VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2017 Bc. Peter Sidor

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH INFRASTRUKTURY ICS PRO PRŮMYSLOVÝ PODNIK
DESIGN OF ICS INFRASTRUCTURE FOR INDUSTRIAL COMPAN

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Peter Sidor

VEDOUCÍ PRÁCE
SUPERVISOR
doc. Ing. Vladislav Škorpil, CSc.

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Peter Sidor ***ID:*** 154868
Ročník: 2 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Návrh infrastruktury ICS pro průmyslový podnik

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se komplexně s problematikou ICS (Industrial Control System), pochopte rozdíly mezi komerční a průmyslovou komunikační sítí a zjištěné skutečnosti popište. Speciální pozornost věnujte bezpečnosti, robustnosti a bezporuchovosti průmyslových sítí. Na základě získaných poznatků navrhněte infrastrukturu ICS pro průmyslový podnik v konkrétním prostředí. V laboratorních podmínkách otestujte datový provoz v ICS a podle výsledků měření rozeberte problémy, které průmyslová síť přináší. Vypracujte úplný návrh ICS pro průmyslový podnik.

DOPORUČENÁ LITERATURA:

[1] Standard NIST ST 800-82. Guide to Industrial Control Systems (ICS) Security. NIST 2011

[2] ANSI/ISA – 99. Industrial Automation and Control Systems Security. ANSI 2009

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 24.5.2017

Vedoucí práce: doc. Ing. Vladislav Škorpil, CSc.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Táto práca sa zaoberá problematikou priemyselnej komunikácie, ktorú je nutné brať do úvahy pred konečným návrhom priemyselnej infraštruktúry a celkovému návrhu sieťovej infraštruktúry pre konkrétny objekt. V prvej časti komplexne popisuje ICS systém, jeho časti a princíp činnosti. Taktiež sa zaoberá aktuálnymi trendmi priemyselných sietí, systémovou komunikáciou, bezpečnostnými požiadavkami fyzickej vrstvy a hlavnými rozdielami od komerčných infraštruktúr. V druhej časti práca popisuje návrh infraštruktúry pre objekt zlievarne. Finálny návrh rieši umiestnenie rozvádzačov, špecifikáciu použitých prvkov, bezpečnosť, ekonomickú rozvahu a finálne riešenie v praxi.

KĽÚČOVÉ SLOVÁ

ICS, IT komunikácia, priemyselná infraštruktúra, bezpečnosť, firewall, Ethernet

ABSTRACT

This thesis deals with the issues of industrial communication, that is necessary to take account before making a final draft of industrial infrastructure and the overall design of a network infrastructure for a particular object. The first part of this thesis describes ICS system, parts of ICS and principle of operation. The thesis also focuses on the current trends in industrial networks, systems communication, security requirements of physical layer and the main differences from commercial infrastructures. The second part of the thesis describes the design of infrastructure for the foundry object. The final draft resolves the location of the switchboards, the specification of the used elements, the security, the cost of the solution and the final solution in practice.

KEYWORDS

ICS, IT communication, industrial infrastructure, security, firewall, Ethernet

SIDOR, Peter *Návrh infrastruktury ICS pro průmyslový podnik*: diplomová práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2016/2017. 72 s. Vedúci práce bol doc. Ing. Vladislav Škorpil, CSc.

PREHLÁSENIE

Prehlasujem, že som svoju diplomovoú prácu na tému „Návrh infrastruktury ICS pro průmyslový podnik“ vypracoval(a) samostatne pod vedením vedúceho diplomovej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorském, o právoch súvisejúcich s právom autorským a o zmeně niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

POĎAKOVANIE

Rád by som poďakoval vedúcim semestrálnej práce pánovi doc. Ing. Vladislavovi Škorpilovi, CSc. a Ing. Petrovi Sedlákovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v tejto diplomovej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
podpis autora(-ky)

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Priemyselné odvetvia naprieč výrobou či energetikou sú závislé na automatizácii svojich procesov. Tieto fungujú vďaka priemyselným systémom, (ICS-Industrial control system), čiže technológiám na správu, monitorovanie, nastavovanie a ovládanie všetkých zložiek procesu. Priemyselné systémy ICS sú všeobecným pojmom, ktorý zahŕňa niekoľko typov riadiacich systémov súvisiacich s prístrojovým vybavením používaným v priemyselnej výrobe, vrátane dispečingu, zberu dát, distribuovaných riadiacich systémov alebo programovateľných automatov PLC. Stručne povedané, priemyselné systémy ICS, sú počítače, ktoré riadia svet okolo nás. Sú zodpovedné za riadenie klimatizácie v našich kanceláriách, turbíny v elektrárňach alebo robotov v továrňach.

Historicky ICS hardvér nebol projektovaný na pripojenie do siete. Mnoho zariadení využívalo proprietárne štandardy a celý výpočet monitorovacích a riadiacich dát prebiehal na lokálnom riadiacom zariadení.

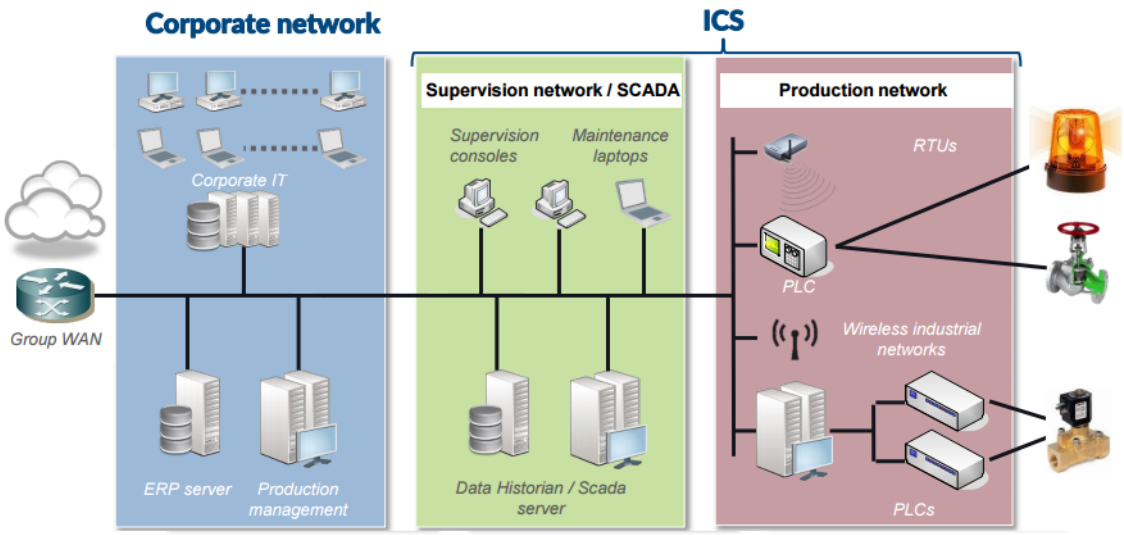
Keďže v dnešnej dobe je snaha o z jednotenie ICS systémov s komerčnými IT systémami, a to pre zjednodušenie zberu dát alebo dohľadu celého systému, je nutné sa zamyslieť nad vznikajúcimi hrozbami, ktoré môžu naskytnúť týmto riešením.

Pre pochopenie celého problému, sú v práci popísané dané rozdiely ICS od komerčných IT systémov, aké štandardy používajú a aké hrozby môžu nastať, ktoré treba zobrať do úvahy pred konečným návrhom celej infraštruktúry.

Následne práca realizuje reálny návrh priemyselnej infraštruktúry pre konkrétny priemyselný objekt zlievarne. Popisuje umiestnenie rozvádzacích prvkov, špecifikáciu aktívnych prvkov a finálne logické riešenie infraštruktúry. Záverom je realizácia návrhu v reálnom prostredí zlievarne.

1 ICS - INDUSTRIAL CONTROL SYSTEM

Ako už bolo povedané v úvode tejto práce, ICS je integrovaný hardvér a softvér určený na monitorovanie a riadenie prevádzky strojov a súvisiacich zariadení v priemyselných prostrediach. ICS používa rôzne technológie ako napríklad distribuovaný riadiaci systém DCS, dispečerské riadenie a zber dát SCADA alebo programovateľné automaty PLC[4].



Obr. 1.1: Industrial control system[7]

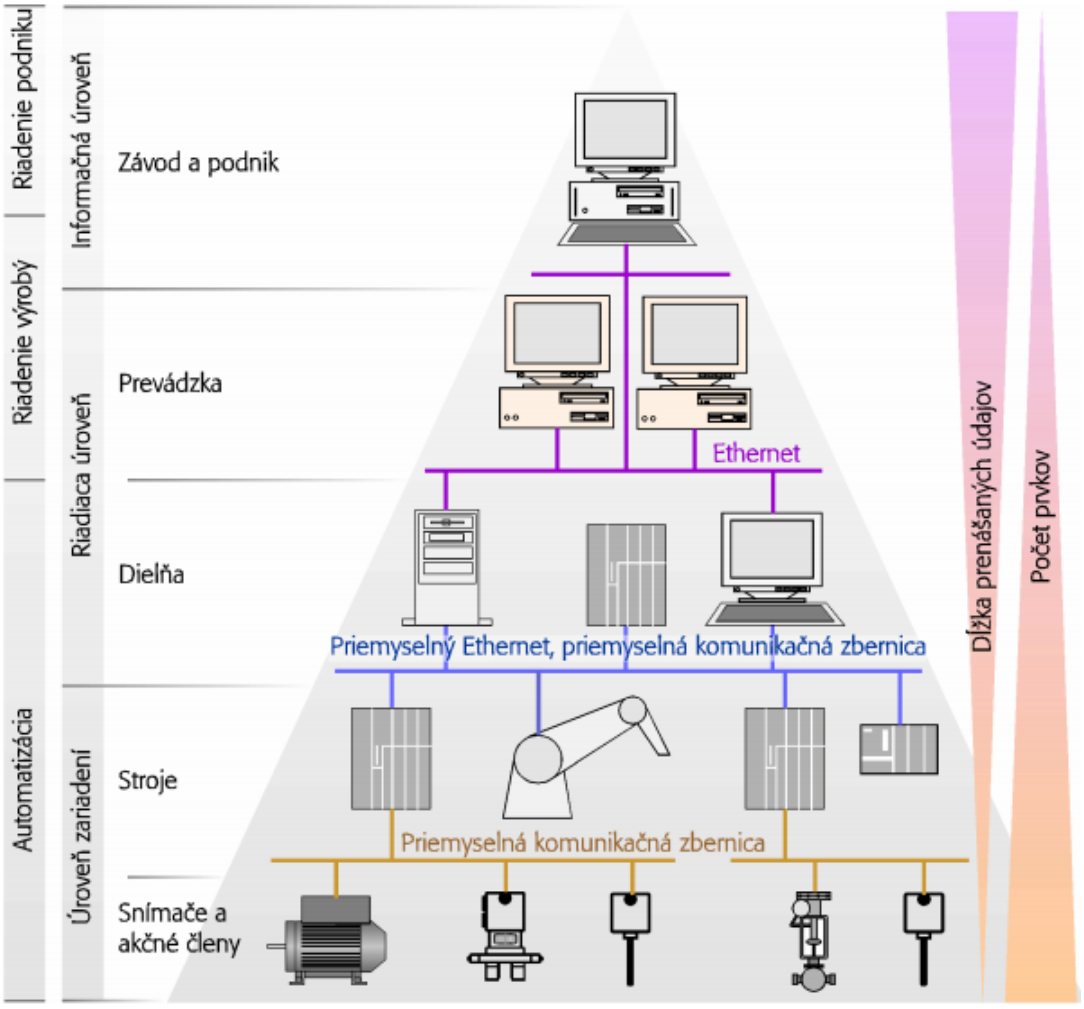
V porovnaní s komerčným IT sa dostávame do nového odvetvia kde je nutné riešiť mnoho ďalších problémov.

ICS systém, ktorý musí fungovať v rámci svojich konkrétnych výkonnostných cieľov alebo obmedzení, začal čoraz častejšie využívať technológie z IT oblasti. Bezprostredným dôsledkom konvergencie týchto technológií je, že niektoré hrozby pre štandardné IT komponenty sa vzťahujú aj na ICS. Kvôli výkonnostným cieľom a pracovnému prostrediu, nie sú bezpečnostné prostriedky používané v IT svete nevyhnutne využiteľné v ICS.

Implementácia týchto systémov sa značne líši na základne konečného priemyselného použitia. Niektoré systémy sú fyzicky koncentrované s obmedzením na definované výrobné zariadenia alebo sa nachádzajú na rozľahlej geografickej oblasti. Všetky systémy však pracujú na základe osobitných výkonnostných očakávaní alebo obmedzení.

2 PRIEMYSELNÁ KOMUNIKÁCIA

Schopnosť vzájomnej komunikácie zariadení a subsystémov je v súčasných priemyselných automatizovaných systémoch nevyhnutnosťou. Komunikácia sa realizuje horizontálne, v rámci jednotlivých úrovní riadenia a vertikálne, medzi jednotlivými úrovňami. Priemyselné automatizované systémy sú zvyčajne štruktúrované do niekoľkých hierarchických úrovní, ktoré sú zobrazené na obrázku 2.1. Každá z týchto hierarchických úrovní obsahuje patričnú komunikačnú úroveň s rôznymi požiadavkami na komunikačný systém[1].



Obr. 2.1: Hierarchia priemyselného systému[1].

2.1 Nároky na komunikačný systém

V porovnaní s komerčnou infraštruktúrou má priemyselná infraštruktúra viacero nárokov. Konkrétne sa jedná o nároky priemyselného komunikačného systému na úrovni zariadení a riadiacej úrovne (obr. 2.1).

Nároky na priemyselnú infraštruktúru:

- Prenos údajov v reálnom čase
- Činnosť v náročných priemyselných podmienkach
- Vysoká funkcie-schopnosť

2.1.1 Prenos údajov v reálnom čase

Systém reálneho času je taký systém, v ktorom správnosť výpočtov nezávisí len na logickej správnosti výpočtu, ale aj na čase vytvorenia výsledku. Ak nie sú splnené časové požiadavky systému, dôjde k nesprávnej činnosti systému. Napríklad nameraná hodnota zo snímača musí byť prenesená do riadiacej jednotky a následne spracovaná s určitým maximálnym oneskorením, inak bude daná hodnota neaktuálna a vypočítaný akčný zásah môže spôsobiť nežiadúce správanie systému[1].

2.1.2 Činnosť v náročných priemyselných podmienkach

Priemyselný komunikačný systém musí byť schopný spoľahlivej prevádzky aj v náročných priemyselných podmienkach. Fyzická vrstva priemyselnej infraštruktúry v porovnaní s komerčnou infraštruktúrou má mnoho odlišností kde sú zvýšené nároky na:

- Zvýšená teplotná odolnosť
- Odolnosť agresivity priemyselného prostredia
- Odolnosť voči vlhkosti
- Odolnosť voči vibráciám
- Odolnosť EMC
- Odolnosť voči kolísaniu napájacích napätí
- Odolnosť prašného prostredia

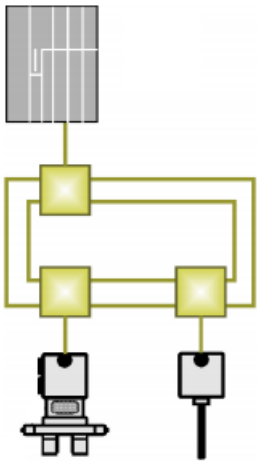
2.1.3 Vysoká funkcieschopnosť

Zvýšená funkcieschopnosť priemyselných komunikačných systémov sa dosahuje redundanciou:

- Napájania
- Prenosového média
- Systému(zariadení)

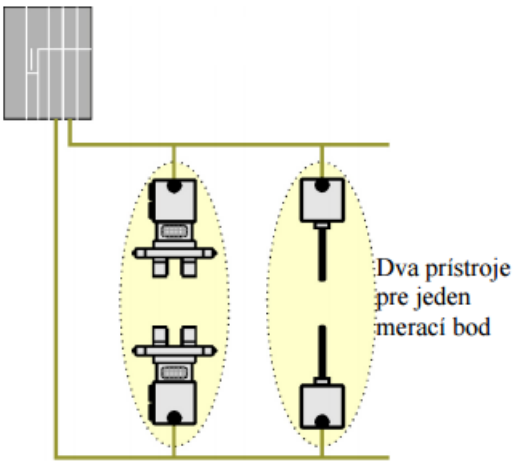
Pre zaobstaranie nepretržitej prevádzky v priemysle, zariadenia sú napájané redundantne. To znamená že každé zariadenie, ktoré spĺňa dôležitú úlohu v prevádzke je napájané dvomi zdrojmi napätia z dvoch rozdielnych sietí alebo druhý napájací zdroj je riešený záložnou batériou.

Obrázok 2.2 zobrazuje redundantnosť prenosového média a topologickú redundanciu, ktorej sa bude práca venovať nižšie.



Obr. 2.2: Príklad redundancie prenosového média[1].

Na obrázku 2.3 je uvedený príklad redundancie systému, ktorý je navrhnutý tak, že na danom konkrétnom procese pracujú aspoň dve zariadenia s rovnakou funkciou.



Obr. 2.3: Príklad redundancie systému[1].

3 PRIEMYSELNÉ RIEŠENIE ICS

Štandard lokálnej siete Ethernet nebol navrhnutý pre používanie v priemysle na spodných úrovniach riadenia a nezohľadňuje potrebu prenosu údajov v reálnom čase. Vyplýva to z použitej prístupovej metódy CSMA/CD (Carrier Sense Multiple Access with Collision Detection), ktorá vychádza z faktu, že zariadenia na LAN Ethernet používajú zdieľané prenosové médium, na ktoré môže v danej chvíli vysielať údaje len jedno zariadenie. Ak zariadenie na sieti chce odoslať údaje inému zariadeniu, musí sledovať či momentálne nevysiela údaje iné zariadenie a ak nie, potom začne vysielať. Môže sa stať, že niekoľko zariadení začne vysielať údaje súčasne. Vznikne kolízia, ktorú zariadenia zaregistrujú, prestanú vysielať a začnú znova vysielať po zvolenom časovom intervale. Ku kolízii principiálne môže dôjsť aj potom. V zásade nie je možné predvídať ako dlho budú jednotlivé zariadenia čakať na prístup na prenosové médium (kým začnú úspešne vysielať údaje) čo znamená, že prístupová metóda CSMA/CD nie je deterministická. Oblasť, v ktorej môže dochádzať ku kolíziám sa nazýva kolízna doména a je obmedzená z hľadiska maximálneho počtu zariadení aj geografického rozsahu[1].

