Integrace BT s ASŘ v energetice

Integration of Security Technology with Control Systems in Power Engineering

Vratislav Křivák

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vratislav KŘIVÁK**
Osobní číslo:	**A07289**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Integrace BT s ASŘ v energetice**

Zásady pro vypracování:

1. **Zpracujte současný stav bezpečnostních systémů a systémů ASŘ v energetice.**
2. **Definujte funkce řídicích systémů MicroSCADA, HONEYWELL a přístupového systému.**
3. **Navrhněte vlastní řešení spolupráce těchto systémů a vyhodnoťte hlavní přínosy tohoto řešení.**
4. **Naznačte další vývoj těchto technologií.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ČSN EN 50133-1 Poplachové systémy Systémy kontroly vstupu; pro použití v bezpečnostních aplikacích**
2. **ČSN EN 50131-1 Poplachové systémy Elektrické zabezpečovací systémy**
3. **MicroSCADA OPC Data Access Server Technical Reference Manual, vydané 15.1 2004, verze: 8.4.5**
4. **Introduction to MicroSCADA Technology Technical Reference Manual, vydané 15.3 2002**
5. **Process Automation College: UxS System Administration Technical Reference Manual, vydané 27.8 1996**
6. **Process Automation College: Local/UCN/APM Maintenance Technical Reference Manual, vydané 4.6 1992**

Vedoucí bakalářské práce:	**Ing. Rudolf Drga** Ústav bezpečnostního inženýrství
Datum zadání bakalářské práce:	**19. února 2010**
Termín odevzdání bakalářské práce:	**19. května 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce pojednává o propojení přístupových bezpečnostních systémů ACCESS, ústředen I&HAS a kamerových systémů se systémy technologických procesů automatického řízení v energetice. Zabývá se nutností koordinace mezi prvky objektové bezpečnosti a řídícími systémy MicroSCADA a Honeywell, definicí a funkcí přístupového systému ACCESS a nezbytnou součinností těchto systémů v návaznosti na omezení bezpečnostních rizik. Bakalářská práce obsahuje návrh technologického propojení bezpečnostních a řídících systémů v jeden multifunkční celek, včetně jejich specifikace a popisu řešení samotného projektu v souvislosti s využitím prvků objektové bezpečnosti za účelem zvýšení spolehlivosti celkového chodu energetických zařízení a zvýšení bezpečnosti práce v energetice.

Klíčová slova: Přístupový systém, Honeywell, MicroSCADA, PLC Beckhoff

ABSTRACT

First of all this thesis investigates the connections of ACCESS control systems as well as the I&HAS centers, the camera systems and the systems including technology porcesses of the automatic processing in power engeneering. In addition this thesis discusses the necessity of relationship and coordination between the elements of the construction safety and the MicroSCADA and Honeywell controling systems, as well as the definition and the function of the Access systems. In addition, those systems have to be constructed in order to ensure the prevention of the dangerous accidents. Second of all, this examination contains the new proposal of the technological connection of the safety systems into one multifunctiuonal unit, including the details and describtion of the final solution of the project that is concluding the usage of the safety building elements. The conclusion of the project is in the increase of the punctuality and work safety at the overall function of the power engines.

Keywords: Access system, Honeywell, MicroSCADA, PLC Beckhoff

Děkuji tímto svému vedoucímu bakalářské práce Ing. Rudolfu Drgovi za odborné vedení, cenné rady a připomínky, které mi poskytoval během konzultací. Děkuji také svým spolupracovníkům Ing. Hrdinovi, Ing. Kořenkovi, CSc. a Ing. Kratochvílovi za praktické rady a umožnění bližšího seznámení se systémy Honeywell a MicroSCADA.

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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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.

Ve Zlíně

……

Podpis diplomanta

OBSAH

ÚVOD

V současné době integrace bezpečnostních systémů prožívá renesanci a na trhu se objevují stále kvalitnější a důmyslnější bezpečnostní systémy. Tyto systémy zvyšují nejen samotnou ochranu objektů a zařízení, ale také umožňují provádět různé regulační a řídící procesy, např. ovládat osvětlení nebo kontrolovat činnosti vzduchotechniky v závislosti na pohybu osob v daných objektech. Tyto regulační procesy byly dříve výhradně doménou systémů automatického řízení procesů, avšak dnes, kdy zaznamenáváme rychlý rozvoj technologií integrovaných bezpečnostních systémů, je tento trend poměrně rychle vyrovnáván.

Energetika je jedním z odvětví průmyslu, kde je nutná kvalitní koordinace všech technologických prostředků bezpečnostního průmyslu a systémů automatického nebo poloautomatického řízení procesů.

Cílem této práce je návrh a realizace vzájemného propojení všech prvků objektové bezpečnosti s řídícími systémy technologických procesů energetických zařízení. Tyto systémy slouží k monitoringu objektů, které při propojení bezpečnostních systémů do technologických procesů umožní obsluze a dispečerům lépe provozovat zařízení a distribuční sítě s ohledem na mimořádné události při napadení objektu energetických zařízení.

Ve své práci se zaměřuji na propojení přístupového systému ACCESS, který je uceleným balíčkem aplikací využívající identifikační prvky a prvků automatického systému řízení technologických procesů MicroSCADA, Honeywell a návrhu propojení všech systémů v jeden funkční celek.

I. TEORETICKÁ ČÁST

1 OBJEKTOVÁ BEZPEČNOST A VÝTAH Z NOREM

Objektová bezpečnost je složitým procesem, který zahrnuje technické a personální zajištění ostrahy objektu tak, aby narušení, napadení nebo zcizení, resp. zničení jakékoliv utajované a citlivé skutečnosti bylo v co největší míře a co nejúčinněji eliminováno na minimum.

V terminologii objektové bezpečnosti se setkáváme s pojmy objekt, což značí budovu nebo jiný stavebně či jinak ohraničený prostor, ve kterém se nacházejí zabezpečené oblasti a druhým pojmem jsou citlivé a utajované skutečnosti, které vynesením, zdokumentováním nebo zničením nepovolanou osobou mohou vážně ohrozit zájmy majitele těchto skutečností. Ochrana objektu se provádí fyzickou ostrahou, technickými prostředky a režimovými opatřeními. Fyzická ostraha objektu se zabezpečuje vyškolenými zaměstnanci provozovatele objektu, příslušníky ozbrojených sil nebo ozbrojených sborů nebo zaměstnanci pověřené bezpečnostní ochranné služby.[1]
Technickým prostředkem je bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu nebo zabezpečené oblasti. Režimová opatření jsou předem určené postupy a procesy vstupu a výstupu osob a vjezdu a výjezdu dopravních prostředků.

K návrhům prvků bezpečnosti v technologických procesech energetických provozů jsou využívány harmonizované evropské normy a ucelené postupy při projektování těchto integrovaných systémů.

1.1 Norma ČSN EN 50133-1 Poplachové systémy – Systémy kontroly vstupů pro použití v zabezpečovacích aplikacích

Norma ČSN EN 50133-1 definuje požadavky na automatizované systémy kontroly vstupů a komponenty uvnitř budov. Tato norma zahrnuje:

- Systémovou architekturu a všeobecné požadavky na systém kontroly vstupů pro zabezpečovací aplikace
- Funkční požadavky
- Definice podmínek okolního prostředí a elektromagnetické komptability

- Požadavky na komunikaci kontroly vstupů s ostatními systémy, jako jsou například ovladače přístupového místa nebo modul pro ovládání popřípadě sledování stavu elektromechanické výbavy (apas), senzory, poplachový systém a jiné

Pokud některá část systému kontroly vstupů tvoří část zabezpečovacího poplachového systému, tak musí splňovat současně i příslušné požadavky norem na zabezpečovací systémy. [2]

1.1.1 Klasifikace zabezpečení dle normy ČSN EN 50133-1

Klasifikace zabezpečení je založena na klasifikaci identifikace a přístupu, které je možno definovat pro každé místo přístupu, kde nezáleží na tom, zda se jedná o vstupní nebo výstupní místo.

Klasifikaci identifikace rozdělujeme do čtyř tříd:

- Třída identifikace 0 – prostý požadavek přístupu bez identity uživatele bez přímé identifikace
- Třída identifikace 1 – založeno na heslech, osobních identifikačních číslech, informace jsou uloženy v paměti
- Třída identifikace 2 – založena na používání identifikačních prvků, karet, insertů, otisku prstů, používá identifikační prvky nebo biometrie
- Třída identifikace 3 – založená na kombinaci třídy identifikace 2 a 3, které jsou společně s informací uložené v paměti.

Klasifikaci přístupů rozdělujeme do dvou tříd:

- Třída přístupu A – platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje jak časový filtr, tak uložení dat o přístupových transakcích
- Třída přístupu B – platí pro místo přístupu, které zahrnuje časové filtry a ukládání dat.

Společné funkční požadavky pro třídy přístupu A a B jsou rozděleny do několika podskupin, které jsou směrodatné a závazné k vlastnímu projektování přístupových systémů. Mezi hlavní podskupiny patří zpracování, napájení, samoochrana, ochrana programovatelnosti, ovládání místa přístupu, identifikace, zobrazení uživatele včetně

komunikace s ostatními systémy. Všeobecné požadavky pro projektování kombinovaných a integrovaných systémech jsou popsány v normě ČSN CLS/TS 50398 [2],[3]

1.1.2 Důležité definice normy ČSN EN 50131-1

Tato norma zavádí termín poplachové zabezpečovací a tísňové systémy místo dříve používaného termínu elektrická zabezpečovací signalizace a uvádí termín pro tyto zabezpečovací systémy se zkratkou (I&HAS). Popisuje také čtyři stupně zabezpečení:

- nízké – předpokládá se, že narušitelé mají znalost I&HAS a že mají k dispozici omezený sortiment snadno dostupných nástrojů
- nízké až střední - předpokládá se, že narušitelé mají určité znalosti I&HAS a že použijí základní sortiment nástrojů a přenosných přístrojů, například multimetr
- střední až vysoké – předpokládá se, že narušitelé jsou obeznámeni s I&HAS a mají úplný sortiment nástrojů a přenosných elektronických zařízení
- vysoké - předpokládá se, že narušitelé jsou schopní nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků v I&HAS

Dále popisuje čtyři třídy vlivu prostředí:

- vnitřní – komponenty I&HAS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytují ve vytápěných prostředí
- vnitřní všeobecné – komponenty I&HAS musí správně pracovat, jsou-li vystaveny vlivům prostředí, kde není udržována stálá teplota
- venkovní chráněné - komponenty I&HAS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty I&HAS nejsou vystaveny plně vlivům počasí
- venkovní všeobecné - komponenty I&HAS musí správně pracovat, jsou-li vystaveny vlivům prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty I&HAS jsou vystaveny plně vlivům počasí

Norma se zabývá také sestavením zabezpečovacích systémů. [4]

1.2 Norma ČSN EN 50131-1 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy

Norma ČSN EN 50131-1 je specifikací pro I&HAS instalované v budovách. Obsahuje čtyři stupně zabezpečení a čtyři třídy vlivu prostředí. Dále uvádí požadavky pro I&HAS při použití specifických, tedy daných požadavků pro danou zemi a prostředí, které nelze dlouhodobě měnit nebo nespecifických pevně zabudovaných propojovacích vedení, případně bezdrátového spojení a také určuje, že I&HAS musí obsahovat prostředky pro detekci vniknutí narušitelů, pro zjišťování poruch, pro zpracování informací, pro ohlášení poplachů a dále prostředky pro provoz. [5]

1.3 Norma ČSN EN 50132 Poplachové systémy – CCTV sledovací systémy

Systém CCTV je uzavřený televizní a střežící okruh, určený k přenosu vizuální informace a je rozdělen na tyto části:

- Snímací
- Přenos signálů
- Zobrazovací část
- Ovládání
- Příslušenství pro monitoring

Norma ČSN EN 50132 definuje požadavky na vlastnosti CCTV podle článků uvedené technické normy, které je nutno respektovat při návrhu, provozu a údržbě celého systému. [6]

2 POPIS STÁVAJÍCÍHO STAVU

Pro realizaci návrhu propojení prvků objektové bezpečnosti do automatických systémů řízení a současně zlepšením současného stavu byl vybrán objekt Teplárny Otrokovice a.s, která disponuje moderní technologií řízení a zpracováním automatických procesů, avšak velmi špatným objektovým zabezpečením celého areálu podniku. Teplárna Otrokovice a.s. je hlídána dvěma pracovníky ostrahy a obvodovou ochranou, která je tvořena pouze mechanickými zábrannými systémy. Jediným zabezpečovacím prvkem je přednastavená sada JK-82 Oasis vyráběná spol. Jablotron s.r.o., která zabezpečuje kancelář generálního ředitele a bezpečnostního technika. V nedávné době byl na Teplárně Otrokovice a.s. realizován ucelený balík aplikací využívající identifikačních prvků, bezkontaktních karet a tagů INFOS od výrobce Cominfo a.s.. Součástí balíku aplikací je přístupový systém ACCESS32, jehož hlavní funkcí je omezit vstup do vytipovaných prostorů. V původním projektu přístupového systému bylo navrhnuto pouze deset míst, které jsou vybaveny tímto systémem, včetně jednoho turniketu a otočné branky na vrátnici do objektu, což se zdá být nedostatečné vzhledem k možnosti využití celkového přístupového systému. Přístupový systém ACCESS32 umožňuje širokou realizaci rozšíření základního systému o prvky ústředen I&HAS a uzavřených dohledových kamerových systémů CCTV. Systém INFOS představuje ucelený balík aplikací využívající identifikačních prvků, bezkontaktních karet, tagů v různých oblastech firemních i jiných činností od řízení vstupů, vjezdů, přes zpracování docházky, evidenci návštěvníků, ovládání parkovišť, řízení výtahů až po obsluhu výdejových automatů na výdej stravy a další. [8]

Základní aplikace systému INFOS jsou:

- Docházkový systém PASSPORT - Slouží pro zpracování docházky na základě událostí vzniklých ze snímačů identifikačních prvků. Docházku nejen vyhodnocuje, ale kontroluje podle předem definovaných modelů pracovních dob a umožňuje i editovat a zavádět nové akce přímo z klávesnice. Data o docházce může přehledně tisknout pomocí různých sestav nebo exportovat do navazujících systémů (mzdových, personálních).
- Přístupový systém ACCESS32 - Je určen pro řízení, kontrolu a zpracování definovaných pohybů osob, vozidel nebo výrobků uskutečněných pomocí identifikačních karet (dále jen ID karty) s využitím podpůrného hardware (zejména

různých typů snímačů identifikačních karet) a souboru programových modulů na příslušných počítačích. Pohybem osob, vozidel a dalších nositelů ID karet rozumíme v terminologii přístupového systému ACCESS32 vstupy a vjezdy do objektů a výstupy z nich, dveře místností, průchozí turnikety a závory, uzavřené nebo technologické prostory.

- Návštěvnický evidenční systém VISIT - Je určen pro evidenci návštěvníků, vjezdů jejich vozidel do objektů. Je možno evidovat dosud přítomné návštěvy v rámci objektu, maximální dobu strávenou v objektu. Systém podporuje různé typy karet (podle oprávnění, kam mají přístup), má podporu více provozu na více vrátnicích. V plné instalaci je svázán se správou karet a přístupovým systémem (kde se například při průchodech zobrazují přímo data návštěvníků).

- SW stravování, obsluhu automatů pro výdej stravy, řízení kopírek CARDPAY. Je určen pro objednávkové a restaurační stravování, obsluhu výdejových automatů a snímačů (pokladen), které pracují v obdobném režimu automatů. Je schopen vést účty v rámci stravování zaměstnancům – držitelům karet, vypočítávat hodnoty odebraných jídel u jednotlivých osob a další funkce, příslušející obslužným SW.

- Systém sledování zakázek je určen pro sledování vytíženosti zakázek, odpracované doby na jednotlivých zakázkách a případnou evidenci kusových výrobků. Systém evidence zakázek je úzce provázán se systémem docházky PASSPORT.

- Administrace uživatelů a organizační struktury je určena pro zabezpečení systému INFOS přístupovými právy. Každému uživateli správce systému přidělí uživatelské jméno. Uživatel musí při každém přihlášení do systému zadat své uživatelské jméno a potvrdit svoji totožnost heslem. Dále obsahuje funkce pro vytvoření organizační struktury firmy, která je využívána v jiných aplikacích.

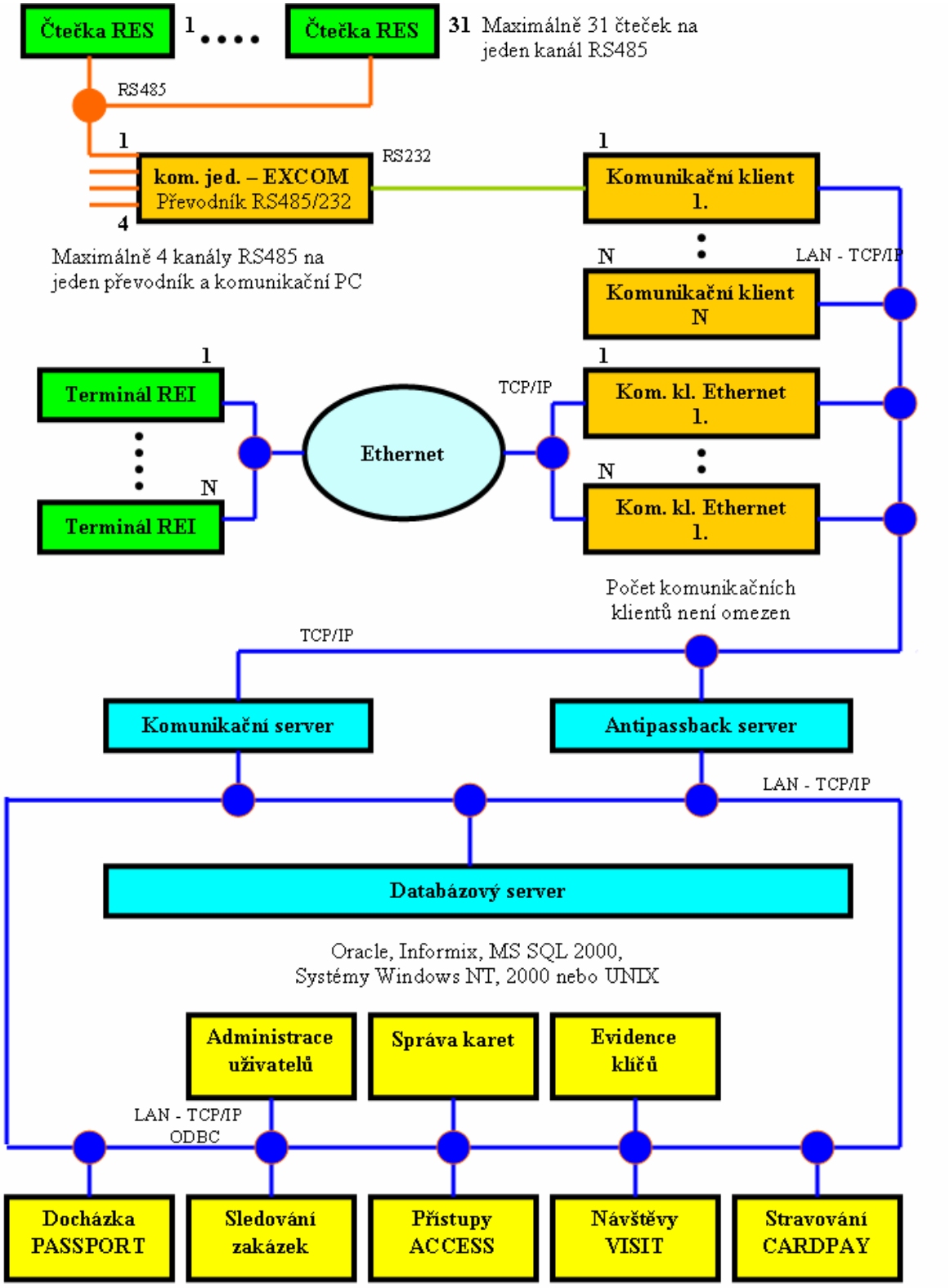
- Správa identifikačních karet je určena pro zavedení osob (držitelů) identifikačních karet do systému INFOS, přiřazení čísel karet těmto osobám a řešení všech činností spojených s kartami - ztráty, nové výdeje a podobně. Podle konfigurace aplikace zde lze přímo pořídit fotografii osoby nebo vyrobit a potisknout příslušnou identifikační kartu.

- Komunikace se snímači místa přístupu jsou určeny pro obsluhu snímačů místa přístupu, přenos definic do snímačů místa přístupu a přenos dat ze snímačů místa přístupu do systému.
- Mimo výše uvedené moduly a aplikace systém INFOS obsahuje několik podpůrných úloh, které doplňují základní funkce – jedná se zejména o moduly:
    - Archivace dat - pro správu tabulek SQL databáze
    - Spouštěč aplikací – pro jednoduchý přístup k jednotlivým aplikacím systému INFOS
    - Exportní a rutiny pro vazby na externí moduly (personalistiku, mzdy,informační systém)

Příslušné programové moduly systému INFOS jsou instalovány podle potřeb a zadání na jeden nebo více počítačů PC s příslušným základním programovým vybavením. Podle požadavků a podmínek lze aplikace systému INFOS provozovat jako jednouživatelské nebo víceuživatelské s více počítači s podporou sítí LAN, případně WAN. INFOS systém důsledně vychází z architektury klient/server. Pro SQL server jsou podporovány platformy 2000, NT, XP a Unix, podporovány jsou základní SQL servery. Klienti pracují s daty na úrovni ODBC a TCP/IP (komunikační moduly využívají přímo TCP/IP). Základní skladba počítačů podle jejich funkce v systému INFOS:

- Sběrné a komunikační počítače jsou určeny pro komunikační moduly, případně antipassback moduly a další moduly nutné pro komunikaci se snímači.
- Uživatelské počítače jsou určeny pro správu definičních, monitorovacích, prohlížecích a dalších podpůrných modulů.
- Datový server, jehož konfigurace se liší podle použitého datového stroje – buď SQL Server v prostředí Windows NT, Win 2000, XP nebo UNIX.

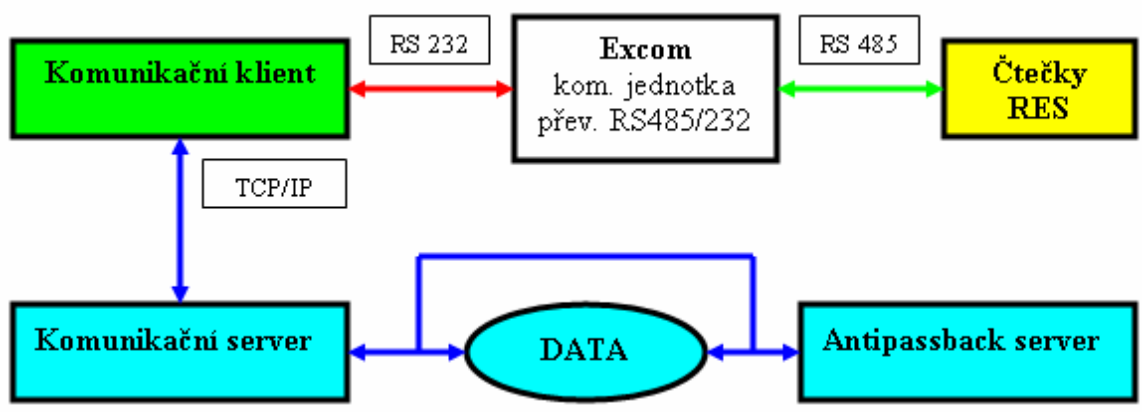
Každá aplikace, u které je to nutné a potřebné, je proti neoprávněným přístupům zabezpečena přístupovými právy, což v systému INFOS znamená, že v rámci přístupu do aplikace systému INFOS je nutno uvést definovaného uživatele s jeho příslušným heslem. Podle nastavených práv může konkrétní uživatel v rámci aplikace provádět pouze jemu povolené operace – například může data prohlížet, ale nemůže je měnit. Blokové schéma systému INFOS je znázorněno na obr. 1.



