ČESKÁ ZEMĚDĚLSKÁ UNIVEZITA V PRAZE
TECHNICKÁ FAKULTA
Katedra technologických zařízení staveb

Tvorba bezpečného web serveru pro vzdálený přístup a ovládání EZS systému

diplomová práce

Vedoucí práce: Ing. Zdeněk Votruba
Autor práce: Jan Bodlák

Praha 2011

Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Akademický rok 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jan Bodlák

obor Obchod a podnikání s technikou

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název práce: **Tvorba bezpečného web serveru pro vzdálený přístup a ovládání EZS systému**

Osnova diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Popis stávajícího řešení
4. Popis komunikace ústředny a interface
5. Definice zásad pro bezpečnou komunikaci
6. Návrh struktury a vlastní realizace interface ústředny
7. Literární rešerše
8. Závěr
9. Seznam literatury
10. Přílohy

Rozsah hlavní textové části: 40 - 60 stran

Doporučené zdroje:

Zdroje Internet
ZAHRÁDKA, J.: Začínáme s EZS. Variant plus s r.o. 2005, 36 s.
KŘEČEK, S.: Příručka zabezpečovací techniky. 2002, Critetus, 313 s. ISBN 80-902938-2-4.
KLUGL, J.:Montáž EZS. 1994, 215 s.
KOKTAN, P. a kol.: Mechanické zábranové systémy. 1998, 268 s.
BEBČÁK, P.: Požárně bezpečnostní zařízení, 2004, SPBI, 226 s. ISBN 80-86634-34-5.
HEŘMAN, J., TRINKEWITZ, Z., a kol.: Elektrotechnické a telekomunikační instalace, 2006, Verlag Dashofer, ISBN 80-86897-06-0
KALLAY, F., PENIAK, P.: Počítačové sítě a jejich aplikace, 2. vydání, Grada, 2003, ISBN 80-247-0545-1
DOUČEK, P.: Řízení projektů informačních systémů, Professional Publishing, 2004
BUCHALCEVOVÁ, A: Metodiky vývoje a údržby informačních systémů, Grada, 2005

Vedoucí diplomové práce: **Ing. Zdeněk Votruba**

Termín zadání diplomové práce: listopad 2009

Termín odevzdání diplomové práce: duben 2011

L.S.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
-3-
TECHNICKÁ FAKULTA

.....
Vedoucí katedry

.....
Děkan

V Praze dne: 30. 11. 2009

Prohlašuji, že diplomovou práci na téma: *„Tvorba bezpečného web serveru pro vzdálený přístup a ovládání EZS systému*“ jsem vypracoval samostatně a použil jen pramenů, které cituji a uvádím v přiložené bibliografii.

Na tomto místě bych rád poděkoval především Ing. Zdeňku Votrubovi za vstřícný přístup během konzultací, cenné náměty a rady. Dále bych rád poděkoval přítelkyni, rodině a kamarádům za podporu při psaní této práce.

Tvorba bezpečného web serveru pro vzdálený přístup a ovládání EZS systému

Abstrakt: Práce se zabývá popisem stávajících řešení vzdáleného webového přístupu k elektronickým zabezpečovacím systémům. V práci jsou popsány používané způsoby ochran před známými metodami napadení komunikace, stran anebo webových serverů těchto modulů. Jako stávající řešení je proveden rozbor modulu IP100 společnosti Paradox Security Systems Ltd. Cílem práce je sestavení webového serveru a vytvoření stran, které mohou být integrovány právě do modulu IP100. Vytvořené strany i server musí zvyšovat úroveň zabezpečení při zachování nebo zvýšení kompatibility s webovými prohlížeči.

Klíčová slova: Web server, IP100, PARADOX, EZS

Secure web for security systems

Summary: Subject of this graduation thesis is description of the existing solutions, remote Web access to the electronic security systems. Methods of protection against known methods of attacking, communication of pages or the web server of these modules are described in theses. As the current solution is used IP 100 of company Paradox Security Systems Ltd to analysis of module. The main point of thesis is making a web server and pages which may be integrated into the IP100 module. Web server and web pages must increase the level of security while maintaining or increasing compatibility with Web browsers

Key words: Web server, IP100, PARADOX, ESS

Obsah

1 Úvod

Zabezpečovací systémy obecně jsou používány od dob, kdy došlo k potřebě člověka vlastnit, potřebě bezpečnosti, pocitu bezpečí. Dle ruského psychologa Maslowa je tedy jednou ze základních potřeb v jeho pyramidě uspokojování osobních potřeb.

Pod pojmem elektrický zabezpečovací systémem dále jen EZS je možné si představit ústředny, čidla a tísňové hlásiče, signalizační, ovládací, přenosová, zapisovací a jiná komplementární zařízení. Za pomoci těchto mechanismů je signalizováno narušení střeženého objektu nebo prostoru na zvoleném místě. EZS slouží k včasné signalizaci nežádoucího vniknutí či pokusu o vniknutí do střeženého prostoru nebo nežádoucí činnosti narušitele. Samočinně anebo prostřednictvím lidského činitele urychluje předání poplachové informace osobě, organizacím jako jsou provozovatelé pultů centrálních ochran. Elektronické zabezpečení výrazným způsobem doplňují možnosti, které nabízejí mechanické zábranové systémy. Webové rozhraní je nepochybně atraktivní možností rozšíření funkčnosti EZS. Webové rozhraní většina výrobců neintegruje přímo do ústředny EZS, ale nabízí ho jako doplněk k EZS ve formě externě či interně umístěného modulu. Modul umožňuje uživateli okamžitě monitorovat stav střeženého objektu nebo prostoru, tento stav na základě zjištěných informací upřesnit a také dle nastavených pravidel a možností webového rozhraní interaktivně zasahovat.

1.1 Základní rozdělení zabezpečovacích systémů

Souhrnné zabezpečení jakéhokoli objektu musí být vždy tvořeno vhodným propojením technické, fyzické, klasické a režimové ochrany (1) (2).

1.1.1.1 Klasická ochrana

Tuto ochranu představují střechy, zdi, podlahy, okna a dveře objektů. Mluvíme o mechanických zábranných prostředcích (dále jen MZP). Jedná se o veškerých MZP, které ztěžují vniknutí do objektu, případně manipulaci neoprávněné osoby se zabezpečenými předměty v objektu. Např. bezpečnostní systémy dveří, mříže, bezpečnostní fólie, tvrzená a vrstvená skla, aj. (3) (2) (1)

1.1.1.2 Fyzická ochrana

Takovouto ochranu zajišťují osoby, které vyhodnocují bezpečnostní situaci a operativně realizují nutná opatření. Fyzickou ochranu objektu je možno podle typu (soukromý, státní) provádět vlastními silami, strážnými, zaměstnanci soukromých bezpečnostních služeb, policií a Armádou ČR. Fyzická ochrana patří mezi ochranu finančně nákladnou. (1)

1.1.1.3 Technická ochrana

Tato ochrana podporuje klasickou a zefektivňuje fyzickou ochranu. Základními reprezentanty této skupiny jsou právě EZS, uzavřené televizní systémy, elektronickou požární signalizaci, přepěťovou ochranu apod. (4) (1)

1.1.1.4 Režimová ochrana

Doplňuje předchozí ochrany o administrativně organizační opatření, tak aby zabezpečovací systém mohl bezchybně fungovat (1). Jedná se zejména o personální záležitosti, řízení přístupu k datům, klíčové hospodářství ale také o pojištění zabezpečeného objektu.

1.2 Historie

Počátkem 19 století rostl počet obyvatel ve městech a tím se také zvyšovala rizika z pohledu bezpečnosti osob a věcí. Nejprve ale zabezpečovací systémy sloužily k ochraně před živelnou pohromou – požárem. Cesta přenosu poplachové informace byla zpočátku velmi jednoduchá – křik, zvonění či troubení. Teprve s vynálezem telegrafu v roce 1835 začala éra rychlého přenosu informací, kdy v roce 1847 sestrojil v New Yorku hlavní inženýr města Cornelius Anderson síť požárních ohlašoven a centrálního „dispečinku“. Došlo k nebývalému zkrácení přenosu poplachové informace od místa ohrožení k požární stanici. Dalším krokem, koncem 19. století, bylo zavedení volacích skříněk – veřejných ohlašoven, které se již vyznačovaly prvky základní automatizace. Skříňky zasílaly samy, po zatažení za páku hlásiče, telegraficky zprávu. Obdobný systém již ale paralelně vznikl také v Evropě v Hamburku. (1) (4)

První známý elektrický zabezpečovací systém si nechal v roce 1853 patentovat pan Augustin Pope z Massachusets. Používá prvky mechanických kontaktů na dveřích a oknech spojených s baterií a zvonkem. V roce 1857 pan Pope svůj patent prodává Edwinu T. Holmsovi, novoanglickému obchodníkovi. Pan Holms ve spolupráci s Williamsem, prvním majitelem obchodů s elektrotechnikou v zemi, začal masověji elektrický zabezpečovací systém vyrábět a také vyvíjet. Vedlejším prvkem tohoto vývoje byly prvky později používané v telefonii. Zabezpečovací systém vznikl 20 let před telefonem a čtvrt století před žárovkou. Holmes svůj systém později propojil s již známou myšlenkou centralizovaných pultů dnes známých pod zkratkou PCO (pult centrální ochrany) se schopností zásahu 24 hodin denně. (4)

Až do 50. let 20. století byly zabezpečovací ústředny zásadně reléovou záležitostí. S objevem polarizovaného relé začaly být bezpečnostní okruhy vyvažovány, čímž podstatně vzrostla bezpečnost sledovaného okruhu.

S příchodem tranzistoru po druhé světové válce vznikají nové snímače, akustické a kapacitní. Mechanické kontakty začínají být vytlačovány magnetickými s jazýčkovým kontaktem. V 60. letech se objevují první krátkovlnné detektory, které vyhodnocují změnu odrazu vln. Teprve s hromadnou výrobou Gunnovy diody, na začátku 70. let, se objevují spolehlivé mikrovlnné detektory pracující na Dopplerově principu. Zhruba ve stejné době se do popředí zájmu dostávají infračervené světelné závory. (4)

Dnes nejúspěšnější detektor se objevuje až v druhé polovině 70 let a to je pasivní infračervené čidlo (PIR). Nedosahují kvalit mikrovlnných čidel. Ovšem spolehlivost, jednoduché nastavení a kvalita vyhodnocení poplachových stavů předčila snímače mikrovlnné. Ostatní čidla tak byly vytlačeny na okraj zájmu. Jako poslední se objevují senzory sledující určité anatomické anebo fyziologické zvláštnosti každého člověka - Biometrické senzory. Přechází z pole přístupových systémů do systémů průmyslové televize.

Se zaváděním počítačů a mikropočítačů dochází k výraznému zjednodušení zapojení ústředen a tím k zlevnění výroby. Jednočipové mikro kontroléry se dnes velmi často používají jak v ústřednách, tak v samotných čidlech. Se sítěmi IEE1984 a technologiemi jako je ZIGBEE se také rozšiřují bezdrátové technologie ať již ve formě bezdrátových čidel nebo bezdrátových ovladačů – klávesnic (4). S masovým rozšířením internetu vzniká poptávka po možnosti spravovat EZS právě touto cestou. Proto se objevují složitější či jednodušší moduly, připojitelné k novým ale také stávajícím ústřednám EZS.

1.3 Poplachové systémy v ČR

V Čechách se bezpečnostní systémy objevují až po roce 1989. Bez znalostí, s jedinou normou ČSN334590 stál obor prakticky na začátku. Přílivu často nekvalitních systému zabezpečení se podařilo čelit opatřeními ministerstva vnitra. Jeho úlohu později převzaly akreditované zkušebny a certifikační orgány. Na dnešním trhu působí v dani oblasti především akreditovaná zkušebna Trezortest, která v rozsahu své činnosti má vedle poplachových systémů i Mechanické zábranné systémy. Svoji roli v oboru hraje dnes i Certifikační institut české asociace pojišťoven (CI ČAP), který po vzoru německé VdS (svazu zřizovatelů) nastartoval systém regulace v obru poplachových systémů. Pojišťovny mají ze zákona možnost stanovovat dodatečné technické požadavky na základě tzv. „blokové výjimky“. Tato výjimka kopíruje pravidla Evropských společenství v oboru Poplachových systémů. (4)

1.4 Předpisová základna v oboru poplachových systémů

1.4.1 Evropská unie

V Evropských společenstvích spadá zabezpečovací technika (zařízení používaná v poplachových systémech) pod působnost směrnic Evropských společenství. Tento typ dokumentu stanovuje základní požadavky. Nemá přímou právní platnost v rámci členských zemí. Po jejich projednání a schválení jsou směrnice vyhlašovány v Úředním věstníku Evropských společenství (Official Journal of European Union). Povinností členských zemí je zásady uvedené ve směrnicích zapracovat do národní legislativy v termínu stanoveném přímo ve směrnicích. Povinnosti ze směrnic technického charakteru jsou pak závazné pro výrobce, dovozce a distributory výrobků spadajících pod působnost příslušného národního legislativního předpisu. (4) (2)

Pro podporu splnění požadavků směrnic jsou vyhlašovány v Úředním věstníku EU Evropské harmonizované normy. Tyto harmonizované normy nejsou závazné, nicméně jejich splnění je po právní stránce chápáno jako precedens splnění právních požadavků stanovených na daný okruh výrobků. Evropské normy jsou zpracovávány Evropskými normalizačními organizacemi CEN (Evropský výbor pro normalizaci) a CENELEC (Evropský výbor pro normalizaci v elektrotechnice). (2) (4)

1.4.2 Česká republika

V České republice jsou technické směrnice EC přejímány formou nařízení vlády České republiky. S ohledem na to, že ČR je od roku 2004 plnoprávným členem EU, kopíruje linie základních legislativních požadavků na výrobky pravidla obvyklá v zemích EU. (4)

1.4.2.1 Oborově specifické normy

V oboru poplachových systémů začaly v posledním desetiletí 20. století vznikat na půdě evropských (CENELEC) a světových (IEC - Mezinárodní výbor pro elektrotechniku) normalizačních organizací oborové standardy nabízející pro jednotlivé skupiny zařízení z oboru poplachových systémů:

- řešení funkčních požadavků na jednotlivá zařízení,
- dále uvádějící metody zkoušení prokazující splnění těchto funkčních požadavků, *)
- požadavky na vlastnosti vztahující se k vlivům prostředí (klimatické odolnosti), *)
- metody zkoušení prokazující splnění klimatické odolnosti, *)
- systémové požadavky vztahující se k podmínkám nasazení těchto systémů, *)
- návody a doporučení na aplikaci poplachových systémů.

*) Poznámka - tylo požadavky a metody zkoušení jsou obsahem tzv. výrobkových norem

Evropské normy (EN) jsou produktem evropských normalizačních organizací. V případě poplachových systémů je to konkrétně technická komice CLC/TC79 a její pracovní skupiny. V případě EPS je to CEN/TC72 a její pracovní skupiny. (4)

1.4.2.2 Skupiny norem pro poplachové systémy

ČSN EN 50130 - Poplachové systémy (všeobecné požadavky) (2)

CSN EN 50131 - Elektrické zabezpečovací systémy (IAS: Intruder Alarm Systems) Funkce: poplachové systémy určené k detekci a signalizaci přítomnosti, vniknutí nebo pokusu o vniknutí narušitele do střežených prostor. (2)

• ČSN EN 50132 - CCTV sledovací systémy (CCTV: Circuit Closed Television) Funkce: poplachové systémy obsahující kamerovou sestavu, zobrazovací a další přídavná zařízení, nezbytná pro přenos signálu a obsluhu při sledování definované bezpečnostní zóny. (2) (4)

• CSN EN 50133 - Systémy kontroly vstupu (ACS: Access Control Systems) Funkce: poplachové systémy, obsahující všechna konstrukční a organizační opatření včetně těch, která se týkají zařízení nutných pro kontrolu a řízení vstupů (2)

• CSN EN 50134 - Systémy přivolání pomoci (SAS: Sociál Alarm Systems) Funkce: poplachové systémy poskytující prostředky k přivolání pomoci a které jsou určené pro použití osobami, které mohou být považovány za osoby žijící v ohrožení (2).

• EN 50135 - Systémy tísňové (HUAS: Hold-Up Alarm Systems) Funkce: poplachové systémy, které v případě přepadení umožňují záměrné vytvoření poplachového stavu

• ČSN EN 50136 - Poplachové přenosové systémy (ATS: Alarm Transmission Systems) Funkce: poplachové systémy, které jsou především určeny k přenosu poplachových hlášení na rozhraní poplachového systému ve střežených prostorech k rozhraní poplachového přenosového zařízení v poplachovém přijímacím centru a dále k ovládacímu a indikačnímu / zobrazovacímu zařízení v poplachovém přijímacím centru. (2)

• EN 50137 - Systémy kombinované nebo integrované Funkce: poplachové systémy, které jsou kombinací dvou nebo více jednoúčelových systémů. (2)

2 Cíl práce a metodika

Cílem práce je návrh a vytvoření bezpečného web serveru. Bezpečným web serverem se rozumí takový server, který bude vhodný pro použití v stávajícím modulu EZS firmy Paradox Security Systems Ltd., IP100 a bude zabezpečen proti v současné době známým chybám. WEB server musí být schopen zpracovávat nejen statické strany, ale také strany dynamicky vytvářet na základě komunikace s ústřednou EZS.

Web server musí komunikovat s klienty pomocí Hypertext Transfer Protokolu dále jen HTTP anebo protokolu Hypertext Transfer Protocol Secure dále jen HTTPS tak aby, přenášená data byla čitelná v aplikacích, jako jsou běžné internetové prohlížeče. Web server musí kromě zabezpečeného přenosu zajišťovat a rozšiřovat stávající způsob autentizace a autorizace oprávněných osob.

2.1 Způsoby zabezpečení web serveru pro komunikaci s webovým klientem

Nutné je zabezpečit přenos dat, autentizaci a autorizaci a také samotný webový server včetně všech aplikací na něm běžících. V následujících kapitolách budou probrány jednotlivé v praxi používané způsoby zabezpečení a naznačeny jejich přednosti či nedostatky.

2.1.1 Zabezpečení přenosu dat

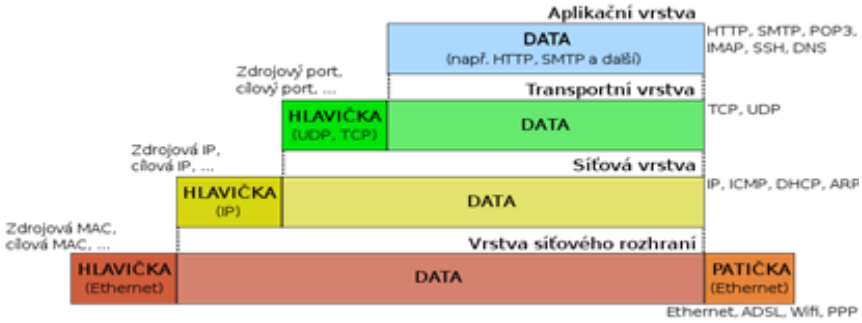
V případě TCP/IP protokolu se používají následující postupy. Tyto metody se mohou vzájemně kombinovat.

2.1.1.1 Užití separátní fyzické linky

Speciální linka připadá v úvahu pouze v lokálních sítích, které nejsou spojeny s jinými sítěmi a podsítěmi. Nepoužívají nezabezpečené bezdrátové části přenosu. Vyžadují, aby všechny aktivní i pasivní prvky takové sítě byly zabezpečeny proti nežádoucímu odposlechu. Jedná se o velmi nákladný způsob zabezpečení a přístup k ovládání není možný odkudkoli. V celé síti je nevhodné používání snadno odposlechnutlených bezdrátových sítí typu IEEE 802.11 apod. (5)

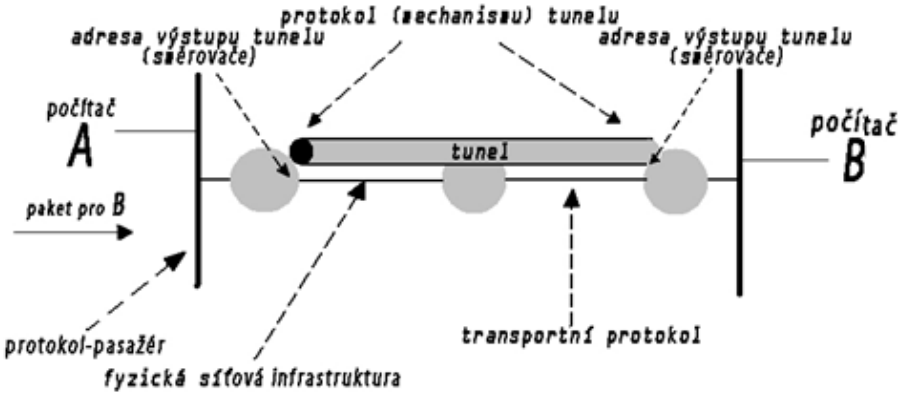
2.1.1.2 Užití separátní virtuální linky

Vytvoření síťového tunelu je způsob kdy dojde k o „obalení“ nešifrovaného přenosu šifrovaným. Vzniká separátní kanál virtuální privátní sítě dále jen VPN mezi serverem a klientem. Klient a server používají specifický software, který ale bývá součástí operačního systému. Jedná se vlastně o vrstvu vloženou mezi vrstvu transportní a aplikační dle referenčního modelu ISO/OSI znázorněného na obrázku 1. Vrstva poskytuje úroveň šifrováním a autentizace. (6)



Obrázek 1 - zapouzdření dat v sítích TCP/IP (7)

Celá komunikace spočívá na principu naznačeném na obrázku 2. Zde je patrné rozložení jednotlivých vrstev.



