Propojení výrobních linek s informačním systémem pomocí bezdrátových sítí IEEE 802.11

Wireless network interconnection IEEE 802.11 between production lines and information systems

Bc. Bořuta Rostislav

Diplomová práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav automatizace a řídicí techniky
akademický rok: 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Rostislav BOŘUTA**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Automatické řízení a informatika**
Téma práce:	**Propojení výrobních linek s informačním systémem pomocí bezdrátových sítí IEEE 802.11**

Zásady pro vypracování:

1. **Hardwarové řešení (Wifi, Ethernet, PLC, PC, Konvektory, Sběrnice, ...)**
2. **Popis výstupních signálů z výrobních linek (Fiat, Porsche, Vulkanizace, ...)**
3. **Zabezpečení a ochrana dat s využitím metod zabezpečení (WEP, WPA, WPA2, Radius)**
4. **Zpracování výstupních dat vizualizačním programem navržený v delphi**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PÍSEK, Slavoj. Začínáme programovat v Delphi : Podrobný průvodce začínajícího uživatele. 1. vyd. Praha : Grada Publishing, 2000. 304 s. ISBN 80-247-9008-4.**
2. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluethoot, GPRS či 3G. Brno : CP Books, 2005. 179 s. ISBN 80-251-0791-4.**
3. **NORTHCUTT, Stephen. Bezpečnost počítačových sítí - Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. 2005th edition. Brno : Computer Press a.s., 2005. 589 s.**
4. **BECKHOFF NEW AUTOMATION TECHNOLOGY [online]. 31.1.2008 , 31.1.2008 [cit. 2008-02-15]. Dostupný z WWW: .**

Vedoucí diplomové práce:	**Ing. Jiří Korbel** Ústav automatizace a řídicí techniky
Datum zadání diplomové práce:	**22. února 2008**
Termín odevzdání diplomové práce:	**6. června 2008**
KONZULTANT:	Lukáš Veselý

Ve Zlíně dne 22. února 2008

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je propojit výrobní linky ve firmě Mubea HZP s.r.o. s pomocí bezdrátových sítí IEEE 802.11 tak, aby byly výrobní linky napojeny na lokální sítě LAN a mohly být pomocí vizualizačního softwaru sledovány či řízeny na dálku. Je použito programového prostředí Delphi k vytvoření vhodného softwaru na vizualizaci chodu výrobních linek. Jedním z bodů, týkajících se diplomové práce, je i zabezpečení přenášených dat.

Klíčová slova: WiFi, WEP, WPA2, Radius, I/O zařízení, LAN, 3COM, Beckhoff

ABSTRACT

The purpose of this thesis is connection production lines in firm Mubea HZP Ltd with using the wireless network IEEE 802.11. The produktion lines are connected to local area network LAN. The produktion lines are controlled and monitored by special software that was created in program Delphi. In this thesis we can found a part about datas safeguard and security

Keywords: Wi-Fi,WEP,WPA2, Radius, Imput/Output, LAN, 3COM, Beckhoff

Rád bych poděkoval touto cestou vedoucímu diplomové práce Ing. Jiřímu Korbelovi, za odborné vedení při vytváření mé práce, zodpovězení mých dotazů, cenné rady v technickém směru a trvalý zájem na úspěšném dokončení a zvládnutí všech problémů, které se během práce vyskytly. Dále bych chtěl poděkovat odbornému konzultantovi Lukášovi Veselému za cenné a odborné rady ohledně použitých technologií ve firmě Mubea HZP s.r.o.

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

Výrobní průmysl se dnes stále často potýká s problémem drahých a složitých instalací zařízení na pevné propojení moderních výrobních automatických linek s informačním systémem firmy. Proto se dnešní trend snaží implementovat do stávajících výrobních systému nové prvky bezdrátových technologií k jednoduššímu a komfortnějšímu přenosu dat.

Hlavní výhodu bezdrátových sítí jistě není potřeba popisovat. Možnost realizovat datovou výměnu či přenos informací bez nutnosti fyzického připojení k přenosovému médiu umožňuje řešit celou řadu úloh, které byly dříve limitovány nutností nemalých investic do zajištění konektivity. Přímým důsledkem a jedním z hlavních přínosů bezdrátových technologií je nesrovnatelně vyšší mobilita.

Je důležité si ale uvědomit, že s nástupem bezdrátové technologie do výrobního procesu se vyskytují i jisté problémy se zabezpečením dat a informací, přenášených pomocí bezdrátových zařízení, používající standardy IEEE 802.11. Proto je potřeba co nejvíce eliminovat možné narušení či nežádoucí vniknutí do IT systému firmy pomocí bezpečnostních prvků jako jsou např. (WEP, WPA, WPA2, Radius, Firewall,…).

Cílem diplomové práce je navrhnout a zrealizovat bezdrátovou síť ve výrobní hale firmy Mubea HZP s.r.o., zabývající se výrobou stabilizačních tyčí pro automobilový průmysl. Díky bezdrátové síti pak propojit některé výrobní linky s informačním systémem firmy (propojení s LAN sítí) a navrhnout v programovacím prostření Delphi vizualizační software k možnému sledování stavů výrobních linek přes vzdálenou plochu.

Celá práce bude implementovaná do stávající infrastruktury IT zařízení a bude realizovaná pouze z hardwarových prostředků povolených v Mubea standard. Jedním z největších dodavatelů a výrobce IT pro Mubea Global je firma 3COM.

I. TEORETICKÁ ČÁST

1 TECHNICKÉ PROSTŘEDKY

V teoretické části se seznámíme s technickými prostředky, které budou použity v následující praktické části. Stručným popisem zařízení používané ve výrobě a dalších hardwarových prostředků týkající se této diplomové práce. Dále si objasníme zabezpečení bezdrátových sítí a dat pomocí metod WEP, WPA, WPA2, Radius.

1.1 Síťové prostředky

1.1.1 Síť všeobecně

Síť je systém více mezi sebou propojených systémů (zařízení), např. počítačů, tiskáren, terminálů, výrobních linek atd. Datová výměna je zajištěna nejčastěji pomocí optických kabelů a kabelů Twisted Pair (kroucená dvojlinka), bezdrátových sítí Wi-Fi ve formě hvězdicové sítě. V sítí jsou zařazeny uzly, ke kterým se připojují počítače, další uzly nebo jiná zařízení. Komunikace probíhá mezi serverem a klientem nebo peer to peer.

Dělení sítí podle rozlehlosti:

- **P**ersonal **A**rea **N**etwork, 10 metrů, často bezdrátové (WiFi), domácí sítě
- **L**ocal **A**rea **N**etwork, 100 metrů, v rámci jedné budovy
- **C**ampus **A**rea **N**etwork, v km, v rámci firmy
- **M**etropolitan **A**rea **N**etwork, v 10 km, v rámci města
- **W**ide **A**rea **N**etwork, 100 km, v rámci ČR, Evropy apod.
- **G**lobal **A**rea **N**etwork

Dělení podle topologie:

- Sběrnicová (Bus topology)
- Hvězdicová (Star topology)
- Kruhová (Ring topology)
- Páteřní síť (Backbone)

Topologie je způsob, jakým jsou stanice v síti propojeny. Topologie je prvkem síťového standardu a podstatně určuje výsledné vlastnosti sítě.

U sběrnicové topologie je použito běžné vedení, od stanice ke stanici. Stanice se k vedení připojují pomocí odbočovacích prvků (např. T – konektor). Jako přenosové médium se používá koaxiální kabel.[]

Hvězdicová topologie je dnes nejvíce rozsáhlá. Každá stanice je připojena vlastním kabelem. Kabely od stanic jsou pak soustředěny do rozbočovače (koncentrátoru, HUBu), který tvoří střed sítě. K hvězdicovému propojení se používá kroucené dvojlinky.

Kruhová topologie spojuje stanice v souvislý kruh, což dovoluje použít metodu postupného předávání zpráv (token). V případě přerušení vedení dojde k poruše na celé síti.

U páteřní sítě (backbone) jde o vedení, kterým jsou propojeny ostatní segmenty sítě. Veškerá komunikace stanic přesahující jeden síťový segment pak prochází právě tímto vedením. Je jasné, že od něho požadujeme vysokou přenosovou rychlost, minimálně 100Mb/s.

Dělení podle komunikace v sítích:

- Sítě spojované (with connection)
- Sítě nespojované (connectionless)

Spojované sítě neboli sítě s navazováním spojení. Před zahájením výměny dat je mezi oběma koncovými stanicemi nutné navázat spojení. Koncové uzly v síti se musí nejdříve domluvit s aktivními prvky a následně vytvořit virtuální kanál, prostřednictvím něhož budou přenášena data. [6]

Sítě nespojové neboli bez navazování spojení. Data jsou vysílána do sítě a koncové stanice si přečtou jen ty packety, které jim patří. Ve skutečnosti je v sítích k dispozici řada aktivních prvků, kterými jsou packety filtrovány a usměrňovány.

Dělení podle přístupových metod:

- CSMA/CD Metoda náhodného přístupu (Carrier Sense Multiple Access/Colision Detection), stochastická metoda
- Token Ring, deterministická metoda
- Token Bus, deterministická metoda

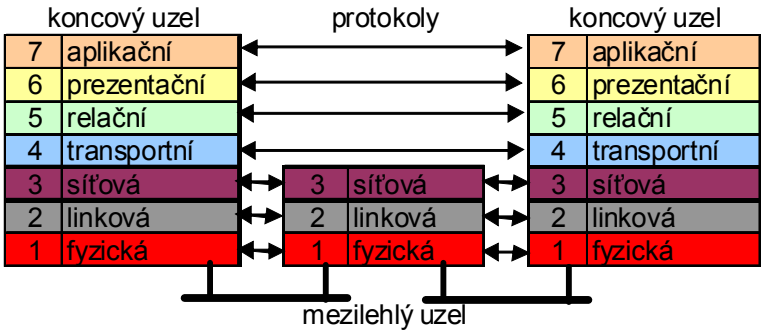
CSMA/CD postupuje při rozhodování o tom, která ze stanic bude vysílat následovně: Stanice, která chce vysílat, zkontroluje, zda již nevysílá jiný počítač. Pokud to tak je, počká, až bude na spojovacím kabelu klid. Když zjistí, že je na kabelu volno, začne vysílat. Může se však stát, že ve stejném okamžiku začne vysílat i jiná stanice. Každá vysílající stanice si kontroluje, zda signály šířící se po vedení odpovídají tomu, co sama stanice vysílá. Pokud tomu tak není, stanice se odmlčí a po náhodně stanovené době se pokusí o nové vysílaní.

Token ring je principiálně jednoduchý. Sítí koluje packet – token. Vysílat může ta stanice, která momentálně token vlastní. Token si stanice postupně předávají. Je tak zajištěno pravidelné rozdělování vysílacího času mezi stanice. Metoda Token ring se používá v sítích s kruhovou topologií, kde packet (token) může putovat od jedné stanice k druhé po kruhu, v němž jsou sanice zapojeny.

Token bus je kopií metody token ring, ale pro její činnost není nutná podmínka kruhové topologie. Každá stanice v síti obdrží logickou adresu. Token pak cyklicky putuje od adresy k adrese.[6]

1.1.2 Model ISO/OSI

Počítačové sítě vyvíjelo více firem, z počátku to byly uzavřené a nekompatibilní systémy. Hlavním účelem sítí je však vzájemné propojování, a tak vyvstala potřeba stanovit pravidla pro přenos dat v sítích a mezi nimi. Mezinárodní ústav pro normalizaci ISO (International Standards Organization) vypracoval tzv. referenční model OSI (Open Systems Interconnection), který rozdělil práci v sítích do 7 vzájemně spolupracujících vrstev.[6]



Obr. 1 Architektura modelu OSI

Aplikační vrstva představuje nejvyšší 7. vrstvu architektury. Při komunikaci poskytuje koncovým aplikačním procesům podpůrné aplikační funkce ASE (Application service element). Obvykle je členěna na podpůrné aplikační funkce SASE (Specific ASE) a podpůrné aplikační služby CASE (Common ASE). Služby CASE jsou obvykle vázány na určitý okruh aplikací jako například k přenosu souboru, elektronické poště, terminálovému přístupu.

Prezentační vrstva určuje a upravuje tvar dat, v jakém jsou dostupné uživateli (abstrakt syntax) a jakým se přenášejí sítí (transfer syntax). Do její působnosti spadá formalizace datových struktur, kryptografické metody a vlastní komprimace přenášených dat.

Relační vrstva vytváří tzv. relace, tj. časové intervaly, v nichž probíhá vlastní komunikace mezi aplikačními procesy. Vrstva řídí synchronizaci přenosu, přiděluje pověření k přenosu.

Funkce synchronizuje a vytváří kontrolní body, od nichž je možno pokračovat v přenosu při poruchách.

Transportní vrstva je poslední vrstvou, která řeší komunikaci koncových prvků systému. Přijímá data z relační vrstvy, rozkládá je na menší části, pakety, potvrzuje správnost přijetí a odevzdává je síťové vrstvě. Zabezpečuje, aby se všechny části zprávy dostaly (přes síťovou vrstvu), multiplexuje a demultiplexuje data mezi transportními spoji koncových procesů, sestavuje nebo ruší několik spojení současně.

Síťová vrstva zabezpečuje adresování a směrování dat (paketů) v síti od zdroje k cíli přes několik mezilehlých prvků. Směrování může být vykonáváno dynamicky na bázi aktuálního stavu komunikačního systému, kdy se přenosová cesta dynamicky mění při průchodu paketů jednotlivými mezilehlými prvky, tzv. *datagramová služba*. V jiném případě se na začátku spojení nejprve vytvoří virtuální cesta přes mezilehlé prvky, kterou jsou potom v průběhu spojení přenášeny pakety, tzv. *spojově orientovaná služba*.

Linková vrstva poskytuje funkce zabezpečení spolehlivého spojení, kterou se přenášejí data po fyzických přenosových médiích mezi komunikujícími prvky. Vrstva formátuje přenášená data (zprávy, pakety) do datových rámců (frame) obsahujících potřebné informace pro adresování uzlů na lince a zabezpečení přenosu proti chybám. Vlastnosti vrstvy je rozpoznávání rámců. Proto každý rámec obsahuje na začátku i na

konci speciální kódy určené k synchronizaci a rozpoznání začátku rámce (preamble). Linková vrstva variantně zabezpečuje řízení toku na lince, respektive obsluhu chybovosti, číslování rámců a opakování přenosů poškozených rámců.

Fyzická vrstva umožňuje přenos jednotlivých bitů komunikačním kanálem bez ohledu na jejich význam. Zabezpečuje též synchronizaci fyzického vysílače a přijímače. Ve fyzické vrstvě jde hlavně o definici fyzických signálů používaných k prezentaci fyzické log.0 a log.1 na konkrétním fyzickém médiu. Vrstva rovněž předepisuje požadované vlastnosti přenosového média, mechanické a elektrické charakteristiky rozhraní.[6]

1.1.3 Model TCP/IP

Architektura TCP/IP (Transport Control Protokol / Internet Protokol) byla vytvořena v rámci výzkumných prací iniciovaných Ministerstvem obrany USA a pokusné akademické síti ARPANet. Protokoly TCP/IP byly vyvíjeny jako přímá náhrada za původní protokoly sítě ARPANet NCP (Network Control Protocol). Porovnání vrstev a protokolů obou architektur naznačuje Tab. 1.[6]

<table>
<tr><th>č.</th><th>Model OSI</th><th>č.</th><th colspan="3">Model TCP/IP</th></tr>
<tr><td>7</td><td>Aplikační</td><td rowspan="3">4</td><td rowspan="3">Aplikační</td><td>HTTP</td><td>DNS,DHCP</td></tr>
<tr><td>6</td><td>Prezentační</td><td>SMTP,POP3</td><td>SMNP</td></tr>
<tr><td>5</td><td>Relační</td><td>Telnet,FTP</td><td>TFTP</td></tr>
<tr><td>4</td><td>Transportní</td><td>3</td><td>Transportní</td><td>TCP</td><td>UDP</td></tr>
<tr><td>3</td><td>Síťová</td><td>2</td><td>Síťová (IP)</td><td>IP</td><td>ICMP</td></tr>
<tr><td>2</td><td>Linková</td><td rowspan="2">1</td><td rowspan="2">Síťové rozhrarní (řadič)</td><td colspan="2" rowspan="2">Packet Driver | ARP</td></tr>
<tr><td>1</td><td>Fyzická</td></tr>
</table>

Tab. 3 Síťové vrstvy podle modelu OSI a TCP/IP

1. **Vrstva síťového rozhraní** má hlavní úlohu zajistit fyzickou komunikaci uzlů sítě, přičemž mapuje funkce fyzické a linkové vrstvy. Je specifikována jen jako rozhraní sloužící k přenosu paketů IP různorodým přenosovým prostředím. Podporované jsou všechny běžné dostupné sítě a technologie přenosu.
2. **Vrstva síťová (IP)** zabezpečuje funkčnost na bázi 3. (síťové) vrstvy modelu OSI. Zajišťuje adresování sítě a nezabezpečenou výměnu paketů protokolem IP v síti,

které jsou přenášeny přes mezilehlé prvky sítě (IP směrovače). Jedná se o klasickou datagramovou službu, samostatná data se posílají po blocích (datagramech) a to nespojitě. S protokolem IP úzce spolupracují protokoly ICMP (Internet Control Message Protokol), ARP (Address Resolution Protokol), RARP (Reverse Address Resolution Protokol), SLIP (Serial Line IP) a PPP (Point-to-Point Protokol).

ICMP – slouží k odhalování a signalizaci chyb

ARP – slouží k mapování IP logických adres na adresy fyzické (HW adresy síťových adaptérů)

RARP – slouží k určování IP adresy z adresy fyzické (ten je využíván hlavně bezdiskovými pracovními stanicemi, které znají svoji fyzickou adresu, ale neznají svoji IP adresu)

SLIP – internet protokol po sériové lince, dnes je pozvolna na ústupu

PPP – dnes nejrozšířenější pro typ přenosu „bod-bod“, má některá vylepšení oproti SLIPu (menší přenosová režie, lepší hospodaření s IP adresami atd.)

SLIP a PPP jsou částečnou výjimkou tvrzení, které říká, že protokol TCP/IP se nestará o fyzický přenos dat, protože tyto dva protokoly se fyzickým přenosem skutečně zabývají.

3. **Transportní vrstva** poskytuje spolehlivou transportní službu se zabezpečením přenosu uspořádaného proudu paketů mezi komunikačními aplikacemi protokolem TCP, resp. nespolehlivý přenos datagramů mezi komunikačními aplikacemi protokolem UDP. Je mapovaná na úrovni 4. (transportní) vrstvy modelu OSI.
4. **Aplikační vrstva nahrazuje** 5. až 7. vrstvu modelu OSI a zabezpečuje vlastní aplikační služby prostřednictvím aplikačních protokolů, např. protokolu HTTP pro přístup k WWW nebo SMTP pro elektronickou poštu.[6]

Architektura TCP/IP na sebe převzala vlastnost otevřenosti zejména rozšiřováním internetu, vzájemným propojováním privátních sítí protokolem IP a podporou internetových aplikací (WWW, B2B/B2C). Architektura TCP/IP tak dosáhla dominantního postavení jako globální standard. Dnešním trendem je protokol IPv6 (Internet Protokol verze 6), který má šířku adresy 128 bitů.[6]

1.1.4 Normalizované sítě LAN / MAN podle IEEE 802

Jednotlivé síťové prvky mohou být různě kombinovány, a proto byly přijaty normy – standardy, které definují základní požadavky na technické provedení síti.

IEEE (Institute of Electrical and Electronics Engineers) standardy pokrývají fyzickou vrstvu a linkovou vrstvu rozdělenou na samostatné podvrstvy MAC a LLC. Organizace IEEE pro tyto vrstvy vypracovala množinu norem ***IEEE 802.xx***, které převzala i mezinárodní organizace ISO (Indistrial Standard Organization) pod označením ISO 8802.

Linková vrstva je v IEEE rozdělena:

1. **LLC** (Logical Link Control), je to podvrstva řízení logického spoje
2. **MAC** (Medium Access Control), je podvrstva řízení přístupu k médiu

LLC tvoří vrchní část linkové vrstvy modelu OSI. Svým horním rozhraním komunikuje se síťovou vrstvou. Je nezávislá na fyzické interpretaci sítě a její úlohou je řízení spoje, tj. vytváření, rušení a kontrola linkových spojení mezi uzly sítě. Obsahuje též funkce, jež rozpoznávají chyby přijatých dat a řídí jejich výměnu mezi uzly sítě. Vrstva tedy řídí bezpečný přenos dat mezi dvěma uzly sítě bez jejich přímého fyzického propojení. Je popsána normou 802.2.

MAC tvoří spodní část linkové vrstvy, má společné rozhraní s fyzickou vrstvou, a proto zabezpečuje hlavně ty funkce linkové vrstvy, které jsou závislé na topologii sítě a použité přístupové metodě. Tato vrstva řídí přístup k médiu, určuje časový multiplex, kontroluje správnost přenášených rámců, hodnotí blokování sítě, její využívání jinými účastníky apod.

Vrstva inicializuje vysílání a příjem dat pro fyzickou vrstvu. [6]

Označení	Význam
IEEE 802.1	Rozhraní pro vyšší vrstvy
IEEE 802.2	Norma pro vrstvu LLC obecné sítě
IEEE 802.3	Ethetnet sítě, přístupová metoda CSMA/CD
IEEE 802.4	Přístupová metoda Token Bus, sítě MAP
IEEE 802.5	Sítě Token Ring, přístupová metoda Token Passing
IEEE 802.6	Sítě MAN (DQDB)
IEEE 802.7	Poradní skupina pro širokopásmové sítě LAN
IEEE 802.8	Poradní skupina pro optické sítě LAN
IEEE 802.9	Rozhraní LAN s integrovanými službami (hlas,data)
IEEE 802.10	Problematika bezpečnosti u sítí LAN
IEEE 802.11	Bezdrátové sítě LAN
IEEE 802.12	Vysokorychlostní sítě 100 VG-AnyLan (HP)
IEEE 802.13	Sítě wireless MAN, nebylo nikdy použito
IEEE 802.14	Rozhraní pro kabelové modemy
IEEE 802.15	Bezdrátové personální sítě
IEEE 802.16	Bezdrátové sítě MAN
IEEE 802.17	Pracovní skupina pro technologii Resilient Packet Ring

Tab. 4 Přehled norem IEEE 802

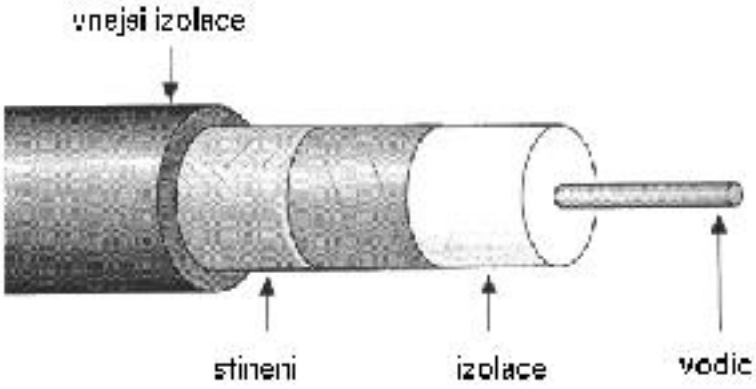
1.1.4.1 ARCnet (Attached Resources Computing network)

Jedno z prvních síťových řešení není standardem IEEE. Mezi jeho hlavní zásady patří nízká přenosová rychlost 2,5 Mb/s, přístupová metoda Token Bus, jednoduchá, nenáročná kabeláž a z ní vyplývající nízká cena. Novější variantou je ARCnet Plus s rychlostí 20 Mb/s. Kabeláž může být koaxiálním kabelem nebo kroucenou dvojlinkou, topologie Bus nebo hvězda.

1.1.4.2 Ethernet (pro 10 Mb/s)

Jedná se o známí standard v sítí LAN. Od roku 1976, kdy jej navrhla firma XEROX, se vyvíjel a dnes tak existuje více jeho variant. Mezi základní znaky Ethernetu patří kolizní přístupová metoda CSMA/CD. Při stavbě ethernetové sítě je nutné dodržovat topologická pravidla, především délku segmentu a celé sítě. Pro přenos signálu po síti je důležité, aby byly použity kabely s vlastnostmi na danou ethernetovskou síť tak, aby nedocházelo ke ztrátě dat. Proto je Ethernet dělen na standardy podle přenosového média.[6]

- 10BASE-5 (tlustý Ethernet)



Obr. 2 Koaxiální kabel

Je prvním standardem Ethernetu. Jeho základem byl tlustý koaxiální kabel s koncovkami. Jeho další vlastností je sběrnicová topologie. V dnešní době se již nepoužívá.[6]

- 10BASE-2 (tenký Ethernet)

Obr. 3 Tenký koaxiální kabel

Je dnes používaným, levným, ale náchylný na poruchy (díky mnoha spojům přenosového kabelu), při poruše kabelu havaruje celá síť, a obtížně se identifikují místa závady. Vlastní systémy propojení pomocí tohoto standardu jsou:

- Stanice se připojuje pomocí T členů nebo EAD zásuvek
- Délka kabelového segmentu je max. 189m celé sítě 910m
- V jednom segmentu max. 30 uzlů (stanic, zesilovačů, můstků atd.), celkový počet uzlů v síti nesmí být větší než 1024

- Konce kabelového segmentu musí být opatřené zakončovacím odporem (terminátorem).[6]

- **10BASE-T (kabeláž kroucenou dvojlinkou)**

Obr. 4 Kroucená dvojlinka

Je dalším standardem 802.3, dnes velmi rozšířená. Jejím základem je kroucená dvojlinka, HUB a topologie hvězda. Podle použitých prvků je možné dosáhnout rychlosti 10Mb/s. Jako jádro sítě je koncentrátor (Hub, Switch). Rozbočovače lze řadit do kaskád, ale mohou být maximálně 4 Huby (ve funkci rozbočovače) za sebou. Maximální délka kabelu mezi HUBem a PC je 100m. Maximální počet větví v kaskádě je 1024. Větší stabilita systému a při poruše jednoho kabelu vyřadí z činnosti jen jeden PC.[6]

- **10BASE-F (kabeláž optickým kabelem)**

Ethernetový předpis pro optické kabely má tři specifikace:

- 10BASE-FP (fiber passive) pro připojování stanic
- 10BASE-FL (fiber link), propojování pracovních stanic a HUBů.
- 10BASE-FB (fiber backbone) pro páteřní rozvody mezi budovami
-

1.1.4.3 Fast Ethernet (Ethernet pro rychlost 100 Mb/s)

- **100BASE-T**

Je normou, odpovídající doporučení IEEE 802.3 jedná se o metodu přenosu dat založenou na přístupu CSMA/CD. Fast Ethernet je definován ve třech variantách:

- 100BASE-TX pracuje na kabeláži s kroucenou, nestíněnou dvojlinkou kategorie 5 s využitím dvou páru. Maximální délka může být 100m.
- 100BASE-FX je určena pro optické kabely. Délka segmentu může být až 412m pro více vidové kabely a poloviční duplex, nebo až 10 km pro jednovidový kabel a duplexní režim.
- 100BASE-T4 je možné použít pro stávající rozvody kroucenou dvojlinkou kategorie 3,4,5. Maximální délka segmentu je 100m. [6]

1.1.4.4 Gigabitový Ethernet (pro rychlost 1000 Mb/s)

V dnešní době nejvíce se rozvíjející standard. Přenosová rychlost je až 1000 Mb/s.