Obr. 1 Blokové schéma systému INFOS

2.1 Současné využití přístupového systému ACCESS32 na Teplárně Otrokovice a.s

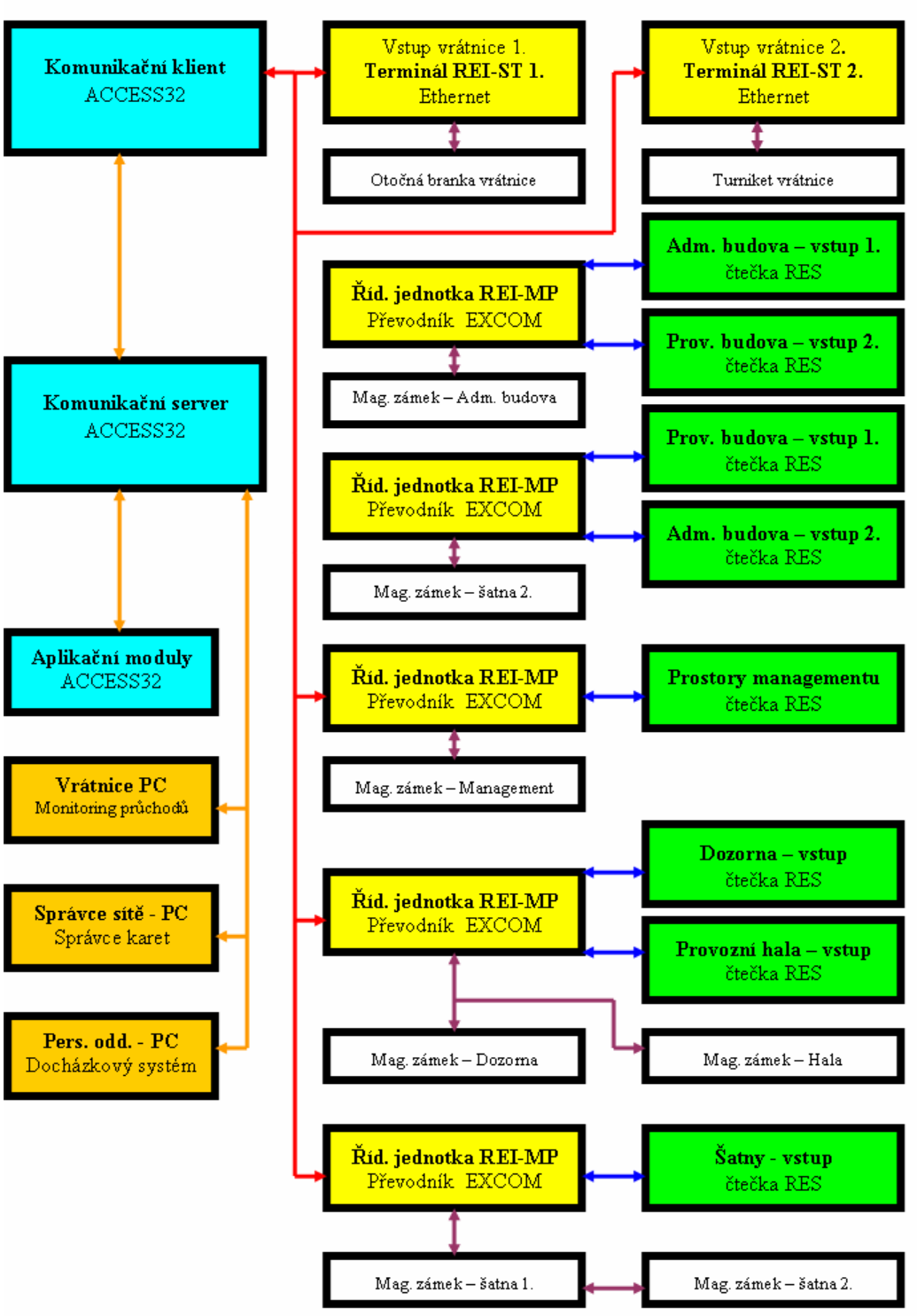
Vzhledem k možnostem, které přístupové a docházkové systému umožňují, je přístupový systém v areálu Teplárny Otrokovice a.s zcela nevyužitý. Systém ACCESS32, který je možno rozšiřovat o další prvky a aplikace je velmi vhodný pro integraci se zařízeními automatických systémů. Zjednodušené schéma systému ACCESS32 je uvedeno na obr. 2. Stávající nainstalovaný přístupový systém je souhrnem několika počítačových stanic, snímačů místa přístupu, jednoho Racku, který integruje všechny fyzické zařízení a základního serveru na kterém je nainstalován MS SQL 2000, jehož pomocí jsou zpracovávány databáze pracovníků, příchodů a odchodů.



Obr. 2 Zjednodušené schéma přístupového systému ACCESS32

Informace, které směřují směrem do základní stanice, jsou získávány ze snímačů místa přístupu RES. Tyto snímače místa přístupu jsou aktivovány pomocí čipů a zasílají informace o pohybu pomocí zařízení komunikačních klientů do komunikačních serverů, které již komunikují s danými aplikacemi jenž rozhodují, zda-li bude pracovník vpuštěn nebo nikoliv. Přístupový systém ACCESS32 je také rozšířen o aplikaci docházkového systému PASSPORT, která zpracovává databázi přístupového systému ze dvou snímačů místa přístupu RES umístěných ve vestibulu vrátnice. Tato aplikace je uvolněna pro vzdálený přístup ze tří PC pomocí sdílení SQL databáze na bázi server/klient. Klientské stanice s licenčním přístupem jsou v administraci tří vedoucích pracovníků v organizaci. Pro možnost vyhodnocování přítomnosti v rámci zón objektů je nutno definovat topologii zón přítomnosti. Členění se provádí podle skutečného provedení jednotlivých budov nebo prostorů. Samotné přiřazení do zóny provádí vždy snímač místa přístupu. Přítomnost lze

vyhodnocovat i na jedné snímací hlavě (čtečce), kde vznikají podle zvoleného kódu na klávesnici různé typy akcí (docházkové – příchodové a odchodové). Celkové schéma systému ACCESS32 je uvedeno na obr. 3.

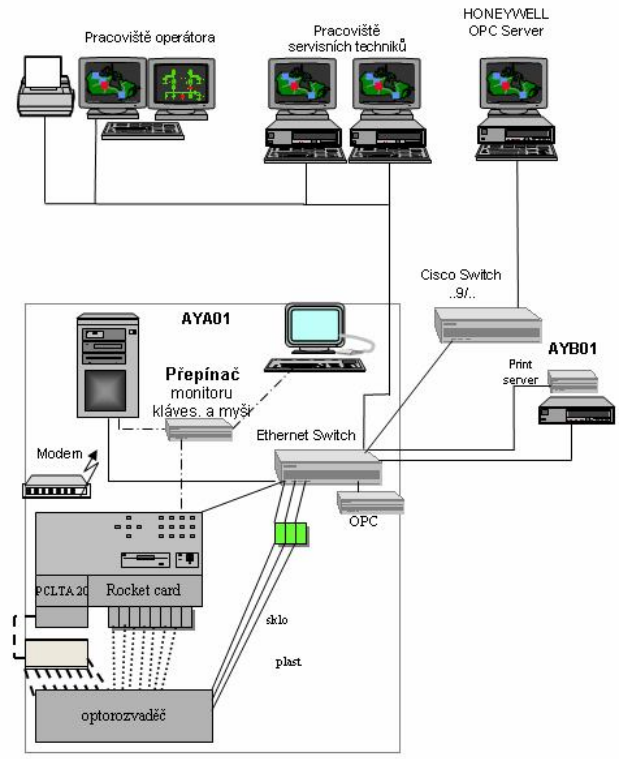


Obr. 3 Celkové schéma přístupového systému ACCESS32

Pro vyhodnocení se pak vyhodnocuje příchodová akce ve směru nastavených zón odkud a kam. Odchodová akce znamená opačný přechod, tedy ze zóny kam do zóny odkud. [9]

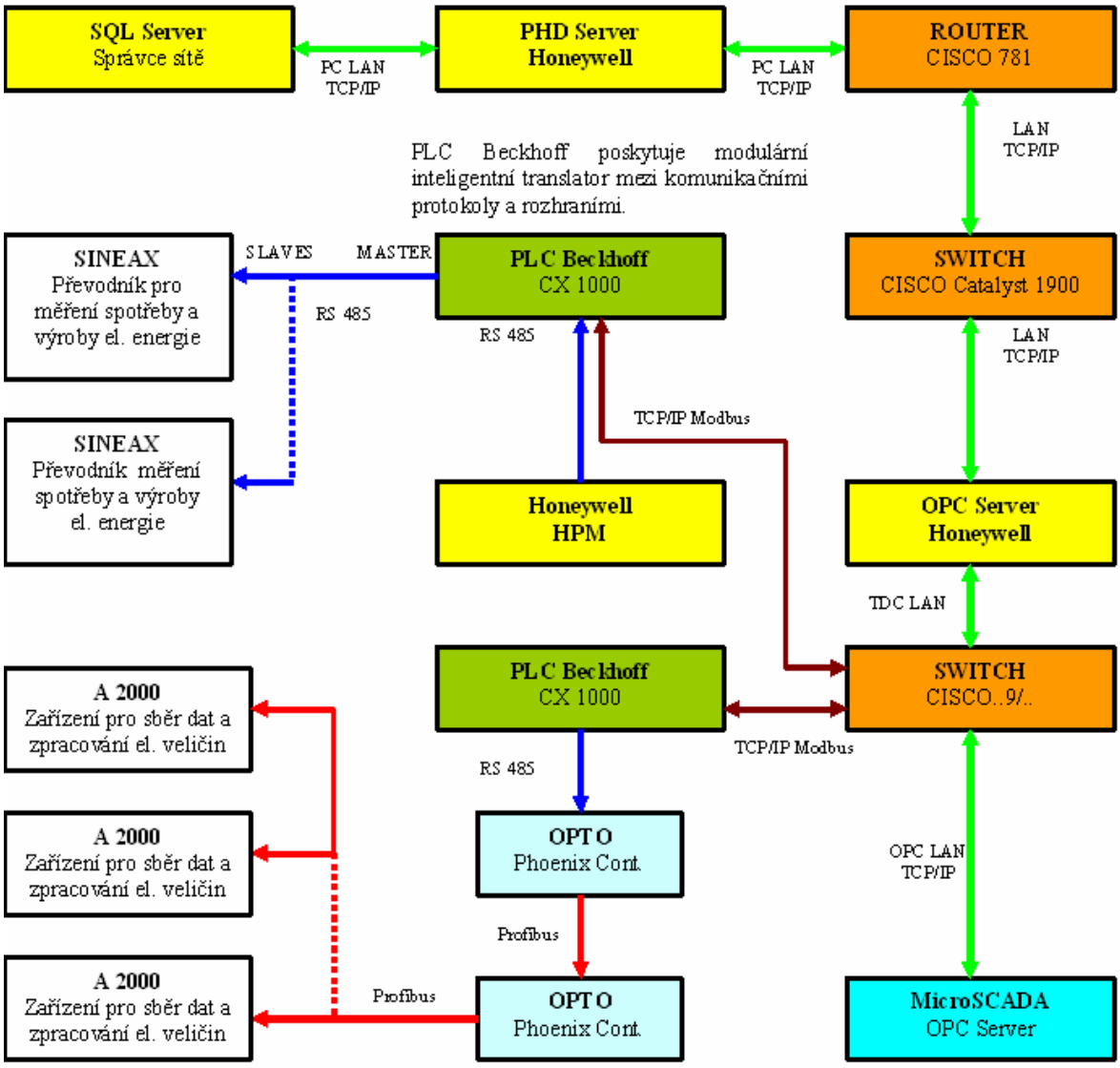
2.2 Současné propojení systémů řízení procesů MicroSCADA a Honeywell

Současná vzájemná komunikace řídících systému je založena na propojení těchto systémů pomocí ethernetového fyzického média a přepínače Cisco Catalyst 1900. Pomocí tohoto přepínače komunikuje OPC Server Honeywell s OPC serverem systému MicroSCADA. Oba systémy jsou tímto komunikačním protokolem standardně vybaveny. Je nutno brát na zřetel, že adresace prostředí v síti MicroSCADA a Honeywell je rozdílná. Převažuje adresace třídy C 192.168.11.xxx pro MicroSCADU a 192.168.169.xxx pro systém Honeywell TDC 3000. Nový systém EXPERION je adresován jako by šlo o sítě třídy A, tedy 10.0.0.x. Tyto adresace jsou standardní a doporučeny přímo výrobcem těchto systémů. Současné propojení systémů ASŘ je zakresleno na obr. 4. Switch Cisco Catalyst obsahuje aplikační bránu, která filtruje vzájemnou komunikaci.



Obr. 4 Současné propojení OPC serveru Honeywell s ASŘ MicroSCADA

Dalším prvkem datové bezpečnosti je PLC BECKHOFF, který také slouží jako brána mezi různými periferiemi a oběma systémy řízení procesů a nejdůležitější funkcí tohoto programovatelného automatu je možnost SW a HD konverze a překladu komunikačních rozhraní a komunikačních protokolů. V našem případě přijímá PLC Beckhoff data z převodníků SINEAX pomocí sériové linky RS485 komunikujících protokolem Profibus a konverzí tohoto protokolu na jeho výstupu již můžeme použít protokolu Modbus na ethernetu. Celý proces probíhá tak, že do RS485 modulu PLC Beckhoffu jsou přiváděny data komunikačním protokolu Profibus, kde je softwarově provedená translace z protokolu Profibus do protokolu Modbus. Aplikace pro translaci je dodávána v aplikačních balíčcích výrobce.



Obr. 5 Současný stav propojení systémů ASŘ Honeywell a MicroSCADA

Konvertovaný protokol Modbus je poté možné využít k přenosu dat buď opět na sériové lince nebo přes ethernet. Záleží pouze na dalším aplikovaném modulu v programovatelném automatu. Tímto způsobem je možno realizovat paralelní propojení komplexu přístupového systému a systému technologického řízení procesů. PLC Beckhoff podporuje vzájemnou konverzi protokolů a rozhraní: EtherCAT, Lightbus, Profibus, Interbus, CANopen, DeviceNET, ControlNet, SERCOS interface, Ethernet, PROFINET, EtherNet/IP, USB, Modbus, FIPIO, CC-Link, RS232/RS485, AS interface, DALI, EIB, LON.

Po naprogramování řídící jednotky zpracovanými vstupně/výstupními informacemi z dveřních kontaktů, externích terminálů REI, informacemi z výstupů I&HAS apod. může tento programovatelný automat kvalitně zastoupit řídící jednotky I&HAS ústředen a jednotek přístupových systémů. Samotné propojení systémů MicroSCADA a Honeywell je znázorněn na obr. 5. Řídící systém MicroSCADA obsahuje dvě Ethernetové karty, každá z těchto karet je adresována jinou IP adresou. První ethernetová karta slouží ke komunikaci s vlastním systémem. Druhá karta je přidána pro komunikace do jiné LAN sítě. V našem případě do sítě systému Honeywell. Z obr. 4 je patrné, že návrh obsahuje dva síťové přepínače (Ethernet switch a Cisco Catalyst 1900). Oba přepínače jsou vybaveny aplikační bránou (Proxy serverem), který řídí vzájemně bezpečnou komunikaci. MicroSCADA je chráněna pomocí varianty oddělující DMZ mezi dvěma firewally, které vytváří mezi vnější a lokální sítí tzv. demilitarizovanou zónu.

2.3 Rozbor současného stavu bezpečnostní situace a spolupráce pracovníků BS a dispečerů v energetice

Následek chybějící integrace bezpečnostních prvků do procesů automatického systému řízení technologií výroby a distribuce elektrických zařízení lze popsat v několika bodech, které monitorují současný nedostačující stav těchto koordinací. Předpokládá se, že každý pracovník, ať už bezpečnostní služby nebo obsluhy technologických procesů se řídí danými směrnicemi bezpečnosti práce, požárními směrnicemi, vnitřními směrnicemi a krizovým plánem, avšak tyto směrnice, které mohou být dokonale zpracované, ještě nezaručí, že všechny zainteresované strany, budou při případné krizové události reagovat na stejnou událost. Rozbor současného stavu bezpečnostní situace při spolupráci mezi všemi zainteresovanými stranami je možné rozdělit do čtyřech bodů:

- Současný stav koordinace dispečerů, pracovníků BS a obsluhy technologických procesů při mimořádné události je nedostatečný. Hlavním koordinátorem při mimořádné události je vedoucí směny, který řídí celkový postup prací a procesů, aby následky mimořádných událostí byly co nejmenší. Ostatní pracovníci vedoucímu směny podléhají a to včetně pracovníkům bezpečnostní služby.
- Zmapováním současného stavu docházkového systému bylo zjištěno, že docházkový systém využívají pouze dva pracovníci personálního oddělení. Využití docházkového systému je tedy minimální vzhledem k jeho obrovským možnostem.
- Současná snaha na koordinace mezi správci řídících systémů a bezpečnostními techniky na integraci systémů byla shledána a vyhodnocena příznivě. S technického hlediska je snaha o implementaci přístupových systémů do struktur systémů řízení v energetice.
- Koordinace současného stavu dispečerů a pracovníků BS při úrazu pracovníka je téměř nulová. Ve všech případech, které byly zmapovány se bezpečnostní služba o úrazu dozvěděla až po příjezdu záchranné zdravotnické služby do závodu. Bezpečnostní služba se tak nemohla aktivně podílet na záchranných činnostech a na nasměrování vozu záchranné zdravotnické služby na místo úrazu.

3 POPIS BEZPEČNOSTNÍCH A ŘÍDÍCÍCH SYSTÉMŮ

3.1 Přístupové a docházkové systémy

Systémy kontroly vstupu ACCESS mohou být používány buď samostatně, nebo v kombinaci s dalším poplachovým systémem, kdy tvoří jednu společnou bezpečnostní aplikaci.

V současné době se většinou používají tyto kombinace systémů kontroly vstupu:

- Samostatný systém kontroly vstupu (ACCESS), který umožňuje chráněný vstup do objektu po elektronické identifikaci a propustí na jednom či více místech osobu do objektu. Do součásti objektu, kam má uvedená osoba povolen vstup správcem systému. Vstup má buď povolen všude nebo s omezením.
- Kombinace přístupového systému (systému kontroly vstupu) a docházkového systému, který umožní vstup do objektu a zároveň zaznamená datové údaje pro potřeby zaměstnavatele. Tím je umožněn nejen vstup do objektu, ale také evidence docházky, tj. příchod a odchod do zaměstnání, odchod na svačinu, oběd, k lékaři, soukromý vstup z objektu, služební odchody, přerušení práce, ranní, odpolední a noční práce, práce o svátcích a dnech pracovního volna apod.
- Kombinace přístupového systému (systému kontroly vstupu, docházky, výdeje stravy, výdeje pracovních pomůcek), který umožní další kombinaci přístupu do zařízení zaměstnavatele a odběr stravy, nápojů, nářadí a jiných pracovních pomůcek, přičemž umožňuje bezhotovostní platby např., za stravu, nebo umožňuje evidenčně podchytit vydávané pracovní pomůcky, nástroje, nářadí apod.
- Kombinace systému kontroly vstupů se zařízením I&HAS, který umožní vstup do objektu oprávněné osobě a současně na trase přístupu, nebo v místnostech, kam má osoba umožněn přístup nebo průchod odalarmuje (odkóduje) systém I&HAS tak, aby nevyvolal nežádoucí poplach. Přitom eviduje a má možnosti i časově sledovat pohyb oprávněné osoby po pracovišti. Používá se všude tam, kde nestačí pouze přístupový systém, ale je nutno ještě zajistit objekt, nebo jeho část elektrickou zabezpečovací signalizací.

- Kombinace systému kontroly vstupu se zařízením CCTV se používá tam, kde je nutno kontrolovat nejen pohyb po objektu, ale i sledovat celkovou činnost osoby nebo osob v objektu a mít permanentní kontrolu veškerého pohybu v objektu s možností včasné reakce na nežádoucí situaci, která může vzniknout např. ve věženích, vojenských skladech, letištích, jaderných elektrárnách, chemických provozech apod.
- Kombinace systému kontroly vstupu do EPS je jednou z nejčastějších a nejjednodušších aplikací, používá se k zajištění automatického otevření únikových východů v případě detekce požáru systémových EPS. Z důvodů rychlosti reakce spolehlivosti a univerzálnosti je integrace prováděna zapojením napájení elektrických zámků přes kontakt signalizačního relé systému EPS.
- Kombinace systému kontroly vstupu do informačních technologií. Rostoucí využití informačních technologií vyžaduje přístup k nim. Ne všechny informace je však možno sdělovat každému a kdykoliv. Tím vznikl požadavek na integraci přístupového systému (EKV-ACCESS) versus informační technologie. Cílem integrace EKV versus informační technologie je snížení nákladů na správu hesel (především zde hrají roli zapomenutá a špatně zadaná hesla) do různých systémů a podpora udržení bezpečnosti správy hesel zajištěním vysokého komfortu uživatelů při přístupu k prostředkům informačních technologií, čímž bráníme odcházení bezpečnostních postupů různými méně zodpovědnými uživateli. [7]

3.2 Popis prvků systému ACCESS32 podle funkce v rámci komunikace

Následující řádky popisují komunikace používané v rámci systému ACCESS32 pro sběr dat a obsluhu snímačů místa přístupu v prostředí operačních systémů Windows (XP, 2000, NT 4.0, W98 a Me). V případě varianty použití komunikačních modulů v prostředí systémů UNIX je nutné použití UNIX verzí komunikačních modulů systému ACCESS32. [9]

3.2.1 Popis a význam komunikačních modulů

Hlavním významem komunikačních modulů je zprostředkování obousměrné komunikace mezi snímači místa přístupu ID karet typu REI AC4, RES AC3, RES AC1/AC2 a RED 2v5

a komunikačním (sběrným) počítačem začleněným v systému INFOS (popřípadě více komunikačními počítači).