Vzhľadom na prístupovú metódu CSMA/CD je v Ethernet sieťach možné požiadavky na reálny čas splniť len za istých podmienok:

- Segmentácia siete prepínačmi - spôsobí rozdelenie siete na niekoľko častí, ktoré sú oddelené z hľadiska vznikajúcich kolízií. Takáto segmentácia môže byť realizovaná až na úroveň jednotlivých zariadení, ktoré sú prepojené výlučne prepínačmi.
- Použitie špeciálnych komunikačných protokolov - nahrádzajú štandardné internetové protokoly

3.1 Metódy prenosu

Používané metódy prenosu údajov nie sú závislé na fyzickej a logickej topológii siete. Používajú sa tri metódy prenosu: Klient/Server, Publisher/Sunscriber a Producent/Konzument. Každá z týchto metód má svoje výhody aj nevýhody a takisto aj svoju oblasť použitia[1].

3.1.1 Metóda prenosu údajov klient/server

Metóda klient/server umožňuje prenos medzi dvoma komunikačnými partnermi, kedy prenášané údaje nepožaduje žiadne iné zariadenie. Pri tejto metóde musí zariadenie požadujúce údaje, t.j. klient vyslať požiadavku zariadeniu, ktoré je zdrojom týchto údajov, čo je server. Po tejto požiadavke server odošle údaje zariadeniu, ktoré

vystupuje vo funkcii klienta. Následne sa spojenie medzi zariadením klient a server zruší a pri opätovnom prenose údajov je ho nutné znova nadviazať. Táto metóda je vhodná na prenos údajov medzi dvomi zariadeniami, napríklad riadiacimi jednotkami (PLC a iné). Nie je príliš vhodná na prenos údajov zo snímačov, pretože pri prenose každej hodnoty – v každom komunikačnom cykle – je nutné aby zariadenie vo funcii klienta (napr. PLC) vyslalo požiadavku zariadeniu vystupujúcemu vo funkcii servera (t.j. snímaču). Ak by hodnotu z daného snímača bolo potrebné preniesť do viacerých zariadení, tak by zaťaženie siete ešte vzrástlo[1].

3.1.2 Metóda prenosu údajov publisher/subscriber

Metóda publisher/subscriber umožňuje príjem prenášaných údajov viacerými partnermi komunikácie súčasne. Zariadenie vysielajúce údaje obsahuje zoznamy zariadení, ktorým sú tieto údaje určené. Každé zariadenie, ktoré chce prijímať údaje od zariadenia publisher, ho musí jednorazovo o to požiadať a až v dôsledku tejto žiadosti si ho zariadenie publisher zaradí do svojho zoznamu. Metóda je vhodná na cyklický prenos časovo kritických údajov v regulačných slučkách. Pri odosielaní správ sa môže použiť skupinová adresácia, na základe ktorej sú správy prijímané len tými účastníkmi komunikácie, ktorým je správa určená, alebo je správa opakovane odosielaná všetkým zariadeniam, ktoré o údaje v správe požiadali[1].

3.1.3 Metóda prenosu údajov producent/konzument

V metóde producent/konzument sa používa pri prenose správ skupinová adresácia, podobne ako v metóde pubslisher/subscriber. Rozdiel je však v tom, že žiadny partner komunikácie nemá vytvorený zoznam komunikačných partnerov, ktorým vysiela, alebo od ktorých prijíma údaje. Pri prenose sú údaje označené špeciálnym identifikátorom. Prvý konzument daných údajov odošle žiadosť o tieto údaje ich producentovi. Producent a konzument sa dohodnú na skupinovej adrese a identifikátore pre tieto údaje. Producent bude odteraz odosielať dané údaje na dohodnutú skupinovú adresu. V prípade, že o tieto údaje má záujem aj iný konzument, tento požiada o pridelenie skupinovej adresy a identifikátora údajov od producenta, alebo iného konzumenta[1].

Metódy publisher/subscriber a producent/konzument znižujú zaťaženie komunikačného systému vychádzajúceho z Ethernetu, avšak niekedy môžu klásť zvýšené nároky na pripojené zariadenia. Ide predovšetkým o vysielanie a príjem správ s globálnou a skupinovou adresáciou, ktoré nemusia byť schopné spracovať všetky zariadenia na sieti[1].

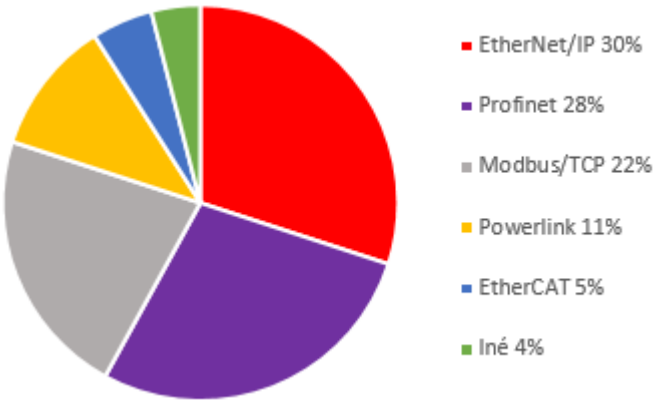
3.2 Štandardy priemyselného Ethernetu

V rámci vývoja a používania siete Ethernet v priemyselnej praxi vzniklo viacero riešení. Medzinárodná elektrotechnická komisia (IEC) prijala návrhy na uznanie za štandard pre 10 ethernetových priemyselných protokolov. Tieto protokoly sú uvedené v tabuľke tab.3.1.

Tab. 3.1: Štandardy priemyselného Etheretu

Názov	Štandart IEC
EPA	IEC/PAS 62409
EtherCAT	IEC/PAS 62407
EtherNet/IP	IEC/PAS 62413
Powerlink	IEC/PAS 62408
MODBUS RTPS	IEC/PAS 62030
P-NET on IP	IEC/PAS 62030
Profinet	IEC/PAS 62412
Sercos 3	IEC/PAS 62410
TCnet	IEC/PAS 62406
Vnet/IP	IEC/PAS 62405

Kedže nie všetky protokoly sú v praxi využívané, práca sa bude venovať iba najpoužívanejším, najkomerčnejším protokolom. Porovnanie využívania protokolov môžme vidieť na obrázku 3.1, kde môžme vidieť dominantný EtherNet/IP nasledovaný Profinetom.



Obr. 3.1: Protokoly ICS

3.2.1 EtherNet/IP

EtherNet/IP definovala firma Rockwell a podporujú ho združenia ODVA (Open DeviceNet Vendor Association) a ControlNet International. Na úrovni aplikačnej vrstvy využíva protokol CIP (Control and Information Protocol), ktorý zastrešuje komunikačné siete Ethernet, ControlNet a DeviceNet. Umožňuje prenos vstupno-výstupných, diagnostických a konfiguračných údajov cez klasický Ethernet. Prenos údajov je acyklický aj cyklický, s dlžkou trvania zbernicového cyklu 10-100 ms. Implementuje algoritmus synchronizácie hodín komunikujúcich zariadení podľa štandardu IEEE 1588 prostredníctvom nového objektu aplikačnej vrstvy CIPsync. Dosiahnuteľná presnosť synchronizácie je lepšia ako 1 ms. Prenosová rýchlosť protokolu je 10/100/1000 Mbps. Ako prenosové médium slúžia metalické a optické káble a možný je aj bezdrôtový prenos. Komunikácia s inými priemyselnými komunikačnými zbernicami sa uskutočňuje cez brány pre zbernice ControlNet a DeviceNet, ktoré používajú rovnaké protokoly aplikačnej vrstvy[1].

3.2.2 ProfiNet

ProfiNet vyvinulo združenie PNO (Profibus Nutzer/User Organisation) so silnou podporou firmy Siemens a je k dispozícii od roku 2000. Prvá verzia ProfiNet zabezpečovala časovo nie kritickú komunikáciu (nie v reálnom čase) zariadení vyššej úrovne riadenia, so zariadeniami na priemyselnej komunikačnej zbernici PROFIBUS DP, na ktorej sa realizoval prenos údajov v reálnom čase. Pri komunikácii sa využívali aj protokoly TCP/UDP/IP. Preto sa ProfiNet v1 radí medzi štandardy priemyselného Ethernetu, ktoré využívajú protokoly spodných troch vrstiev Internetu. Druhá verzia ProfiNet v2 už umožňuje prenos údajov v reálnom čase pomocou špeciálneho protokolu, ktorý obchádza sieťovú a transportnú vrstvu. Prenos údajov je acyklický aj cyklický, s dlžkou trvania komunikačného cyklu 5-10 ms. Možný je aj prenos údajov paralelným kanálom prostredníctvom protokolov TCP/IP, ale bez nárokov na reálny čas. V najnovšej verzii ProfiNet v3 je časť funkcií zabezpečujúcich prenos v reálnom čase implementovaná vo vrstve sieťového rozhrania, z čoho vyplýva, že na prepojenie jednotlivých zariadení sú potrebné špeciálne prepínače a komunikačné karty, čo nebolo nutné v predchádzajúcich verziách. Hardvérová podpora komunikácie v reálnom čase sa prejavila v skrátení dĺžky zbernicového cyklu na 1 ms, s možnosťou synchronizácie hodín komunikujúcich zariadení pri časovej neistote menšej ako 1 ms. Prenosová rýchlosť používaná v systémoch ProfiNet je 10/100 Mbps[1].

3.2.3 MODBUS RTPS

Predstavuje doplnenie komunikačného protokolu MODBUS/TCP o prenos údajov v reálnom čase. Modbus/TCP je odvodený z protokolu Modbus a bol vyvinutý firmou Modicon (Schnieder Electric) v roku 1979. Umožňuje jednoduché prepojenie zbernice Modbus so sieťou Ethernet. Minimálna doba odozvy s protokolom je 20 ms bez možnosti synchronizácie komunikujúcich zariadení. Prenosová rýchlosť je 10/100 Mbps[1].

3.2.4 Powerlink

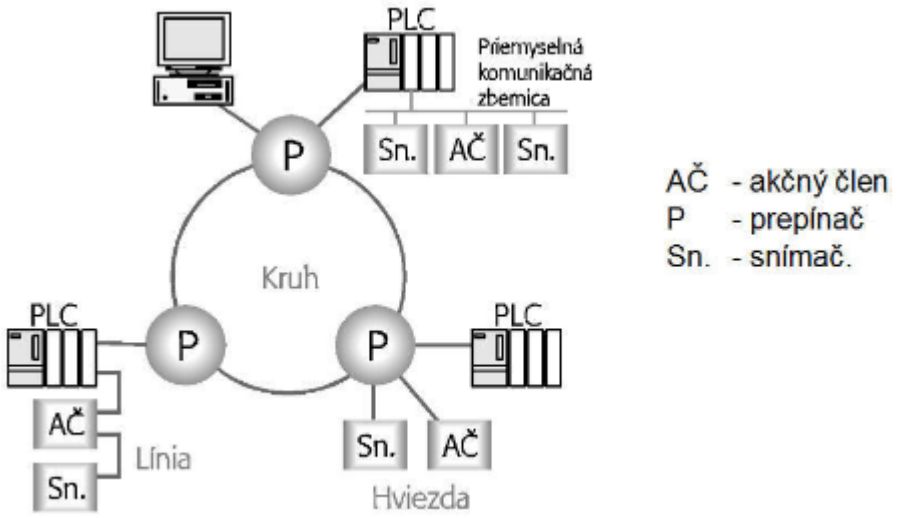
Powerlink vyvinula rakúska firma Bernecker + Reiner a podporuje ho združenie EPSG (Ethernet Powerlink Standardisation Group). Pôvodne bol uvedený na trh spolu s produktami na riadenie pohybu. Dĺžka zbernicového cyklu je viac ako 0,1 ms a časová neistota pri synchronizácii komunikujúcich zariadení algoritmom IEEE 1588 je menšia ako 1 ms. Cyklický prenos údajov procesných veličín je realizovaný protokolom EPL, na acyklický prenos údajov (napr. parametre zariadení) sa využívajú protokoly UDP/IP. Aplikačná vrstva EPL je odvodená zo štandardu CANopen. Integrácia EPL a CANopen zlučuje profily, účinný prenos údajov a otvorenú komunikáciu s protokolmi TCP/UDP/IP. Prenosová rýchlosť je 100 Mbps[1].

3.2.5 EtherCAT

EtherCAT (Ethernet for Control Automation Technology) vyvinula nemecká firma Beckhoff a podporuje ju združenie ETG (EtherCAT Technology Group). Dĺžka komunikačného cyklu je 30 ms pre 1000 vstupných a výstupných binárnych signálov, alebo 100 ms pre 100 servopohonov. Presnosť synchronizácie komunikujúcich zariadení algoritmom IEEE 1588 je lepšia ako 1 ms, pričom prenos údajov v reálnom čase je možné zabezpečiť štandardnými ethernetovými kartami. EtherCAT podporuje zariadenia a aplikačné profily CANopen. Štandard CANopen definuje komunikačné profily, profily zariadení a aplikačné profily. Prenosová rýchlosť v sieti EtherCAT je 100 Mbps[1].

3.3 Fyzická topológia

Zariadenia na fyzickej vrstve môžu byť prepojené na základe rôznych topológii, ktoré sú zobrazené na obrázku 3.2.



Obr. 3.2: Príklad prepojenia zariadení v priemysle[1]

3.3.1 Zbernica

V prvých ethernetovských sieťach sa používala topológia zbernica, v ktorej bol ako prenosové médium použitý koaxiálny kábel. V takomto prípade sa jednotlivé zariadenia pripájajú paralelne ku spoločným vodičom. Pri prenose údajov medzi prepojenými zariadeniami môže dochádzať ku kolíziám.

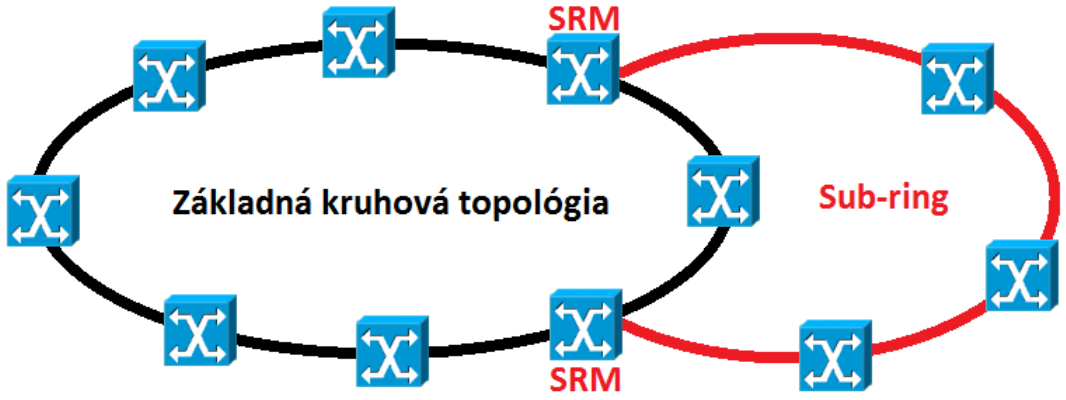
3.3.2 Hviezda-Strom

Ďalšou, v súčasnosti najrozšírenejšou topológiou v oblasti lokálnych sietí, je hviezda, respektíve strom. Zariadenia sú zapájané kaskádovito za sebou v tvare stromu čo z pohľadu zabezpečenia prenosu nieje ideálne. Pri poruche jedného zariadenia nastáva strata konektivity ostatných zariadení, ktoré komunikovali prostredníctvom komunikačného zariadenia s poruchou.

3.3.3 Kruh

Najbezpečnejšou topológiou v priemyselných sieťach je kruhová topológia. Všetky dôležité komunikačné zariadenia sú zapojené za sebou do kruhu. V prípade poškode-

nia niektorého zariadenia v kruhu, údaje sa prenášajú náhradnou trasou. Kruhovú topológiu je možné vetviť na ďalšie takzvané sub-ringy pomocou sub-ring manažérov (SRM).



Obr. 3.3: Príklad vetvenia kruhovej topológie

Výber trasy prenosu dát, ako aj pri poruche a neduplicitu dát zabezpečujú redundantné protokoly, ktoré sa taktiež používajú aj v komerčných sieťach. Pre zvýšené nároky v priemysle, kde pri výpadku zariadenia musí byť zabezpečená čo najrýchlejšia konvergencia siete, boli navrhnuté špeciálne redundantné protokoly pre priemysel, ktoré disponujú veľmi malými reakčnými časmi. V tabuľke 3.2 je možné vidieť porovnanie protokolov komerčnej a priemyselnej siete.

Tab. 3.2: Štandardy redundantných protokolov

Protokol- komerčná sieť	Štandard IEC	Čas obnovy	Topológia
STP-Spanning Tree	IEEE802.1	30 s	všetky
RSTP-Rapid Spanning Tree	IEEE802.1	2 s	všetky
CRP-Cross Network	IEC 62439-2008	1 s	všetky
BRP-Beacon Redundancy	IEC 62439-2008	4,8 ms	hviezda, kruh
Protokol- priemyselná sieť	Štandard IEC	Čas obnovy	Topológia
MRP-Media Redundancy	IEC 62439-2008	200 ms	kruh
Fast MRP-Media Redundancy	IEC 62439-2	10-15 ms	kruh
PRP-Parallel Redundancy	IEC 62439-2008	0 ms	všetky
High Available Saemless Ring	IEC 62439-3	0 ms	kruh

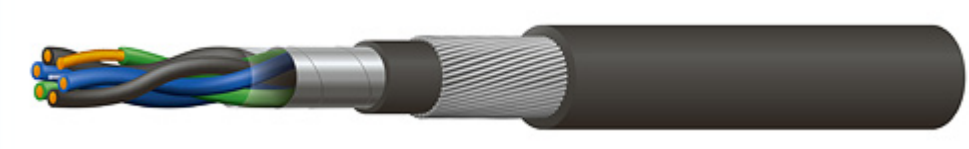
3.4 Pasívna vrstva

3.4.1 Požadované vlastnosti komponentov

- Životnosť 10 až 30 rokov
- Montáž zariadení do 19",21/23", 26"rozvádzačov a na DIN lištu
- Malé rozmery zariadení
- Zariadenia s pasívnym chladením
- Zodolnené prevedenie z pohľadu korózie
- Zodolnené zariadenie z pohľadu krytia (vodotesnosť)

3.4.2 Káblové spoje

Kvôli špecifickému priemyselnému prostrediu musia káble používane v ňom, byť odolné voči priemyselným nástrahám ako napríklad elektromagnetické rušenie, rôzne chemikálie, voda a oleje. Taktiež plášte káblov musia byť odolné voči mechanickému poškodeniu. To je zabezpečené pomocou špeciálneho konštrukčného materiálu plášťa alebo špeciálnym výrobným procesom napríklad pridaním tienenia alebo ochranného kovového obalu (tkvz. armované káble, obr. 3.4).