- **1000BASE-X (802.3z – pro optické kabely)**
  - 1000BASE-SX je určena pro levné mnohovidodové optické kabely, pro kratší horizontální vedení nebo páteřní propojení.
  - 1000BASE-LX, pro dražší jednovidové a mnohovidové kabely na překlenutí delších vzdáleností
  - 1000BASE-CX definuje použití metalických kabelů – stíněné kroucené dvojlinky (STP) nebo koaxiálu, pro propojení na krátké vzdálenosti (servery, přepínače, atd.).
- **1000BASE-T (802.3ab – pro kovové kabely)**

Definují použití čtyřpásové kroucené dvojlinky kategorie 5. Je určena pro horizontální rozvody v budovách do délky 100m.

Norma [Mb/s]	Kabel	Konektor	Délka segmentu	Topologie	Maximální délka sítě	Přenosová rychlost [Mb/s]
Ethernet						
10BASE-5	koaxiální (tlustý)	AUI	500m	sběrnice	2500m	10
10BASE-2	koaxiální (tenký)	BNC	185m	sběrnice	910m	10
10BASE-T	kroucená dvojlinka	RJ-45	100m	hvězda	2000m	10
10BASE-FL	optický kabel	ST,SC	2000m			10
Fast Ethernet						
100BASE-TX	kroucená dvojlinka	RJ 45 pro UTP DB-9 pro STP	100m	hvězda		100
100BASE-FX	optický kabel	ST,SC	412m 10km			100
Giga Ethernet						
1000BASE-X	optický kabel	ST,SC				1000
1000BASE-T	kroucená dvojlinka	RJ-45				1000

Tab. 5 Přehled Ethernetů [6]

1.1.4.5 100VG AnyLAN

Vysokorychlostní síť firmy Hewlett Packard. Tento standard 100VG AnyLAN je začleněn do doporučení IEEE 802.12. Mezi základní vlastnosti sítě patří možnost přenosů rámců Ethernet i Token Ring, schopnost práce se stávajících kabeláží 10BASE-T i Token Ring a přenosová rychlost 100Mb/s.

Pro přístup ke spojovacímu vedení je použita přístupová metoda DPP (Demand Priority Protocol). Ta zajišťuje přidělování vysílacího času na žádost. Přidělování času se dělí na dvě priority, normální (pro data) a vysoká (pro servisní požadavky).[6]

1.1.4.6 Token Ring

Síť založenou na kruhové topologii a přístupové metodě Token Ring zkonstruovala firma IBM s cílem propojit počítače lokální sítě se sálovými systémy (AS4000, S390). Původní rychlost byla 4 Mb/s, později zvýšená na 16 Mb/s, posledním vylepšením je 100 Mb/s. Kategorie kabelů IBM má 6 typů. (STP, Optický kabely, kroucené dvojlinky, atd.).[6]

1.1.4.7 FDDI (Fiber Distributed Data Interface)

Síťový standard pro vysoce zatížené sítě se používal na začátku devadesátých let k propojování vzdálených areálů, metropolitních sítí a páteřních vedení. Mezi podstatné znaky patří 100 Mb/s a dvojitá protisměrná kruhová síť, optická kabeláž a přístupová metoda Token. Dva typy připojení stanic (DAS-připojeno na oba okruhy, SAS-pouze jeden kruh).[6]

1.1.4.8 ATM (Asynchronous Transfer Mode)

Používá se pro páteřní vedení a je technologií spojově orientovanou. Má konstantní délku packetu, který má 5 hlavičku a nese 48 bitů dat. Pevná délka packetu dovoluje optimalizovat ATM přepínače a dosahovat přenosových rychlostí v řádech Gb/s. Pravidelný sled krátkých packetů zajišťuje nepřetržitý tok dat, takže ATM je možné použít kromě přenosu dat rovněž pro přenos zvuku a obrazu. Hvězdicová topologie a optické kabely jsou typickými vlastnostmi ATM.[6]

1.1.5 WiFi bezdrátové sítě

Obr. 5 Logo Wi-Fi sítě

Bezdrátové sítě, Wireless LAN, nabízejí stejnou funkcionalitu a obsluhu jako klasické kabelové sítě. Pro praktické použití bezdrátových sítí je použitelná pouze jedna technologie: Wi-Fi sítě (**Wi**rless **Fi**delity, bezdrátová věrnost) podle standardu IEEE 802.11 (b, g, a, n).

Všechny varianty standardu IEEE 802.11 pracují na základě přenosu rádiových vln, liší se však frekvencemi, na kterých jsou data přenášena. Standardy **b** a **g** pracují na frekvenci 2,4-2,4835 GHz, standard **a** na frekvenci 5,150-5,350 GHz a 5,250-5,350 GHz a 5,470-5,725 GHz, standard **n** 2,4-2,4835 nebo 5,150-725 GHz.[7]

Síť	Frekvenční pásmo
Radio UKV (VKV)	87,5 - 108 MHz
Televize VHF pásmo III	174 - 216 MHz
Televize UHF pásmo IV/V	470 _ 790 MHz
Televize UHF pásmo V	814 - 838 MHz
Mobilní GSM síť D	900 MHz
Mobilní GSM síť E	1 800 MHz
Mobilní GSM síť v USA	1 900 MHz
IEEE 802.11b a odrůdy	2 400 - 2 483,5 MHz
IEEE 802.11g a odrůdy	2 400 - 2 483,5 MHz
IEEE 802.11a	5 150 - 5 725 MHz

Tab. 6 Další používané frekvenční rozsahy

1.1.5.1 Technologie IEEE 802.11

Místo kabelů je u bezdrátové sítě jako přenosové médium použit vzduch, nebo lépe řečeno schopnost vzduchu přenášet elektromagnetické vlny. Informace se na těchto vlnách v pásmu 2,4 a 5 GHz šíří od odesílatele k příjemci. Stejně jako je to u dnes již známých radiových standardů jako například FM a AM, funguje přenos signálu nabalením informace k šířícím se vlnám.

U standardu Wireless existuje několik typů modulací např.:

- CCK/DSSS (Complementary Code Keying)
- PBCC (Packet Binary Convulation Coding)
- CCK/OFDM (Coded Orthogonal Frequency Division Multiplex)
- MIMO (Multiple Input Multiple Output)

Všechny typy modulace mají společné to, že posílají datový paket sestavený ze dvou částí. Skládá se z hlavičky a datové části. Přenos dat se uskutečňuje ve formě paketů. Tento postup odpovídá postupu, který používá internetový protokol **TCP/IP** pro přenos dat. Dvě části datových paketů u bezdrátových sítí jsou informační a datové. První část slouží jako upozornění celé síti, že bude hned následovat přenos dat pro nějakého účastníka sítě (preambule). Ten má v tu chvíli se připravit pro příjem. Poté je zaslána hlavička, která příjemci sděluje, jak velká jsou přenášená data a nakonec se přenesou data jako druhá část paketu.[3]

Kontrola dat a přenos informace po síti bez kolizních stavů se musí řídit podle nějakých pravidel. Jedno z těchto pravidel je pokud se posílají data tak zařízení v síti nejdříve počkají na sdělení, jak dlouho to bude trvat (hlavička), a teprve po uplynutí této doby začnou opět komunikovat. **RTS/CTS** (Request to Send/Clear to Send). Pouze pokud na přijímacím/vysílacím kanálu žádná komunikace neprobíhá, je nový paket poslán.

U standardu Wireless LAN IEEE 802.11b jsou obě části pomocí **CCK** (Complementary Code keying) modulovány pouze na jeden nosič. Rychlejší Wireless LAN 802.11a používá modulaci na více nosičů (**OFDM**) pro data a pro preambuli (hlavičku).

Standard 802.11n

Je WiFi standard, který si klade za cíl upravit fyzickou vrstvu a část linkové vrstvy, takzvanou (Media Access Kontrol (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100Mbit/s. Nicméně maximální rychlost může být až 540 Mbit/s. Zvýšení rychlosti se dosahuje použitím **MIMO** technologie, která využívá vícero vysílacích a přijímacích antén.

Standard 802.11 b

Když se řekne „WiFi“, pak se má namysli většinou 802.11b, což je podmnožina obecného standardu 802.11. Většina zařízení Wi-Fi, která se v současné době používají, podporuje právě 802.11b. Technologie se ale rychle vylepšuje a tak nastupuje 802.11g. Standard 802.11b využívá spektrum 2,4 GHz, dále používá technologii Dotec Sequence Spread Spektrum (DSSS), která minimalizuje interference s dalšími zařízeními vysílající ve spektru 2,4 GHz. Standard 802.11b má teoretickou propustnost 11 Mb/s. Rychlost 11 Mb/s je srovnatelná s rychlostí 10 Mb/s standardní kabelové ethernetové sítě 10BASE-T. Z různých důvodů však připojení Wi-Fi jen velmi výjimečně dosahuje svého teoretického maxima (kupříkladu šifrování zpomaluje 802.11b, přenosy které probíhají v simplexním a ne v duplexním režimu, slabý signál atd.).

Standard 802.11a a 802.11g

Standardy 802.11a a 802.11g jsou odlišnými variantami 802.11, které lze považovat za chytřejší a mladší bratry 802.11b. Standard 802.11a využívá k přenosu 5 GHz pásmo, čímž se minimalizuje možnost interference s řadou existujících zařízení

pracujících na frekvenci 2,4 GHz (mikrovlnné trouby, otvírače garážových vrat apd.) a slibuje teoretickou propustnost až na úrovni 24 Mb/s.

Ještě novější než 802.11a je standard 802.11g fungující na spektru o frekvenci 2,4GHz a nabízející propustnost až 54 Mb/s.

Standard 802.11a zavádí určitou nekompatibilitu se standardem 802.11b. Někteří výrobci však nabízejí vybavení 802.11a, které je zpětně kompatibilní se zařízeními 802.11b. Hlavní výhodou 802.11a je to, že trpí méně poruchami od ostatních zařízení, protože nepoužívá přeplněné pásmo 2,4 GHz.

Standard 802.11i

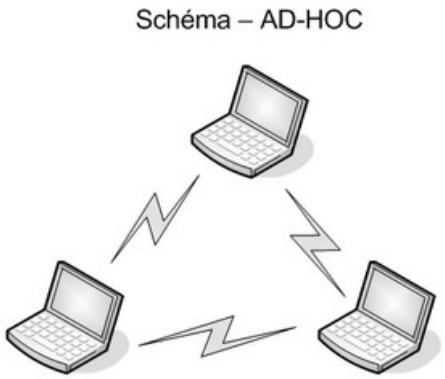
Organizace IEEE vyvíjí nový bezpečnostní standard pro 802.11 nazvaný 802.11i. Aliance Wi-Fi uvolnila podmnožinu standardu 802.11i, kterou označuje za „Wi-Fi Protected Access“ neboli WPA.

Tenhle standard zajišťuje silnější úroveň šifrování a ověřování, než je vestavěná v aktuálních standardech Wi-Fi. To znamená, že sítě Wi-Fi budou lépe chráněny před neoprávněným přístupem a dalšími bezpečnostními problémy. WPA nahradí dnes již prolomené WEP šifrování.[8]

1.1.5.2 Architektura Wireless LAN

Bezdrátová síť se od normální sítě fakticky neliší. Místo síťových karet se používají adaptéry WLAN s anténami, které jsou zodpovědné za odesílání a příjem dat. Každý WLAN je vybaven vysílačem, přijímačem a anténou. WLAN Access Point vytváří buňku, která šíří radiový signál. Počítače připojené k buňce WLAN mohou mezi sebou komunikovat přes AP nebo pomocí režimu přímého spojení.

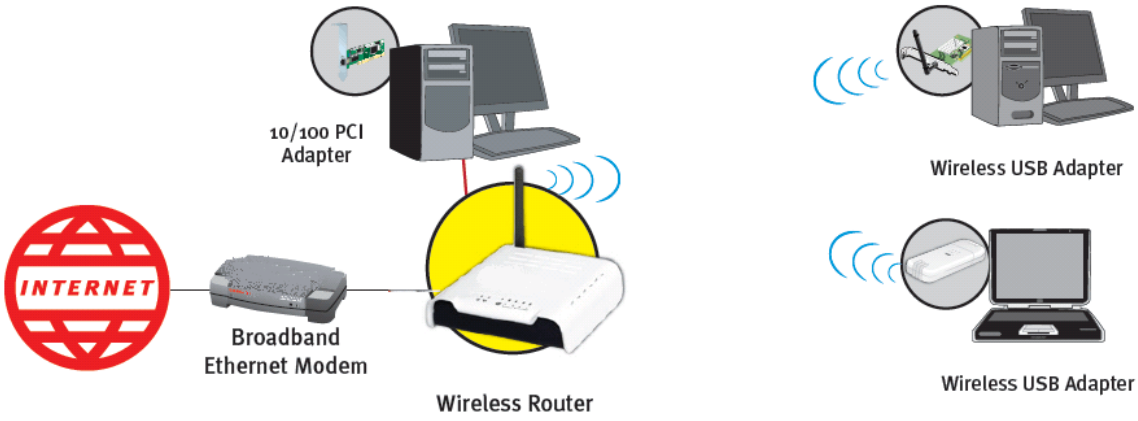
- Sítě Ad Hoc



Obr. 6 Schéma – AD-HOC

V síti typu Ad Hoc (ad hoc = ihned) spolu komunikují jednotliví klienti přímo bez jakéhokoli prostředníka. Dělí se o celou šířku pásma dostupnou v buňce, v závislosti na modelu a vzdálenosti o 11, resp. o 54 MBps brutto. Reálná šířka pásma je zhruba o 40% nižší. V této síti je každá stanice zároveň malým AP přístupovým bodem. Takto nezávislá síť se nazývá Independent Basic Service Set (IBSS).

- Sítě s Infrastrukturou



Obr. 7 Schéma sítě s infrastrukturou

V sítích s infrastrukturou musí být umístěn jeden centrální přístupový bod AP. Základní stanice (Basic Station) je připojena pomocí kabelu do klasické sítě LAN. Díky této přípojce může do sítě připojit další počítače nebo zajistit připojení internetu. Adaptéry WLAN nekomunikují mezi sebou, ale s přístupovým bodem, který vytváří bezdrátovou buňku. [7]

1.1.5.3 Aktivní prvky k přístupu síti

Bezdrátový přístupový bod (Access Point)

Přechod mezi „pevnou sítí“ a bezdrátovou sítí zajišťuje zařízení zvané přístupový bod (Access Point). Toto zařízení obsahuje konektor pro připojení sítě (RJ 45), k němuž lze připojit buď samostatný počítač, nebo rozbočovač, případně přepínač (hub, switch). Access point posílá všechna data poslaná po pevné síti také bezdrátově. Všechny počítače připojené k přístupovému bodu se dělí o dostupnou šířku pásma. U přístupových bodů nelze jednoznačně určit maximální počet klientů, toto číslo je závislé na použitém zařízení.

Obr. 8 Wireless Access Point od firmy D- Link

Dosah bezdrátových sítí je možné zvětšit použitím dalšího přístupového bodu. Stejně jako u mobilních sítí se může každý počítač při opuštění oblasti signálu jednoho AP přihlásit k jinému přístupovému bodu, který patří ke stejné síti. Tento princip se nazývá ***Roaming***.

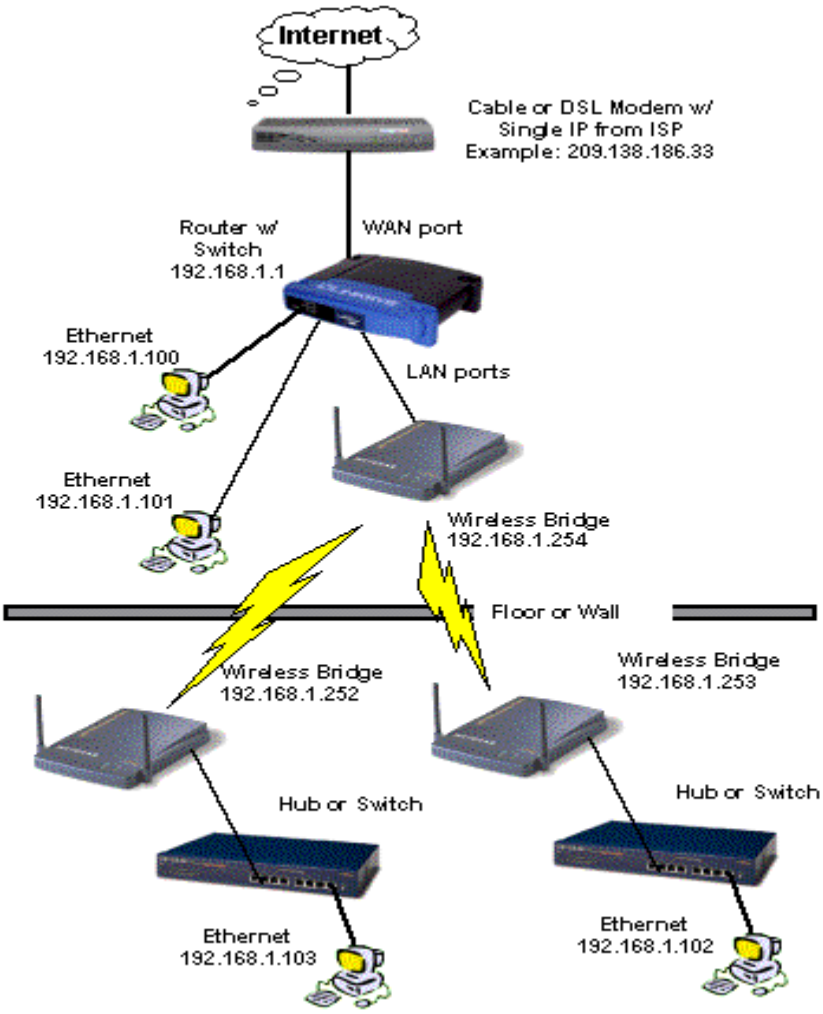
Přístupové body je často nutné propojit se síťovými rozbočovači nebo přepínači (hub nebo switch). Samostatné přístupové body spolu komunikovat neumí. Napájení AP zařízení je možné buď že sítě 220V pomocí adaptéru nebo přímo pomocí síťového zařízení které umí napájet AP po ethernetu (např. Switch 3COM 4400 PWR).

Bezdrátový přístupový bod (Access point) s AP – Bridge/Wireless Bridge

Normální přístupový bod má velmi omezené funkce. Umožňuje počítačům, které jsou vybaveny kartou WLAN, přístup k připojené kabelové síti. Spojení s dalším přístupovým bodem však není možné.

Tento typ přístupových bodů neumožňuje pouze bezdrátovou komunikaci s koncovým zařízením, ale také spojení s dalším Access pointem nebo routrem (směrovačem).

Pomocí dvou bezdrátových přístupových bodů a nainstalovaného mostu (bridge) lze bezdrátově spojit dvě sítě.



Obr. 9 Bezdrátové připojení více sítí pomocí

Wireless Bridge AP

Technikou roaming lze zvětšovat dosah bezdrátové sítě. Pomocí vloženého přístupového bodu s funkcí bridge je možné pokrýt bezdrátovou sítí relativně velký prostor. Jak AP bez tak s Bridge používá protokol TCP/IP, konektor RJ 45 pro připojení do sítě. Ke konfiguraci AP lze se setkat s konektory USB a RS232.

Broadband Router s bezdrátovým přístupovým bodem (Access Point),

Dalším bezdrátovým zařízením je router, který usnadňuje přístup k internetu. Přebírá starosti s připojením a s předáváním dat z Internetu jednotlivým počítačům a z jednotlivých počítačů na Internet. Je to vlastně jakýsi most mezi dvěma sítěmi (Internet a

WLAN). Může také regulovat přenos dat mezi těmito sítěmi. Modem (56K,DSL nebo kabelový modem) nebo kartu ISDN jako samostatný hardware pro přístup k Internetu potřebujeme i při použití routeru.

Obr. 10 Router s integrovaným přístupovým bodem a switchem

Zařízení se neskládá pouze z routeru a integrovaného přístupového bodu, ale také ze switche 10/100 Mbit, který umožňuje připojení dalších počítačů pomocí kabelu (RJ45).

Klientské zařízení k přístupu k síti

- PC Card pro notebooky jsou jedním se zařízení které je potřeba k připojení k bezdrátové síti. Jsou to High Tech zařízení s minimálními rozměry určené pro sběrnice PCMCIA. Na vylepšení signálu se používají externí antény.
- Integrovaná karta Mini PCI adaptérem WLAN přímo v notebooku je další možnost mobilního připojení na bezdrátovou síť. Anténa se obvykle ukrývá pod panelem LCD daného notebooku. V dnešní době je to standardem výrobců implementovat Wi-Fi adapter přímo do notebooku.

- Přídavné karty pro stolní počítače s adaptérem WLAN, které jsou použity, pokud uživatel chce připojit stacionární PC do bezdrátové sítě. Karty fungují na rozhraní PCI slotu je zde opět použito externích antén pro zlepšení síly signálu.
- Bezdrátový přístup s PDA (Personal Digital Asistent) pomocí karty Wireless Compact Flash a Wireless SD Card, ty mohou být použity jen v případě, že dané zařízení PDA má odpovídající slot a funkci I/O (input/output)
- Wireless printserver umožňuje připojení k síti bezdrátově zařízení, jako jsou tiskárny s paralerním a USB portem.
- Jiná zařízení trendem dnešních výrobců hardwaru je implementování WiFi adaptéru skoro do všech zařízení kterým by mobilita a nestacionarita mohla pomoci (kamery, USB zařízení, adt.) [7]

1.1.5.4 Antény

Anténa je zařízení schopné střídavou vysokofrekvenční energii (přivedenou k jejím vstupním svorkám kabelem z vysílače) vyzářit do prostoru, tedy vytvořit v prostoru vysokofrekvenční elektromagnetické pole o určité intenzitě (při vysílání). Antény pracují recipročně. To znamená, že umístíme-li je do prostředí vysokofrekvenčního elektromagnetického pole, můžeme z jejich svorek odebírat energii, jejíž velikost je intenzitě tohoto pole úměrná. To využíváme v režimu příjmu. Obecně se anténa chová jako rezonanční obvod, naladěný na kmitočet (kmitočtové pásmo), na kterém se přenos vysokofrekvenčních signálů uskutečňuje. [10]

Sledované parametry u antén:

- Pracovní kmitočet (nebo kmitočtové pásmo)
- Polarizace vyzářeného elektromagnetického vlnění
- Napájecí vlastnosti, ke kterým počítáme:
  a - jmenovitou impedanci antény
  b - činitel přizpůsobení (SWR)

- Vyzařovací vlastnosti, patří k nim hlavně:
  a - směrové vlastnosti
  b - zisk antény (dBi, dBd).

PSV (Poměr Stojatých Vln - SWR)

neboli ČSV (Činitel Stojatých Vln) je v konečném důsledku jedním z důležitých ukazatelů účinnosti celého vysílacího zařízení. V podstatě jde o to, že všechny součásti, jako výstup vysílače, vf vedení (koaxiální kabel) a anténa musí být k sobě impedančně přizpůsobeny - jejich impedance na daném kmitočtu musí být shodná. Pokud nastane tento stav je PSV rovno 1.

Impedanční nepřizpůsobení je na závadu, protože v místě připojení dochází k odrazu vf energie zpět ke zdroji. To je také důvod, proč může dojít ke zničení vysílače, pokud je použita nepřizpůsobená nebo vůbec žádná anténa. Velké množství odražené energie putuje zpět do vysílače, který se nadměrně zahřívá a nemusí to vydržet. Pokud není k vf vedení přizpůsobena ani anténa ani výstup vysílače, vzniknou mnohonásobné odrazy ve vedení, které jsou postupně ztrátami ve vedení utlumeny. Z tohoto důvodu bývá velké PSV příčinou rušení televizních pásem, kdy se odražená energie projevuje vznikem více harmonických kmitočtů (rušení televizních kanálů apod.). Odraz energie znamená samozřejmě ztrátu výkonu.[10]

PSV	Vyzářený výkon v [%]	Vyzářený výkon ve [W]
1	100	4,00
1,2	99	3,96
1,5	95	3,80
2	89	3,56
3	75	3,00
5	55	2,20
10	34	1,36
20	18	0,72

Tab. 7 Vliv PSV na vyzářený výkon

Polarizace antén

U Wi-Fi antén se nejčastěji používá kruhová nebo lineární polarizace. Lineární polarizace se v praxi používá dvojí - horizontální a vertikální. Kruhová polarizace může

být pravotočivá nebo levotočivá. Rovina polarizace vyzářeného vlnění je dána výhradně konstrukčním uspořádáním antény.

Všesměrové antény

Jak již bylo naznačeno v úvodu, všesměrové antény vyzařují signál horizontálně v rozsahu 360°, to znamená do všech stran. Vertikální vyzařování se pohybuje většinou okolo 15°. Oproti směrovým anténám mají všesměrové antény obecně podstatně nižší zisk antény. S rostoucím ziskem roste i cena, a to velice nepoměrně.

Obr. 11 Všesměrová anténa s konzolou

Běžné všesměrové antény mají tvar tyčky o délce kolem 500mm, které se obyčejně uchycují na vrchol stožáru. Není možné je umístit moc blízko zdi, protože vyzařované radiové paprsky by se od ní odrážely, a to by nebylo dobře (v tomto případě je nutné použít anténu sektorovou).