Snímače místa přístupu mohou být připojeny k ovládacímu PC přes sériový port počítače (COMx nebo přes USB a virtuální sériový port) několika způsoby:

- snímače místa přístupu v provedení RS 485 prostřednictvím komunikačního převodníku EXCOM 1.5, který umožňuje připojení až 31 snímačů místa přístupu
- snímače místa přístupu v provedení RS 485 pomocí převodníku EXCOM4/2 (až 62 snímačů místa přístupu),
- snímače místa přístupu v provedení RS 485 pomocí EXCOM 4/4 (až 124 snímačů místa přístupu),
- snímač místa přístupu v provedení RS 232 lze připojit max. jeden snímač místa přístupu přímo do daného sériového portu počítače.

Přenosová rychlost mezi komunikačním počítačem a převodníkem může být nastavena na 9600 b/s nebo až na 115200 b/s (pouze v případě převodníku EXCOM4/2, resp. EXCOM4/4). Dále lze připojit snímače místa přístupu pomocí TCP/IP protokolu sítě Ethernet. Tento efektivní způsob podporují pouze snímače místa přístupu REI AC4. Snímače místa přístupu místa přístupu mohou mít přidělenu pevnou IP adresu nebo ji mohou získat dynamicky DHCP serveru sítě.

V rámci komunikačních úloh rozlišujeme následující programové moduly, které se liší implementovanými funkcemi:

- komunikační klienti - sběrná PC (1-n), která mají na komunikačních portech připojeny převodníky EXCOM nebo komunikují se snímači místa přístupu pomocí protokolu TCP/IP sítě Ethernet a zabezpečují přímou obsluhu snímačů místa přístupu. Klienti musí být schopni také práce bez běžícího databázového stroje, proto neprovádějí přímý přístup do tabulek.
- komunikační server (vždy jeden v rámci instalace), který provádí fyzický přístup do databáze generuje definice pro klienty a zpracovává povely s ostatních modulů,

- řídicí server (maximálně jeden v rámci instalace), vyhodnocující oprávněnost APB nebo jiných kontrolních dotazů od komunikačních klientů, resp. jednotlivých snímačů místa přístupu ID karet.

V rámci menších instalací mohou být server a maximálně dva klienti provozováni na jednom PC. Samotné komunikace plní následující základní funkce, které jsou buď součástí klienta nebo serveru.

3.2.2 Snímač místa přístupu ID karet

Snímače místa přístupu místa přístupu jsou zapojeny na sběrnici RS485 (max. 31 snímačů místa přístupu na jeden kanál RS485). Veškeré definice snímačů místa přístupu, nastavení režimů činnosti a seznamy oprávněných karet pro daný snímač místa přístupu má snímač místa přístupu uložen ve vlastních pamětech (EEPROM, FLASH a zálohované RAM), čímž je zaručeno uložení dat v paměti po dobu řádově let při výpadku napájení.. Dále řídící modul obsahuje hodiny přesného času RTC, které zabezpečují přesný čas v rámci ročních cyklů s maximální odchylkou max. 4 sekund za den. Novější řada snímačů místa přístupu může být připojena i přes rozhraní Ethenet. Při běžné činnosti po přiložení karty dojde ve snímači místa přístupu k off-line ověření karty a režimů, zda může danou akci vykonat, následně vykonání akce (sepnutí relé, registrace docházkové akce,…) a odeslání záznamu o akci do nadřízeného koncentrátoru. Dojde-li v danou chvíli k výpadku spojení na komunikačního klienta, jsou data ukládána do vnitřní paměti snímače místa přístupu (řádově tisíce záznamů podle parametrizace seznamu karet lze nastavit režim přepisování nejstarší akce nebo zablokování snímače místa přístupu v případě naplnění paměti). Po obnově spojení se neodeslané záznamy automaticky odešlou. Výjimku z předchozího popisu tvoří režim kontroly násobných průchodů (antipassback), kdy po všech off-line kontrolách ve snímači místa přístupu se ještě on-line dotazuje na Antipassbackový server, který kontroluje místo předchozího výskytu karty a povoluje samotný průchod zpět do prostoru umístění prvního záznamu. Snímač místa přístupu je případě výpadku komunikačních linek schopen pracovat naprosto autonomně bez omezení jeho funkcí nebo režimů.

3.2.3 Datový server

Veškeré definice, nastavení snímačů místa přístupu, povolení karet a uložení dat ze snímačů místa přístupu je realizováno centrálně v rámci tabulek SQL databáze. Samotné definice a

vyhodnocení probíhají z definičních a vyhodnocovacích modulů systému INFOS, které jsou dle požadavků instalovány na různých PC. Následující dvě úlohy ve spojení s převodníkem RS485/232 EXCOM nebo rozhraním Ethernet pouze zabezpečují přenos definic a nastavení ze samotné databáze do snímačů přístupového místa.

3.2.4 Komunikační jednotka EXCOM – převodník RS485/232

Představuje inteligentní HW zařízení, které umožňuje připojit na jeden port sériového rozhraní komunikačního počítače RS 232 až čtyři kanály RS485 s maximálně 31 snímači místa přístupu na jednom kanále RS485. Inteligentností se v tomto případě myslí řešení kolizí na sběrnici RS 485, jinak se jedná o převodník linek (nedrží definice). Data o záznamech akcí od snímačů místa přístupu předává dále do komunikačního klienta.

3.2.5 Řídící server

- Provádí vyhodnocení příchozích dotazů od čteček (přes komunikační klienty) a následné (ne)povolení průchodu,
- Eviduje příjem a zpracování uskutečněných průchodů
- Využití možnosti použití specifické logiky pro vyhodnocení postupu výroby a jiných událostí.

3.2.6 Komunikační server

Jeho základní funkcí je sběr dat o událostech od jednotlivých sběrných počítačů s moduly komunikačních klientů a zápisu těchto dat do tabulek databáze systému, který je nejčastěji ve formátu sestavených tabulek. Další funkcí je zpracování definic snímačů místa přístupu z tabulek databáze po jejich definování definičním modulem pro zajištění přenosu dat do sběrného PC (SQL server). Dále vytvoření definičních dat snímačů místa přístupu dle nastavení z tabulek systému, správa a distribuce těchto definic ke komunikačním klientům, příjem dat a událostí z jednotlivých klientů (TCP/IP) a zápis těchto dat :

- do tabulky událostí.
- dle nastavení do monitorovacích souborů (stacků).
- podle potřeby do jiných systému (SW I&HAS atd.).

- příjem povelů od jiných modulů systému a jejich přenos na klienty (testy, redefinice systému, snímačů místa přístupu, zařazení karty, požární poplach atd.).
- Komunikace z externími systémy (poskytování přijatých dat a událostí, příjem povelů).

V rámci komunikací zabezpečuje přístup do databáze – tj. vyčítá definice a nastavení z databáze pro jednotlivé snímače místa přístupu a ukládá je předzpracované pro jednotlivé komunikační klienty – tato filozofie u většího počtu komunikačních klientů omezuje nutný počet licencí na databázi. Dále server ukládá data ze snímačů místa přístupu, která mu předávají jednotliví klienti. V rámci jedné instalace běží vždy pouze jedna instalace komunikační serveru. Systém INFOS podporuje komunikační server v rámci prostředí Windows NT, 2000, XP nebo UNIX (HP, SCO,Linux,…). V případě výpadku SQL serveru nebo některých klientů je schopen běžet dále s posledně vygenerovanými definicemi.

3.2.7 Komunikační klient

Je modul, který je instalován na každém sběrném počítači a jeho základní funkcí je přenos dat o událostech od snímačů místa přístupu např. pomocí převodníků EXCOM do komunikačních serverů. Další funkci, která je pro realizaci nezbytná, je náležitě specifikovaná vlastnost snímačů místa přístupu, které jsou schopné být generovány z definic komunikačního serveru. Pouze zprostředkovávají přenos definic a nastavení od komunikačního serveru do snímačů místa přístupu a předávání dat o průchodech opačným směrem. Mohou běžet ve více instalacích na různých strojích (o prostředí platí totéž co pro server). Toto se s výhodou používá u rozlehlých instalací v místech s počítačovou sítí, kdy místo řešení dlouhých kabeláží se připojí linka RS485 s několika lokálními snímači místa přístupu k PC, na kterém pak běží samostatný komunikační klient. Komunikační klient je schopen provozu i v případě výpadku nadřízeného komunikačního serveru, potom všechny akce ukládá dočasně na disk a zamezí tak v případě dlouhodobé poruchy serveru zahlcení snímačů místa přístupu. Základní funkce komunikačního klienta:

- převzetí definic systému od komunikačního serveru.
- obsluha komunikačních portů s připojenými snímači místa přístupu.
- kontrola připojených snímačů místa přístupu.

- definice snímačů místa přístupu.
- sběr dat od snímačů místa přístupu.
- přenos dat od snímačů místa přístupu na komunikační server.
- přenos řídicích antipassback dotazů ze snímačů místa přístupu do řídicího antipassback serveru a zpět.
- základní monitorování připojených snímačů místa přístupu.
- zpracování povelů od komunikačního serveru.

3.2.8 Komunikační klient Ethernet

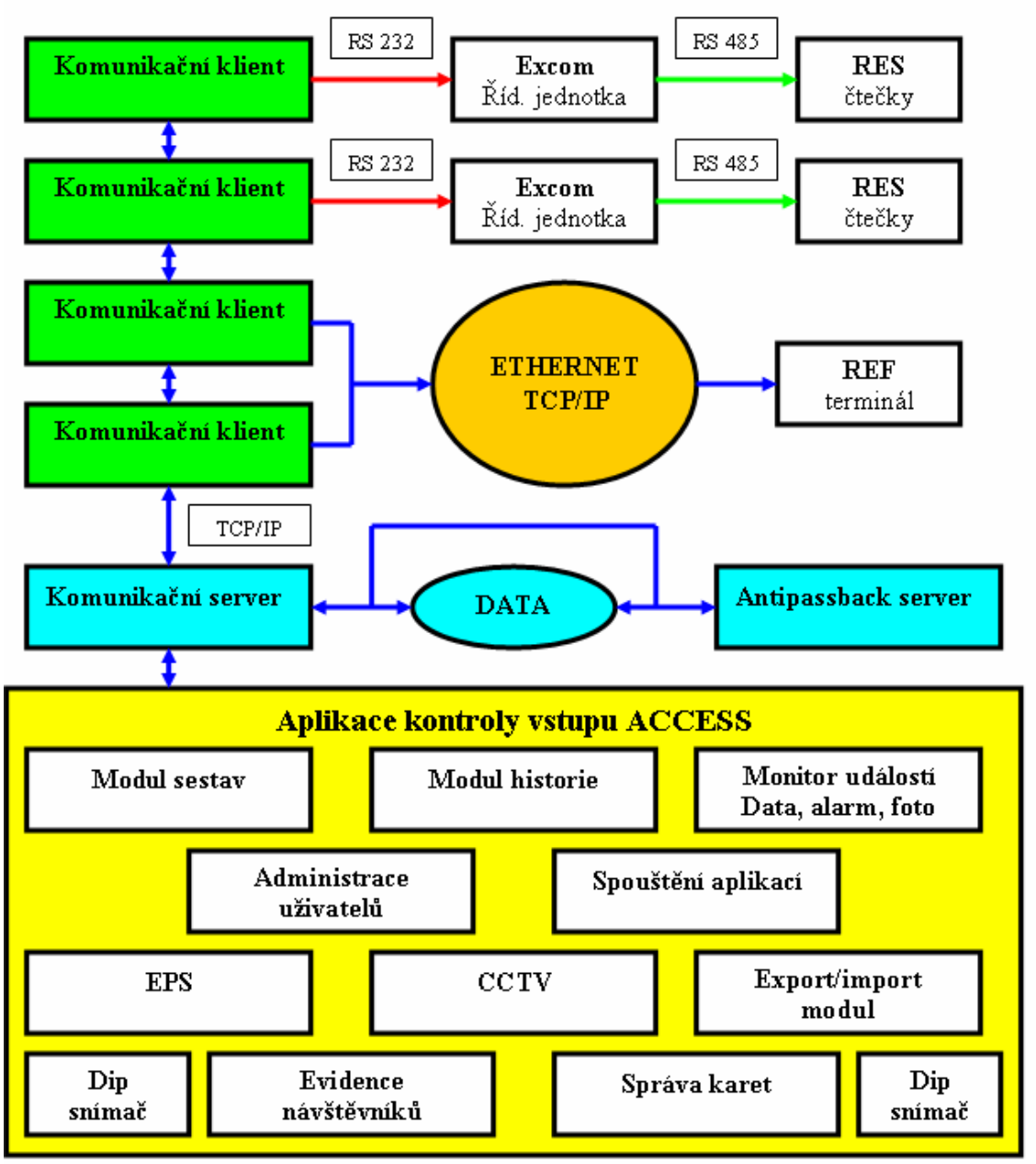
Je služba, která je nainstalována kdekoliv na síti, na které jsou připojené snímače místa přístupu. Funkčně je totožný s Komunikačním klientem. Zprostředkovává přenos definic a nastavení od komunikačního serveru do snímačů místa přístupu a předávání dat o průchodech opačným směrem. Mohou běžet ve více instalacích na různých strojích. Podle konfigurace komunikují pouze s těmi snímači místa přístupu, které jsou k nim přiřazeny i když leží na stejné síti. Komunikační klient je schopen provozu i v případě výpadku nadřízeného komunikačního serveru, potom všechny akce ukládá dočasně na disk a zamezí tak v případě dlouhodobé poruchy serveru zahlcení snímačů místa přístupu.

3.3 Aplikace kontroly vstupu ACCESS32

Systémy kontroly vstupu jsou také rozděleny do jednotlivých komunikačních a aplikačních podmnožin z pohledu nainstalovaného softwaru. Softwarové vybavení implementované v systémech kontroly vstupů je rozděleno dle specifikace a požadavků zákazníka, pro kterého jsou tyto bezpečnostní aplikace projektovány. Tyto aplikace jsou rozděleny do několika skupin podle významu, který v systému zastávají. Jedná se komunikační server, komunikační klient, komunikační klient ethernet, antipassback server, modul monitorování událostí, definiční modul, modul historie, modul tiskových sestav, spouštění aplikací, správa karet, administrace uživatelů, modul správy návštěvníků, modul Exportů a Importů.

Velmi důležitou funkcí přístupových systémů je modul Exportů a Importů, jehož prostřednictvím je možné oboustranně využívat komunikaci mezi jinými systémy jako jsou I&HAS, CCTV, automatické systémy řízení a pod. Rozšíření základních funkcí

přístupového systému ACCESS32 o více komunikačních klientů, a také o možnost komunikace těchto periferií pomocí Ethernetu, uživatel dostává možnost zavádět databáze do systému řízení procesů, výroby a provozu.



Obr. 6 Aplikace kontroly vstupu ACCESS32

Komunikace mezi řídícími a přístupovými systémy může být oboustranná. Přístupový systém ACCESS32 může také zpracovávat databáze z externích programovatelných automatů, řídících systémů MicroSCADA a Honeywell. Na obrázku 6 je znázorněn systém ACCESS32. Základními aplikacemi přístupového systému jsou: [9]

3.3.1 Antipassback server

Je server, který je určen pro vyhodnocování vícenásobných průchodů v rámci celého systému. Jeho základní funkcí je vyhodnocování on-line dotazů z komunikačních klientů na aktuální stav karet a zón. Tedy zjednodušeně, kde se daná karta nachází.

3.3.2 Modul monitorování událostí

Tento modul slouží pro přehledné zobrazování a monitorování událostí v rámci přístupového systému ACCESS32. Nejčastěji pracuje ve dvou základních modech. První je mód s oknem s potvrzením správných průchodů a druhý nás informuje o chybových událostech.

3.3.3 Definiční modul

Tento modul je určen k nadefinování systému, vlastností snímačů místa přístupu a nastavení přístupových práv jednotlivým kartám. Mezi důležité vlastnosti definičních modulů patří tyto atributy:

- Konfigurace komunikační topologie samotných snímačů místa přístupu
- Nastavení obecné topologie samotných snímačů místa přístupu
- Definice prostorových zón pro řízení vícenásobných průchodů a vyhodnocení přítomnosti
- Definice přístupových práv k jednotlivým kartám
- Časové zóny s případnou platností
- Integrovaná definice pro ovládací systémy
- Podpora režimů dvou karet a průvodcovských karet
- Zavedení definice typů karet pro danou skupinu lidí
- Zavedení časových atributů (provoz jen v určitou dobu)
- Podpora více kalendářů v rámci systému

3.3.4 Modul historie

Tento modul zpřístupňuje události, které v určitou dobu vznikly v systému. Jeho atributy jsou zpřístupnění dat systému podle různých výběrových kategorií a možnost tisku a jejich uložení do souboru.

3.3.5 Modul tiskových sestav

Nabízí užitečné tiskové sestavy a je neustále rozšiřován. Mezi hlavní vlastnosti patří:

- Sestavy o vydaných kartách nebo přístupových právech jednotlivých karet
- Možnost tisku sestav nebo jejich uložení do souborů

3.3.6 Spouštění aplikací

Představuje často univerzální spouštěč aplikací, který uživateli po přihlášení do systému zobrazí nabídku modulů. Každý modul je uživateli povolen po volbě aplikace administrátorem systému.

3.3.7 Správa karet

Implementuje funkce pro údržbu seznamu osob a karet v celém systému. Patří sem následující atributy: správa seznamů karet, přiřazování karet s využitím snímačů místa přístupu ID karet, správa seznamů osob a podpora pro práci s fotografiemi.

3.3.8 Administrace uživatelů

Zahrnuje funkce pro správu organizační struktury a definuje uživatele a jejich oprávnění pro jednotlivé moduly Integrovaných bezpečnostních systémů. Obsahuje administraci uživatelů jednotlivých modulů a administraci daných úloh pro dané typy uživatelů.

3.3.9 Modul správy návštěvníků

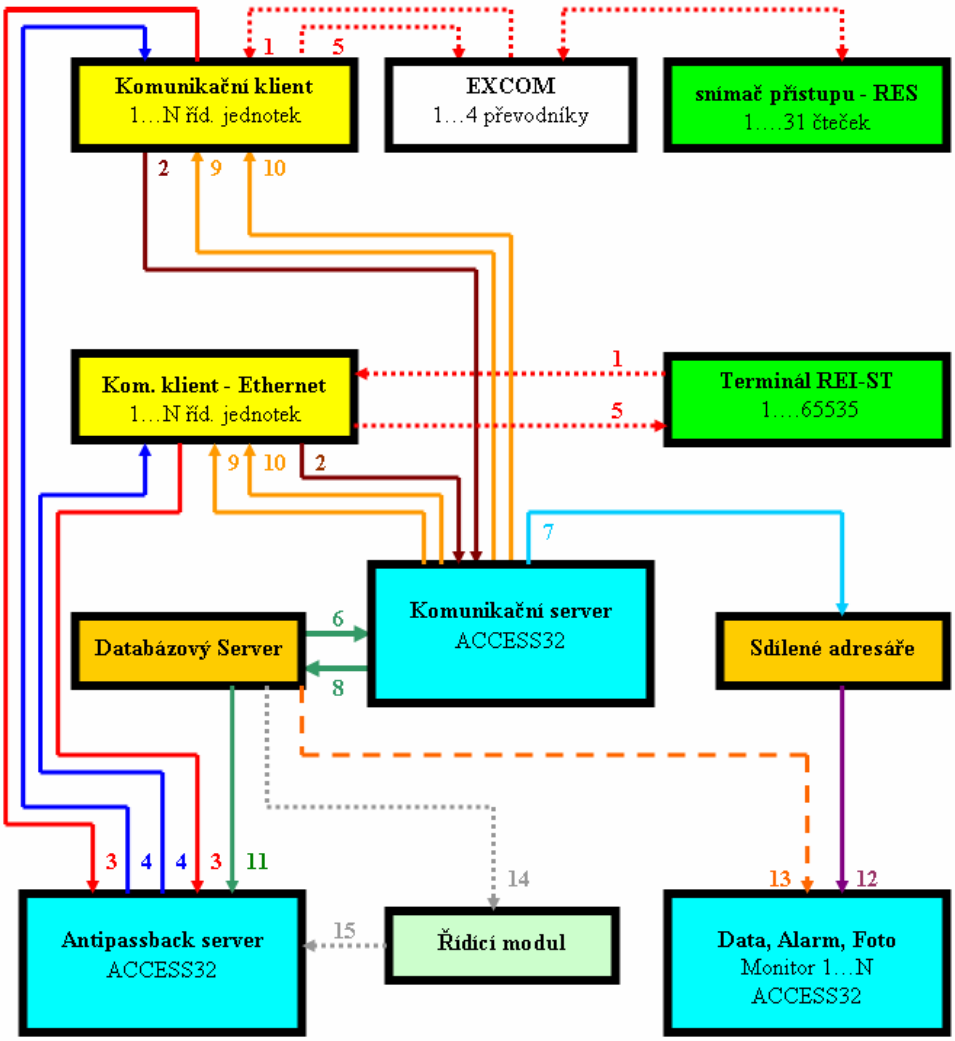
Je určen pro evidenci návštěvníků objektů a jejich vozidel, kdy eviduje návštěvníky, vyhledává předchozí příchody, přiřazuje kartu návštěvníkům a spravuje předefinované seznamy návštěvníků.

3.3.10 Modul Exportů a Importů

Je považován za doplňující modul, kde se implementují vazby na jiné systémy, se kterými přístupový a docházkový systém spolupracuje. Tento modul je považován za bránu mezi různými automatickými systémy řízení a integrovaným bezpečnostním systémem. Pro představu je nutno připomenout, že se jedná o softwarový program, který umožňuje sdílet systémové databáze pro ASŘ.

3.4 Schéma procesů v rámci komunikací systému ACCESS32

Proces v rámci komunikace je rozložen do 15ti procesů v rámci komunikace se snímači přístupového bodu systému ACCESS32. Procesy v rámci komunikace jsou zobrazeny na obr. 7. [8]



Obr. 7 Schéma procesů v rámci komunikací

Tyto procesy jsou prováděny v následujícím pořadí:

1) RS232, (TCP/IP – pro Ethernet) - z linky RS 485 (mimo Ethernet) přes EXCOM přijdou data o události na snímači místa přístupu nebo antipassback dotaz. Tyto události zpracovává komunikační klient a v případě antipassback dotazu provádí bod 3, jinak provádí bod 2.
2) TCP/IP – klient předává data do komunikačního serveru, který je pak podle konfigurace dále zpracovává.
3) TCP/IP – antipassback dotaz jde do antipassback serveru, který operuje nad daty v paměti (drží poslední průchod - antipassback. zónu) a v případě splnění podmínek antipassbacku posílá kladnou odpověď na komunikačního klienta.
4) TCP/IP – odpověď (kladná či záporná) z APB serveru na klienta.
5) RS232, (TCP/IP – pro Ethernet) – přenos odpovědi na antipassback, povelů a definic na jednotlivé snímače místa přístupu.
6) TCP/IP-OLEDB – zápis dat o událostech do tabulek databázového stroje podle konfigurace.
7) FILE PŘÍSTUP – zápis dat do stacků (zásobník – datová struktura) pro monitorování systému.
8) TCP/IP-OLEDB – zpracování a předkompilování definičních dat systému pro čtečky seskupených podle jednotlivých komunikačních klientů – výsledná data jsou uložena v souborech (pro každého komunikačního klienta zvlášť). Jejich organizaci si řídí komunikační server.
9) TCP/IP – komunikační klienti se v pravidelných intervalech dotazují na aktuální verzi definičních souborů – pokud jsou novější – přenesou si je do svého pracovního prostoru a zase jsou schopni pracovat samostatně i bez běžícího komunikačního serveru.
10) TCP/IP – zasílání povelů a příkazů pro jednotlivé komunikační klienty.
11) TCP/IP-OLEDB - při náběhu a běhu antipassback serveru si tento stahuje informace o platných kartách a o konfiguraci jednotlivých snímačů místa přístupu a zón

definovaných v rámci antipassbacku. (při náběhu každá karta dostane jednu možnou chybu)

12) FILE PŘÍSTUP - on-line monitory monitorují data v alarm a datových stacích, kde si pouze posouvají zarážky. Stacky spravuje komunikační server.

