobile: Manuál uživatele aplikace* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/72-asset-mobile.html>

- [23] TRADE FIDES, a.s. *Asset Control: Manuál správce systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/68-asset-control.html>
- [24] TRADE FIDES, a.s. *Asset Control Mobile Android: Manuál uživatele aplikace* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/72-asset-mobile.html>
- [25] TRADE FIDES, a.s. *Fides Device Configurator: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/76-fides-device-config.html>
- [26] TRADE FIDES, a.s. *Fides Device Configurator 1.0.0.49*. Brno, 2014 [cit. 2015-05-12].
- [27] TRADE FIDES, a.s. *Asset Guestbook: Manuál správce systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/71-asset-guestbook.html>
- [28] TRADE FIDES, a.s. *Asset monitor: Manuál technika systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/73-asset-monitor.html>
- [29] TRADE FIDES, a.s. *Asset Web Interface: Uživatelský manuál* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/74-asset-web.html>
- [30] TRADE FIDES, a.s. *Autorizační portál: Manuál správce systému*. Brno, 2015.
- [31] TRADE FIDES, a.s. *Fides Software Storage Client: manuál správce systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/13-fides-software-storage-client.html>
- [32] TRADE FIDES, a.s. *Fides Software Storage Administrator: manuál správce systému* [online]. Brno, 2014. Dostupné z: <https://www.fides.cz/technicka-podpora-hlavni-menu/soubory-ke-stazeni/category/12-fides-software-storage.html>
- [33] DRUCKER, Peter Ferdinand. *To nejdůležitější z Druckera v jednom svazku*. Vyd. 1. Praha: Management Press, 2002, 300 s. ISBN 80-7261-066-x.

- [34] ADAM, Vladislav. 2009. *Význam měření v montážích elektronických systémů PKB*. Zlín. Dostupné také z: http://portal.utb.cz/wps/PA_StagPortletsJSR168/KvalifPraceDownloadServlet?typ=1&adipidno=11376. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně Fakulta Aplikované informatiky. Vedoucí práce JUDr. Vladimír Laucký.
- [35] KYNCL, Jaromír. *Odborná způsobilost v komerční bezpečnosti*. 1. vyd. Praha: Professional Publishing, 2010, 219 s. ISBN 978-80-7431-028-7.
- [36] Ipodnikatel. *Školení zaměstnanců v oblasti BOZP*. 2011. [online]. Dostupné z: <http://www.ipodnikatel.cz/Bezpecnost-a-ochrana-zdravi-pri-praci/skoleni-zamestnancu-v-oblasti-bozp.html>
- [37] ŠPAČKOVÁ, Alena. *Umění dialogu: jak si s lidmi opravdu porozumět*. 1. vyd. Praha: Grada, 2011, 196 s. ISBN 978-80-247-3810-9.
- [38] SIDHU, Inder. *Cisco umí obojí: jak dnes vydělávat a zároveň zajistit budoucí růst*. Vyd. 1. Brno: Computer Press, 2011, 248 s. ISBN 978-80-251-3537-2.
- [39] CHROMÝ, Jan. *Komunikace, média, vzdělávání, kultura*. Vyd. 1. Praha: Extrasystem Praha, 2014, 201 s. ISBN 978-80-87570-19-7.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A	Ampér - Jednotka elektrického proudu
ACFG	Asset Config
ACLT	Asset Client
ACNS	Asset Console
ASVR	Asset Server
AWI	Asset Web Interface
CID	Contact ID – Přenosový protokol pro DPPC
ČSN	Česká státní norma
DEOL	Double End Of Line – Dvojitě vyvážená smyčka
EN	Evropská norma
EB	Expander base
EPS	Elektrická požární signalizace
FDC	Fides Device Configurator
FSS	Fides Software Storage
FXP	File eXchange Protocol – metoda výměny dat
GPRS	General Packet Radio Service – Služba přenosu dat v mobilních sítích
GSM	Groupe Spécial Mobile – Systém pro mobilní komunikaci
IIS	Internet Information Service – Softwarový webový server
IP	Internet Protocol – Protokol síťové vrstvy
ISO	International Organization for Standardization – Mezinárodní organizace pro standardizaci
JTS	Jednotná telefonní síť
LAN	Local area network-Místní síť
MaR	Měření a regulace

MS	Microsoft
OCR	Optical Character Recognition – Optické rozpoznávání znaků
ONVIF	Open Network Video Interface Forum – Protokol pro přenos obrazu z IP kamer
OS	Operační systém
OSI	Open Systems Interconnection – Otevřený systém propojení
PeS	Personální Systém
PKB	Průmysl komerční bezpečnosti
PZTS	Poplachové zabezpečovací a tísňové systémy
RFID	Radio Frequency Identification – Identifikace pomocí radiových frekvencí
RS	Recommended Standard-doporučený standard
ŘJ	Řídící jednotka
Sb	Sbírka
SDK	Software Development Kit -
SKV	Systém kontroly vstupu
SMS	Short Message Service – Služba krátkých textových zpráv
SQL	Structured Query Language – Strukturovaný dotazovací jazyk
TCP	Transmission Control Protocol – Spojitý protokol transportní vrstvy
V	Volt – jednotka elektrického napětí

SEZNAM OBRÁZKŮ

Obr. 1: Hardwarová struktura	13
Obr. 2: Asset 801 Z.....	14
Obr. 3: Elektronika KMU-4.....	15
Obr. 4: KMU-7	16
Obr. 5: Dveřní jednotka Asset-20	17
Obr. 6: Modul LML-8.....	18
Obr. 7: PZL-10.....	19
Obr. 8: KWAD-15	20
Obr. 9: Softwarová struktura	21
Obr. 10: Asset Config [17]	22
Obr. 11: Asset Client[21].....	24
Obr. 12: Fides Device Configurator[26].....	25
Obr. 13: Přednáškové tablo.....	41
Obr. 14: Hardwarové komponenty cvičení.....	42