Obr. 3.4: Príklad armovaného káblu[2]

Najčastejšie používané materiály plášťov káblov:

- **PVC** - najčastejšie používaný materiál. Horľavý, taktiež pri horení vznikajú jedovaté splodiny. Rozsah pracovných teplôt od -20 do 60 °C. Existujú aj priemyselné verzie odolné voči vode, olejom a chemikáliám s vyšším rozsahom pracovných teplôt.
- **NH materiály** - Bezhalogenové materiály - sú charakteristické nehorľavosťou, preto sa používajú v miestach so zvýšenou koncentráciou osôb (nemocniciach, školách, divadlách. . .)
- **Polyetylén** - sa vyznačuje pomerne vysokou odolnosťou voči kyselinám, zásadám a niektorým chemikáliám. Horľavý, vhodný do vonkajších prostredí.
- **HDPE** - Polyetylén s vysokou hustotou je chemicky odolný, bez zápachu, netoxický, vodeodolný ale UV žiarením degradujúci. Vhodný pre priame uloženie do zeme.

- **FCP** - Fluorokopolymery sú charakteristické hlavne vysokou teplotnou odolnosťou, niektoré materiály až do 260 °C.
- **PUR** - Polyuretan je veľmi perspektívny materiál s vysokou odolnosťou voči vode, olejom, chemikáliám, UV žiareniu a oderom. Pracovné teploty sú od -25 do 80 °C.

3.4.3 Konektory

Taktiež konektory využívané v priemyselnom prostredí sa v porovnaní s komerčným využitím líšia v konštrukcii. Musia spĺňať kritéria priemyslu a obsahovať krytie odpovedajúce danému prostrediu. Najčastejšie sa používajú klasické konektory RJ45 s ochranou alebo štandardnejšie priemyselné konektory typu M12.

- **Konektor RJ45 s ochranou** - štandardné zapojenie ako v komerčnej IT, ľubovolná prenosová rýchlosť, podpore PoE

Obr. 3.5: Príklad konektoru RJ45[2]

- **Konektor M12** - rôzne zapojenie konektorov pre rôzne prenosové rýchlosti, podpora PoE, integrovaná ochrana

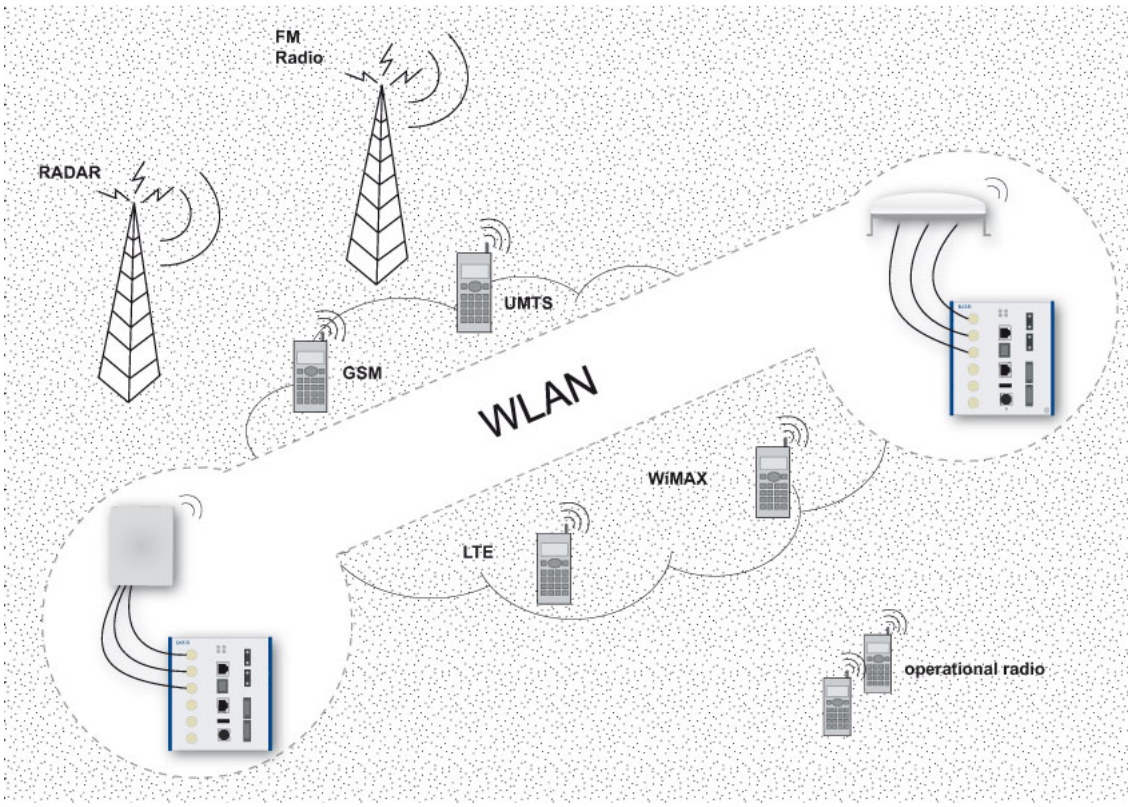
Obr. 3.6: Príklad konektoru M12[2]

- **Optický konektor s ochranou** - štandardné zapojenie, ľubovolná prenosová rýchlosť

Obr. 3.7: Príklad optického konektoru pre priemysel[2]

3.4.4 Bezdrôtové spoje

Technológie WLAN pre priemyselné prostredie by mali disponovať technológiou, ktorá umožňuje vyhradiť komunikačný spoj komunikujúcim zariadeniam. Technológia zaručuje neprerušovaný bezdrôtový prenos tým, že eliminuje všetky súbežné rádiové frekvencie. Výsledkom je nižšia hladina šumu a menšia strata paketov.



Obr. 3.8: Príklad princípu technológie[2]

4 BEZPEČNOSŤ

Donedávna sa väčšina priemyselných riadiacich systémov vyvíjala s dôrazom na vysokú spoľahlivosť, bezpečnosť a maximálnu prevádzkyschopnosť. Desaťročia sa priemysel zameriaval na plnenie týchto požiadaviek bez akéhokoľvek dôrazu na digitálnu bezpečnosť.

Priemyselné systémy sa v posledných rokoch presunuli z uzavretých proprietárnych sietí do prostredia Internetu. Vďaka tomu sa mnoho prevádzok zo všetkých oblastí priemyslu stalo predmetom záujmu útočníkov, ktorí ku kompromitácii využívajú tradičné i novo objavené zraniteľnosti, podobne ako pre iné systémy a aplikácie fungujúce na internete.

4.1 Rizikové faktory

Niekoľko faktorov v súčastnosti prispieva k rastúcemu riziku narušenia bezpečnosti priemyselnej infraštruktúry:

- Používanie štandardizovaných protokolov a technológii so známymi zraniteľnosťami
- Pripojenie riadiacich systémov do ostatných sietí
- Rozšírená dostupnosť technických informácii o riadiacich systémoch
- Nezabezpečené a neisté pripojenie

4.1.1 Štandardizované protokoly a technológie

Pre uľahčenie výroby kompatibilného príslušenstva tretím stranám, výrobcovia ICS začali zverejňovať svoje proprietárne protokoly a špecifikovať ich vlastnosti. Kvôli zníženiu nákladov, zvýšenie výkonu a zabezpečenie interakcie medzi priemyselnými systémami a počítačovými aplikáciami, niektoré organizácie prechádzajú z proprietárnych technológií na lacnejšie štandardizované technológie ako napríklad bežný sieťový TCP/IP protokol. Prechod na používanie týchto otvorených štandardov stanovuje hospodárske a technické výhody, ale tiež zvyšuje náchylnosť ICS na počítačové incidenty[8].

4.1.2 Pripojenie ICS do ostatných sietí

ICS a IT systémy sú často vzájomne prepojené v dôsledku správy informácií, prevádzkových a obchodných potrieb. Dopyt na vzdialený prístup podnietil mnoho organizácií nadviazať spojenie s ICS, ktoré umožňuje sledovanie a ovládanie systému z miest mimo priemyselnej siete. Táto integrácia ICS s verejnou alebo podnikovou

sieťou zvyšuje dostupnosť zraniteľnosti systému. Ak nie sú začlenené konkrétne bezpečnostné podmienky, systém je vystavený možným kybernetickým útokom[8].

4.1.3 Rozšírená dostupnosť technických informácii

Verejné informácie týkajúce sa dizajnu ICS, údržby, prepojenia a komunikácie sú ľahko dostupné na internete, pre uľahčenie výberu produktu alebo umožnenie používania otvorených štandardov. Predajcovia ICS taktiež umožňujú zakúpiť pomôcky, ktoré pomáhajú vyvíjať softvér ktorý implementuje rôzne štandardy ICS. Z toho vyplýva, informácie a zdroje sú potencionálnym protivníkom k dispozícii všade na svete[8].

4.1.4 Nezabezpečené a neisté pripojenie

Mnoho predajcov ICS dodali systémy s modemami dial-up, ktoré poskytujú vzdialený prístup k odľahčeniu záťaže na údržbu pre technickú podporu. Vzdialený prístup niekedy poskytuje personál s prístupovými právami správcu napríklad identifikácia a heslo. Útočníci pomocou špeciálneho softvéru môžu získať tieto informácie a následne získať prístup k systému prostredníctvom týchto schopností vzdialeného prístupu[8].

4.2 Sieťová architektúra

Pri návrhu sieťovej architektúry a pre nasadenie ICS sa obvykle odporúča oddeliť ICS od podnikovej siete. Povaha týchto dvoch sietí je rozdielna. Prístup na internet FTP, mail alebo vzdialený prístup je zvyčajne dovolený pre podnikovú sieť ale nemal by byť umožnený pre sieť ICS.

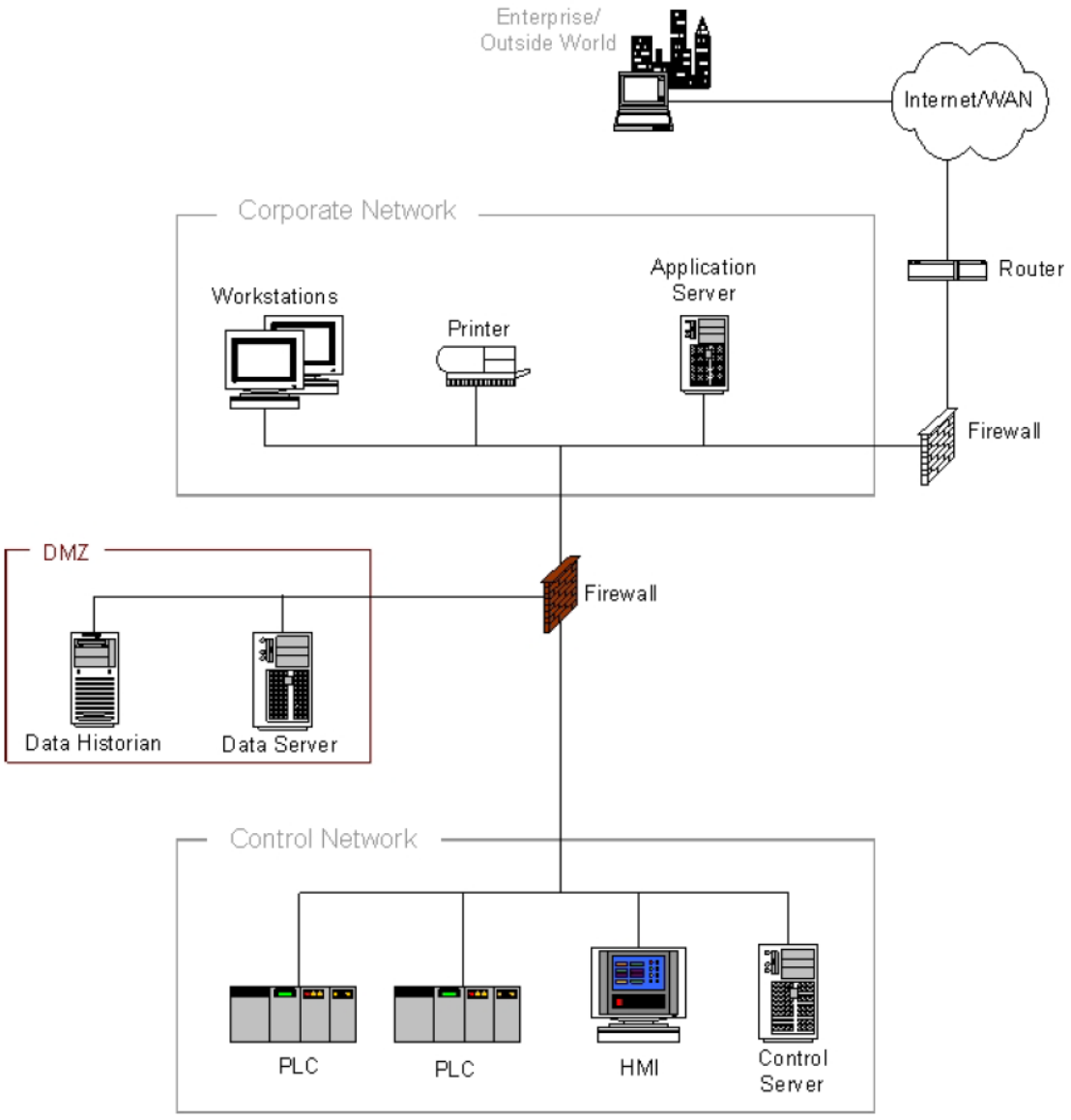
Praktické úvahy často ale smerujú ku zjednoteniu a prepojeniu ICS a podnikovej siete. Toto riešenie významne navyšuje bezpečnostné riziko a malo by sa starostlivo zvážiť pri návrhu a implementácii. Ak je nutné prepojenie týchto sietí, dôrazne sa odporúča obmedziť spojenie iba na nevyhnutné služby pomocou firewallu alebo DMZ.

DMZ je samostatný sieťový segment, ktorý sa pripája priamo k firewallu. Servery, ktoré obsahujú dáta z ICS, ku ktorým je potrebné pristupovať z podnikovej siete sú prevádzkované v tomto segmente siete. Len tieto systémy firemnej siete by mali mať možnosť pristupovať k týmto dátam.

Vonkajší prístup by mal byť obmedzený na minimum pomocou brány firewall, vrátane otvorenia portov nevyhnutných pre konkrétnu komunikáciu[8].

4.2.1 Firewall

Sieťové firewally sú zariadenia alebo systémy, ktoré riadia tok sieťovej prevádzky medzi sieťami, ktoré patria do rozdielnych bezpečnostných zón. Vo väčšine moderných aplikácií, firewally sú popisované v súvislosti s pripojením internetu a protokolov TCP/IP. Avšak, firewally majú využitie v sieťových prostrediach, ktoré nemajú a nevyžadujú pripojenie k internetu. Napríklad mnoho podnikových sietí využíva firewally pre oddelenie citlivejších služieb ako napríklad účtovníctvo alebo oddelenie ľudských zdrojov[8].



Obr. 4.1: Príklad prepojenia ICS s podnikovou sieťou [8]

5 ROZBOR SÚČASNÉHO STAVU OBJEKTU

Cieľom práce je spracovať návrh riešenia pre jednotný priemyselný komunikačný systém priemyselného objektu zlievarne. Návrh systému bude slúžiť ako realizačná dokumentácia pre rekonštrukciu súčasného nevyhovujúceho stavu komunikačného systému zlievarne.

V tejto kapitole je podrobne popísaný východzí stav priemyselného komunikačného systému zlievarne, pre ktorý následne bude spravený konkrétny návrh priemyselného komunikačného systému.

5.1 Popis súčastného stavu

Na základe predloženej dokumentácie a fyzického prieskumu objektu je objekt rozdelený na dva logické bloky:

- Administratívna časť - v tejto časti sa nachádza sieťová infraštruktúra prvého a tretieho poschodia administratívnej budovy. Tieto priestory sú z elektrotechnického pohľadu normálne, bez žiadnych vonkajších vplyvov.
- Výrobná (priemyselná) časť - súvisí s výrobou a je definovaná ako priemyselné prostredie, pretože ide o ťažké výrobné procesy (zlievareň), s vonkajšími vplyvmi typu vysoké pracovné teploty, agresivné prašné prostredie, mechanicke otrasy a vonkajšie vlhkosti.

5.2 Popis súčasnej infraštruktúry

V súčasnosti je sieťová infraštruktúra v stave odpovedajúcemu postupnému a dlhodobému nekoordinovanému budovaniu. Nedbá sa na rozdelenie prostredia na normálne a priemyselné prostredie. Taktiež sa nejedná o certifikovaný kabelážny systém so zárukou výrobcu. S veľkou pravdepodobnosťou bola sieťová infraštruktúra budovaná svojpomocne.

5.2.1 Topológia siete

Súčasná topológia siete je realizovaná zapojením do hviezdy, zároveň bez žiadnej redundancie zariadení alebo redundancie napájania zariadení. Vybrané koncové body sú osadené iba záložnými UPS zdrojmi (obr. 5.1), ktoré však nespĺňajú priemyselné podmienky.

Obr. 5.1: Nevyhovujúci záložný UPS zdroj.

5.2.2 Optický rozvod

Je realizovaný zapojením do hviezdy začínajúci v centrálnom optickom rozvádzači, nachádzajúcim sa v hlavnom dátovom rozvádzači v technickej miestnosti. Optické rozvody pozostávajú z piatich segmentov ukončených v podružných dátových rozvádzačoch. Jeden segment je ukončený v závese na borovici v mieste pôvodného umiestnenia bunky obr. 3.1. K vedeniu optických trás neexistuje dokumentácia.

Obr. 5.2: Ukončenie optickej vetvy.

5.2.3 Metalické vedenie

Káblové trasy sú uložené v PVC lištách, v PVC káblových žľaboch alebo voľne zväzované do zväzkov. Vedenie v administratívnej budove je v prevedení UTP (netienená kabeláž kategórie 5e) budovaná pravdepodobne v dvoch etapách. Kabely sú ukončené v patch paneloch LYNX. K vedeniu metalických trás neexistuje dokumentácia.

V priestoroch výroby je metalické vedenie realizované pripojením k rozvodným lávkam silnoprúdu, prípadne sú ťahané po strechách výrobných hál v ochranných žľaboch. Nie sú rešpektované základné pravidlá realizácie metalického vedenia z pohľadu elektromagnetickej kompatibility. Taktiež nieje dodržaná norma ČSN 50173-3-A1 pre priemyselné priestory.

5.2.4 Bezdrôtové technológie - Wifi

V priestoroch administratívnej budovy sa nachádzajú štyri bezdrôtové zariadenia pracujúce na štandarde 802.11.

V priestoroch expedície je umiestnené bezdrôtové proprietárne riešenie pre zber dát s napojením na obslužné PC pripojené na aktívny prvok v podružnom dátovom rozvádzači.

5.2.5 Logické rozdelenie

Z pohľadu logickej topológie, sieť je bez segmentácie či zónového rozdelenia.

Pre administratívnu časť je zvolený privátny adresný priestor 192.165.200.0/24, ktorý je pre prevádzku nedostatočný.