13) TCP/IP-OLEDB – pro monitorování jednotlivých událostí je nutno načítat data o snímačích a osobách.

14) TCP/IP-OLEDB – řídící modul čte konfiguraci systému a zapisuje povely pro server zpět do databáze. Následně si načítá výsledky povelů z jednotlivých čteček.

15) TCP/IP – zasílání povelů pro antipassback server z řídícího modulu

3.5 Blokové schéma a popis systému kontroly vstupu ACCESS32

Přístupový systém ACCESS32, na kterém jsem postavil svojí bakalářskou práci, je koncipován pro systémy evidence docházky s centrální databází a správou karet. Základní data pro přístupový systém, se kterými ACCESS32 pracuje, jsou snímána snímači místa přístupu typu REI, určené pro komunikaci po Ethernetu protokolem TCP/IP. Celý systém se skládá z terminálů bezkontaktních identifikačních ID karet, napájecích zdrojů, počítačových pracovišť s nainstalovanými softwarovými moduly PASSPORT. Pro systém kontroly vstupu je použita řídící jednotka a převodník EXCOM s externími snímači místa přístupu ID karet RES, popřípadě řídící jednotkou REI-MP/ET, elektromagnetické otvírače, napájecích obvodů a sestavy motorových turniketů a branek. Přístupový systém využívá společnou databázi a software INFOS. ACCESS32 využívá lokální síť a datové soubory ukládá na paměťové místo serveru. V základní technické dokumentaci, kterou dodává výrobce zařízení ACCESS32 je počítáno s instalací pouze jednoho síťového přepínače. V základním režimu je počítáno s propojením komunikačního serveru, komunikačního klienta, úložiště dat, DHCP a DNS serveru, identifikačního programu a řídících jednotek REI-MP/ET. Tento systém pracuje autonomně a nekomunikuje s jinými řídícími systémy. Dnes už jsou přístupové systémy koncipovány tak, aby uměly za určitých podmínek s různými systémy komunikovat a vyměňovat si vzájemně důležitá data. Snímač místa přístupu REI je nainstalován na ethernetové síti jako síťové zařízení a obsahuje vlastní MAC adresu. Komunikuje pomocí IP protokolu. Samotná komunikace mezi REI a aplikacemi se děje pomocí TCP protokolu. Snímače místa přístupu místa RES komunikují s

komunikačními jednotkami EXCOM pomocí sériového rozhraní a tyto jednotky EXCOM vysílají data do komunikačních serverů pomocí sady protokolů TCP/IP.

Přístupový systém ACCESS32 obsahuje tyto základní funkce:

- zavedení definice snímač místa přístupu (kontrolované místo vstupu) a zóna (množina snímačů místa přístupu definující vstupy do určité oblasti)
- definování množiny ID karet i s případným organizačním rozdělením (stromová organizační struktura i s právy na jednotlivá střediska)
- definování práv jednotlivých ID karet pro vstup do zóny (časová práva vstupu se definují v rámci dne a týdne)
- kontrola násobných vstupů antipassbacku - je řešen časový (určitou dobu se nesmí opakovat pokus o průchod) a globální (kdy doba není definována)
- zpřístupnění aktuálních stavů systému (kde se která identifikační karta, osoba nachází,
- stav zařízení, signalizace alarmových stavů) pomocí monitorovacích úloh
- definice a vyhodnocení nátlakových kódů (tajný alarm)
- funkce sledování překročení doby nutné k zavření dveří, kontrola otevření dveří jiným způsobem než identifikační kartou
- definice různých úrovní alarmových stavů systému (zejména z hlediska jejich vyhodnocování a potvrzování)

Přístupový systém ACCESS32 komunikuje mezi svými periferiemi pomoci sady protokolů TCP/IP. To umožňuje uživateli kombinovat přístupové systémy se zařízeními I&HAS a CCTV. Systém ACCESS32 umožňuje připojení až 255 adres a při softwarovém definování je možné využít až 4095 adres, tedy takové množství snímačů místa přístupu, které je více než dostačující. Důležitým aspektem pro praktickou část práce je aktivita řídící jednotky, kterou dělíme do tří skupin:

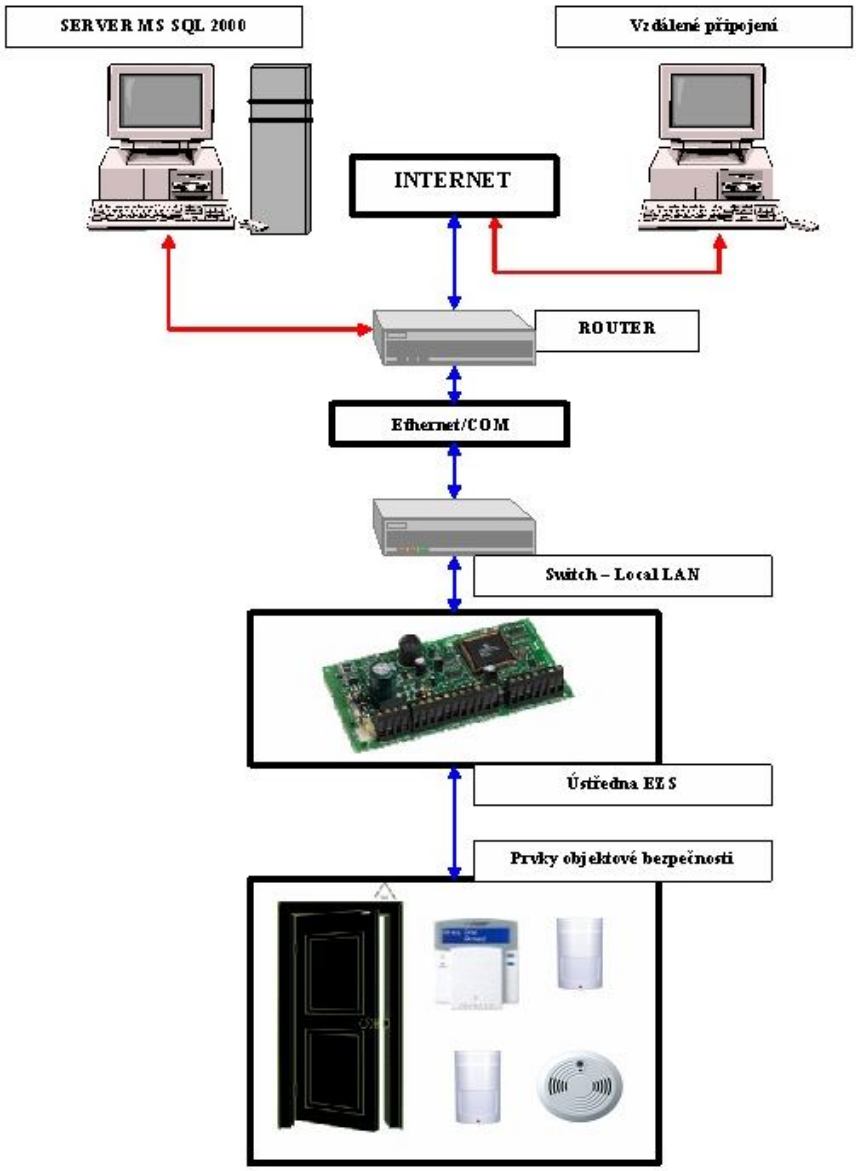
- Registrace do sítě
    - Statická registrace, kdy snímač místa přístupu má pevně nastavenou IP adresu, masku sítě, IP adresu základní stanice
    - Dynamická registrace, kdy snímač místa přístupu získá parametry z DHCP serveru (při této registraci používá porty 67,68)
- Nastartování komunikace s běžící aplikací
    - Snímač místa přístupu posílá cyklicky s intervalem 1 sekundy broadcoast TCP paket na portech 2611 až 2620. Na tomto portu běží také základní aplikace, která paket přijme a snímač místa přístupu REI odpoví na jakém portu se nachází komunikační klient pro komunikaci se snímači místa přístupu.
- Rutinní komunikace
    - Probíhá pomocí TCP paketů. Struktura paketu je podobná jako při použití RS485 s novým protokolem.

V základním zapojení dodávané výrobcem systému ACCESS32 si klient snímače místa přístupu sám registruje komunikačního klienta a poté komunikuje na stejné síti s komunikačním serverem. Komunikační sítě lze rozšiřovat pomocí externích směrovačů a následně tak komunikovat se vzdálenými stanicemi, které se nacházejí v jiných sítích, než-li komunikační server, komunikační klient a snímače místa přístupu RES. [9]

3.5.1 Kombinace systému kontroly vstupů ACCESS32 se zařízením I&HAS

Zařízení elektrické zabezpečovací signalizace (zařízení I&HAS) je soubor detektorů, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovacích zařízení a ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. Ústředna elektrické zabezpečovací signalizace je zařízení, které přijímá a vyhodnocuje výstupní elektrické signály od detektorů I&HAS, ovládá signalizační, přenosová, zapisovací a jiná zařízení, která indikují narušení střeženého místa, napájí detektory a další prvky I&HAS elektrickou energií, pomocí elektromechanických nebo kódových zámků, popřípadě vlastních ovládacích klávesnic, umožňuje ovládání celého systému I&HAS nebo jeho částí

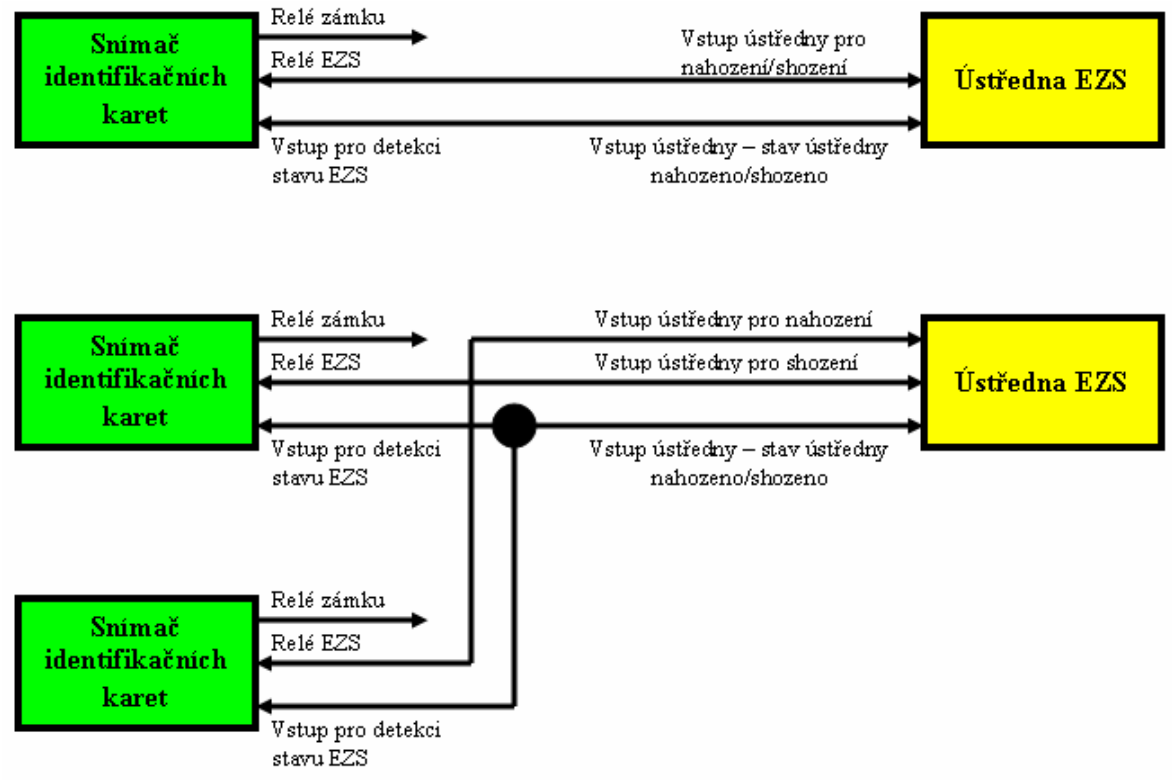
do stavu střežení a do stavu klidu a umožňuje diagnostiku systému I&HAS. V zásadě lze ústředny I&HAS rozdělit do čtyř hlavních skupin a to na ústředny smyčkové, s přímou adresací, smíšeného typu, ústředny s bezdrátovým přenosem poplachového signálu od čidel. [10]



Obr. 8 Přehledové schéma komponentů I&HAS

Komunikační topologie prvků je zobrazena na obr. 8. Mezi ústřednou I&HAS a komunikačním serverem je vřazený přepínač a směrovač, pro vzájemnou komunikaci zařízení. Systém ACCESS32 v současné době podporuje ovládání I&HAS ústředen pomocí jednoho relé (impulsem pro shození a dalším impulsem pro nahození) nebo dvěma relé (samostatné relé pro shození a nahození I&HAS). Principiální schéma ovládání I&HAS

ústředny snímači místa přístupu ID karet je zobrazeno na obr. 9.



Obr. 9 Schéma nahození a shození I&HAS s jedním a dvěma snímači místa přístupu

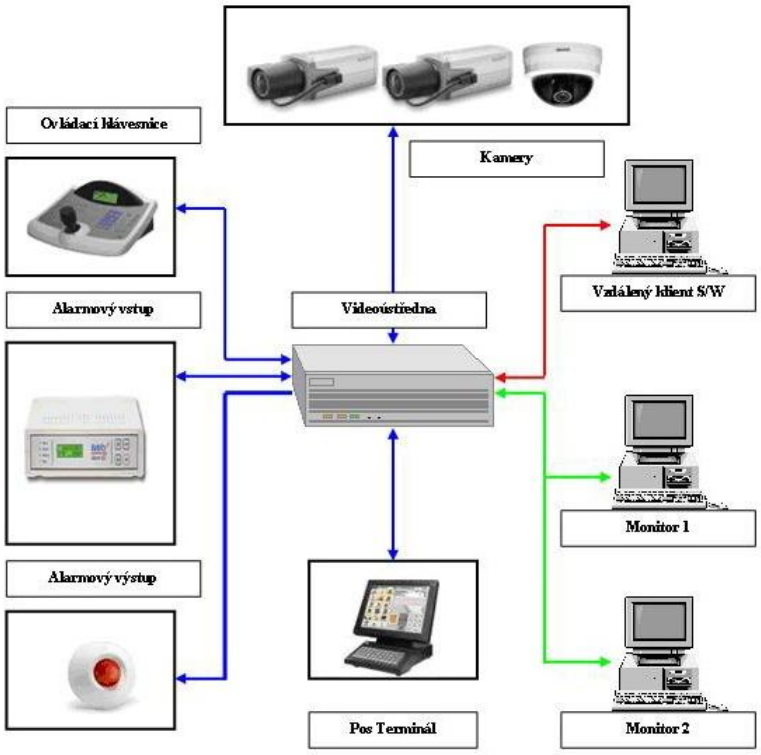
Pro správnou činnost ovládání je nutné mít připojen na snímač místa přístupu stav I&HAS ústředny. Možností kombinací režimů i způsobu ovládání je více. Příklady doporučených způsobů režimů a ovládání pro variantu s jedním a dvěma snímači místa přístupu: [9]

- REŽIM 1- přepínání I&HAS bez kontroly stavu po prezentaci oprávněné karty spojené se sepnutím relé zámku a vysláním standardního paketu
- REŽIM 2 - vypínání I&HAS s kontrolou stavu po prezentaci oprávněné karty spojené se sepnutím relé zámku, vysláním standardního paketu a vysláním paketu „vypnutí I&HAS“
- REŽIM 3 - zapínání I&HAS s kontrolou stavu po stisku klávesy „MENU“ a po prezentaci oprávněné karty spojené se sepnutím relé zámku, vysláním standardního paketu a vysláním paketu „zapnutí I&HAS“
- REŽIM 4 - zapínání a vypínání I&HAS s kontrolou stavu po prezentaci oprávněné karty. Funkce vypínání I&HAS je shodná s režimem 2. Funkce zapínání I&HAS je

shodná s režimem 3 s jediným rozdílem, a to že není spínáno relé zámku a není vysílán standardní paket.

3.5.2 Kombinace systému kontroly vstupu se zařízením CCTV

Systém CCTV ,znázorněný na obr. 10, je uzavřený televizní a střežící okruh, který je přímo určený k přenosu vizuální informace. Celý systém je možno rozdělit do několika částí. Jedná se o části snímací, přenosové, zobrazovací, ovládací a monitorovací. Důležitým kritériem pro činnosti CCTV je rozdělení systému na analogové nebo digitální zpracování signálu. Digitální přenosy kladou vysoké nároky na kapacitu datových linek. Pro menší nároky již existují digitální kamery s vlastní IP adresou, které jsou vhodné pro přímou integraci se zařízeními pomocí sítě Ethernet. Systém CCTV může mít také vazby s jinými systémy, například se systémy I&HAS.



Obr. 10 Přehledové schéma CCTV

Při požadavku spolupráce systému CCTV s nadřazenými systémy je nezbytné, aby systémový integrátor dokázal komunikovat se zařízeními CCTV a bylo plně možné využít jejich komunikačních možností. [10]

3.5.3 Kontrola a signalizace stavů dveří

Dveře mohou být osazeny z každé strany snímačem místa přístupu nebo tlačítkem pro evidenci průchodů.

Samotný průchod použitím tlačítka lze evidovat jako „volný průchod“ (bez určení karty).

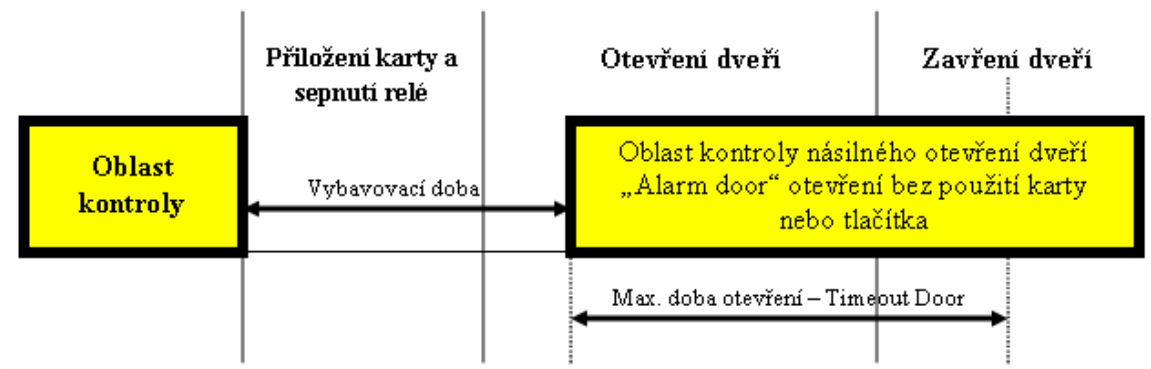
Snímač místa přístupu při přiložení karty s příslušnými oprávněními a případného zadání PIN spíná relé pro otevření dveří. V rámci systému ACCESS32 je možno nastavit způsob odesílání dat o události:[9]

- ihned po sepnutí relé – v rámci této varianty nemusí být připojen dveřní kontakt a stačí jednodušší verze turniketu (bez rozlišení směru otáčení), data jsou po sepnutí relé ihned odesílána do komunikačního klienta.
- až po skutečném průchodu (po otevření dveří nebo protočení turniketu), v tomto případě musí být zapojen a na snímači místa přístupu povolen dveřní kontakt nebo výstup z turniketu pro rozlišení směru otáčení. Dále se tato funkce musí povolit v rámci nastavení snímače místa přístupu, a pak jsou data odeslána až pro skutečném průchodu.[9]

Systém ACCESS32 umožňuje sledovat doby otevření dveří. Pro tuto funkce musí mít rovněž připojen dveřní kontakt a povoleno jeho monitorování. Pro každý snímač místa přístupu se definují následující položky:

- Definuje se maximální doba (Timeout Door), po jakou mohou být dveře otevřeny (doba od otevření dveří). Pokud zůstanou dveře po uplynutí této doby otevřeny, je vyhlášen „alarm – dlouhá doba otevření“ (nezáleží, zda byl průchod uskutečněn s kartou nebo například klíčem). Sleduje se pouze skutečná doba otevření. Tuto funkce je možno použít bez funkce Alarm Door z bodu 2 i pro snímací hlavu pouze z jedné strany dveří. Po signalizaci alarmu je při zavření dveří generována událost „zavření dveří“.
- Povoluje se kontrola Alarm Door – sledování násilného otevření dveří. Za násilné otevření se považuje otevření dveří při nesepnutém relé určeného pro zámek. Okamžitě po násilném otevření je generován „alarm – násilné otevření dveří“. Při správném průchodu (relé pro zámek je sepnuto) se vyhodnocuje dlouhé otevření dveří Timeout Door z bodu 1 (po alarm stavu následuje událost „zavření dveří“).

Pro funkci Alarm Door musí být snímací hlavy nebo tlačítka pro sepnutí relé instalovány z obou stran dveří.