SEZNAM TABULEK

<i>Tabulka č. 1: Kvalifikace montážních pracovníků v PKB[34].....</i>	<i>27</i>
<i>Tabulka č. 2: Úspěšnost montážních techniků test OS</i>	<i>39</i>
<i>Tabulka č. 3: Úspěšnost montážních techniků test počítačové sítě</i>	<i>39</i>
<i>Tabulka č. 4: Úspěšnost servisních techniků test OS.....</i>	<i>40</i>
<i>Tabulka č. 5: Úspěšnost servisních techniků test počítačové sítě.....</i>	<i>40</i>

SEZNAM PŘÍLOH

- P I: Vstupní test počítačové sítě
- P II: Scénáře elektrotechnika
- P III: Vstupní test operační systémy a databáze
- P IV: Prezentace první lekce (CD)
- P V: Scénář první lekce
- P VI: Konfigurace (CD)
- P VII: Prezentace druhá lekce (CD)
- P VIII: Scénář druhé lekce
- P IX: Prezentace třetí lekce (CD)
- P X: Scénář třetí lekce
- P XI: Databáze (CD)
- P XII: Prezentace čtvrté lekce (CD)
- P XIII: Scénář čtvrtá lekce
- P XIV: Prezentace pátá lekce (CD)
- P XV: Scénář páté lekce
- P XVI: Prezentace šestá lekce (CD)
- P XVII: Scénář šesté lekce
- P XVIII: Prezentace sedmá lekce (CD)
- P XIX: Scénář sedmé lekce
- P XX: Prezentace osmá lekce (CD)
- P XXI: Scénář osmé lekce
- P XXII: Prezentace devátá lekce (CD)
- P XXIII: Scénář deváté lekce
- P XXIV: Závěrečný test
- P XXV: Testový scénář

P XXVI: Certifikát

PŘÍLOHA P I: VSTUPNÍ TEST POČÍTAČOVÉ SÍTĚ

Vstupní test z počítačových sítí pro školení Asset

Pro úspěšné zvládnutí testu je nutno získat 70% bodů. Každá otázka je hodnocena 1 bodem. Správná je vždy právě jedna odpověď. Za špatné odpovědi se body nestráhávají. Časový limit testu je 15 minut.

Jméno a příjmení:

Datum:

1. Jaký je význam IP adresy 127.0.0.1
 - a. Výchozí brána sítě 127.0.0.0
 - b. Broadcastová adresa sítě 127.0.0.0
 - c. Vnitřní adresa počítače (loopback)
 - d. Univerzální adresa, na které se vždy nachází serverové zařízení
 - e. Jiný (doplňte).....
2. Příkaz „telnet 192.168.0.23 7777“ aplikovaný v počítačové síti
 - a. Zjistí dostupnost TCP portu 7777 na počítači s adresou 192.168.0.23
 - b. Proveďte simulovaný telefonát na IP telefon s adresou 192.168.0.23 s parametrem 7777, který určuje číslo volajícího
 - c. Nakonfiguruje na počítači s IP adresou 192.168.0.23 firewall tak, aby propouštěl komunikaci na TCP portu 7777
 - d. Způsobí chybovou hlášku z důvodu špatného tvaru zápisu příkazu. Není totiž možné zadat tomuto příkazu dva parametry
3. IP adresa v4 192.168.0.48 je
 - a. Veřejná adresa v Internetu
 - b. Adresa v privátní síti
 - c. Vnitřní adresa počítače (loopback)
 - d. Neexistuje
4. Šíření broadcastového paketu je standardně omezeno
 - a. Síťovým rozhraním vysílajícího počítače (broadcast se šíří pouze v rámci počítače)
 - b. Switchem
 - c. Routerem
 - d. Není omezeno
5. Co je v IPv4 výchozí brána a k čemu se používá
 - a. Není v IPv4 známo, pojem výchozí brána je používán až v IPv6
 - b. Hostitel zodpovědný za směrování do cizích sítí
 - c. Pojem výchozí brána je totožný s pojmem firewall
 - d. Překlad doménových jmen na adresy
6. Co platí pro PAT (Port Address Translation) specifický případ NAT
 - a. Privátní adresy jsou překládány na jednu vnější
 - b. Privátní adresy jsou pevně přiřazeny vnějším adresám
 - c. Zachovává čísla portů
 - d. Provádí logování provozu na lokální počítačové síti

7. Zkratka GSM označuje
 - a. Systém mobilní komunikace
 - b. Kategorii připojení k internetu v rámci mobilních sítí s možností současně probíhajícího hovoru
 - c. Kategorii připojení k internetu v rámci mobilních sítí vylučující možnost současně probíhajícího hovoru
 - d. Schopnost zařízení připojit se k síti provozované na standardu IEEE 802.11
8. Který příkaz slouží k výpisu zařízení třetí vrstvy, přes které probíhá komunikace k cíli
 - a. NSLOOKUP
 - b. PING
 - c. IPCONFIG
 - d. TRACERT případně TRACEROUTE
9. K čemu slouží v IPv4 maska
 - a. Není v IPv4 známo, pojem maska je používán až v IPv6
 - b. Překládá adresy vnitřní sítě na adresy sítě vnější
 - c. Číslo popisující rozdělení počítačové sítě na části podsítí a host
 - d. Skryté ukládání dat na síťovém úložišti
10. Komunikační port slouží k
 - a. Rozlišení aplikace na transportní vrstvě modelu ISO/OSI
 - b. Odesílání emailů
 - c. Přijímání emailů
 - d. Směrování rámců na úrovni linkové vrstvy modelu ISO/OSI
11. Který z následujících protokolů označuje spojový protokol transportní vrstvy se spolehlivým doručováním
 - a. HTTP/HTTPS
 - b. IP
 - c. UDP
 - d. TCP
12. Maximální délka sběrnice RS 232 je za optimálních podmínek
 - a. 0,5metru
 - b. 15metrů
 - c. 100metrů
 - d. 1500metrů
13. Maximální délka sběrnice RS 485 je za optimálních podmínek
 - a. 15metrů
 - b. 100metrů
 - c. 1200metrů
 - d. 5000metrů
14. Kolik zařízení může komunikovat prostřednictvím RS 232
 - a. Není omezeno
 - b. Dvě
 - c. Až třicet
 - d. Tato hodnota se liší v závislosti na nastavené komunikační rychlosti

15. RS 485 má nejlepší parametry při zapojení zařízení do topologie

- a. Kruhu
- b. Sběrnice
- c. Hvězdy
- d. Plné topologie (každý s každým)
- e. Jiná (doplňte).....