Výrobná priemyselná časť obsahuje dva adresné priestory:

- - 128.0.0.0/16 (výrobná linka PLC HWS)
- - 172.17.0.0/16 (výrobná linka Eirich – pieskovňa)

5.2.6 Aktívne prvky

Niektoré z aktívnych prvkov sú nevhodne umiestnené a prevádzkované. Zároveň nieje aplikovaná jednotná koncepcia zariadení a taktiež nieje aplikovaný jednotný manažment siete. Neexistuje žiadna evidencia zariadení.

5.2.7 Pripojenie k internetu

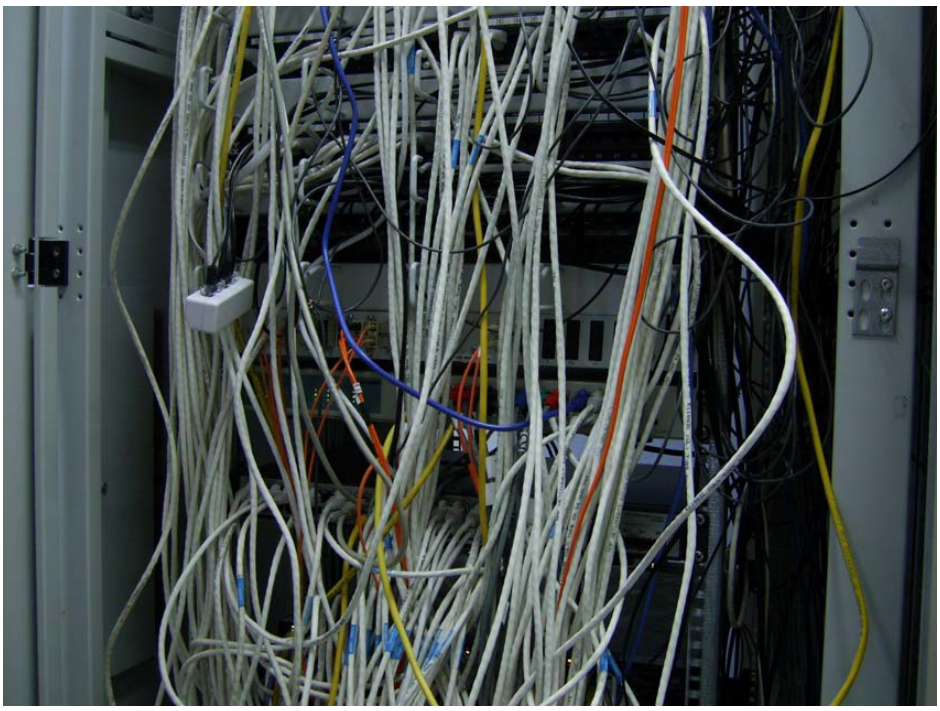
V serverovni je umiestnený nástenný dátový rozvádzač s technológiami zabezpečujúcu konektivitu na Internet (riešene v rámci zmluvy s poskytovateľom internetu). Bezdrôtové pripojenie poskytuje firma GTS s parametrami konektivity 8 mbps a symetrickým pripojením.

5.2.8 Serverovňa

Je umiestnená na treťom poschodí administratívnej budovy. Je vybavená týmito dátovými rozvádzačmi:

- Samostatný nástenný dátový rozvádzač poskytovateľa pripojenia na internet
- Samostatný dátový rozvádzač pre ukončenie horizontálnej kabeláže a hlavného optického rozvodu
- Stojanový dátový rozvádzač pre servery a telefónnu ústredňu

Oba stojanové rozvádzače sú v prevedení uzavretých skríň, čo z pohľadu centrálneho chladenie je nevyhovujúce.



Obr. 5.3: Stojanový dátový rozvádzač v serverovni

6 NÁVRH ICS PRE PRIEMYSELNÝ PODNIK

Cieľom tejto kapitoly je spracovať návrh riešenia pre jednotný priemyselný komunikačný systém priemyselného objektu zlievarne.

Základné požiadavky sú vysoká spoľahlivosť, bezporuchový chod a bezpečnosť prevádzky celého systému. Taktiež riešenie celého systému musí vykazovať potrebný stupeň flexibility a modularity prípojných bodov systému v závislosti na budúce možné zmeny konfigurácie jednotlivých pracovísk. Flexibilita a modularita plynie aj z požiadavky klienta z dôvodu rekonštrukcie systému po etapách bez žiadneho vplyvu na súčasnú infraštruktúru.

Vysoká miera spoľahlivosti bude riešená použitím robustných priemyselných aktívnych prvkov, redundantných komunikačných spojení a redundantných sieťových napájaní. Chod komunikačného systému bude realizovaná monitorovacím dohliadacím a konfiguračným softvérom.

Celkový návrh vychádza a musí spĺňať určité zadanie, ktoré investor vyžaduje:

- Návrh riešenia ICS
- Napojenie na súčasnú infraštruktúru ICT podniku
- Realizácia riešenia bez vplyvu na súčasnú infraštruktúru
- Budovanie po etapách
- Realizácia v plnej prevádzke

6.1 Obecné riešenie ICS

Všetky atribúty vychádzajú z požiadavkov na bezpečnú a spoľahlivú prevádzku zlievarne. Finálny návrh pre komunikačný priemyselný systém vychádza z určitých obecných požiadaviek investora a musí ich systém spĺňať:

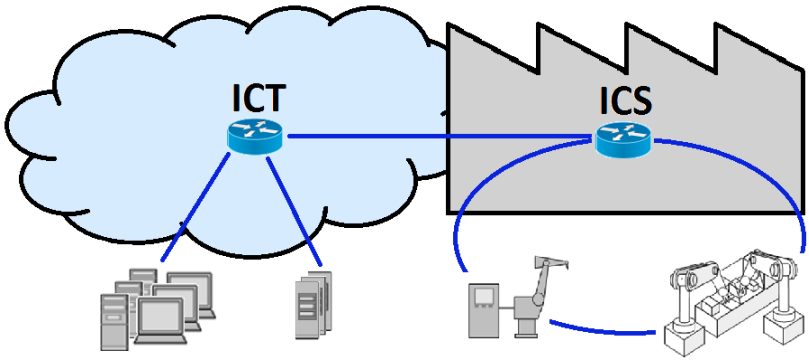
- Normované riešenie
- Redundancia
- Modularita
- Kruhová topológia ICS siete
- Výber jednotnej platformy aktívnych prvkov
- Pokrytie mobilných pracovísk - priemyselné Wi-fi technológie
- Jednotný dohľad nad celou infraštruktúrou
- Hlavný kruhový rozvod - optický rozvod

6.2 Topologické riešenie

Topologické riešenie vychádza zo základného rozdelenia návrhu riešenia na dva základné celky:

- Administratívna časť (ICT)
- Výrobná (priemyselná ICS) časť

Problematika rozdelenia komunikačného systému je blokovo znázornená na obrázku 6.1.



Obr. 6.1: Obecné riešenie systému

V konkrétnom prípade zlievarne, ICT blok značí administratívnu časť sieťovej infraštruktúry. Jedná sa o prvé a tretie podlažie administratívnej budovy, kde sú situované kancelárie podniku, hlavná rozvodňa a serverovňa. Topológia rozvodov administratívnej časti je distribuovaná hviezda.

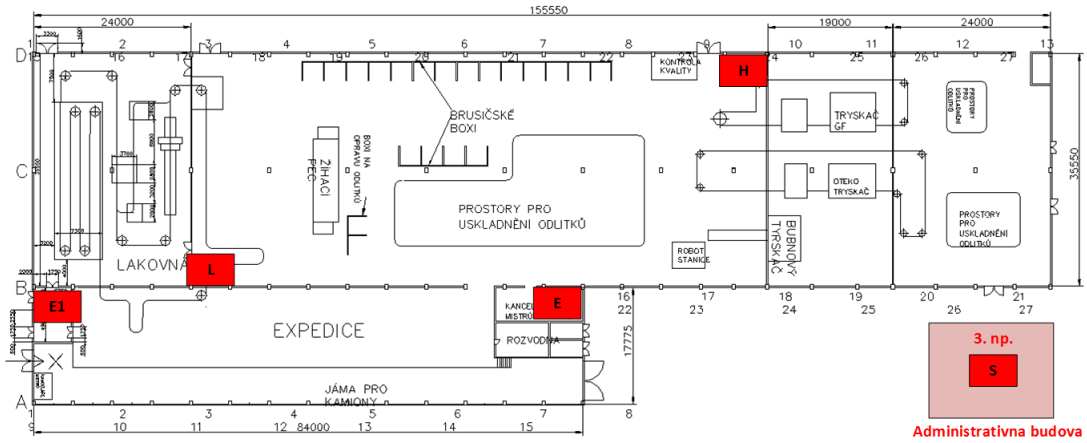
Výrobnú časť zlievarne značí blok ICS. Táto časť je definovaná ako priemyselné výrobné prostredie rešpektujúce požiadavky priemyselnej siete. Z pohľadu topológie to znamená návrh optického rozvodu zapojeného v kruhovej topológii, čo automaticky spĺňa požiadavky na redundantné riešenie zapojenia.

Výrobná časť zlievarne je rozdelená na štyri hlavné časti:

- Expedícia - časť výrobnej haly určená pre expedíciu vyrobených produktov. Je tu situovaná nákladná plošina pre nakladacie zariadenia a parkovacia oblasť pre nákladné vozidlá. Taktiež sa tu nachádzajú kancelárie pre obsluhu a rozvodňa.
- Lakovňa - nachádza sa tu lakovacia linka s automatizovanou linkou pre sušenie lakovaných materiálov.
- Hlavná hala - v tejto hale sa nachádza obsluha kontroly kvality, žíhacia pec a automatizovaný robot Kuka.
- Tryskovňa - miestnosť určená pre tryskacie roboty.

6.2.1 Určenie hlavných rozvodných uzlov

Prvým krokom návrhu je určenie kde sa budú nachádzať hlavné rozvodné uzly hlavného optického kruhového rozvodu.



Obr. 6.2: Rozmiestnenie hlavných rozvodných uzlov

Z pohľadu modularity a flexibilnosti budúceho rozšírenia systému boli stanovené štyri hlavné rozvodné body umiestnené vo výrobnej časti zlievarne a jeden hlavný bod nachádzajúci sa v administratívnej budove slúžiaci na ukončenie kruhového optického rozvodu.

Hlavné rozvodné body:

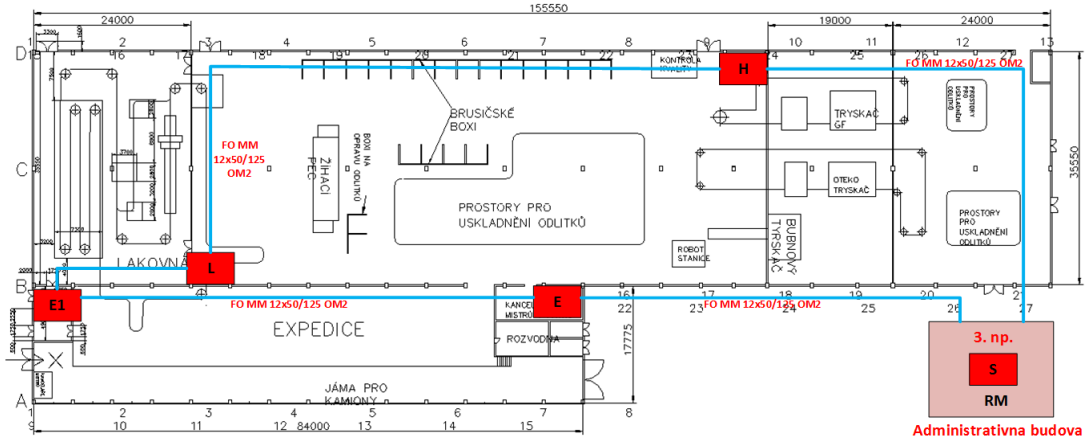
- E - rozvodný bod umiestnený v kanceláriách expedičnej haly - pripojenie kancelárií a wi-fi technológii pre expedíciu.
- E1 - rozvodný bod umiestnený v kanceláriách expedičnej haly (podmienka investora)
- L - rozvodný bod umiestnený v lakovni slúžiaci na pripojenie lakovacích liniek
- H - rozvodný bod umiestnený v hlavnej hale - kontrola kvality, pripojenie ďalších výrobných zariadení haly
- S - rozvodný bod umiestnený na treťom podlaží administratívnej budovy

Konštrukcia hlavného dátového rozvádzača je typizovaná pre použitie v celej výrobnej časti. Jedná se o modulárny prvok typu hlavný rozvodný bod, ktorý je možné realizovať postupne podla priorít a potrieb rekonštrukcie prevádzky. Platí však omedzenie súvisiace s pripojovaním týchto rozvádzačov postupne ku súčasným rozvodom, pokiaľ nebude vybudovaná hlavná optická kruhová topológia.

6.2.2 Návrh hlavného optického rozvodu

Druhým krokom návrhu je určenie optických trás hlavného kruhového rozvodu.

Návrh hlavného kruhového optického rozvodu vyplýva z požiadavky na topologickú redundanciu zapojenia, prenosové vlastnosti a elektromagnetickú odolnosť proti rušeniu. Z toho vyplýva jednoduchšia a menej nákladná montáž. Vedenie je možné uložiť do súčasných trás napájacích rozvodov bez nutnosti riešenia elektromagnetickej kompatibility. Kvôli zabráneniu mechanického poškodenia vedenia je nutné vo výrobných halách umiestniť optické vedenie do pevných (kovových) chráničiek.



Obr. 6.3: Prepojenie hlavných rozvodných uzlov

Z požiadavkov investora na budovanie po etapách, zároveň bez vplyvu na súčasnú infraštruktúru vyplýva:

- Kruhová topológia sa skladá z piatich uzlových bodov
- Pri postupnom pripojovaní uzlových bodov (realizácia po etapách) je potrebné pripojiť štyri segmenty - dočasne topológia hviezda
- Výpočet počtu potrebných vlákien pre hlavný rozvod
- Výber vhodného optického vedenia
- Maximálna predpokladaná dĺžka segmentu do 300 m

Hlavný kruhový optický rozvod bol navrhnutý, kvôli prenosovým vlastnostiam a dlžke vedia do 300 m, v prevedí minimálne OM2. Pre rekonštrukciu po etapách bolo stanovené 12 optických vlákien. Pre každý segment 2 vlákna. Ďalšie 4 vlákna sú navrhnuté ako redundantné. Konkrétne ide o typ FO MM 12x50/125 OM2.

Ukončenie optických vlákien je v administratívnej časti v 19“ optických vaniach na konektoroch SC a v uzlových bodoch priemyselnej časti, v modulárnych priemyselných optických rozvádzačoch na konektoroch SC.

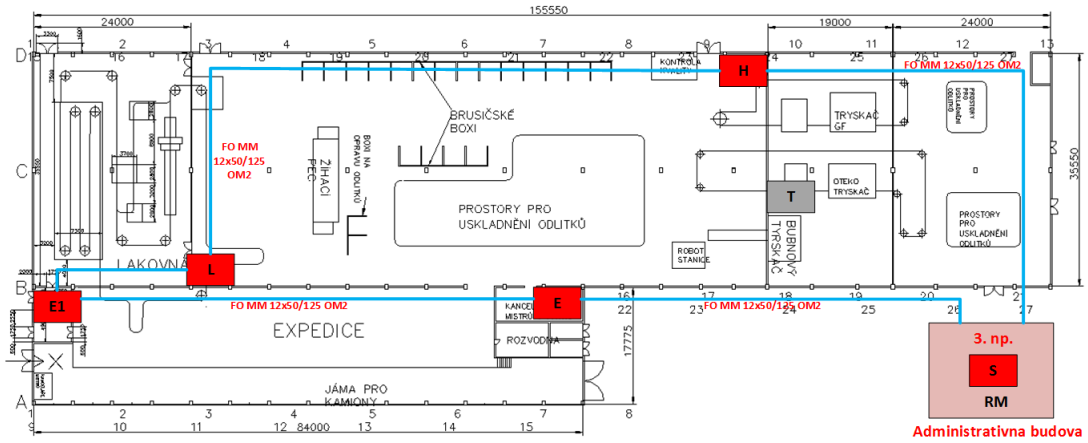
6.2.3 Určenie vedľajších uzlov

Z požiadavkov investora a momentálneho stavu zlievarne bol navrhnutý jeden podružný rozvádzač s označením T, ktorý bude slúžiť na pripojenie wi-fi zariadení a priemyselných strojov.

Požiadavky na podružný dátový rozvádzač:

- Metalické rozvody pre pripojenie zariadení
- Priemyselný záložný zdroj UPS
- Optický modulárny rozvádzač
- Aktívny prvok PoE pre pripojenie Wi-Fi
- Napájací zdroj pre aktívny prvok PoE 48 V DC

Podružný rozvádzač T, je situovaný v miestnosti, kde sa nachádzajú tryskacie zariadenia. Rozhodnutie umiestnenia tohto rozvádzača plynie z pohľadu felxibility zapojenia sieťovej infraštruktúry a budúcej plánovanej rozšíriteľnosti prevádzky, ktorú investor plánuje.



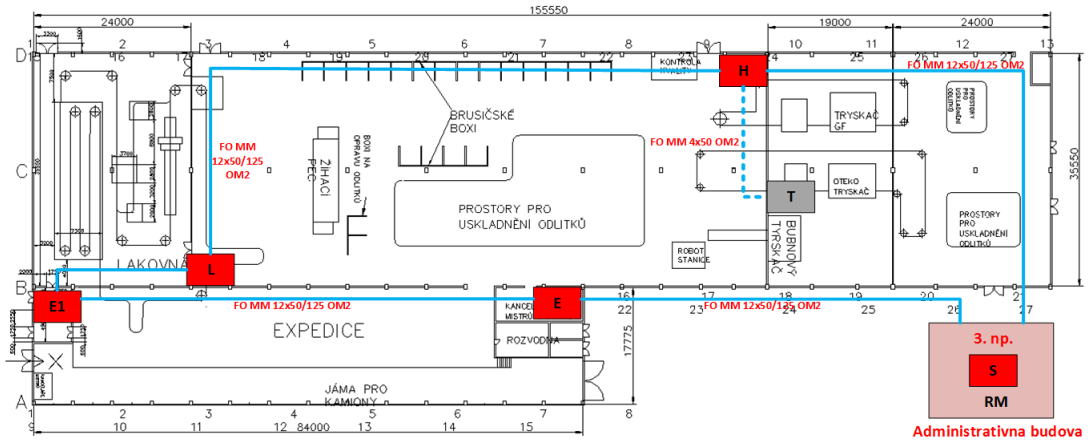
Obr. 6.4: Umiestnenie podružného uzlu T.

Podružné body sú realizované malými priemyselnými rozvádzačmi uzatvoreného typu s montážnou prípravou pre aktívne prvky určené pre montáž na DIN lištu. Konštrukcia vedľajšieho bodu je prispôsobená aktívnym prvkom, ktoré budú v ňom umiestnené (DIN lišta). Vo vedľajších bodoch sa počíta s umiestnením napájacieho zdroja 24/48 V DC pre lokálne potreby, ale aj potreby napájania aktívnych prvkov v prípojných bodoch (Wi-fi).

6.2.4 Návrh prepojenia vedľajších uzlov

Ďalším krokom návrhu je prepojenie podružného rozvádzača s hlavným kruhovým rozvodom.

Taktiež pripojenie podružných dátových rozvádzačov je realizované optickým vedením. Tento návrh riešešnia plynie z požiadaviek na priemyselné prostredie a taktiež optimalizácie elektromagnetickej kompatibility vedenia. Z pohladu elektromagnetickej kompatibility je možné vedenie uložiť do súčasných trás napájacích rozvodov, čo zníži náklady na rekonštrukciu sieťovej infraštruktúry.



Obr. 6.5: Pripojenie podružného uzlu T.

Návrh pripojenia podružného rozvádzača je realizovaný pre pripojenie k hlavnému rozvádzaciemu bodu H, v hlavnej hale zlievarne. Ak by táto varianta nebola možná vo finálnej rekonštrukcii, flexibilita návrhu umožňuje pripojiť podružný rozvádzač na iný hlavný bod kruhovej topológie (napr. rozvádzač E).

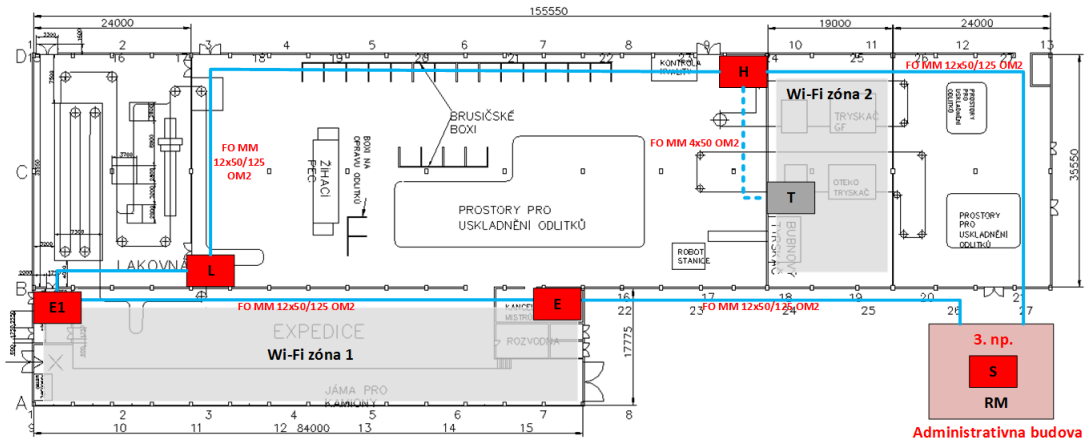
Optické pripojenie konkrétne podružného rozvádzača T, je realizované štyrmi optickými vláknami. Dve vlákna slúžia pre pripojenie aktívneho prvku v podružnom rozvádzači, ďalšie dve sú realizované ako redundancia vedenia.

Pripojovacie vedenie nebude presahovať vzdialenosť 300 m, preto bolo navrhnuté vedenie typu MM 4x50/125 OM2, ktoré bude ukončené v optických modulárnych rozvádzačoch, ktoré zabezpečujú optickú konektivitu medzi aktívnymi prvkami.

Kvôli zabráneniu mechanického poškodenia vedenia je nutné vo výrobných halách umiestniť optické vedenie do pevných (kovových) chráničiek.

6.2.5 Návrh pokrytia Wi-fi

Požiadavkom investora je wi-fi komunikácia v hale pre expedíciu a v hale kde sa nachádzajú tryskacie linky. Prioritou investora je realizácia infraštruktúry pre expedíciu. Je nutné urobiť vhodný návrh wi-fi pokrytia pre bezdrôtovú komunikáciu vysokozdvižných vozíkov a obsluhu s databázou uskladnených výrobkov.



Obr. 6.6: Určenie Wi-fi zón

Vo finálnej realizácii je nutné brať do úvahy kanálové riešenie wi-fi prípojných bodov a taktiež nastaviť vyžarovací výkon pre priechodnosť signálu.

6.2.6 Rozmiestnenie Wi-fi bodov

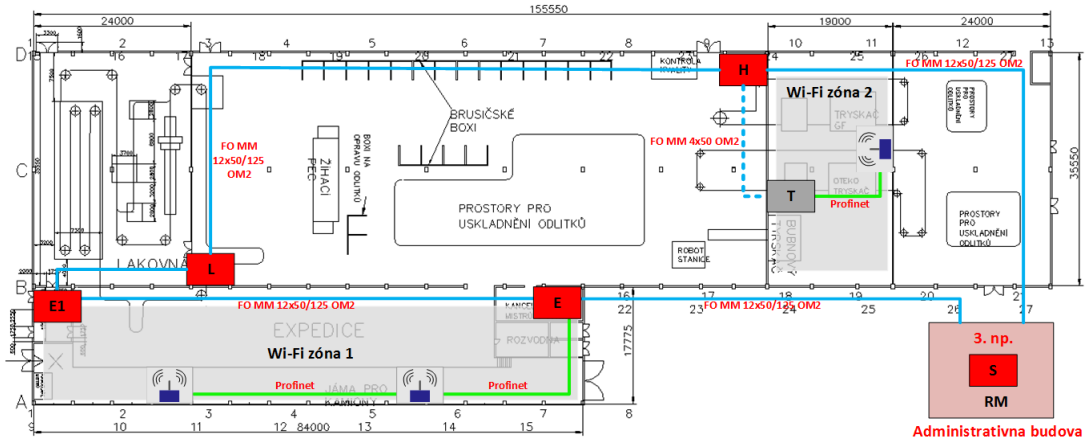
Je prioritne požadované riešenie odolnej bezdrôtovej technológie pre ťažkú priemyselnú prevádzku. Boli navrhnuté zariadenia typu AP, ktoré sú pripojené na hlavný aktívny prvok a bezdrôtový klienti pre zvlášť ťažké priemyselné podmienky prevádzky.

Požiadavky na wi-fi zariadenia ICS siete:

- Odolné priemyselné prevedenie
- Napájanie cez PoE
- Metalická linka s dostatočným prierezom (úbytky napájacieho napätia)
- Napojenie na spádové dátové rozvádzače odolnou metalickou linkou
- Uloženie metalického káblu v prostredí výrobných hál do pevnej (kovovej) chráničky.

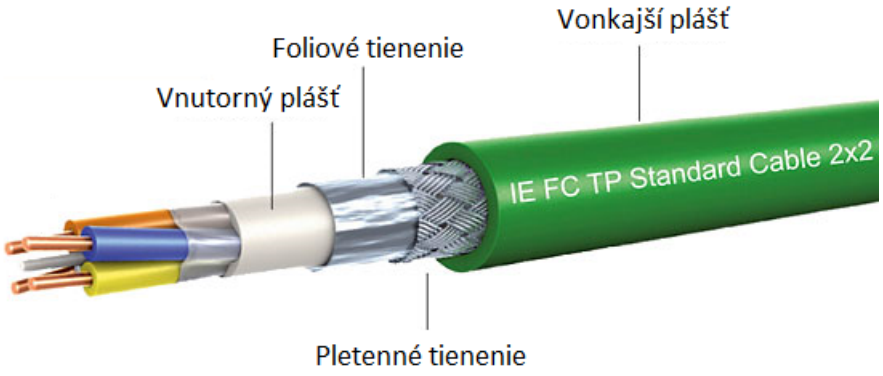
Pripojenie wi-fi zariadení v hale expedície je realizované na hlavný rozvádzací uzol. Pre pokrytie druhej wi-fi zóny je zariadenie pripájané na podružný rozvodný uzol.

Napájanie prístupových wi-fi bodov je realizované centrálne pomocou PoE technológie, z napájacieho priemyselného zdroja AC24/DC48 umiestneného v hlavnom alebo podružnom rozvádzači.



Obr. 6.7: Pripojenie Wi-fi zariadení

Pre splnenie požiadavkov, pripojenie wi-fi zariadení je nutné realizovať odolným metalickým vedením. Pre toto riešenie bolo vybrané metalické štandardizované vedenie typu Profinet. Toto riešenie vyhovuje požiadavkám, je navrhnuté do ťažkých priemyselných podmienok a obsahuje dvojité tienenie proti elektromagnetickému rušeniu.



Obr. 6.8: Príklad Profinet vedenia[2]

6.3 Technologické riešenie

V tejto kapitole sa práca venuje výberu a špecifikácii hlavných a podružných navrhnutých dátových rozvádzačov.

6.3.1 Administratívna časť

V administratívnej budove na treťom poschodí je umiestnená serverovňa, v ktorej sú realizované dátové rozvádzače pre aktívne prvky, slúžiace na ukončenie hlavnej kruhovej optickej trasy.

Prevedenie dátových rozvádzačov je navrhnuté pre umiestnenie 19“ aktívnych prvkov. Z pohľadu flexibility a rozšíriteľnosti bol navrhnutý dvojitý otvorený 19“ rám zobrazený na obrázku 6.9. Hlavnou výhodu tohto riešenia je veľmi dobrý odvod stratového tepla aktívnych prvkov v ňom umiestnených, zároveň veľmi dobrá prístupnosť z pohľadu servisu a zapojenia zariadení.

Obr. 6.9: Otvorený 19“ rám[2]

V prvej etape rekonštrukcie sieťovej infraštruktúry bude namontovaný iba jeden 19“ rám a osadený potrebnými aktívnymi prvkami.

6.3.2 Výrobná časť

Výrobná časť úzko súvisí z výrobou a platí pre ňu definícia priemyselného prostredia, pretože sa jedná o ťažké výrobné procesy kde pôsobia nepriaznivé podmienky ako napríklad agresívne prašné prostredie, vlhkosť alebo mechanické otrasy.

Konštrukcia hlavných uzlových rozvádzačov výrobnej časti je typizovaná pre celý výrobný celok. Tieto dátové rozvádzače sú navrhnuté tak aby bolo možné ich realizovať po etapách a podla priorít a potrieb investora. Jedná sa o modulárny prvok, do ktorého je možné umiestniť aktívne prvky v 19“ prevedení. Taktiež je možné umiestniť aktívne prvky s konštrukciou na prichytenie o DIN lištu (napájací zdroj).

Obr. 6.10: Príklad hlavného uzlový rozvádzača[2]

Konštrukcia podružných uzlových rozvádzačov je navrhnutá pre montáž aktívnych prvkov na DIN lištu. Taktiež sa v týchto bodoch počíta s umiestnením napájacieho zdroja 24/48V DC pre lokálne potreby, ale zároveň aj pre napájanie aktívnych prvkov umiestnených v prípojných bodoch (Wi-fi).

Obr. 6.11: Príklad podružného rozvádzača[2]

Prvky pre bezdrôtové Wi-fi technológie sú navrhnuté na inštaláciu do malých plastových prípojných rozvádzačov pripojených pomocou metalických káblov.

Obr. 6.12: Príklad prípojného bodu[2]

6.4 Špecifikácia prvkov infraštruktúry

Táto kapitola sa venuje porovnaniu a výberu prvkov, ktoré budú použité vo finálnom návrhu rekonštrukcie sieťovej infraštruktúry zlievarne.

6.4.1 Všeobecné kritéria výberu

- Výber jednotnej platformy aktívnych prvkov
- Všetky prvky musia podporovať spoločný dohľadový systém
- Typizácia priemyselných 19 palcových aktívnych prvkov v hlavnom rozvode
- Typizácia priemyselných DIN aktívnych prvkov pre prípojné miesta
- Odolné priemyselné riešenie bezdrôtových technológií
- Podpora redundantnej kruhovej topológie
- Podpora priemyselných redundantných protokolov

6.4.2 Aktívne prvky optického rozvodu

Výber aktívnych prvkov optického rozvodu bol uskutočnený na základe stanovených požiadaviek:

- L2 prepínače GE
- Priemyselné prevedenie, montáž do 19 palcových rozvodných skríň

- Bez ventilátorové prevedenie
- Modulárna konštrukcia
- Zásuvné moduly pre metalické a optické segmenty
- Redundantné napájanie
- Podpora kruhových topológii RM a SRM
- Podpora redundantných priemyselných protokolov MRP, Hiper-Ring, MSTP
- Kompatibilita s dohľadovým softvérom

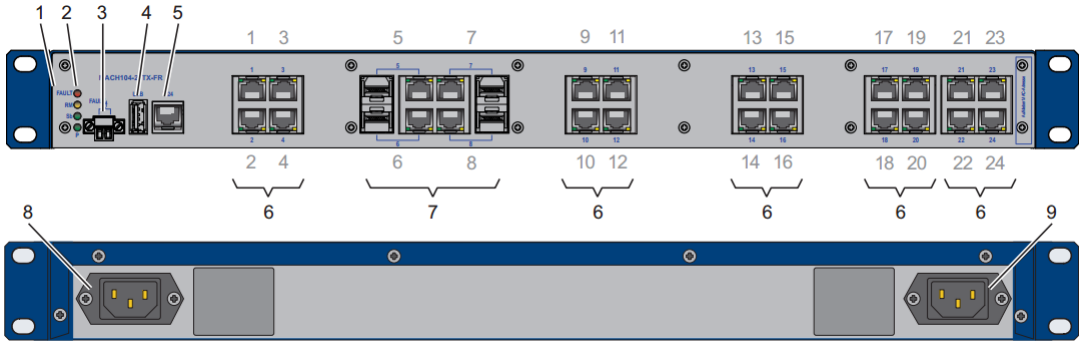
Špecifikácia aktívnych prvkov pre hlavný kruhový rozvod bola urobená z produktov známych výrobcov. Boli porovnávané prepínače z produktovej škály, ktorá vyhovuje stanoveným požiadavkám.

Tab. 6.1: Porovnanie priemyselných prepínačov rôznych výrobcov

Výrobca - typ	10/100/1000 BASE-TX port	100/1000 BASE-FX port	Podpora Hiper-Ring	Podpora MRP	Podpora MSTP	Bez ventilátorové prevedenie	Redundantné napájanie	Dohľadový systém	Montáž 19“	Cena (€)
Belden MACH104-20TX-FR	20	4	x	x	x	x	x	x	x	3000
Cisco IE-4010	24	4	x	x	x	x	x	x	x	4800
Siemens SCALANCE XR-30	16	8		x	x	x	x	x	x	3400
Comtrol ES9528	20	4		x	x		x	x	x	1200
Moxa IKS-G6524A	20	4	x		x	x	x	x	x	3500
Redlion EL326-AA-1	20	4		x	x	x		x	x	4100
Schneider TCSESM083	6	2			x	x		x		2500

Z porovnania aktívnych prvkov (tabuľka 6.1) vyplýva, že viaceré požadované podmienky spĺňajú zariadenia od výrobcov Cisco a Belden. Pre konkrétny návrh zlievarne boli vybraté zariadenia od výrobcu Belden, z dôvodu splnenia požiadaviek, veľkej škále produktov, cene a asociácie zlievarne s nemeckými výrobcami. Taktiež mnoho výrobcov priemyselných sieťových prvkov ako napríklad Honeywell alebo ABB, vyrába sieťové aktívne prvky na platforme firmy Belden.

Konkrétne bol vybraný prepínač z rady MACH typu MACH104-20TX-FR. Parametrami spĺňa všetky stanovené požiadavky. Taktiež toto riešenie je dostatočne modulárne pre budúce rozšírenia infraštruktúry.



Obr. 6.13: MACH104-20TX-FR[2]

1. MACH104-20TX-FR
2. LED signalizácia
3. Signálové kontakty
4. USB
5. V.24 pripojenie - manažment
6. RJ45, 10/100/1000 BASE-TX porty
7. 100/1000 Mbit/s F/O, SFP sloty
8. Napájanie
9. Redundantné napájanie

Konštrukcia prepínača je zhotovená na umiestnenie do 19“ rámov. Tento prepínač obsahuje dvadsať portov podporujúcich technológiu 10/100/1000Base-TX, štyri kombinované optické porty s podporou 100/1000 BASE-FX technológie. Poskytuje možnosť redundantného napájania z dvoch oddelených sietí. Taktiež podporuje dohľadový systém výrobcu.

6.4.3 Aktívne prvky prípojných bodov rozvodu

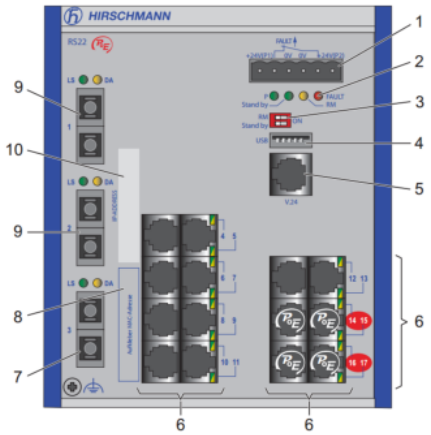
Aktívne prvky prípojných bodov budú situované v podružných rozvádzačoch alebo v niektorých rozvádzačoch hlavného optického rozvodu. Budú plniť úlohu prípojného komunikačného bodu pre konkrétne technológie ako napríklad napájanie a komunikácia s jednotlivými wi-fi prvkami.

Výber aktívnych prvkov prípojných bodov rozvodu bol uskutočnený na základe stanovených požiadaviek:

- L2 prepínač
- Priemyselné prevedenie, montáž na DIN lištu
- Bez ventilátorové prevedenie
- Modulárna konštrukcia
- Optické porty
- Podpora PoE
- Podpora kruhových topológii RM a SRM
- Podpora redundantných priemyselných protokolov MRP, HiperRing, MSTP
- Kompatibilita s dohľadovým softvérom

Aktívne prvky boli vyberané z produktovej rady firmy Belden - Hirschmann čo vyplýva z podmienky jednotnej platformy všetkých produktov a výberu výrobcu v predchádzajúcom bode.

Vyšpecifikovaný bol prepínač z rady RS22, ktorý má všetky vyžadované vlastnosti. Je to plne nastaviteľný prepínač s konštrukciou umožňujúcu montáž na DIN lištu. Obsahuje štrnásť portov podporujúcich technológiu 10/100Base-TX, z toho štyri porty s podporou PoE a tri optické porty 100Base-FX. Taktiež je kompatibilný s dohľadovým softvérom výrobcu.



1. Signálové kontakty
2. LED signalizácia
3. Konfiguračný prepínač
4. USB
5. V.24 pripojenie - manažment
6. RJ45, 10/100 BASE-TX porty
7. SC, 100 BASE-FX porty
8. MAC adresa
9. SC, 100 BASE-FX porty
10. Popisné pole

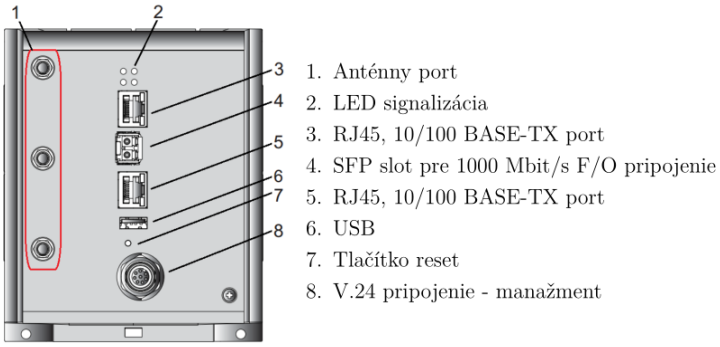
Obr. 6.14: Prepínač rady RS22[2]

6.4.4 Aktívne prvky bezdrôtovej technológie Wi-fi

Výber bezdrôtových prvkov rozvodu bol uskutočnený na základe stanovených požiadaviek:

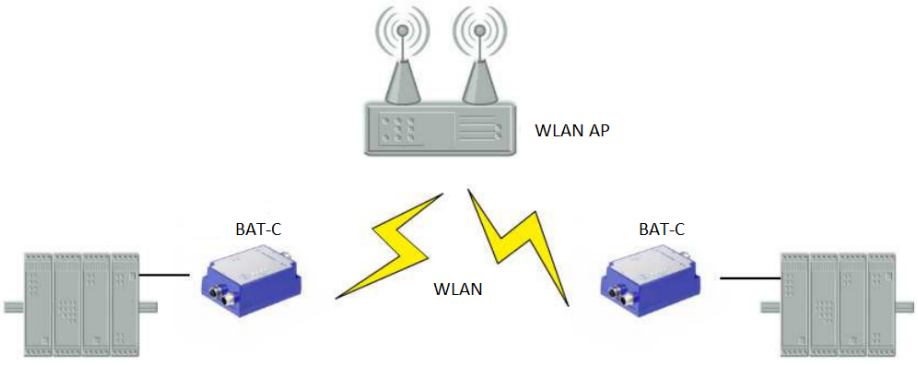
- Bezdrôtové AP
- Priemyselné prevedenie
- Bezdrôtový klient
- Clear Space technológia

Ako prístupový bod bolo vybraté wi-fi zariadenie typu BAT-R od firmy Hirschmann podporujúce štandard IEEE 802.11a/b/g/h/n. Podporuje 2,4 GHz a 5 GHz frekvenčné pásma a umožňuje komunikáciu Profinet, EtherNet/IP protokolov. Využíva technológiu Clear Space, ktorá spoľahlivo eliminuje konkurenčné rádiové frekvencie čo zaručí stabilné pripojenie k WLAN po celý čas.



Obr. 6.15: Wi-fi prvok rady BAT-R[2]

Pre bezdrôtovú komunikáciu výrobných liniek bol vybraný bezdrôtový wi-fi klient typu BAT-C.



Obr. 6.16: Wi-fi klient rady BAT-C[2]

6.4.5 Pasívne prvky infraštruktúry

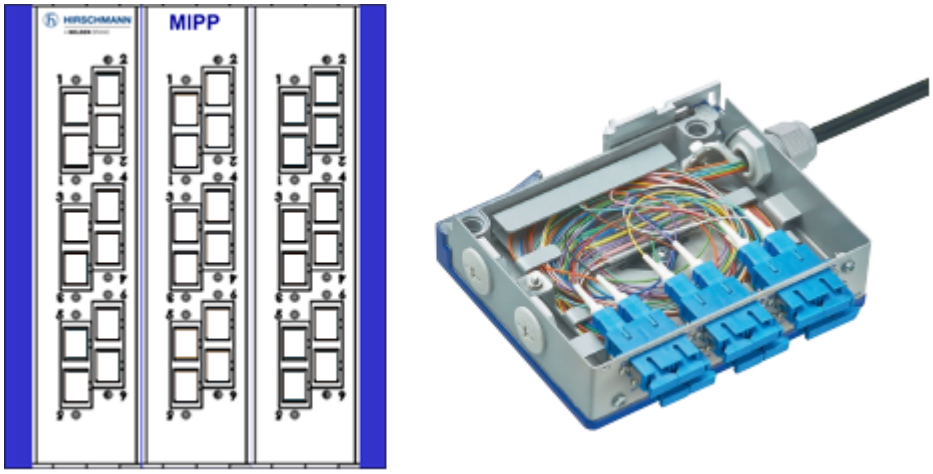
Pasívnymi prvkami infraštruktúry sú myslené všetky prvky, ktoré sa nepodieľajú aktívne na prenose informácií sieťou. Sú to napríklad všetky optické rozvody, metalické rozvody, konektory a modulárne prepojovacie jednotky.

Pre metalické rozvody bolo vyšpecifikované vedenie typu Profinet pre pripojenie wi-fi prípojných bodov a FTP tienené káble pre ostatné prepojenia prvkov čo vyplýva z požiadavok na priemyselné prostredie.

Pre optické rozvody, ako už bolo popísané v kapitole topologické riešenie, boli vybraté dva typy optických vlákien s konektormi typu SC:

- FO MM 12x50/125 OM2 - 1Gb/s
- FO MM 4x50/125 OM2 - 100Mb/s

Vzhľadom na požiadavku rekonštrukcie po etapách bolo nutné použiť prepojovacie optické jednotky, takzvaný patch panel. Firma Hirschmann ponúka tieto jednotky typu MIPP v modulárnom riešení.



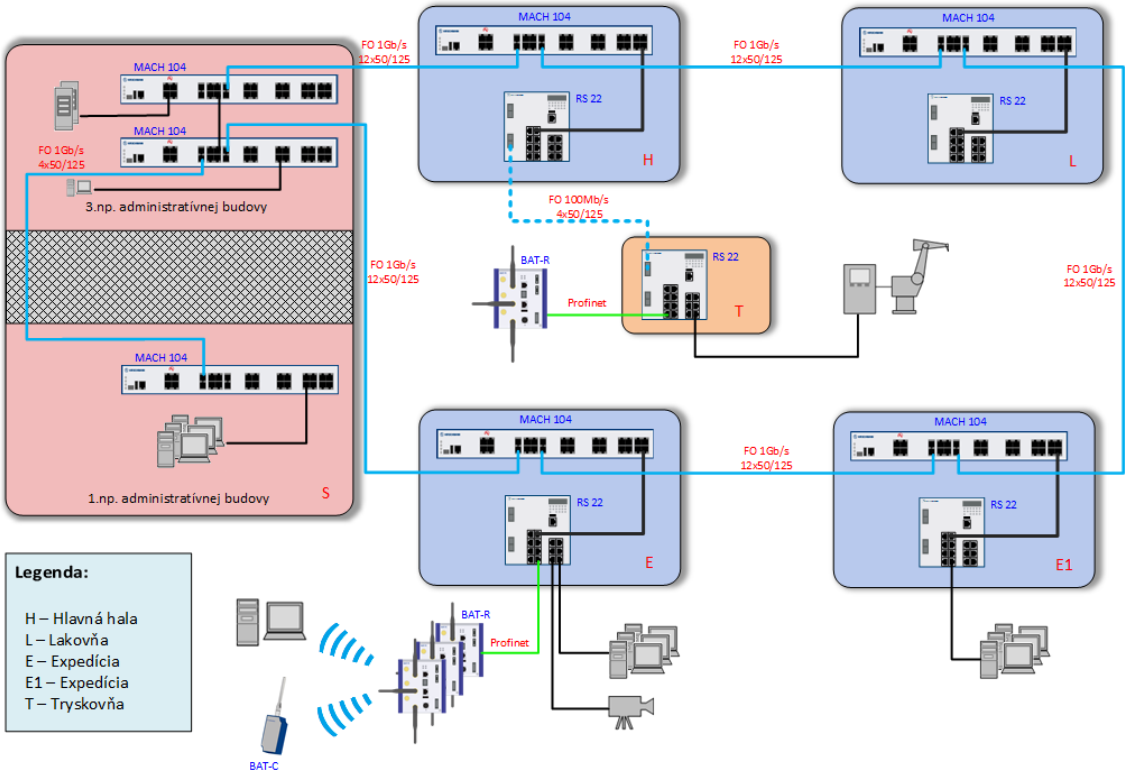
Obr. 6.17: Patch panel MIPP[2]

Modulárny patch panel MIPP je všestranne robustné zakončenie optických vlákien, ktoré sú potrebné prepojiť z priemyselného prostredia na aktívny prvok. Ich prevedenie zodpovedá ľahkej inštalácii na DIN lištu. MIPP má veľkú hustou portov pre splnenie budúceho rozšírenia sieťového pripojenia. Jeden modul obsahuje šesť duplexných SC pripojení.

V rozvádzačoch v hlavnej optickej vetve budú použité tri modulárne prepojovacie jednotky. Dve budú slúžiť na prepojenie hlavnej vetvy s prepínačom MACH104 a jedna jednotka pre prepojenie podružných uzlov.

6.5 Finálny návrh infraštruktúry

Táto kapitola sa zaoberá finálnym návrhom infraštruktúry zlievarne. Popisuje finálne zapojenie vyšpecifikovaných prvkov, zobrazuje umiestnenie rozvádzačov a konečnú realizáciu v zlievarni.



Obr. 6.18: Bloková schéma zapojenia - osadenie aktívnych prvkov

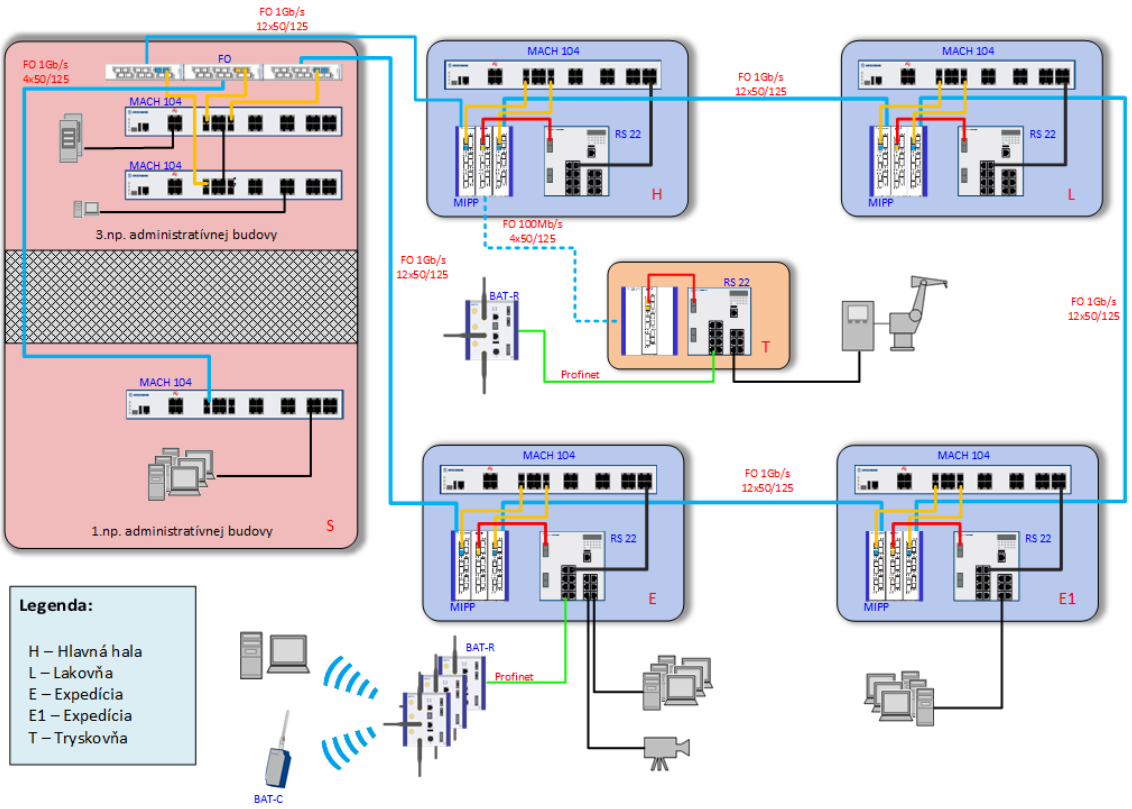
Bloková schéma (obrázok 6.18) zobrazuje finálne zapojenie aktívnych prvkov v administratívnej a výrobnej časti zlievarne. V administratívnej časti zlievarne na treťom poschodí budovy boli navrhnuté dva prepínače typu MACH104 pre ukončenie hlavného kruhového optického rozvodu pre výrobnú časť a pripojenie administratívnych kancelárií. Tento rozvod administratívnej časti sa vetví na prvé poschodie s ukončením v prepínači typu MACH104.

Optický kruhový rozvod výrobnej časti obsahuje štyri rozvodné uzly, tvorené prepínačmi MACH104 s podružnými prepínačmi RS22 s podporou PoE. Návrh uzlov s prepínačmi typu RS22 plynie z požiadavky na flexibilnosť, budúce rozšírenie sieťovej topológie a pripojenie prípojných wi-fi bodov.

Bol navrhnutý jeden podružný rozvádzač T, v hale kde sa nachádzajú tryskacie linky, pre pripojenie wi-fi prípojného bodu a pripojenie výrobných liniek. Infraštruktúra je plne modulárna čo znamená možnosť rozšírenia o podružné body

z akéhokoľvek rozvodného bodu hlavnej kruhovej vetvy.

Prepojenie hlavnej kruhovej topológie je riešené optickým vedením typu OM2 zakončeným SC konektormi v modulárnych pach paneloch MIPP viď obrázok 6.19.



Obr. 6.19: Plnohodnotná bloková schéma zapojenia

Je doporučené redundantné napájanie aktívnych prvkov topológie, ale konečný výber záleží na investorovi. To vyplýva z požiadaviek tejto práce na sieťovú infraštruktúru ICS, z čoho plynie, že práca nerieši konečný návrh elektroinštalácie zlievarne.

Celý návrh sieťovej topológie zlievarne vychádza z teórie popísanej v tejto práci.

6.5.1 Konečná realizácia infraštruktúry

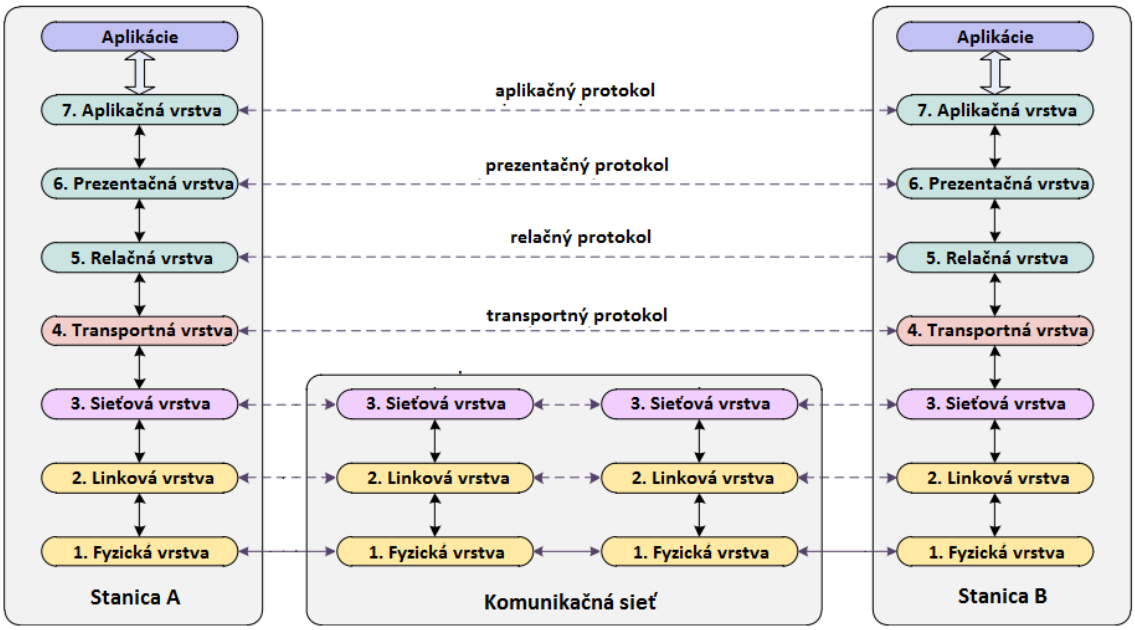
Následne podla vypracovaných návrhov bola uskutočnená rekonštrukcia sieťovej infraštruktúry zlievarne. Finálny návrh bol v praxi minimálne pozmenený. Návrh je veľmi flexibilný a modulárny a záleží na investorovi aký koncept zvolí. Celková fotodokumentácia realizovaných rozvádzačov je umiestnená v prílohách tejto práce.

6.6 Logické riešenie

Logické riešenie siete vychádza z niekoľkých rozdielnych prevádzok prebiehajúcich súčasne na sieťovej infraštruktúre:

- Administratívna časť
- Dohliadacia prevádzka výrobnej časti
- Komunikácia riadenia PLC
- Kamerový systém

Základným princípom logického riešenia siete je logické oddelenie týchto prevádzok. Oddelenie je možné realizovať na prvých troch vrstvách sieťového modelu ISO/OSI.



Obr. 6.20: Referenčný model ISO/OSI

6.6.1 Fyzická vrstva

Oddelenie na fyzickej vrstve plynie z vyhradenia konkrétnych fyzických portov istým aplikáciam.

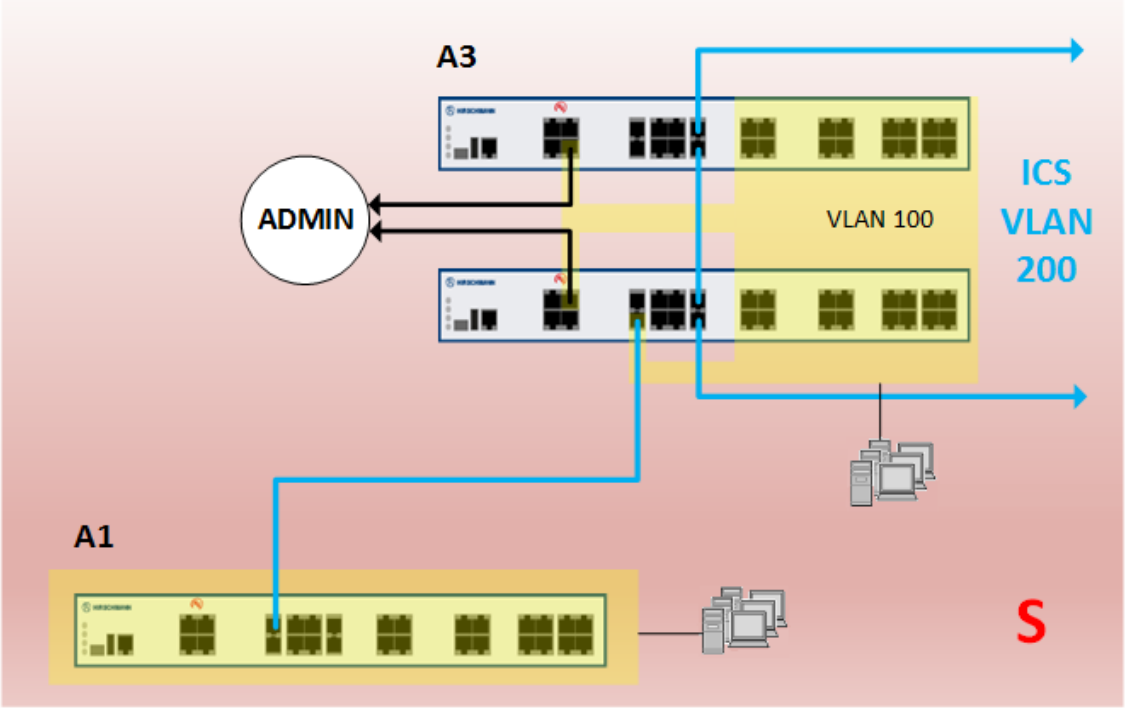
Oddelenie je doporučované hlavne pre kamerový systém. Prístup do siete kamerového systému bude zabezpečený cez vyhradený port na stanovenom zariadení.