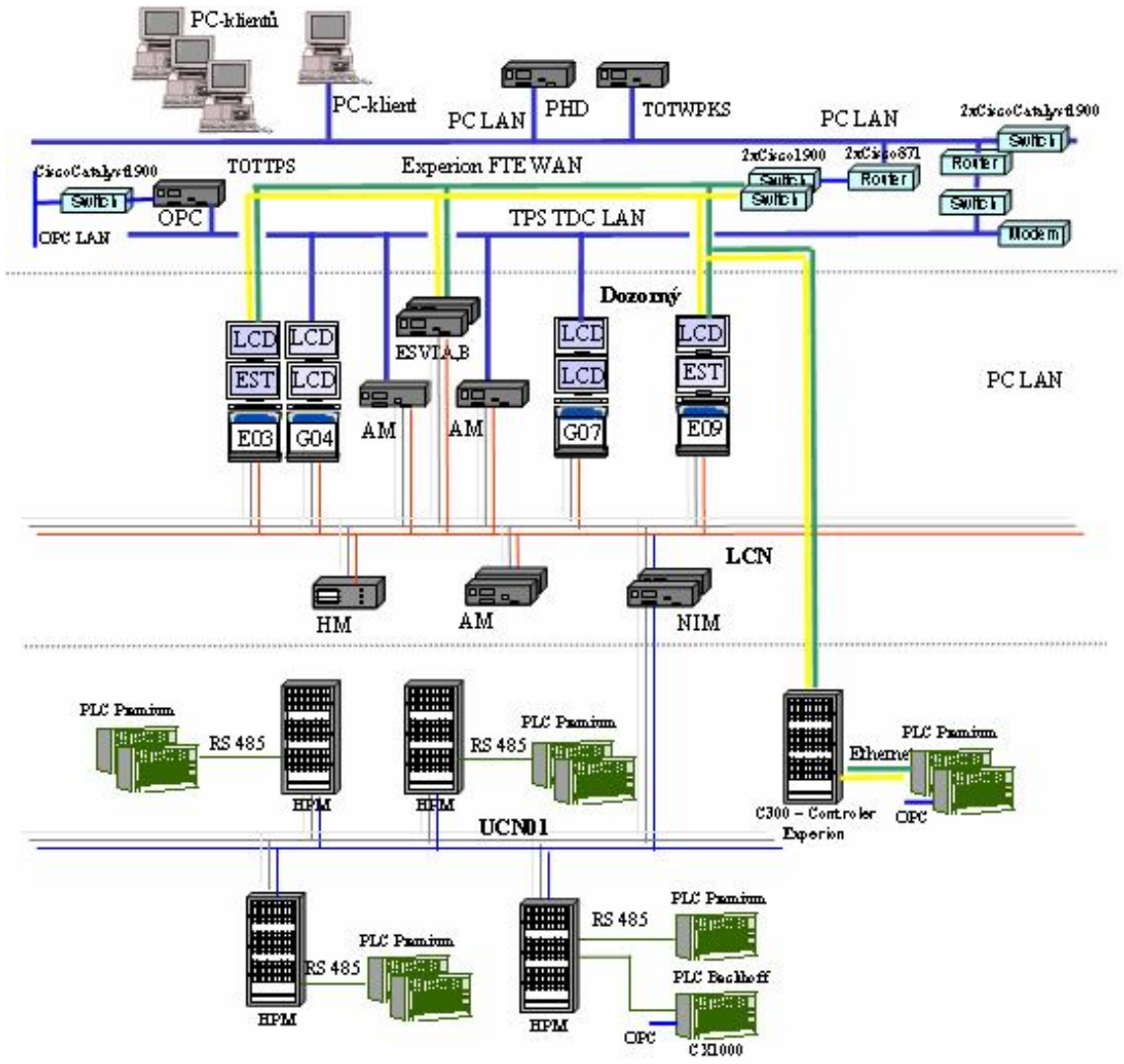
Obr. 11 Kontrola a signalizace stavu dveří

3.6 Řídící systém Honeywell

Global User Station (GUS) byla vyvinuta firmou Honeywell pro průmyslový řídící systém TDC3000/TPS a nyní také pro zcela nový systém EXPERION jako prostředek na systémové a softwarové práce, řízení průmyslových procesů a pro prezentaci nebo sběr technicko-ekonomických dat. Schéma je zobrazeno na obrázku 10. Zásadním rozdílem v činnosti těchto stanic je rozdílné komunikační rozhraní. Původní sériové komunikační rozhraní (TDC 3000) je nahrazováno rozhraním Ethernet (EXPERION), které má v současné době větší technickou podporu a je všeobecně rozšířenější než rozhraní pracující na sériové lince. GUS pracuje pod operačním systémem Microsoft WINDOWS NT. Technické zpracování stanice umožňuje připojení jak na místní síť, tak i v reálném čase na Local Control Network (LCN). Obsluze je umožněn přímý vstup k procesním údajům a řízení procesů z displejů nakonfigurovaných v rámci softwarového vybavení GUS (Native Window). GUS může disponovat celou řadou přídavných periferií, jako jsou zařízení pro záznam dat (Hard disk, jednotek CD-ROM, Floppy disků a zařízení pro tisk kompatibilních s Windows NT.

Systémy TDC3000/TPS (Totally Distributed Control system / Total Plant Solution) a EXPERION jsou distribuované řídicí systémy s definovanou hierarchií. To znamená, že všechny jejich řídicí, regulační, dohlížecí, prezentační a další prvky jsou rozděleny mezi řadu specializovaných procesorů mezi sebou navzájem komunikujících v rámci příslušné sítě na základě pravidel daných strukturou sítě a na základě vzájemné hierarchie mezi jednotlivými

prvky na síti. Běžný uživatel nepozná, zda pracuje na systému TDC 3000 nebo EXPERION, protože koncové zařízení jsou společná. Rozdílné je pouze technologie přenosu dat. Technik nebo projektant, který bezpečnostní prvky implementuje do těchto zařízení, musí být obeznámen správcem ASŘ do kterého z těchto systému budou data importována. Technická dokumentace a technická podpora obou systémů jsou na slušné úrovni. V České republice existuje několik firem, které vysílají své pracovníky na školení a umí tyto systémy nakonfigurovat. Silnější technická podpora je všeobecně shledávána v systému TDC 3000. Systém EXPERION ještě není tolik rozšířený, ale postupně nahrazuje původní systém TDC 3000 pracující na sériovém rozhraní. Přístup k procesním údajům, operátorské stanice a technologie zpracování dat zůstala zachována. Oba systémy tedy pracují v bezkolizní součinnosti. [11]



Obr. 12 Schéma ASŘ Honeywell na Teplárně Otrokovice a.s

Hierarchicky se síť skládá z několika částí:

- lokální řídicí sítě (LCN), které představují nejvyšší úroveň a nemají přímý styk s technologickým procesem.
- jedné nebo více procesních sítí, které přímo komunikují s technologickým procesem, ale mají omezené funkce, zejména prezentační (X-vrstva, vrstva s WINDOWS NT).
- Součástí LCN několik základních typů specializovaných procesorů.
- Operátorská stanice, jinak Universal Station (US). US má dva hlavní režimy práce:
    - operátorský - je možná přímá interakce (řízení) s technologickým procesem
    - inženýrský - není možná interakce s technologickým procesem, ale zato je možné mít přístup ke všem detailům a prostředkům operačního systému. Pouze v tomto režimu je možné např. vytvářet grafická schémata, provádět softwarové práce a systémové operace.

  Na US se pracuje pouze ve standardním programovém prostředí TDC 3000.
- Operátorská stanice s X-vrstvou, jinak Universal Station X (U^XS), která kromě plné funkčnosti jako US umožňuje i přístup na ethernetovou podnikovou informační síť pomocí tzv. X-vrstvy. U^XS umožňuje práci nejen ve standardním programovém prostředí TDC 3000, ale i v programovém prostředí X-vrstvy.
- Operátorská/inženýrská stanice Global User Station (GUS). Na GUS se pracuje v programovém prostředí WINDOWS NT. Kromě základního softwarového vybavení GUS operačním systémem WINDOWS NT a softwarem umožňujícím přístup do prostředí odpovídajícího US - tzv. Native Window, může být stanice navíc vybavena (podle rozsahu dodávky určené zákazníkem) řadou softwarových podpůrných prostředků umožňujících efektivní provádění inženýrských prací na TDC 3000 a ovládání procesu z nestandardních uživatelsky navržených a nakonfigurovaných displejů.
- Aplikační modul (AM), jedná se o pomocný programový modul, na kterém obvykle běží programy, starající se o vazby mezi různými procesními proměnnými, programy pro směnové, denní a měsíční přehledy a bilance apod.

- Modul historie (HM), což je záznamová jednotka (disk), který jednak obsahuje všechny soubory patřící k operačnímu systému TDC3000 a EXPERION, jako jsou konfigurační programy, textový editor, obrazový editor, kompilátor programovacího jazyka a mnoho dalších a jednak jsou na něm ukládány vybrané procesní hodnoty, procesní alarmy, zásahy operátora a další hodnoty, dokumentující činnost řízeného technologického procesu a jeho okolí
- Computer Gateway (CG) zprostředkovává styk mezi LCN a jiným počítačem (PC), který je použit pro další funkce, nesloužící bezprostředně k řízení technologie, ale vyžadující znalost hodnot z technologického procesu (např. zpracování údajů docházkového systému)
- Network Gateway (NG) spojuje 2 různé LCN:
    - Network Interface Module (NIM) spojuje LCN s Universal Control Network (UCN). UCN integruje nejvýkonnější zařízení pro řízení provozu, technologie a koordinaci systémů.

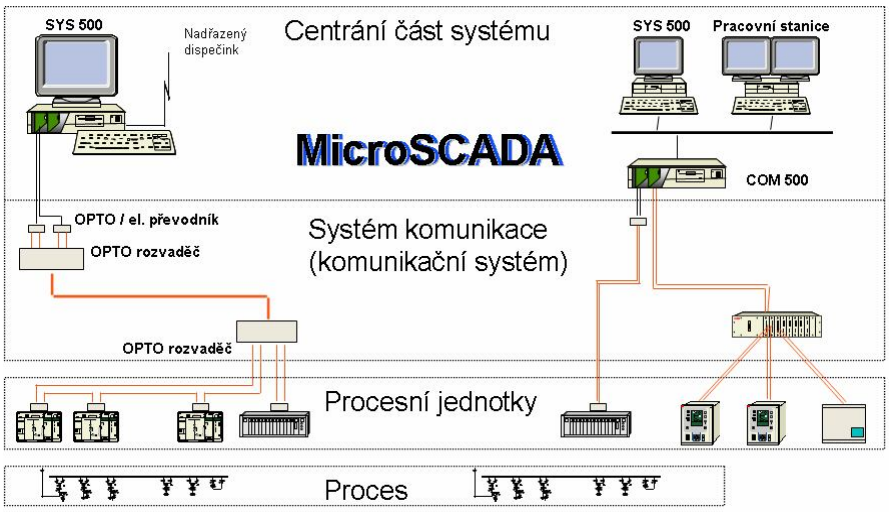
Universal Control Network (UCN) je vysokorychlostní a poměrně funkčně spolehlivá procesní síť. K UCN je možné připojit řadu zařízení pro přímé řízení procesů jako např. Advanced Process Manager (APM), High-Performance Process Manager / History Process Modul (HPM) pro systém TDC 3000 a Controler C300 pro systém Experion, Logic Manager (LM) nebo libovolnou kombinaci těchto zařízení. [12]

K základním součástem těchto zařízení patří I/O Modul a Process Modul. I/O Modul poskytuje širokou paletu vstupně-výstupních (I/O) funkcí jak pro vlastní ovládání pohonů, tak pro monitorování dat. Process Modul obstarává řídící funkce včetně regulačních, logických, sekvenčních, binárních.[13]

3.7 Řídící systém MicroSCADA

Automatický systém řízení MicroSCADA (schéma uvedeno na obr. 13) je produkt společnosti ABB, která slouží k automatizaci rozvoden VN a VVN a systému řízení energetických sítí. Celý systém byl navrhován s cílem, aby bylo možné provádět integraci mnoha různých automatizačních podsystémů a rozdělit tyto subsystémy do několika aplikačních oblastí pro systémy řízení sítí (Network Control System), systémy pro řízení a měření spotřeby (Metering and Load management System), systémy automatizací rozvoden

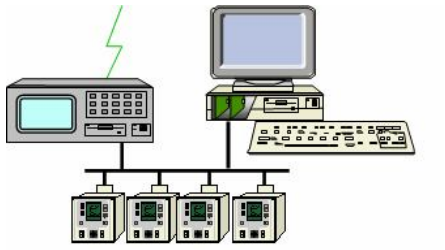
(Station Automation System), informační systémy (Information System), systémy pro komunikaci (Communication Systems). [14]



Obr. 13 Schéma systému MicroSCADA

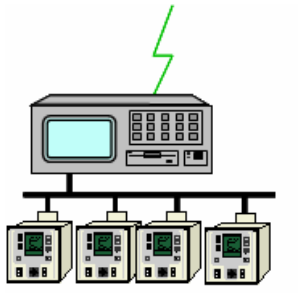
Systém MicroSCADA pracuje ve třech základních variantách:

- Oddělené základní systémy SYS a komunikační systémy COM 500, kde se předpokládá nezávislé řízení rozvodny ze dvou míst (Obr. 14)



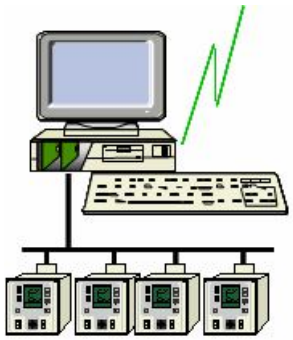
Obr. 14 Oddělené základní systémy a komunikační systémy

- Samostatně pracující stanice COM 500, kde se předpokládá, že rozvodna pracuje bez místního MMI a využívá se pouze funkcí COM 500. Tato varianta je vhodná pro bezobslužné rozvodny (Obr. 15)



Obr. 15 Samostatně pracující stanice

- Stanice kombinující systémy SYS a COM 500, kde jsou oba systémy instalovány v jednom PC, k aplikaci nám postačí pouze jedno hardwarové zařízení (PC), avšak je vhodný pouze pro malé systémy řízení (Obr. 16)



Obr. 16 Kombinované systémy

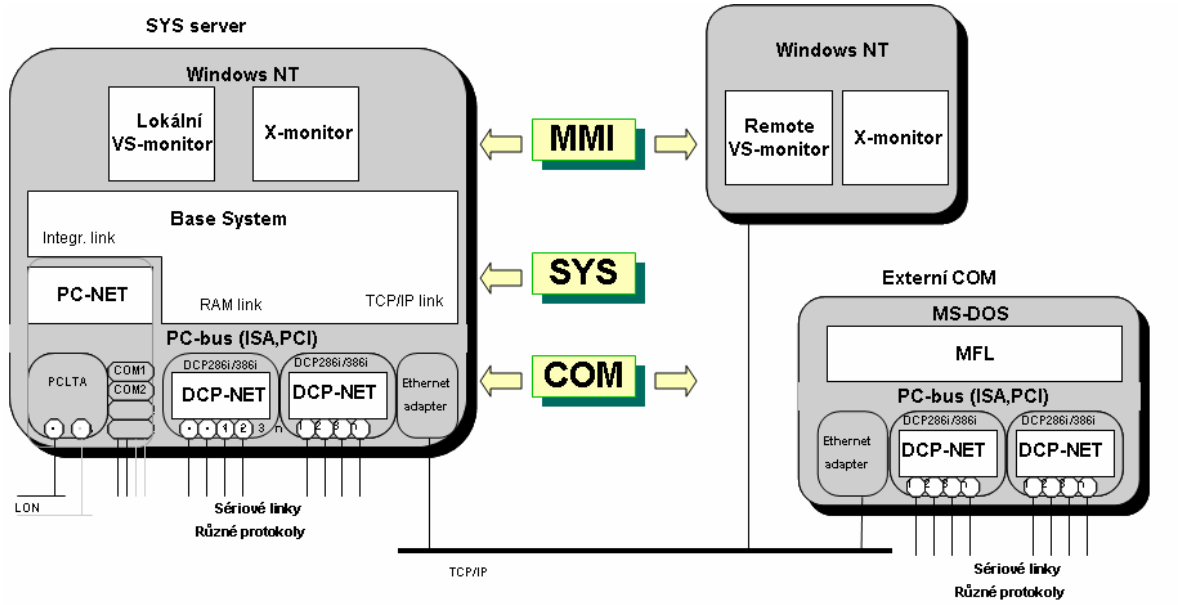
3.7.1 Základní systém

Veškeré kontrolní a ovládací funkce jsou implementovány v základních systémech ASŘ MicroSCADA. Jeden a více základních systémů vytváří řídící středisko systému řízení. Funkční členění systému tvoří tři podskupiny:

- Základní systém, který se skládá s jádra systému SYS 500 a jeho programovacích nástrojů, s knihoven LIB 500 a nástrojů SMS 500, CAP 500
- Komunikace, která se sestává z ovladačů a komunikací na NCC (National Control Centrum) přes komunikační rozhraní COM 500.
- Rozhraní pro komunikaci s obsluhou HMI, postavená na základě pracovní stanice MMC 500 a aplikací na bázi HMI

3.7.2 Komunikační systém

Základním článkem komunikace každého řídícího systému je komunikace mezi základním systémem a procesními jednotkami (Obr. 17). Tuto funkci zajišťují jednotky PC-NET a DCP-NET. PC-NET je software ovládající COM porty počítače nebo maximálně 2 karty Echelon PCLTA, z nichž každá obsahuje 2 LON kanály. PC-NET musí vždy běžet na počítači základního systému. DCP-NET je ovladač určený pro karty Emulex DCP. Každá z těchto karet má 8 sériových komunikačních portů. Karty DCP mohou být instalovány v počítači základního systému (maximálně však 2 karty) nebo v počítačích samotných frontendů (max. 4 výstupní jednotky v jednom frontendu).



Obr. 17 Schéma komunikačního systému MicroSCADA

PC-NET a DCP-NET zajišťují pomocí různých protokolů komunikaci s procesními jednotkami nebo jinými řídícími systémy. Právě pomocí PC-NETu a DCP-NETu je možná implementace přístupového systému do systému ASŘ MicroSCADA. MicroSCADA podporuje jak Modbus Master, tak Modbus Slave, avšak funkce Master je pro ni přirozenější. Pro aplikaci v Modbus Slave se musí místo PC-NET použít externí aplikace CPI, protože interní komunikační část PC-NET jej nepodporuje. Nová MicroSCADA 9.2 obsahuje kompletně nové grafické rozhraní s podporou nového protokolu IEC61850. Definice protokolu se provádí na úrovni linkové vrstvy modelu ISO OSI. Na tuto linkovou vrstvu jsou napojeny všechny komunikační stanice. [14]

3.7.3 Komunikace mezi uzly sytému

Komunikace mezi uzly systému se zpravidla realizuje pomocí lokální Ethernet sítě LAN. V případě systému MicroSCADA se standardně používá TCP/IP síť s hvězdicovou strukturou. Přenosová media jsou rozdělena dle vzdálenosti uzlů. Používá se kroucen8 dvoulinka nebo skleněné optické vlákno. V případě extremních vzdálenosti uzlů je pro komunikaci možné využít sériových výstupů DCP-NET a komutovaných sériových linek s integrovanými modemy.

II. PRAKTICKÁ ČÁST

4 DEFINOVÁNÍ ÚKOLŮ, VYTÝČENÍ REALIZACE A VÝHODY INTEGRACE SYSTÉMŮ

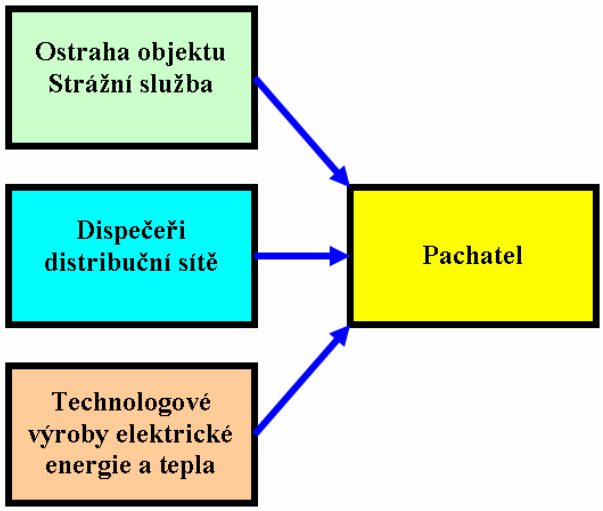
Pro vypracování praktické části je nutné vytýčit si úkoly pro realizaci projektu a objasnit si konkrétní cíle, ke kterým je třeba dospět a zvolit vhodné průsečíky spojení prvků bezpečnostních systémů s prvky automatického systému řízení technologického procesu výroby a distribuce elektrické energie. Celý projekt je postaven na čtyřech základních bodech kompletního propojení všech systémů a to:

- Detekce a monitoring pohybu nepovolané osoby v rozvodnách vysokého a nízkého napětí
- Detekce a monitoring pohybu nepovolané osoby v prostorách technologické výroby elektrické energie a tepla
- Zvýšení účinnosti zásad bezpečnosti práce na energetických zařízeních
- Monitoring pracovní činnosti pro vedoucí pracovníky pomocí docházkového systému PASSPORT, který je součástí celkového přístupového a docházkového systému ACCESS.

4.1 Koordinace dispečerů a pracovníků BS a obsluhy technologických procesů při krizové události po integraci systémů

Modelový vzor (Obr. 18) představuje požadovanou koordinaci dispečerů, obsluhy a pracovníků ostrahy při napadení energetických zařízení, vzdálených rozvoden a distribuční sítě. Vybrané vzdálené energetické objekty jsou napojeny na I&HAS systémy se signalizací na pulty centrální ochrany PCO, které monitoruje najmutá bezpečnostní agentura. Z pohledu ostrahy objektů a zařízení je vše v pořádku, ale často při napadení energetických zařízení dochází jak k úmyslnému, tak neúmyslnému vypnutí určitého prvku distribučního vybavení nebo technologického zařízení. Avšak informace, že k odstavení došlo z důvodu napadení objektu fyzickou osobou, obsluze a dispečerům zcela chybí. Dochází tak často ke zbytečnému havarijnímu vypnutí celých linek a odstavení zařízení, protože obsluha neměla informaci o tom, proč k této události došlo. V případě, že jsou dispečeři připraveni na to, že se ve vzdáleném energetickém objektu pohybuje nepovolaná osoba, tak je obsluha

energetických zařízení včas připravena na možnou mimořádnou událost a na možný výpadek sítě.



Obr. 18 Koordinace BS, dispečerů a technologů

Velmi často se stává, že ostraha a bezpečnostní služba již delší čas monitoruje pohyb nepovolané osoby, připravuje se na zakročení proti této osobě, ale dispečery výroby nikdo o této události neinformuje. Je pravidlo, že pokud dojde k nespecifikované havárii, je nutné odstavit celé zařízení a hledat příčiny výpadku. Jestliže obsluha zná příčiny odstavení zařízení a dokonce již zná skutečnost, že k něčemu takovému může dojít, nemusí tak docházet ke zbytečným výpadkům energetických dodávek a finančním ztrátám způsobených přerušením výroby. Integrace bezpečnostních systémů s prvky ASŘ snižuje tato rizika na minimum.

4.2 Nové využití docházkového systému po integraci systémů

Zjednodušený model (obr.19) představuje požadovaný stav koordinace vedoucích pracovníků, řídících techniků a obsluhy zařízení po implementaci přístupových a docházkových systémů do řídících energetických systémů. Přestože se vzájemná komunikace postupně zlepšuje po zavedení osobních vysílaček a mobilních telefonů pro operativní pracovníky, tak není stav spolupráce mezi zainteresovanými stranami zcela ideální a to z důvodu, že osobní vysílačky jsou plně funkční v některých objektech nebo prostředí pouze do určité vzdálenosti mezi vysílačem a přijímačem. Stavby elektráren a tepláren jsou kombinací železa a betonu, proto některé části těchto objektů spíše působí jako dobře odrušené prostory rádiových vln. Jestliže k tomuto přidáme také atribut

vysokého a velmi vysokého napětí, tak je zcela nezpochybnitelné, že osobní vysílače nejsou vždy plně funkční.

Obr. 19 Koordinace vedoucích pracovníků s BS

Docházkový systém, který je součástí přístupového systému, může tyto nedostatky plně nahradit, pokud je vhodně integrován do řídících systémů energetických zařízení. Vedoucí pracovník zná pohyb zaměstnance v dané chvíli a může jej kdykoliv převést na jinou práci nebo dokonce odvolat, jestliže se blíží krizová situace nebo nebezpečí.