16. Maximální délka ethernetového kabelu cat5e je

- a. 3 metry
- b. 10metrů
- c. 100metrů
- d. 1200metrů

17. Maximální proud vícevláknovým optickým vláknem je

- a. 50mA
- b. 500mA
- c. 5A
- d. jiná odpověď (doplňte):.....

PŘÍLOHA P II: SCÉNÁŘE ELEKTROTECHNIKA

1. Zachyťte prostřednictvím vhodného měřicího nástroje průběh napětí na obou kanálech linky RS 485, odhalte anomálie a navrhnete vhodné řešení odhalených anomálií.
2. Posuďte prostřednictvím vhodných technických prostředků, zdali je záložní baterie zdroje v pořádku a může být použita.
3. Prostřednictvím vhodných nástrojů ověřte, zdali je kanál Rx a Tx linky RS 232 správně zapojen.
4. Zachyťte na osciloskopu průběh signálu Wiegand ze čtecí hlavy
5. Vypočítejte, jaké napětí bude na svorkách zabezpečovací ústředny s odběrem 1A pokud na svorkách zdroje je napětí 13,2 V a celkový odpor vodičů je 0,5 Ω
6. Změřte proudový odběr předloženého zařízení
7. Vyjádřete číslo $(17)_{DEC}$ binárně
8. Navrhnete způsob odstranění napěťové špičky cívky elektromagnetického zámku vznikající při rozpojení stejnosměrného napájecího obvodu
9. Nakrumpujte křížený UTP kabel
10. Změřte NEXT a FEXT předloženého UTP kabelu

PŘÍLOHA P III: VSTUPNÍ TEST OPERAČNÍ SYSTÉMY A DATABÁZE

Pro úspěšné zvládnutí testu je nutno získat 70% bodů. Každá otázka je hodnocena 1 bodem. Správná je vždy právě jedna odpověď. Za špatné odpovědi se body nestrhávají. Časový limit testu je 15 minut.

Vstupní test z OS Windows a DB pro školení Asset

Jméno a příjmení:

Datum:

1. Manuální zálohu databáze MS SQL je možno provést
 - a. Prostřednictvím nástroje SQL Server Management Studio, kdy po kliknutí na databázi pravým tlačítkem vybereme možnost Back Up
 - b. Prostřednictvím nástroje SQL Server Management Studio, kdy označíme zobrazenou databázi a stiskem klávesové zkratky „Ctrl+C“ databázi zkopírujeme. Tuto kopii pak vložíme prostřednictvím zkratky „Ctrl+V“ do souboru pro zálohu
 - c. Prostřednictvím příkazového řádku příkazem „backupdatabase –jméno_databáze“
 - d. Zálohu databáze není z důvodu zvýšení bezpečnosti od verze MS SQL 2005 dovoleno dělat
2. Instalaci software do Program Files může provádět
 - a. Každý
 - b. Uživatel patřící do skupiny Administrators
 - c. Do složky Program Files nelze instalovat
 - d. Složka Program Files není součástí operačního systému Windows ale Linux
3. Povolení portu ve firewallu operačního systému Windows pro příchozí spojení se provede
 - a. Není potřeba povolovat firewall vždy blokuje pouze porty, které uživatel vyjmenuje
 - b. Je možné pouze úplným vypnutím Firewallu v ovládacích panelech
 - c. Přidáním příchozího pravidla v nastavení Firewallu v ovládacích panelech
 - d. Prostřednictvím příkazu „telnet –in příchozí _port “
4. Jakým příkazem zjistím nastavení síťového rozhraní počítače
 - a. NSLOOKUP
 - b. PING
 - c. IPCONFIG
 - d. TRACERT případně TRACEROUTE
 - e. Jiným (dopíšte).....
5. Přehled spuštěných služeb v systému Windows získáme
 - a. Spuštěním modulu „services.msc“ nebo po otevření „Správy počítače“
 - b. V souboru services.txt složky C:\Windows\aktuálně_přihlášený_uživatel
 - c. Globální přehled spuštěných služeb v OS Windows neexistuje, zjišťuje se ve složce každé služby
 - d. V BIOSu počítače

6. Operační systém Windows 8.1 X86 je operačním systémem
- 32 bitovým
 - 64 bitovým
 - 86 bitovým
 - Jinak (dopíšte).....
7. Stránkovací soubor v systému Windows
- Soubor pro odkládání neužívaných stránek RAM
 - Soubor, ve kterém jsou uloženy konfigurace síťových adaptérů
 - Soubor pro instalaci ovladačů systému
 - Soubor, do kterého jsou ukládány cookies webových stránek
8. V případě absence ikony vzdálená plocha spustím aplikaci
- Nespustím
 - Příkazem „MSTSC“
 - Současným stiskem kláves „Ctrl“+ „Alt“+ „Win“
 - Příkazem „WINRDP“
9. Souborový systém operačního systému Windows umožňující uložení souborů až do velikosti 16TB je
- FAT 16
 - FAT 32
 - NTFS
 - EXT
10. Co je „BIOS“
- Způsob zpracování dat vícejádrovým procesorem
 - Základní vstupně výstupní program základní desky počítače
 - Protokol pro šifrování dat na disku
 - Předchůdce složky „Program files“
11. Omezení MS SQL 2012 verze Express oproti plné verzi spočívá v
- Lze nainstalovat pouze na serverovou distribuci OS Windows
 - Je omezena maximální velikost databáze
 - Je omezen počet tabulek v databázi
 - Není možné použít závislosti mezi jednotlivými tabulkami
12. Zástupce aplikace v operačním systému Windows je
- Odkaz na program
 - Kopie programu
 - Nekomerční software použitelný jako alternativa placeného software
 - Soubor zastupující funkci programu v případě smazání originálu
13. Soubor „soubor.exe.zip“
- Je archiv komprimovaný metodou zip
 - Je dávkový soubor operačního systému
 - Je databázový skript
 - Soubor se základním informačním programem