Obrázek 2 – princip tunelování (8)

2.1.1.2.1 Šifrování přenášených dat

Šifrování je proces, kdy měníme otevřený text (tj. nešifrovaný) pomocí šifry a hesla v text bez hesla nesrozumitelný. Na rozdíl od kódování je tedy heslo nutné, nestačí znalost samotného postupu. (9) (10)

Musí být zajištěna efektivita přenosu a kompatibilita s webovým klientem. Pod efektivitou přenosu se rozumí míra zatížení koncových zařízení, klienta mezičlánků a serveru při zpracovávání šifrovaných dat a také objem přenášených dat. (9) Základní rozdělení:

1) Symetrické šifry

Pro zašifrování a dešifrování přednášených informací je použit stejný klíč. Šifrování lze dále rozdělit dle principu. V oblasti informačních technologií se používají tzv. „Moderní symetrické šifry“, které jsou dle způsobu proudové, tedy šifrují po jednotlivých bitech a blokové. Blokové šifrují data po stanovených délkách bitových bloků. Příkladem je: AES (Advanced Encryption Standard), DES nebo Blowfish. (10) (9)

2) Asymetrické šífry

Klíč je rozdělen na soukromou a veřejnou část, kdy veřejnou částí lze data zašifrovat a teprve při použití soukromé části je možné data dešifrovat. Příkladem jsou šifry DHM (Diffie, Hellman, Merkle), RSA (Rivest, Shamir, Adleman). (9)

3) Kombinace obou způsobů šifrování

Jde o způsob šifrování kdy v určitém okamžiku je použit přenos asymetrickou šifrou a v jiném symetrickou. Ošetřují se tak např. problémy s předáváním klíče pro symetrické šifrování. Příkladem je protokol PGP (Pretty Good Privacy). (9)

2.1.2 Zabezpečení autentizace

Autentizace je jednoznačné stanovení osoby – uživatele, který přistupuje k danému systému. Cílem je ověření identity uživatele. Každý bezpečný systém musí autentizaci v určité formě používat. Nejčastěji se používá ověřování pomocí uživatelského jména anebo identifikátoru současně s heslem. K autentizaci se využívají softwarová nebo hardwarová zařízení v podobě čipových karet či adresářových serverů. (11)

1) uživatelské jméno a heslo

Nejjednodušší, nejpoužívanější způsob, uživatel musí znát pouze svoje jméno či identifikátor a heslo. Pro přístup nepotřebuje žádné speciální pomůcky, vyjma software pro práci s daným systémem. (11)

2) uživatelské jméno a osobní certifikát

Uživatel musí znát jméno nebo svůj identifikátor a zařízení - datový nosič, který obsahuje veřejnou část osobního certifikátu asymetrické šifry. (11)

3) uživatelské jméno a heslo současně s ověření aut entity jinou cestou

Uživatel zadává známé jméno nebo osobní identifikátor a heslo po úspěšném ověření probíhá fáze do ověření. V této části probíhá ověření aut entity zasláním verifikační zprávy jinou cestou jako je mail, či krátká textová zpráva. Po zadání verifikačního kódu obsaženého ve zprávě je klient autentizován. (11) (12)

4) metoda plovoucích hesel

Tato metoda je používána v případě možnosti odposlechnutí celé i nešifrované komunikace a je založena na neopakovatelnosti autentizačních údajů. Jedná se o metodu plovoucího hesla, kdy je uživateli předán omezený počet předgenerovaných hesel. Předání probíhá například formou autentizačního generátoru. Tato hesla je nutná zadávat v pořadí generování, jak strana autentizující, tak strana autentizovaná jsou synchronizovány. (13)

5) metody ověření 3. stranou

Typickým příkladem je metoda Kerberos. Kerberos je založen na Needham-Schroeder Symmetric Key Protokolu. Používá důvěryhodné třetí strany nazývané též Key Distribution Center (KDC) sestávající ze dvou logicky oddělených částí: Autentizačního serveru (AS) a Ticket-Granting Serveru (TGS). Kerberos pracuje na principu tiketů sloužících k ověření identity uživatelů. KDC si udržuje databázi tajných klíčů; každá entita v sítí, ať již klient nebo server, vlastní svůj tajný klíč známý pouze jí a KDC. Znalost tohoto klíče slouží k prokázání identity dané entity. Pro komunikaci mezi entitami KDC vygeneruje „session key“, kterým obě protistrany zabezpečí vzájemnou komunikaci. (14)

2.1.3 Zabezpečení autorizace

Autorizace je proces ověření přístupových práv autentizovaného uživatele. V některých případech nemusí autorizaci předcházet autentizace. Pod přístupovými právy se rozumí oprávnění k provedení patřičné akce nebo k přístupu k danému objektu. Akce, respektive skupiny akcí jsou zpravidla rozděleny mezi několik administrátorů či bezpečnostních správců a mezi běžné uživatele systému (15). Z pohledu HTTP komunikace mezi serverem a klientem lze říci, že problém spočívá právě ve vícenásobném přenosu – přístupu. Komunikace je navázána pouze na konkrétní požadavek klienta a je bez stavová. K autorizaci musí docházet vždy při konkrétním požadavku klienta. Autorizace je vždy řízena na základě seznamů pro řízení přístupu dále jen ACL (acces control list) (16). Před provedením jakékoli operace je prohledána databáze ACL a je-li nalezen odpovídající záznam, vyžadovaná operace je vykonána.

2.1.3.1 Způsoby autorizace

Lze rozlišit dle způsobu práce právě s ACL tabulkou na tzv volitelné řízení přístupu DAC (Discretionary Access Control) a povinné MAC (Mandatory Access Control) řízení přístupu. Systémy s volitelným řízením přístupu umožní vlastníkovi objektu plně řídit přístupy tak aby mohl zasahovat také kdokoli jiný. Správce pak nemá plnou kontrolu nad spravovaným systémem. (17) (18)

Systémy s povinným řízením přístupu zavádí pro každý proces, každého uživatele systému vlastní práva a určuje také jeho prostředky. Práva jsou stanovena správcem a vynucena na úrovní operačního systému. Pokud se pokusí útočník dostat přes chybu v aplikaci, získá pouze kontrolu nad daným programem s takto omezenými právy. (17)

Obvyklé ACL systémy nastavují oprávnění jednotlivě. Systém s velkým počtem objektů anebo uživatelů se poté obtížně spravuje. Novější metoda spočívá ve vytvoření bezpečnostního modelu, kdy se sdružují skupiny oprávnění do. rolí. Role jsou pak přidělovány jednotlivým uživatelům. (17)

2.1.4 Autentizace a autorizace u webových serverů

Jelikož webové servery používají standardizovaný protokol HTTP, ve kterém je již protokol implementován lze rozdělit na tzv. vestavěnou HTTP autorizaci a autentizaci a vlastní, ta využívá HTTP formuláře, cookies na straně klienta nebo serveru potom mluvíme o sessions. (18)

2.1.4.1 Vestavěná autorizace a autentizace HTTP

Přímo protokol HTTP obsahuje hlavičku určenou pro vestavěnou autorizaci. Komunikace mezi serverem a klientem poté vypadá následovně:

Klient při žádosti o stránku „/private/index.html“ posílá serveru localhost:

```
GET /private/index.html HTTP/1.0
Host: localhost
```

Server odpovídá:

```
HTTP/1.0 401 Authorization Required
Server: HTTPd/1.0
Date: Sat, 27 Nov 2004 10:18:15 GMT
WWW-Authenticate: Basic realm="Secure Area"
Content-Type: text/html
Content-Length: 311
<HTML>
 <HEAD>
  <TITLE>Error</TITLE>
  <META HTTP-EQUIV="Content-Type" CONTENT="text/html" charset="XY">
 </HEAD>
  <BODY><H1>401 Unauthorised.</H1></BODY>
 </HTML>
```

Klient poté znovu odesílá autentizační a autorizační požadavek serveru doplněný o přístupové informace zakódované metodou BASE64.

```
GET /private/index.html HTTP/1.0
Host: localhost
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

Pokud jsou informace správné, server odpovídá:

```
HTTP/1.0 200 OK
Server: HTTPd/1.0
```

Date: Sat, 27 Nov 2004 10:19:07 GMT
Content-Type: text/html
Content-Length: 10476
…HTML či jiný obsah stránky…

Použití tohoto způsobu autorizace má širokou podporu webových prohlížečů. Problémem je odhlašování. Je nutné ukládat pomocná data do databáze, čím ztrácí HTTP Autorizace výhodu oproti sessions autorizaci, druhou možností je provést chybné přihlášení. Třetí a poslední možností je uzavřít okno prohlížeče uživatelem nebo skriptem při ukončení práce. (19).

2.1.4.2 Autorizace a autentizace s použitím sessions

Session tj. relace řeší problém bezstavovosti protokolu HTTP. Umožňuje udržet další informace definované vývojářem stran např. o stavu aplikace nebo práci uživatele. Princip spočívá v tom, že webový server si udržuje ke každému spojení s klientem informace na serverovém souborovém systému zpravidla v podobě malých textových souborů, serverových cookies. Ke klientovi se dostává pouze informace o jedinečném session ID. Session ID je na klienta předáváno buď jako cookie anebo jako součást URL adresy. (20) (21)

Příklad aktivního skriptu PHP verze 5:

Strana index.php

```
<?php
session_start(): //start session
session_register("jméno"): //registrace proměnné
$jmeno-"jakub": // přiřazeni hodnoty
?>
<a href-"next.php">Další</a>
```

Strana next.php

```
<?php
session_start(): / / s t a r t session
i f (session_is_regi steredí"jméno")):
echo $HTTP_SESSION_VARS["jméno"];
endif:
session_destroy();
?>
<a href-"test index.php">Start</a>
```

2.1.4.3 Cookies

Jedná se o přenos malého množství dat, které si klient udržuje na své straně. Název nemá český ekvivalent a překlad koláček, oplatka, sušenka je nevhodný. Myšlenku cookies navrhl v 90. letech Lou Montulli. Název cookie asociuje zvyklost ze Spojených států nebo Velké Británie nabídnout účastníkům určitého zájmového spolku nebo skupiny jejich oblíbenou sušenku pro vytvoření příjemnější atmosféry. (22) (21)

Cookie je zaslána klientovi s definovanou platností. Klient tak může při každé další návštěvě stejného serveru jednu nebo více cookie poslat serveru zpět a obnovit tak stav před opuštěním webových stran. (22)

2.1.4.4 Jedinečný identifikátor předávaný v URL

Metoda jedinečného identifikátoru zasílaná protokolem HTTP metodou GET se kvůli jednoduchosti pozměnění, proměnná je přímo vepsána do URL, příliš nepoužívá. Principem je vygenerování identifikátoru na základě provedené poslední akce a času. Vygenerovaný identifikátor se ukládá do databáze na straně serveru. Při pohybu uživatele po stránkách se uživateli předá identifikátor právě jako parametr v URL. Klient se dotazuje na novou HTTP stranu s tímto parametrem a server generuje nový identifikátor, který vrací klientovi. (21)

2.1.4.5 IP Adresa

Metoda založená na sledování IP adresy klienta je použitelná pouze v lokálních sítích. Vzhledem k omezenému počtu veřejných IP adres a zvyšování bezpečnosti lokálních sítí bývá použita pouze jedna veřejná adresa, prostředník ve formě Proxy serveru nebo Network Address Translation dále jen NAT serveru, pro více uživatelů. Tak je rozlišení jednotlivých klientů nejednoznačné a v praxi nepoužitelné. (21)

2.1.5 Způsoby zabezpečení webového serveru

U webového serveru komunikujícího protokoly HTTP nebo HTTPS musí být vždy dosažena rovnováha mezi dostupností a bezpečností. Každý webový server zpravidla běží pod operačním systémem, proto je nutné rozdělit zabezpečení na zabezpečení operačního systému a zabezpečení samotné aplikace webového serveru.

Server i aplikace musí být ošetřeny proti známým chybám. Musí být zavedena pravidla pro komunikaci protokolem TCP/IP. Musí být řízena oprávnění na úrovni webového serveru i samotného operačního systému tak aby se snížilo riziko napadení v případě chyby kódu webových stran. (23)

2.1.6 Způsoby zabezpečení webových stran

Webové servery dnes již výhradně používají aktivní webové strany, tj. strany kdy je obsah dynamicky generován na základě požadavků webového prohlížeče, klienta. Jednotlivé způsoby zabezpečení lze rozdělit dle použitého programovacího jazyka.

2.1.6.1 Nebezpečné úpravy kódu

Problém vzniká právě u programovacích jazyků, které jsou kompilovány až v momentě spuštění (PHP, ASP). Můžeme je dále rozdělit na úpravy kódu, kdy dojde k podstrčení proměnné nebo celého cizího kódu anebo vzdálenému spuštění kódu.

a) Podstrčení proměnných

Jde o specifický útok pro jazyk PHP, který využívá bezpečnostní mezery, vzniklé při použití direktivy register_globals. Tato direktiva automaticky převádí všechny hodnoty, získané z tzv. superglobálních proměnných (GET a POST data, SESSIONS, COOKIES) na globální proměnné pod patřičným názvem. Nejlepší obranou je, pokud máme tuto možnost, direktivu register_globals úplně vypnout a postarat se o příchozí data ze superglobálních proměnných pomocí polí $_GET, $_POST, $_SESSION a $_COOKIE. (24)

b) Podstrčení cizího kódu

Jedná se o extrémně nebezpečný útok, kdy je škodlivý kód podstrčen aplikaci s parametrem spuštění. Např. v PHP funkce exec(), která vykoná externí program nebo eval(), která vykoná jakýkoliv vložený PHP kód. Řešením je tyto funkce v PHP programu vůbec nepoužívat nebo zajistit taková oprávnění aby funkci nemohl spustit kdokoli. (24)

c) Vzdálené spuštění

Tento problém vzniká právě u PHP u interních příkazů include* a require*. Problém vzniká právě ve způsobu vkládání proměnných. Pokud bychom používali proměnné z metody GET protokolu HTTP, útočník jednoduše nahradí text URL výrazem např. /etc/pass, která na UNIXovém serveru vloží soubor s přihlašovacími intonacemi uživatelů (24). Vhodným ošetřením je odstranění cest z vkládaného souboru tj. zachování pouze jména souboru nebo povolit vkládání pouze s předdefinovaných seznamů.

2.1.6.2 Jiné útoky

a) Úprava protokolových hlaviček

Útok je založen na změnách hlavičky HTTP. Takto lze do hlavičky přidat vlastní řádky kódu. U HTTP hlavičky je problematický parametr „location“ sloužící k přesměrování prohlížeče na jinou URL adresu. Řešením je důsledná kontrola dat hlavičky a zákaz dělení řádků v hlavičce generované strany. (25) (24)

b) Zafixování session

Útok spočívá v tom, že třetí strana předgeneruje session ID a přesvědčí uživatele o jejím využití. Jakmile uživatel provede authentizaci tak může pod stejným session ID přistoupit na stránku také útočník. Zabránit útoku lze s použitím cookies a také v častém regenerování session ID. Po odhlášení uživatele je nutné také session ukončit. (24)

c) VIEWSTATE

VIEWSTATE je vlastnost specifická pro ASP.NET stránky. Jedná se o nástroj umožňující uchování stavu stránky a serverových objektů na ní umístěných mezi jejím opakovaným zpracováním jako skryté pole na stránce. Na rozdíl od jiných metod uchování stavu v ASP.NET aplikacích, které je možno použít v rozsahu platnosti uživatele aplikace (session) nebo celé aplikace (Application, Cache apod..) je tedy jeho platnost omezena pouze po dobu tohoto opakovaného zpracování jedné stránky. VIEWSTATE je využívána zejména pro uchování hodnot vlastností ovládacích prvků umístěných na stránce, ale lze ji samozřejmě také použít v kódu stránky. (24)

Problémem VIEWSTATE je, že standardně není šifrován. Proto není vyloučenou, že někdo může data ve VIEWSTATE pozměnit či přečíst. Řešení existují v podstatě dvě. Vytvoření otisku a porovnání otisku některou hashovaní funkcí nebo použitím šifrovacího algoritmu 3DES. (24) (24)

2.2 Metodika práce

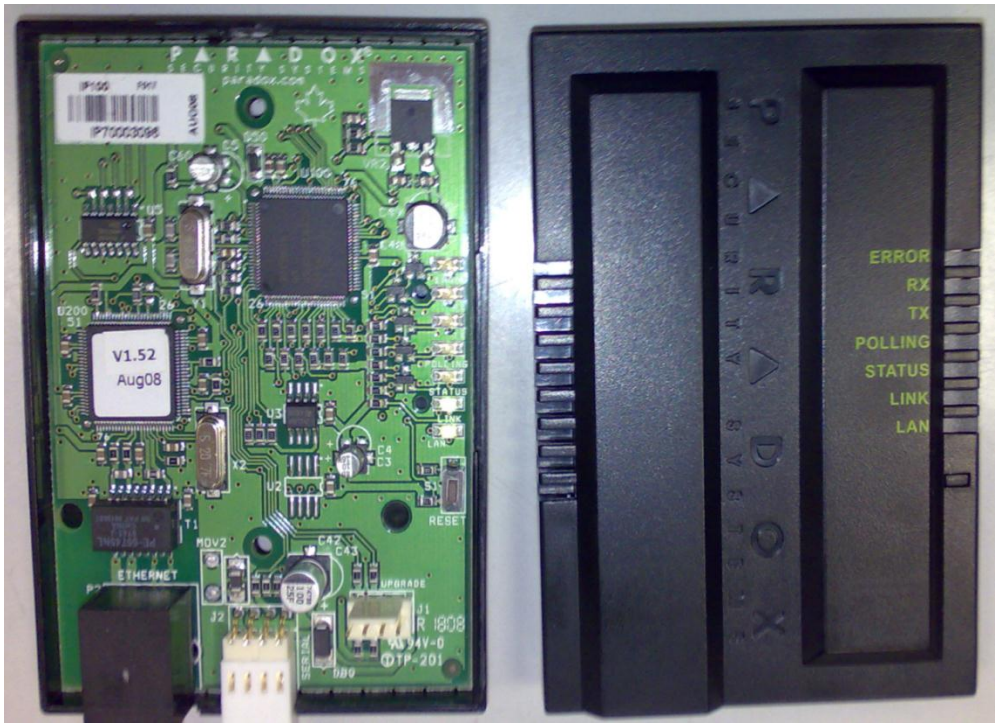
Na základě znalostí o stávajícím webovém modulu bude zvolen možný operační systém, pod kterým poběží aplikace – webový server.

Volba webového serveru bude provedena na základě požadavků, jako jsou operační systém, celková velikost software, podpora dynamického vytváření obsahu stran, bezpečnost a v neposlední řadě zda je software šířen jako otevřený pod některou z licencí pro svobodný software např. GNU General Public License či. GNU GPL „všeobecná veřejná licence GNU“. Pro webový server musí být zabezpečeno vydávání pravidelných nejen bezpečnostních aktualizací a musí splňovat alespoň pravidla uvedená v kapitole 2.1.5. s podporou uvedených autentizačních a autorizačních protokolů. Musí také umožnit vytvoření šifrovaného přenosového kanálu.

Na bázi volby webového serveru bude vybrán jazyk pro dynamické vytváření obsahu stran. Jazyk musí splňovat podmínky bezpečnosti a musí být odolný vůči možným útokům dle kapitoly 2.1.6.

3 Popis stávajícího řešení

Stávající řešení využívá modulu Kanadské společnosti Paradox Security Systems Ltd. pod označením IP100. Jedná se o zařízení, které je schopné komunikovat pomocí protokolu TCP/IP a ve vyšší vrstvě obsahuje jednoduchý webový server s podporou tvorby dynamických stran.



Obrázek 3 - modul IP100

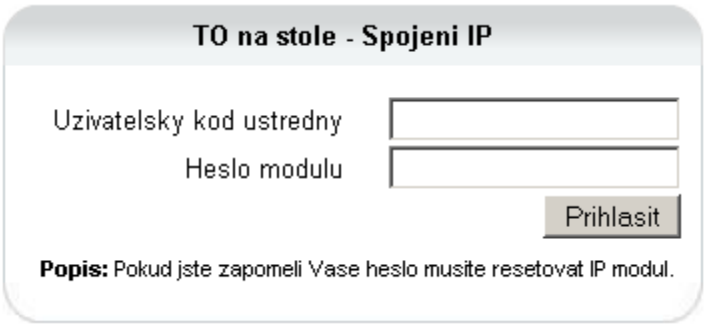
3.1 Ovládání ústředny EZS

Po zadání uživatelského kódu je možné zobrazit stav všech podsystémů ústředny a ovládat jednotlivě tyto podsystémy. Modul IP100 umožňuje za použití definovaného Simple Mail Transfer Protocol serveru dále jen SMTP serveru sestavit a odeslat emailovou zprávu na definované emailové adresy. Zprávy jsou vztažené k akcím ústředny: zapnuto, vypnuto, poplach, porucha a blokování přístupu do IP100. Jako doplňková funkce je zde možnost komunikace se softwarem stejného dodavatele WinLoad IP na separátním portu modulu.

Pro přístup z internetu v případě nestatické IP adresy modul nabízí dynamickou aktualizaci veřejných DNS záznamů, ale tyto záznamy jsou vedeny pouze u společnosti Paradox Security Systems Ltd. dále jen Paradox na stránkách www.paradoxmyhome.com. Modul je připojen šifrovanou sériovou linkou označenou jako SERIAL k EZS ústředně MG5000, z této ústředny je také napájen (26).

3.1.1 Autentizace a autorizace webové části modulu IP100

Přihlášení k HTTP webovému rozhraní je možné při znalosti uživatelského kódu ústředny a hesla modulu (Obrázek 4). Systém hesel je založen na databázi uživatelských účtů uložených přímo v ústředně a společném heslu, které je udržováno v modulu IP100 pro všechny uživatele.



Obrázek 4 - IP100 přihlášení

Role administrátor a uživatel nabízí dva pohledy. Jako administrátor je možné nastavovat veškeré parametry modulu, jako uživatel je možné si tyto parametry nechat zobrazit a měnit stav ústředny EZS pro jednotlivé podsystémy. Definování rolí je prováděno na základě připojené ústředny, kdy roli administrátor získává vždy uživatel se znalostí uživatelského kódu ústředny, tzv. „master kódu“, anebo kódu správce, „instalačního kódu“ EZS ústředny. Všichni ostatní uživatelé EZS ústředny mají, přístup pouze v roli uživatele (27).

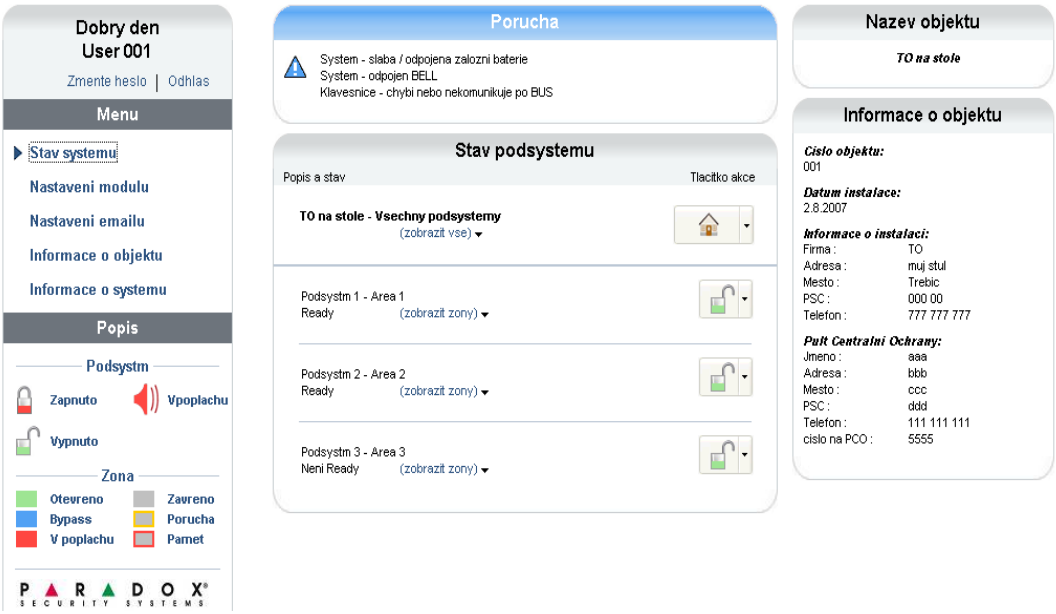
V testovaném provedení nabízí modul se softwarem verze 5. 02. 01 pouze jednouživatelský režim přihlášení s tím, že uživatel s nadřízenou rolí administrátora systému nemá možnost jiného přihlášeného uživatele jakkoli odhlásit. Veškerá HTTP komunikace je vedena na zvoleném portu jako nešifrovaná. Uživatelský kód ústředny a heslo modulu jsou z formuláře odesílány HTTP metodou GET v hashované a šifrované podobě (Obrázek 5) do modulu IP100. Hashovaní i šifrování uživatelského kódu a hesla modulu je prováděno skriptovacím jazykem na straně klienta. Lze tak snadno získat algoritmus šifrování a při odposlechu TCP/IP komunikace také veškeré přístupové informace. Uživatelské účty jsou dočasně zamykány po několika neúspěšných pokusech o přihlášení. Počet pokusů je řízen nastavením EZS ústředny. K odhlášení z modulu dochází při nečinnosti po 5 minutách nebo okamžitě při stisku tlačítka „odhlas“.

Obrázek 5 - IP100 přihlášení uživatele

Webové strany uložené v modulu IP100 využívají pro aktualizaci stavu skripty na klientské straně, straně webového prohlížeče. Jedná se o technologii nebo část technologie Asynchronous JavaScript and XML dále jen AJAX. Technologie umožňuje komfortnější zobrazování okamžitých stavů ústředny EZS. Přináší, ale vyšší nároky na webový prohlížeč klienta, vyžaduje podporu skriptovacího jazyka JavaScript. (27)

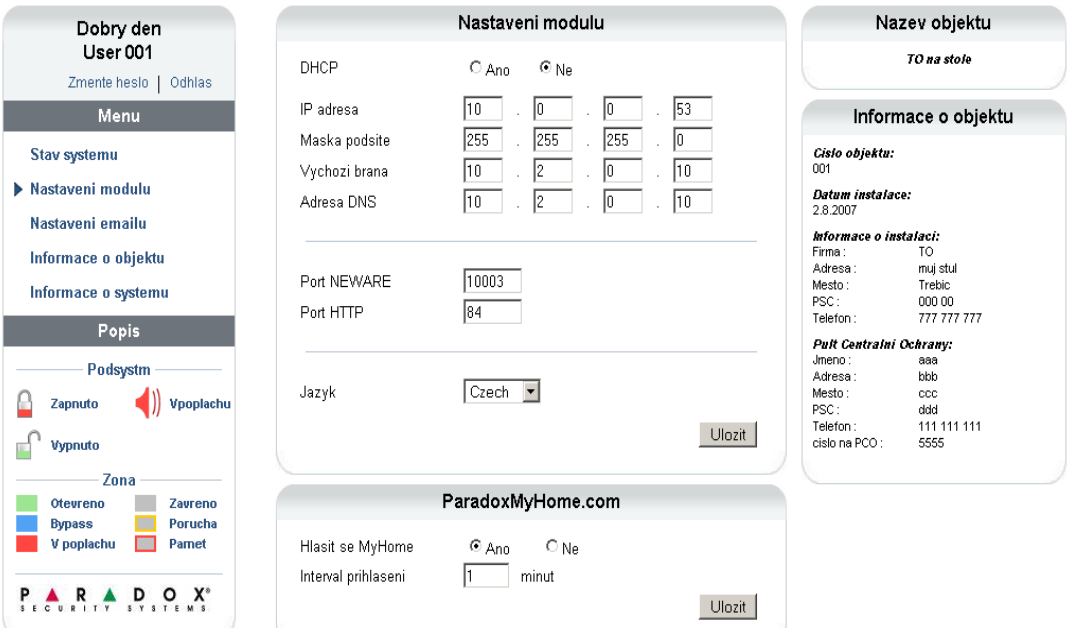
3.1.1.1 Role administrátor

Jak již bylo řečeno role administrátor je určena uživateli EZS ústředny se znalostí uživatelského kódu ústředny tzv. „master kódu“ anebo kódu správce, „instalačního kódu“. Výchozí obrazovka po přihlášení nabízí administrační menu s tabulkou piktografických značek a jejich krátkého slovního popisu. Dále pak pohled na aktuální stav systému a textové informace o objektu. Automaticky aktualizovaná část strany je prostřední horní část a levá část stran kde jsou zobrazeny aktuální stavové hlášky systému a stavy jednotlivých podsystémů (Obrázek 6).



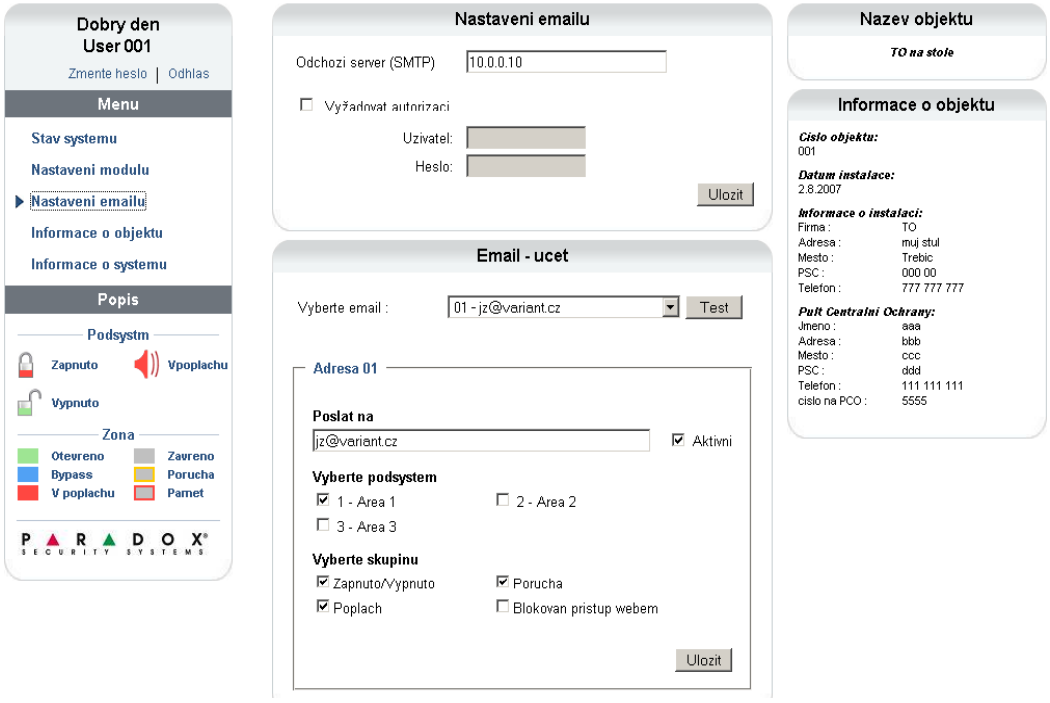
Obrázek 6 - výchozí pohled role administrátor

Po přechodu na nabídku nastavení modulu se zobrazí nabídka (Obrázek 7) určená pro nastavení TCP/IP protokolu a volba jazyka platná pro celý modul IP100. Sekce ParadoxMyHome.com je určena registrovaným uživatelům právě pro dynamickou aktualizaci doménových jmenných záznamů DNS.



Obrázek 7 - nastavení modulu

Nastavení emailu dle obrázku 8 vyžaduje zadání SMTP serveru, včetně ověření je-li požadováno. Následuje nastavení emailových účtů. Modul umožňuje uložení 16 emailových adres nezávislých na uživateli. Volba, za jakých podmínek se odešle emailová zpráva, je nastavitelná zaškrtávacími poli dle podsystémů ústředny a čtyř základních stavů - poplach, zapnuto a vypnuto, porucha, blokován přístup.

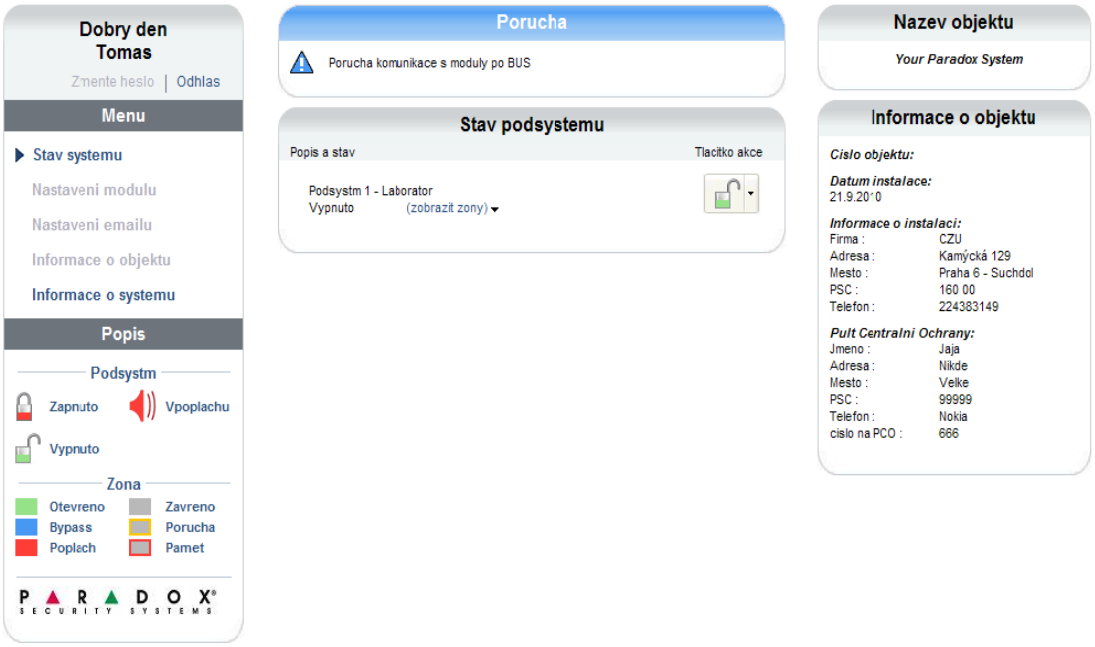


Obrázek 8 - nastavení emailu

Dále role administrátora umožňuje změnu jednotného hesla modulu platnou pro všechny uživatele, změny informací o objektu a zobrazení informací o IP100 a připojené EZS ústředně.

3.1.1.2 Role uživatel

Tato role poskytuje pouze přehled o stavu EZS ústředny a monitorovaném objektu a umožňuje také provádět změny v nastavení akcí na podsystémech. Výchozí pohled role se shoduje s administrátorskou rolí, pouze nejsou přístupné strany a menu určené pro nastavení modulu, emailu, hesla modulu a informacích o objektu. Náhled stran pro roli uživatele je na obrázku 9.



Obrázek 9 - IP100 role uživatel

3.1.2 Ovládání podsystémů

Modul IP100 umožňuje jakémukoli přihlášenému uživateli změnit stav podsystémů do výše oprávnění daných jeho uživatelským kódem a nastaveným oprávněním v EZS ústředně. Podsystémem se rozumí logicky uspořádaná skupina zabezpečovacích čidel a prvků, určených pro komunikaci s ústřednou, tzv. zón. Ovládání reprezentuje tlačítko akce dle obrázku 10. Tlačítko nabízí dle oprávnění volby: běžné zapnutí, stay zapnutí, zapnutí noc a vypnutí. Ovládat lze jednotlivé podsystémy ale také všechny podsystémy najednou.

Obrázek 10 - akce na podsystémech

Popisy zón a podsystémů jsou načítány z dat uložených v EZS ústředně. Do těchto textů není možné jakkoli zasahovat přes webové rozhraní.

3.2 Základní technická specifikace IP100

Modul IP100 je kompatibilní s ústřednami: EVO48 EVO192 SPECTRA SP 5500, 6000, 7000 MAGELLAN 5000, 5050. S ústřednami je propojen 4 vodičovou sériovou linkou, kde 2 vodiče slouží k napájení modulu (12V/ 110mA) a 2 datové. Hardware IP 100 obsahuje standardní RJ45 konektor pro připojení ethernetu a sériovou linku pro aktualizaci firmware modulu. Aktualizaci firmware je možné provést také přes TCP/IP a to jak lokálně tak vzdáleně přes NEWARE port, lze takto změnit či doplnit jazyk celého webu. V každém případě pro aktualizaci je vyžadováno heslo modulu. Výrobce uvádí podporu šifrování dat šifrou AES256, RC4 a hashovací funkci MD5. Ač se systém tváří jako více jazykový nemá podporu národního prostředí a jiného kódování jazyka. Podporu výrobce obchází nepoužíváním speciálních znaků a diakritiky typických pro různé jazykové verze. Kvůli aktivnímu skriptovacímu jazyku na straně prohlížeče, musí být použit pouze kompatibilní prohlížeč webových stran, jako jsou: Mozilla Firefox ve verzi 1,5 a vyšší anebo Internet Explorer ve verzi 6 a vyšší. (26)

3.3 Podrobný rozbor přihlašování k modulu

Jak již bylo řečeno zabezpečení přístupových informací, uživatelského kódu ústředny a hesla modulu je prováděno na straně klienta. Vyplnění přihlašovacích údajů je realizováno standardní formulářovou metodou, formulář je uložen v JavaScriptu, souboru login_page.js a odeslán přes před generovanou stranu login_page.html. Strana „login_page.html“ obsahuje volání funkce JavaScriptu:

function loginaff(sesv, errn, snme, user)
např.: loginaff("7E485E1BA46409CD",0,"Your Paradox System","€")

Zde je definován na první pozici klíč relace - session id, na druhé pozici je definován chybový stav přihlášení, dále jsou zde doplňkové texty pro označení ústředny a uživatele. V těle funkce loginaff je obsaženo volání funkce logc ta obsahuje HTML kód s formulářem pro zadání uživatelského kódu ústředny a hesla modulu. Jedná se o pole s identifikátory user a pass.

```
<form name='lf' action='default.html' method='get' onSubmit='return loginencrypt();'>
<input size=20 maxlength=6 type=password id=user>
<input size=20 maxlength=16 type=password id=pass>
<input type=submit name='loginsub' value='';sre+=parent.ln_logpage[0]+''>
<input type=hidden name='u' size=16>
<input type=hidden name='p' size=32>
<input type=hidden id='ses' size=32 value=''+sesv+''>
```

Před odesláním přihlašovacích dat modulu IP100, po stisku potvrzovacího tlačítka submit, je formulář zpracování JavaScript funkcí onSubmit='return loginencrypt();' Tato funkce zaručí zabezpečení přenášených informací. Pole pass je nejprve ošetřeno funkcí, která zabezpečí nahrazení znaků mimo American Standard Code for Information Interchange, dále jen ASCII tabulku, funkcí keeplowbyte. Samotné šifrování probíhá tak, že funkce hex_md5 vytvoří otisk hesla modulu IP100 a ten je doplněn do proměnné spass, která již obsahuje před generované session id. Z celé proměnné spass je nyní znovu vytvořen otisk funkcí hex_md5 a výsledný výraz je vložen do skrytého formulářového pole „p“. Uživatelský kód ústředny je vkládán do skrytého formulářového pole „u“ a šifrován algoritmem RC4 za použití klíče spass tj. hashovaného hesla modulu a sesion id.

```
s_low = top.keeplowbyte(document.lf.pass.value);
document.lf.pass.value = s_low;
temp = hex_md5(document.lf.pass.value);
spass = temp + document.lf.ses.value;
document.lf.p.value = hex_md5(spass);
document.lf.u.value = rc4(spass, document.lf.user.value);
document.lf.user.value = "";
document.lf.pass.value = "";
}
if(val == true)
{
document.lf.loginsub.disabled = true;
}
 return val;
```

Výsledný kód je zobrazen na obrázku 5. Tento kód je předáván metodou GET na server, modul IP100. Uvedený způsob zabezpečení zajišťuje ochranu před odhalením předávaného hesla modulu a také uživatelského kódu. Heslo modulu se přes HTTP protokol od klienta k serveru vlastně nepřenáší, přenáší se pouze otisk tohoto hesla vytvořený hashovacím algoritmem JavaScriptu.

3.4 Udržování přihlášeného uživatele a odhlášení uživatele

Pro udržení přihlášení uživatele modul opět používá JavaScript, který zabezpečuje pravidelné obnovování stran. Bezprostředně po přihlášení dochází k inicializaci modulu, jedná se o volání obsahu strany waitlive.html a po úspěšném přihlášení přechází k statuslive.html. Strana statuslive.html obsahuje skrytá formulářová pole, která jsou periodicky odesílána metodou GET na stranu serveru. Na straně serveru dochází k opakovanému porovnávání přihlašovacích údajů. JavaScriptem je dále nastaveno časové omezení pro přihlášení uživatele a bezpečné odhlášení při nečinnosti. Odhlášení je realizováno zavoláním strany logout.html ta obsahuje pouze směrovací skript:

```
<script language="javascript"type="text/javascript">
top.location.replace("login.html");</script>
```

Skript zajistí přesměrování na přihlašovací stranu login.html, tato strana vymaže nastavení proměnných „u“ a „p“ a také skrytých formulářových polí.

3.5 Rizika provozování WEB rozehranní IP100

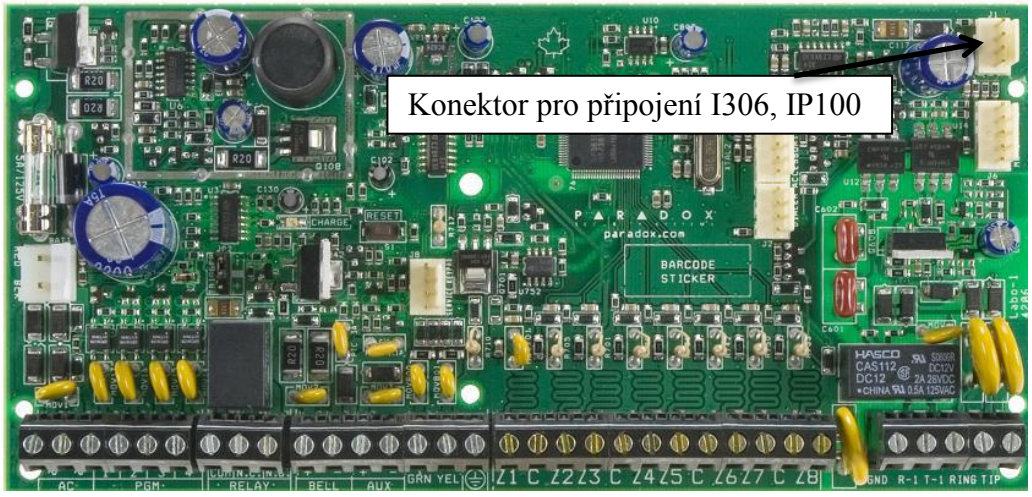
V případě modulu IP100 je několik rizik spojených s provozem a využíváním webového rozhraní. Většina s těchto rizik leží právě v způsobu útoku Man in the middle kdy je mezi komunikujícími stranami útočník, který odposlouchává komunikaci a aktivně se do ní také může zapojit. Tato rizika můžeme rozdělit do několika skupin:

1. Riziko odposlechu komunikace – spočívá v odposlechnutí komunikace a zjištění šifrovaných formulářových dat polí „p“ a „u“. Tato data sice nestačí k odhalení hesla modulu ani k odhalení uživatelského hesla. Stačí k přihlášení pod stejným session ID s právy platného uživatele.
2. Riziko pozměnění JavaScriptu – v případě jednoduché úpravy JavaScriptu, který je odesílán během načítání přihlašovací stránky je možné docílit zobrazení a odeslání všech přihlašovacích informací v nešifrované podobě.
3. Riziko podstrčení jiných stran – jelikož web server nepoužívá žádné z bezpečnostních protokolů, není možné ověřit jeho identitu, a proto není problém přesměrovat komunikaci např. změnou DNS záznamu nebo úpravou MAC adres.

4 Popis komunikace ústředny a interface

Komunikace je realizována sériovou linkou. Výrobce ji na ústřednách MG5000, MG5050 verze 3.00 a SP5500, SP6000, SP7000 verze. 3.00 a E55, E65 verze 2.00 označuje slovem SERIAL. Linka je vyhrazena pouze pro připojení modulu IP100 a modulu rozhraní I306 pro sériovou komunikaci s počítačem (Obrázek 11). Rozhraní je určeno pro konfiguraci ústředny a také pro aktualizaci firmware. (26)

Tato čtyř vodičová sériová linka poskytuje 2 vodiče pro napájení stejnosměrným napětím 12V, které slouží také pro napájení obou typů periférií. Další 2 vodiče jsou datové rozlišené směrem komunikace. Rozhraní nabízí pouze spojení bod - bod a není možné připojit oba moduly zároveň. Použitý komunikační protokol ani jeho vrstvy výrobce neuvádí.



Obrázek 11 - EZS ústředna SPECTRA SP

5 Definice zásad pro bezpečnou komunikaci

Z hlediska definování zásad pro bezpečnou webovou komunikaci si musíme nejprve stanovit co komunikace vlastně je a co není. Slovo „komunikace“ nemá jednoznačnou definici. Vyjdeme-li z latinského „communicare“ potom slovo znamená činit něco společným, společně sdílet. V užším pohledu vyjadřuje výměnu informací mezi účastníky komunikace. Účastnící komunikace si předávají žádoucí anebo očekávaná pravidla, podle nichž má probíhat komunikace a dále pak samotné informace. Informace zde vyjadřuje poměr známých před přijetím nové zprávy, vůči známému po jejím přijetí. Vztaženo k elektronické komunikaci můžeme říci, že účastníci si pomocí domluveného protokolu předávají informace. (28)

Bezpečná komunikace je komunikace doplněná o bezpečnost. Bezpečnost má několik definic. Obecně, bezpečný je ten, kdo není vystaven nebezpečí, popřípadě poskytuje ochranu před nebezpečím, nebo je nepochybný, zaručený, důvěryhodný. Dle Arnolda Wolferse (subjektivita bezpečnosti), bezpečnost není pouze objektivní, ale i subjektivní. Je absencí ohrožení vzácných hodnot (objektivní dimenze) i absencí vnímání ohrožení vzácných hodnot (subjektivní dimenze) (29). Vztaženo k elektronické komunikaci můžeme vyjádřit bezpečnou komunikaci, jako komunikaci kde se předpokládá existence:

1. předávání informací dle domluvených pravidel
2. ochrany před nebezpečím
3. nepochybnosti, zaručenosti a důvěryhodnosti komunikujících subjektů

Tedy bezpečná elektronická komunikace zahrnuje prostředky, s jejichž pomocí je možné sdílet informaci pouze s oprávněnými účastníky a to s různým stupněm jistoty. Neoprávněný účastník tak má ztíženu možnost získání obsahu komunikace.

5.1 Předávání informací dle domluvených pravidel

Webová komunikace vyjadřuje soubor domluvených pravidel. Tato pravidla jsou vyjádřena následujícími vymezeními:

Definice web, World Wide Web (WWW), je označení pro aplikace internetového protokolu HTTP dle specifikace RFC 2616 pro HTTP verze 1.1. (30)

Internetový protokol dále jen IP je datový přenosový paketový protokol, který tvoří základ dnešní komunikace – internetu. Vychází z rodiny protokolů TCP/IP definovaných pod RFC 1180. (31) Informace jsou tedy předávány bez stavovým HTTP protokolem. Je tedy nutné implementovat nepostradatelnou stavovost definovanou dle RFC 2965. (32)

5.2 Ochrana před nebezpečím

Nebezpečí lze v případě webové komunikace rozdělit do částí na nebezpečí vznikající na komunikujících stranách a mezi komunikačními stranami.

V případě webové komunikace tvoří komunikující strany poskytovatel hypertextových dokumentů – HTTP server a konzument, příjemce tedy klient těchto dokumentů. Mezi komunikujícími stranami se nachází komunikační protokol, nejčastěji TCP/IP.

5.2.1 Ochrana před nebezpečím na straně HTTP serveru

Server a samotný HTTP server musí splňovat tyto podmínky:

- Musí být bezpečný vůči již známým chybám.
- Musí mít definován systém oprávnění uživatele.
- Musí být přístupné pouze ty funkce serveru, které jsou používané.
- Musí být zavedena kontrola přístupu na server a logování událostí.

Způsoby ochrana byly popsány v kapitole 2.1.5 a 2.1.6. (23)

5.2.2 Ochrana před nebezpečím na straně klienta

Na straně klienta je situace složitější, jelikož klientem může být více aplikací pracujících s protokolem HTTP, klientská stanice zpravidla není určena pouze pro práci s webem (33). V zásadě platí obdobná pravidla jako pro server a HTTP server tj.:

- Klientská aplikace pro práci s HTTP musí být bezpečna vůči již známým chybám.
- Klientská stanice, operační systém musí být zabezpečen vůči již známým chybám.
- Musí být zavedena kontrola klientské stanice na škodlivý software, Malware.

- Musí být definována pravidla pro řízení komunikace mezi sítěmi.
- Musí být zavedena kontrola přístupu a logování událostí

5.2.3 Ochrana před nebezpečím mezi komunikačními stranami

Zde spočívá ochrana ve stanovení domluvených komunikačních pravidel. Aplikační protokol HTTP žádnou ochranu neposkytuje. Informaci je tak možné získat třetí stranou za použití běžných technických zařízení. Obecně lze rozdělit ochrany dle způsobu a objektu skrývaní:

- Skrytí obsahu nebo povahy komunikace (metody kryptografie)
- Skrytí stran komunikace (prevence identifikace, nebo anonymita)
- Skrýt, že ke komunikaci dochází (metody stenografie)

Jelikož je nutné dodržet standardy, pro webové prohlížeče je pro praktickou část použitelné pouze skrývání obsahu komunikace. Je tedy vhodné, aby bylo zajištěno:

- Zabezpečení komunikace pouze mezi oprávněnými stranami s určitým stupněm jistoty. Zavedením kryptografie, protokolu HTTPS (34).
- Zabezpečení nepochybnosti, důvěryhodnosti komunikujících subjektů. Např. ověřením subjektu třetí stranou.

5.3 Nepochybnost, zaručenost a důvěryhodnost komunikujících subjektů

Subjekty, které mezi sebou chtějí komunikovat, se musí vzájemně „představit“, ověřit autentičnost. V případě komunikace mezi subjekty však vzniká problém, kdy útočník může provést záměnu identity anebo ohrozit důvěryhodnost komunikujících stran.

Pro nepochybnost, zaručenost a důvěryhodnost komunikujících subjektů je vhodné zavést kontrolní mechanismus, který ověří nezávisle oba subjekty. Tento princip je zahrnut do komunikačního protokolu HTTPS ve specifikaci RFC 2660. (35)

6 Návrh struktury a vlastní realizace interface ústředny

Webové rozhraní ústředny vychází z webového rozhraní modulu IP 100 a rozšiřuje jeho použití. V návrhu je přihlédnuto k možnostem RISC procesoru M30624FGAFP dále jen MCU modulu IP100.

Volba operačního systému byla z důvodu možnosti multiplatformní integrace a integrace také s procesory RISC jednoznačná. Vybraný operační systém musí obsahovat monolitické jádro unixového typu. Z tohoto důvodu byl pro provoz aplikačního serveru Linux v 16 bitové verzi dle MCU (36).

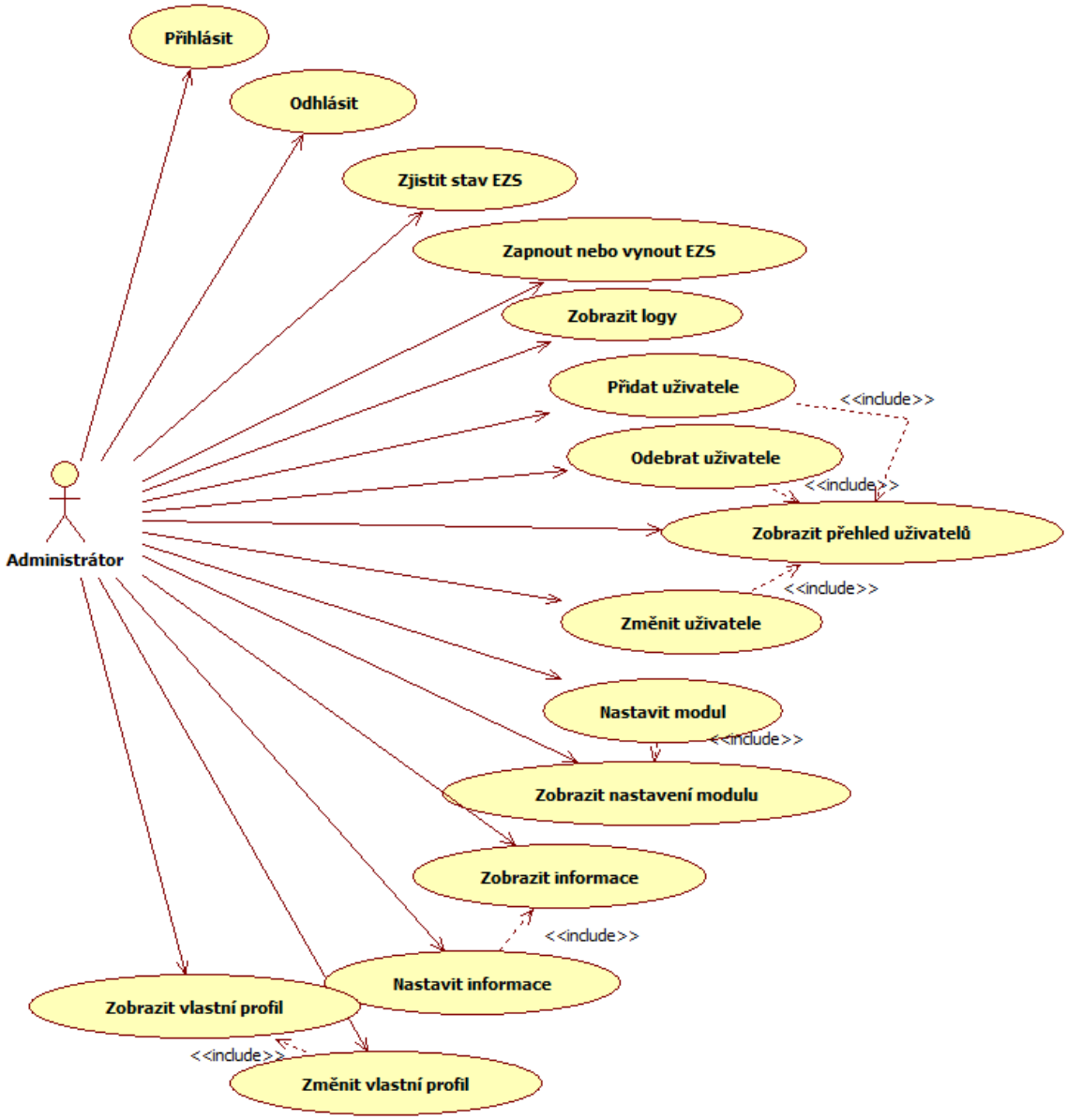
Volba HTTP serveru vychází z použitého operačního systému. HTTP server musí být modulární s podporou skriptovacích jazyků. Tj. používat Common Gateway Interface dále jen CGI dle standardu RFC3875 (37). HTTP serverů existuje pro linuxové prostředí celá řada. Rozhodujícími faktory byly možnosti získání zdrojového kódu HTTP serveru a jeho dalšího šíření nebo pozměňování pod GNU GPL licencí a možnost následné kompilace pro MCU. Proto byl zvolen HTTP server APACHE, v aktuální verzi 2. 2. 17. APACHE podporuje nejen CGI, ale také komunikaci Application Programming Interface dále jen API. Jako modul API byl zvolen jazyk PHP5.

Datová komunikace mezi modulem IP100 a ústřednou EZS není výrobcem dle dostupné dokumentace specifikována. Z tohoto důvodu je rozhraní realizováno jako otevřené ve formátu značkovacího jazyka XML.

6.1 Požadavky webového rozhraní

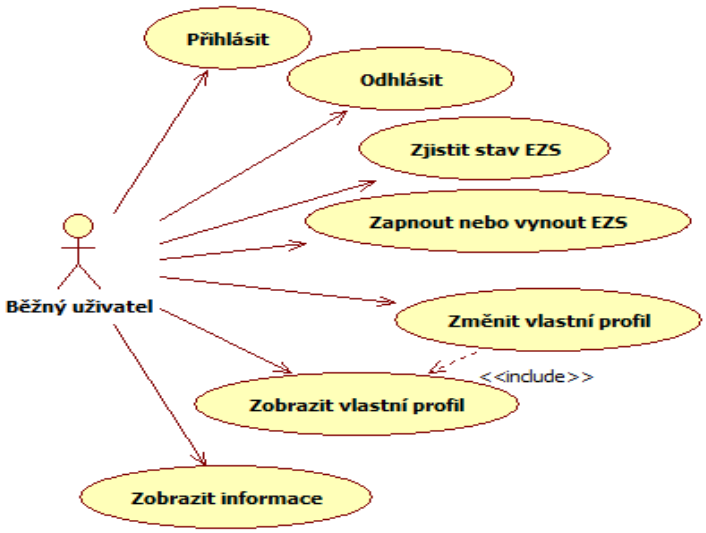
Pomocí webového rozhraní budou přistupovat uživatelé. Tyto uživatele lze rozdělit do několika typů-rolí dle očekávaného způsobu použití. (38)

Administrátor – držitel této role má znalosti o nastaveních modulu i ústředny a zajišťuje veškerá nastavení. Volitelně si přeje být informován převážně o technickém stavu ústředny. Informace požaduje také jinou cestou např. elektronickou poštou. Role uživatele umožňuje veškerá nastavení ostatních uživatelů a je porovnatelná s rolí správce dle dokumentace k ústřednám MAGELLAN MG5000, MG5050, SPECTRA SP5500, SP6000, SP7000 a ESPRIT E55, E65. Případy užití role jsou uvedeny na obrázku 12.



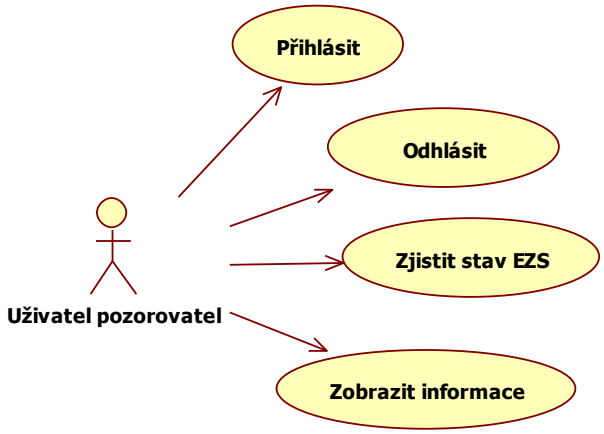
Obrázek 12 - role Administrátor

Běžný uživatel – (obrázek 13) jako běžný uživatel byl označen uživatel, který k systému přistupuje z důvodů zapnutí nebo vypnutí EZS a požaduje zobrazení informace o stavu monitorovaného objektu včetně informací o stavu monitorování tj. technickém stavu ústředny, periférií a také stavu vlastního uživatelského účtu. Uživatel nemusí mít znalosti správy modulu ani ústředny. Uživatel si také volitelně přeje být informován jinou cestou, např. elektronickou poštou anebo formou krátké textové zprávy SMS.



Obrázek 13 - role Běžný uživatel

Uživatel pozorovatel – role určená pro dohled z pultu centralizované ochrany v případě vyvolání poplachového stavu v objektu (Obrázek 14). Tato role umožňuje podrobný přehled o stavu jednotlivých zón a celkový přehled o systému bez možnosti provádět aktivní operace.



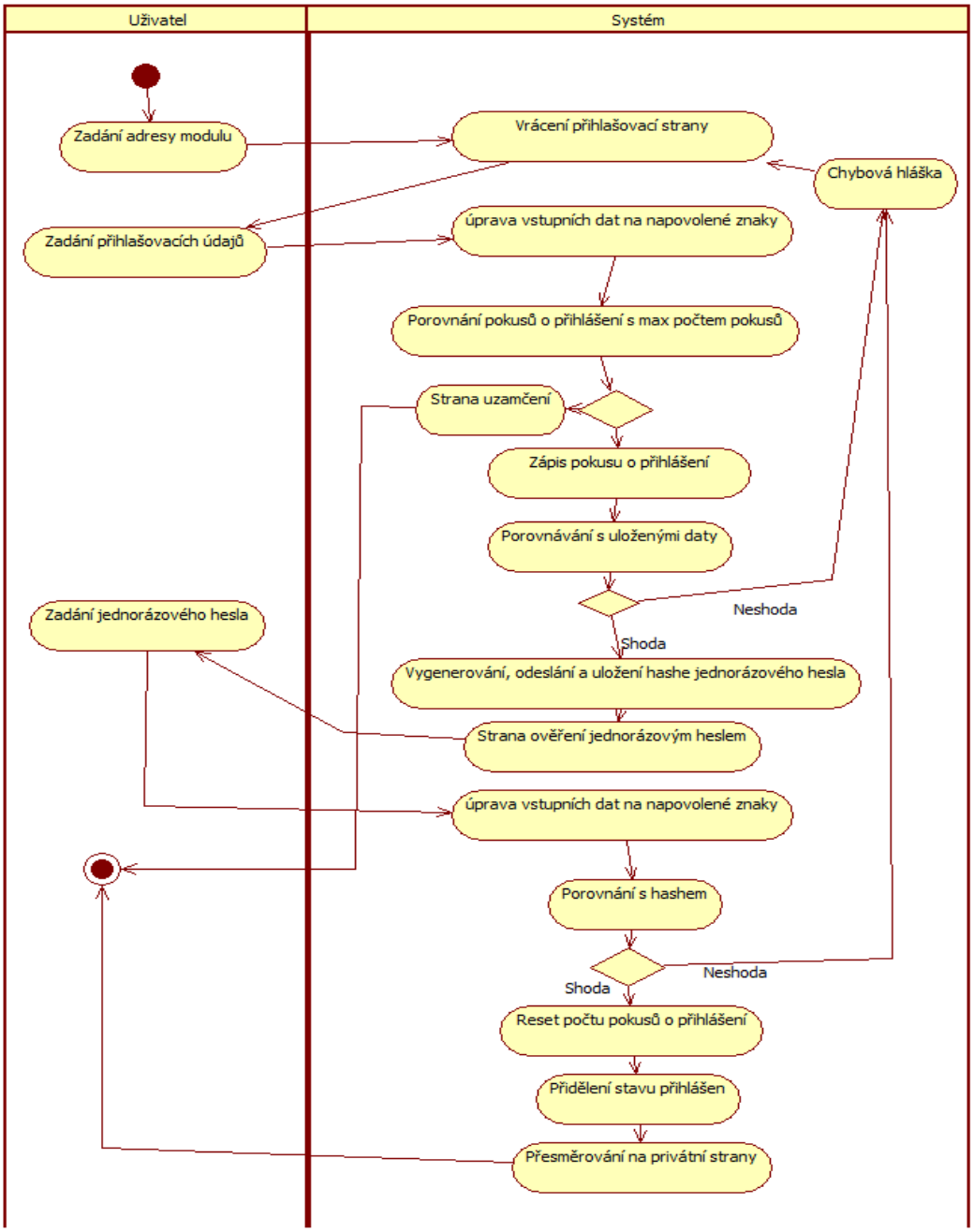
Obrázek 14 - role Uživatel pozorovatel

6.2 Rozbor případů užití

V rozboru jsou pomocí diagramu aktivit znázorněny složitější případy užití. Ostatní případy jsou specifikovány strukturovanými texty. (38)

6.2.1 Přihlásit

Kvůli zvýšení bezpečnosti je pro autentizaci přidáno kromě standardního uživatelského přihlašovacího jména a hesla také generování jednorázového klíče. Klíč po prvotní autorizaci je předáván jiným komunikačním kanálem. V návrhu je zvolen mailový kanál. Zároveň je pro ochranu stávajících uživatelů porovnáván počet pokusů o přihlášení a v případě překročení je účet trvale uzamčen.



Obrázek 15 - případ užití Přihlásit

6.2.2 Odhlásit

V případě, že má uživatel přidělen stav přihlášen, může požadovat odhlášení. To proběhne buď po provedení akce uživatelem anebo při nečinnosti, kdy je přidělený stav uložen s omezenou časovou platností po uplynutí dojde k zrušení tohoto stavu.

ID	Role	Akce
1	uživatel	zadání webové adresy odhlášení nebo volba menu odhlásit
2	systém	zobrazí odpověď ve formě informace o odhlášení strany a zruší přidělení stavu přihlášen

Tabulka 1 - případ užití Odhlásit

6.2.3 Zjistit stav EZS

Patří mezi základní funkčnosti. Uživateli je zobrazen aktuální stav po přihlášení v oblasti hlavičky webové strany. Obdobného zobrazení lze dosáhnout tímto případem.

ID	Role	Akce
1	uživatel	volba uživatelského menu stav systému
2	systém	prověření oprávnění zobrazí stranu stav systému

Tabulka 2 - případ užití Zjistit stav EZS

6.2.4 Zapnout nebo vypnout EZS

Případ užití používá případu Zjisti stav EZS a dle nastavených oprávnění umožní uživateli systému měnit stav EZS.

ID	Role	Akce
1		VLOŽENO - Zjisti stav EZS
2	uživatel	výběr stavu a odeslání
3	systém	prověření oprávnění, změna stavu a vracení strany potvrzení

Tabulka 3 - případ užití Zapnout nebo vypnout EZS

6.2.5 Zobrazit logy, informace, modul, vlastní profil a přehled uživatelů

Uvedené případy užití mají téměř shodnou textovou specifikaci. Specifikace se liší pouze ve volbě uživatelského menu. Z tohoto důvodu je zbytečné ji uvádět samostatně.

ID	Role	Akce
1	uživatel	volba uživatelského menu pro jednotlivé typy případů užití
2.1	systém	KDYŽ prověření oprávnění v pořádku, zobrazí stranu stav systému
2.2	systém	KDYŽ prověření oprávnění chyba, zobrazí prázdnou stranu

Tabulka 4 - případ užití Zobrazit

6.2.6 Nastavit informace, modul, změnit vlastní profil, přidat uživatele

Také u těchto případů užití je shoda opět s rozdílem ve volbě menu a v prováděných serverových operacích.