6.6.2 Linková vrstva

Oddelením na linkovej vrstve je možné sieť rozdeliť na viacero virtuálnych sietí VLAN. Virtuálne siete sú definované ako domény broadcastového vysielania s cieľom zabezpečiť logickú organizáciu siete nezávislú na fyzickej konektivite. Toto riešenie zabezpečí ľahšiu správu, zvýši výkon a podporí bezpečnosť siete.

Pre vybrané aktívne prvky je možné jednotlivo priradiť každý port do určitej VLAN siete. Logicky bude sieť rozdelená na tri VLAN siete:

- VLAN 1 - Manažment siete
- VLAN 100 - Administratívna časť
- VLAN 200 - Výrobná časť



Obr. 6.21: Príklad rozdelenia portov do VLAN

6.6.3 Sieťová vrstva

Oddelením na sieťovej vrstve je možné sieť rozdeliť na viacero sietí LAN pomocou aktívneho prvku typu smerovač. Týmto riešením je možné sieť rozdeliť na viaceré časti, ktoré budú používať rozdielne adresné celky. Aktívny prvok smerovač zabezpečuje perifernú bránu siete a smerovanie paketov v sieti. Pomocou smerovača je

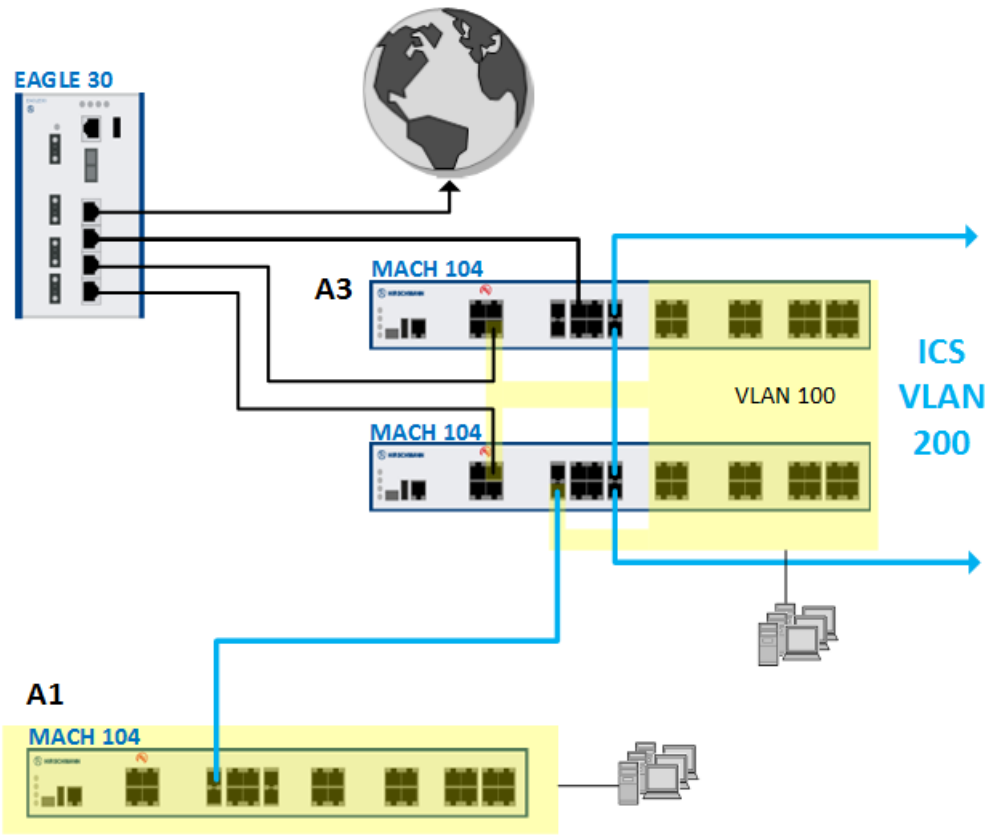
možné splniť požiadavky investora. Rozdeliť sieť na dva adresné priestory, čo znamená konfiguráciu dvoch DHCP serverov.

Požiadavky na oddelenie adresných priestorov s vlastným DHCP serverom:

- LAN Admin
- LAN ICS

Pre splnenie požiadaviek bol vybratý centrálny smerovač kombinovaný s firewallom, čo znamená plné zabezpečenie siete s vonkajším svetom.

Konkrétne bol vybraný smerovač typu EAGLE 30 od firmy Hirschmann. Je to priemyselný zabezpečený smerovač s firewallom obsahujúci štyri 10/100BASE TX porty, dva 100/1000 BASE TX porty a dva SFP sloty pre optické pripojenie. Disponuje množstvom podporovaných protokolov a taktiež protokolom VRRP pre redundantné smerovanie siete. Samozrejme umožňuje možnosť redundantného napájania.



Obr. 6.22: Rozdelenie siete pomocou prvku L3

Na obrázku 6.22 je možné vidieť pripojenie siete zlievarne na vonkajšiu sieť Internet, pomocou smerovača EAGLE 30. Pripojenie na porty prepínačov značí rozdelenie siete na dva adresné nezávislé celky.

6.7 Jednotná správa riešenia

Pod jednotnou správou riešenia je myslený dohliadací nástroj, ktorý bude monitorovať a spravovať celú podnikovú sieť. Hlavnou požiadavkou na dohliadací nástroj je jednoduchosť a robustnosť softvéru odpovedajúcemu priemyselnému riešeniu.

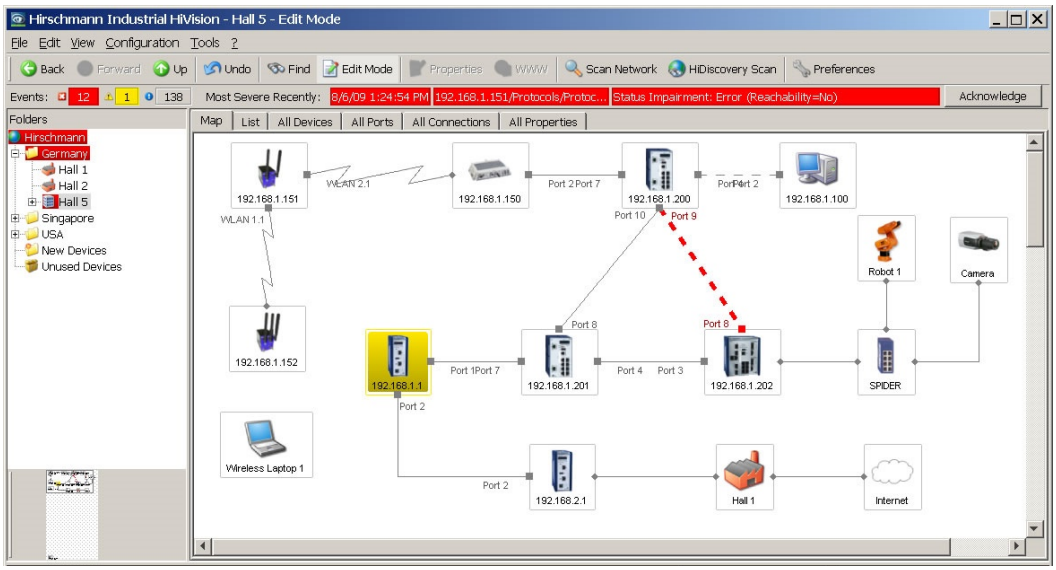
Základom je diagnostika redundantnej priemyselnej sieťovej infraštruktúry. Súčasťou monitorovacieho systému siete je:

- Konfigurácia zariadení
- Monitorovanie výkonnosti zariadení
- Monitorovanie chybovosti zariadení
- Monitorovanie bezpečnosti
- Monitorovanie udalostí v sieťovej infraštruktúre

6.7.1 HiVision

Grafický softvér pre správu a sledovanie priemyselných sietí od výrobcu Hirschmann. Umožňuje konfiguráciu a zobrazenie stavu všetkých zariadení siete ako napríklad smerovače, prepínače, WLAN zariadenia a koncové zariadenia, ktoré podporujú protokol SNMP.

Umožňuje konfiguráciu identických parametrov pre viac zariadení súčasne. Podporuje automatické rozpoznanie a vizualizáciu topológie siete. Zobrazuje celú hierarchiu siete. Rozpoznávanie topológie je založené na protokoloch LLDP (Link Layer Discovery Protocol).



Obr. 6.23: Príklad rozpoznania siete softvérom HiVision[2]

HiVision je schopný mapovať stav zariadení, správnosť pripojení a vlastnosti zariadení. Môže byť použitý v systémoch SCADA prostredníctvom rozhrania OPC Data Access alebo OPC UA. Taktiež grafické užívateľské rozhranie môže byť implementované do systému SCADA.

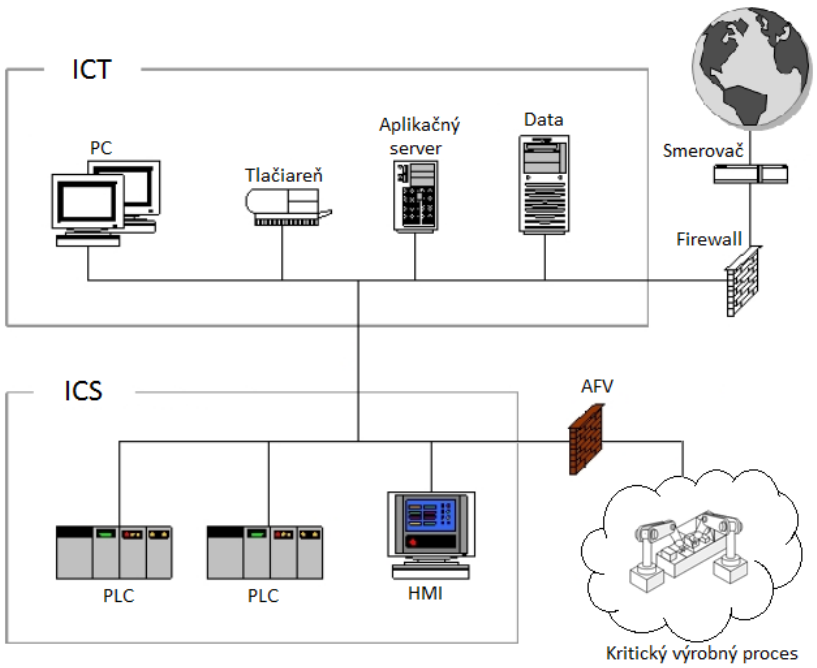
Správcovský program HiVision je plne škálovateľný a nastaviteľný pre ďalšie udalosti. Podporuje nastavenie mnoho alarmov a poplachových akcií ako napríklad zaslanie SMS alebo e-mailu.

Taktiež je možná vzdialená diagnostika pomocou aplikácie HiMobile App, ktorá je podporovaná všetkými operačnými systémami mobilných telefónov.

6.8 Bezpečnosť riešenia

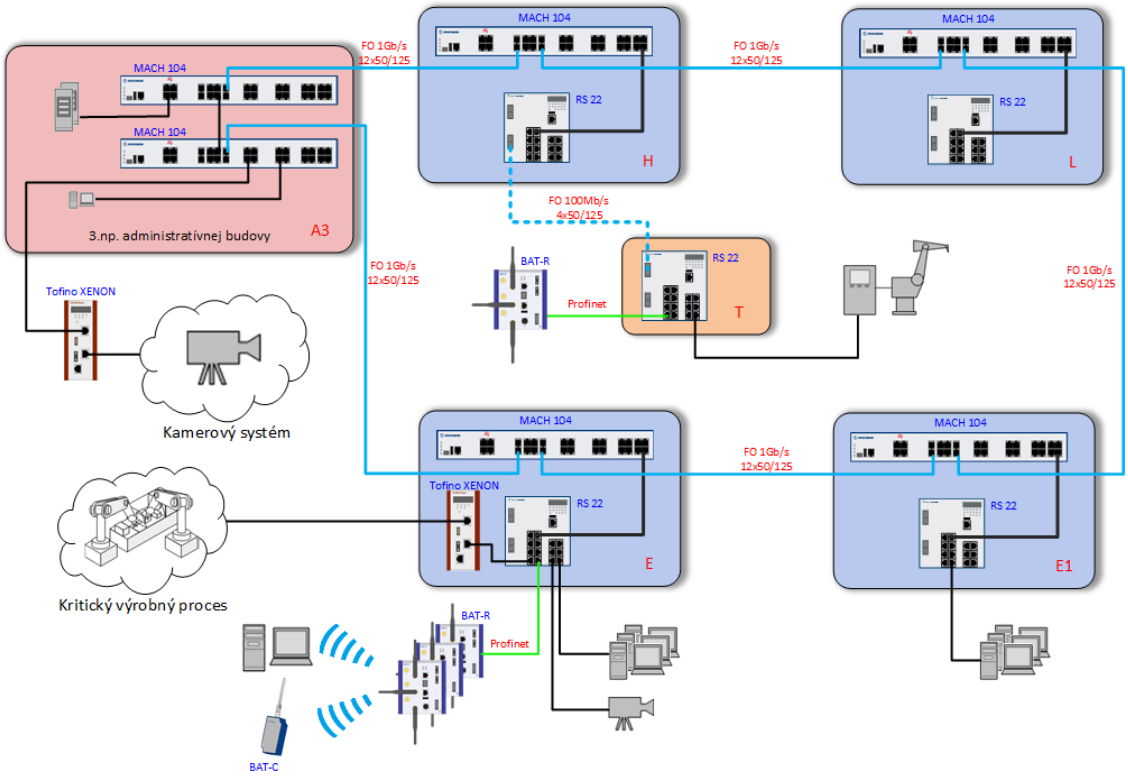
Kapitola sa nezaoberá zabezpečením proti poruchám, ktoré boli už v práci popísané ale zabezpečením infraštruktúry proti vonkajším útokom. Pred týmto typom útokov je možné sa chrániť sieťovými zariadeniami typu firewall.

Firewally sú sieťové zariadenia zabezpečujúcu sieťovú prevádzku medzi sieťami rôznych úrovní bezpečnosti. Takéto bezpečnostné riešenie je možné zvoliť na periférii siete so spojením s vonkajšou sieťou Internet, čo je riešené kombinovaným zabezpečeným smerovačom s firewalom (EAGLE 30), alebo na perifériách rozdielnych sieťových aplikácií ICS, takzvanými aplikačnými firewalmi AFW.



Obr. 6.24: Príklad využitia AFW firewalu[8]

Konkrétny návrh riešenia zlievarne odporúča použiť AFW firewall pre konkrétne kritické výrobné procesy a inštalovaný kamerový systém.



Obr. 6.25: Príklad využitia AFW firewalu v zlievarni

Výrobca Hirschmann ponúka aplikačný firewall typu Tofino Xenon. Je to priemyselný stavový fiwewall (SPI) s možnosťou hĺbkovej paketovej detekcie DPI. Disponuje s dvomi 100BASE-TX ethernetovými portami, redundantným napájaním a montážnym prevedením na DIN lištu.

Stavový firewall je schopný sledovať a udržovať všetky naviazané TCP/UDP relácie, čo znamená že pracuje na transportnej vrstve ISO/OSI modelu. Rozlišuje rôzne stavy paketov v rámci jednotlivých spojení a prepúšťa iba predom preddefinované povolené relácie. Napríklad pri kamerovom systéme, umožňuje iba spojenie blízko súvisiace s video prenosom, čo zabezpečuje bezpečnosť pred vonkajším útokom cez kamerový systém. Podobne je to pri zabezpečení kritických výrobných procesov. Týmto procesom firewall zabezpečí iba potrebnú komunikáciu súvisiacu s výrobným procesom.

6.9 Meranie realizovanej siete

Funkčnosť riešenia jednotlivých technologických celkov (Wifi, uzlové body, jednotlivé prepojenia) boli odskúšané najskôr laboratórne na testovacom polygóne, preverením overovacou rutinnou prevádzkou.

Vzhľadom k relatívne malým požiadavkám priemyselnej komunikácie na šírku prenosového pásma (10 Mbps), bola zvolená varianta návrhu s dostatočnou rezervou (1 Gbps pre hlavné uzlové prvky, 100 Mbps pre podružné prvky).

Vyťaženie hlavných trás siete zlievarne, v rutinnej prevádzke dosahuje približne 9 - 15 % navrhnutej šírky pásma, podla monitorovania infraštruktúry dohliadacím softvérom HiVision.

6.10 Náklady riešenia

Kapitola sa zaoberá koncovými celkovými nákladmi na realizáciu rekonštrukcie sieťovej infraštruktúry. Náklady na riešenie rekonštrukcie sieťovej priemyselnej infraštruktúry zahŕňajú viacero faktorov, ktoré sú uvedené nižšie.

6.10.1 Projektová príprava

Vypracováva dopredu stanovená spoločnosť, ktorá bude celý projekt zastrešovať.

- Štúdie uskutočniteľnosti
- Realizačný projekt

6.10.2 Inštalačné práce

Záleží na stave objektu v akom sa nachádza a kto bude stanovený na rekonštrukčné práce. Väčšinou sa jedná o rovnakú spoločnosť, ktorá vytvorila projekt rekonštrukcie.

- Realizácia ICS kabeláže
- Inštalácia aktívnych prvkov ICS
- Nastavenie infraštruktúry ICS

Celkové ceny jednotlivých prác sú väčšinou odvodené od celkových nákupných nákladov (NN).

- Inštalačné a montážne práce - 10% NN
- Inštalácia technológie - 40% NN

6.10.3 Komponenty ICS

Najväčšia čiastka nákladov rekonštrukcie. Tvoria ju všetky komponenty použité pre rekonštrukciu.