14. Ovladač v operačním systému je

- a. Skupina uživatelů operačního systému Windows
- b. Program pro využívání hardwarové komponenty
- c. Konfigurační nástroj služeb operačního systému
- d. Nový systém nápovědy v operačním systému

15. Upgrade je

- a. Zálohování dat
- b. Nahrazení starší verze software novější verzí
- c. Návrat z novější verze software na verzi starší
- d. Instalace Firewallu

PŘÍLOHA P V: SCÉNÁŘ PRVNÍ LEKCE

1. Na linku RS 485 řídící jednotky Asset připojte moduly s následující adresací
 - LML-8 adresa 1
 - KMU-4 adresa 2
 - Asset 10 adresa 3
 - Asset 10 adresa 4
 - Asset 10 adresa 5
2. Prostřednictvím odporové zátěže vyvažte vstupy 1-5 LML-8 do stavu „klid“. Do vstupů 6,7,8 zapojte pomocí vyvažovací destičky signalizační výstupy zdroje, připojte reléový modul
3. K modulu Asset 10 na adrese 3 připojte prostřednictvím svorkovnice čtecí hlavu R10 a rozpínací tlačítko do vstupu č. 1
4. K modulu Asset 10 na adrese 4 připojte prostřednictvím svorkovnice čtecí hlavu RP40 a rozpínací tlačítko do vstupu č. 1
5. K modulu Asset 10 na adrese 5 připojte prostřednictvím svorkovnice biometrický terminál a rozpínací tlačítko do vstupu č. 1
6. Připojte baterii a napájení
7. Nainstalujte aplikaci Asset Config
8. Připojte k řídící jednotce přímo prostřednictvím ethernetového kabelu počítač a nastavte pevnou IP adresu 10.0.0.65
9. Otevřete prostřednictvím aplikace Asset Config přiloženou konfiguraci
10. Konfiguraci odešlete do řídící jednotky
11. V modulu Prohlížení linek aplikace Asset Config zkontrolujte, zdali všechna zařízení komunikují a odstraňte případné závady.
12. V modulu Prohlížení historie zkontrolujte, zdali připojené čtecí hlavy odesílají informace
13. Připojte osciloskop k oběma vodičům RS 485 včetně připojení signálové země.
14. Odeberte veškeré zakončovací odpory a následně pozorujte vliv přidávání zakončovacích odporů na průběh signálu. Pozorování provádějte současně na osciloskopu a také v modulu prohlížení linek v aplikaci Asset Config
15. Paralelním připojením kondenzátoru o kapacitě 20nF nasimulujte vliv větvení linky RS 485

PŘÍLOHA P VIII: SCÉNÁŘ DRUHÉ LEKCE

1. Řídící jednotku uveďte do továrního nastavení
2. Pomocí ethernetového kabelu připojte počítač, který má nastavenou pevnou IP adresu 10.0.0.65
3. Nainstalujte a spusťte aplikaci Fides Device Configurator
4. V programu povolte řídící jednotce DHCP a konfiguraci odešlete
5. Připojte počítač (povolte DHCP) i řídící jednotku do sítě LAN
6. V aplikaci Fides Device Configurator zjistěte pomocí MAC adresy napsané na desce řídící jednotky novou IP adresu zařízení
7. Spusťte software Asset Config
8. Vytvořte novou konfiguraci (instalaci) s následujícími parametry:
 - Název instalace: Školení
 - Kód oblasti: 5
 - Název oblasti: Brno
 - Kód objektu: Asset-2
 - Technické heslo objektu: 16
9. Přidejte řídící jednotku, které nastavte jméno „Školení“, typ jednotky: ASSET 801(bez expandéru) a kód objektu: „Školení“
10. Na záložce konfigurace připojení přidejte nové připojení, nastavte adresu, kde zvolte rozhraní TCP/IP a adresu vaší řídící jednotky zjištěnou v programu Fides Device Configurator, a z roletového menu objekt vyberte vámi definovanou řídící jednotku
11. Klikněte na záložku podsystémy pro vygenerování základních podsystémů
12. Klikněte na záložku aktivity pro vygenerování systémových aktivit
13. Přesuňte se na záložku zařízení na linkách
14. Označte první linku a prostřednictvím tlačítka „přidat“ popřidávejte do konfigurace zařízení z minulé lekce. Zachovejte adresaci modulů
15. U linkového modulu nastavte Smyčky 1,2,3,4,5 jako poplachové. Smyčku číslo 6 nastavte jako „Výpadek sítě“, smyčku 7 jako „Vybitá baterie“ a smyčku 8 jako „Porucha zdroje“
16. Modulu KMU-4 nastavte „Přihlášení kartou/heslem EZS“ a přiřadte oba vygenerované podsystémy
17. U dveřních jednotek nastavte „průchozí režim“, intervaly sepnutí zámků a připojení čtecí hlavy přes svorkovnici. U dveřní jednotky s biometrickým terminálem navíc přidejte parametr: „připojený biometrický terminál“
18. Vtvořenou konfiguraci odešlete do řídící jednotky
19. V tomto okamžiku je v řídící jednotce nahrána konfigurace totožná s konfigurací z první lekce s odlišným GUID. Provedte kontrolu funkčnosti v modulech „Prohlížení linek a prohlížení historie“
20. Vytvořte aktivitu, která bude spínat výstup 1 linkového modulu, a tuto aktivitu pojmenujte zóna
21. Vytvořte zónu, které nakonfigurujte automatické ovládání EZS, přiřadte podsystém 1 a nastavte ukončení akce zóna při vyprázdnění zóny
22. Kartové čtečky nastavte jako vstupní a výstupní a přiřadte zónu 1.
23. Tato část konfigurace bude ověřena ve 4. lekci