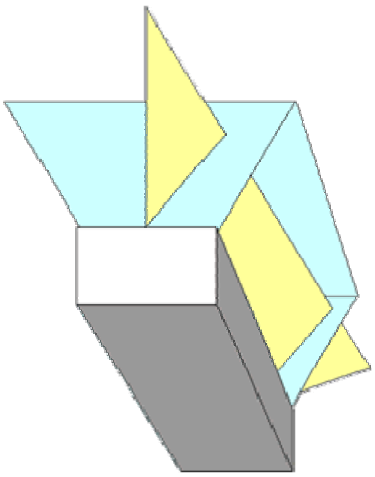
Sektorové antény

Užití sektorových antén je obdobné jako u všesměrových, to znamená, že se primárně používají jako externí antény pro přístupové body. Při jejich výběru je nutné

sledovat tři základní parametry: a) zisk antény - ten se obecně pohybuje někde mezi všesměrovými a směrovými anténami (10 - 16 dBi), b) horizontální vyzařování - až na extrémy od 30° do 180° c) vertikální vyzařování - až 30°.

Obr. 12 Sektorová anténa

Již z předchozích parametrů můžeme vyčíst, že díky variabilitě jednotlivých druhů sektorových antén můžeme lehce nalézt tu, která nám umožní pokrýt přesně to, co potřebujeme.



Obr. 13 Model vyzařování antény:

Modrá-horizontální,žlutá-vertikální

Instalace sektorových antén je stejně jednoduchá jako jakákoli jiná instalace antény. Držáky dodávané k anténě nám umožní přidělat anténu na zeď či sloup a vertikálně nastavit podle potřeby.[10]

Směrové antény

se vyrábějí buď v provedení YAGI nebo jako parabolické reflektory. YAGI antény jsou dlouhé tyče s mnoha sfázovanými půlvlnnými dipóly, které navzájem rezonují a zesilují přijímaný či vysílaný signál. Výhodou YAGI antén jsou kompaktní rozměry a nižší cena. Naopak nevýhodou jsou horší mechanické a fyzikální vlastnosti - antény často v zimě namrzají.

Obr. 14 Směrové antény YAGI, parabolická s mřížovým reflektorem, parabolická s plným reflektorem

Parabolické reflektory jsou tvořeny zářičem (dipól, malá YAGI anténa, plechovka) a parabolickým reflektorem (síto, plná parabola). Zářič ozařuje parabolickou plochu, která vlnění soustředí do úzkého paprsku. Tyto antény mohou mít zisk i 30 dBd a vyzařovací úhel menší než 10 stupňů. [10]

Velký rozdíl je mezi parabolickou anténou s mřížovým reflektorem a plným (lisovaným) reflektorem. Tzv. síto má mnohem větší postraní a zadní vyzařování a nedosahuje zdaleka kvalit plného hliníkového reflektoru.

Samostatnou skupinou jsou směrové antény s kruhovou polarizací. Jsou to "šroubovice" s vyzařovacím úhlem cca 30 stupňů, jejichž hlavní výhoda spočívá ve schopnosti přijímat jak horizontální, tak vertikální polarizaci. Používají se v lokalitách s mnoha odrazy, kde může docházet k přepolarizování signálu

(panelová sídliště, šikmé ulice atd.). Naopak jsou silně nevhodné pro point-to-point spoje - dokáží spolehlivě zarušit vše kolem sebe.[10]

1.1.5.5 Kabely a konektory

Kabely patří mezi hlavní strůjce ztrát v bezdrátových sítích, proto je vhodné volit kabely s co nejlepším hodnocením útlumu (s nejnižším útlumem) a nejlépe s předem instalovanými konektory. Kabely musí mít stejnou impedanci (obvykle 50 ohmů) jako ostatní bezdrátové prvky.

Pro WLAN je maximálně důležitý silný a jasný signál a dobrá citlivost přijímače. Z provozního a bezpečnostního hlediska mohou nevhodné kabely znamenat výraznou ztrátu signálu, a tím otevřít cestu útokům *man-in-the-middle* na fyzické vrstvě a prostřednictvím *jamming*.[10]

1.1.5.6 Výkon rádiových systémů

Vysílací výkon se odhaduje na dvou místech radiového systému. Prvním je záměrný vyzařovač (IR, *Intentional Radiator*), který zahrnuje radiový přijímač, kabeláž a konektory, druhým bodem je anténa (*EIRP, Equivalent Isotropically Radiated Power*). IR a EIRP jsou regulovány, v Evropě na základě norem ETSI.

Výstupní úroveň vysílače a vstupní úroveň přijímače se vyjadřuje v jednotce **watt [W],** nebo v jednotce **dBm ,** vztažené k 1 mW (1 mW = 0 dBm). Vztah mezi oběma jednotkami je následující:

$$P_{dBm} = 10 * \log P_{mW} \tag{1}$$

Zisk se vyjadřuje v **dBi** (i ~ izotropický). Decibely mají s watty logaritmickou vazbu:

$$X(dBm) = 10 \log X(mW) \tag{2}$$

Pro výpočet EIRP celého bezdrátového systému se hodnoty všech zařízení a konektorů sčítají. Každé zvýšení o 6 dBi zdvojnásobuje vysílací dosah (pravidlo 6 dB). Výkon souvisí se ziskem antény a také s kmitočtem, na němž bezdrátová síť pracuje.[10]

1.1.5.7 Ztráty signálu

Ztráta, kterou signál „získá“ na cestě **volným prostorem** (*FSL, Free Space Loss*), tvoří hlavní složku energetických ztrát v bezdrátových sítích. Signál samozřejmě ještě více utlumí **překážky** v jeho cestě. I skleněné okno snižuje sílu signálu v pásmu ISM o přibližně 2 dBm. Vliv na útlum signálu může, mít také počasí nebo rušení dalšími rádiovými signály.

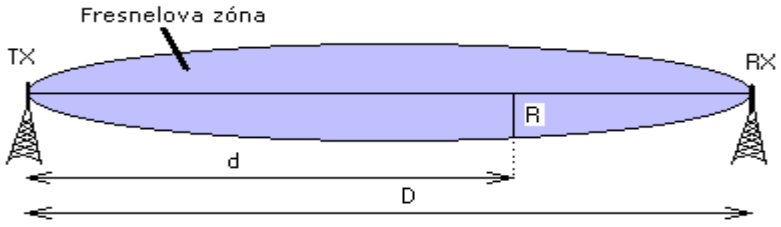
Útlum se udává v dB a je vyjádřen následujícím vztahem:

$$P_{dB} = 10 * \log(P_{in} / P_{out}) \tag{3}$$

Výpočet přibližně síly signálu v místě měření lze provést odečtením ztráty signálu na cestě volným prostorem a odhadovaných ztrát způsobených překážkami od EIRP.[10]

1.1.5.8 Fresnelova zóna

Při budování bezdrátového spoje je zpravidla uváděno, že jednou z nutných podmínek (v kmitočtových pásmech 2,4GHz a 5GHz) je přímá viditelnost mezi přijímací a vysílací anténou. To ale není podmínka postačující! Pro kvalitní přenos musí být volná (bez překážek) ještě tzv. Fresnelova zóna, tedy určitý prostor kolem spojnice (přímky) mezi vysílací a přijímací anténou. Fresnelova zóna má doutníkový tvar (elipsoid) s nejširším
průměrem uprostřed vzdálenosti mezi anténami.[11]



Obr. 15 Fresnelova zóna

V prostoru uvnitř této zóny by se neměla vyskytovat žádná překážka, ani by do ní neměla třeba částečně zasahovat (např. střecha nějakého domu nebo strom).

Narušená Fresnelova zóna většinou nemá za následek příliš podstatné snížení úrovně signálu. Jelikož ale v případě jejího narušení dochází k rušivým odrazům, snižuje se kvalita přenosu dat (ztráta paketů, nižší dosažitelná rychlost), stejně jako u nevyhovujícího přizpůsobení.

Při realizaci každého spoje by se mělo vyvinout maximální úsilí k tomu, aby bylo volných aspoň 60% uvedeného průměru zóny. Často stačí umístit anténu o kus výš, ale nezapomínejte, že Fresnelova zóna má kruhový průřez, a že její limity tedy platí i do stran. Průměr Fresnelovy zóny v jejím libovolném místě lze vypočítat, na webu naleznete mnoho stránek, které vám umožní vypočíst poloměr Fresnelovy zóny v závislosti na délce spoje, použité frekvenci a vzdálenosti překážky.V tab.6 je ukázaný maximální průměr Fresnelovy zóny v následující stručné přehledové tabulce. Je sestavena pro různé celkové délky trasy mezi anténami:

Maximální průměr první Fresnelovy zóny podle vzdálenosti a frekvence		
Vzdálenost	Pásmo 2,4GHz	Pásmo 5GHz
100m	1,37m	1,22m
200m	1,93m	1.73m
300m	2,37m	2,12m
400m	2,73m	2,44m
500m	3,06m	2,73m
700m	3,62m	3,23m
1000m	4.32m	3.87m
1200m	4.73m	4.23m
1500m	5.29m	4.73m
2000m	6.11m	5.47m
2500m	6.83m	6.11m
3000m	7.48m	6.69m
4000m	8.64m	7.73m

Tab. 8 Maximální průměr Fresnelovy zóny

podle vzdálenosti a frekvence

1.2 Průmyslové počítače (PLC)

1.2.1 Beckhoff (průmyslové počítače)

Beckhoff vyrábí otevřené řídicí systémy založené na platformě PC. Sortiment produktů zahrnuje průmyslové PC, komponenty průmyslových sítí, servopohony a automatizační software. Výrobky mohou být použity jako samostatné komponenty nebo mohou být integrovány do kompletního řídicího systému. Komponenty a systémová řešení z Beckhoffu jsou využívány v široké řadě aplikací po celém světě.

Beckhoff IPC vyhovují požadavkům v průmyslu:

- Počítače s výkonnostními procesory Intel Pentium 4
- Otevřený standard plně kompatibilní s normou ATX
- integrace elektromechanických tlačítek, přepínačů, skenerů, otočných ovládacích prvků a ostatních komponent do ovládacích panelů
- počítače vhodné pro všechny průmyslové aplikace

Obr. 16 Kontrolní panel s PC řady CP62xx a Embedded PC

Vývojové oddělení Beckhoffu provádí testování PC komponent pro průmyslové prostředí a jejich uzpůsobení pro začlenění do průmyslových PC. Mezinárodní standardy a zkušenosti s použitím počítačových systémů v těžkých průmyslových podmínkách poskytují základ pro systémové řešení Beckhoff. Ne všechny základní desky, LCD displeje, svorky nebo harddisky jsou vhodné pro využití v tvrdém průmyslovém prostředí. Při hledání komponent, které mají vyhovět náročným požadavkům na odolnost vůči

vysokým teplotám a vibracím a mají splňovat standardy elektromagnetické kompatibility, jsou vyžadovány rozsáhlé testy.

Odolnost průmyslových počítačů Beckhoff, používaných k řízení strojů a zařízení, je prověřena dlouhodobým používáním v průmyslu. Jsou alternativou tradičního řízení, která je v souladu s budoucím rozvojem systému.

Průmyslové počítače Beckhoff splňují normy a nesou značku CE. Průmyslové počítače, svorky a další počítačové komponenty jsou testovány Beckhoffem na elektromagnetickou kompatibilitu (EMC).[4]

1.2.2 Software pro Beckhoff PC, TwinCAT

Beckhoff TwinCAT software mění standardní počítač na real-time řídicí systém představující PLC systém, NC systém pro řízení os a stanici pro vývoj aplikace. TwinCAT nahrazuje běžné PLC a NC řídicí systémy s těmito prostředky:

- Otevřená platforma PC kompatibilního hardwaru
- PLC a NC software dle normy IEC 61131-3 pro operační systémy Windows NT/2000/XP, NT/XP Embedded, CE
- Možnost programování a chodu aplikace na stejném PC nebo odděleně
- připojení ke všem běžným průmyslovým komunikačním sběrnicím a počítačovým rozhranním pro I/O signály
- výměnu dat přes uživatelská rozhranní a další programy podporující otevřené Microsoft standardy (OPC, OCX, DLL atd.)

Systém TwinCAT se skládá z run-time systémů, které provádí řízení programů v reálném čase, a vývojových prostředí pro programování, diagnostiku a konfiguraci systému. Všechny programy pracující na platformě Windows, např. vizualizační programy nebo programy MS Office, mohou zpřístupnit data přes rozhranní Microsoft nebo mohou být ovládány příkazy TwinCAT.[4]

1.2.3 Beckhoff fieldbus komponenty (I/O jednotky pro všechny běžné signály)

Fieldbus toolkit

Beckhoff vyrábí širokou řadu komponent komunikačních modulů pro všechny běžné systémy průmyslových sběrnic. S inteligentními svorkami v třídě krytí IP20 a Fieldbus Box moduly v IP67 je řada kompletní pro všechny významné typy signálů a systémy průmyslových sběrnic. Komunikační karty do PC byly vyvinuty pro rychlé řízení a real-timové úlohy a mohou být použity v široké řadě aplikací. Systém inteligentních svorek je doplněn vhodnými sadami kabelů, programovacími a konfiguračními nástroji. Široká možnost výběru distribuovaných jednotek umožňuje nezávislou volbu nejvhodnějšího typu komunikačního protokolu.[4]

EtherCAT

(Ethernet for Control Automation Technology) je otevřená sběrnice Ethernet pracující v reálném čase.

Lightbus

Osvědčená optická sběrnice je charakterizována zejména dobrou odolností vůči rušení, snadnou instalací a velmi rychlým, cyklickým a deterministickým tokem dat.

Profibus

Profibus je široce užíván jako rychlá sběrnice pro decentralizované periferní komponenty (Profibus DP). Beckhoff podporuje mimo Profibus-DP a FMS také standardy pro komunikaci na servojednotky - Profibus MC.

Interbus

Interbus se snadno konfiguruje, je rychlý a spolehlivý. Posuvný registr master/slave systému nabízí vysokou efektivitu v cyklické komunikaci.

CANopen

Efektivní využití šířky sběrnice CANopen umožňuje dosáhnout rychlé reakce systému při poměrně nízké úrovni dat. Jsou zachovány typické výhody CAN, jako je vysoká bezpečnost dat a multi-master.

DeviceNet

DeviceNet je *senzor/actuator* sběrnice původem z USA, ale používá se v stále více v Evropě a v Asii. Je založena na CAN (Controller Area Net).

ControlNet

ControlNet je otevřený, standardizovaný systém komunikační sběrnice. Protokol umožňuje výměnu cyklických i necyklických dat bez jejich vzájemného ovlivnění.

SERCOS

SERCOS byl původně vyvinut jako rychlý sběrnicový systém optických vláken pro řízení os. Díky Beckhoff SERCOS komunikačnímu modulu mohou být výhody jako je vysoká míra dat a krátký cyklický čas použity také pro I/O periferie.

Ethernet

Ethernet, nejrozšířenější standard v kancelářském světě, je nyní aplikován také v automatizační technologii. Ve výrobcích lze nyní nalézt výhody Ethernetu, jako je rychlý přenos dat, snadná integrace do existujících sítí a široká řada služeb a rozhranní.

USB

USB se začlenilo mezi standardní rozhranní pro PC technologie. Díky jeho vysokému přenosu dat, flexibilní topologii a může být komunikační modul použit při malých vzdálenostech jako náhrada za komunikační sběrnici.

Modbus

Modbus je otevřený, sériový komunikační protokol založený na architektuře master/slave. Získal si přijetí díky své snadné implementaci na všechny typy sériových rozhranní.

Fipio

FIP (Flux Information Processus) je sběrnice z roku 1985, která byla později přejmenována na WorldFIP.

RS232/RS485

Klasická sériová rozhranní RS232 a RS485 jsou široce užívána. Komunikační moduly RS485/RS232 využívají jednoduchý, veřejný sériový komunikační protokol, který lze snadno implementovat.

ASi

ASi sběrnice spojuje pomocí jednoduché a energeticky nenáročné metody senzory a výkonové prvky s vyšší úrovní řízení. Toto rozhranní je mezinárodně standardizované normou EN 50295 a IEC 62026-2.

DALI

„Digital Addressable Lighting Interface“ je standardem v automatizaci budov pro ovládání elektrické instalace. DALI se používá jako subsystém, např. pro řízení osvětlení, rolet nebo teploty, a může komunikovat přímo s řídicím systémem budovy.

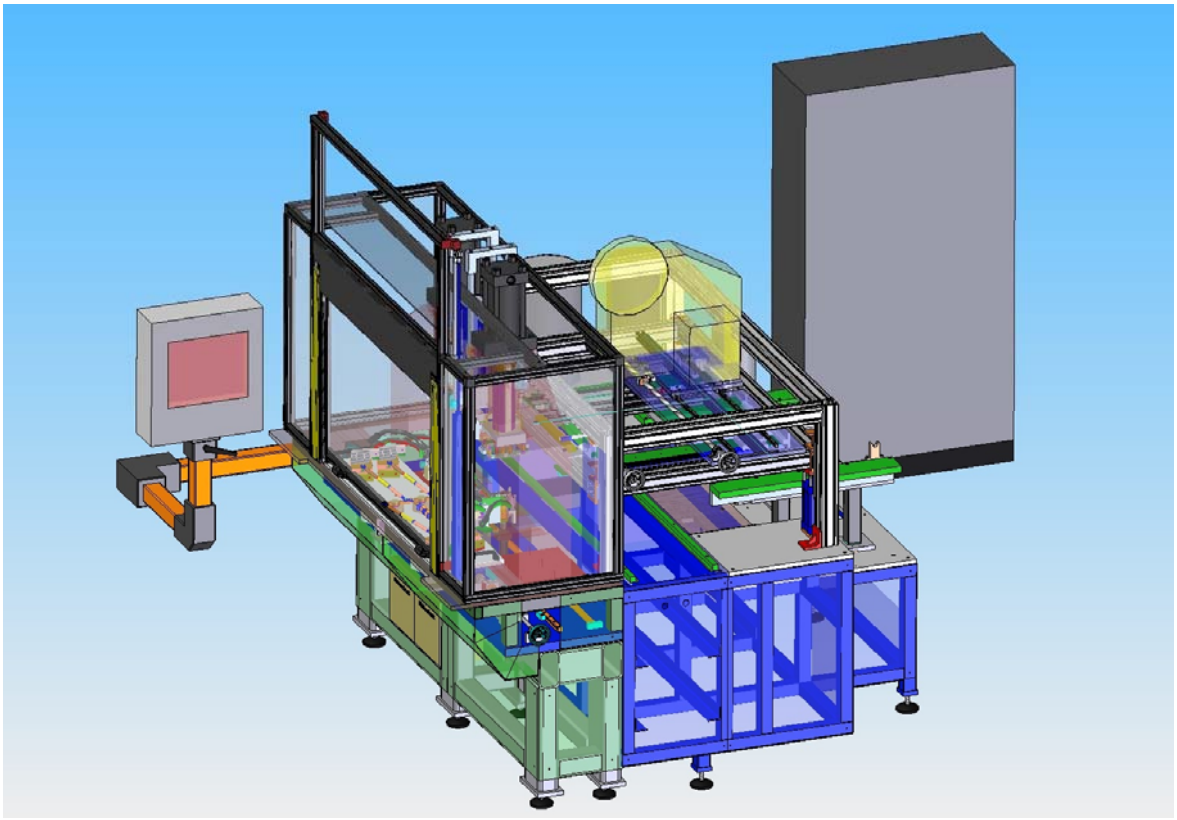
1.3 Výrobní linky

Výrobní linky jsou konstruovány pro výrobu stabilizačních tyčí do předních náprav automobilů. Jedná se o automobilní průmysl, a proto se zde kladou požadavky na přesnost a kvalitu daného výrobku. Na poloautomatických výrobních linkách je použito několik snímačů a senzorů pro různé potřeby řízení, kontroly a bezpečnostních prvků.

1.3.1 Fiat 312

Výrobní linka fiat 312 má ovládací panel firmy Beckhoff CP6202 a používá podružné Beckhoff panely BK1120 s digitálními a analogovými vstupní a výstupní moduly. Komunikace mezi jednotlivými moduly probíhá přes ethernet protokolem TCP/IP. Výstupní signály zde používají síťové karty integrované v programovatelné jednotce CP6202. Celá linka používá několik snímačů a senzorů od firmy FESTO a IFM.

Jako základní snímače jsou použity snímače indukční, protože materiál, který linka zpracovává, je s FE (železa). Dále je zde použito pneumatických pohonných mechanizmů k posunu materiálu po pásovém dopravníku. Linka má i bezpečnostní prvky jako optické snímače polohy, proudové chrániče a mechanické ochranné prvky vnitřního prostoru výrobní linky.



Obr. 17 Ovládací část výrobní linky Fiat 312

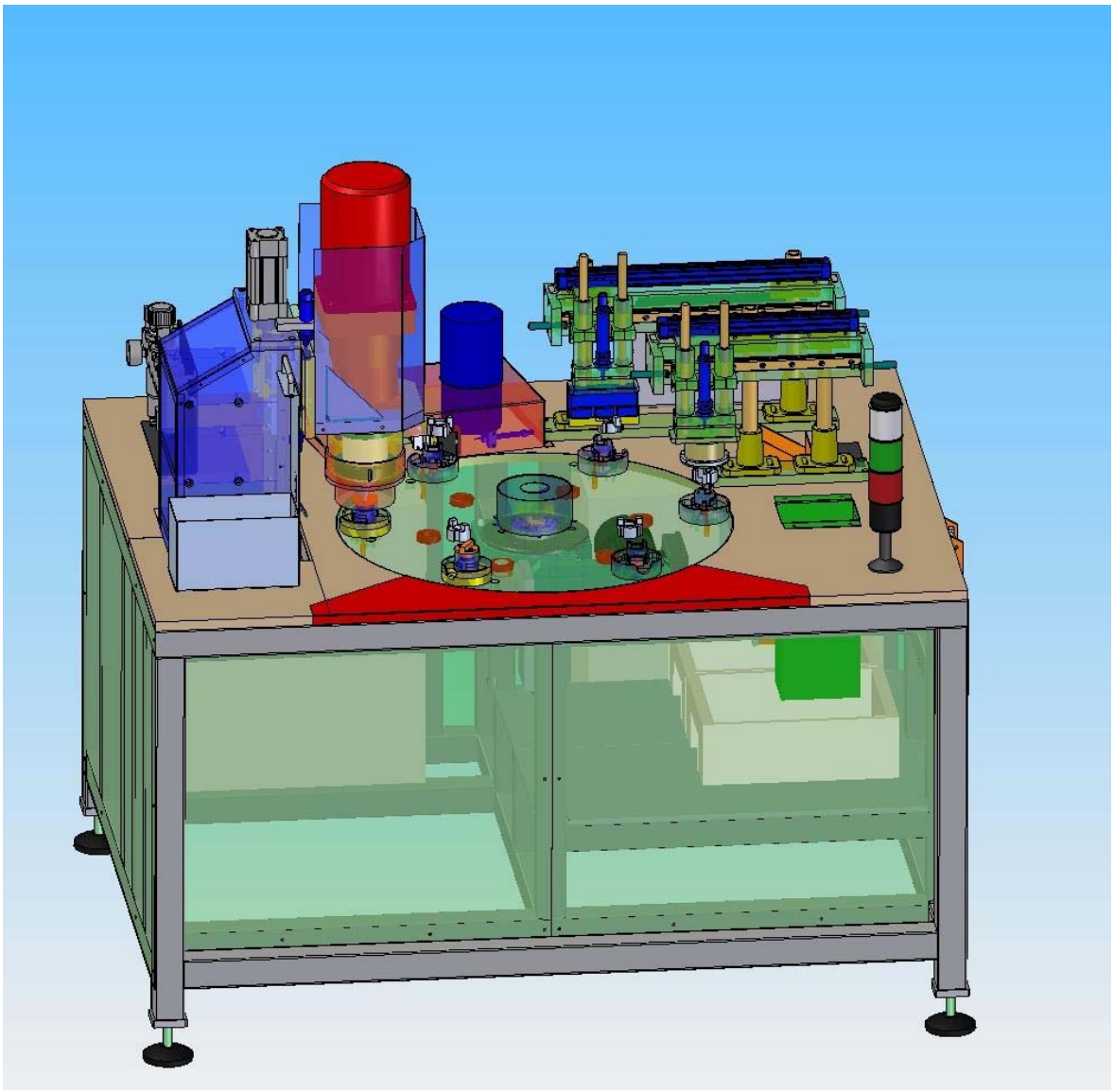
1.3.2 Porsche

Výrobní linka Porsche používá programový automat od firmy Siemens Simatic S7 - 200. V hlavním racku je namontované několik jednotek (modulů) se vstupy a výstupy jak digitálních tak analogových. Komunikace rozhraní používané v hlavní řídící jednotce je DP/MP/PPI a jednotlivé moduly vstupů a výstupů mají označení EM231 (Analog-imput), EM223 (Digital-Imput/Output), EM221 (Digital-Imput). Linka používá čtečku čárových kódů a hydraulické pohony, snímače indukční, magnetické, optické. Jako komunikační software pro programování programovatelného automatu je zde použito softwarového prostředí Microwin určené pro Siemens.

1.3.3 Vulkanizace

Výrobní linka Vulkanizace je postavena pro vulkanizaci gumových silentbloků na kovové tyče pro stabilizační účinky předních náprav u automobilů. Jako programovatelný automat je zde použito Siemens S7 400 s kontrolním panelem MV 370. Pro komunikaci je

použito sběrnice ProfiBus. Výrobní linka Vulkanizace má snímače indukční, magnetické, optické, teplotní PT100, Infra a další k hlídání celého procesu vulkanizace a posuvu materiálu po dopravním pásu. Vstupní moduly a výstupní moduly analogové a digitální jsou umístěné v rozvodné skříni společně s kompletními elektro-díly (stykače, relátka, jističe, proudové chrániče atd.). Snímače jsou zde použity od firmy FESTO a IFM.