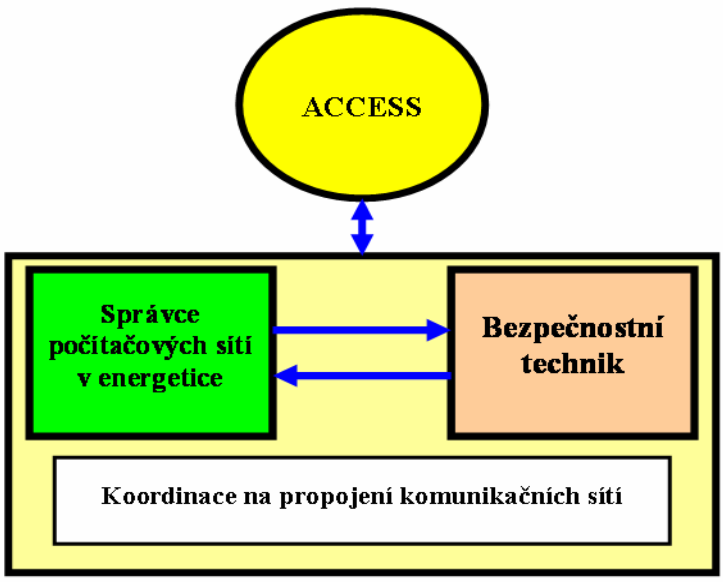
Rád bych připomenul, že hranice mezi porušením etických pravidel při monitoringu osob na pracovišti má své meze a pravidla, ale pokud je monitoring provozován z důvodů bezpečnosti práce, zlepšení koordinace při řešených úkolech a zvýšení produktivity práce, je možno takové opatření pochopit. Docházkový systém je dnes již často využíván pro snižování administrativy při vypisování výkazů práce pro jednotlivého pracovníka s tím, kde v danou chvíli pracoval a co v danou chvíli dělal. Integrace docházkového systému do systémů řízení ASŘ dovoluje dispečerovi sledovat pohyb pracovníka v prostorách nebezpečných a snižuje při případných manipulacích možnost chybných rozhodnutí a opomenutí, že na zařízení ještě někdo pracuje. Chyby a selhání lidského faktoru jsou nejčastější příčinou těžkých pracovních úrazů v energetice. Implementace informací z docházkových a přístupových systému do ASŘ, které jsou přímo naprogramovány v blokovacích podmínkách automatických systémů tyto faktory snižuje téměř na minimum. Zjednodušeně řečeno, pracuje-li montér v kobce vysokého napětí, je díky blokovacím podmínkám vyloučeno, že chybnou manipulací bude tento pracovník zraněn zpětným proudem na straně vysokého napětí, který se může objevit například chybnou manipulací na nízkonapěťovém zařízení transformovaném na vysoké napětí přes sekundární a následně primární vinutí transformátoru.

Propojením a implementací přístupového a především docházkového systému do bezpečnostních databází distribučních řídících systémů se o pohybu elektromontérů dozvídá nejen vedoucí pracovník, ale také dispečer, který je zodpovědný za provádění manipulací na distribučních sítí. Každý montér, který pracuje na zařízení, vyplňuje tzv.

příkaz „B“ pro práci na vysokém napětí a velmi vysokém napětí a bezpečnostní instruktážní příkaz „BIP“ pro práci na zařízeních nízkého napětí. Často se tedy stává, že pracovník po dokončení prací příkaz okamžitě neodepíše a tím blokuje zařízení do té doby, než je vyhledán, aby obeznámil dispečera, že svojí práci ukončil. Také častou situací se stává, že dispečer má provádět manipulace a zdlouhavě se snaží zjistit, zda na zařízení nikdo nepracuje. Nejčastější těžké úrazy se stávají, když je dispečer mylně přesvědčen, že zařízení je v beznapěťovém stavu a po jeho manipulacích dojde k těžkému zranění pracovníka, který na zařízení ještě pracoval a to pouze z toho důvodu, že přehlédl vyplněný bezpečnostní příkaz „B“. K těmto těžkým úrazům by nemuselo docházet, kdyby byl dispečer upozorněn, že pracovník prošel přes přístupový systém do rozvodny a ještě tuto rozvodnu neopustil. ASŘ by tak chybnou manipulaci nepovolil.

4.3 Požadovaná kooperace techniků na propojení systémů

Správci počítačových sítí neradi vidí, když se pracovníci externích firem snaží cokoliv implementovat do technologických datových sítí. To je docela pochopitelné, protože technologické automatické systémy řízení zpravidla v sobě nezahrnují žádný antivirový program, a to z důvodu možného zpomalování přenosu informací mezi systémy technologických procesů při kontrole, které provádí právě antivirové programy. Je tedy nezbytné dbát na datové bezpečnosti při propojení technologických, datových sítí a sítí, které nesou informace a databáze z bezpečnostních systémů.

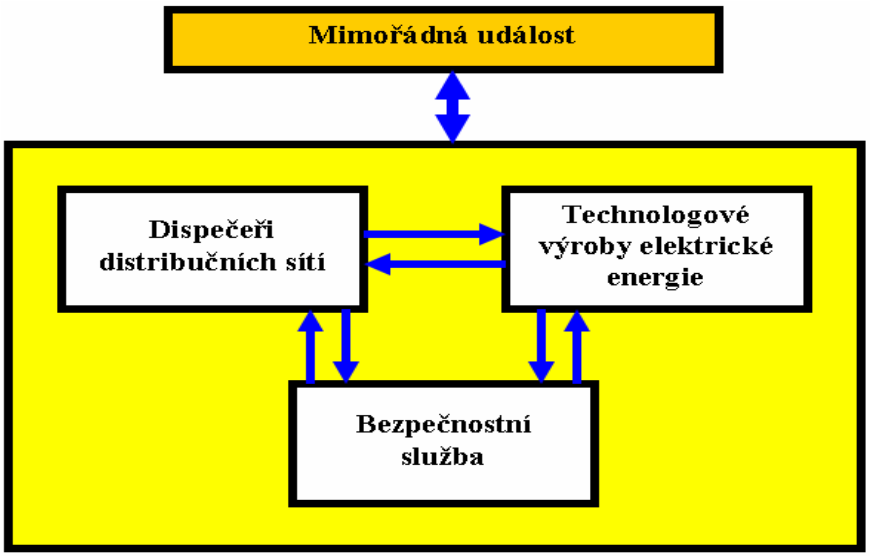


Obr. 20 Koordinace na propojení komunikačních sítí

Koordinace správců stávajících počítačových nebo také technologických počítačových sítí, které se zabývají realizací bezpečnostních systémů (ACCESS, PASSPORT, I&HAS, EPS apod.) je nezbytná, protože narušení komunikace mezi zařízeními technologických procesů nebo dokonce jejich selhání může zapříčinit obrovské materiální škody. Je mnoho způsobů, jak integrovat bezpečnostní systémy do ASŘ a přitom neporušit základní pravidla datové bezpečnosti. Ve kapitole 5. je popsán návrh na integraci přístupových systémů a ASŘ.

4.4 Požadovaná koordinace dispečerů a pracovníků BS při úrazu pracovníka

Při bližším prozkoumání spolupráce pracovníků bezpečnostních služeb a dispečerů při úrazu jsem došel k závěru, že při možném úrazu pracovníka je celková koordinace závislá pouze na pevné telefonní přípojce, která spojuje velín elektrárny popř. teplárny s ostrahou na vrátnici. Jestliže vezmeme v úvahu, že střediska objektu jsou od sebe často velmi vzdálena, tak je přímo nutností zvýšit kvalitu koordinovanosti při krizové situaci. Někdy o životě rozhodují sekundy a jakékoliv zdržení při poskytnutí první pomoci může mít za následek zbytečnou smrt pracovníka z důvodu, že lékař rychlé zdravotní služby nebyl na místě úrazu včas, protože jeho rychlý zásah skončil před branami energetického objektu, jelikož ostraha nebyla informována o neštěstí a nevpustila lékaře do objektu.



Obr. 21 Koordinace dispečerů a bezpečnostních služeb při úrazu

Podle vnitropodnikových směrnic nesmí ostraha nikomu svévolně dovolit vstup do závodu. Prodlení také vzniká časovým posunutím telefonického spojení mezi vedoucím směny

a navedením pomoci na místo úrazu. Jestliže by fungoval spolehlivě přenos informací z přístupových a docházkových systémů do řídících systémů, tak by každá ze zainteresovaných stran měla na monitoru výpis, kde a kdy se něco stalo a komu se to stalo (obr. 21). Stačilo by pouze spojit databáze z přístupových a docházkových systémů se systémy ASŘ, které používá obsluha pro vlastní činnost a při případné mimořádné události ji pomocí klávesnice nebo myši aktivovat. Každá ze zainteresovaných stran by měla okamžitý přehled, kdo se nachází v inkriminovaném místě a na jakém zařízení a úkolu pracoval. Podle daných směrnic by už každý pracovník, ať už ostrahy nebo obsluhy věděl, jak se má při dané krizové událost zachovat.

4.5 Detekce a monitoring pohybu nepovolané osoby v rozvodnách po integraci systémů

Každá zainteresovaná skupina může pomocí propojení všech prvků objektové bezpečnosti při napadení objektu odvrátit bezpečnostní riziko na minimum a sledovat své úkoly při tomto nestandardním stavu. Rozdělení je navrženo do tří skupin, a to podle pracovního zaměření každé zainteresované skupiny:

Dispečink distribuce elektrické energie - ASŘ MicroSCADA

- Možnost sledování narušitele pomocí CCTV
- Monitoring počínaní pachatele v kobkách VVN a VN
- Monitoring počínaní pachatele v rozvodnách NN
- Sledování jeho činnosti v prostorách nebezpečných

Obsluha procesů výroby elektrické energie – ASŘ Honeywell

- Upozornění obsluhy na možnost odstavení zařízení
- Časová schopnost okamžité reakce na událost popřípadě sabotáž

Bezpečnostní služba – I&HAS, PCO, CCTV a ACCESS

- Okamžitý zákrok pracovníků bezpečnostní služby
- Monitoring pohybu dle CCTV
- Spolupráce s obsluhou technologických zařízení a dispečery energetických sítí

4.6 Zvýšení účinnosti v prevenci bezpečnosti práce na zařízení

Vzhledem k častým manipulacím na energetických zařízeních je požadováno přísnější dodržování pravidel bezpečnosti práce. S příchodem německého kapitálu a změnou vlastníků bývalé JME Energetika na současné E-ON Energo a.s Česká republika se přejímají německé standardy pravidel bezpečnosti práce. Integrace BT v zařízeních ASŘ umožňuje zlepšit tyto procesy:

Dispečink distribuce elektrické energie – ASŘ MicroSCADA

- Zvýšení bezpečnosti práce na zařízeních VVN, VN a NN tak, že se monitorují a následně zasílají informace o pohybu pracovníka obsluze na energetických zařízeních
- Doplnění údajů o pohybu pracovníka do blokovacích algoritmů ASŘ se technologicky minimalizuje chyba dispečera při manipulacích na energetických zařízeních.
- Již stávající datové sítě a technologické vybavení kobek VVN a VN, popřípadě rozvaděčů NN pro přenos informací mezi systémy ACCESS, MicroSCADA, Honeywell musí být datově propojeny v jeden celek s nejvyššími požadavky na datovou bezpečnost.

Obsluha procesů výroby elektrické energie – ASŘ Honeywell

- Obsluha technologických zařízení pro výrobu energie pomocí propojení databáze přístupového systému ACCESS a ASŘ Honeywell má přehled o pohybu pracovníků v technologických úsecích výroby elektrické energie a tepla. Obsluze je tím umožněno předvídání budoucí situace při chybných manipulacích.

Bezpečnostní služba – I&HAS, PCO, EPS, CCTV a ACCESS

- Pracovník BS při případném úrazu zná totožnost zraněné osoby a místo úrazu. Tím může okamžitě a přesně nasměrovat na místo úrazu zdravotnickou záchrannou službu, PČR a Hasičský záchranný sbor.

4.7 Monitoring pracovní činnosti za využití docházkového systému PASSPORT

V energetice je běžné, že jsou technologické budovy rozděleny dle prostředí a jednotlivá prostředí jsou rozdílně nebezpečné pro výkon pracovníka. Pomocí docházkového systému by odpadlo nepříjemné papírování při vypisování časového úseku, kdy pracovník pracoval v objektu, který podléhá zvláštním příplatkům a bezpečnostním podmínkám za prostředí. Vše by přímo bylo zaznamenáno do docházkového systému a odpadlo by zdržující ruční vypisování do těchto systémů.

- Okamžité uložení dat a on-line monitoring pracovníka v ztíženém prostředí.
- Možnost monitoringu pracovníka z důvodu odvolání z pracoviště nebo naopak z důvodu dalšího úkolování.
- Snadnější vedení agendy pro odměňování pracovníků za práci.

5 TECHNICKÉ ŘEŠENÍ INTEGRACE BT S ASŘ V ENERGETICE

Při návrhu na propojení přístupového a řídícího systému je nutné dodržovat několik zásad z hlediska bezpečnosti dat a bezpečného propojení sítí. Technologické systémy jsou velmi důležité pro bezchybný provoz zařízení, a proto nesmí dojít k jejich poškození, zavirování nebo odstavení. Návrh bezpečné realizace je shrnut do několika bodů:

- Definování binárních vstupů/výstupů a přivedením těchto signálu do příslušných PLC (Programable logic controler) systémů řízení, jejich zpracování a odeslání do příslušných systémů
- Samostatně pracující zařízení (ústředny I&HAS, CCTV, ACCESS), ze kterých jsou data přenášena k dalšímu zpracování, kde jsou zálohovány, archivovány nebo případně využity k on-line monitoringu ASŘ a posléze využity pro zpřístupnění do jiných systémů automatického řízení procesů z důvodu vyžádání žádosti událostí pověřeného pracovníka.
- Datově softwarové propojení mezi systémy řízení využívající stávající sítě za příslušných podmínek požadavků na datovou bezpečnost a bezpečnost sítí.
- Práce s daty je povoleno pouze osobě s administrátorskými pravomocemi.
- Práce s externími hardwarovými médii (CD/DVD jednotky, USB nebo sériové porty) je povoleno pouze osobám s administrátorskými právy.
- Zajistit dokonalou ochranu systémových a uživatelských PC s antivirovými programy.
- Pro přenos poplachových a přístupových dat je doporučeno vyhnout se protokolu TCP/IP v rámci rozdílných sítí, pokud nejsou dostatečně filtrována procházející data. Tento protokol je nejlépe převádět na sériovou linku pomocí převodníku TCP/IP – Modbus a posléze data zpracovávat pomocí PLC (Programmable logic controller), který je pracuje na bázi OS UNIX a je naprogramován pouze příkazy využívající databázi pouze žádaných vstupů a výstupů patřičných operací. Tímto dosáhneme poměrně vysoké datové bezpečnosti. S hlediska datové bezpečnosti vycházejí systémy Honeywell TDC 3000 nejlépe, protože mezi externími a interními zařízeními komunikují prostřednictvím sériového rozhraní. Nové systémy EXPERION jsou již postaveny na komunikaci prostřednictvím rozhraní ethernet,

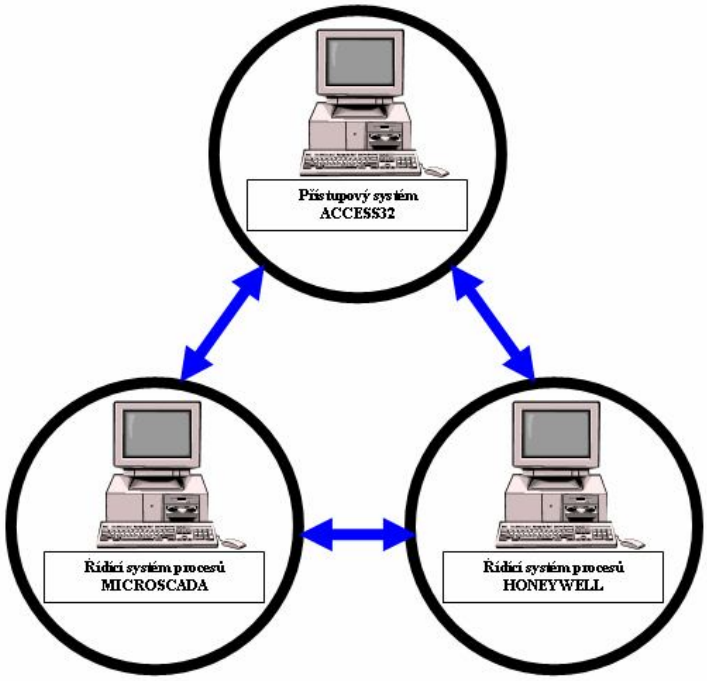
které je levnější a rozšířenější než-li sériová komunikace, avšak více rizikovější z hlediska datové bezpečnosti. Řízení a kontrola toku dat je u sériové linky jednodušeji proveditelná a kontrolovatelná. Každý z komunikačních rozhraní má své výhody a nevýhody.

- Využívat routery, které obsahují zdrojové kódy (nejčastěji jsou psané v C, C++), a sledovat, aby firmware těchto routerů byl založen na nějaké Linuxové distribuci (jádru)
- Máme-li funkční software a hardware a navíc zdrojový kód na bázi Linuxové distribuce, můžeme tímto vytvořit nestandardní, nedokumentovatelnou verzi. Pro třetí stranu (myšleno hacker, záškodník) se tímto síť stává nečitelnou a nemůže dojít k jejímu napadnutí zvenku.
- Router musí propouštět jen záměrně upravené, modifikované pakety TCP/IP protokolu vložením nějakého klíče, nejlépe využitím určité sekvence znaku.
- Aby bylo možné tuto sekvenci měnit (z jakékoliv potřeby, například změna odpovědného pracovníka) bude se její tvar, hodnota načítat s USB klíčenky vložené do USB portu routeru.
- Všechny poplachové signály automaticky přivádět na pulty centrální ochrany:
    - Přes ústředny I&HAS do PCO
    - Přes systém ACCESS32 do I&HAS a následně do PCO
- Definování systému ACCESS32, které je nutné provést před a v rámci běhu systému:
    - Vytvoření komunikační topologie
    - Adresování fyzického zapojení snímačů místa přístupu a vytvoření přístupové databáze do systému ACCESS32
    - Vytvoření logického schématu pro přiřazování přístupových práv
    - Vytvoření zóny pro vyhodnocení přítomnosti a definování funkce antipassback

- Nadefinování speciální, popřípadě časové vlastnosti snímačů místa přístupu
- Definování logických skupin snímačů místa přístupu a jejich vlastností
- Vytvoření požadované databáze pro vstup a kontrolu osob

5.1 Integrace přístupového systému ACCESS se systémy MicroSCADA a Honeywell

Blokové schéma (Obr. 22) zobrazuje návrh vzájemného propojení tří nezávislých řídících lokálních systému v jeden multifunkční celek. Návrh spočívá v propojení přístupového systému s ústřednou I&HAS a realizaci samostatně pracujícího CCTV systému, který je možno zahrnout do dvou samostatných jednotek, které budou mezi sebou softwarově propojeny a budou si předávat jen ty části snímaného obrazu, kterého plně využije ostraha pro ochranu technologických procesů a také obsluha a dispečeři zařízení.



Obr. 22 Požadované vzájemné propojení systémů

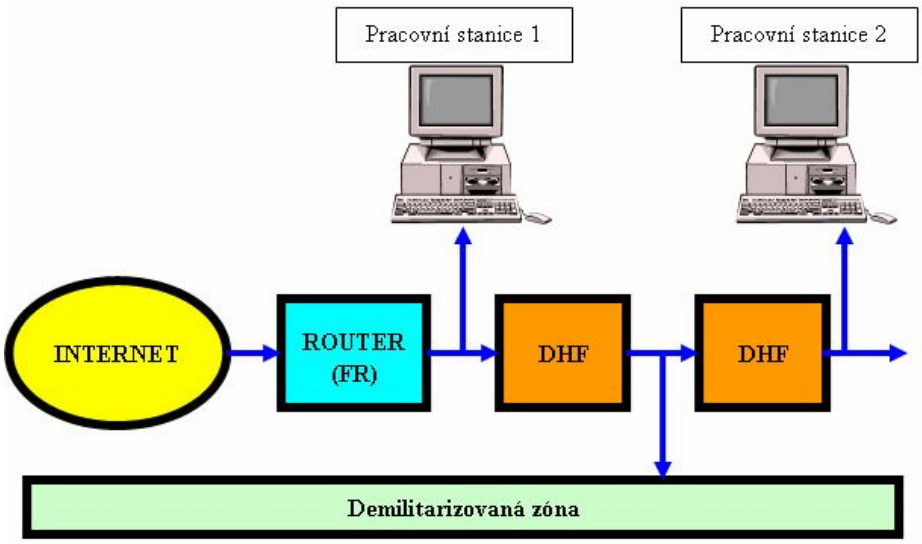
Každý z těchto systémů používá vlastní lokální síť. Systém kontroly vstupu ACCESS využívá vlastní lokální sítě, která je určená pro komunikaci po ethernetu sadou protokolů TCP/IP. Ústředna I&HAS, která komunikuje pouze s přístupovým systémem ACCESS nejčastěji přes interface ETHERNET/COM na switch vnitřní sítě.

Nejvíce rozšířená komunikace je fyzické propojení přes ethernet, který je společný pro přístupový systém ACCESS, a také pro ústřednu I&HAS. Automatický systém řízení Honeywell, který byl vyvinut pro řízení výrobních energetických procesů, komunikuje prostřednictvím LCN (Local Control Network) a UCN (Universal Control Network) se svými periferiemi HPM, které využívají vlastní komunikační protokol. Automatický systém řízení MicroSCADA, který v energetice slouží pro řízení distribuce elektrické energie, komunikuje po vlastní lokální síti s vlastním komunikačním protokolem. Pro zvýšení funkčnosti celého systému se také zabývám návrhem uzavřeného dohledového kamerového systému, který však bude pracovat zcela samostatně, jelikož připojení kamerových systémů do technologických zobrazení na monitorech určených k řízení procesů MicroSCADA a Honeywell není vhodné. Zcela postačí, když celý systém CCTV bude pokryt dvěma monitory, z nichž jeden bude sloužit dispečerské obsluze a druhý ostraze objektu umístěné na vrátnici Teplárny Otrokovice a.s.

Na rozdíl od původní dokumentace, kterou dodává výrobce doplňuji zařízení síťové topologie o směrovač a další přepínač Cisco Catalyst 1900. Router obsahuje implementovaný překladač adres (NAT), který je nutný pro širší komunikaci do veřejných počítačových sítí WAN nebo do systému ASŘ Honeywell EXPERION. Přepínač Cisco Catalyst 1900 je přidán ze dvou důvodů. Prvním důvodem je možnost nainstalování komunikačního klienta systému ACCESS32 do kruhové síťové topologie a druhým důvodem je přítomnost aplikační brány (proxy serveru), která umožňuje řízení vzájemné datově bezpečné komunikace mezi počítačovými sítěmi.