PŘÍLOHA P X: SCÉNÁŘ TŘETÍ LEKCE

1. Nainstalujte aplikaci Asset Client
2. Nainstalujte Asset Server s nasměrováním na místní databázi a spusťte službu
3. Spusťte aplikaci Asset Client v režimu Asset Console s jménem uživatele „admin“ a heslem „master“
4. V pokročilých nastaveních na záložce příchozí připojení povolte příchozí připojení na portu 12345. Konfiguraci uložte a Asset server restartujte
5. V aplikaci Asset Config otevřete konfiguraci z minulé lekce, přidejte technický parametr Asset Server, kde nastavte jako adresu Asset serveru IP adresu svého počítače a port 12345. Konfiguraci následně odešlete do řídicí jednotky
6. V aplikaci Asset Console povolte v seznamu neznámých ústředen vytvořenou ústřednu a zadejte technické heslo
7. V seznamu objektů potvrďte nově vytvořený objekt
8. Nadefinujte mezi komunikačními kanály e-mailovou adresu pro odeslání e-mailů
9. Za pomoci průvodce vytvořte systémovou notifikaci, která bude v případě vzniku nové události historie typu tamper smyčky nebo alarm smyčky odesílat e-mail s vámi zvoleným textem na Vaši emailovou adresu
10. Odpojte a opět připojte libovolný vstup linkového modulu a vyčkejte příchodu informačního emailu. V případě, že email nedorazí, odstraňte závadu
11. Nastavte automatické vytváření záloh databáze každý den s mazání záloh starších než 4 dny
12. V pokročilých nastaveních nastavte blokování klienta po dobu 10 minut v případě, že je 5x zadáno chybné heslo

PŘÍLOHA P XIII: SCÉNÁŘ ČTVRTÉ LEKCE

1. Smažte vámi vytvořenou databázi a místo ní si nainportujte přiloženou databázi
2. Restartujte Asset Server
3. V aplikaci Asset Console smažte u vytvořeného ovladače řídicí jednotky parametry GUID a číslo revize
4. Na záložce uživatelské zvuky, přidejte zvukovou nahrávku, kterou použijete jako zvuk varování při spuštění aktivity
5. Přihlaste se do aplikace Asset Client
6. Obnovte databázi zařízení
7. Vytvořte časové pásmo s neomezenou platností
8. Vytvořte uživatele s vaším jménem. Tomuto uživateli přiřadíte právo EZS na úrovni „uživatel 1“ s plným právem ke všem podsystémům a kartu s neomezenou platností a neustálým přístupem na veškeré čtečky a uživatele uložte.
9. Vytvořte uživatelskou notifikaci přehrávající zvuk při vstupu uživatele do zóny
10. Ověřte správnost vytvoření uživatele, notifikace a konfigurace z druhé lekce přiložením karty na vstupní čtečku a provedte simulovaný průchod dveřmi. Mělo by dojít k následujícím událostem:
 - a. V okně průběžných událostí bude informace o vstupu do zóny, odstřežení podsystému a spuštění aktivity
 - b. V okně sledování zón, monitorování osob počet osob v zónách dojde k připsání osoby do zóny
 - c. V okně EZS dojde ke změně stavu podsystému na odstřežený stav
 - d. V okně Aktivity bude aktivita zóna zobrazena jako spuštěná
 - e. Dojde k sepnutí relé na výstupu č. 1
 - f. Dojde k přehrání varovného zvuku z notifikace

Při odchodu ze zóny na druhé čtečce dojde inverzně k výše popsaným událostem. V případě, že k výše popsaným událostem nedochází, odstraňte závady

11. Z aplikace se odhlaste a v konfiguračním menu aplikace zapněte požadování odbavení poplachu operátorem. Následně se opět přihlaste.
12. Odpojením a zpětným připojením vstupu linkového modulu vyhlase poruchu. Tuto poruchu odbavte a následně zrušte poplach
13. V okně prohlížení historie zjistěte, kolikrát uživatel s vaším jménem vygeneroval platný průchod libovolnou čtečkou

PŘÍLOHA P XV: SCÉNÁŘ PÁTÉ LEKCE

1. V aplikaci Asset Client vytvořte nové oddělení, které pojmenujte „Školení“
2. Uživateli s vaším jménem nadefinujte příslušnost k oddělení „Školení“ s právem prohlížet v tomto oddělení pouze sám sebe a právem prohlížet v cizích odděleních ostatní uživatele, kterým může navíc upravovat docházku
3. S jiným kolegou na cvičení si vyměňte RFID karty a svému uživateli změňte číslo karty se zachováním všech ostatních parametrů
4. V pokročilých nastaveních povolte systémový audit s evidencí stavu a vytvořte referenční stav
5. Přehlaste se do aplikace Asset Console
6. Nadefinujte zásady jmen, tak aby jméno i příjmení muselo začínat velkým písmenem
7. Nastavte zásady osobních čísel tak, aby nově vytvářená osobní čísla musela začínat písmeny „b“ nebo „t“ a byla následována čtveřicí číslic 0-9
8. Vytvořte systémového uživatele pro aplikaci Client uživatele odpovídajícího vašemu uživateli s přidělením všech práv prostřednictvím uživatelského profilu
9. Přihlaste se do aplikace Client jako vámi vytvořený uživatel
10. V modulu docházky vyberte uživatele Pavel Novák a tomuto doplňte všechny chybějící průchody v posledních 10 pracovních dnech za měsíc duben 2015.
11. Vytvořte tiskovou sestavu docházky za měsíc duben 2015 a tuto uložte
12. Nadefinujte pomocné skupiny čteček, kde oddělte dveřní jednotky pro biometrická a nebiometrická zařízení
13. Všem kartám v systému omezte platnost do konce následujícího měsíce
14. Povolte vámi vytvořenému uživateli docházku
15. V Prohlížení plného auditu zkontrolujte, jaké změny se udály u vašeho uživatele a kdo byl jejich autorem
16. Z klávesnice aktivujte přemostění smyčky č. 1 linkového modulu a smyčku narušte. Poplach by neměl být vyhlášen
17. Přihlaste se na klávesnici technickým heslem a v technickém menu prohlédněte linky a stavy vstupů a výstupů
18. V technické menu proveďte regulérní restartování řídicí jednotky
19. Jako master zastřežte a odstřežte podsystém
20. Změňte heslo uživatele master