Obr. 18 Obráběcí část výrobní linky vulkanizace

2 ZABEZPEČENÍ BEZDRATOVÝCH SÍTÍ

Bezpečnostní politika je obecně založena na principu rozpoznání autorizovaného a neautorizovaného chování. Dlouholetá bezpečnostní politika se implementuje za použití různých mechanismů, které slouží k prevenci, detekci nebo nápravě. Bezpečnostní politika podnikové sítě musí podporovat cíle celého podniku, musí být jasně definovaná jako součást organizačního řízení a odpovědnosti musí být jasně deklarovány. Politiku je třeba také periodicky prověřovat, nejlépe externími zdroji. Současně musí být použity bezpečnostní prostředky i nákladově efektivní, s vědomím, že 100% zabezpečení nejde nikdy dosáhnout.[2]

Mezi bezpečnostní služby v sítích patří následující kategorie:

- **Autentizace** (*Authenticattion*) – ověřování totožnosti druhé komunikující strany (druhá strana je tím, kým tvrdí, že je)
- **Řízení přístupu** (*Access kontrol*) – na základě identifikace uživatele umožnění přístupu do systému na základě přidělených práv
- **Zajištění utajení a důvěryhodnosti přenášených dat** (*Data confidentiality a privacy*) – ochrana před neautorizovaných únikem informací (přenášené zprávy v případě odposlechu nevydávají útočníkovi smysluplná data), typicky šifrováním
- **Zabezpečení integrity dat** (*Data integrity*) – ochrana proti neautorizované změně dat zabráněním modifikaci, duplikaci nebo zničení posílaných dat (zpráva přijatá je identická se zprávou vyslanou)
- **Ochrana proti odmítnutí původu zprávy** (nepopíratelnost, *nonrepudiation*) – zabránění odesílateli nebo příjemci odmítnout potvrzení o vyslání nebo přijetí zprávy (popření odpovědnosti) pomocí důkazu o původu a nebo důkazu o doručení

Mezi bezpečnostní služby v bezdrátových sítích patří tyto kategorie:

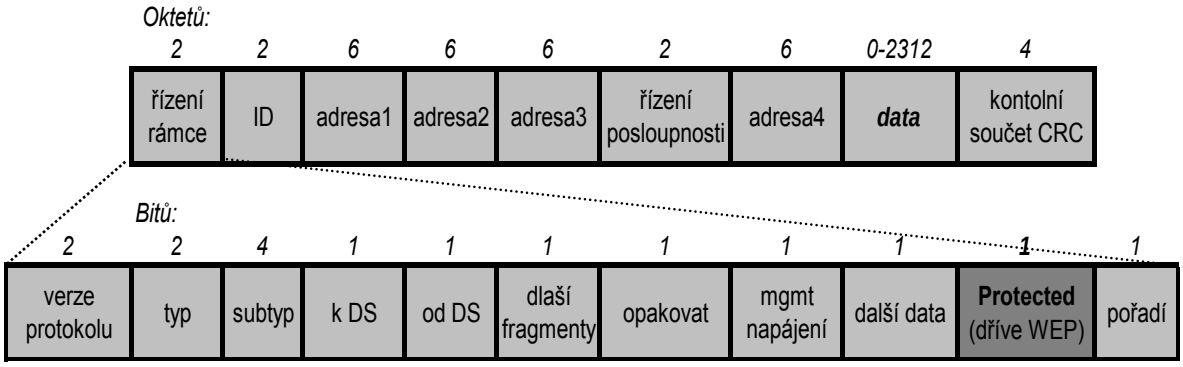
- **Kompletní a aktuální přehled o bezdrátových zařízeních** – kontrola, registrace aktualizace a monitorování používaných zařízení pro možnosti zabezpečení, aktualizaci MAC adres pro filtraci, konsistentní upgrade bezpečnostních prvků zařízení, odmítnutí přístupu pro ztracená či ukradená zařízení
- **Vzdělávání a zodpovědnost uživatelů** – důkladná znalost bezpečnostní politiky a podmínek používání bezdrátových zařízení (WLAN, bluetooth apod.)
- **Fyzické zabezpečení** – umístění prvků bezdrátové sítě tak, aby se zabránilo krádeži či odcizení nebo zničení
- **Zabezpečení na fyzické vrstvě** – EIRP v povolených mezích, volba a umístění antény, v případě potřeby použít parabolické reflektory pro blokování šíření signálu nechtěným směrem
- **Instalace sítě** – více přístupových bodů zvyšuje odolnost sítě vůči útokům *man-in-the-middle* a DoS, WLAN by měla být v jiné broadcast doméně než pevná část sítě, u přístupových bodů připojeným k různým přepínačům by všechny přístupové body měly patřit do stejné WLAN
- **Zabezpečení sítě** – u WLAN by identifikátor sítě, E(SSID), neměl obsahovat žádné informace užitečné pro potencionálního útočníka. Nastavení filtrace MAC adres, WEP, WPA/WPA2, VPN, SSH přesměrování portů atd.
- **Politika hesel** – volba délky a stylu všech hesel (nejen pro bezdrátové sítě) tak, aby se minimalizovaly možnosti útoku na hesla jak hrubou silou, tak na základě slovníku
- **Monitorování sítě a reakce na události narušení bezpečnosti** – důkladná dokumentace a řešení zjištěných narušení.
- **Audit bezpečnosti sítě** – pravidelné prověrky nejlépe externími specialisty s cílem odhalit všechna slabá místa a navrhnout jejich řešení

Bezpečnost je v každé komunikační síti na prvním místě. U radiových sítí je třeba vždy počítat s možným (snadným) odposlechem, takže je třeba zabezpečit samostatnou komunikaci tak, aby útočníkům působilo její dekódování co největší problémy.[2]

2.1 Rámec 802.11

Rámce 802.11 jsou tří typu: datové, řídící (RTS, CTS, ACK), managementu. Formát rámce MAC je naznačen na obr.15. Záhlaví rámce se skládá z následujících polí:

- **řízení rámce** (*Frame Control*) – obsahuje informace o verzi protokolu, typu rámce, pro fragmentaci rámců, management napájení a pro zabezpečení WEP
- **identifikátor** (*Duration/ID*) – obsahuje informace o době trvání rámce
- **adresy** (*Address*) – čtyři adresová pole indikují adresu sítě, zdrojovou, cílovou adresu, adresu vysílače a přijímače
- **data** (*Frame Body*) – pole proměnné délky obsahuje data a informace potřebné pro WEP
- **kontrolní součet** (*FCS, Frame Check Sequence*) – slouží pro zabezpečení rámce proti chybám



Obr. 19 Formát rámce MAC 802.11

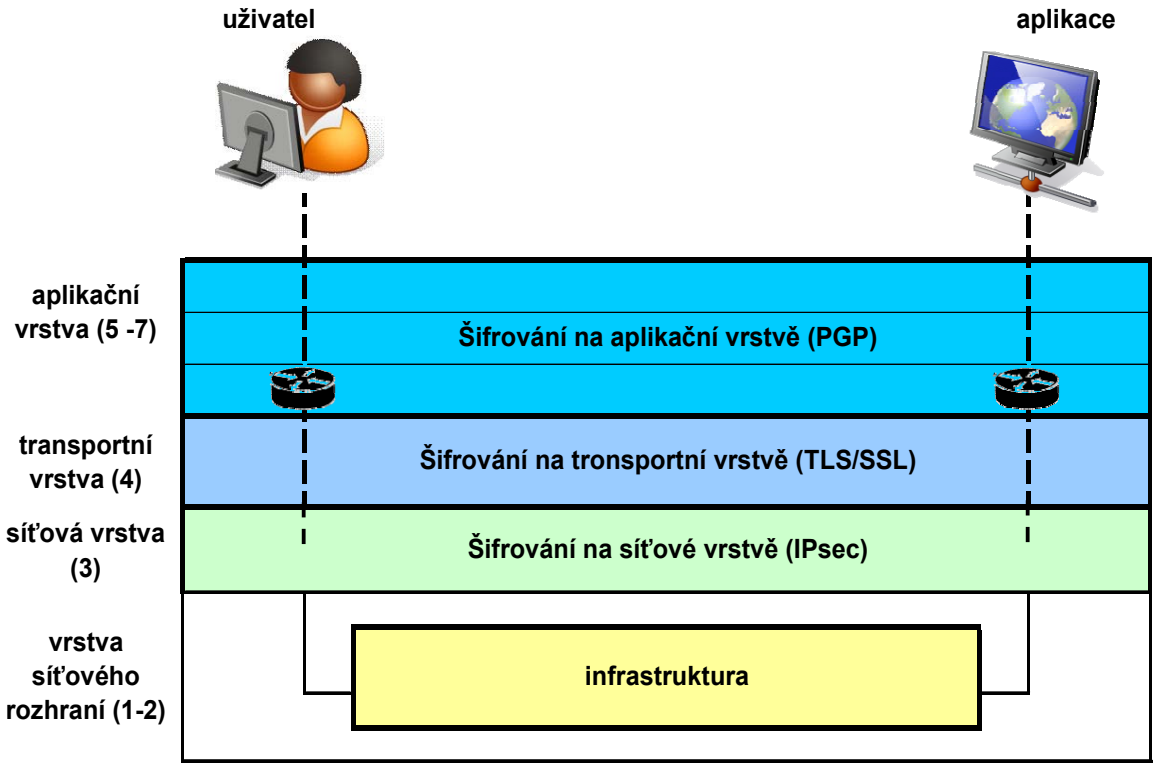
Nastavení WEP představuje jeden jediný bit (patnáctý, označovaný jako *Protected Frame*, původně *WEP bit*) uvnitř pole řízení rámce:[3]

- 0 ~ WEP není nastaven
- 1 ~ WEP nastaven

2.2 Šifrování

Existují dva základní přístupy k **šifrování**: symetricky, soukromým klíčem, a asymetricky, dvěma klíči – soukromím a veřejným.

Šifrování se může uplatňovat na různých vrstvách síťové infrastruktury jak ukazuje obr.16.[2]



Obr. 20 Implementace šifrování v sítích

2.2.1 Symetrické šifrování

Při šifrování soukromím klíčem (private key) obě strany komunikace sdílejí stejný klíč, který se tak používá symetricky (pro šifrování i dešifrování). Šifrování lze použít jak pro autentizaci, tak to ochranu dat při přenosu. Jedno z hlavních omezení používání soukromého klíče je distribuce klíče všem, kteří jej potřebují, neboť je třeba zajistit bezpečnost (silné šifrování) samotného klíče při jeho přenosu sítí. Z toho důvodu se soukromý klíč často mění. Soukromí klíč může být bezpečně uložen na počítači nebo čipové kartě.

Příklady šifrování soukromím klíčem:

- **DES** (*Data Encryption Standard, 1977*) – 56bitový klíč se používá na blok dat o délce 64 bitů (každý osmý bit se používá jako parita), rozluštěn byl v roce 1997.
- **3DES** je vylepšením s trojitým použitím klíče DES
- **AES (***Advanced Encryption Standard, 1997)* – délka klíčů 128 ($3,4 * 10^{38}$ možných klíčů), 192 ($6,2 * 10^{57}$ možných klíčů), 256 bitů ($1,1 * 10^{77}$ možných klíčů) se používají na šifrování bloků o dálkách 128, 192 nebo 256 bitů (všechny kombinace délky klíčů a šifrovaných bloků jsou možné). AES nabízí o 10^{21} více 128bitových klíčů než DES. AES se stal normou FIPS (*Federal Information Processing Standard*).

Blokové šifrovací algoritmy jako DES nebo AES mohou pracovat v různých režimech:

ECB (*Electronic Code Book)* nebo CBC (*Cipher Block Chaining)*. ECB je slabší, neboť stejný blok textu vede vždy ke stejnému bloku šifrovaného textu. CBC se proto dává přednost (např. IEEE 802.11i). CBC používá ještě inicializační vektor (**IV)**, tedy posloupnost náhodných bitů používaných jako vstup algoritmu spolu s textem. IV nemusí být tajný, ale neměl by být předvídatelný.[2]

	DES	AES
délka klíče	56 bitů	128,192 nebo 256 bitů
velikost bloku	64 bitů	128,192 nebo 256 bitů
vytvořeno	1977	2000
počet klíčů	2^{56}	2^{128}, 2^{192} nebo 2^{256}

Tab. 9 Porovnání symetrických šifrovacích metod DES a AES

2.2.2 Asymetrické šifrování

S veřejným klíčem (*Public key*) se šifrování provádí asymetricky, kdy data zašifrovaná jedním klíčem lze dešifrovat klíčem druhým, přičemž oba tyto klíče tvoří jedinečný pár vzájemně korespondujících klíčů. Jeden klíč je pak veřejně dostupný komukoli, zatím co druhý je přísně soukromý. Asymetrické šifrování tedy slouží k ochraně přenášených dat, ale nikoli k autentizaci původce zprávy, pokud použil dostupný veřejný

klíč. Každé dvě stanice mohou bezpečně komunikovat bez předchozího předávání klíčů dvojím šifrováním, soukromím a veřejným klíčem, a to v libovolném pořadí.

Velkou výhodou asymetrického šifrování je relativně jednoduchá správa šifrovacích klíčů, protože pro distribuci veřejných klíčů není potřeba zabezpečená komunikace. Soukromí klíč je udržován v bezpečí v lokálním systému a sítí se nedistribuuje, nebo se generuje nová dvojice klíčů pro každou novou relaci nebo transakci.[2]

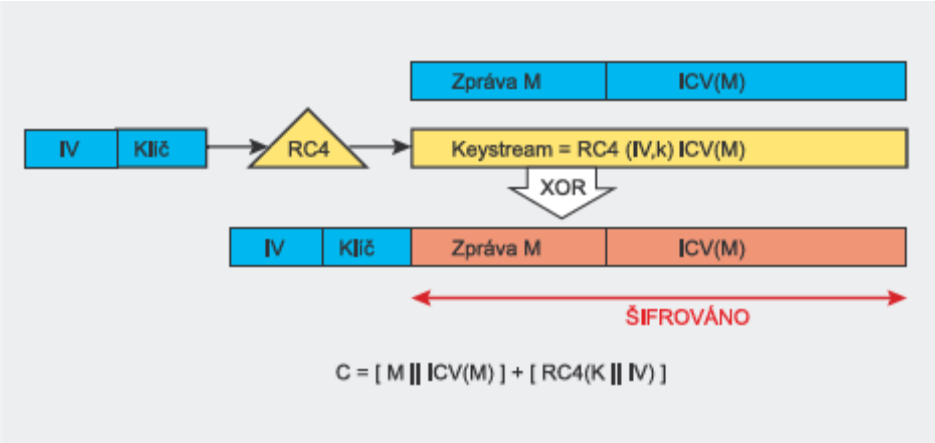
2.3 Šifrovací protokoly pro bezdrátovou bezpečnost

2.3.1 WEP

Protokol WEP (*Wired Equivalent Privacy*) pracuje jako volitelný doplněk k 802.11b *(Wi-Fi Alliance* pro certifikaci WiFi produktů WEP požaduje povinně) pro řízení přístupu k síti a zabezpečení přenášených dat. WEP byl určený pro dosažení takové bezpečnosti komunikace v bezdrátové síti, jaká odpovídá bezpečnosti v tradičních LAN (jak ostatně jeho název napovídá), ale ve výsledku tato očekávání nesplnil.

Všechny sítě 802.11 mají zabudovaný protokol WEP (*Wired Equivalent Privacy*). WEP používá symetrický postup šifrování, kdy pro šifrování dešifrování se používá stejný algoritmus i stejný klíč. Autentizace v rámci WEP je považována za velmi slabou, až nulovou. 40bitový uživatelský klíč pro autentizaci je statický a stejný pro všechny uživatele dané sítě (sdílený klíč, shared secret). Klienti jej používají spolu se svou adresou MAC pro autentizaci vůči přístupovému bodu. Autentizace se provádí pouze jednostranně, přístupový bod se neautorizuje.

V 802.11 není definován mechanismus managementu WEP klíčů, který by se staral o automatickou distribuci klíčů a jejich obnovu. Šifrování přenášených dat se provádí pomocí 64bitovým klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (Initialization Vector) v délce 24 bitů, nebo lépe 128bitovým klíčem. IV se posílá v otevřené formě a mění se většinou s každým paketem, takže výsledné šifrování je jedinečné pro každý jednotlivý paket ve WLAN. WEP používá šifrovací algoritmus RC4. Bezpečnost sítě s WEP lze narušit jak mechanicky tak odposlechem.[12]



Obr. 21 Šifrovací protokol WEP

2.3.2 WPA

WEP byl již od roku 2001 považován za zcela nedostatečný mechanismus pro WLAN, nesplňující současné požadavky na bezpečnost sítí. Proto se začalo pracovat na jeho vylepšení. Na konci roku 2002 sdružení výrobců Wi-Fi Alliance oznámilo momentální řešení pro problémy s bezpečností WLAN, pod označením Wi-Fi Protected Access (WPA). WPA bylo přijato jako dočasné řešení do doby, než bude schválen bezpečnostní doplněk normy IEEE 802.11i a než budou k dispozici slučitelné produkty.

WPA hraje roli jakéhosi mezistupně zabezpečení WLAN: je zpětně slučitelné s WEP a dopředně slučitelné s 802.11i/WPA2. Výhodou WPA jsou dynamické klíče, ale nechává si prostor i pro statické sdílené klíče. WPA používá stejný šifrovací mechanismus RC4 jako WEP. Matematická rovnice vyjádření WPA vypadá následovně:

$$WPA = \{802.1X + EAP + TKIP + MIC + (RADIUS * X)\}$$
$$If.WPA - PSK, X = 0; ELSE.X = 1 \quad (4)$$

funkce	technologie	význam
autentizace a management klíčů	**IEEE 802.1x**	rozšíření šifrování WEP prostřednictvím autorizace na portech AP s dynamickou distibucí klíčů
	EAP	různé metody vzájemné autentizace bezdrátových klientů a serverů na zálkadě hesla nebo digitálního certifikátu
autorizace a účtování	**RADIUS**	autorizace klientů pro přístup do sítě a účtování používaných služeb
utajené přenášení dat	**Temporal Key Integrity Protocol (TKIP)**	silné šifrování (dynamicky se měnící klíč pro každý paket a prodloužená délka IV) a kontrola integrity zpráv (MIC) prostřdnictvím dynamicky se měnících klíčů (s klientem, relací i paketem)

Tab. 10 Bezpečnostní prvky WPA

2.3.3 WPA2

802.11i nesoucí označení RSN (Robust Security Network), zcela nahrazuje WEP. Pro plně bezpečnou síť je nezbytný nový protokol CCMP s šifrováním podle AES, zatímco TKIP používaný pro WAP je již jen volitelný TSN (Transient Security Network). 801.11i se zaměřuje na autentizaci a utajení datových rámců. Neřeší ochranu rámců managamentu, obranu vůči DoS ani proti útokům na vyšších vrstvách. Nad protokoly TKIP nebo CCMP pracuje 802.1x starající se o robustní autentizaci a správu klíčů.

Jako autentizaci používá dvojí režim PSK a 802.1x. Autentizace probíhá oboustranně. Aby se docílilo co možná nejvyšší náhodnosti pro PSK, definuje se funkce (povinná u certifikovaných produktů) pro generování PSK z PMK.

Odvození PMK (*Pairwise Master Key*) závisí na používané autentizační metodě:

Používá-li se PSK (*Pre-Shared Key*), PMK = PSK. PSK se generuje z hesla, které tvoří více slov či shluků znaku (od 8 do 63 znaků) nebo 256bitového řetězce a poskytuje řešení pro domácí sítě a malé podniky, které nemají autentizační server.

Používá-li se autentizační server, PMK se odvodí z autentizace 802.1X MK.

K šifrování nebo kontrolu integrity se však nikdy nebude používat samotný PMK, slouží totiž pro generování dočasného šifrovacího klíče – u provozu unicast to je PTK (*Pairwise Transient Key*). Délka PTK je odvislá od šifrovacího protokolu: 412 bitů u TKIP a 384 bitů u CCMP. PTK se skládá z několika přidělených dočasných klíčů:

- **KCK** (*Key Confirmation Key* – 128 bitů): Klíč pro autentizační zprávy (MIC) během *4-Way Handshake* a *Group Key Handshake*,
- **KEK** (*Key Encryption Key* – 128 bitů): Klíč pro zajištění utajení dat během *4-Way Handshake* a *Group Key Handshake*,
- **TK** (*Temporary Key* – 128 bitů): Klíč pro šifrování dat (používaný TKIP a CMMP),
- **TMK** (*Temporary MIC Key* – 2x64 bitů): Klíč pro autentizaci dat (pracuje s ním pouze algoritmus Michael s TKIP). Přidělený klíč se používá na každé straně komunikace.[12]

2.3.4 Radius

RADIUS (Remote Authentication Dial In User Service, česky Uživatelská vytáčená služba pro vzdálenou autentizaci) je AAA protokol (authentication, authorization and accounting, česky autentizace, autorizace a účtování) používaný pro přístup k síti nebo pro IP mobilitu. Může pracovat jak lokálně tak i v roamingu.

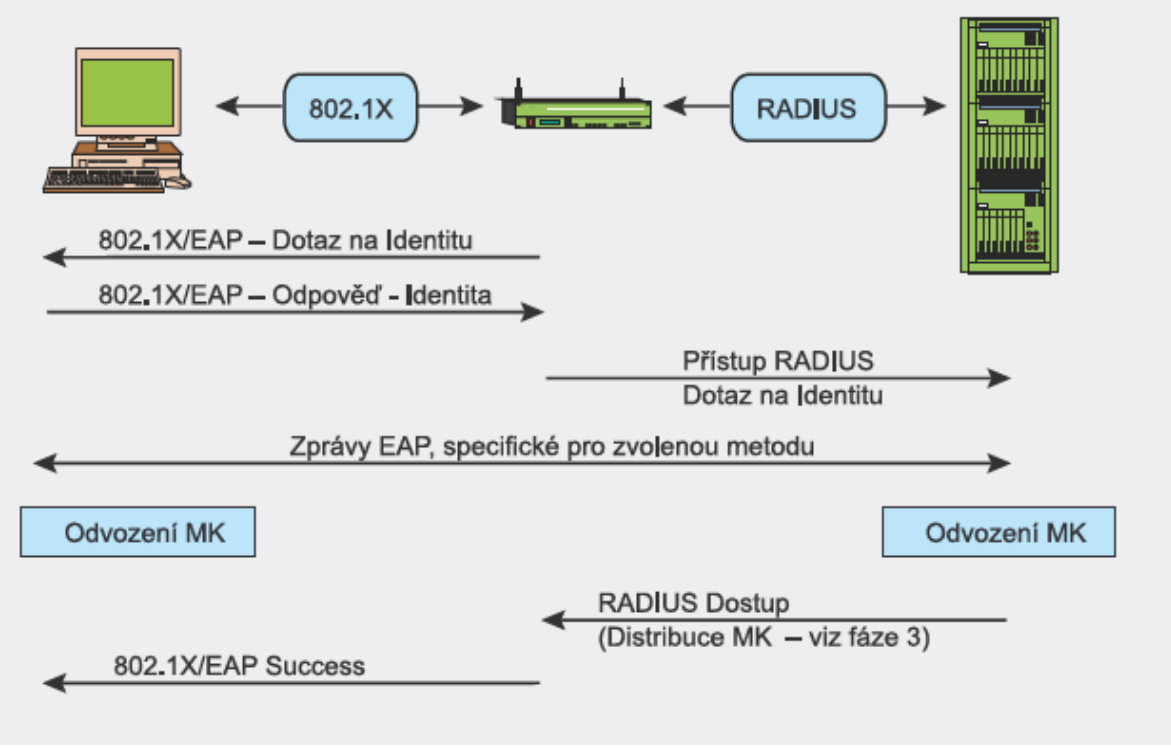
Při připojení k poskytovateli Internetu pomocí vytáčeného připojení, DSL, nebo Wi-Fi je u některých poskytovatelů vyžadováno přihlašovací uživatelské jméno a heslo. Tato informace je poslána do takzvaného Network Access Server (NAS) zařízení přes Point-to-Point Protocol (PPP). Poté je předána RADIUS serveru přes RADIUS protokol. RADIUS server ověří pravost informace použitím autentizačních schémat jako PAP, CHAP nebo EAP. Pokud je uživatelské jméno a heslo přijato, server autorizuje přístup k poskytovateli internetu a vybere IP adresu (popřípadě rozsah adres) a další parametry spojení, což mohou být např. L2TP přihlašovací údaje, doba, po kterou může být uživatel

připojen, rychlost připojení, kterou může uživatel používat, nebo jiná omezení. RADIUS protokol neposílá hesla mezi NAS a RADIUS serverem v čistém textu (ani při použití s PAP protokolem), používá se MD5 hashování.

RADIUS je jako autentizační protokol běžně používán v IEEE 802.1x bezpečnostním standardu (často používán v bezdrátových sítích). I když nebyl RADIUS původně vytvořen pro autentizační metody v bezdrátových sítích, vylepšuje WEP zabezpečení ve spojení s ostatními bezpečnostními metodami jako EAP-PEAP.

DIAMETER protokol je plánován jako náhrada RADIUS. DIAMETER používá jako transportní vrstvu TCP zatímco RADIUS používá UDP.

Oficiálně přidělené čísla UDP portů pro RADIUS protokol jsou pro autentizaci 1812 a pro účtování 1813. Přesto některé implementace používají jako výchozí UDP porty 1645 resp. 1646 (například Cisco nebo Juniper).[11]



Obr. 22 Autentizace 802.1x se serverem RADIUS

II. PRAKTICKÁ ČÁST

3 ÚVOD DO PRAKTICKÉ ČÁSTI

3.1 Rozbor základních bodů

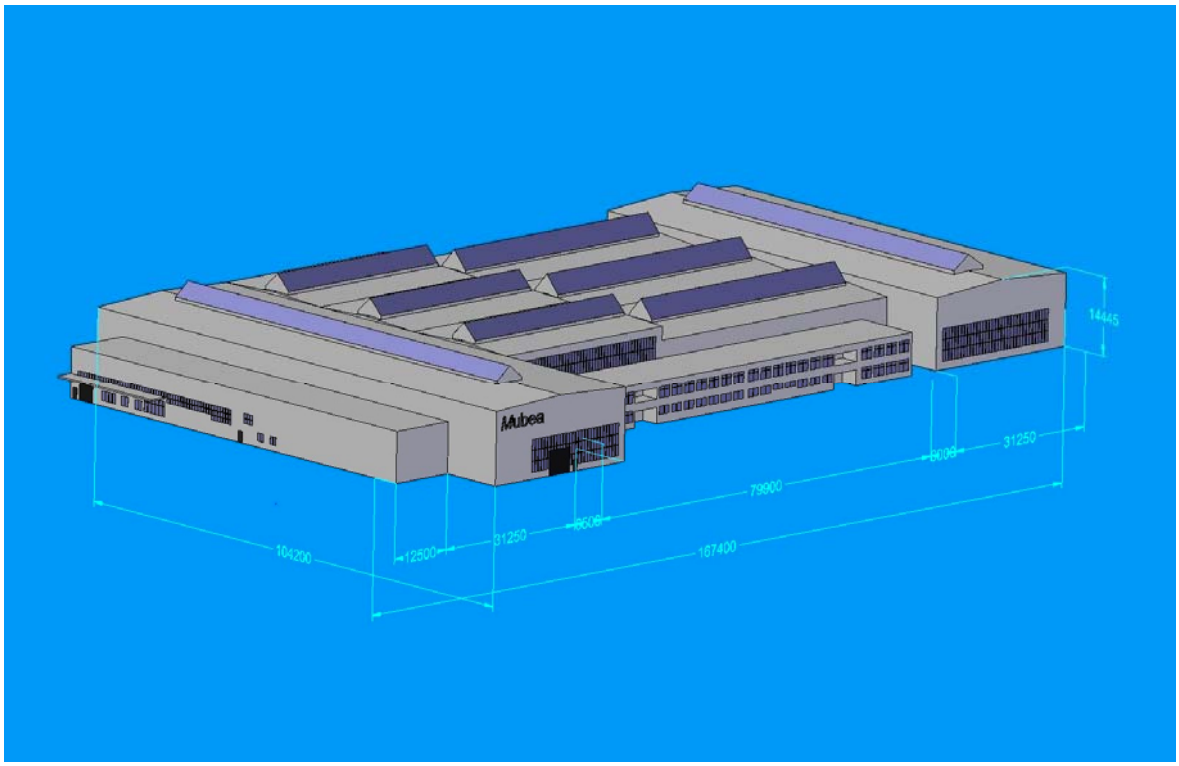
- Hlavní úkol diplomové práce je připojení výrobních linek na hale SF ve firmě Mubea HZP s.r.o. do lokální sítě LAN pomocí bezdrátových zařízení.
- Identifikace umístění výrobních linek na hale.
- Návrh na rozmístění přístupových bodů AP na hale k vytvoření kvalitní bezdrátové síti s postačující sílou signálu pro bezdrátovou komunikaci.
- Schématické zobrazení IT infrastruktury.
- Instalace, konfigurace a zabezpečení AP na výrobní hale.
- Zjištění komunikačních rozhraní na výrobních linkách a přizpůsobení zařízení na komunikaci po ethernetu.
- Instalace AP na výrobní linky, konfigurace a nastavení zabezpečení.
- Nastavení pevných IP adres na průmyslových počítačích, řídící výrobní linky, které přistupující pomocí bezdrátové technologie do sítě LAN.
- Měření odezvy při komunikaci výrobní linky -> PC v LAN síti
- Vytvoření softwaru pro vizualizaci stavů linek.
- Závěr.