Základem technického řešení integrace bezpečnostních technologií a ASŘ je dokonalé zmapování možností komunikace mezi zařízeními a dokonalé zpracování bezpečnostní politiky. Přístupový Firewall je jedním z prvků této bezpečnostní politiky. Prosazení bezpečnosti k přístupu do vnějších nezabezpečených sítí pomocí plně funkčního Firewalu, který při správné činnosti je jediným přístupovým bodem do zabezpečené sítě je základem celého návrhu integrace. Dalším prvkem dokonalé bezpečnostní politiky je zajištění, že v chráněné síti není možné jednoduše vytvořit další pevné spojení sítě s internetem. K tomuto účelu slouží kvalitně zpracovaná komplexní bezpečností politika celé organizace v oblasti datové bezpečnosti. Pokud nedokonale zpracovaná politika umožní připojování cizích počítačů do lokální sítě, tak je vysoká pravděpodobnost nekontrolovaného útoku z vnějších i z vnitřních počítačových sítí.

Pro řešení a implementaci bezpečnostní politiky integrace systémů je důležité mít na zřeteli zapojení Firewallů. Z hlediska konfigurování softwaru je zabezpečení sítě mezi dvěma firewally DHF (dual-homed firewal), které vytváří mezi vnější a lokální sítí tzv. demilitarizovanou zónu (DMZ) pro návrh integrace systémů nejvhodnější. Uvnitř této zóny jsou umístěné prvky technologických procesů a z vnějším okolím komunikují pouze za přísných datově bezpečnostních podmínek.

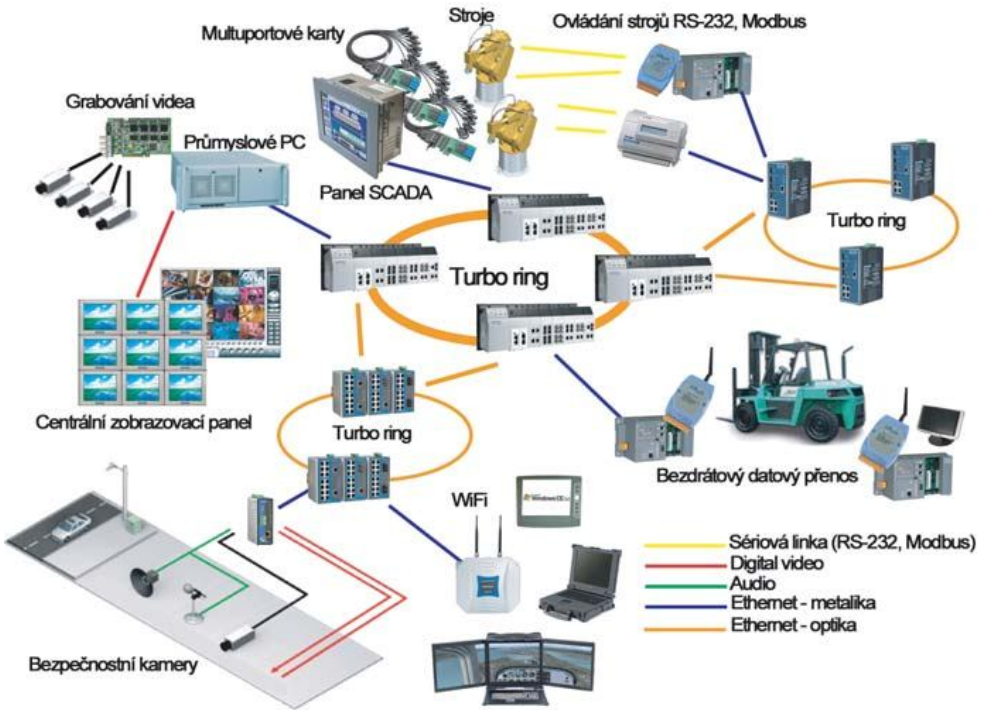


Obr. 23 Vytvoření DMZ pomocí dvou firewallů

Vhodné je vytvořit demilitarizovanou zónu pro komunikační server přístupového systému, který přenáší data mezi vzájemně propojenými systémy. Schéma je znázorněno na obr. 23. Před přímým napadením z vnější sítě je DMZ chráněna pomocí Firewalu č.1 a napadení demilitarizované zóny z lokální sítě je bráněno pomocí Firewalu č.2. Nevýhodou tohoto řešení je cenová náročnost, menší rychlost přenosu dat mezi vnější a lokální sítí a pomalejší přístup k DMZ serverům z lokální sítě. Pro realizaci integrace přístupových a systémů řízení je nutné vytvořit nejméně dvě demilitarizované zóny, jednu pro systém Honeywell a druhou pro systém MicroSCADA. Především je nutné dbát na datovou bezpečnost počítačů, které používají ke své běžné práci klienti, a které jsou jakýmkoliv způsobem propojeny se sítí přístupového systému ACCESS32. Především se jedná o PC, kde běží monitorující software a software docházkového systému PASSPORT, který je také součástí systému ACCESS. [15]

5.2 Využití podnikové počítačové sítě a přenos videa a audia na Ethernetu

Automatické řídící systémy jsou zařízení, na kterých je vyžadována velmi rychlá odezva technologických událostí, proto není jakékoliv přetěžování těchto sítí doporučeno. Pro bezpečnostní techniky to znamená vyhnout se těmto sítím pro přenos video a audio signálu. Jsou tedy dvě možnosti, jak tento problém vyřešit. Vybudovat vlastní přenosovou síť pro přenos audio a video signálu nebo maximálně využít již stávající datovou síť v podniku, avšak nikoliv technologické datové sítě. Využitím již stávající komerční datové sítě můžeme značně snížit finanční a výrobní náklady. Ve většině případů je centrální větev podnikové sítě tvořena optickým kabelem a tento optický rozvod je opatřen několika záložními větvemi.



Obr. 24 Využití podnikové sítě pro přenos videosignálu

Zajímavým řešením je zapojení průmyslových modulárních přepínačů do kruhové topologie, které je možno propojit dalšími přepínači v zapojení s dalšími kruhovými větvemi (Obr. 24).

Přes tyto sítě můžeme následně přenášet snímaný signál z bezpečnostních kamer, který byl před přenosem digitalizován pomocí videopřepínačů. Na trhu existuje velké množství těchto video přepínačů a je jen na nás jaký typ přístroje si vybereme. [16]

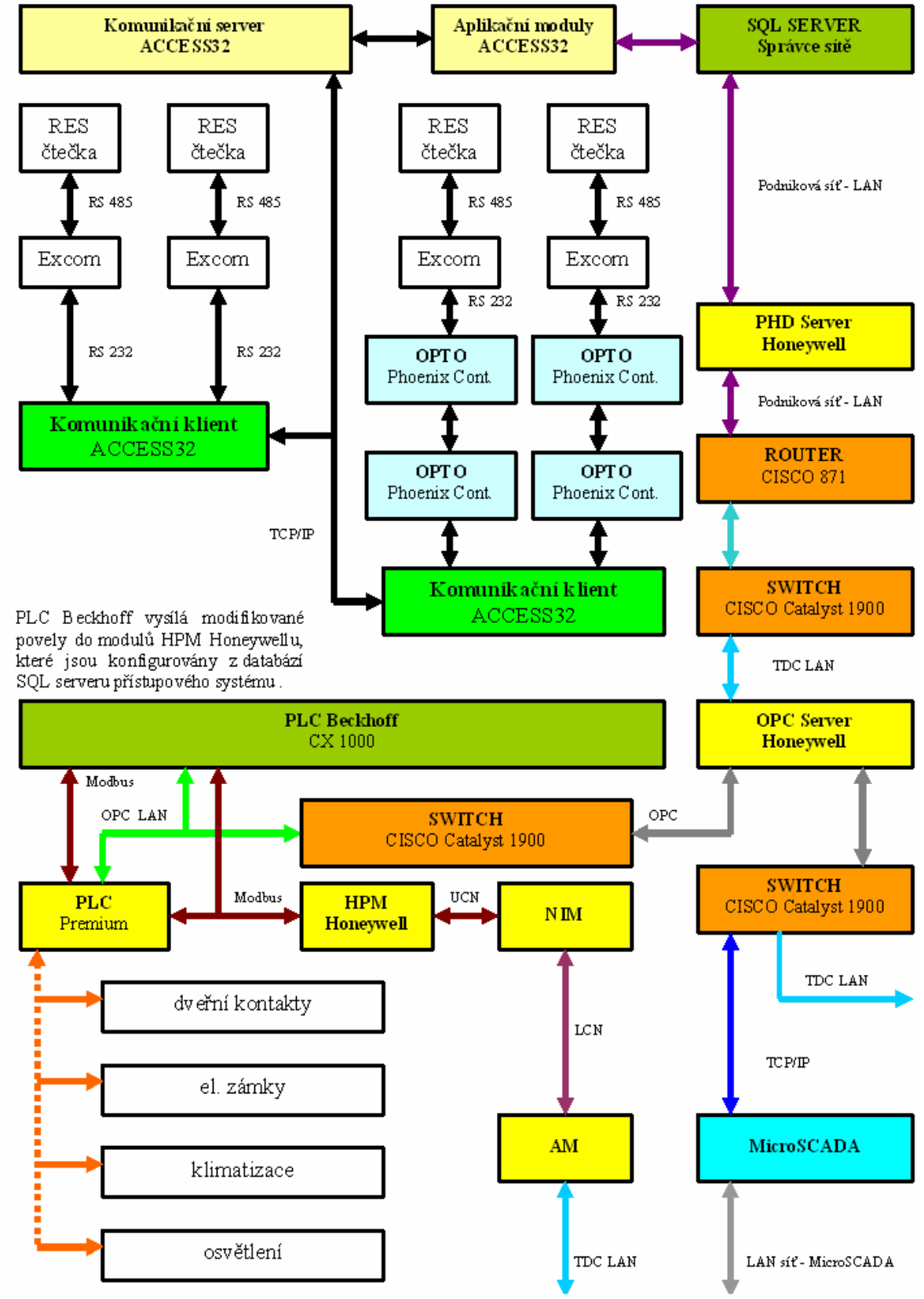
5.3 Návrh síťového propojení systémů MicroSCADA, ACCESS32 a Honeywell

Systém ASŘ Honeywell je v návrhu zvolený za koordinační systém, který komunikuje z jedné strany s přístupovým systémem ACCESS a z druhé strany se systémem MicroSCADA. Systém Honeywell vyhodnocuje, ukládá a používá k procesům data, které přijal z přístupového systému a pracuje také jako zprostředkovatel pro přenos databází mezi systémy ACCESS a MicroSCADA. Řešení s ASŘ Honeywell uprostřed bylo zvoleno z důvodu univerzálnosti tohoto systému pro všechny možné technologie procesy řízení. Koordinací ASŘ Honeywell s přístupovými systémy vzniká možnost vytvoření dokonalého a rozsáhlého systému, popřípadě otevřený webový nástroj pro integrovaná řešení umožňující centrální dálkovou správu a dohled.

Návrh realizace na implementaci přístupového systému do systémů ASŘ je zobrazen na obrázku 25. Základním prvkem návrhu je komunikační server systému ACCESS32, který sbírá data s komunikačních klientů přístupového systému. Komunikační klienti ovládají komunikační jednotky s převodníky EXCOM, do který je možné připojit až 4 snímače místa přístupu RES. Tyto komunikační jednotky mohou být vzdáleně konfigurovatelné pomocí komunikačního serveru na kterém běží základní aplikace. Komunikační klient sbírá data ze snímačů místa přístupu RES přes komunikační rozhraní RS 232. Rozhodneme-li se využít řídící jednotky REI-ST, tak značná výhoda spočívá v tom, že obsahuje dvě zásuvky pro ethernet. Tím odpadá další externí switch pro hardwarové propojení komunikačního serveru systému ACCESS32 s komunikačními klienty. PLC Beckhoff bylo zvoleno z důvodu možnosti modulárního rozšiřování základního systému o další komunikační a I/O prvky. Z důvodu velkých vzdáleností mezi zařízeními, odloučenými pracovišti a rozvodnami je v návrhu také počítáno s využitím optických kabelů a optických převodníků.

Komunikační server obsahuje aplikační moduly, což je vlastně softwarové vybavení základní stanice systému INFOS. Tyto aplikace zpracovávají databáze, které je možno pomocí modulu Export/Import přenášet na SQL server správce počítačové sítě. Protože je podnikový SQL server propojen pomocí podnikové sítě s PHD serverem systému Honeywell, který také umí s databázemi pracovat, je možné tyto databáze využít pro požadovaný monitoring a regulace. PHD server systému Honeywell je umístěn na podnikové počítačové síti, tedy na stejné síti, na kterých jsou implementovány klientské

počítačové stanice, bázový SQL server správce sítě a také komunikační server systému ACCESS32. Abychom byli schopní zprostředkovat data kontrolerům PLC, které jsou umístěny ve výrobních prostorech energetických zařízení, je nutné nějakým způsobem tyto povely k těmto programovatelným automatům dodat. PLC Beckhoff a většina programovatelných automatů dnes již umí komunikovat pomocí komunikačního protokolu OPC. Systém Honeywell obsahuje OPC server, který komunikuje se všemi klientskými stanicemi. Tím je okruh vzájemné komunikace uzavřený, protože informace, příkazy a databáze je možné opětně přes PLC Beckhoff implementovat do jednotky komunikačního klienta zpětně přes aplikační moduly přístupového systému. Tyto aplikace zpracovávají databáze, které je možno pomocí modulu Export/Import přenášet na SQL server správce počítačové sítě. Je-li OPC server systému Honeywell zprostředkovatelem výměny databází, tak zařízení HPM pro systém TDC 3000 a zařízení C300 pro Experion Honeywell vykonává požadované procesy a řízení. HPM modul komunikuje mezi svými periferiemi pomocí sériového rozhraní RS 485 a Modbus protokolu. Modul C300 systému EXPERION je jednoduší v tom, že ke komunikaci používá rozhraní Ethernet a komunikuje pomocí sady protokolů TCP/IP. Protože základní operační systém PLC Beckhoff je postaven na operačním systému Windows NT, je možné pro ethernethovskou komunikaci zapojit také firewall a tím filtrovat vzájemnou komunikaci mezi HPM modulem a komunikačním klientem systému ACCESS32. HPM modul komunikuje také nepřímo s SQL serverem správce počítačové sítě přes NIM modul a AM modul. Tím se opět dostaneme z vnitřní TDC LAN sítě systému Honeywell přes stávající switch a router na podnikovou síť LAN, kde je instalováno komunikační rozhraní komunikačního serveru systému ACCESS32. Koncové zařízení PLC Premium komunikuje z PLC Beckhoff a HPM Honeywellu pomocí sériového rozhraní RS 485 a protokolu Modbus. PLC Premium také dokáže zpracovávat přímo běžící aplikace systému Honeywell pomocí komunikace mezi OPC klientem na straně PLC a OPC serverem na straně Honeywellu. V návrhu vykonávají regulace, uzamykání dveří, regulaci osvětlení a klimatizace programovatelné automaty Premium a Beckhoff. Záleží jen na technikovi pro který z těchto automatů se rozhodne, a které I/O výstupní moduly z těchto PLC využije. Celková topologie programovatelných automatů, řídících jednotek systému ACCESS32, HPM a C300 modulů je navržena v kruhové a hvězdicové topologii síťového propojení všech zařízení.

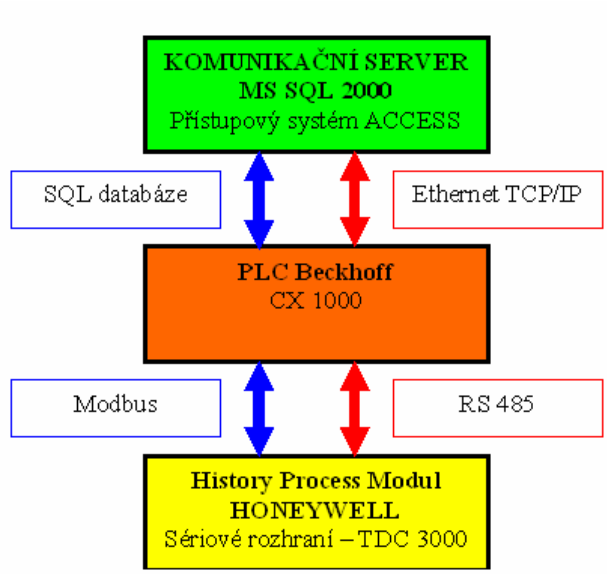


Obr. 25 Návrh integrace přístupového systému ACCESS32 se systémy ASŘ TDC 3000

Tento návrh poskytuje tzv. two-way process, což znamená, že automatické systémy Honeywell a MicroSCADA získávájí databáze z přístupového a docházkového systému a naopak přístupový systém zpracovává data získané z I/O svorek programovatelných automatů. Odpadá tím náročné a poměrně drahé vybudování topologie pro samotný přístupový systém a naopak dochází zde k možnosti začlenění databází z přístupových systémů do řídících procesů v distribuci a výroby elektrické energie.

5.3.1 Návrh na propojení přístupového systému se systémem ASŘ Honeywell TDC 3000 přes sériové rozhraní RS485

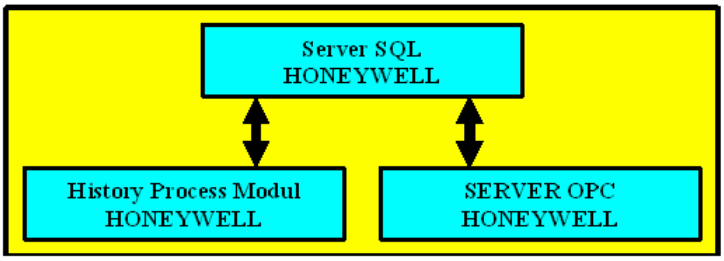
ASŘ Honeywell TDC 3000 je v dnešní době nejrozšířenějším systémem pro zpracování technologických procesů, přestože je již nahrazován novějšími systémy EXPERION pracující na ethernetovském rozhraní využívající protokol TCP/IP. TDC 3000 je postaven na vzájemné komunikaci mezi systémy pomocí sériové linky RS 485 komunikujících protokolem MODBUS.



Obr. 26 Propojení pomocí sériového rozhraní

PLC Beckhoff vysílá modifikované povely do modulu HPM Honeywellu, které jsou konfigurovány z databází SQL serveru přístupového systému. Celý proces komunikace je vysvětlen na obr. 26. Propojení komunikačního serveru MS SQL přístupového systému a TDC 3000 přes PLC BECKHOFF pomocí sériové linky je řešením především ze strany datové bezpečnosti a konverze rozdílných komunikačních protokolů a rozhraní.

Přivedením databáze do History Proccess Modulu je možnost tuto databázi pomocí vnitřního softwarového vybavení systému TDC 3000 jednoduše uvolnit pro SQL server tohoto zařízení, popřípadě jej definovat, přiřadit a následně aplikovat do formátu OPC serveru vnitřního systému, tak jak to znázorňuje obr. 27.



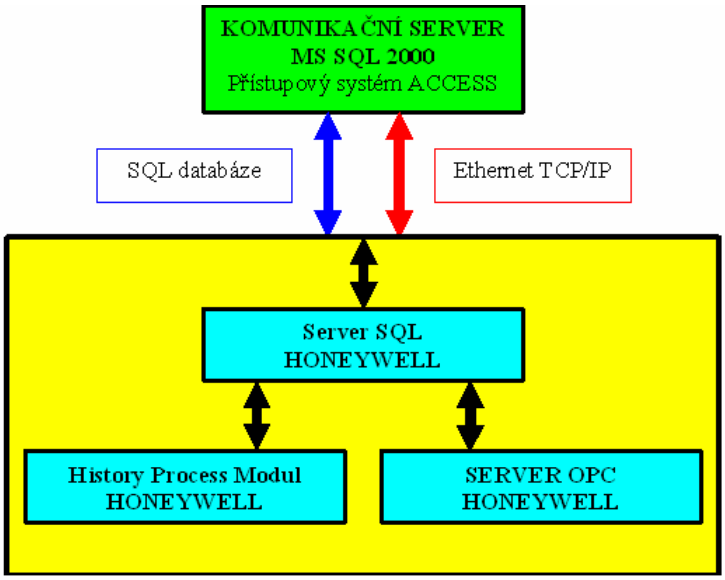
Obr. 27 Systémové moduly zařízení TDC 3000

Základním pravidlem toho návrhu pro bezpečnou výměnu dat je použití sériové linky, která zprostředkovává datovou výměnu mezi daným PLC a History Process Modulem, ze kterého si už systém TDC 3000 přímo zpracovává data v takovém formátu, v jakém si jej správce tohoto systému zvolí. Propojení modulů uvnitř systému TDC 3000 je standardní ze strany jak softwarového, tak hardwarového. Bezpečnostní technik nemusí tyto procesy znát podrobně, protože zpracování databáze uvnitř TDC 3000 již řeší osoba zodpovědná za provoz ASŘ Honeywell.

5.3.2 Návrh na propojení přístupového systému se systémem ASŘ Honeywell EXPERION přes Ethernet a protokol TCP/IP

Jednoduchým řešením jak přenášet data a informace z přístupového systému do systému ASŘ EXPERION je výměna databáze mezi přístupovým systémem a systémy ASŘ využitím komunikačního serveru MS SQL 2000 (obr. 28). Přechod komunikace ze sériového rozhraní, které je používáno u starších, ale velmi rozšířenějších systémů Honeywell TDC 3000 na ethernetové rozhraní systému EXPERION umožnil snadnější implementaci přístupových a docházkových systémů. Využití protokolu TCP/IP usnadnilo celkovou realizaci integrace různorodých systémů v multifunkční celek. Celkové zjednodušení možnosti realizace daného projektu je nejlépe vidět při porovnání obr. 26 a obr. 28. Propojení přístupového systému a systému EXPERION odpadá jeden prvek navíc. Tímto prvkem je, který je obsažen v návrhu pro TDC 3000 je PLC, který zpracovává příkazy vysílané z přístupového systému po sériové lince prostřednictvím komunikačního protokolu

MODBUS do systému ASŘ TDC 3000. Návrh vychází z fyzického propojení dvou různých komunikačních serverů, kdy jeden je nainstalován na straně ASŘ Honeywell a druhý v komunikačním serveru přístupového systému.