PŘÍLOHA P XVII: SCÉNÁŘ ŠESTÉ LEKCE

1. Propojte prostřednictvím RS 232 Asset a zařízení PZL-10
2. Připojte zařízení PZL-10 do sítě LAN
3. Ověřte napětově správnost zapojení ověřením napěťových úrovní
4. Spusťte software Fides Device Configurator
5. Dle MAC adresy identifikujte v softwaru zařízení
6. Zařízení povolte DHCP a odešlete konfiguraci
7. Nadefinujte ID sítě a ID objektu dle informací, která vám sdělí školitel
8. a Nakonfigurujte typ připojené technologie „Asset“, operační mód „LAN>GPRS>SMS“ povolte komunikaci s modulem smyček a odesílání metadat
9. Nakonfigurujte na záložce LAN adresu a port DPPC, které vám sdělí školitel
10. Pojmenujte vstupy IEZS 1poplach celkový, 2tíseň, 8zastřeženo
11. Konfiguraci uložte do souboru a odešlete do zařízení
12. V aplikaci Asset Config otevřete vámi dříve vytvořenou konfiguraci
13. Přidejte technický parametr Latis/Latis SQL a tento nastavte na „Latis SQL::FXP“
14. Přidejte parametr Latis LTNI/Pzl10/Latis3 a nastavte typ komunikace „RS232(PZL 10)“ přenos kompletní události
15. Pro aktivitu celkový poplach nadefinujte sepnutí 2. výstup linkového modulu, pro aktivitu tíseň a tíseň tichá nadefinujte sepnutí 3. výstupu linkového modulu, pro aktivitu zastřeženo vše nadefinujte, nadefinujte sepnutí 4. výstupu linkového modulu
16. Konfiguraci uložte a odešlete do řídicí jednotky
17. Obě konfigurace uložte a odešlete školiteli
18. Propojte dle natavených aktivit a pojmenování smyčkami DEOL výstupy reléového modulu a vstupy expanzního modulu smyček
19. Ověřte, zdali došlo k navázání datové komunikace mezi DPPC a PZL, případnou závadu odstraňte
20. Ověřte, zdali došlo k navázání komunikace mezi PZL a řídicí jednotkou Asset případné závady odstraňte
21. Narušte vstupní smyčku linkového modulu a ověřte, zdali poplachová informace bude na straně DPPC prezentována 2 záznamy
 - a. Záznamem datovým včetně metadat události
 - b. Záznamem typu poplach prezentovaným rychlou smyčkou PZL

Případné závady odstraňte

PŘÍLOHA P XIX: SCÉNÁŘ SEDMÉ LEKCE

1. Na linku RS 485 vaší instalace připojte rádiový linkový Octopus
2. Modulu nastavte adresu 6
3. V softwaru Asset Config přidejte tento modul do seznamu zařízení se správnou adresou
4. Do rádiového linkového modulu přiřadte na první adresu otřesový detektor
5. Do rádiového linkového modulu přiřadte na druhou adresu detektor PIR
6. V softwaru Asset Config přiřadte s patřičnou adresací k reléovému modulu bezdrátové detektory, u kterých přehledně pojmenujte první vstupy, které identifikují detektor v systému při vzniku poplachu
7. Odešlete konfiguraci do řídicí jednotky
8. Odešlete konfiguraci školiteli
9. Zastřežte podsystém 1 a vygenerujte na obou detektorech poplachy
10. Zkontrolujte správnost doručených poplachových informací prostřednictvím systémové klávesnice, software Asset Client a na straně dohledového přijímacího poplachového centra. V případě výskytu závad tyto odstraňte.

PŘÍLOHA P XXI: SCÉNÁŘ OSMÉ LEKCE

1. Připojte do sítě LAN docházkový terminál KMU-7
2. Zjistěte IP adresu zařízení
3. V SW Asset Console vytvořte ovladač KMU-7 a nadefinujte adresu zařízení s portem 10666
4. Nakonfigurujte tlačítka Příchod, Odchod a Oběd, kterým přidejte patřičné docházkové události a nastavte spínání zámků
5. Parametr čtecí hlava nakonfigurujte dle reálně připojené čtecí hlavy
6. Dveřím nastavte dobu sepnutí a frekvenci pípáku
7. V aplikaci Asset Client odešlete do KMU-7 nejnovější firmware ve verzi AP
8. Odešlete do terminálu konfiguraci
9. Provedte obnovu databáze KMU-7
10. Provedte hromadné úpravy všech uživatelů a karet přidáním přístupového práva na čtečku KMU-7 a povolením docházky
11. S vámi používanou kartou proveďte událost příchod
12. Zkontrolujte, zdali byla docházková událost správně
 - a. Zobrazena na obrazovce terminálu
 - b. Byl sepnut zámek (nastavené pípnutí čtečky)
 - c. V aplikaci Asset Client bylo zaznamenáno sepnutí zámku
 - d. V modulu docházka u daného uživatele zkontrolujte novou docházkovou událost

Případné závady odstraňte

13. Nainstalujte IIS
14. Nakopírujte soubory softwaru Asset Web Interface do složky
15. Nastavte potřebné údaje jako je aplikační fond, konfigurace výchozího webu, připojení k databázi Asset nebo výchozí stránka
16. Otevřete v prohlížeči Asset Web Interface
17. Přihlaste se a zkontrolujte docházku, případně odstraňte potíže.