3.2 Rozměry haly a fyzické rozmístění výrobních linek

Jedním z nejdůležitějším parametrem při vytvoření bezdrátové sítě je, aby byl prostor, na kterém má vzniknout bezdrátová síť, zmapován kvůli případným rušícím elementům či překážkám v bezdrátové komunikaci (šíření signálu). Rozměry výrobní haly a umístěním výrobních linek, může hrát podstatnou roli v kvalitě signálu, v případě použití omezeného počtu bezdrátových přístupových bodů.

3.2.1 Technické parametry výrobní haly

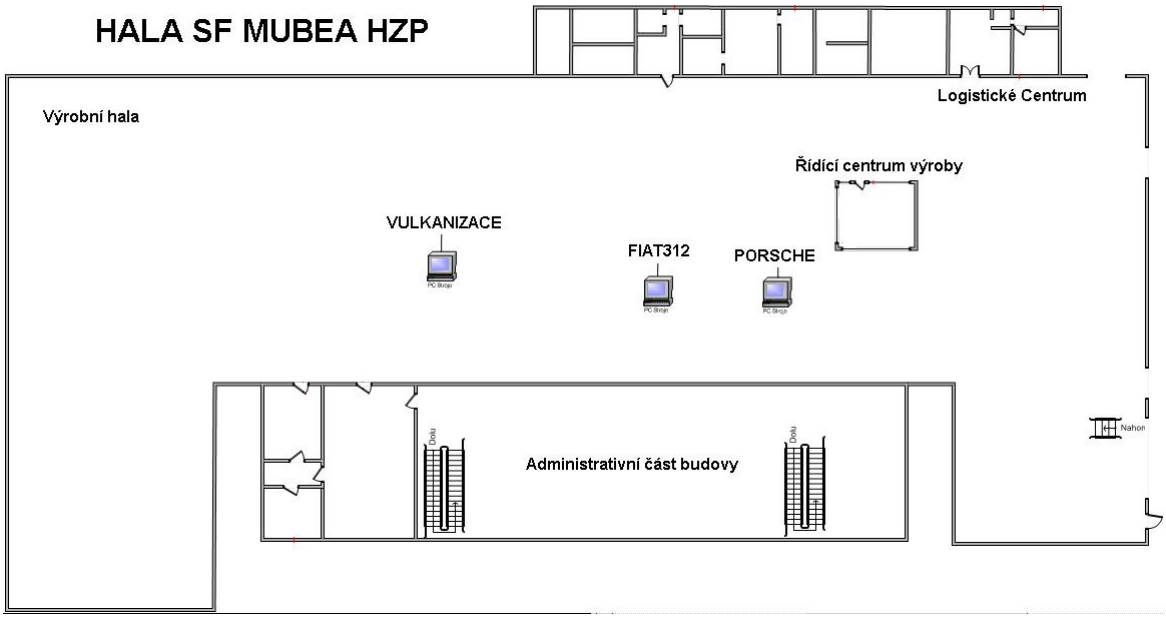
Výrobní hala SF má rozměry: délka je 160m, šířka je 104m a výška je 14m. Má ocelovou konstrukci. Střešní a stěnový pláš,ť střešní plášť, přestřešení haly ve složení: nosné tr. plechy 158/250/0,88mm. Stěnové sendvičové PUR panely tl. 60mm s viditelným kotvením kladeny svisle v barvě šedá. Celková plocha je 16 640 m^2 .



Obr. 23 Výrobní hala SF v Prostějově

3.2.2 Fyzické rozmístění výrobních linek na hale

Výrobní linky FIAT 312 a PORSCHE jsou rozmístěny v pravé části výrobní haly a výrobní linka VULKANIZACE je v části pravé. Vzájemná vzdálenost mezi sebou nepřesahuje 20m. Každá z výrobní linky má vyvýšené místo cca. 2-3m vysoké, kde je možné umístění AP zařízení. Vzdálenost výrobních linek od stěn haly je v případě linky FIAT 312 kolem 6m, linky Porsche kolem 5m a linky Vulkanizace asi kolem 10m. Schéma haly s rozmístěním výrobních linek je na obr.24

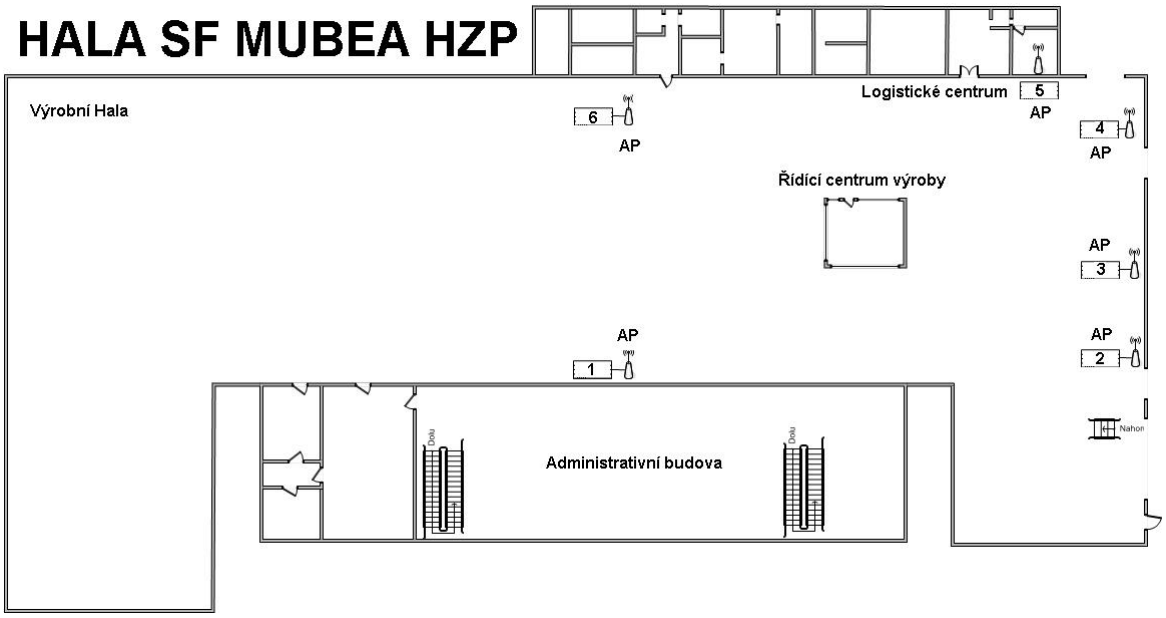


Obr. 24 Schéma Haly SF s rozmístěním výrobních linek (pohled shora)

3.3 Infrastruktura IT zařízení

3.3.1 Rozmístění AP na hale SF

Rozmístění bezdrátových zařízení na hale se rozdělilo na dvě etapy. První etapa, byla umístění AP na kovovou konstrukci haly tak, aby se dosáhlo možná co nevyšší síly signálů při komunikaci dvou bezdrátových zařízení. Zařízení bylo namontováno asi do výšky 3m, aby byla pokryta co největší část výrobní haly, z experimentálního ověření, byla tahle výška stanovena za přípustnou a dostačující. Postupným přidáváním AP po obvodu haly se zvyšovala síla signálu a tím pádem pokrytí větší a větší plochy haly. Schéma rozmístění AP zařízení na hale je na obr.25.



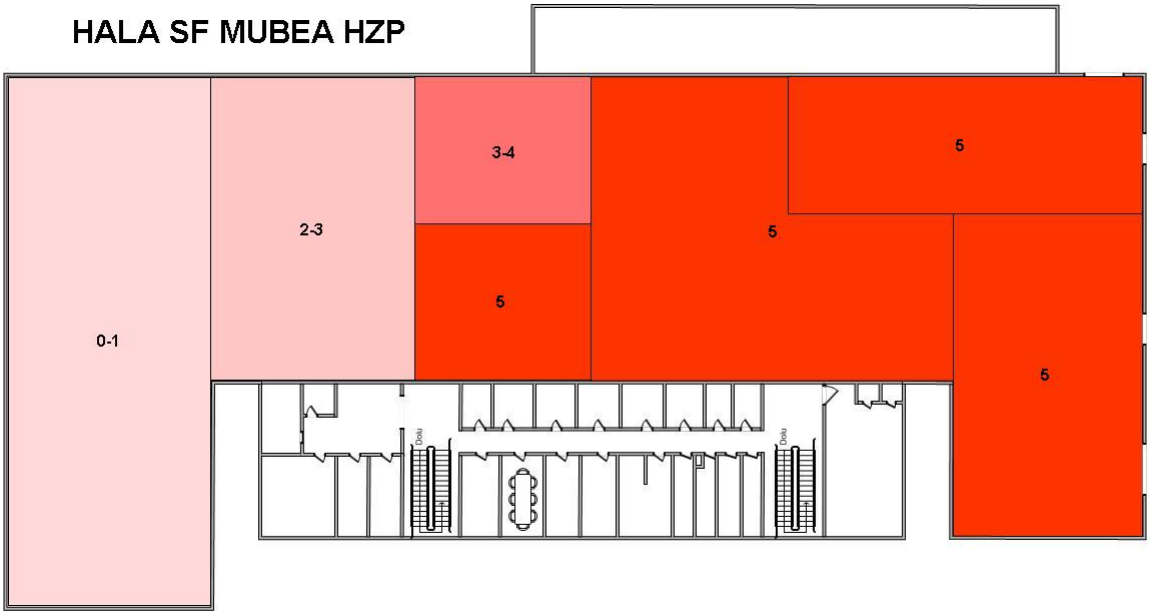
Obr. 25 Schéma rozmístění zařízení AP na hale SF

3.3.2 Měření síly signálu na hale SF

Síla signálu byla změřena pomocí dvou bezdrátových zařízení s vizualizací síly signálu připojení.

- Notebook Acer 4233WLMi s integrovanou bezdrátovou WiFi kartou (Wireless LAN 802.11a/b/g, Intel 3945ABG)
- Mobilní terminál Intermec CK31 i integrovanou WiFi kartou podporující 802.11g/b

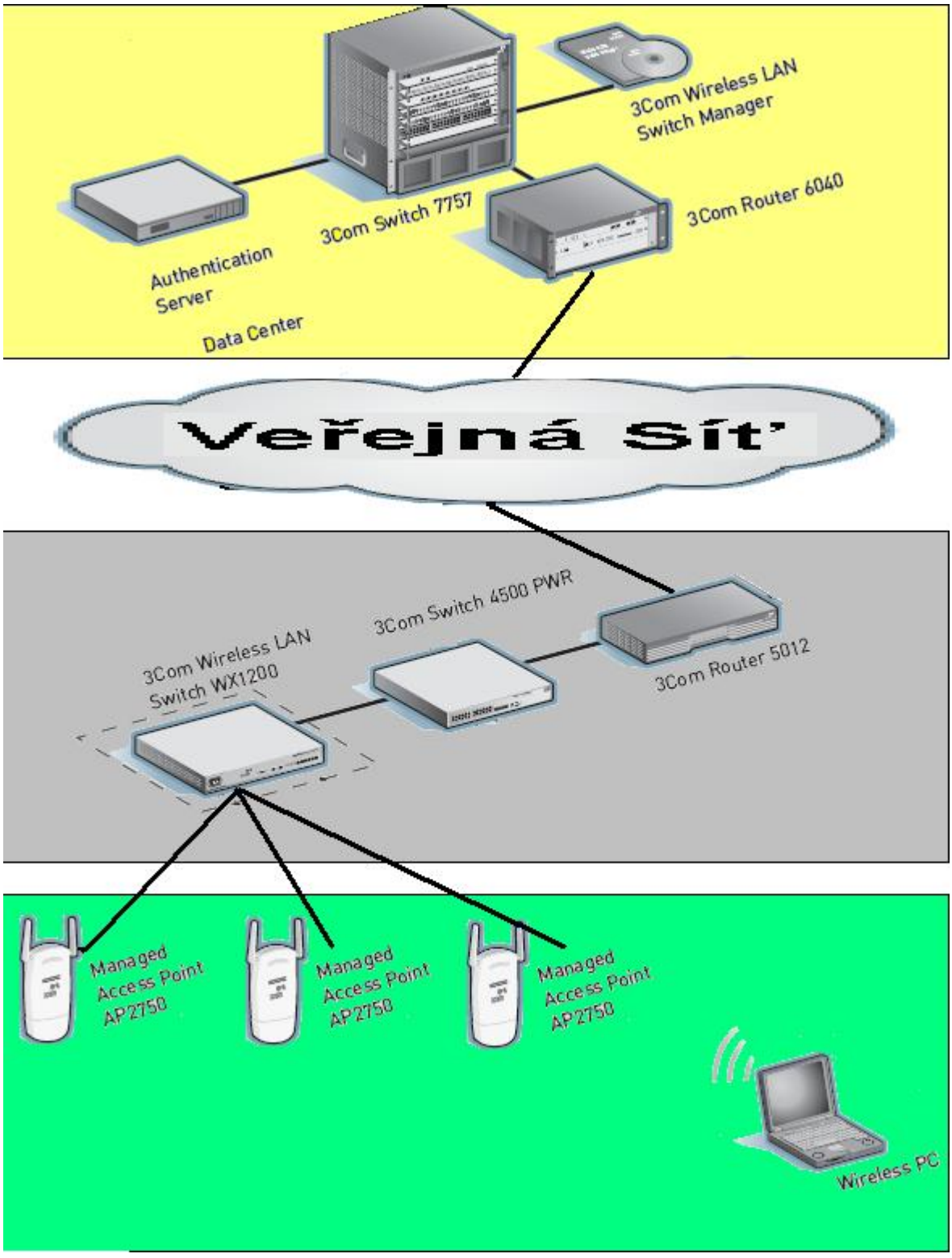
Hodnocení a stupnice síly signálu je zobrazeno na obrázku 26. Měření bylo pouze orientační a zobrazené informace o síle signálu v rozsahu 0-5 kdy 5 je nejsilnější signál a 0 žádný signál. Na spolehlivou, bezdrátovou, komunikaci mezi AP a výrobními linkami byla určena postačující hodnota síly signálu 3-4.



Obr. 26 Pokrytí signálu na hale SF (legenda: 5 velmi dobrý, 3-4 dostačující, 2-3 nedostačující, 0-1 žádný signál)

3.3.3 IT infrastruktura zařízení

IT infrastruktura podniku Mubea je založena na hardwarových prostředcích firmy 3COM. Celý centrální systém bezdrátových zařízení a ověřování autority nových bezdrátových zařízení je umístěný v hlavním IT oddělení v Atendornu v Německu (Žlutá barva v obr.28). Dále přes veřejnou síť (Internet) je komunikace zavedena do serverovny v Mubea HZP (Šedá barva v obr.28) a přes Wireless Svitch jsou připojeny jednotlivá tenká AP, která jsou rozmístěna na hale SF (barva zelená v obr.28).



Obr. 27 Centralizované bezdrátové řízení ve firmě Mubea HZP s.r.o.

4 HARDWAROVÉ PROSTŘEDKY

4.1 3COM WX1200 switch

3COM Wireless Switch WX1200 je jedním s možných řešení, při vytváření bezpečné, koncepční, bezdrátové sítě, v podnikovém prostředí, s plnou odolností proti výpadku všech komponentů. Prostředí 3COM WX1200 je určen pro připojení až 12 tenkých AP.

Obr. 28 Wireless Switche řady WX od firmy 3COM v pořadí s hora WRX100, WX1200, WX2200, WX4400

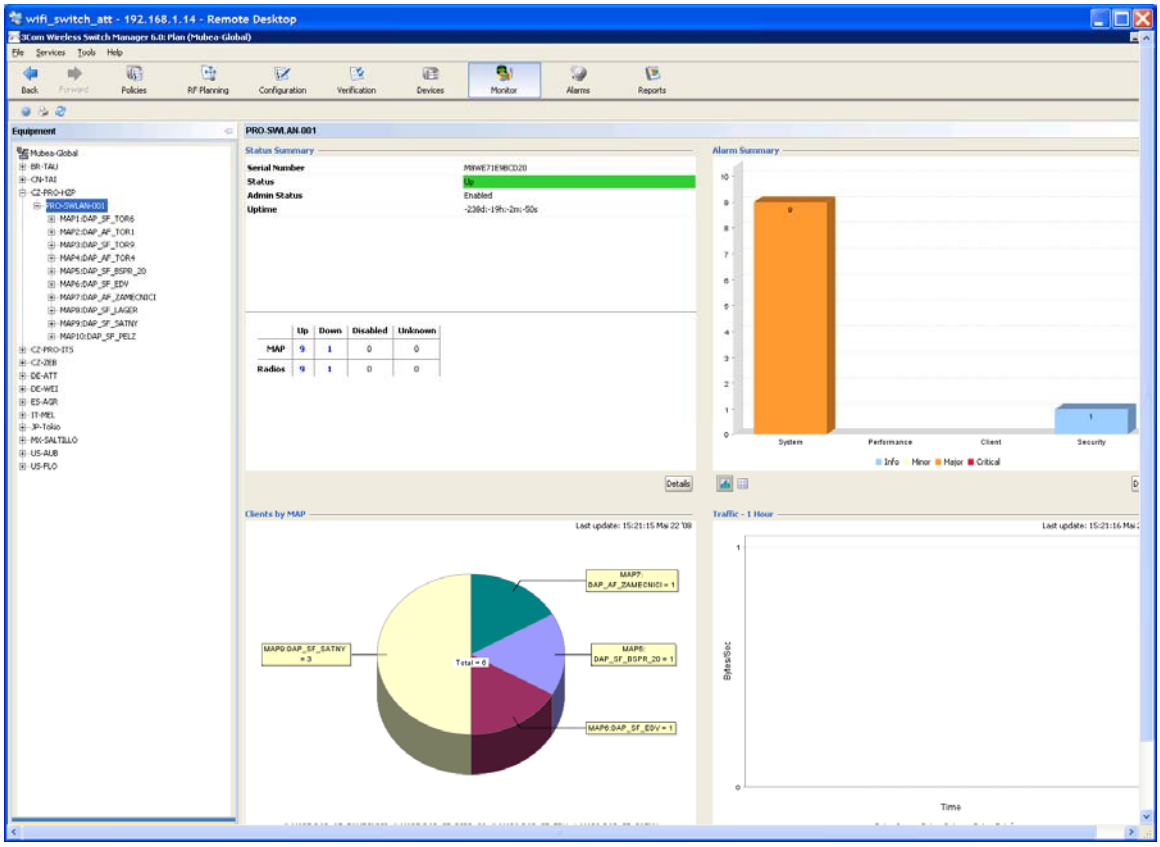
Nejzajímavější vlastnosti 3COM Wireless Switch řešení:

- Nejmodernější technologie pro ověřování, šifrování a zařazování uživatelů – bez nutné vazby na název obsluhované bezdrátové oblasti může být uživateli na základě ověření zvolen typ šifrování (WEP [64,128], WPA[TKIP], WPA2[AES]), mohou mu být přiřazeny přístupové filtry s QoS pravidla a výstup z bezdrátové sítě směrován do konkrétní virtuální sítě. Switch mimo jiné podporuje ověřování na externím nebo integrovaném webovém ověřovacím rozhraní s překvapivě snadnou obsluhou.

- Integrovaný RADIUS – V bezdrátovém switchi je integrován RADIUS server s podporou do 1000 klientů, ale systémy samozřejmě podporují i externí ověřovací autority.
- Řízení přístupů hostů – Snadné vytváření hostujících uživatelů prostřednictvím integrovaného nástroje bez dalších administrativních práv.
- Roaming bez přerušení – Systém se chová jako jeden přístupový bod s možností rádiových interface. Takže pokud provádí klientské zařízení roaming mezi jednotlivými radii systému, je stále připojen k témuž přístupovému bodu a nemusí znovu procházet celou ověřovací proceduru.
- Podpora QoS – WX dokáže klasifikovat provoz a řadit jej k odeslání na tenkých AP. WX podporuje IGMP a je kompatibilní s pre-standardem 802.11e (WMM). Splňuje požadavky na QoS dle výrobce VoIP telefonů Spectralink.
- Nízké nároky na administraci – Automatické řízení kanálů a vysílacích výkonů tenkých AP na základě topologie sítě.
- Škálovatelnost – Systém lze pomocí licenčního systému navyšovat na potřebný počet uživatelů.

4.1.1 Software 3Com Wireless Switch Manager

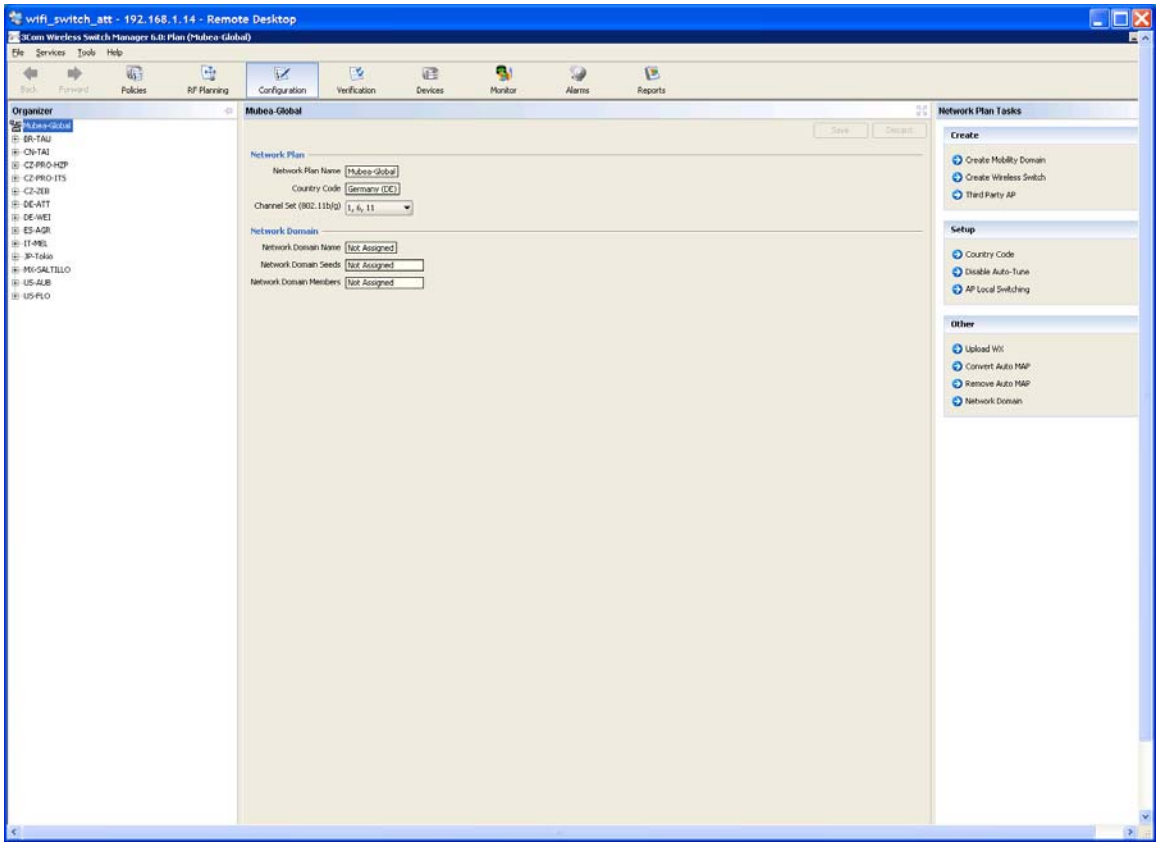
Software 3Com Wireless Switch Manager je nástroj na řízení bezdrátových přepínačů WX a jejich administrace. Pomocí tohoto softwaru je také možné konfigurovat jak jednotlivá zařízení pro řízení tenkých AP, tak jednotlivé přístupové body (AP). Software umožňuje i zobrazování historie vytíženosti sítě, aktuální monitoring sítě přehledy nových zařízení v bezdrátové síti a konfigurace jednotlivých metod zabezpečení bezdrátových zařízení.



Obr. 29 Software Wireless Switch Manager

4.1.2 Základní konfigurace Wireless Switche WX1200

V firmě Mubea Global je nakonfigurované několik wireless svitchů. Podle potřeby připojení tenkých AP jsou voleny typy switchů 3Com (WX1200,WX2200,WX4400). Jednotlivé switche umožňují připojit pouze omezené množství tenkých APOD. V našem případě je použito WX1200, který umožňuje připojit maximálně 12 AP. Celý systém je tvořen jako jeden centrální síťový plán použitý pro všechny pobočky Mubea v různých státech. Každá pobočka Mubea má nastavené svoje wireless switche stejným způsobem pro dodržení centralizovaného řízení bezdrátových zařízení. Obr. 30 zobrazuje síťový plán a jednotlivé pobočky s názvy země.