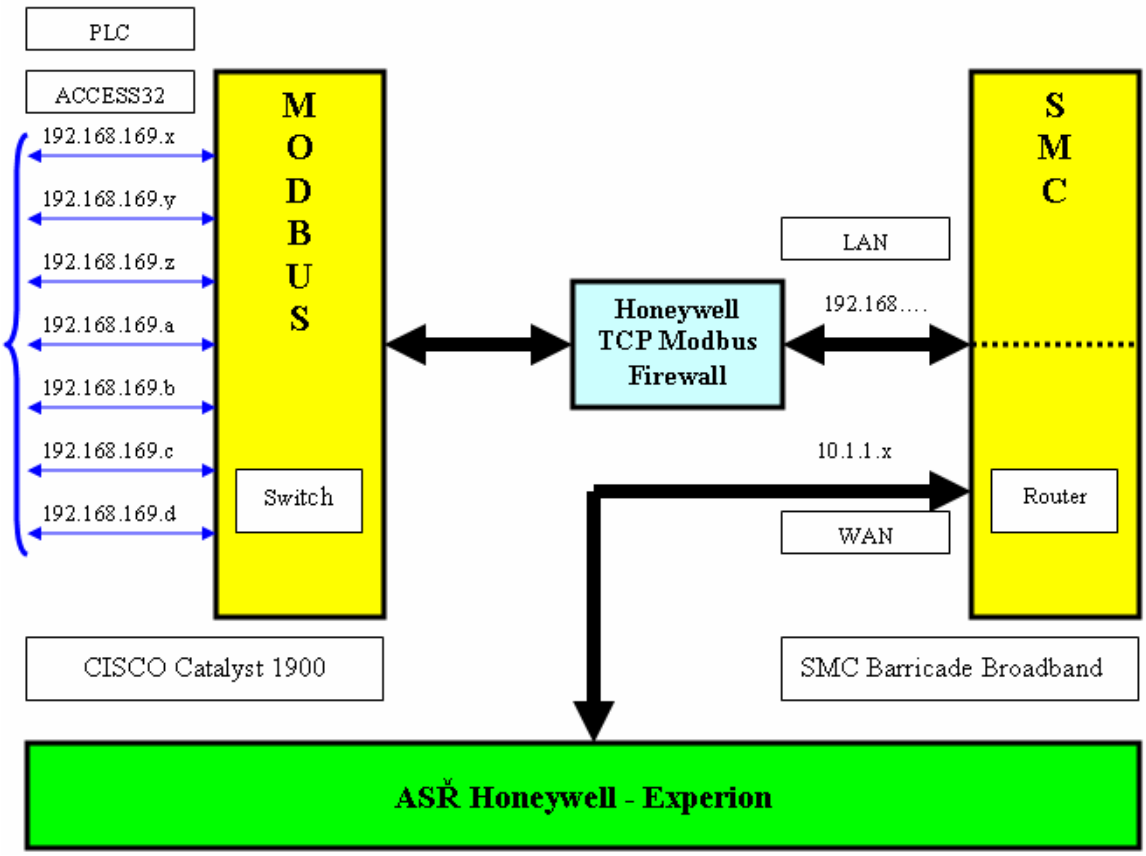
Obr. 28 Propojení systémů pomocí protokolu TCP/IP

Pro jakou alternativu se technik rozhodne, záleží pouze na operativním jednání mezi pracovníkem, který přístupový systém navrhuje a správcem sítě ASŘ. Oba servery jsou v návrhu propojeny pomocí přepínače Cisco Catalyst 1900. Tento přepínač je také vybaven aplikační bránou (Proxy Firewall), jehož pomocí můžeme zabezpečit a řídit síťovou komunikaci mezi sítěmi s různou úrovní důvěryhodností a zabezpečením. Databázové systémy jsou velmi často využívány v přístupových a docházkových systémech pro jejich jednoduchost a rozšířenost.

5.3.3 Návrh na propojení přístupového a docházkového systému se ASŘ Honeywell - Experion SMC Barricade Broadband Routeru

Jistým problémem se může jevit případ, kde pracují systém Honeywell TDC 3000 a systém EXPERION současně. Systém TDC 3000 pracuje v oblasti lokálních adres sítě třídy C 192.168.169.xxx a systém EXPERION je adresován do sítí Wide Area Network (WAN), tedy adresování sítě třídy A typu 10.1.1.xxx. Ethernetový přepínač CISCO Catalyst 1900 je znázorněn na obr. 29 jako jedna z části síťové topologie Ring, která je složena z několika menších kruhových topologií spojené v jeden celek. Vstup přepínače je charakterizován IP adresami zařízení, které s přepínačem komunikují. Tyto zařízení mohou být reprezentovány

jako například Programmable Logic Controler (PLC), modulem Exportů a Importů přístupových systémů, které implementují vazby na jiné systémy, řídících jednotek, kontrolerů a podobně.



Obr. 29 Návrh propojení systému ACCESS do ASŘ EXPERION

Výstup přepínače je na obr. 29 zakreslen jako jeden výstup, ale počet těchto výstupů je dán použitím typu přepínače a jeho konstrukcí. CISCO Catalyst 1900 obsahuje 12 a 24 programovatelných portů. Výstup z přepínače je datově zpracován Honeywell TCP Modbus Firewallem. Tímto opatřením dosáhneme vytvoření demilitarizované zóny, tak jak je v práci popsáno v kap. 5.1 na obr. 23. Data, které jsou filtrována firewallem, jsou adresována adresací pro lokální sítě třídy C 192.168.169.xxx na vstup směrovače (Routeru) SMC Barricade Broadband, který obsahuje překladač adres (NAT).

Network Address Translation převede formát lokálních adres LAN na formát jedinečné adresy WAN. Tímto způsobem dokáže Ethernetovská karta systému EXPERION zpracovat 12 nebo 24 samostatně pracujících zařízení. Základem tohoto návrhu je implementovat zařízení komunikačně pracující s IP adresami lokálních sítí do zařízení EXPERION, které pracuje na bázi sítí třídy A. Virtual Router SMC Barricade Broadband dokáže udělat

z několika LAN IP adres jednu WAN IP adresu. V SMC dochází k překladu adres. Obecně přepínač a směrovač jsou vybaveny firmware, který umožňuje příjemné uživatelské rozhraní.

5.4 Příklad využití integrace přístupového systému ACCESS32 v technologických procesech výroby a distribuce elektrické energie

Využití přístupových systému je velmi rozmanité a nemusí být pouze využívány k evidenci docházky a umožnění přístupových práv pro vstup povolaných osob do budov nebo objektů. Využití integrace přístupového systému v technologických procesech je znázorněno na obr. 30. Přístupový a docházkový systém slouží k monitorování pohybu osob v prostorech technologických procesů (rozvodny, strojovna, kotelna, úpravna vod apod.). PLC Beckhoff CX 1000 slouží jako sběrna dat z terminálů elektrických zařízení a z HPM modulu nebo EXPERION modulu. Systém Honeywell poskytuje informace do PLC, které získal z komunikačního serveru přístupového systému. Programovatelný automat při vhodném naprogramování binárních vstupů/výstupů a analogových vstupně/výstupních modulů je schopen provádět nebo zprostředkovat žádané příkazy a požadované regulace. Terminály frekvenčních měničů, regulátorů, optimilizátorů slouží k nastavení, programování a monitorování nastavených procesů. Komunikace mezi PLC Beckhoff a programovacími terminály elektrických zařízení je vzájemná, to znamená, že je možné provádět příkazy dálkově ze systému Honeywell a naopak systém Honeywell přijímá příkazy, které obsluha zadala pomocí těchto terminálů. Z pohledu bezpečnostní technologie je možné ovlivnit přístupová práva obsluze, která s terminálem manipuluje. Je možné zcela zakázat možnost nastavování parametrů pro zařízení pomocí terminálu nepovolaným osobám, povolit pouze některá přístupová práva k manipulaci s terminály, monitoring elektrických veličin na terminálech zařízení nebo umožnit plná administrátorská práva pro znalého pracovníka. Většina těchto zařízení dokáže komunikovat pomocí rozhraní RS-485 využívající komunikačních protokolů Modbus popřípadě Profibus. To je značná výhoda, když si uvědomíme, že jak systém Honeywell, tak systém MicroSCADA tyto komunikační protokoly podporují. Sériová komunikace je konfigurována pro jedno řídící zařízení Master (PLC) a maximálně 31 řízených jednotek Slave (měnič, regulátor apod.). Návrh na využití integrace přístupového systému ACCESS32 v technologických procesech výroby a distribuce elektrické energie je založen na tom, že pracovník se do rozvodny nebo objektu

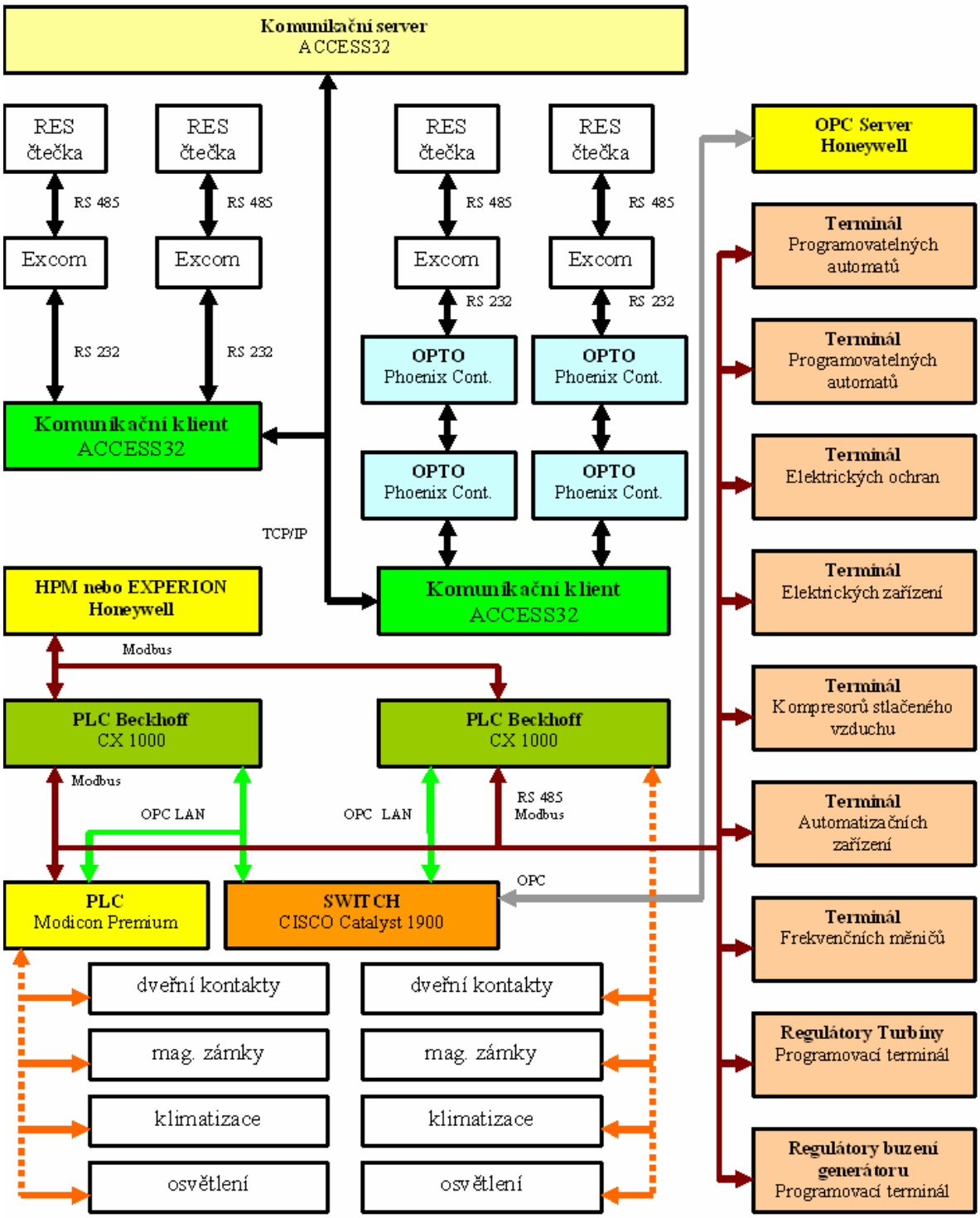
dostane pouze pomocí přístupového systému a ID karty, která je pro každého pracovníka jedinečná. Průchodem přes snímač místa přístupu se tento průstup pracovníka zaznamená do celkové databáze systému ACCESS32 případně nadřazeného systému INFOS. Data z databázového serveru jsou přes komunikační server přenášena až do SQL serveru ACCESS32. SQL server předává zpracované databáze pomocí modulu AM do HPM modulu systému řízení procesů Honeywell, který se stará o celkové provádění všech technologických procesů (obr. 26, 27 a 28). HPM modul komunikuje s PLC Beckhoff pomocí protokolu Modbus nebo také umí vzájemně komunikovat pomocí standardizovaná specifikace rozhraní pro aplikace OPC, které jsou zaměřeny na řízení a monitorování rychlých procesů. [17]

Programovatelný automat Beckhoff CX 1000 zablokuje pomocí vzájemné komunikace všechny programovací terminály na zařízeních, které se nacházejí v prostorách do kterých pracovník vstoupil. Programovací terminály obsahují programové vybavení přístupového kódu k možnému zablokování a odblokování klávesnice. Tyto blokace jdou provádět také softwarově ze vzdálených stanic. Každý pracovník disponuje vlastním přihlašovacím kódem. Tyto kódy jsou obvykle rozděleny do těchto administrátorských práv:

- Odemčeno / plný přístup – pro pracovníky znalé zařízení a technologických procesů. Tento přístup umožňuje všechny činnosti na zařízení včetně změn administrátorských práv.
- Částečně odemčeno / částečný přístup – pro pracovníky, kteří provádí monitoring zařízení a mohou provádět jednoduché programování z terminálů zařízení.
- Zamčeno / omezený přístup – pro pracovníky, kteří smějí pouze monitorovat velikost elektrických a fyzikálních veličin na terminálech zařízení.

Jestliže pracovník zadá některý z těchto kódů do terminálu zařízení a přístupový systém zaznamenal jeho průchod přes snímač místa přístupu, PLC Beckhoff povolí pomocí vzájemné komunikace nebo pouze nahozením patřičného relé na základní desce terminálu provádět požadované úkony. Dále docházkový systém zaznamená počátek a ukončení práce na zařízení. Start práce je zaznamenán od odkódování terminálu a čas ukončení práce je uložen do databáze po zakódování terminálu. Pomocí PLC Beckhoff 1000 jsou data z terminálů přenesena do komunikačního serveru systému ACCESS32, kde se registruje kdy a kdo změny prováděl, a také do Modulu historie (HM) systému Honeywell, kde jsou

ukládány data o tom, jaké změny se prováděly. Uložené databáze je možné kdykoliv zpětně kontrolovat a zjistit kdo prováděl změny v technologických zařízeních.



Obr. 30 Omezení přístupových práv technologických zařízení pomocí systému ACCESS32

Pro energetické společnosti jsou najímány pro většinu dodavatelských a údržbářských prací externí firmy a pracovníci. Není v možnostech interních pracovníků, aby všechny pracovní

úkony externích pracovníků sledovali. Toto řešení integrace přístupového a docházkového systému do technologie procesů v energetice umožňuje zpětně zjistit kdy, kdo a proč změny prováděl. To však není možné, pokud není dobře vedená papírová agenda provedených prací.

ZÁVĚR

Rozvoj moderních informačních a elektronických systémů znamená velký pokrok ve vytváření rozsáhlých bezpečnostních zařízení, které je možné implementovat do stávajících automatických systémů řízení a vytvářet tak rozsáhlé integrované bezpečnostní systémy. Cílem této práce bylo blíže seznámit bezpečnostního technika s možností integrace bezpečnostních technologií se systémy řízení v energetice a podat základní informace o tom, jak tyto systémy pracují a jak mezi sebou komunikují. Bezpečnostní systémy a systémy ASŘ mohou na sobě pracovat nezávisle, a to tak, že si pouze mezi sebou vyměňují data pro monitoring pohybu osob v objektu nebo také mohou kooperovat společně jako jeden velký integrovaný celek, kdy data jsou implementovány do procesů řízení a vzájemně se tyto systémy mezi sebou doplňují. Tyto data se stávají součástí programů a algoritmů v různých procesech řízení a pomáhají zodpovědným pracovníkům operativně řešit případné mimořádné události. Tato práce představuje dva nejrozšířenější automatické systémy řízení pro výrobu a distribuci elektrické energie v České republice – ASŘ Honeywell a MicroSCADA a přístupový a docházkový systém ACCESS32, jehož integrací se systémy ASŘ je možnost vzniku velmi rozsáhlého integrovaného systému. Důležitým aspektem při vytváření a integraci těchto systémů je důraz na dodržování pravidel datové bezpečnosti. Automatické systémy řízení Honeywell a MicroSCADA nejsou vybaveny antivirovými programy a jakékoliv napadení těchto systémů z účastnických pracovních stanic je velmi nebezpečná pro bezporuchový chod celého systému. Potřebuje-li bezpečnostní technik realizovat integraci přístupových systémů s technologickými systémy je třeba, aby byl obeznámen s tím jak tyto systémy ASŘ fungují, a také jak mezi sebou komunikují. Poté je možné vytvářet kvalitní, levné a spolehlivé integrované systémy, které zaručují mnohonásobné zvýšení bezpečnosti práce, ostrahu objektů a operativní chování při mimořádných událostech. Integrace přináší mnoho výhod pro všechny zainteresované subjekty. Pro osoby, které provádí bezpečnostní projektování přináší tento způsob integrace flexibilní návrhy, které lze kdykoliv a levně obměňovat. Pro investora tyto řešení znamenají nízké pořizovací náklady, ponechání stávajících systémů automatizace a možnost bezproblémově celý systém rozšiřovat o další prvky bezpečnostních systémů. Největším problémem při projektování integrace přístupových systémů se systémy ASŘ v energetice se jeví pro projektanta bezpečnostních systémů možnost dostat se ke kvalitní technické dokumentaci technologicko-informačních energetických systémů ASŘ. Cílem této práce

bylo pokusit se nashromáždit co nejvíce informací o těchto systémech, navrhnout plně funkční kooperaci bezpečnostních a technologických systémů v energetických zařízení a vyzvednout výhody, které integrace přístupových systémů se systémy ASŘ přináší.

ZÁVĚR V ANGLIČTINĚ

The improvement of the modern informative and electronic systems spawns the advencement in the production of extensive safety machineries. Those machineries are inserted into automatic systems and result in the integration of safety systems.

The purpose of this projects is the training (that is conlucluding very specific information) of the safety technician workers in order to be able to integrate those new safety technologies in other directory systems in the power engeneering. The training would involve the information about the structure and differences in the functioning, connection and the communication of the new systems.

The safety system and control systems work independetly on each other, however they are exchanging the data for the monitoring of motion of the people in the building. On the other hand, the systems can cooparate as the whole unit. In other words, the data of both systems can be exchanged or adapted.

The data becomes part of the programs and algoritms in various processes of the direction and support. The data helps solve significant actions and prossegers for the workers.

The processing work involves two most common automatical system for the dicrection, production and distribution of the electric power in the Czech Republic.

The control system Honeywell and The MicroSCADA as well as ACCESS32 are the pioneer elements of the origin of the enlarged integeration system.

The importanr part at the porduction of the integration of the systems is the importance of following the rules of the data safety.

Automatical systems (Honeywell and MicroSCADA) and their direction are not provided by anti-virus programs, therefore any attack from the membership worker units is very dangerous for the fluent processor of the whole system.

If the safety worker needs to work with the integration of the access systems with the technology systems, he has to be familiar with the control systems and their function as well as communication.

If all those requested points are fulfilled, there is possibility of qualitative, cheap and reliable inteagration systems as well as the work that is done. The systems are afterwards able to

increase the safety of the work, but also the safety of the buildings and organize probelm-solving at the error events.

The integration brings many benefits for all involved buisnesses and corporations. In addition, the integration systems bring new suggestions and new solution combinations for the safety- energetic workers.

The invetors may be interested in the integrative systems for its low finances and the automatic direction of the processes and systems.

The bigest disadvantage of the projecting of the integration systems with control systems is the lack of the technical documentation and quality information of the control systems.

The goal of this project was to extend and collect more information about the mentioned systems, and come up with the new ideas for full- functioning coorperation of the safety and technology systems in the energetic engeneering, as well as highlight the benefits that the control systems bring.

SEZNAM POUŽITÉ LITERATURY

[1] SZCZOLKA, Marek, *Objektová bezpečnost,* [online]. [cit. 2010-01-28]. Dostupný z WWW: <http://www.junfan.ic.cz/?p=52>.

[2] ČSN EN 50133-1 Poplachové systémy – Systémy kontroly vstup; pro použití v bezpečnostních aplikacích Část 1 : Systémové požadavky

[3] Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky ČSN CLC/TS 50398, Březen 2005

[4] KINDL, Jiří *Projektování bezpečnostních systémů I. díl*, 2. vyd. Univerzita Tomáše Bati ve Zlíně, 2007. 134 s. ISBN 978-80-7318-554-1. Kapitola 4.6, Stupně zabezpečení komponentů I&HAS s.101

[5] ČSN EN 50131-1 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy

[6] ČSN EN 50132 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích

[7] LAUDSKÝ, Vladimír. *Technologie komerční bezpečnosti II.* 2. vyd. UTB ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9. Kapitola 8, Základy technických prostředků ochrany majetku a osob II.s.118-119

[8] *Operátorská příručka, Úvod do systému INFOS*. Zlín: Cominfo a.s., 2003. verze 1.0.6. 15 s.

[9] *Operátorská příručka, Přístupový systém ACCESS32*. Zlín: Cominfo a.s., 2005. 57 s.

[10] KŘEČEK, Stanislav a kol.,. *Příručka zabezpečovací techniky*. Blatenská tiskárna, spol. s r.o., 2003, 351 s., ISBN 80-902938-2-4. 2003. s. 104.

[11] *Process Automation College: UxS System Administration* – Technical Reference Manual, vydané 27.8 1996,

[12] *Process Automation College: Local/UCN/APM Maintenance* – Technical Reference Manual, vydané 4.6 1992,

[13] *Operátorská příručka TCD 3000*. Praha: Honeywell a.s., 2004. 48 s.

[14] *Introduction to MicroSCADA Technology* – Technical Reference Manual, vydané 15.3 2002

[15] KOŠŤÁL, David., STAUDEK, Jan. *Firewally, bezpečnostní oddělovací uzly.* Praha : Lancom, spol. s r.o., 1997, ISSN 1210-2997. 1997. s. 22-28.

[16] ROSULEK, Miroslav. Maximální využití podnikové sítě – data, video a audio na Ethernetu. Automatizace. 2008, roč. 51, č. 7-8, s. 474.

[17] MicroSCADA OPC Data Access Server Technical Reference Manual, vydané 15.1 2004, verze 8.4.5

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČSN	České technické normy.
I&HAS	Poplachové zabezpečovací a tísňové systémy
LAN	Local Area Network – lokální datová síť
WAN	Wide Area Network – veřejná datová síť
SQL	Strukturovaný dotazovací jazyk
ODBC	Standardní aplikační rozhraní
TCP/IP	Komunikační protokol
CCTV	Uzavřený televizní a střežící okruh.
OPC	Komunikační protokol
PLC	Programovatelný automat
BS	Bezpečnostní služby
EPS	Elektrická požární signalizace
REI	Snímač místa přístupu
RES	Snímač místa přístupu
DHCP	Aplikační protokol
OLE DB	Ovladač starající se o interpretaci SQL dotazů
GUS	Global User Station
TDC	Totally Distributed Control Systém
TPS	Total Plant Solution
US	Universal Station
AM	Aplication Modul
HM	History Modul
CG	Computer Gateway
NG	Network Gateway

HPM	High-Performance Process Manager / History Process Modul
LCN	Local Connection Network
UCN	Universal Connection Network
APM	Advanced Process Manager
LM	Logic Manager
VN	Vysoké napětí
VVN	Velmi vysoké napětí
SYS	Základní systém MicroSCADA
COM	Komunikační systém MicroSCADA
PCO	Pult centralizované ochrany
ASŘ	Automatický systém řízení
DMZ	Demilitarizovaná zóna
PHD	Proces History Database
RS485	Komunikační rozhraní
RS232	Komunikační rozhraní
DHF	Dual-Homed Firewall

SEZNAM OBRÁZKŮ