ID	Role	Akce
1		VLOŽENO - zobrazit
2	uživatel	výběr prováděné akce
3	systém	prověření oprávnění, zobrazení formuláře pro nastavení
4	uživatel	vyplnění/změny formuláře a odeslání
5.1	systém	KDYŽ ověření oprávnění, ověření obsahu, uložení v pořádku, dojde k zobrazení potvrzení
5.2	systém	KDYŽ ověření oprávnění, ověření obsahu, uložení obsahuje chybu, dojde k zobrazení informace o chybě

Tabulka 5 - případy Nastavit informace, modul, změnit vlastní profil, přidat uživatele

6.2.7 Odebrat uživatele a změnit uživatele

Tyto případy jsou určeny pouze pro správce a slouží k úpravám všech záznamů stávajících uživatelů. V případě odebrání přihlášeného uživatele anebo změně hesla tohoto uživatele dojde k jeho odhlášení.

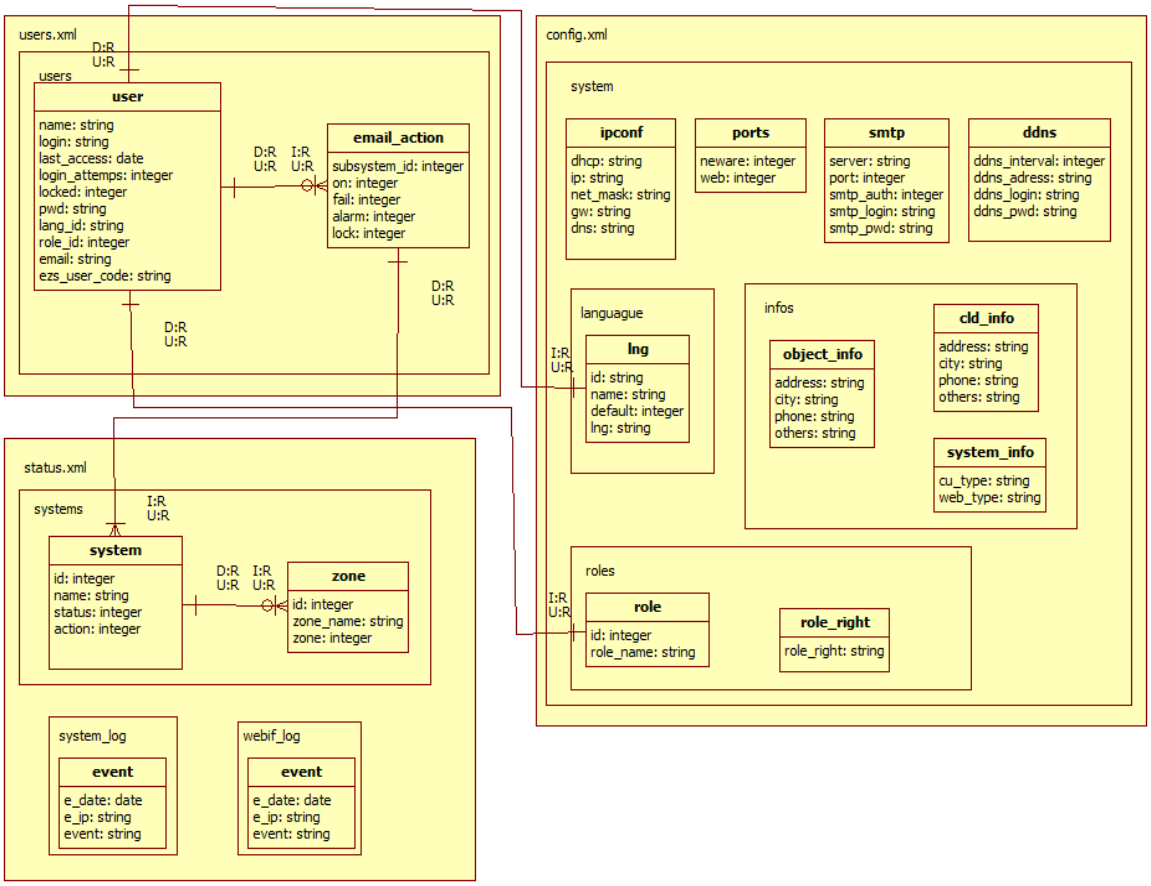
ID	Role	Akce
1		VLOŽENO - přehled uživatelů
2	uživatel	výběr uživatele z přehledu stisk tlačítka editace nebo mazání
3	systém	prověření oprávnění, zobrazení formuláře pro nastavení nebo formuláře pro potvrzení výmazu
4	uživatel	odesílá upravený formulář nebo potvrdí výmaz
5.1	systém	KDYŽ ověření oprávnění, ověření obsahu, uložení/výmaz v pořádku dojde k zobrazení potvrzení
5.2	systém	KDYŽ ověření oprávnění, ověření obsahu, uložení/výmaz obsahuje chybu dojde k zobrazení informace o chybě

Tabulka 6 - případy odebrat a změnit uživatele

6.3 Datový model

Datový model zahrnuje správu uživatelů, monitoring stavu EZS a samotné nastavení EZS i modulu. Celý systém je vytvořen s kódováním UTF-8 dle specifikace ISO 10646. To umožňuje rozšířenou podporu specifických národních znaků.

Použitý model nabízí možnost oddělit uživatele EZS od uživatelů webového rozhraní. Uživatelé webového rozhraní mohou k EZS přistupovat nezávisle na přihlášení ostatních uživatelů, mají možnost výběru jazyka a vlastního nastavení emailových notifikací. Vyspecifikované role jsou rozlišeny do úrovní dle přístupového listu ACL. Podle rolí je rozhodováno, zda má přihlášený uživatel právo danou operaci provést anebo zda se specifikovaná nabídka zobrazí. (18)



Obrázek 16 - datový model

Datový model na obrázku 16 je založen na XML souborech users.xml, config.xml a status.xml. Soubory jsou uloženy v souborovém systému mimo sdílený webový prostor v místě kam uživatel operačního systému, modul PHP, má udělen přístup pro operace čtení i zápis.

6.3.1 Uživatelé - users.xml

Soubor je určen k uchování informací o nastavení uživatele webového rozhraní, zajišťuje propojení uživatele s uživatelským kódem databáze EZS ústředny a definuje roli uživatele, jazyková nastavení a nastavení událostí při, při kterých má být uživatel kontaktován.

V souboru jsou uloženy následující informace:

- zobrazované jméno uživatele „name“
- přihlašovací jméno „login“
- počet neúspěšných pokusů „loggin_attemps“ a poslední úspěšné přihlášení
- zámek účtu „locked“
- otisk uživatelského hesla „pwd“
- identifikátor jazyka „lang_id“
- identifikátor role uživatele „role_id“
- email nebo emaily uživatele v „email“
- uživatelský kód ústředny „ezs_user_code“
- definice mailových akcí pro subsystémy EZS „email_action“

6.3.2 Nastavení – config.xml

Soubor slouží pro uložení veškerých nastavení modulu, jako jsou: nastavení parametrů protokolu TCP/IP, nastavení dynamických změn IP adresy akceptovatelných DNS serverem, nastavení pro emailovou komunikaci, definice rolí, povolených jazykových mutací stran a zobrazovaných informací.

V souboru jsou uložena data:

- povolena konfigurace DHCP „dhcp“
- uložená nebo DHCP nastavená IP adresa „ip“
- síťová maska „net_mask“
- výchozí brána podsítě „gw“
- nastavení DNS „dns“
- porty modulu pro software neware a webového serveru „ports“
- nastavení dynamického DNS „ddns“

- nastavení SMTP serveru
- definované povolené jazyky „languague“
- definice rolí uživatel „roles“
- informace o objektu, systému a pultu centralizované ochrany „infos“

6.3.3 Nastavení – status.xml

Toto úložiště obsahuje informace o stavu ústředny do úrovně jednotlivých zón a nastavuje požadovanou akci uživatele. Dále je soubor úložištěm logu ústředny.

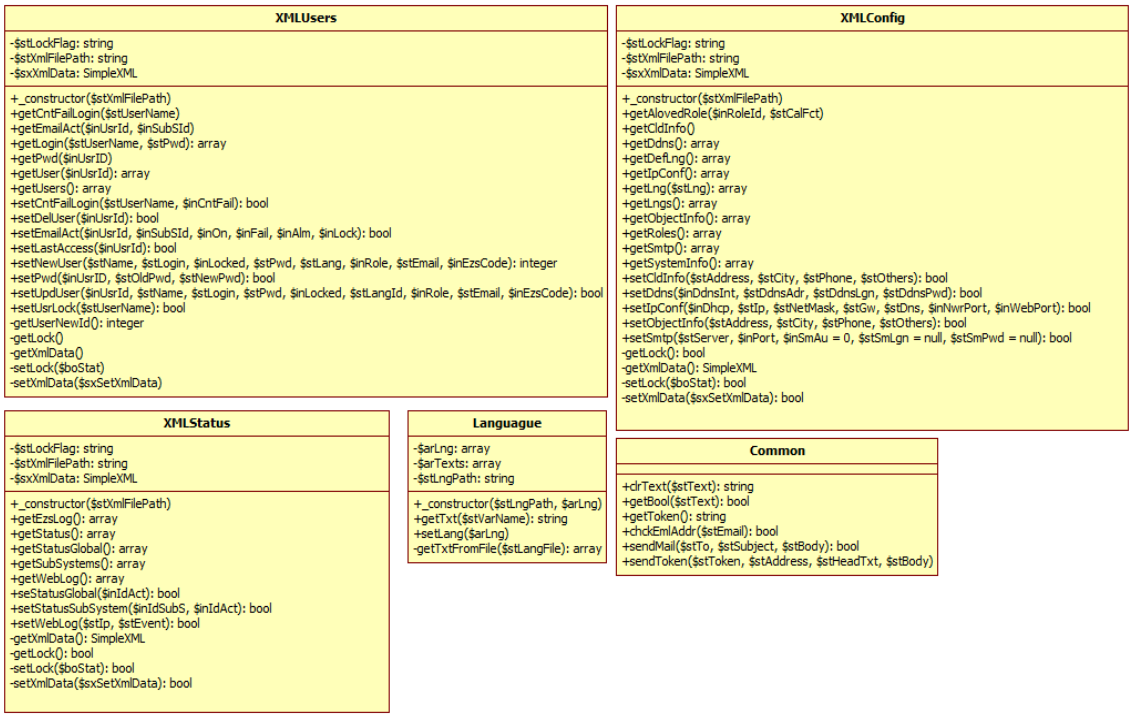
Soubor zahrnuje:

- Název systému a jeho identifikátor „system“
- Stav systému „status“
- Požadovanou akci „action“ a žadatele „ezs_user_code“
- Definici zón systému nebo podsystému její název a stav „zone“

6.4 Diagram tříd

Při návrhu byl použit návrhový vzor Model-View-Controller dále jen MVC. (39) Vzor rozděluje aplikaci do tří částí, které jsou navzájem propojené. Část Model obsahuje logiku ukládání a načítání dat z XML souborů tato logika je načítána jako externí soubor ke každé webové straně. Část View a Controller zajišťuje komunikaci s uživatelem a je uložena přímo v jednotlivých stranách případně dle povahy je uložena v společné části Model.

Rozdělená aplikace dle tohoto modelu je snáze upravitelná pro případ změny nebo nahrazení datového modelu XML. Část Model obsahuje třídy, funkce a proměnné dle obrázku 17, rozdělené dle datového modelu. Část View a Controller propojuje část Model a je unikátní pro každou webovou stránku, dle požadavků na zobrazení a interakci uživatele.



Obrázek 17 - diagram tříd pro část „Model“

Třídy XMLUsers, XMLStatus a XMLConfig jsou určeny pro práci s XML soubory a implementují v sobě metody kontroly přístupu k vyžádanému úložišti. Při žádosti o přístup je nastaven parametr, „lock“ a po ukončení práce se soborem je tento parametr vymazán. Třída Languague v sobě implementuje funkce pro získání textů v různých jazykových variantách Webu. Třída Common obsahuje funkce pro mailovou komunikaci, generátor náhodného řetězce a funkce pro práci s textem. (40) (41)

6.5 Struktura dat z pohledu souborového systému

Výchozí adresář obsahuje PHP skripty, ve kterých jsou připraveny HTML kódy pro přímé generování webových stran. Ostatní objekty jsou popsány v tabulce 7.

Objekt	Typ	Práva	Popis
_lgusr.php	skript PHP	WEB	strana pro dynamické načítání přihlášených uživatelů
_status.php	skript PHP	WEB	strana pro dynamické načítání stavu systému
_syslog.php	skript PHP	WEB	strana pro dynamické načítání systémového logu
conf\	adresář	PHP	obsahuje konfigurační xml soubory
conf\config.xml	XML	PHP	datový soubor s nastavením modulu
conf\status.xml	XML	PHP	datový soubor stavu
conf\users.xml	XML	PHP	datový soubor uživatelé
img\	adresář	WEB	obrázky pro webové strany
img\alarm.png	obrázek	WEB	obrázek stavu
img\alarm_history.png	obrázek	WEB	obrázek stavu
img\alarm_small.png	obrázek	WEB	obrázek stavu
img\alarm_zone.png	obrázek	WEB	obrázek stavu
img\bypas.png	obrázek	WEB	obrázek stavu
img\closed.png	obrázek	WEB	obrázek stavu
img\corners.gif	obrázek	WEB	obrázek designu
img\fail.png	obrázek	WEB	obrázek stavu
img\info.png	obrázek	WEB	obrázek stavu
img\locked.png	obrázek	WEB	obrázek stavu
img\open.png	obrázek	WEB	obrázek stavu
img\unlocked.png	obrázek	WEB	obrázek stavu
inc\	adresář	WEB	vkládané PHP strany vícenásobně použité
inc\footer.inc.php	skript PHP	WEB	pata všech webových stran
inc\header.inc.php	skript PHP	WEB	hlavička všech webových stran
inc\jquery.min.js	skript JS	WEB	externí skript pro skriptování na straně klienta
inc\lmenu.inc.php	skript PHP	WEB	menu všech webových stran
inc\status.inc.php	skript PHP	WEB	stav všech webových stran
index.php	skript PHP	WEB	přihlašovací webové strany
infos.php	skript PHP	WEB	webové strany informací o systému a jejich nastavení
lang\	adresář	WEB	soubory pro jazykové verze
lang\cs.ini	INI	WEB	jazyková verze CS
lang\en.ini	INI	WEB	jazyková verze EN
logoff.php	skript PHP	WEB	odhlašovací strana
logs.php	skript PHP	WEB	strana pro práci s logy
main.php	skript PHP	WEB	webové strany pro zobrazení a zapínání/vypínání EZS
plugins\	adresář	WEB	PHP strany pomocných i hlavních funkcí
plugins\define.php	skript PHP	WEB	konfigurační soubor s nastavením pomocných proměnných
plugins\function.php	skript PHP	WEB	hlavní funkce programu
profile.php	skript PHP	WEB	strany pro zobrazení anebo editaci vlastního profilu
Robots.txt	txt	WEB	soubor pro nastavení zákazu přístupu webových vyhledávačů
styleset.css	soubor CSS stylů	WEB	soubor kaskádových stylů
system.php	skript PHP	WEB	strany zobrazení a nastavení systémových proměnných
users.php	skript PHP	WEB	strany pro správu uživatelů

Tabulka 7 - struktura dat na souborovém systému

6.5.1 Uložení proměnných mimo XML soubory

Mimo konfigurační soubory jsou uložena základní data určená pro vyhledání vkládaných konfiguračních souborů, anebo taková data, kde nedochází k podstatným změnám při provozu aplikace. Přehled včetně popisu je uveden v tabulce 8.

Definice	Popis
define('PATH_INC', "inc");	cesta pro vkládané PHP strany vícenásobně použité
define('PATH_CONF', "conf");	cesta pro konfigurační xml soubory
define('PATH_LANG', "lang");	cesta pro uložení jazykových mutací
define('FILE_CONF', "config.xml");	název konfiguračního souboru nastavení
define('FILE_USR', "users.xml");	název konfiguračního souboru uživatelé
define('FILE_STAT', "status.xml");	název konfiguračního souboru status
define('LOGIN_ATTEMPS', 3);	počet pokusů pro zamčení účtu
define('TOKEN_LENGHT', 8);	délka posílaného jednorázového hesla
define('CASCSTYLE', "styleset.css");	definice kaskádových stylů
define('LIFETIME', 1000);	doba odhlášení ve vteřinách
define('DATE_FORMAT', "d.m.Y H:i:s");	formát datumu pro zobrazení
define('REFRESH_TIME', 30000);	doba obnovy automaticky načítaných stran
define('LOGCOUNT', 20);	max. počet záznamů logu než dojde k přepisování
define('EMAIL_FROM', "ezs@ezs.cz");	mailová adresa odesílatele událostí

Tabulka 8 - proměnné mimo XML

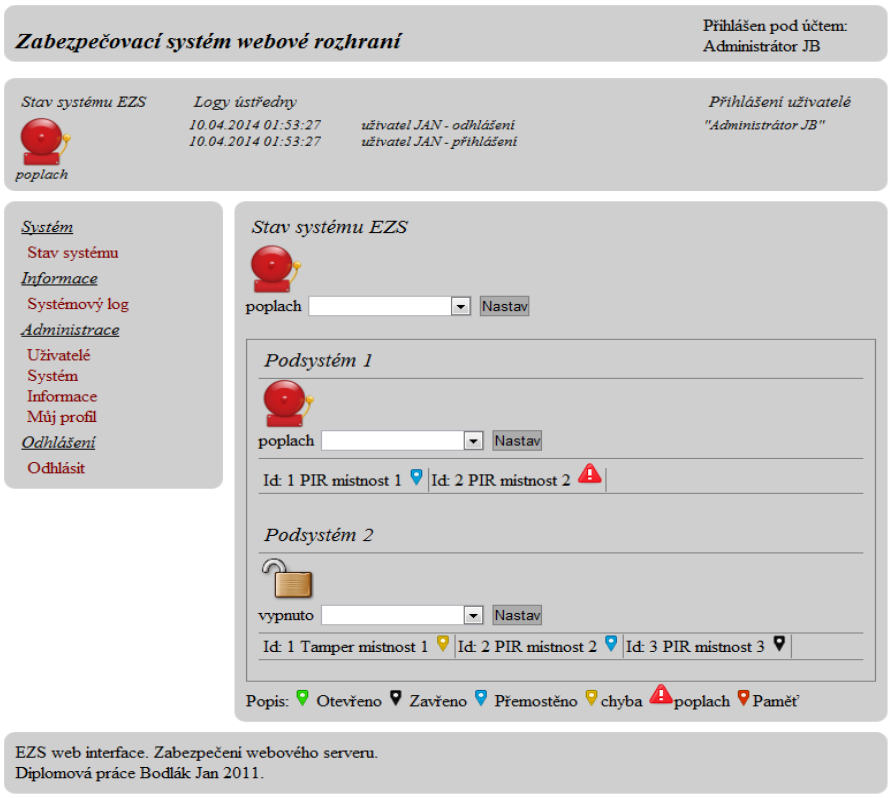
6.6 Zobrazení v prohlížečích a design

Aplikace používá pro zobrazení HTML 4.0 Transitional. Všechny dynamicky vytvářené strany byly s touto verzí validovány na stranách konsorcia W3C (World Wide Web Consortium). Pro zobrazení je nutné používat kompatibilní prohlížeč. Do stran byly implementovány metody pro automatickou obnovu stran a to v několika stupních.

1. Jako základní stupeň je pro obnovení stavu voleno použití odkazu a po otevření nového okna kódem „<a href="_strana.php" target="_blank …“ je následně toto okno prohlížeče obnovováno použitím „<meta http-equiv='refresh' …“.
2. V případě, že prohlížeč podporuje metodu vkládání stran IFRAME je použita strana základního stupně a vložena do obsahu hlavní strany. Automatická obnova stavu strany probíhá shodně.

3. Poslední dnes již nejčastěji používanou variantou je klientské skriptování za použití JavaScriptu. Pro aktualizaci je v tomto případě použita volně šiřitelná a modifikovatelná knihovna skriptů JQuery. Knihovna je dostupná ze stran http://jquery.com/.

Design je vytvořen za použití kaskádových stylů. Zobrazení bylo testováno v prohlížečích: Internet Explorer 8, Mozilla Firefox 3.6 a Google Chrome 10.0. Pro zmenšení datové velikosti stran bylo pro účely designu použito 12 obrázků, z toho 11 je použito pro ilustraci stavu EZS ústředny. Náhled designu je patrný z obrázku 18.



Obrázek 18 - design stran

6.7 Bezpečnost stran

Jak již bylo uvedeno, přihlášení je realizováno dvěma různými cestami (obrázek 19), a to zadáním uživatele a hesla. V případě že je zadání totožné s daty v úložišti, probíhá druhá část ověření. Ta spočívá v odeslání generovaného jednorázového hesla elektronickou poštou.

Obrázek 19 - ověření přihlášení

Přihlašování je tedy formulářové a stavová data jsou uchovávána v sessions. Je zavedena automatická změna identifikátoru session při každé návštěvě nebo obnově strany. Stavová data neobsahují kompletní uživatelské informace vhodné pro přihlášení a bez znalosti algoritmu nelze upravit stav nepřihlášeného uživatele. Zobrazení každé webové strany přihlášeným uživatelům je monitorováno, stejně tak i příchod a odchod z těchto stran. Z důvodů kompatibility nejsou přenášená data na straně klienta šifrována. Šifrovací algoritmus je použit pouze pro skrytí uložených a uživatelských hesel a stavu přihlášen na straně serveru. Konkrétně zde vystupuje hashovací funkce MD5.

6.8 Konfigurace webového serveru

Webový server zajišťuje kromě samotné HTTP komunikace, také šifrování přenášených dat. Šifrování je z důvodu kompatibility realizováno bezpečnostní nadstavbou protokolem HTTPS. Webový server má také nastavenu podporu PHP. Pro šifrování mezi komunikujícími stranami protokolem HTTPS je využito asymetrické šifrovací techniky. Potřebujeme tedy pár veřejný a soukromý klíč. V případě, že budeme chtít předejít útoku typu Man in the middle musí být tento veřejný klíč digitálně podepsán certifikační autoritou. Pro účely testování byl vygenerován tzv. self-signed certifikát tj. certifikát, který je podepsán jeho vydavatelem – tvůrcem.

6.8.1 Konfigurace apache

Minimální konfigurace obnáší zakázání protokolu HTTP, nastavení protokolu HTTPS a nastavení cest k webovým stranám. Hlavní konfigurační soubor apache je soubor httpd.conf zde je povolen modul určený pro nadstavbu HTTPS: LoadModule ssl_module mod_ssl.so a modul pro PHP: LoadModule php5_module libphp5.so. Dále jsou přidány následující řádky pro spuštění virtuální HTTPS serveru. (42)

```
<virtualhost *:443>
 DocumentRoot "/cesta k adresáři se stranami"
```

```
 ErrorLog "/cesta k apache logs error.log"
 TransferLog "/cesta k apache logs access.log"
SSLEngine on
SSLCertificateFile "/cesta k  certifikátu"
SSLCertificateKeyFile "/cesta k privátnímu klíči"
 </virtualhost>
```

6.8.2 Konfigurace PHP

V hlavním konfiguračním souboru php.ini je nutná změna zobrazování chybových hlášek „error_reporting“ jinak není vyžadována žádná speciální konfigurace. (43)

7 Literární rešerše

Webové moduly, určené k ovládání EZS se objevují u většiny výrobců zabezpečovacích zařízení. Zaměřením jsou tyto moduly spíše směřovány k instalačním firmám a možnostem vzdáleného nastavování ústředen.

7.1 Jablotron JA-80V

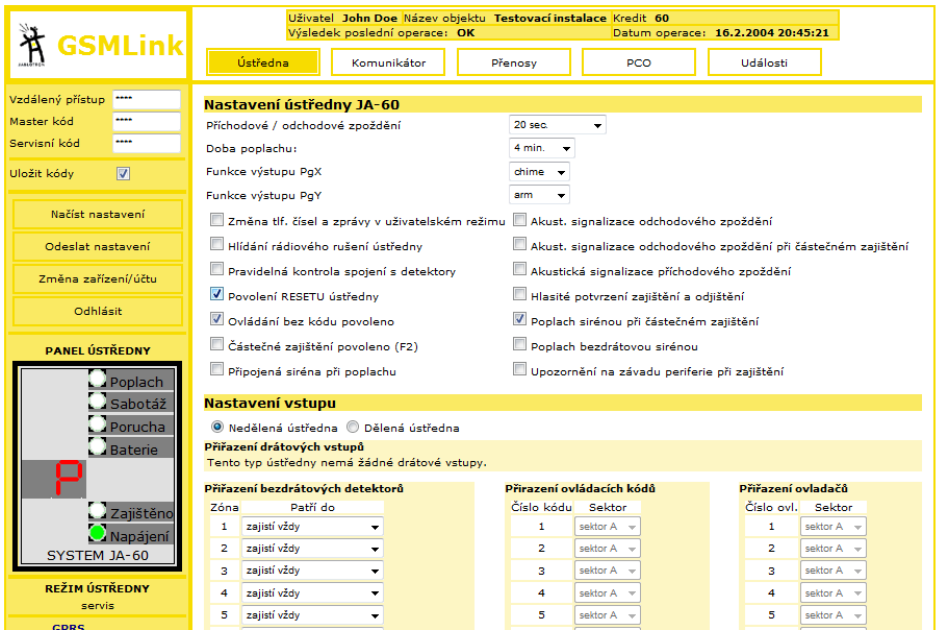
Modul JA-80V je kombinovaný komunikátor LAN a telefonní linka. Umožňuje dálkové ovládání systému telefonicky nebo přes internet. Modul obsahuje také telefonní hlásič. Připojení je proveditelné přes sítové rozhraní typu ethernetu konektorem RJ45 a analogovou telefonní linkou konektorem RJ 11. Instaluje se přímo do skříně ústředny EZS. Základní funkčnosti dle výrobce jsou:

- reportovat události formou SMS zpráv (až na 8 tel. čísel)
- reportovat události zavoláním a předáním akustického signálu
- předávat data na pult centrální ochrany (PCO), až 2 pulty
- dálkově ovládat a programovat systém telefonem (zavoláním a použitím klávesnice telefonu nebo pomocí SMS příkazů)
- dálkově ovládat a nastavovat systém z Internetu (www.GSMlink.cz)
- komunikátor lze připojit také pouze jen k telefonní lince, nebo jen k síti LAN. V takovém případě budou k dispozici následující funkce:
- jen tel. linka: dálkové ovládání telefonem, reportování událostí SMS a zavoláním, reportování na PCO2 (CID)
- jen LAN: dálkový přístup z Internetu, reportování na PCO1 (IP CID)

Kompletní specifikace je dostupná z webových stran výrobce. (44)

7.1.1 Webové rozhraní modulu JA-80V

Modul samotný webové rozhraní nenabízí, po nastavení pracuje se stranami výrobce dle obrázku 20. Komunikační protokol mezi modulem a stranami výrobce není popsán. Webové strany jsou již ale zabezpečené protokolem HTTPS a jako třetí strana, certifikační autorita, je společností JABLOTRON ALARMS a.s. dále jen Jablotron vybrána Thawte Consulting cc. (44)



Obrázek 20 - strany GSMLink

7.1.2 Zabezpečení přístupu

Pro přístup k modulu je nutné nejen nastavit IP adresu, ale také vytvořit uživatelský účet právě na stranách výrobce. Před přihlášením k nastavenému modulu se vždy zadává zvolené uživatelské jméno a heslo po přihlášení je možná volba některého z registrovaných modulů. Následné přihlášení vyžaduje pro specifické úlohy ještě znalost hesla modulu pro vzdálený přístup a v případě konfigurace také znalost master a servisního kódu. Nastavení protokolu TCP/IP modulu se provádí přes klávesnici EZS pomocí zadávání specifických kódů a proměnných anebo je možná vzdálená konfigurace prostřednictvím SMS brány, SMS zpráv. (44)

7.1.3 Porovnání s modulem IP100

Modul společnosti Jablotron JA-80V je více zaměřen na vzdálenou správu než na monitoring či jednodušší uživatelské ovládání ústředny. Oproti IP100 je kvůli vyššímu stupni zabezpečení centralizován systém webových stran a zabezpečen protokolem HTTPS. Modul JA-80V webové strany neobsahuje. JA-80V není jednoúčelový, pravděpodobně proto popsaný způsob nastavení tohoto modulu rozhodně nepatří k jednodušším ani komfortním.

7.2 Modul JA-60WEB

Modul výrobce Jablotron není nabízen na českém trhu (obrázek 18). Spolupracuje s ústřednami EZS JA-63 a JA-65. Modul disponuje RJ-45 konektorem pro připojení ethernetu, dále pak datovým konektorem pro napájení a připojení k ústředně a svorkovnicí pro připojení externích ovládaných zařízení. Pro ovládání 16. dalších zařízení je na modulu konektor standardu X10. (45) JA-60WEB umožňuje následující operace:

- Vzdálenou kontrolu a nastavení modulu i ústředny EZS přes internetový prohlížeč
- Vzdálenou kontrolu a nastavení modulu i ústředny EZS s použitím JAVA aplikace pro mobilní zařízení
- Vzdálené řízení externích zařízení objektu (topení, osvětlení, apod.) pomocí webového prohlížeče a JAVA aplikace pro mobilní zařízení.
- Nastavení a vzdálený monitoring přes strany www.GSMlink.cz

Obrázek 21 - modul JA-60WEB

7.2.1 Webové rozhraní modulu JA-60WEB

Modul obsahuje jednoduchý HTTP server. Po přihlášení je zobrazen stav ústředny a lze měnit nastavení jak modulu, tak ústředny EZS i připojených periférií. Prvotní nastavení TCP/IP je prováděno přes dodávaný vyhledávač modulu. Změna portu HTTP serveru není možná.

7.2.2 Zabezpečení přístupu

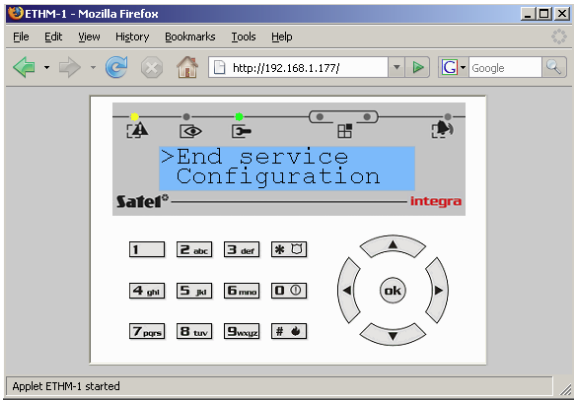
Přihlášení probíhá zadáním uživatelského jména a hesla, autentizace je oddělena od autentizace k EZS ústředně. Modul využívá jednoduché HTTP autentizace, ta má sice širokou podporu webových prohlížečů, ale ochrana přenášených autentizačních údajů je minimální, pouze kódování metodou „base64“. Pro změny stavu sledování objektu je nutné před každou takovouto změnou opakované zadání uživatelského kódu EZS ústředny. Zda a jak se kód přenáší, není dle dostupné dokumentace patrné. Zabezpečení komunikace mezi modulem a klientem není prakticky žádné. (45)

7.2.3 Porovnání s modulem IP100

IP100 má oproti tomuto modulu integrované přihlášení, zobrazované strany IP100 jsou sestavovány vždy na straně klienta. Velkou nevýhodu tohoto modulu vidím právě v použití integrované HTTP autentizace. Výhodou je možnost přímého ovládání externích zařízení a integrace IP kamer objektu do jednoho místa.

7.3 Modul Satel INTEGRA ETHM-1

Tento modul patří mezi jednodušší. Konfigurace modulu se provádí pouze přes sériové rozhraní RS232. Modul kromě uvedeného sériového rozhraní obsahuje konektor RJ45 pro připojení k ethernetu a svorkovnici pro připojení ústředny i napájení. Konfigurace nastavuje také heslo modulu pro web/wap rozhraní označované jako GuardX a heslo pro přístup programem DloadX. Kompletní specifikace je uvedena v přiložených manuálech. (46)



Obrázek 22 - webové rozhraní modulu ETHM-1 (47)

7.3.1 Webové rozhraní modulu

Po přihlášení prováděné nastaveným klíčem modulu je zobrazena vzdálená, virtuální klávesnice EZS dle obrázku 22, která nabízí úroveň ovládání dle zadaného přístupového kódu lokální klávesnice. Webové rozhraní je sestaveno v programovacím jazyku JAVA a pro svůj běh je požadována instalace JAVA Virtual Machine dále jen JVM. Modul také nabízí obdobnou aplikaci pro mobilní telefon, který opět musí podporovat interpreter jazyka JAVA. (46)

7.3.2 Zabezpečení přístupu

ETHM-1 je zabezpečen heslem modulu. Pro další práci je použit program jazyka JAVA, ve které může být zavedeno šifrování např. klíčem hesla modulu. Tento způsob sice brání odposlechu obsahu komunikace nicméně přesměrování útočníkem a nahrazení vlastní komunikací je možné, vzhledem k tomu, že není použito žádné ověření obou komunikujících stran. (47)

7.3.3 Porovnání s modulem IP100

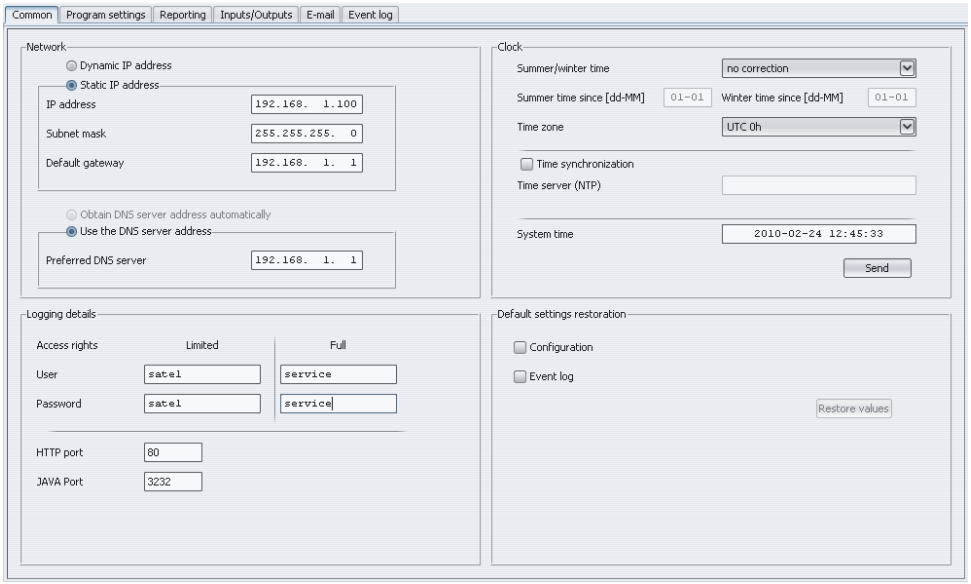
Modul IP100 oproti ETHM-1 používá pouze JavaScriptu, má větší podporu webových prohlížečů. Způsobem nastavení nejen TCP/IP se bohužel tento modul dostává na poslední místa pomyslného žebříčku. Jistou výhodu nabízí podpora mobilních zařízení ve formě speciální JAVA aplikace. Webové rozhraní tohoto modulu je použito pouze pro předání aplikace JAVA, která po spuštění již komunikuje na zcela jiném principu a portu.

7.4 Modul Satel INTEGRA ETHM-2

Je nástupcem modulu ETHM-1 a lze ho kombinovat s ostatními typy ústředen Satel. Oproti jednoduššímu modulu přináší řadu vylepšení, ovšem i dle specifikace výrobce není vhodný pro použití mimo sítě typu LAN. Jedním z hlavních vylepšení je konfigurace modulu také prostřednictvím webových stran. (48)

7.4.1 Webové rozhraní modulu

U tohoto modulu je pro zobrazení obsahu stran opět nutná instalace JVM na straně klienta. Webové rozhraní je prakticky využito pouze pro zobrazení strany přihlášení a pro předání JAVA aplikace. Veškerá komunikace probíhá na jiném portu konkrétně je nastaven výchozí port 33333. Ukázka aplikace je na obrázku 23. (49)



Obrázek 23 - Satel ETHM-2 (48)

7.4.2 Zabezpečení přístupu

Výrobce používá etehrnetové rozhraní pouze k přenosu HTTP a služeb. Přičemž uvádí, že datový přenos v síti je šifrován 192 bitovým klíčem. Šifrování je použito po prvotním přihlášení a hrozí tak riziko odposlechu i útoku typu Man-in-the-middle. (49)

7.4.3 Porovnání s modulem IP100

Modul IP100 oproti ETHM-2 používá pouze JavaScriptu, má tedy větší podporu webových prohlížečů. Webový server je v ETHM-2 pouze doplněk určený pro stažení aplikace JAVA.

8 Závěr

Vyjdeme-li z představ o použití webového modulu v zabezpečovací technice, můžeme vlastní aplikaci takovýchto modulů rozdělit na moduly určené pro monitoring stavu systému, které mají upřesnit stav celého zabezpečovacího zařízení, a moduly pro monitoring a aktivní operace. Dále je možné říci, že webové moduly typu IP100 jsou vhodné pro objekty s nízkým až středním stupněm zabezpečení. Pro vyšší stupně zabezpečení výrobci přímo ve vlastním modulu webový server nepoužívají. Používají vlastní chráněné protokoly pro přenos do vlastního centralizovaného systému, kde dochází k dešifrování komunikace a interpretaci získaných informací pomocí centrálního webového serveru již s protokolem HTTPS a veřejnou ověřovací identitou – certifikační autoritou. Nebo používají vlastní chráněný protokol s vlastní aplikací spouštěnou na straně klienta. Toto řešení vede k úsporám na straně výrobce i konečného zákazníka. U výrobce není nutné do HTTP modulů integrovat složitější SSL vrstvu. Hardware je tak jednodušší. Na straně odběratele a koncového zákazníka odpadá náročné nastavení a hlavně nákup a monitoring stavu certifikátu pro šifrování protokolem HTTPS, vztažené k doménovému jménu veřejné IP adresy.

Výrobci webových modulů se snaží zvýšit bezpečnost přístupu použitím jednouživatelského režimu a předáváním pouze nezbytných informací anebo šifrováním na straně klienta. Tato opatření zabraňují nebo ztěžují přímému zjištění autentizačních údajů. Opačným efektem tohoto opatření je nutnost podpory interpreteru jazyka také na straně klienta a tím snížená podpora všech klientů, různých webových prohlížečů.

Navrhované řešení používá standardu, protokolu HTTPS. Pro dosažení vyšší podpory webových prohlížečů je použit standardizovaný komunikačního protokol HTTP verze 1.1. Návrh nepočítá s použitím dalšího interpreteru jiného jazyka na straně klienta. V případě, že je zjištěna podpora dalších interpreterů, konkrétně JavaScriptu, je použit jazyk jako nadstavba základního zobrazení.

Realizace spojení a komunikace mezi navrhovaným řešením a EZS ústřednou je souborová ve formě rozšířeného značkovacího jazyka XML, to umožní v budoucnu jednodušší výměnu zpráv. Důvodem tohoto rozhodnutí je neznámá a výrobcem nepopsaná komunikace sériovým rozhraním I306 modulu IP100. Návrh počítá s případnými modifikacemi struktury XML nebo s kompletním nahrazením tohoto způsobu komunikace.

Výhody oproti stávajícímu řešení v modulu IP100 jsou právě v použití modelu metody MVC dále nejsou potřeba skripty a podpora skriptovacího jazyka na straně klienta a dále oddělení uživatelů uložených v databázi EZS ústředny od uživatelů webových stran. Ověření autorizace uživatele jinou cestou zvyšuje bezpečnost při stanovení identity uživatele. Oprávnění dle zjednodušeného ACL také umožňuje jednoduše vytvořit profily šité na míru potřebám klientů. Nevýhodou zůstává nutnost použití HTTPS a tím nákup časově omezeného certifikátu. V případě self-signed certifikátu je komunikace šifrovaná ovšem není prověřena autenticita obou stran jinou, třetí stranou. Tuto nevýhodu by bylo možné definitivně smazat, v případě že by výrobce modulu působil také jako certifikační autorita a v případě koupě modulu s následnou instalací by byl certifikát ověřován právě výrobcem.

V případě nasazení mnou navrženého řešení do modulu IP100 bude nutné provést rozšíření velikosti paměťového prostoru pro uložení webových stran. Jelikož celková velikost webových stran je 236Kb bez HTTPS serveru, serverového certifikátu, PHP a linuxového jádra. Bude tedy nutné navýšit náklady na rozšíření hardware modulu. Přehled očekávané cenové kalkulace je uveden v tabulce 9.

Změnová akce	Popis	Cenové navýšení	Poznámka
Změna na hardware modulu	rozšíření ROM a RAM paměti modulu	20 000 Kč	10-20 pracovních dnů rozpočítává se mezi moduly
Dodatečná úprava software modulu	implementační úpravy a nahrazení stávajícího webového serveru	40 000 Kč	20-50 pracovních dnů rozpočítává se mezi moduly
Serverový certifikát pro HTTPS	v případě využití externí certifikační autority Thawte	4 500 Kč	na rok a modul
	v případě využití vlastní certifikační autority Thawte	12 000 Kč	cena je rozpočítávána mezi prodané moduly
	v případě využidí self-signed certifikátu	0	
Odhadované dodatečné náklady		72 000 Kč	

Tabulka 9 - cenové navýšení

Jelikož nejsou známy prodejní výsledky modulu IP100 nelze přesně stanovit navýšení výrobní ceny jednoho modulu. Proto byl proveden orientační výpočet pro cílových 1000 prodaných kusů tohoto modulu. Výstup výpočtu je uveden v tabulce 10 a počítá s vytvořením vlastní certifikační autority právě pro serverový certifikát. Funkční porovnání ukazuje výhody použití navrhovaného webového modulu a je uvedeno v tabulce 10. Kromě cenového srovnání obsahuje porovnání v oblastech použitých protokolů, bezpečnosti a uživatelského komfortu.

		Moduly					
	Popis	IP100	JA80	JA60	ETHM-1	ETHM-2	Navržené řešení
Protokoly	Protokol HTTPS		není součástí modulu				x
	Pouze protokol HTTP						x
	HTTP v kombinaci se skriptovacím jazykem na straně klienta	x	x	x			x
	Software vyjma webového prohlížeče na straně klienta				x	x	
Bezpečnost	Zablokování účtu dočasné	x					
	Zablokování účtu trvalé						x
	Ochrana přenosu hesel	x	x	x	x	x	x
	Oddělení uživatele EZS od uživatele modulu				x	x	x
	Logování událostí webu	x	x	x			x
	Uživatelské profily	x					x
	Ochrana před útoky typu: Man-in-the-middle		x				x
	Ochrna před útoky typu: Denial of Service						
Komfort	Konfigurace modulu přes webové rozhraní	x	x			x	x
	Změna hesel přes webové rozhraní						x
	Jazykové verze	x	x	x	x	x	x
	Volba jazyka pro uživatele a profil						
	Více uživatelský přístup		x				x
	Dynamická aktualizace obsahu	x	x	x	x	x	x
	Správa uživatelů modulu na stránkách						x
	Maloobchodní cena modulu v Kč	5 400	2 736	5 160	3 900	3 900	5 472

Tabulka 10 - funkční srovnání modulů

Práce si kladla za cíl vytvořit webový server a strany, které budou použitelné v modulu IP100. Podařilo se vytvořit řešení, které svoji velikostí a rozsahem odpovídá možnostem tohoto modulu a může být s úpravami v tomto modulu použito.

Seznam literatury

1. **Tomáš Koníček, Pavel Kocábek.** *Cesta k bezpečí.* Praha : BEN - technická literatura, 2002. str. 255. ISBN 80-7300-032-6.

2. **Jiří, Kindl.** *Projektování bezpečnostních systémů: EPS, EZS. I.díl.* Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta technologická. str. 134. ISBN 80-7318-165-7.

3. **P., Koktan a kol.** *Mechanické zábranové systémy.* 1998. str. 268.

4. **Stanislav, Křeček a kol.** *Příručka zabezpečovací techniky.* místo neznámé : Critetus, 2002. str. 313. ISBN 80-902938-2-4.

5. **F., Kallay a P., Peniak.** *Počítačové sítě a jejich aplikace.* 2. místo neznámé : Grada, 2003. ISBN 80-247-0545-1.

6. **Luhový, Karel.** VPN. *Svět sítí.* [Online] 6. leden 2003. http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=220.

7. **Mudrák, David.** Soubor:Tcpip zapouzdreni.svg. *Wikipedie otevřená encyklopedie.* [Online] 11. říjen 2008. http://cs.wikipedia.org/wiki/Soubor:Tcpip_zapouzdreni.svg.

8. **Wikimedia.** Princip tunelování. *Wikimedia org.* [Online] http://upload.wikimedia.org/wikipedia/commons/5/54/Princip_tunelovani.jpg.

9. **Štráfelda, Jan.** Šifrování a signály. *Shaman.cz.* [Online] http://www.shaman.cz/sifrovani/.

10. **Wikipedie.** Kryptografie. *Wikipedie otevřená webová encyklopedie.* [Online] 5. duben 2011. http://cs.wikipedia.org/wiki/Kryptografie.

11. **Krhovják, J. a Matyáš, V.** *Autentizace a identifikace uživatelů.* místo neznámé : Zpravodaj ÚVT MU, 2007. ISSN 1212-0901.

12. **metacentrum.cz.** Public Key Infrastructure. *metacentrum.cz.* [Online] 20. srpen 2009. http://metavo.metacentrum.cz/cs/docs/login/PKI.html.

13. **Griffin, Dan.** Safer Authentication with a One-Time Password Solution. *MSDN Magazine.* [Online] Microsoft, 2011. http://msdn.microsoft.com/en-us/magazine/cc507635.aspx.

14. **Wikipedie.** Kerberos (protokol). *Wikipedie otevřená encyklopedie.* [Online] 3. duben 2011. http://cs.wikipedia.org/wiki/Kerberos_(protokol).

15. **web4company.cz.** Autentizace a autorizace. *web4company.* [Online] [Citace: 15. leden 2011.] http://www.web4company.cz/bezpecnost-autentizace-autorizace/.

16. **Ellen, Nanci.** access control list (ACL). *Software Quality.* [Online] 4. srpen 2000. http://searchsoftwarequality.techtarget.com/definition/access-control-list.

17. **Techotopia.com.** Mandatory, Discretionary, Role and Rule Based Access Control. *Techotopia.* [Online] techotopia.com. http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control.

18. **The Apache Software Foundation.** Authentication, Authorization, and Access Control. *Apache.org.* [Online] http://httpd.apache.org/docs/1.3/howto/auth.html.

19. **tukni.cz.** Přihlášení pomocí HTTP autentizace. *tukni.cz.* [Online] 29. srpen 2010. http://blog.tukni.cz/tvorba-www-stranek-php-mysql/prihlaseni-pomoci-http-autentizace/.

20. **php.net.** HTTP authentication with PHP. *PHP.* [Online] php.net, 4. březen 2011. [Citace: 30. březen 2011.] http://php.net/manual/en/features.http-auth.php.

21. **Šrámek, Jan.** Autorizace pomocí PHP a MySQL II. *reboot.cz.* [Online] 17. září 2001. http://reboot.cz/howto/webcoding/autorizace-pomoci-php-a-mysql-ii/articles.html?id=185.

22. **Wikipedie.** HTTP cookie. *Wikipedie otevřená encyklopedie.* [Online] Wikipedie, 4. leden 2011. http://cs.wikipedia.org/wiki/HTTP_cookie.

23. **Saitraje.** Zabezpečení serveru. *soom.cz.* [Online] 7. únor 2008. http://www.soom.cz/index.php?name=usertexts/show&aid=584.

24. **Malý, J. a Kacálek, J.** Zabezpečení webových aplikací III. - ostatní útoky a nastavení prostředí. *Access server.* [Online] 15. říjen 2007. http://access.feld.cvut.cz/view.php?cisloclanku=2007080003. ISSN 1214-9675.

25. **SecuriTeam.** Introduction to HTTP Response Splitting. *SecuriTeam.* [Online] 14. duben 2005. http://www.securiteam.com/securityreviews/5WP0E2KFGK.html.

26. *IP 100 manuál.* **VARIANT plus spol. s r.o.** místo neznámé : VARIANT plus spol. s r.o., 2007.

27. *IP100 UŽIVATELSKÝ MANUÁL PRO SPRÁVCE SÍTĚ A IT.* **VARIANT plus spol. s r.o.** 1.10, místo neznámé : VARIANT plus spol. s r.o., 2007.

28. **Paulík, Karel.** *Psychologické základy lidské.* [Dokument PDF] Ostrava : Ostravská univerzita v Ostravě, 2007.

29. **Jireš, Jan.** Vybrané definice bezpečnosti. *Jan Jireš.* [Online] http://www.google.cz/url?sa=t&source=web&cd=1&sqi=2&ved=0CBcQFjAA&url=http%3A%2F%2Ffiles.janjires.webnode.cz%2F200000090-3657337516%2FDefinice%2520bezpe%25C4%258Dnosti.pdf&rct=j&q=bezpe%C4%8Dnost%20definice&ei=tQmfTbTfD8288gPv3cWoAw&usg=AFQjCNEZjH0NesBDbz.

30. **R. Fielding; UC Irvine; J. Gettys;Compaq/W3C; J. Mogul; Compaq H. Frystyk; W3C/MIT; L. Masinter;Xerox;P. Leach; Microsoft; T. Berners-Lee.** Hypertext Transfer Protocol -- HTTP/1.1. *Hypertext Transfer Protocol.* [Online] W3C, červen 1999. [Citace: 3. duben 2011.] http://www.w3.org/Protocols/rfc2616/rfc2616.html.

31. **T. Socolofsky; C. Kale; Spider Systems Limited.** RFC1180. *potaroo.net.* [Online] leden 1991. http://potaroo.net/ietf/idref/rfc1180/index.html.

32. **D. Kristol;Bell Laboratories, Lucent Technologies;L. Montulli;Epinions.com, Inc.** HTTP State Management Mechanism. *apps.ietf.org.* [Online] říjen 2000. http://www.apps.ietf.org/rfc/rfc2965.html.

33. **University Information Technology Services.** Best practices for computer security. *University Information Technology Services.* [Online] 8. duben 2011. http://kb.iu.edu/data/akln.html.

34. **E. Rescorla;RTFM, Inc.** HTTP Over TLS. *RFC2817.* [Online] květen 2000. http://tools.ietf.org/html/rfc2818.

35. **The Internet Society.** The Secure HyperText Transfer Protocol. *apps.ietf.org.* [Online] The Internet Society, srpen 1999. http://www.apps.ietf.org/rfc/rfc2660.html.

36. **Renesas Electronics Canada Limited.** M16C/30P Group. *Renesas.com.* [Online] 2011. http://www.renesas.com/products/mpumcu/m16c/m16c30/m16c30p/m16c30p_root.jsp.

37. **The Internet Society.** The Common Gateway Interface (CGI) Version 1.1. *faqs.org.* [Online] The Internet Society, říjen 2004. http://www.faqs.org/rfcs/rfc3875.html.

38. **Kanisová, Hana a Muller, Miroslav.** *UML srozumitelně.* Brno : Cpmputer Press, 2004. ISBN 80-251-0231-9.

39. **Vrána, Jakub.** *1001 tipů a triků pro PHP.* Brno : Computer Press, 2010. ISBN 978-80-251-2940-1.

40. **Schlossnagle, George.** *pokročilé programování v PHP5.* Brno : Zoner Press, 2004. ISBN 80-86815-14-5.

41. **Mercer, Dave W., a další, a další.** *Beginning PHP5.* Indianapolis : Wiley Publishing, Inc., 2004. ISBN 0-7645-5783-1.

42. **The Apache Software Foundation.** Apache HTTP Server Version 2.2 Documentation. *Apache HTTP Server.* [Online] The Apache Software Foundation, 2011. http://httpd.apache.org/docs/current/.

43. **php.net.** Apache 2.x on Unix systems. *php.net.* [Online] 4. duben 2011. [Citace: 6. duben 2011.] http://www.php.net/manual/en/install.unix.apache2.php.

44. **Jablotron a. s.** JA-80V kombinovaný komunikátor LAN a telefonní linka. *jablotron.* [Online] Jablotron a. s., 2008. http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/komunikace/ja+80v+kombinovany+komunikator+lan+a+telefonni+linka/.

45. **Jablotron a.s.** JA-60WEB-EN LAN Communicator. *jablotron.* [Online] Jablotron a.s., 2008. http://www.jablotron.com/en/Catalog/house+alarms/profi+433+mhz/communication/ja60weben+lan+communicator/.

46. **SATEL sp. z o.o.** ETHM-1. *satel.pl.* [Online] SATEL sp. z o.o., 2008. http://www.satel.pl/en/product/115/ETHM-1,TCP-IP-communication-module-for-INTEGRA-control-panels.

47. *Ethernet Module ETHM-1.* **SATEL sp. z o.o.** Gdańsk : SATEL sp. z o.o., 2008.

48. **SATEL sp. z o.o.** ETHM-2 Universal TCP/IP communcation module. *satel.* [Online] SATEL sp. z o.o., březen 2010. http://www.satel.pl/en/produktid/471 .

49. *Ethernet Module ETHM-2.* **SATEL sp. z o.o.** Firmware version 1.01, Gdańsk : SATEL sp. z o.o., 2010.

50. *Začínáme s EZS.* **Zahrádka, J.** místo neznámé : Variant plus s r.o, 2005.

51. **P., Douček.** *Řízení projektů informačních systémů.* Praha : Professional Publishing, 2004. ISBN 80-86419-71-1.

52. **A., Buchalcevová.** *Metodiky vývoje a údržby informačních systémů.* Praha : Grada, 2005. ISBN 80-247-1075-7.

53. **J., Heřman, Z., Trinkewitz a kol.** *Elektrotechnické a telekomunikační instalace.* místo neznámé : Verlag Dashofer, 2006. ISBN 80-86897-06-0.

Seznam obrázků

Seznam tabulek

Příloha 1 - Manuál IP 100

IP 100

verze 1.21

Manuál

tovární heslo pro IP100 (module pasword) je „paradox"

VARIANT plus, spol. s .r.o., U Obůrky 5, 674 01 TŘEBÍČ, tel.: 565 659 625,
technická linka 777 55 77 02 (pracovní doba 7:30 – 16:00, hot line do 18:00)
www.variant.cz technik@variant.cz

Dokumentace vytvořena dne 27. 7. 2007
poslední korekce dne 18. 2. 2008

Popis

Modul IP100 slouží pro spojení s ústřednou pomocí LAN nebo internetu. Modul IP 100 lze použít pro několik funkcí:

Ovládání ústředny
Modul obsahuje LAN server a v okamžiku, kdy se uživatel spojí s IP100 a zadá svůj uživatelský kód, je mu umožněno vidět stav svých podsystémů a má možnost je i ovládat.

Informace o stavu
Modul IP100 umožňuje zasílání emailových zpráv na zvolené emailové adresy. Je možné volit jaké zprávy se mají na danou adresu posílat. Modul umí zaslat zprávu o stavu zapnuto/vypnuto, poplach, porucha a blokován přístup do IP100. Tímto způsobem je možné informovat jak uživatele tak instalační firmu o případných poruchách nebo bezpečnostní agenturu o poplachu v objektu.

Spojení se SW WinLoad 4.0 IP a vyšší
Verze programu WinLoad IP umožňuje instalační firmě spojení s ústřednou pomocí LAN nebo internetu.

Spojení s NEWARE 4.0 IP a vyšší
Verze programu NEWARE IP umožňuje uživateli spojení s ústřednou pomocí LAN nebo internetu.

Instalace
Modul IP100 se instaluje do boxu k ústředně. Propojovací kabel mezi ústřednou a modulem není možné prodlužovat. Modul IP100 je napájen přes připojovací konektor přímo z ústředny. Odběr IP100 se přičítá k odběru AUX.

Zapojení
1. Připojte kabel IP100 do konektoru SERIAL ústředny.
2. Kabel má být do SERIAL na IP100.
3. Připojte síťový kabel do RJ45.
4. IP100 je zapojen.

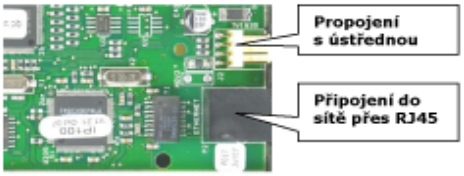
Pro propojení PC-IP100 doporučujeme vždy používat SWITCH nebo HUB. Nedoporučujeme používat přímé propojení pomocí kříženého kabelu PC–IP100. Toto přímé spojení nemusí být spolehlivé.

Nastavení
Pro nastavení IP komunikace je nezbytná spolupráce se správcem sítě. Pro nastavení parametrů pro síť a internet je nutné mít znalosti o této problematice.

RESET
1. Stiskněte a držte tlačítko RESET, dokud nezačne blikat dioda ERROR (asi 5 sec.)
2. Tlačítko pusťte a stiskněte znovu.
3. Dojde k resetu modulu na tovární hodnoty.

Vlastnosti

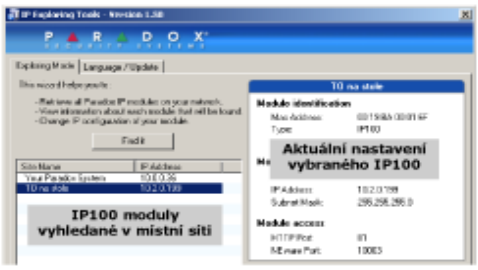
Kompatibilita	EVO48
	EVO192
	SPECTRA SP 5500, 6000, 7000
	MAGELLAN 5000, 5050
Připojení	Místo I306 (konektor SERIAL)
Napájení	Z konektoru 12V
Odběr	110mA
Prohlížeč	Mozilla 1,5 a vyšší
	Explorer 6 a vyšší
Kryptování dat	AES 256-bit, MD5, RC4
Konektor na síť	RJ45
Konektor SERIAL	Pro připojení k ústředně na konektor SERIAL ústředny
Konektor UPGRADE	Pro připojení I306 za účelem provést upgrade firmware IP100
tovární heslo IP100 (module password)	**paradox**
Síť - spojení	**Lokální síť**
	Pevná veřejná IP adresa
	Veřejná dynamicky přidělovaná IP adresa



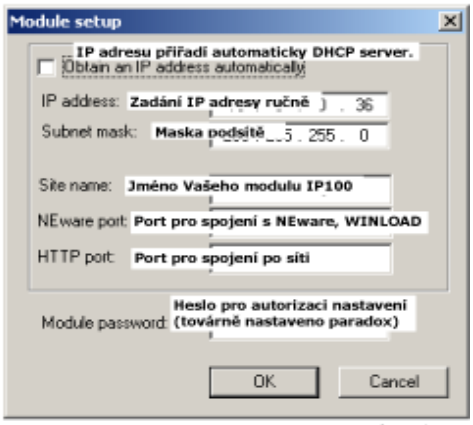
Nastavení IP a portu na IP100

Nastavení IP a vlastností se provádí na vnitřní síti pomocí programu **Vyhledávač IP100.exe**. Program je ke stažení na www.variant.cz nebo na CD Variant. Program se neinstaluje ale pouze se jedná o exe utilitu, která se spouští.

1. Spusťte **Vyhledávač IP100.exe** na PC, které je připojené do sítě s IP100.
2. Dojde k vyhledání všech IP100 v síti. Nezáleží na tom, jakou IP adresu modul má.
3. Zvolte spodním tlačítkem ***More detail***



4. Pravým tlačítkem myši klikněte na IP adresu IP100 modulu, který potřebujete konfigurovat.
5. Zvolte ***Module setup***



Sítě a spojení

Teorie Provoz IP100 v rámci jedné sítě je vcelku bez zásadních nastavování a po zadání IP je možné s IP100 pracovat. Pokud je požadavek na přístup k IP100 z veřejné sítě (internet), je nezbytně nutné, aby poskytovatel internetového připojení umožnil vaši privátní (firemní) síti přidělit veřejnou IP nebo povolil směrování potřebných portů na svém routeru. **Vždy se informujte o možnostech Vaší sítě a možnostech Vašeho poskytovatele. Ne u všech typů připojení je možné modul IP100 použít.**

Spojení přes lokální síť

Jedná se o nejjednodušší případ, kdy máte IP100 a PC připojen do „stejného SWITCHE" v rámci jedné sítě. V tomto případě, ale není možné komunikovat s IP100 přes internet nebo z jiné sítě. Jedná se o jednoduché zapojení použitelné v rámci jedné budovy nebo jedné firmy.
Pomocí **Vyhledávače IP100.exe** vyhledejte všechny IP100 v místní síti. Dvakrát klikněte myší na vybraný IP100. Dojde k otevření webových stránek modulu a jste vyzváni k zadání uživatelského kódu a hesla modulu. Po autorizaci je možné pracovat s IP100.
Toto lokální spojení proveďte a oživte před dalším navazováním spojení přes internet.

Spojení přes internet – pevná veřejná IP

Pokud máte možnost přiřadit k IP100 pevnou veřejnou IP adresu a port, použijte opět **Vyhledávač IP100.exe**. Pokud má Vaše síť veřejnou IP adresu, nastavte v routeru patřičný překlad a můžete se s IP100 spojit z libovolného místa s přístupem na internet. Do internetového prohlížeče zadáte veřejnou IP adresu a port a následně dojde ke spojení s IP100. Nastavení routeru a překladu není možné obecně popsat, protože se liší dle typu sítě a routeru. V tomto bodě je nezbytně nutné **spolupracovat se správcem sítě.**
(Dále zmiňovanou funkci ParadoxMyHome lze použít pro zpřehlednění spojení i u pevných veřejných IP)

Spojení přes internet – veřejná dynamická IP

Pokud používáte spojení, při kterém máte přidělovanou veřejnou IP adresu dynamicky, je potřeba použít služby ParadoxMyHome. IP100 se automaticky spojí se stránkami ParadoxMyHome a udá svoji IP adresu a port. Pomocí tohoto přihlášení je možné se zpětně s IP100 spojit. Dynamicky přidělované veřejné adresy jsou u některých ADSL nebo ISDN modemů. V tomto bodě je nezbytně nutné **spolupracovat se správcem sítě.**

Následující nastavení se skládá z těchto kroků:
1. Nastavte v IP100 DNS server.
2. Přihlaste se na ParadoxMyHome.
3. Nastavte IP100.
4. IP100 registrujte na ParadoxMyHome a zadejte jeho **jméno.**

Instalační firma
Instalační firma vstupuje na www.paradoxmyhome.com a přihlašuje se pomocí svého emailu a hesla. Po vstupu se zobrazí všechny IP100 moduly, které instalovala a je možná jejich správa.

Uživatel
Uživatel zadává do prohlížeče adresu, kterou vytvořila instalační firma. Tato adresa má tvar www.paradoxmyhome.com/**jméno**. Jedná se o jméno, které v předcházejícím bodě 4 přiřadila danému IP100 instalační firma.

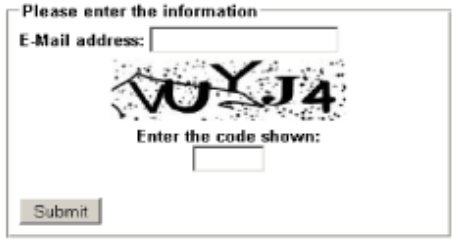
Nastavení DNS
DNS server převádí text (www.paradoxmyhome.com) na IP adresu a pomocí té dojde ke spojení se serverem v Paradoxu. Zjednodušeně řečeno DNS server ví, kam Vás má nasměrovat, pokud zadáte www stránku. DNS servery jsou umístěny různě po světě a Vy pouze zadáte IP adresu DNS serveru, který budete používat. Ne všechny DNS servery podporují přihlášení, které používá IP100. V případě, že doporučovaný DNS server Vašeho poskytovatele nepracuje s technologií IP100, zkuste zvolit některý z veřejných DNS serverů, jejichž IP adresy uvádíme.

213.133.106.251
213.133.105.2
208.67.222.222
208.67.220.220

IP adresa DNS serveru se zadává přímo v IP100 modulu v záložce **Nastavení modulu** viz. obrázek uvedený na straně 5 dole.

Registrace na paradoxmyhome
Následující popis se týká registrace instalační firmy na ParadoxMyHome. Ve Vašem prohlížeči zadejte adresu
www.paradoxmyhome.com

vyberte spodní odkaz **Request login**



Vyplňte Váš email a opište z obrázku kód do pole „**Enter the code shown**".

Obdržíte tento mail.

Kliknutím na odkaz v těle mailu vstoupíte na přihlašovací stránku.

X

Vyplňte políčka označené *. Emailová adresa je použitá z části Request login. **ZAPAMATUJTE SI PASSWORD – HESLO**, které Vám umožní vstup na ParadoxMyHome. Po vyplnění formuláře klikněte na Submit.

Po těchto krocích již můžete zadat www.paradoxmyhome.com, vyplnit Váš email a heslo a vstoupit do vaší databáze IP100 modulů.

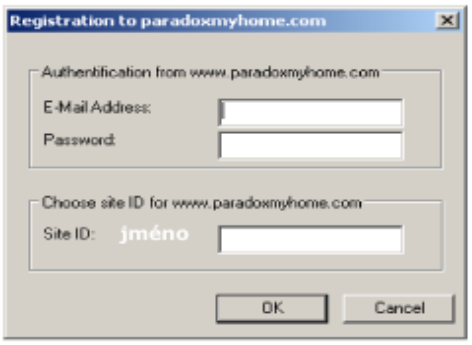
Takto bude vypadat Vaše prázdná databáze.

Tento postup je určen pro instalační firmy a není určen konečným zákazníkům..

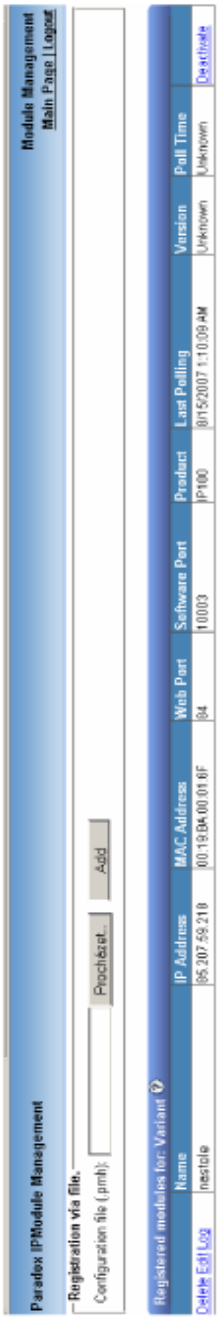
Přihlášení IP100 do ParadoxMyHome

V místní síti spusťte Vyhledávač IP100.exe. Dojde k vyhledání všech IP100 v místní síti. Klikněte pravým tlačítkem na vybraný IP100 modul a zvolte **Register to ParadoxMyHome**. Zobrazí se okno pro autorizaci přihlášení. Zadejte Váš email (ten co jste zadávali při registraci na ParadoxMyHome), heslo a **jmeno** IP100. Toto jméno bude uživatel používat v jeho prohlížeči. Pro jméno nepoužívejte diakritiku a nepoužívejte mezery. Pro případné oddělení slov použijte podtržítko _.

www.paradoxmyhome.com/**jmeno**



Po vstupu do databáze na ParadoxMyHome se již bude zobrazovat tento modul IP100



Uživatelský vstup

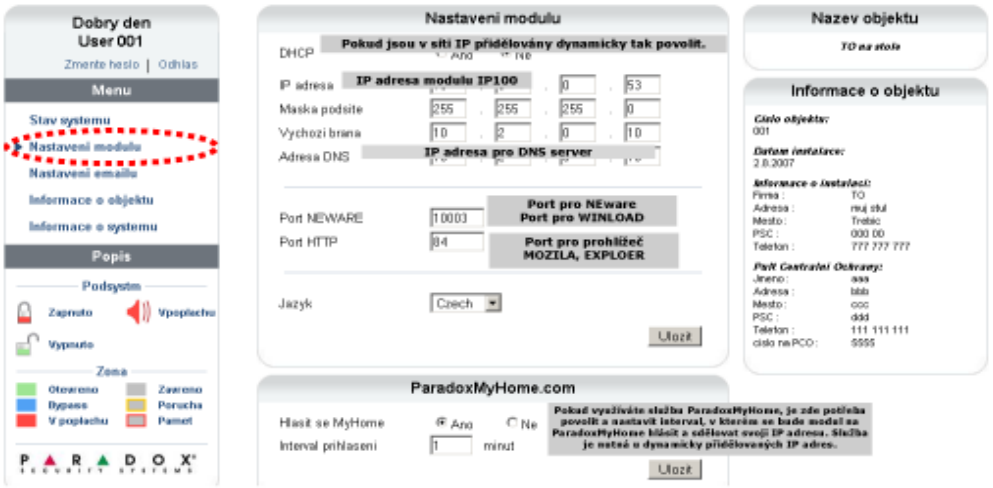
Pokud je použita pevná veřejná IP adresa, je možné do prohlížeče zadat přímo tuto adresu a port. Pokud je IP adresa dynamická, je potřeba na modul IP100 vstupovat přes stránky ParadoxMyHome.
Spojte se s Vaším IP100

Zadejte Váš uživatelský kód, stejný jako pro klávesnici
Zadejte heslo modulu (továrně „paradox")
Pokud je autorizace v pořádku, dojde k načítání dat
Modul IP100 umožňuje přes webové rozhraní vstup pouze jednomu uživateli. Pokud při ukončení spojení nepoužijete tlačítko ***ODHLAŠ,*** je uživatel neustále přihlášen a k další vstup je možný až asi po 5 min..

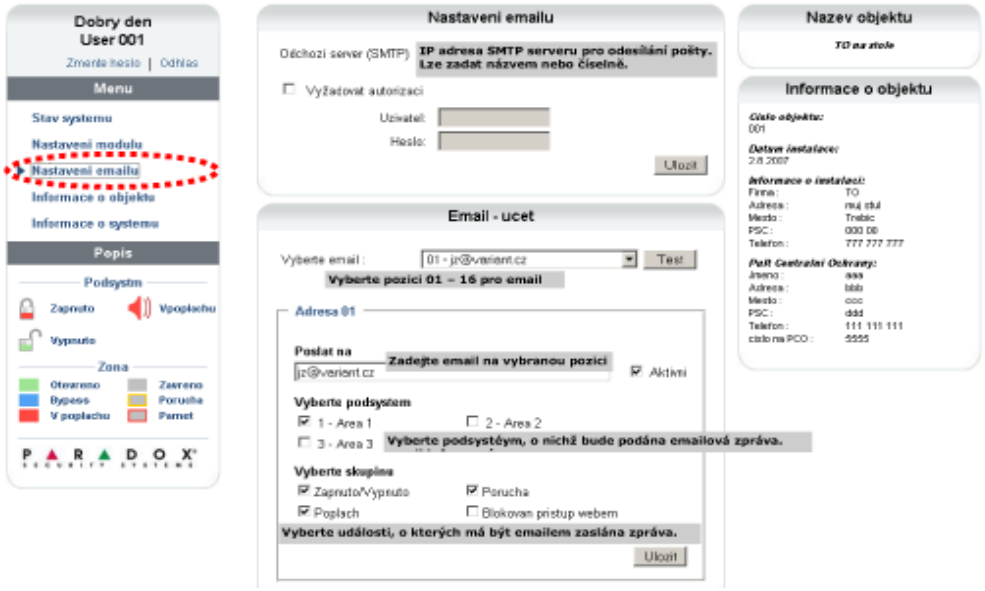
Na následujících stranách jsou popsána jednotlivá okna modulu IP100

Stav systému – uživatelé dle oprávnění

Nastavení modulu – pouze IK a MK



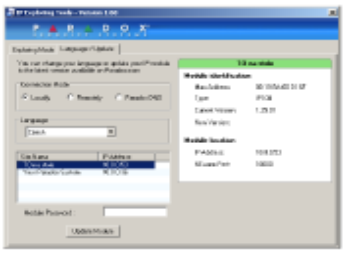
Nastavení emailu – pouze IK a MK



Upgrade Firmware

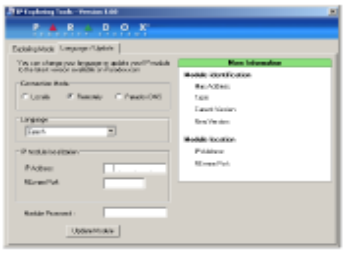
Upgrade Firmware se provádí přes utilitku „Vyhledávač IP100.exe".

LOKÁLNĚ



V místní síti vyberte IP100 modul, který budete upgradovat.
Klikněte na záložku LANGUAGE / UPDATE, zadejte heslo pro modul, vyberte jazyk a zvolte UPDATE. PC se spojí na www PARADOX, stáhne si aktuální FIRMWARE a provede update firmware.

VZDÁLENĚ



Zvolte Remotely, vyberte jazyk a zadejte IP adresu, port a heslo pro IP modul a potvrdte UPDATE. PC se spojí na www PARADOX, stáhne si aktuální FIRMWARE a provede update firmware.

Příloha 2 - XML datové soubory navrhovaného řešení

config.xml

```
<?xml version="1.0" encoding="utf-8"?>
<system>
  <ipconf>
    <dhcp>1</dhcp>
    <ip>192.168.0.1</ip>
    <net_mask>255.255.0.0</net_mask>
    <gw>192.168.0.1</gw>
    <dns>123.4.5.6</dns>
    <ports>
      <neware>5000</neware>
      <web>443</web>
    </ports>
  </ipconf>
  <ddns>
    <ddns_interval>0</ddns_interval>
    <ddns_adress>ezc.no-ip.com</ddns_adress>
    <ddns_login></ddns_login>
    <ddns_pwd></ddns_pwd>
  </ddns>
  <smtp>
    <server>smtp.seznam.cz</server>
    <port>25</port>
    <smtp_auth>1</smtp_auth>
    <smtp_login>jan</smtp_login>
    <smtp_pwd>test</smtp_pwd>
  </smtp>
  <languague>
    <lng id="cs" name="Česky" default="1">cs.ini</lng>
    <lng id="en" name="English" default="0">en.ini</lng>
  </languague>
  <roles>
    <role id="1" role_name="Administrator">
      <!--správa všeho-->
      <role_right>show_adm_menu</role_right>
      <role_right>show_ezsstatus</role_right>
      <role_right>change_ezsstatus</role_right>
      <role_right>show_infos</role_right>
      <role_right>change_infos</role_right>
      <role_right>show_logs</role_right>
      <role_right>show_users</role_right>
      <role_right>change_users</role_right>
      <role_right>show_system</role_right>
      <role_right>change_system</role_right>
      <role_right>show_profile</role_right>
```

```
    <role_right>change_profile</role_right>
   </role>
   <role id="2" role_name="User">
    <!--změny v status.xml a users.xml-->
    <role_right>show_usr_menu</role_right>
    <role_right>show_ezsstatus</role_right>
    <role_right>change_ezsstatus</role_right>
    <role_right>show_infos</role_right>
    <role_right>show_logs</role_right>
    <role_right>show_users</role_right>
    <role_right>change_users</role_right>
    <role_right>add_users</role_right>
    <role_right>del_users</role_right>
    <role_right>show_system</role_right>
    <role_right>change_system</role_right>
    <role_right>show_profile</role_right>
    <role_right>change_profile</role_right>
   </role>
   <role id="3" role_name="Viewer">
    <!--pouze zobrazit žádné změny-->
    <role_right>show_view_menu</role_right>
    <role_right>show_ezsstatus</role_right>
    <role_right>show_infos</role_right>
    <role_right>show_system</role_right>
    <role_right>show_profile</role_right>
   </role>
  </roles>
  <!-- informace o objektu a ústředně -->
  <infos>
   <object_info>
    <address>Školní 13</address>
    <city>Praha43</city>
    <phone>7372162893</phone>
    <others>Domácí adresa3</others>
   </object_info>
   <system_info>
    <cu_type>MG5050 v1.5</cu_type>
    <web_type>EZS 1.0.0</web_type>
   </system_info>
   <cld_info>
    <address>Školní 12</address>
    <city>Praha 81</city>
    <phone>12345689</phone>
    <others>Placený pult PCO1</others>
   </cld_info>
  </infos>
</system>
```

users.xml

```
<?xml version="1.0" encoding="utf-8"?>
<users>
  <user id="0">
    <name>Administrátor JB</name>
    <login>janbod</login>
    <last_access>1302114048</last_access>
    <!--poslední přístup datum v unix formátu -->
    <login_attemps>0</login_attemps>
    <!--počet neúspěšných pokusů reset po přihlášení -->
    <locked>0</locked>
    <!--účet uzamčen =1-->
    <pwd>4124bc0a9335c27f086f24ba207a4912</pwd>
    <lang_id>cs</lang_id>
    <role_id>1</role_id>
    <email>jan.bodlak@email.cz</email>
    <ezs_user_code>0000</ezs_user_code>
    <email_action>
      <subsystem id="1">
        <on>1</on>
        <fail>0</fail>
        <alarm>1</alarm>
        <lock>0</lock>
      </subsystem>
      <subsystem id="2">
        <on>1</on>
        <fail>0</fail>
        <alarm>1</alarm>
        <lock>0</lock>
      </subsystem>
    </email_action>
  </user>
  <user id="1">
    <name>Jan Bodlák</name>
    <login>janb</login>
    <last_access>1301998147</last_access>
    <login_attemps>1</login_attemps>
    <!--počet neúspěšných pokusů reset po přihlášení -->
    <locked>0</locked>
    <!--účet uzamčen =1-->
    <pwd>720a5c8ef79b595fcb8d263bedb1e2d7</pwd>
    <lang_id>cs</lang_id>
    <role_id>2</role_id>
    <email>jan.bodlak@email.cz</email>
    <ezs_user_code>2810</ezs_user_code>
    <email_action active="1" if_acc_lck="1">
      <subsystem id="2">
```

```
      <on>0</on>
      <fail>0</fail>
      <alarm>0</alarm>
      <lock>0</lock>
     </subsystem>
     <subsystem id="1">
      <on>0</on>
      <fail>0</fail>
      <alarm>0</alarm>
      <lock>0</lock>
     </subsystem>
   </email_action>
 </user></users>
```

status.xml

```
<?xml version="1.0" encoding="utf-8"?>
<systems>
 <system id="1" name="Podsystém 1">
  <status>100</status>
  <action>2</action>
  <zones>
   <zone id="1" zone_name="PIR místnost 1">2</zone>
   <zone id="2" zone_name="PIR místnost 2">100</zone>
  </zones>
 </system>
 <system id="2" name="Podsystém 2">
  <status>0</status>
  <!--zapnuto a typ zapnutí /vypnuto / v poplachu-->
  <action>2</action>
  <!--zapnout a typ zapnutí/vypnout-->
  <zones>
   <zone id="1" zone_name="Tamper místnost 1">3</zone>
   <zone id="2" zone_name="PIR místnost 2">2</zone>
   <zone id="3" zone_name="PIR místnost 3">1</zone>
  </zones>
 </system>
 <!--log ústředny -->
 <system_log>
  <event e_date="1297094807">ústředna - výpadek napájení</event>
 </system_log>
 <!--log webu -->
 <webif_log>
        <event e_date="1302036478" e_ip="127.0.0.1">User id: 3 on
        /px_web/profile.php</event>
 </webif_log>
</systems>
```

Příloha 3 - ukázky důležitých částí kódu PHP

Kontrola stavu session, kontrola přihlášení

```
//kontrola přihlášení
$boIsLoggedin=false;

getPlugins(); //připojené fce a definice

session_set_cookie_params(LIFETIME);
session_start();

if (isset($_SESSION["ULOG"]))
   {
   session_regenerate_id(true);

   $arLgn=$_SESSION["ULOG"]; //dej uživatelská data
   $cXc  =new XmlConfig(PATH_CONF . DS . FILE_CONF);
   $cLng =new Languague(PATH_LANG . DS, $cXc->getLng($arLgn["lang_id"]));
   $cXu  =new XMLUsers(PATH_CONF . DS . FILE_USR);
   $cXs  =new XMLStatus(PATH_CONF . DS . FILE_STAT);
         $cXs->setWebLog($_SERVER["REMOTE_ADDR"], "User id: " . $arLgn["id"] . " on " . $_SERVER['SCRIPT_NAME']);

   $stPwd=$cXu->getPwd($arLgn["id"]); //dej MD5 heslo z xml
   $cXu->setLastAccess($arLgn["id"]); //nastav poslední přístup

   if ($arLgn["lgn_stat"] == md5($stPwd . 2))
      {
      $boIsLoggedin=true;
      }
   }

if ($boIsLoggedin == false) //není přihlášen
   {
   session_destroy();
   header("location:index.php");
   exit();
   }
```

Práce s XML souborem

```
private $stXmlFilePath;
   private $sxXmlData;
   private $stLockFlag = ".lock";

   function XMLStatus($stXmlFilePath)
      {
      $this->stXmlFilePath=($stXmlFilePath);
      $this->getXmlData();
      }

   private function getXmlData()
      {
      while ($this->getLock()) //čekej na zámek true
         {
         usleep(10000000);    //10ms
         }

      $this->setLock(true);
      $this->sxXmlData=simplexml_load_file($this->stXmlFilePath);
      $this->setLock(false);
      }

   private function setXmlData($sxSetXmlData)
      {
      while ($this->getLock()) //čekej na zámek true
         {
         usleep(10000000);    //10ms
         }

      $this->setLock(true);
      $data=$this->sxXmlData;
      $data->asXml($this->stXmlFilePath); //zápis
      unset($data);
      $this->setLock(false);
      }

   private function setLock($boStat)
      { //nastavení a odnastavení zámku souboru
      if ($boStat)
         {
         $file=fopen($this->stXmlFilePath . $this->stLockFlag, "w");
         fwrite($file, " ");

         fclose($file);
         }
      else //odnastav
```

```
        {
        if (file_exists($this->stXmlFilePath . $this->stLockFlag))
           {
           unlink($this->stXmlFilePath . $this->stLockFlag);
           }
        }
     }

   private function getLock()
     { //zjištění zámku souboru
     if (file_exists($this->stXmlFilePath . $this->stLockFlag))
        {
        return true; //uzamčen
        }
     else
        {
        return false; //lze zapisovat
        }
     }
```

Automatická obnova zobrazovaných stavů

```
function getAutoRefreshHtm($stPageLink, $stDivID)
   {
   global $cLng;
   $stHtm="<script type='text/javascript' > \$(document).ready(function()
    {\$('#" . $stDivID . "').load('" . $stPageLink . "?ID='+ Math.random());
              var refreshId = setInterval(function() {\$('#" . $stDivID . "').load('" .
         $stPageLink . "?ID='+ Math.random());
     }, " . REFRESH_TIME . ");    });</script><noscript>
                      <iframe frameborder=0  src='" . $stPageLink . "' class='" .
                $stDivID . "'> " . $cLng->getTxt( 'NOT_SUPPORTED') . "<a
                href='" . $stPageLink . "' target='_blank'>" . $cLng-
                >getTxt('NEW_WINDOW') . "</a></iframe>
    </noscript><div id='" . $stDivID . "'></div>";
   return $stHtm;
   }
```