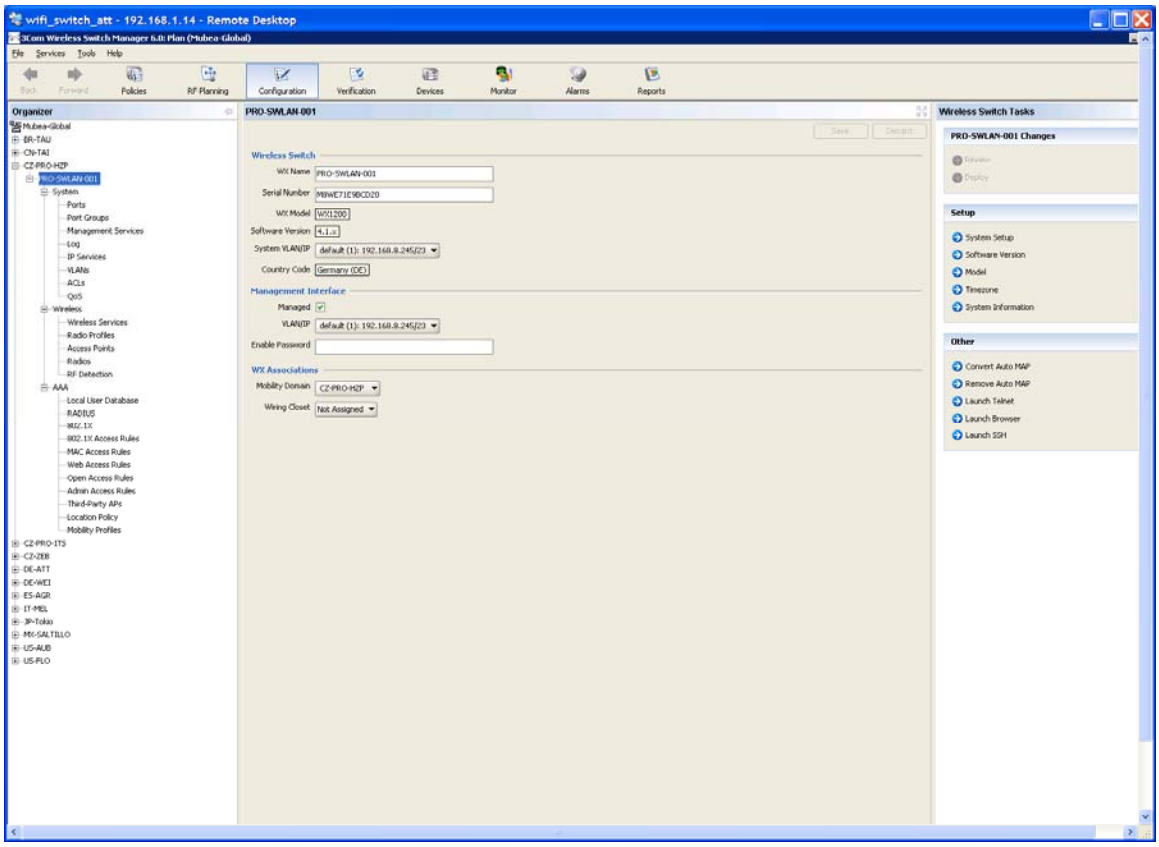
Obr. 30 Wireless Switch Manager s ukázkou síťového plánu a jednotlivých poboček Mubea

Vlastní konfigurace wireless switche probíhá pomocí wireless switche manageru. Jedním základním parametrem je pro lepší identifikaci název switche, podle umístění v jednotlivé zemi a pobočce Mubea, dále je potřeba zadat typ switche, doménu a další. (viz. Obr 31).

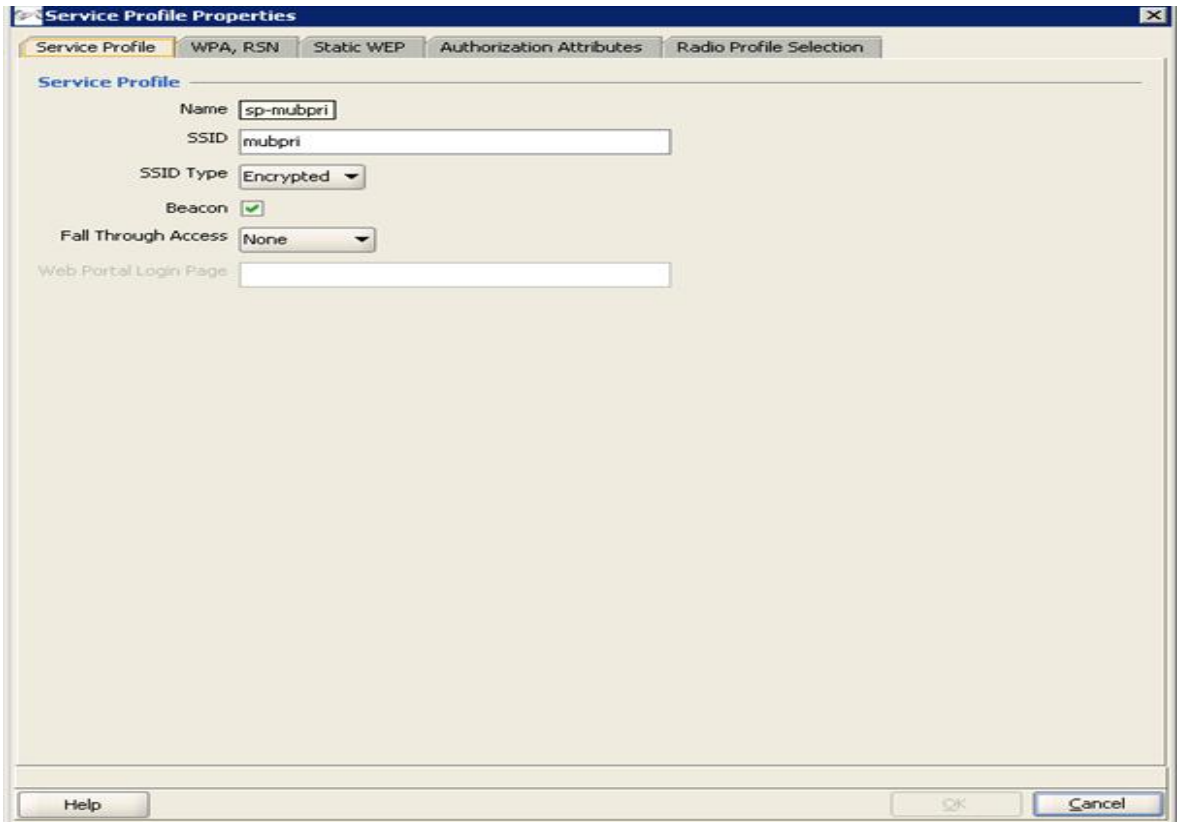
V části Wireless jsou nastaveny nejzákladnější vlastnosti wireless switche k řízení bezdrátových řízení AP. Nastavované parametry:

- Název sítě SSID (mubpri)
- Typ SSID šifrování
- Typ šifrování WPA, WPA2
- Typ autentifikačního klíče PSK, 802.11x
- Sdílený klíč mezi dvěma WiFi zařízeními periodicky se měnící (WPA)

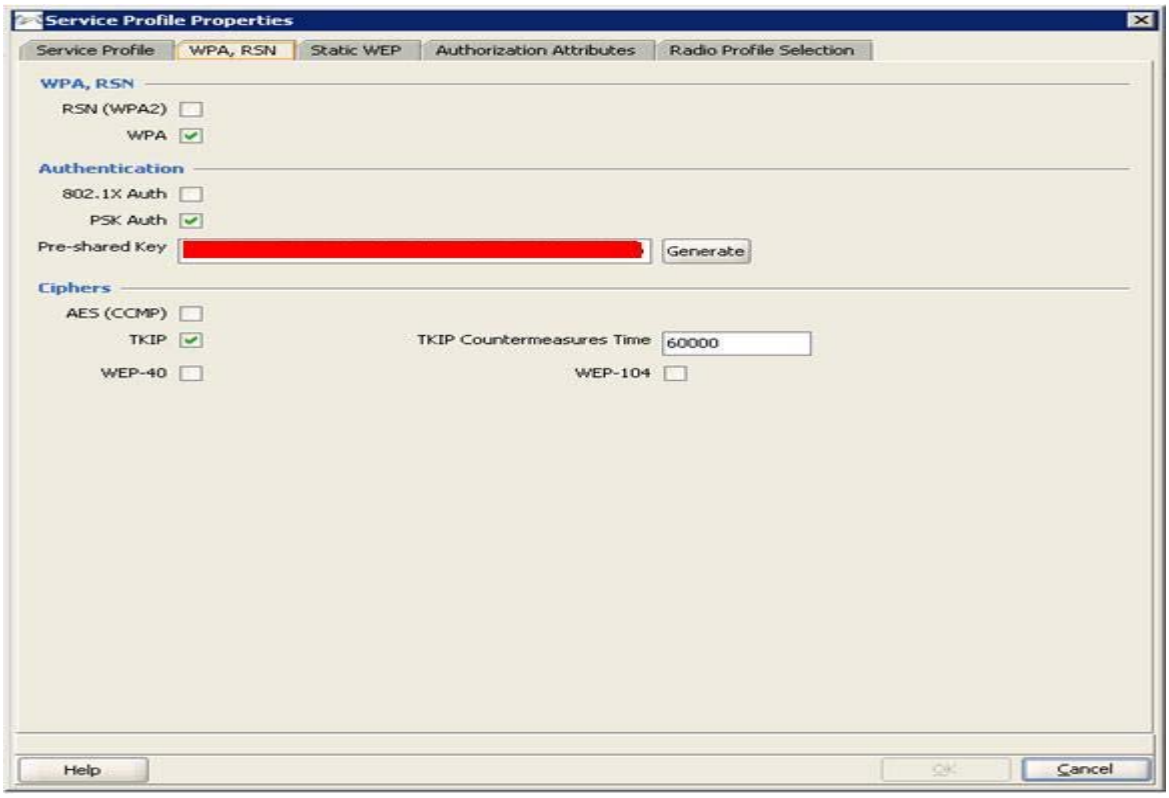
- Použitá šifra TKIP, AES, WEP-40



Obr. 31 Základní nastavení 3Com WX1200



Obr. 32 Nastavení základních Wireless funkcí WX1200



Obr. 33 Nastavení jednotlivých zabezpečení WX1200

4.2 3COM AP

Při vytváření bezdrátové sítě je důležité si uvědomit, které přístupové body budou pracovat v režimu AP a které budou sloužit pouze jako most (bridge), k připojení pevné síťové karty do bezdrátové sítě.

4.2.1 Tenké bezdrátové 3COM AP 2750

Jako hlavní přístupové body byly zvoleny AP s označením 3COM 2750. Jejich výběr byl z praxe, kdy po vyzkoušení ve výrobním prostředí, dostatečně splňovali potřebné požadavky, na bezdrátové zasíťování výrobní haly. Podporuje technologii Mesh, Bridging a Distributed Forwarding. Jsou standardizovány na a/b/g, ale je třeba zvolit u každého kanálu, zda bude vysílat v 2,4GHz nebo 5GHz pásmu. Napájení prostřednictvím Ethernetu je výhodou. Podporuje 3COM Dual-Band externí antény (R-SMA konektor) a řízení vysílacího výkonu dle generálního povolení.

Obr. 34 3COM 2750

4.2.1.1 Technické parametry AP 2750

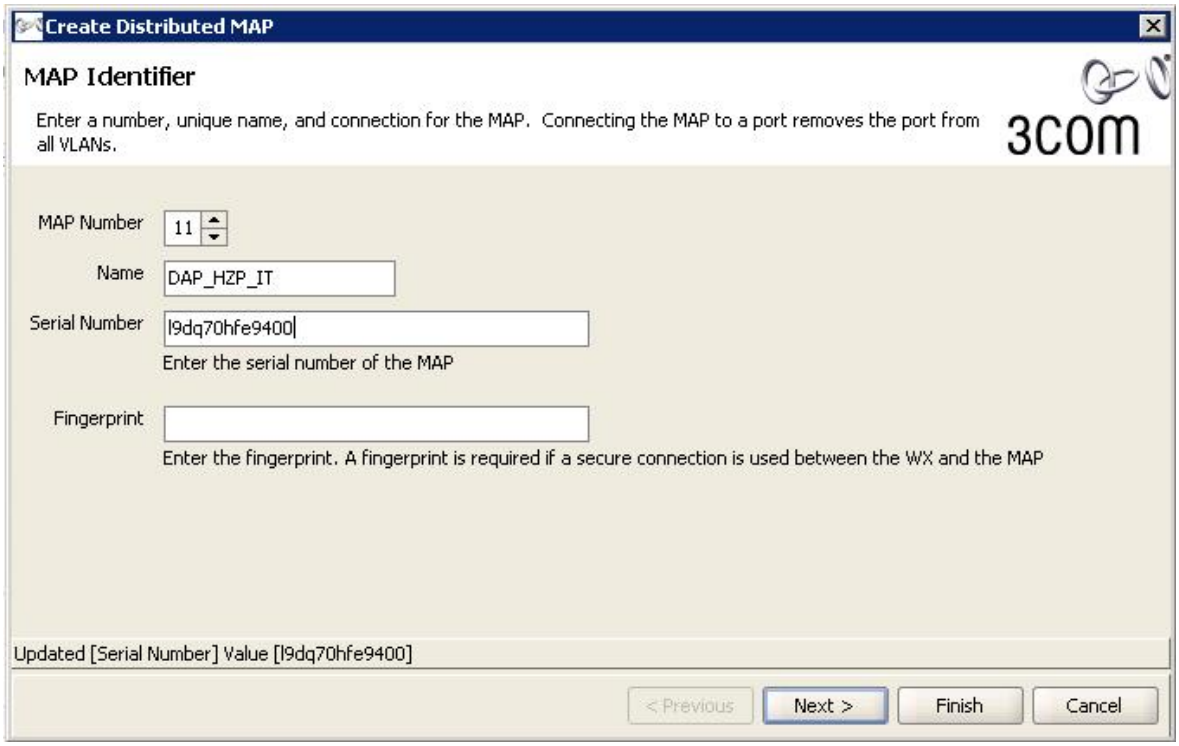
- Porty: Jeden 10BASE-T/100BASE-TX s podporou PoE napájení
- Rozhraní (Media interfaces): RJ45, 802.11a/b/g, DB-9
- Frekvence : 802.11a: 5GHz, 802.11b/g: 2,4 GHz
- Automatické načítání pracovních kanálů v jednotlivých zemí, při nastavení v administrátorském Wirelless LAN systému zemi, kde je použito AP
- Dosah signálu: u 802.11a: až do 50m příjem i vysílání a u 802.11b/g až do 100m
- Napájení: 6W maximální přípustná hodnota (podpora PoE port or external power adapter)
- Zabezpečení: 40/64 a 104/128- bitový WEP šifrování, TKIP WPA a WPA2, AES šifrování, IEEE 802.1X síťové ověřování, RADIUS, 802.11i
- Rozměry: 16,6 x 8,3 x 3,3 cm
- Duální režim antén: 2,4 a 5,15 GHz antény

4.2.2 Konfigurace AP 2750 přes Wireless Switch Manager 6.0

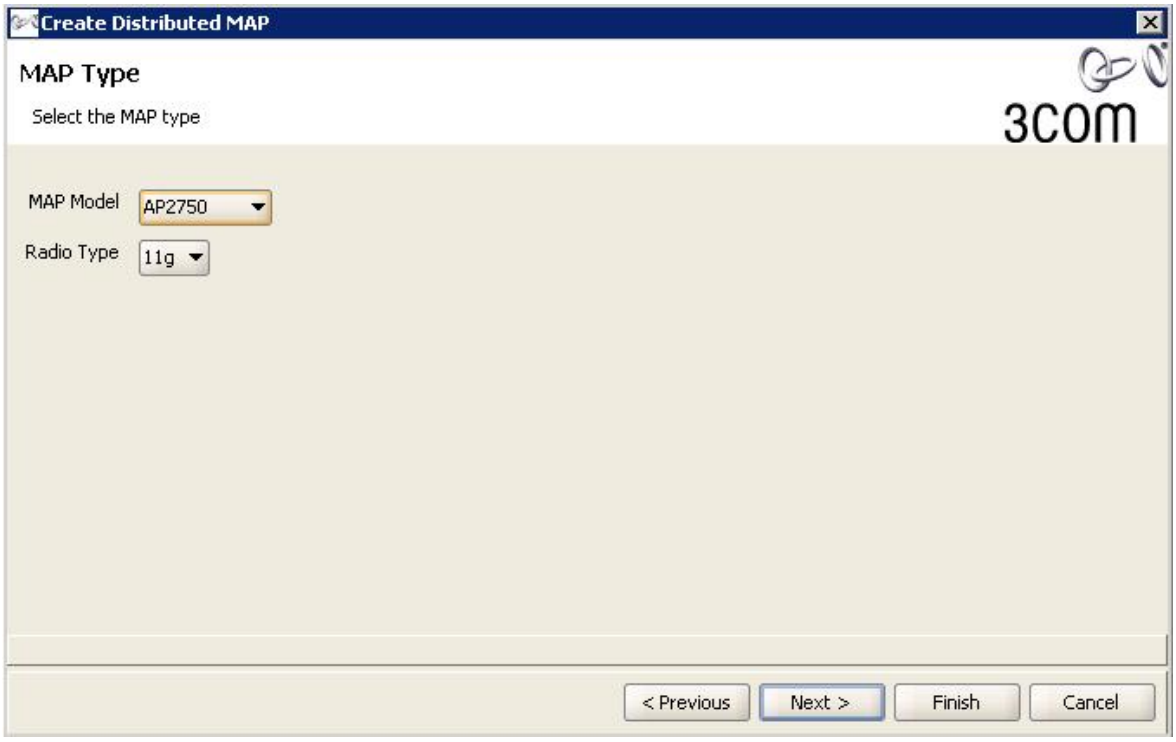
Konfigurace AP 2750 je možná pouze s použitím Wireless Switch Manageru. AP nemá možnost konfigurace přes webové rozhraní, proto je pro běžné domácí použití nevyužité. Nastavení probíhá pomocí softwaru na správu bezdrátové sítě. Wireless Switch Manager je klient/server nástroj, který umožňuje v základní licenční verzi spravovat až 10 bezdrátových přepínačů (bez omezení připojených AP).

Díky centrální správě bezdrátových zařízení se nové AP nakonfiguruje podle základních postupů:

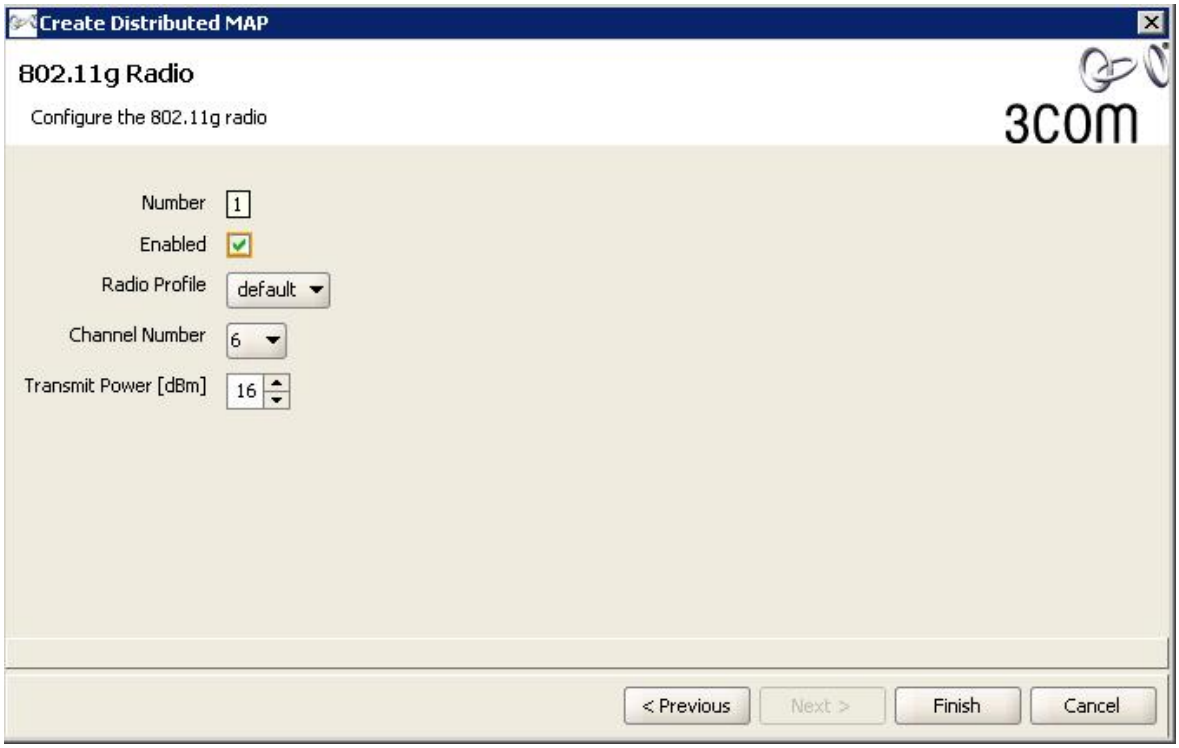
1. V hlavním Wireless Manager Switch se zadá nové MAP zařízení, kde je nutné vyplnit serial number AP, číslo AP (kolikáté v pořadí je AP), název AP, modelové označení, nastavení radiového vysílání 2,4GHz, síla vyzařování dBm a číslo kanálu (Viz.obr.35,36,37).
2. AP se připojí do LAN sítě pomocí patch kabelu (RJ45) viz.obr.38 a po 10 sec se v prostředí Wireless Switche Manageru se nechá vyhledat jako nové zařízení v bezdrátové síti.viz obr.39.



Obr. 35 Založení nového AP v Wireless Switch WX1200

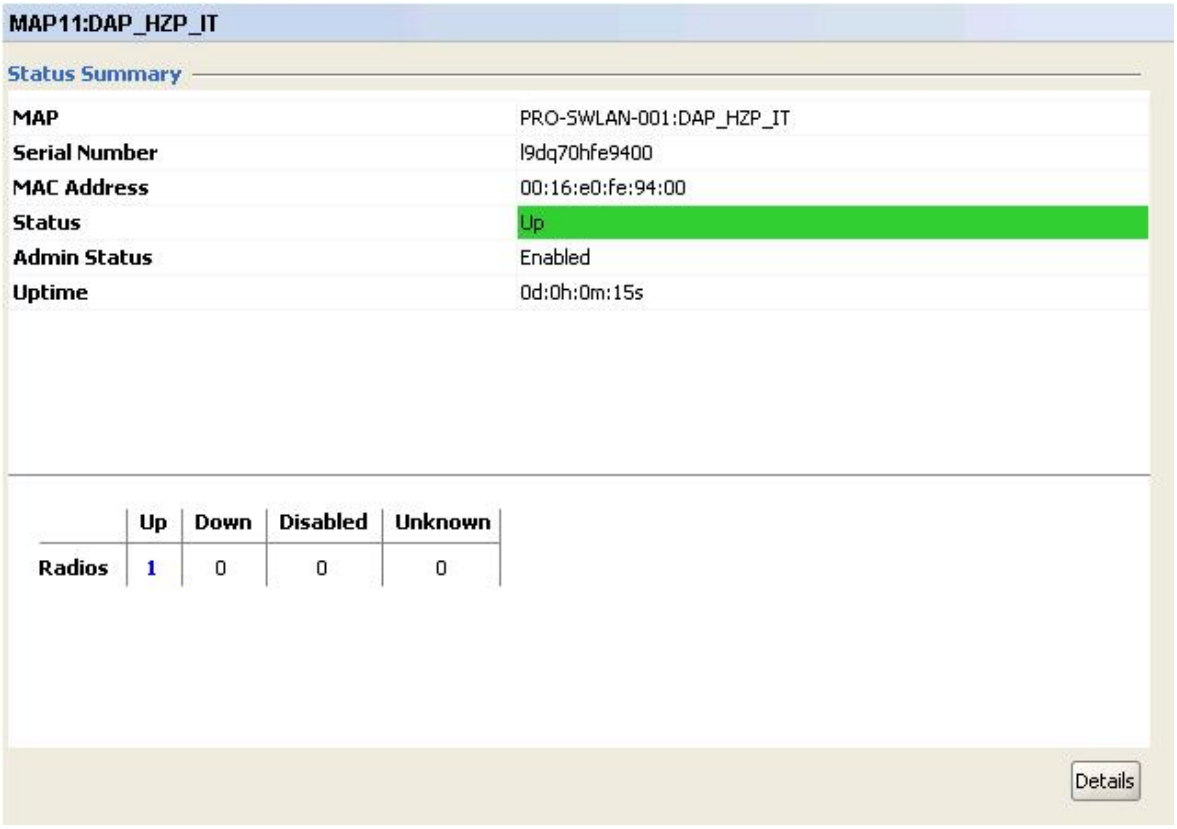


Obr. 36 Nastavení modelového označení a typu radiového vysílání.



Obr. 37 Nastavení základních parametrů radiového vysílaní AP zařízení.

Obr. 38 Připojení AP do sítě LAN přes patch kabel CAT 5.e



Obr. 39 Zobrazení nastaveného, nového AP ve Wireless Switchi.

3. Další modifikaci AP je možné provést přes Manager Access Point Properties, kde se dá upřesnit některá z nastavení AP. Například zda má signalizovat pomocí led diod stavy zapnuto, vypnuto, komunikaci atd.

Byly nastaveny veškeré potřebné vlastnosti AP 2750 a Wireless Switche WX1200, tak aby mohli AP být montovány na halu a nedocházelo k nejakým komunikačním problémů mezi jednotlivými bezdrátovými zařízeními.

4.2.3 Instalace AP 2750 zařízení na výrobní hale SF

Při instalaci AP zařízení na hale se muselo brát v potaz, kde je potřeba mít co největší signál a do jaké výšky umístit samotné zařízení, aby byly splněny možná co nejlepší vyzařovací schopnosti AP a zároveň bylo zamezeno k fyzickému poškození či odcizení AP.

Vlastní instalace byla provedena na kovové, nosné pilíře typu I, které tvoří kostru haly a výška AP od země činí 3m +- 0,5m. Připojení AP do LAN sítě je pomocí CAT.5e kabelu a vedení nepřesahuje 30m. Na obrázku 32 jsou znázorněné AP na kovových I konstrukcích haly.