PŘÍLOHA P XXIII: SCÉNÁŘ DEVÁTÉ LEKCE

1. V aplikaci Asset Console připojte do serveru kamerový systém, jehož přihlašovací údaje Vám sdělí vedoucí školení.
2. Nastavte uložení kamerového záznamu v délce 10 vteřin při vzniku poplachu na otřesovém detektoru
3. Přihlaste se do aplikace Asset Client
4. Nadefinujte rozvržení kamer, do kterého si kamery přidejte
5. Zastřežte podsystém jedna a vygenerujte poplach na otřesovém detektoru
6. S časovým odstupem cca 2 minuty ověřte, zdali došlo k uložení obrazu z kamery a odstraňte případné potíže
7. Nainstalujte aplikace FSS Manager, FSS Server, FSS service a FSS Notifier, kdy FSS Service nastavte připojení k databázi vytvořené instalací FSS Server
8. Spustíte aplikaci FSS manager
9. Přidejte nový typ aplikace „Asset Client“
10. Přidejte novou verzi aplikace Asset Client
11. Aplikaci Asset Client v menu schovaném za klávesovou zkratku „Ctrl+Alt+F12“ přidejte parametr povolit automatické aktualizace a aplikaci restartujte
12. Nainstalujte odpovídající verzi serveru
13. Přihlaste se do aplikace Asset Client
14. V případě, že se přihlášení nedaří, odstraňte potíže

PŘÍLOHA P XXIV: ZÁVĚREČNÝ TEST

Závěrečný test pro školení Asset

Pro úspěšné zvládnutí testu je nutno získat 80% bodů. Každá otázka je hodnocena 1. bodem.
Za špatné odpovědi se body nestráhávají. Časový limit testu je 30 minut.

Jméno a příjmení:

Datum:

1. Na linku RS 485 ŘJ Asset 804 je možné připojit až
 - a. 4 moduly
 - b. 8 modulů
 - c. 30 modulů
 - d. 84 modulů
2. Hodnota, při které smyčka linkového modulu v napěťovém režimu hlásí klid je
 - a. 0Ω
 - b. 10Ω
 - c. 20Ω
 - d. $10k\Omega$
 - e. $20k\Omega$
3. Modul Asset 10 je
 - a. Dveřní jednotka
 - b. Linkový modul
 - c. Klávesnice 1. generace
 - d. Klávesnice 10. generace
4. Konfigurace řídicí jednotky se provádí prostřednictvím
 - a. Softwarů Asset Config, Fides Device Configurator a systémové klávesnice
 - b. Softwaru Asset Console, Fides Device Configurator a systémové klávesnice
 - c. Softwaru Asset Instal a Fides Device Configurator
 - d. Softwaru Asset Config a Fides Device Configurator
5. Vstup číslo 1 modulu Asset 10 (vstup dveří)
 - a. Musí být zapojen vždy
 - b. V případě, že je čtečka zónová
 - c. V případě ovládání PZTS čtečkou
 - d. Vstup číslo jedna má reálný význam pouze u modulu Asset 20
6. Výhodou pasivního připojení ŘJ k serveru je
 - a. Mnohonásobně rychlejší komunikace
 - b. Možnost současného připojení další aplikace k ŘJ a použití DHCP při přidělování adresy
 - c. Úspora energie
 - d. Tento způsob připojení žádné výhody nepřináší

7. Vyhlášení přístupu pod nátlakem z klávesnice KMU-4 proběhne
 - a. Zadáním čísla „99“ na konec platného kódu
 - b. Zadáním čísla „99“ před platný kód
 - c. Přičtením čísla „1“ k platnému kódu
 - d. Odečtením čísla „1“ od platného kódu
8. Trvalé sepnutí zámku dveří se nastavuje v aplikaci
 - a. Asset Config
 - b. Asset Client
 - c. Asset Console
 - d. Asset Control
9. Funkce “Antimasking“ bezdrátového detektoru Minipir Octopus slouží k
 - a. Odhalení maskovaného pachatele
 - b. Detekci zakrytí detektoru
 - c. Zamezení záměny detektorů
 - d. Vyřazení části prostoru z režimu sledování
10. Fides Device Configurator neumožňuje nastavit
 - a. IP adresu DPPC, ke kterému se připojuje PZL
 - b. IP adresu DPPC, ke kterému se připojuje Asset
 - c. IP adresu KMU-7
 - d. Chování interní PZTS
11. Maximální počet uživatelů systému Asset je omezen
 - a. 500
 - b. 1000
 - c. 5000
 - d. Není omezen
12. TCP port pro naslouchání připojení ústředěn Asset v aplikaci Asset Server je vždy
 - a. 7777
 - b. 12345
 - c. 7778
 - d. Volně konfigurovatelný
13. Virtuální klávesnice není součástí aplikace
 - a. Asset Client
 - b. Fides Device Configurator
 - c. Asset Config
 - d. Asset Client Mobile
14. Nastavení bezdrátových tísňů Octopus probíhá
 - a. Pouze na systémové klávesnici
 - b. V aplikaci Asset Config a na systémové klávesnici
 - c. Pouze v aplikaci Asset Client
 - d. V aplikaci Asset Config a Asset Client

15. Konfigurace autonomní klávesnice KMU-7 probíhá
- Pouze v aplikaci Fides Device Configurator
 - V aplikacích Fides Device Configurator a Asset Config
 - V aplikacích Fides Device Configurator a Asset Console
 - Pouze v aplikaci Asset Config
16. Stažení obrazu z kamerového systému je možné v případě
- Vzniku poplachu v systému
 - Vzniku poruchy v systému
 - Vzniku poplachu nebo poruchy v systému
 - Při vzniku jakékoliv události v systému
17. Pokud má Asset Server nastavené připojení k databázi na stejném počítači ve tvaru „127.0.0.1“ a aplikace Client má nastaveno pouze připojení k Serveru pak
- Nebude možné připojit žádnou aplikaci Asset Client
 - Nebude možno připojit aplikaci Asset Client na tomto počítači
 - Nebude možné připojit aplikaci Asset Client na jiném počítači
 - Všechny aplikace Asset Client se budou připojovat bez problémů
18. Zařízení PZL má 4 základní smyčky na desce typu
- NO
 - NC
 - EOL
 - DEOL
 - ATZ
19. Zobrazení vlastní docházky uživatele v aplikaci Asset Web Interface je mimo existence systémového účtu záležitostí
- Nastavení parametru „EVS“ při editaci uživatele v Asset Client
 - Nastavení parametru „Docházka“ při editaci uživatele v Asset Client
 - Nastavení parametru „Web Service“ v Asset Console
 - Nastavení parametru „Rozšířené monitorování Historie“ v Asset Console
20. Redundance v systému Asset spočívá ve:
- Zdvojení řídicích jednotek, kdy obě aktivně naslouchají provozu na linkách
 - Zdvojení řídicích jednotek, kdy je naslouchání připojeným linkám HW přepínáno
 - Zdvojení modulů na linkách, kdy všechny aktivně naslouchají provozu na linkách
 - Zdvojení modulů na linkách, kdy je naslouchání připojeným linkám HW přepínáno

PŘÍLOHA P XXV: TESTOVÝ SCÉNÁŘ

Závěrečný testovací scénář školení Asset

Pro úspěšné zvládnutí scénáře je nutno získat 80% bodů. U úkolů je definována bodová hodnota, kdy je možno udělit částečné bodové ohodnocení. Časový limit testu je 90 minut. Pro účely konfigurace je možné používat manuály dostupné na stránkách Trade Fides. Splnění úkolů hodnotí školicí pracovník. Výchozím bodem testovacího scénáře je řídicí jednotka v továrním režimu a databáze obnovena z předloženého souboru.

Jméno a příjmení:

Datum:

Úkol	Maximální bodová hodnota	Počet získaných bodů
Zapojte na linku Asset: LML8, 2x Asset 10, KMU-7	5	
Vytvořte konfiguraci s parametry Název instalace: „Školení“, Kód oblasti: „5“, Název oblasti: „Brno“, Kód objektu: „Asset-2“, Technické heslo objektu: „16“	5	
Vytvořte řídicí jednotku Asset 801 s názvem a kódem objektu „Školení“	2	
Nadefinujte připojení aplikace Config k řídicí jednotce, která má povolené DHCP	5	
Moduly nakonfigurujte tak, aby komunikovaly s řídicí jednotkou	13	
K linkovému modulu připojte teplotní čidlo Dallas	1	
Povolte měření analogových hodnot v konfiguraci	3	
Ke dveřním jednotkám připojte správně čtecí hlavy a tlačítka simulující dveřní kontakt	5	
Ke klávesnici KMU-7 připojte předloženou čtecí hlavu	2	
Do klávesnice KMU-7 odešlete firmware ve verzi OP	5	

Konfiguraci dveřních jednotek ponechte v průchozím režimu s připojením čtecích hlav přes svorkovnici	2	
Vytvořte zónu SKV	3	
Nakonfigurujte KMU -7 jako SWD	2	
Vytvořte tlačítka „Příchod“ a „Odchod“ s příslušnými docházkovými událostmi spínajícími zámek	3	
Nakonfigurujte správně dveře a čtecí hlavu klávesnice KMU-7	2	
Nakonfigurujte připojení řídicí jednotky k vašemu serveru	3	
Asset Server nasměrujte na svou databázi	2	
Smažte původní GUID a revizi existujícího ovladače řídicí jednotky „Školení“	3	
Obnovte databázi do řídicí jednotky	1	
Hromadnou editaci povolte všem uživatelům v systému docházku a přístup na veškeré čtečky	6	
Zjistěte a vepište, kdy a kým byl vytvořen uživatel „Daniel Černý“	5	
Zjistěte a vepište, kdy a jakou první událost v systému vygeneroval uživatel „Pavel Novák“	5	
Nakonfigurujte dle informací od školitele připojení k DPPC Latis prostřednictvím LAN a odevzdejte konfiguraci	9	
Vytvořte uživatelský účet uživatele s vaším jménem a plnými právy PZTS (EVS)	4	
Vytvořte k výše zmíněnému uživateli účet systémového uživatele s právy „Zobrazení událostí EVS“, „Změna vlastního hesla“, „Přihlášení do aplikace PZTS“ a základním právem pro Firmy, Ovladače a Objekty.	4	
Součet bodů	100	

Po dokončení se řiďte pokyny školitele

PŘÍLOHA P XXVI: CERTIFIKÁT



Trade Fides, a.s.

Dornych 57, Brno

IČO: 61974731

Certifikát

O absolvování školení poplachového zabezpečovacího a tísňového systému

Asset

Číslo certifikátu A 150601

Proškolený: **František Vomáčka** Datum narození: **20. 4. 1989**

Společnost: **UTB** IČO: **70883521**

Tento certifikát je platný po dobu **2** let ode dne vystavení

Certifikát potvrzuje, že jeho držitel absolvoval 30 hodinové školení na systém Asset zakončené testem. Tento certifikát opravňuje k nákupu, instalaci a provádění servisu na systému Asset. Držitel je povinen respektovat veškeré související normy a zákony.

V Brně, dne 1. 6. 2015

Bc. Martin Buňka

Vedoucí školení

Robert Exner

Vedoucí technické podpory