- Sieťové komponenty ICS kabeláže
- Aktívne prvky ICS
- Jednotný dohliadací softvér

Tab. 6.2: Rozpočet

Položka	Počet jednotiek	Cena za jednotku (€)	Cena (€)
MACH104-20TX-FR	7	2550	17850
RS22	5	2690	13450
BAT-R	3	1290	3870
BAT-C	2	520	1040
EAGLE20	1	1390	1390
Tofino Xenon	2	2980	5960
MIPP	5	1100	5500
HiVision	1	2850	2850
SFP modul	12	205	2460
Hlavný optický segment	1200 m	26,5	31800
Metalický segment	300 m	3,1	930
Dátový rozvádzač	5	1490	7450
Inštalačný materiál	1	1000	1000
Celkom NN			**95550**

7 ZÁVER

Na začiatku tejto práce bola zhrnutá teória, potrebná pre realizáciu finálneho návrhu sieťovej priemyselnej infraštruktúry. Bolo nutné pochopiť rozdiely medzi priemyselnou komunikáciou a komerčnými sieťami a prepojenia medzi nimi. Komplexné pochopenie problematiky je potrebné pre konečný návrh priemyselnej infraštruktúry v konkrétnom prostredí.

Boli popísané konkrétne komunikačné požiadavky, ktoré musí spĺňať priemyselná infraštruktúra ako napríklad, zodolnená fyzická vrstva prispôsobená do priemyselných podmienok, redundantné požiadavky siete alebo komunikačné štandardy a ich rozdiely od komerčných sietí. Taktiež bola uvedená problematika analýzy rizík a popis bezpečnostných hrozieb, ktoré môžu nastať. Následne práca popisuje teoretické bezpečnostné východiská, ktoré je možné realizovať pomocou firewallu.

Praktická časť diplomovej práce sa z skladá z časti kde je popísaný rozbor súčastného stavu konkrétneho prostredia zlievarne a časti, ktorá finálny návrh realizuje.

V analýze súčastného stavu infraštruktúry zlievarne, boli popísané časti zlievarne, topológia siete a prvky, ktoré sieť využíva. Zo získaných výsledkov boli vyvodené nedostatky infraštruktúry a konečný verdikt nevyhovujúceho stavu siete.

Samotný návrh sieťovej infraštruktúry mal niekoľko častí. Najskôr boli určené miesta kde sa budú nachádzať uzlové body redundantnej kruhovej topológie siete a kade budú vedené optické trasy. Boli stanovené štyri uzlové body nachádzajúce sa vo výrobnej časti zlievarne a jeden uzlový bod v administratívnej časti pre ukončenie optického rozvodu. Ďalej bol stanovený podružný rozvádzač v hale pre tryskacie linky. Následne z požiadavky investora na pokrytie vymedzenej oblasti Wi-fi signálom, boli stanovené vhodné miesta pre Wi-fi prípojné body. Optické prepojenie uzlových a podružných bodov siete bolo realizované optickými vláknami typu MM 50/125 OM2. Pre pripojenie Wi-fi prípojných bodov bolo vybraté metalické vedenie typu Profinet a to z dôvodu mechanickej pevnosti a elektromagnetickej kompatibility.

Po predchádzajúcich úkonoch boli vyšpecifikované pasívne a aktívne prvky siete. Všetky vyšpecifikované prvky boli vyberané podla kvality, požiadavkov na priemyselné riešenie a obecných požiadavkov investora. Boli vybrané prvky od výrobcu Hirshmann a to z dôvodu splnenia počiatočných podmienok investora, známej vysokej kvality a precíznej výroby prvkov a asociácie zlievarne s nemeckými výrobcami.

Kvôli bezpečnosti bolo nutné oddeliť administratívnu sieť od priemyselnej siete a zabezpečiť kritické výrobné procesy. Boli stanovené dva adresné priestory pre administratívnu časť a výrobnú časť. Následne sieť bola logicky rozdelená na dve virtuálne siete VLAN, čo zvyšuje bezpečnosť siete. Taktiež pre bezpečnosť celej infraštruktúry a konkrétnych kritických výrobných procesov boli použité firewally

alebo zónové firewally pre konkrétne procesy.

Celá sieťová infraštruktúra sa na záver zastrešila dohliadacím konfiguračným softvérom HiVision, ktorý bude celú sieť monitorovať a upozorňovať na vzniknuté výpadky a nedostatky.

Návrh sieťovej infraštruktúry bol zhodnotený v nákladoch riešenia, kde sú popísané jednotlivé komponenty s príslušnou cenou.

Záverom celého návrhu bola realizácia rekonštrukcie zlievarne a overenie funkčnosti návrhu v prevádzke. Vďaka novej infraštruktúre a návrhom zavedenia informačnej bezpečnosti, bola firme poskytnutá metodika pre zavedenie informačnej bezpečnosti a k jej následnej správe.

LITERATÚRA

[1] BÉLAI, I. *Komunikácia v priemyselnej automatizácii* [online]. 2007, [cit. 8. 11. 2016]. Dostupné z URL: <http://www.atpjournal.sk/buxus/docs/atp-2007-08-57.pdf>.

[2] BELDEN Inc. *Stránky produktov výrobcu Hirschmann* [online]. 2017, [cit. 3. 3. 2017]. Dostupné z URL: <http://www.hirschmann.com/en/Hirschmann_Produkte/index.phtml>.

[3] DIJEV, S. *Industrial Networks for Communication and Control* [online]. 2007, [cit. 8. 11. 2016]. Dostupné z URL: <http://anp.tu-sofia.bg/djiev/PDF%20files/Industrial%20Networks.pdf>.

[4] HAUGHN, M. *Industrial control system (ICS)* [online]. 2016, posledná aktualizácia 21. 3. 2016 [cit. 3. 12. 2016]. Dostupné z URL: <http://whatis.techtarget.com/definition/industrial-control-system-ICS>.

[5] KARBOVANEC, M. *Priemyselné systémy* [online]. 2013, [cit. 8. 11. 2016]. Dostupné z URL: <http://www.atpjournal.sk/rubriky/prehladove-clanky/priemyselne-systemy-potrebuju-dodatocnu-ochranu-pomocou.-bezpecnostnych-integrovanych-obvodov.html?page_id=16476>.

[6] MAREŠ, J. *Bezpečnost systémů ICS/SCADA* [online]. 2015, [cit. 8. 11. 2016]. Dostupné z URL: <https://www.systemonline.cz/clanky/bezpecnost-systemu-ics-scada.htm>.

[7] SOULLIÉ, A. *Industrial control system* [online]. 2015, [cit. 7. 11. 2016]. Dostupné z URL: <https://www.blackhat.com/docs/eu-14/materials/eu-14-Soullie-Industrial-Control-Systems-Pentesting-PLCs-101.pdf>.

[8] STOUFFER Keith, FALCO Joe, SCARFONE Karen.

Guide to Industrial Control Systems (ICS) Security [online]. 2011, [cit. 8. 11. 2016]. Dostupné z URL: <https://govcert.es/publico/InfraestructurasCriticaspublico/Guide%20to%20Industrial%20Control%20.pdf>.

[9] Wikipedia contributors, *Industrial control system* [online], Wikipédia: Otvorená encyklopédia, 2016, posledná aktualizácia 28. 11. 2016 [cit. 29. 11. 2016]. Dostupné z URL: <https://en.wikipedia.org/w/index.php?title=Industrial_control_system&oldid=751984473>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

AP	Access Point
CIP	Control and Information Protocol
DCS	Distribuovaný riadiaci systém – Distributed Control System
DMZ	Demilitarizovaná zóna – Demilitarized zone
DPI	Deep Packet Inspection
EMC	Electromagnetic Compatibility
FE	Fast Ethernet
GE	Gigabit Ethernet
HMI	Human–Machine Interface
ICS	Industrial control system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
NN	Nákupné Náklady
OM2	Optical Multimode 2
PoE	Power over Ethernet
PVC	Polyvinylchlorid
RM	Ring Manager
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection
SRM	Sub-Ring Manager
UPS	Uninterruptible Power Supply

ZOZNAM PRÍLOH

A OBSAH PRILOŽENÉHO CD

Priložené CD obsahuje tri priečinky diplomová práca, podklady a finálny návrh a fotodokumentácia.

A.1 Diplomová práca

Tento priečinok priloženého CD obsahuje celú diplomovu prácu v digitálnej podobe, vo formáte pdf.

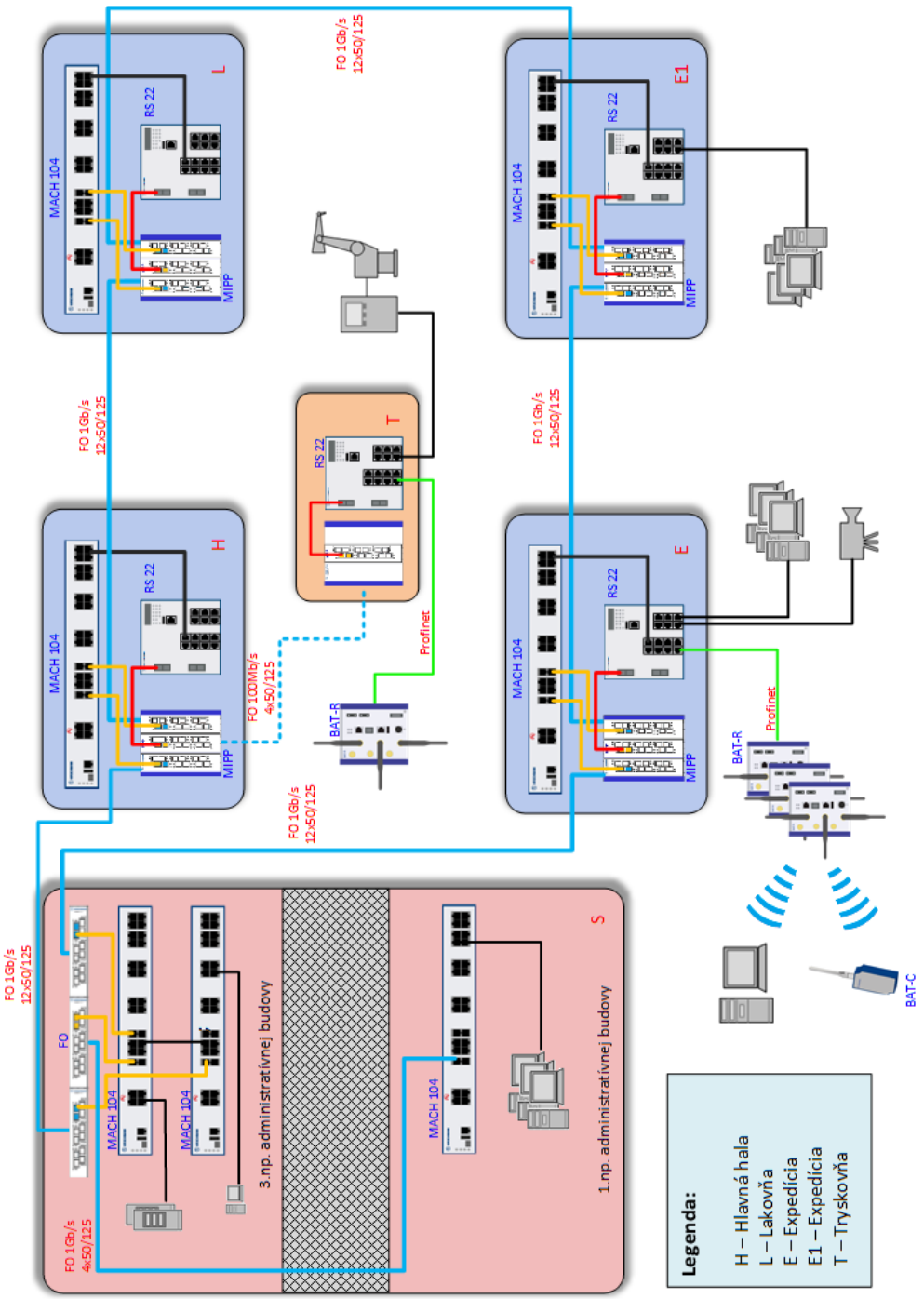
A.2 Podklady a finálny návrh

V tomto priečinku sa nachádzajú všetky podklady pre finálny návrh (pôdorys) a blokové schémy zapojenia sieťovej infraštruktúry zlievarne

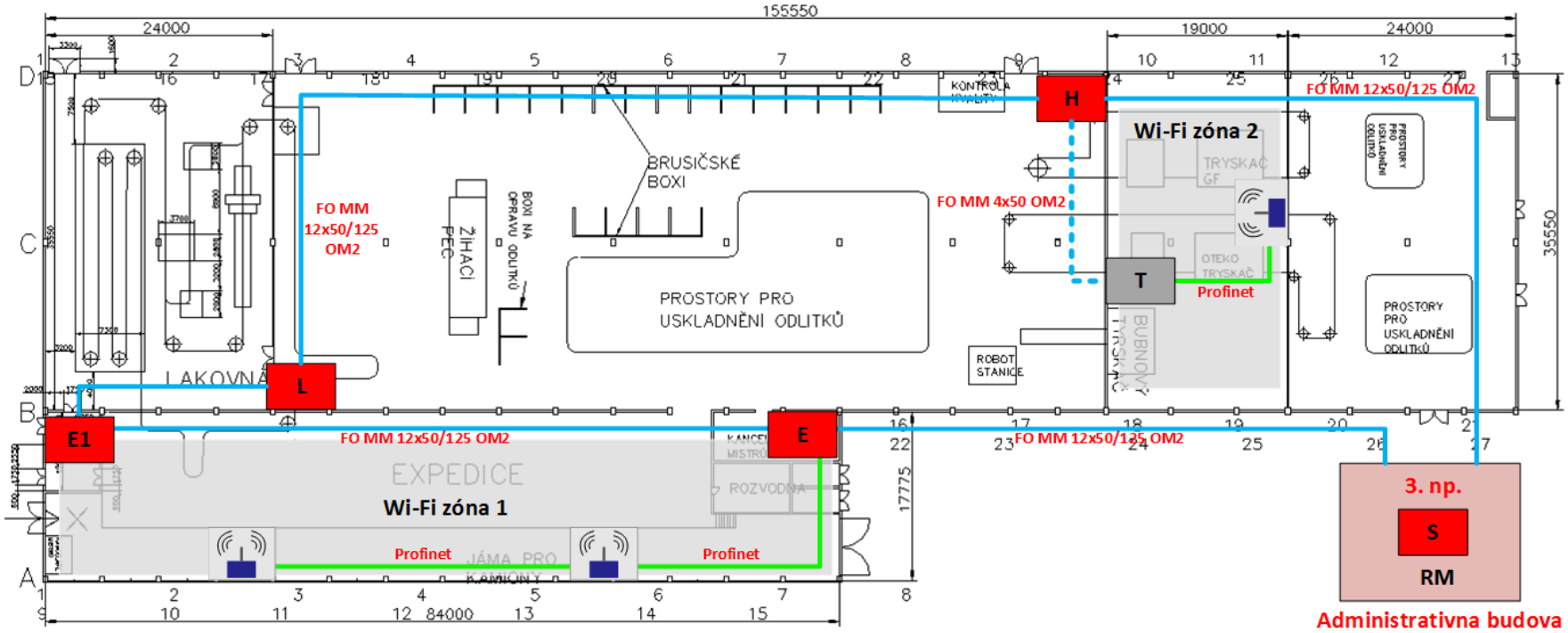
A.3 Fotodokumentácia

Celková fotodokumentácia realizovaných rozvádzačov podla návrhu.

B FINÁLNY NÁVRH INFRAŠTRUKTÚRY

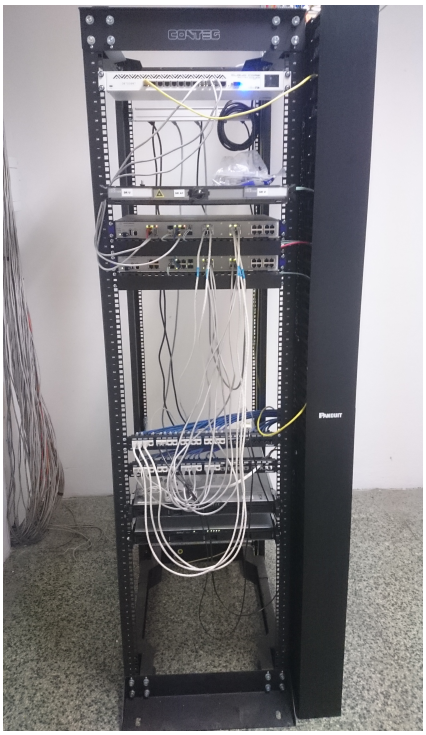


Obr. B.1: Plnohodnotná blokvá schéma infraštruktúry



Obr. B.2: Finálny nákres infraštruktúry v pôdoryse

C FOTODOKUMENTÁCIA



Obr. C.1: Serverovňa - hlavný rozvádzač

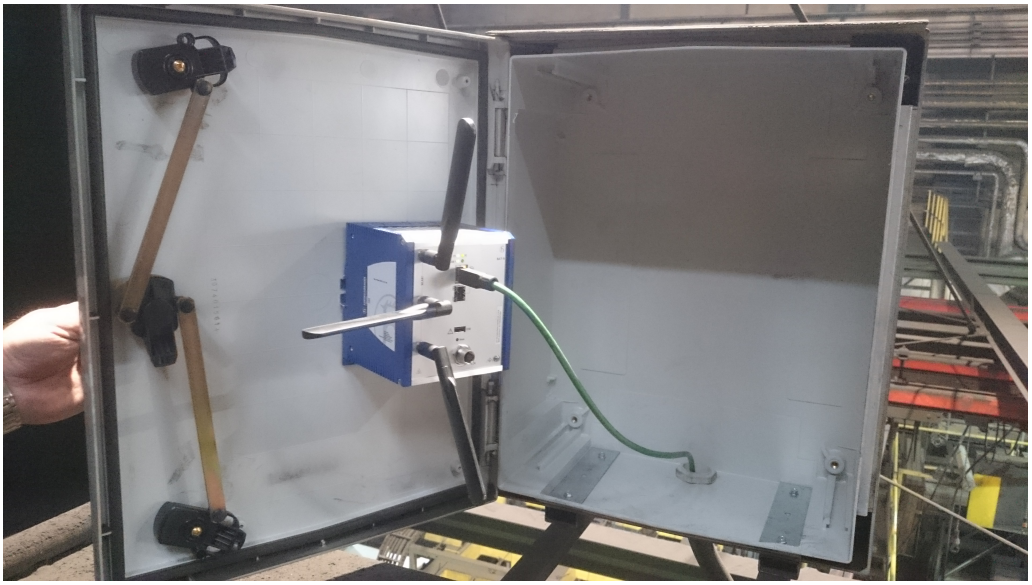
Obr. C.2: Serverovňa - Prepojenie MACH104

Obr. C.3: Rozvádzač hlavného optického rozvodu

Obr. C.4: Zapojenie rozvádzača hlavného optického rozvodu

Obr. C.5: Vedľajší rozvádzač T

Obr. C.6: Vedľajší rozvádzač T - prepojenie prvkov



Obr. C.7: Prístupový wi-fi bod BAT-R