Obr. 40 Namontovaná AP na kovových konstrukcích haly

4.3 3COM AP jako Wireless Workgroup Bridge

V případě, že potřebujeme napojit výrobní linky do LAN sítě s použitím bezdrátových technologií neobejdeme se bez zařízení jako je AP s Wireless Workgroup Bridge. Celé zařízení se vyrábí v provedení, jak s podporou 802.11a, tak 802.11b/g s plnou funkčností WDS pro snadné a univerzální nastavení. Pracují s integrovanými, směrovými, anténami vyzařující až 18dB. K připojení je zapotřebí metalického Ethernetu a přímá viditelnost s ostatními AP.

4.3.1 AP 3Com Wireless 7760

Podnikové bezdrátové přístupové body 802.11a/b/g jsou řešením pro bezpečný, mobilní, přístup do „drátové“ části sítě. Přístupové body mají WiFi certifikaci a jsou napájené prostřednictvím Ethernetu. Pro každý kanál je třeba zvolit frekvenční pásmo 2,4GHz (b/g) nebo 5GHz (a). Podporují 3Com Dual-Band externí antény (R-SMA konektor) a řízení vysílacího výkonu dle generálního povolení. Správa zařízení prostřednictvím zabezpečených protokolů SNMPv3, SSHv2 a SSL. Je možné provádět až čtyři souběžné bezpečnostní profily na každém kanálu. Automatické zařazování do VLAN na základě ověření, izolací bezdrátových klientů a podpora point to point i point to multipoint WDS spojů. Jedná se o jednokanálovou verzi AP.

Obr. 41 3Com AP 7760

4.3.1.1 Technické parametry 3Com AP 7760

- Porty: Jeden 10BASE-T/100BASE-TX s podporou PoE napájení
- Rozhraní (Media interfaces): RJ45, 802.11a/b/g, DB-9
- Frekvence : 802.11a: 5GHz, 802.11b/g: 2,4 GHz
- Dosah signálu: u 802.11a: až do 50m příjem i vysílání a u 802.11b/g až do 100m akční rádius je maximálně 457m.
- Napájení: 48V DC a 400 mA (podpora PoE port or external power adapter)
- Zabezpečení: WPA/WPA2 AES a TKIP šifrování; 64/128/152-bit WEP šifrování; 802.1X s EAP-TLS, EAP-TTLS a PEAP; WPA-/WPA2-PSK autentifikace; filtrování MAC adres; 802.1Q VLAN; multiple SSID; RADIUS client AAA
- Rozměry: 16,6 x 8,3 x 3,2 cm
- Duální režim antén: 2,4 a 5,15 GHz antény
- Přístupová metoda: CSMA/CA
- 802.11a : Přijímací citlivost antén

  36 Mbps: ≤-75 dBm
  48 Mbps: ≤-72 dBm
  54 Mbps: ≤-71 dBm

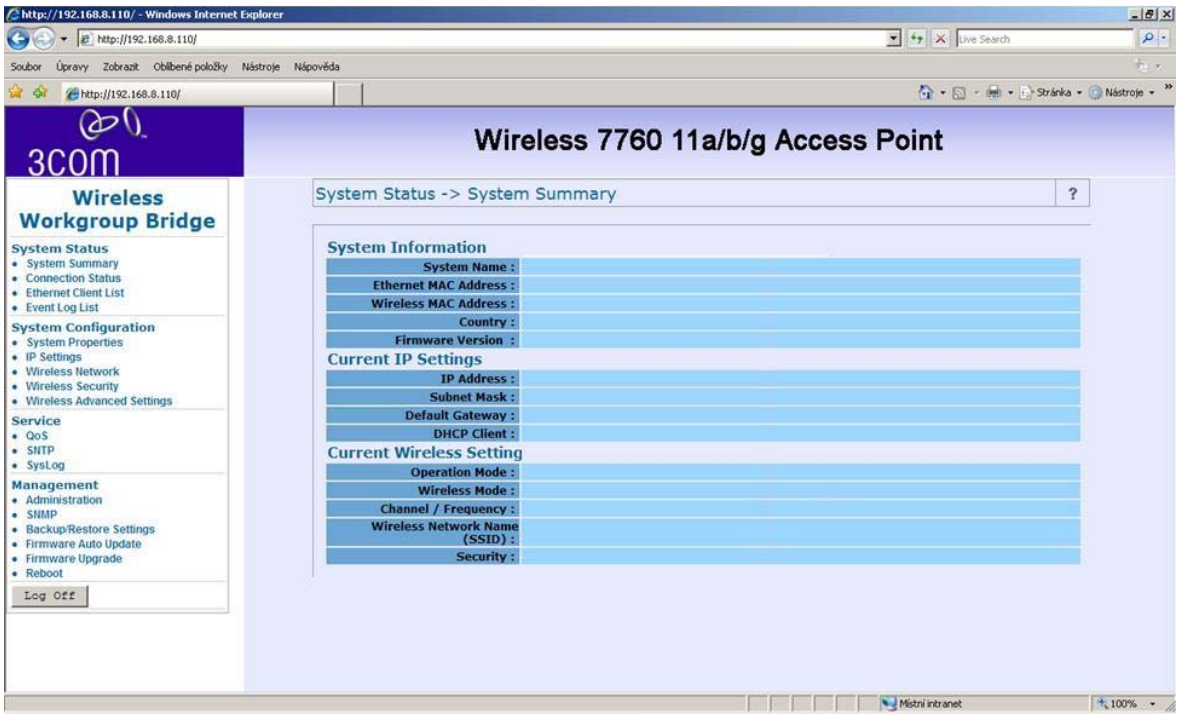
- 802.11b/g: Přijímací citlivost antén

  18 Mbps: ≤-84 dBm
  24 Mbps: ≤-81 dBm
  36 Mbps: ≤-77 dBm
  48 Mbps: ≤-73 dBm
  54 Mbps: ≤-72 dBm

4.3.2 Konfigurace AP 7760 přes Webový prohlížeč IE7

Konfigurace AP zařízení je možně přes webové prostření pomocí HTTP. AP podporuje také SNMPv1 a v2, Telnet. Jako softwarové prostředí je možné použít Microsoft XP,Vista, Server. Případná modifikace AP, již nastavených parametrů, je nejvýhodnější přes http, kdy do vyhledávače v síti LAN se zadá IP Adresa zařízení a zobrazí se nám úvodní přihlašovací okno AP nastavení. Po přihlášení do AP se objeví základní parametry AP a jejich možnosti nastavení.

1 Pří přihlášení do AP se zobrazí menu kde se nastavují parametry a vlastnosti AP.

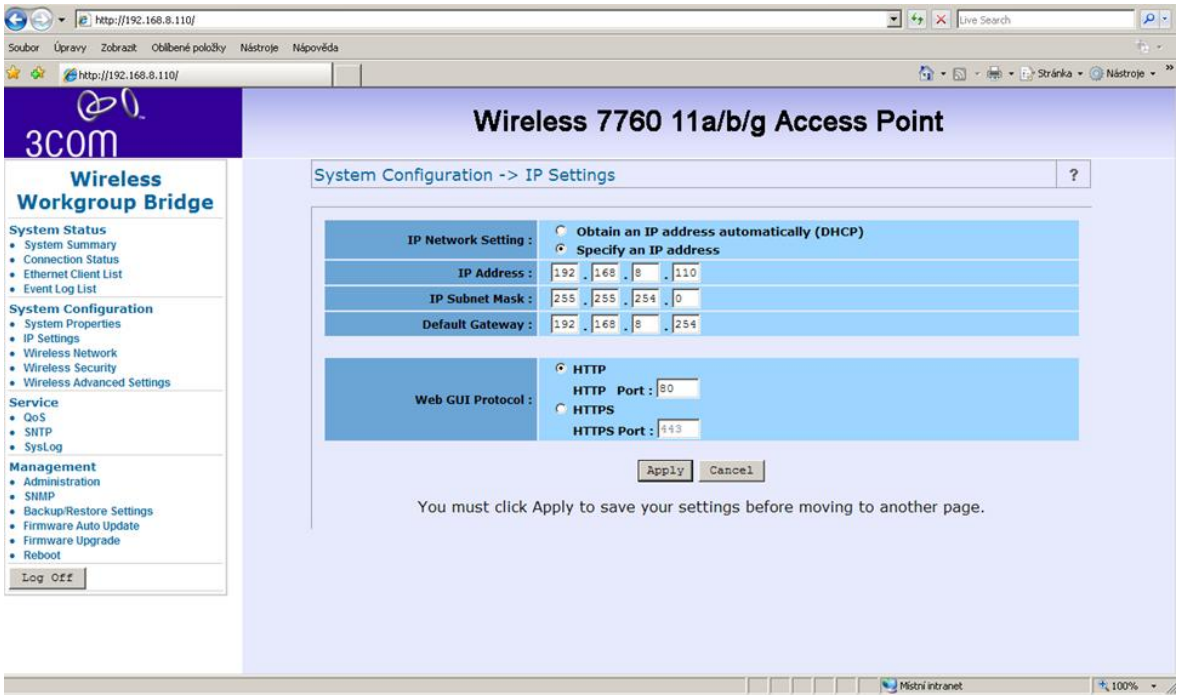


Obr. 42 Základní nastavení AP 7760 přes webové rozhraní

2 Nastavení jména AP a lokalizace umístění, operačního módu (Wireless Workgroup Bridge, sytém manažerování (jako samostatné AP v síti). Konfigurace tohohle nastavení je důležitá při identifikaci zařízení v síti a pro případné softwarové 3Com utility na řízení a správu AP zařízení.

Obr. 43 Nastavení Wireless AP 7760 do režimu Wireless Workgroup Bridge

3 Při zadávání IP adresy musí platit zásadní pravidla sítě, do které se zařízení bude připojovat. Je potřeba nastavit http port a volnou, pevnou IP adresu, aby nedocházelo ke kolizi, s již existujícími zadanými adresy (zařízení), v LAN síti.

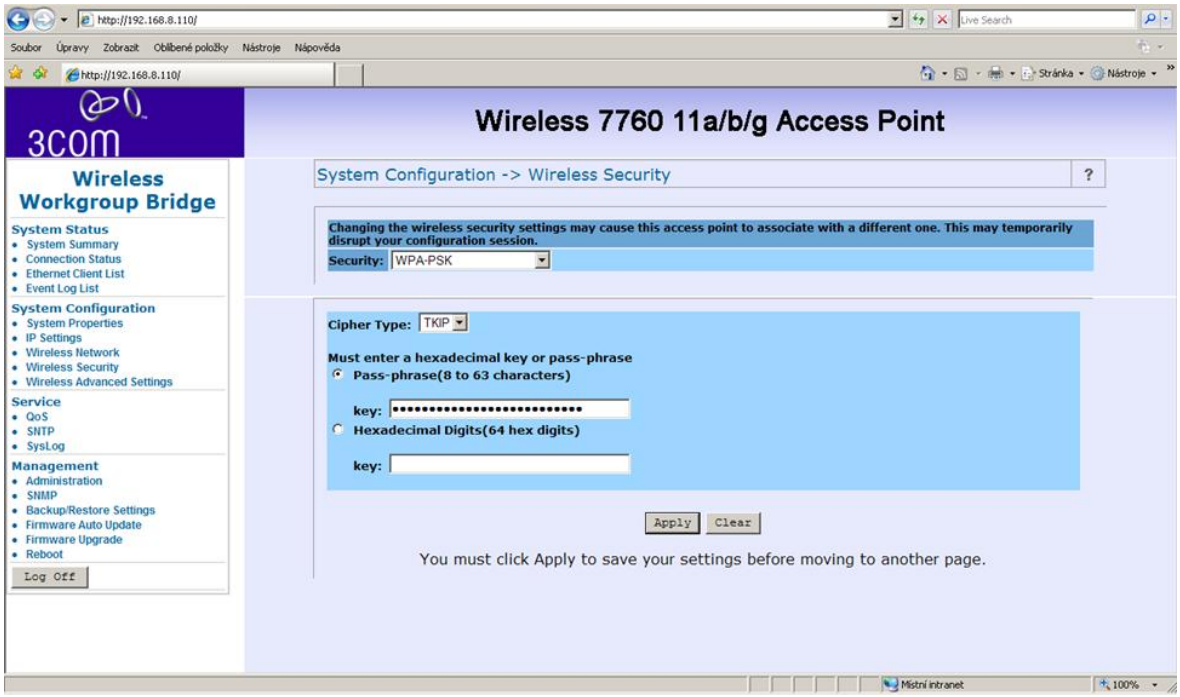


Obr. 44 Nastavení AP 7760 IP adresa a http port

4 Nastavení názvu SSID sítě, bezdrátového Wirless módu a síťového módu. V případě nezadání SSID sítě AP se nepřipojí do bezdrátové sítě a nebude plnit funkci Bridge.

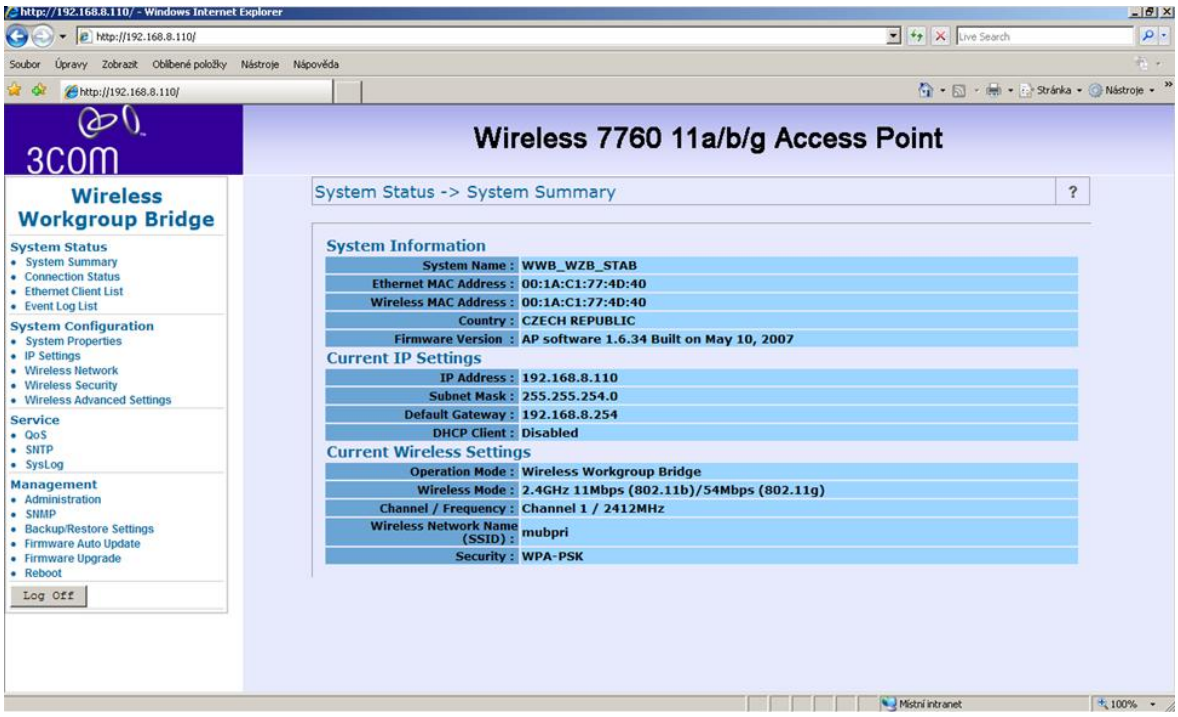
Obr. 45 Nastavení AP 7760 SSID sítě, bezdrátový a síťový režim

5 Důležitým parametrem nastavení AP do bezdrátové sitě je jeho vlastní zabezpečení a přístupové klíče k autentifikaci nového bezdrátového zařízení v síti. Zde je použit šifrovacího protokolu WPA- PSK s TKIP sdílení klíče. Při připojení AP do sítě je pomocí klíče zařízení autentifikováno a bráno za povolené zařízení a nadřazené AP a switche se zařízením komunikují.



Obr. 46 Nastavení AP 7760 bezpečnostní a ověřovací parametry AP

6 Po nakonfigurování AP se v základním statutu objeví veškerá nastavení povedené přes webové rozhraní pomocí http protokolu.



Obr. 47 Nastavení AP 7760 systémové shrnutí nakonfigurovaného AP

4.3.3 Instalace zařízení AP 7760 na výrobní hale

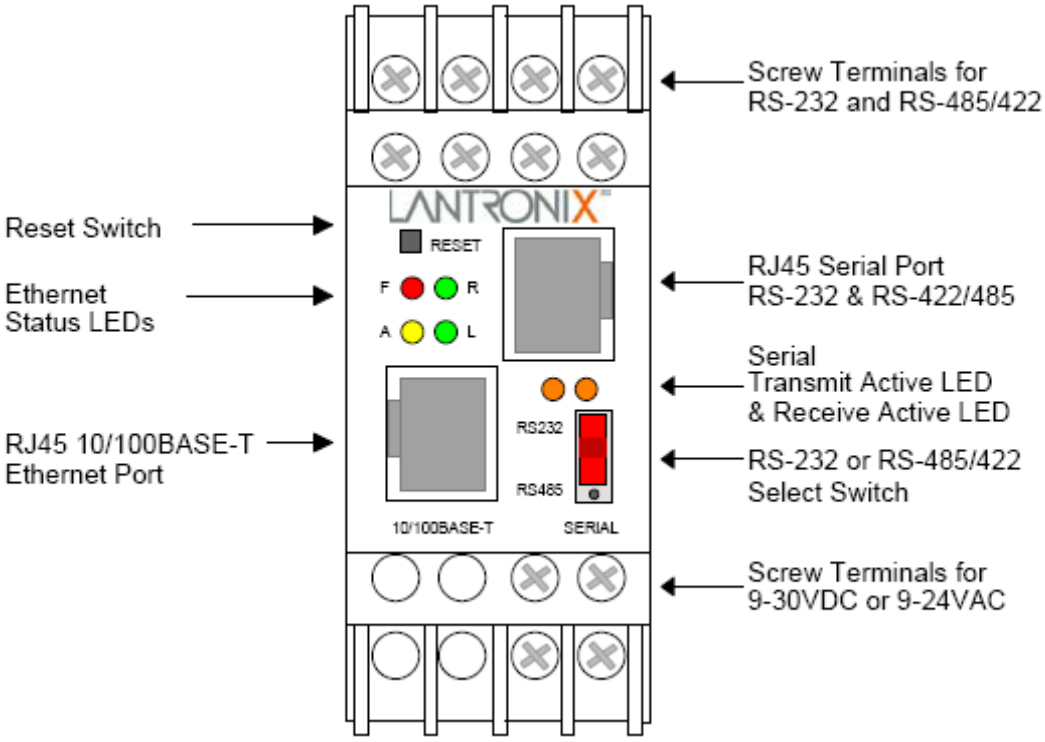
Instalace zařízení AP na výrobní hale byla provedena pouze na linku FIAT 312, kde se fyzicky AP zařízení ve funkci Bridge namontovalo na zadní, plechou část kontrolního panelu Beckhoff , protože jako jediný má výstupní rozhraní uzpůsobeno na komunikaci po ethernetu. Tím pádem, nebyl žádný problém připojit pomocí metalického pacht kabelu, síťovou kartu řídícího Beckhoff panelu, s AP ve funkci bridge.

Obr. 48 Montáž AP zařízení na linku FIAT 312

U linky Porsche a Vulkanizace je nutné nejdříve uzpůsobit komunikační rozhraní RS232 na ethernet, tak aby se mohla připojit pomocí AP zařízení do LAN sítě. Bylo vytvořeno mobilní bezdrátové zařízení s AP a zabudovaným převodníkem RS232 a Ethernet.Viz. (kapitola Převodník RS232 x Ethernet).

4.4 Převodník RS232 x Ethernet

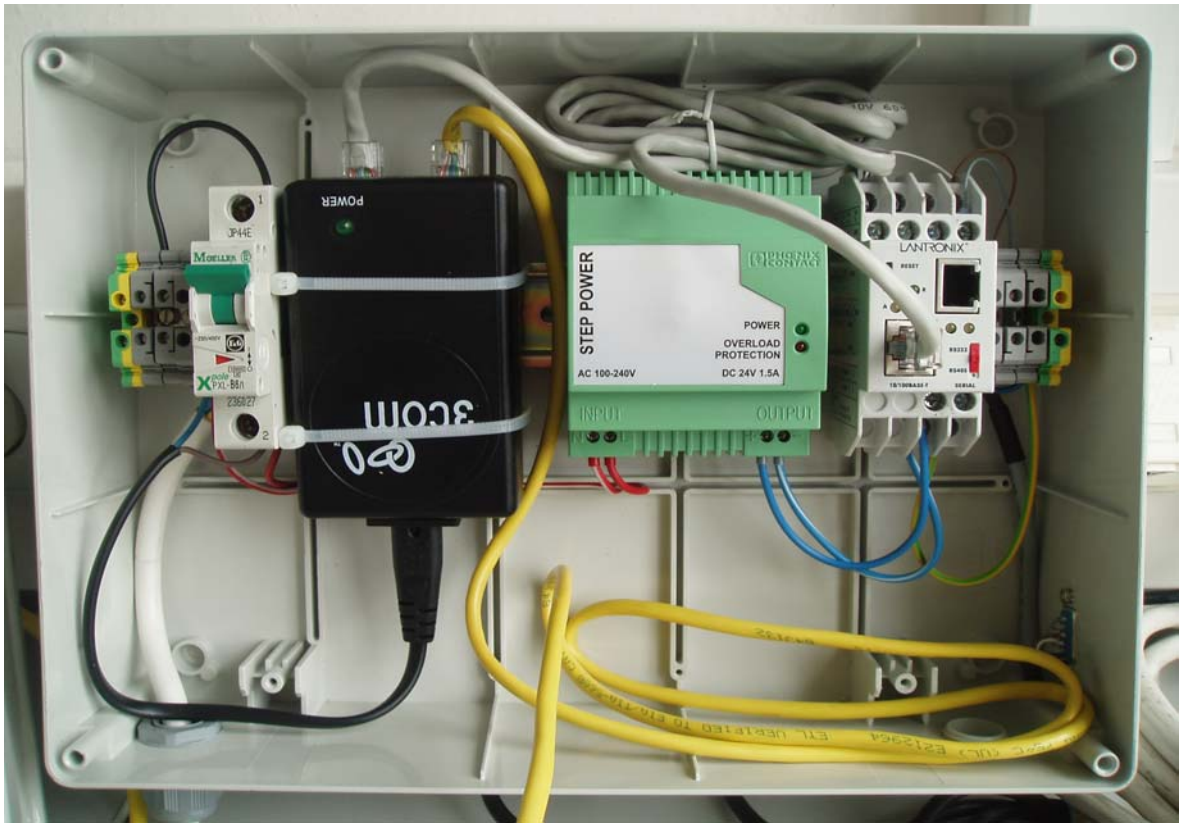
4.4.1 DSTni XPress DR-IAP



Obr. 49 Pohled na přední část převodníku Lantronix

Zařízení bylo použito pro převod výstupních signálů programovatelných automatu Siemens RS232 na Ethernet. Na vlastní nastavení (konfiguraci převodníku) je použito softwarového prostředí dodávané firmou LANTRONIX, jako nejdůležitější parametry jsou nastavení IP adresy, zadání MAC adresy převodníku do seznamu zařízení v listu menu, nastavení komunikačních portů 3001 na otvírání a 14001 na straně RS232.

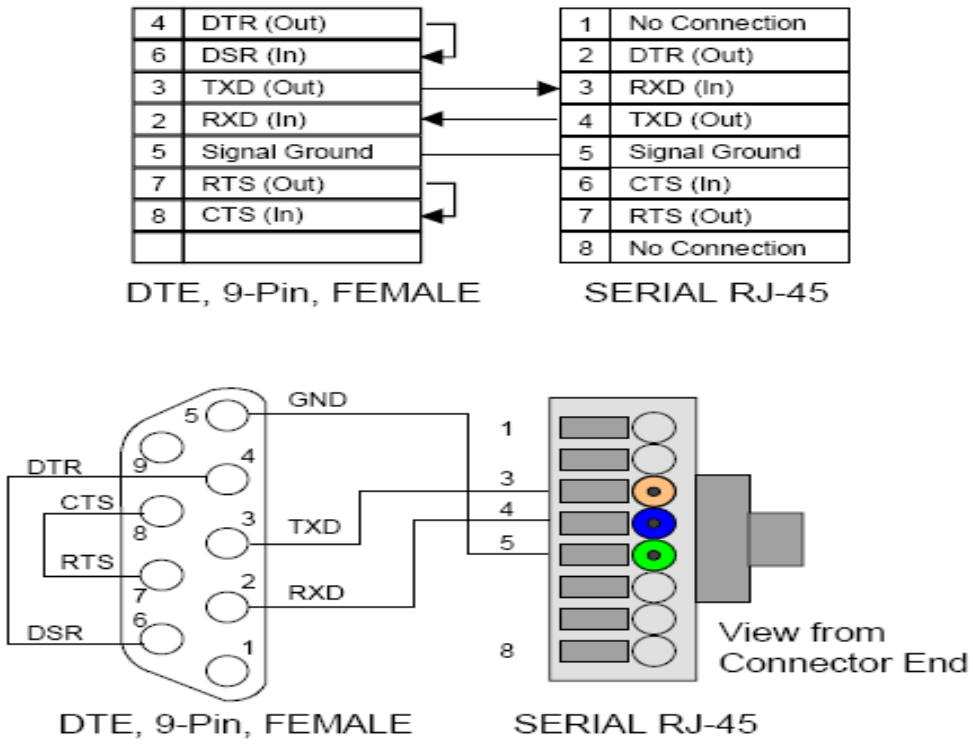
Bylo potřeba vytvořit celkový modul použitelný pro mobilní komunikaci se výrobními linkami přes bezdrátovou síť. Převodník je napájen 24VDC a 1,5A trafem, kde je potřeba ještě napájet trafo pro AP zařízení, připojené na přední straně celého modulu, v režimu Wireless Workgroup Bridge, které je napájeno přímo ze svorkovnice 240v AC. Vlastní AP je napájeno přímo z převodníku po ethernetu. Dále je použito jističe, montážních svorkovnic a platové krabice.



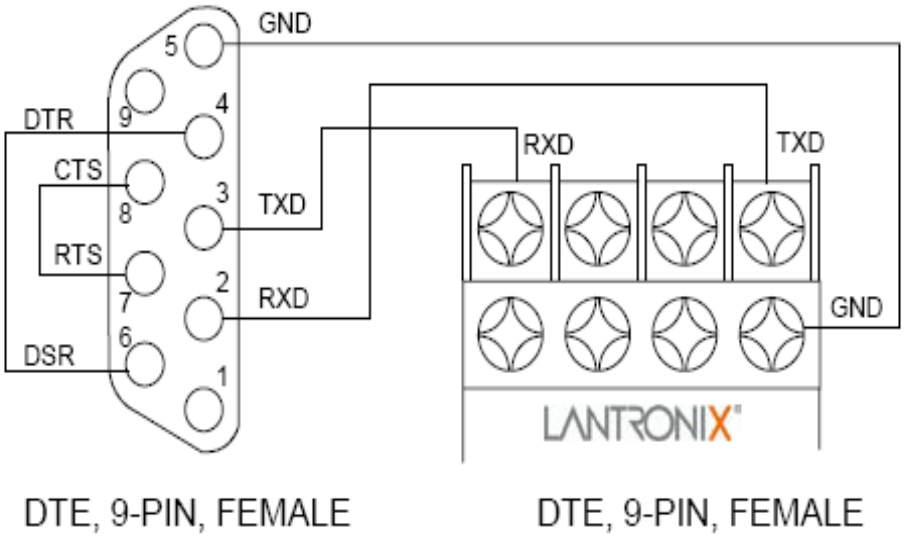
Obr. 50 Otevřený modul mobilního zařízení na převod RS232 ethernet

Obr. 51 Celkový pohled na mobilní modul i s AP zařízením

Na obrázku 52,53 je znázorněné vlastní zapojení komunikačních cest připojených mediích jak u COM tak u RJ45 konektoru.



Obr. 52 Klasický PC (COM1) kabel připojený na DSTni Xpress DR s RJ45 konektorem



Obr. 53 Klasický PC (COM1) kabel připojený na DSTni Xpress DR přes sériový terminál LANTRONIX

4.5 Měření odezvy výrobní linky Fiat 312

K měření odezvy bylo použito hardware a software uvedený níže.

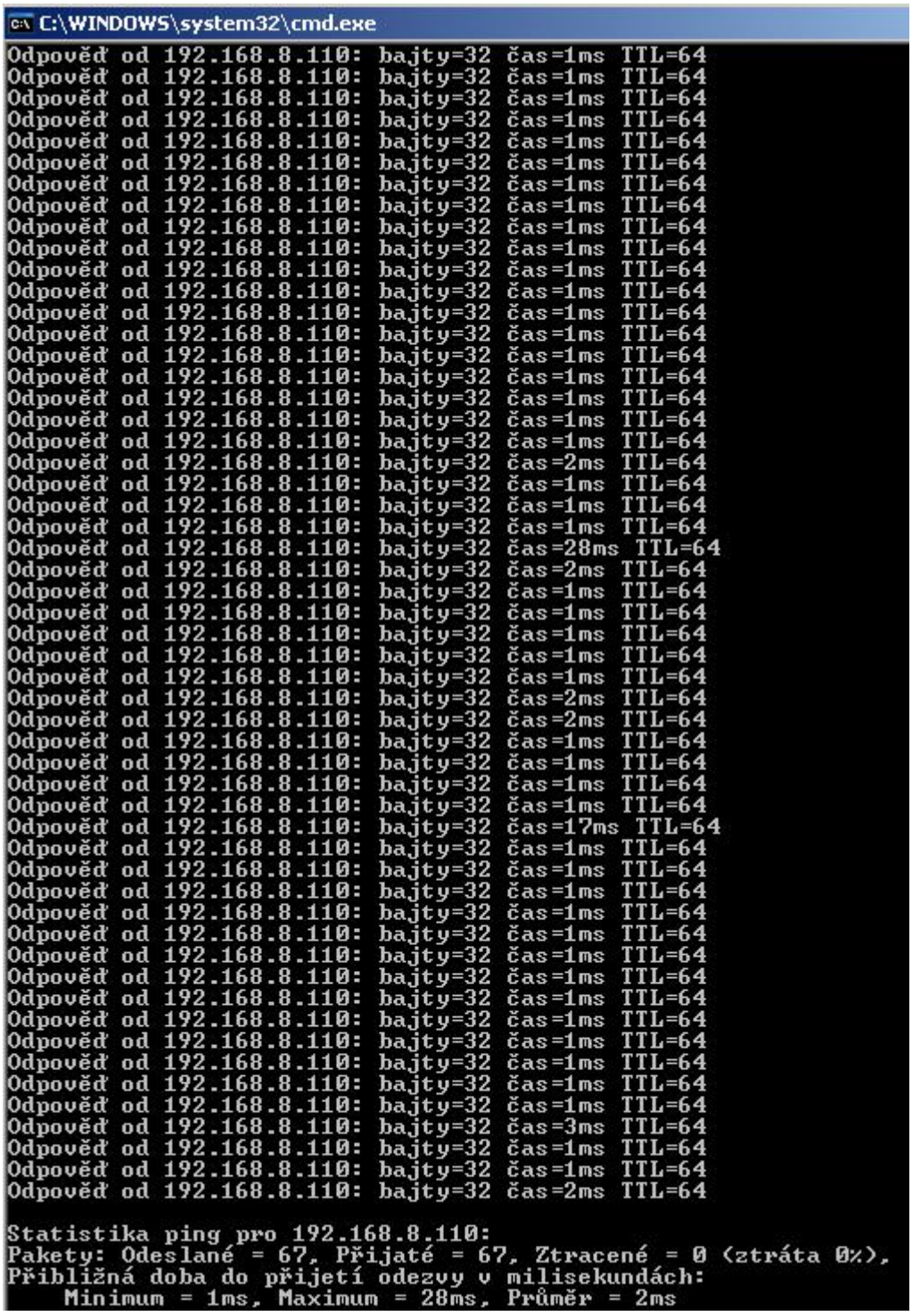
Hardwarové parametry zařízení notebook ACER Travel Mate 4233 WLMi

Technické parametry:

- Intel Core 2 Duo procesor T5500 (1,66 GHz, 667 MHz FSB, 2MB L2 cache)
- 15,4“ WXGA LCD
- Grafická karta GeForce GO 7300 TurboCache
- 120 GB HDD
- DVD- Super Multi double layer (DVD+- RW)
- 2 GB RAM DDR2
- 802.11a/b/g wireless LAN
- Síťová karta Ethernet Broadcom 440x 10/100 Mb Full

A softwarového prostředí Microsoft Windows XP Profesional SP2, a příkazu ping v DOSovském prostředí cmd.

Jednotlivé odezvy v [ms] na výrobní linku FIAT 312 byly měřeny pomocí softwarové utility implementované v Microsoft Windows systému a jejich výsledné a statistické hodnoty zobrazuje obr.54. Při odezvě 1 [ms] se dá říci že daná výrobní linka komunikuje přes bezdrátovou síť s LAN sítí velice spolehlivě s minimální řečeno žádnou ztrátou odeslaných a přijatých paketů. Taková komunikace je braná za dostatečnou a spolehlivou.



Obr. 54 Jednotlivé odezvy [ms] výrobní linky FIAT 312

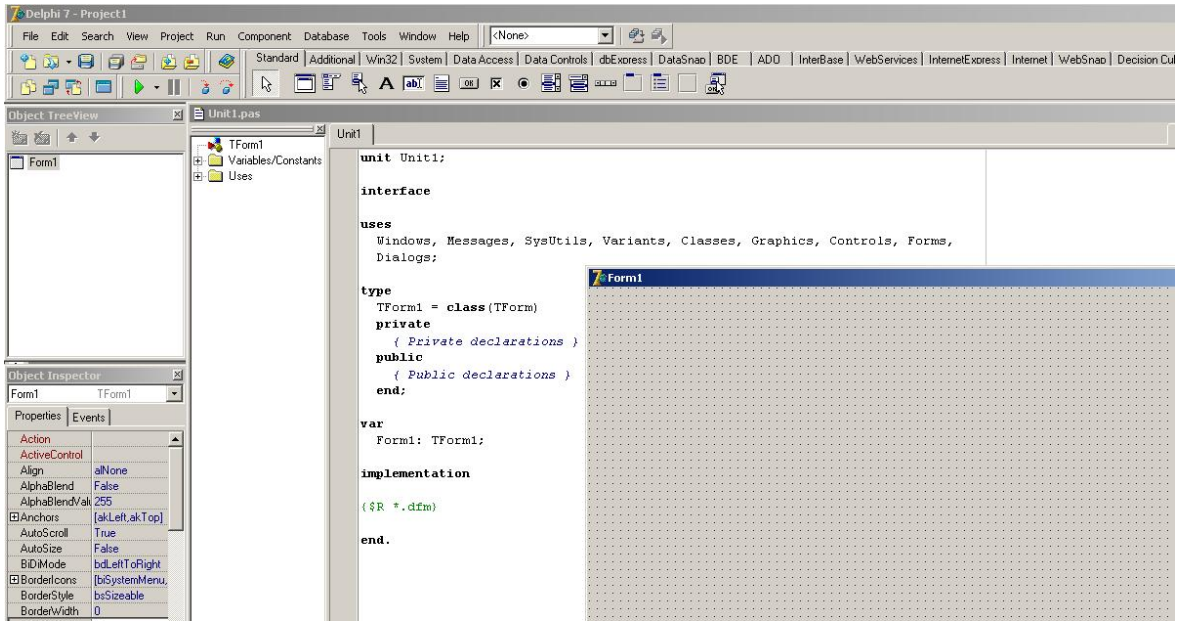
5 SOFTWAROVÉ PROSTŘEDKY

5.1 Delphi

Delphi je takzvaný nástroj RAD (Rapid Application Development) rychlý vývoj aplikací. Velkou část programování představuje tvorba rozhraní aplikace, která sestává z komponent, předem předem vytvořených stavebních kamenů s danou zákadní funkčností. Delphi je jeden z nejkompletnějších nástrojů pro programování pod Windows. Základem je programovací jazyk Object Pascal. Podporuje základní řídící prvky ActiveX, kterými se obklopují především programátoři ve Visual Basicu.

5.1.1 Vývojové prostředí Delphi 7

Vývojové prostředí Delphi (IDE – Integrated Development Environment) sestává z několika oken uspořádaných na ploše obrazovky. Mnohé z těchto oken je možné navzájem dokovat (přiřadit jejich obsah jako panel či lištu k jinému oknu) a mohou se také zcela překrývat.



Obr. 55 Vývojové prostředí Delphi 7

IDE je tvořeno hlavním oknem, seznamem objektů, inspektorem objektů, editačním oknem a samozřejmě také oknem s vizuální reprezentací formulář. Aplikace ve Windows jsou z velké části tvořeny formuláři, které později tvoří jednotlivá okna.

5.1.2 Datové typy a proměnné

Během činnosti programu dochází často k přesouvání dat, která jsou uložena v paměti. Bloky paměti, které slouží k ukládání potřebných dat, se nazývají proměnné. Každá proměnná je pojmenována identifikátorem, pomocí něhož se přistupuje k jejímu obsahu. Dříve než se v programu použije jakákoli proměnná, je nutné, aby se na začátku programu objevilo slovo var a za ním její deklarace. To znamená, že hned na začátku musí být kompilátoru jasné, kolik proměnných bude použito, aby pro ně vyhradil dostatečné množství paměti.

Je zřejmé že data, která se v programu zpytovávají, jsou pokaždé jiná. Jednou jsou to celá čísla, podruhé reálná čísla, jindy znaky, nebo dokonce celé řetězce znaků. Všechna tato data jsou natolik nesourodná, že je nutné mít i několik druhů proměnných, které se budou od sebe lišit typem dat, který je v nich uložen.

Dělení datových typů v Delphi :

- Celočíselné typy
- Reálné typy
- Znaky
- Řetězce
- Ukazatele
- A uživatelem definované typy

Dále se dají dělit na dvě základní skupiny:

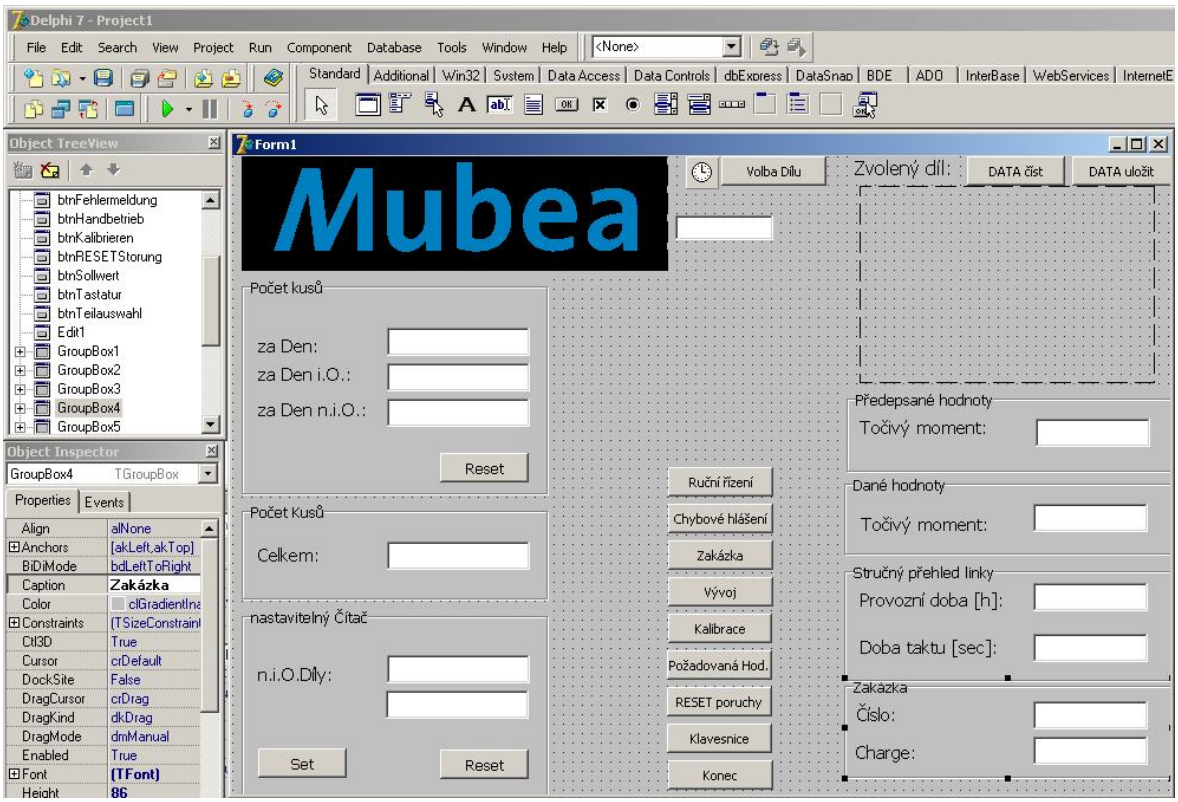
- Ordinální
- Neordinální

Do ordinální skupiny patří všechny typy, u kterých je přesně daná posloupnost mezi jednotlivými hodnotami.

Do neordinální skupiny patří reálné datové typy, protože u nich nelze určit následující prvek v posloupnosti. [1]

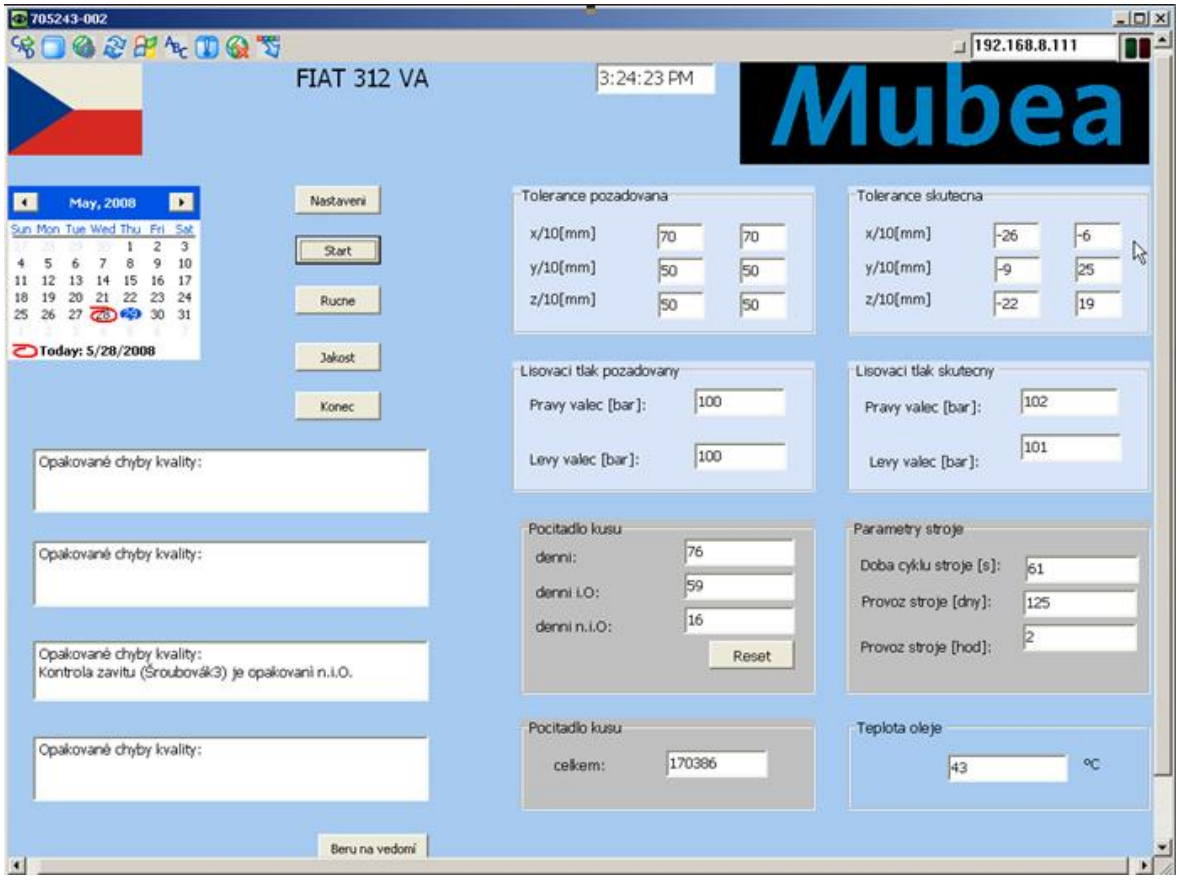
5.2 Software na vizualizaci výrobní linky

Při monitorování chodu a stavu linky bylo vytvořeno, v programovém prostředí Delphi 7 Enterprise, software na vizualizaci základních výstupních dat z výrobní linky. U výrobní linky Fiat 312 a Vulkanizace se jednotlivé data importovala z již funkčních, hlavních řídících, výrobních systému dodávané k programovatelným automatům nebo dodávaný k řídícímu, průmyslovému PC od Beckhoff (TwinCAT). Bylo zapotřebí si vymezit určitou část prostoru v paměti PC, kde se budou jednotlivé hodnoty vstupů a výstupů načítat.



Obr. 56 Aplikace na linku Porsche vytvořená v Delphi 7

Při vzdálené správě výrobní linky Fait 312 bylo nastaveno na oprávněných, uživatelských stanicí VNC (Virtual Network Computing) software, pro přímí přístup jednotlivých uživatelů přímo na průmyslový PC. Beckhoff Contol Panel je průmyslový pc fungující na platformě Microsoft. Pc byl nakonfigurován s pevnou, síťovou IP adresou 192.168.8.111, Maskou 255.255.254.0 a bránou 192.168.8.254. Díky tomu se uživatelské stanice mohou vzdáleně připojovat na průmyslový Pc a sledovat chod celé výrobní linky, zasíťované prostřednictvím bezdrátových sítí IEEE 802.11.



Obr. 57 Aplikace na Fiat 312 vytvořená v Delphi 7

ZÁVĚR

V teoretické části byla zpracovaná literární rešerše na dané téma. Byla zde nastíněna problematika zabezpečení a hardwarové prostředky spojené s instalací v praktické části a základní síťové vlastnosti a komunikační média.

Bylo zpracováno fyzické rozvržení výrobních linek na hale Mubea HZP s.r.o. s návrhem na umístění AP zařízení. Jednotlivé výrobní linky byly připojeny do sítě LAN s použitím bezdrátových technologií. Byl zvolen minimální počet AP, které je nutné umístit na halu SF pro bezpečnou komunikaci mezi dvěma, bezdrátovými zařízeními s dostačující sílou signálu.

Další části byl vytvořen přehled jednotlivých hardwarových zařízení použitých diplomové práci a IT infrastruktura podniku HZP s.r.o. Schématické rozložení IT infrastruktury bylo vytvořeno ve programovém prostředí Microsoft Visio Studio.

Jednotlivé AP byly nastaveny ve dvojím režimu. První režim AP byl nastaven na funkci přístupového bodu, k pokrytí celého prostoru, kde se nacházejí výrobní linky. Druhý režim byl nastaven na Wireless Workgroup Bridge pro přemostění síťové karty řídícího PC nebo výstupního rozhraní programovatelného automatu.

AP v režimu přístupového bodu byly namontovány na halu SF, kde se využilo kovové konstrukce kostry haly. AP zařízení byly chráněny proti náhodnému či fyzickému poškození díky výšce, do které byly připevněny a ta činila 3m nad povrchem haly. Bezdrátové zařízení v režimu Bridge byly umístěny na výrobní linku FIAT 312. Linky Vulkanizace a Porsche neměli výstupní komunikaci po Ethernetu, a proto byl vytvořen modul na převod výstupních signálu z RS232 na Ethernet. Převodník Lantonix DSTni XPress DR-IAP byl nejlepším řešením, splňoval veškeré požadavky na převod komunikace RS232 x ethernet, AP zařízení v režimu Bridge .

Byly nastaveny jednotlivé prvky bezdrátového zabezpečení WPA-PSK, TKIP, filtrování MAC adres a ověřování uživatelů na serveru RADIUS. Byl zvolen síťový klíč, který umožňuje jednotlivým novým, bezdrátovým zařízením přistupovat do bezdrátové sítě.

K vizualizaci stavu a provozu výrobních linek bylo vytvořeno v softwarovém prostředí Delphi nástroj na zobrazování naměřených dat použitých při chodu linky.

ZÁVĚR V ANGLIČTINĚ

Inside the theoretical part is the IT summery, that I used in the practical part . Main parts are safeguard and security of data transfer , hardware instruments, basic network properties and communications media .

I made layout of produktions lines area in the produktion hall Mubea HZP . In this layout I projected position of AP in the hall . The produktion lines were connected to the LAN with using the wireless technologi . I defined minimal numbers of AP , which were located in the hall . It was required the secure comunication between two wireless equipments and strenght of this signal.

I created summary of MHZP infractructure and hardware equipment, which i use in this thesis . The schematic lay - out IT infrastructure was created in programme environment Microsoft Visio studio.

AP in mode access point was mounted in the hall SF. I used metallic construction in the hall. AP equipment were installed in height 3m . Main reasen was protection agains mechanical crasches. Wireless equipments in mode Bridge were placed on production line FIAT 312. Machines vulcanization and Porsche didn't have communication output to the Ethernet, and therefore I created modul to convert output signal RS232 to Ethernet. Converter Lantonix DSTni XPress DR- IAP was the best solution. This equipment respond all standards of transfer communication RS232 x Ethernet, AP establishment in mode Bridge.

I setted individual elements of wireless safeguard WPA- PSK, TKIP, filtering MAC address and users verification on server RADIUS. I elected network key for new users to login in the wireless network.

Visualization was created by Delphi . This software measures and displays running of produktion lines.

SEZNAM POUŽITÉ LITERATURY

[1] PÍSEK, Slavoj. Začínáme programovat v Delphi : Podrobný průvodce začínajícího uživatele. 1. vyd. Praha : Grada Publishing, 2000. 304 s. ISBN 80-247-9008-4.

[2] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluethoot, GPRS či 3G. Brno : CP Books, 2005. 179 s. ISBN 80-251-0791-4.

[3] NORTHCUTT, Stephen. Bezpečnost počítačových sítí - Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. 2005th edition. Brno : Computer Press a.s., 2005. 589 s.

[4] BECKHOFF NEW AUTOMATION TECHNOLOGY [online]. 31.1.2008 , 31.1.2008 [cit. 2008-02-15]. Dostupný z WWW:*http://www.beckhoff.com*

[5] FRANK, Eller. *Delphi 6 : příručka programátora*. Irena Randusová; Jiří Bráza. 1. vyd. Praha 7, Holešovice : Grada Publishing a.s., 2002. 272 s. ISBN 80-247-0303-3.

[6] KÁLLAY, Fedor, PENIAK, Peter. *Počítačové sítě a jejich aplikace : LAN/MAN/WAN*. Petr Novotný. 2. aktualiz. vyd. Praha 7, Holešovice : Grada Publishing a.s., 2003. 356 s. ISBN 80-247-0545-1.

[7] KÖHE, Thomas. *Stavíme si bezdrátovou síť Wi-Fi*. Jindřich Jonák; Marek Šiler. 1. vyd. Brno 635 00 : Computer Press, 2004. 295 s., CD. ISBN 80-251-0391-9.

[8] DAVIS, Harold. *Bezdrátové sítě Wi-Fi*. Karel Voráček. 1. vyd. Praha 7, Holešovice : Grada Publishing a.s., 2006. 336 s. ISBN 80-247-1421-3.

[9] THOMAS M., Thomas. *Zabezpečení počítačových sítí bez předchozích znalostí* . Miroslav Hausknecht; David Krásenský. 1. vyd. Brno 635 00 : Computer Press, 2005. 341 s. ISBN 80-251-0417-6.

[10] Jak na Wi-Fi [online]. [cit. 2007-4-15]. Dostupné z URL: http://www.bezdratovepripojeni.cz/wi-fi/

[11] Wikipedie – otevřená encyklopedie: Ethernet [online]. [cit. 2007-4-16]. Dostupné z URL: http://cs.wikipedia.org/wiki/Ethernet

[12] Bezpečnost Wi-Fi–WEP, WPA a WPA2 [online]Dostupné z URL:*http://hakin9.org*

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization and Accounting.
AES	Advanced Encryption Standard.
AP	Access Poin.(přístupový bod)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DES	Data Encryption Standard
EAP	Extensible Authencitation Protocol
FTP	File Transfer Protocol
HTTP	HyperText Transport Protocol
ICMP	Internet Kontrol Message Protocol
IV	Initialization Vector
MAC	Message Authentication Code
MK	Master Key
OFDM	Orthogonal Frequency Division Multiplex
P2P	Peer-to-Peer
PSK	Pre-Shared Key
QoS	Duality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron´s code number 4
RSN	Robust Security Network
RTS	Request-To-Send
SSID	Service Set IDentifier
SSL	Security Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol

UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH