VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH NA ZAVEDENÍ PRŮMYSLOVÉHO ŘEŠENÍ ISMS VE VÝROBNÍ SPOLEČNOSTI

A PROPOSAL FOR INDUSTRIAL ISMS IMPLEMENTATION IN MANUFACTURING COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Radek Kulhánek

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Petr Sedlák

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kulhánek Radek, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh na zavedení průmyslového řešení ISMS ve výrobní společnosti

v anglickém jazyce:

A Proposal for Industrial ISMS Implementation in Manufacturing Company

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Seznam odborné literatury:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut. 2014.
ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut. 2014.
DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
JORDÁN, V. a V. ONDRÁK. Infrastruktura komunikačních systémů III: Integrovaná podniková infrastruktura. Brno: CERM, Akademické nakladatelství, 2016. ISBN 978-80-214-5241-1.
ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 29.2.2016

ABSTRAKT

Tato diplomová práce se zabývá zavedením průmyslového řešení ISMS ve výrobní společnosti. Teoretická část práce shrnuje teoretické poznatky z oblasti bezpečnosti informací a průmyslové bezpečnosti. V další části je provedena analýza společnosti AB Komponenty s.r.o. Poté je provedena analýza rizik na základě vybraných aktiv a možných hrozeb působících na podnik. Následuje návrh opatření, které má za úkol minimalizovat potencionální hrozby.

ABSTRACT

This diploma thesis deals with industrial ISMS implementation in manufacturing company. The theoretical part of thesis summarizes the theoretical knowledge in the field of information security and industrial security. In the following section company AB Komponenty s.r.o. is analysed. Then is performed analysis of risks based on selected assets and potential threats. Followed by design of the countermeasure to minimalize potential threats.

KLÍČOVÁ SLOVA

ISMS, ICS, systém řízení bezpečnosti informací, průmyslové řídící systémy, průmyslové řešení, průmyslová bezpečnost, analýza rizik

KEYWORDS

ISMS, ICS, information security management system, industrial control systems, industrial solution, industrial security, risk analysis

BIBLIOGRAFICKÁ CITACE

KULHÁNEK, R. *Návrh na zavedení průmyslového řešení ISMS ve výrobní společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 75 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 26. května 2016 .....

Radek Kulhánek

PODĚKOVÁNÍ

Děkuji vedoucímu práce Ing. Petru Sedlákovi za odbornou pomoc při psaní této diplomové práce. Dále děkuji společnosti AB Komponenty s.r.o., která mi umožnila vypracovat praktickou část.

OBSAH

ÚVOD

Nacházíme se v době, kdy informace znamenají klíčovou roli v jakémkoliv ohledu. Ať už chceme nebo ne, data o nás se nachází hned v řadě systémů. V prostředí firem je to podobné, dnes už k úspěšnému konkurenčnímu boji nestačí pouze znalosti a zkušenosti klíčových manažerů. Neustálý vývoj informačních technologií zapříčiňuje generování obrovského objemu podnikových dat. Všechny tyto data můžou být pro společnost důležitá a nastává tedy zde potřeba tyto data nějakým způsobem chránit. Oblast, která se zabývá ochranou dat v podniku, se nazývá systém řízení informační bezpečnosti (Information Security Management System). ISMS zahrnuje celou řadu problémů a jejich řešení.

V průmyslovém prostředí hraje důležitou roli zejména dostupnost jednotlivých výrobních procesů. Každý výpadek služeb, které podporují výrobní procesy, má za následek zastavení těchto procesů, kde tato nečinnost může být posouzena jako finanční ztráta. A právě tímto tématem se tato diplomová práce zabývá.

Práce je rozdělena do tří základních částí. V první části jsou popsány základní pojmy bezpečnosti informací.

V druhé části je představena společnost AB Komponenty s.r.o., která se zabývá výrobou dílců a komponent v oblasti strojírenské výroby a elektrotechnického průmyslu. Následně je provedena analýza ICT, včetně její infrastruktury.

V poslední části je sestavena analýza rizik, která odhaluje potencionální rizika. Po vyhodnocení rizik následuje návrh opatření. Návrh opatření je pak zaměřen na síťovou infrastrukturu.

CÍL PRÁCE

Cílem práce je vytvoření návrhu na zavedení průmyslového řešení systému řízení bezpečnosti informací ve výrobní společnosti. Vstup pro tento návrh bude vycházet z analýzy současného stavu, která by měla skrze analýzu rizik odhalit nedostatky v podobě potencionálních rizik. Návrh tedy bude obsahovat vhodná opatření pro pokrytí určitých nedostatků. Součástí práce je teoretická část, kde se čtenář seznámí s problematikou ISMS a průmyslové bezpečnosti.

1 TEORETICKÁ VÝCHODISKA

V této kapitole budou popsána teoretická východiska, která jsou důležitá pro pochopení problematiky ISMS, jejichž hlavní cíl je ochrana aktiv společnosti (zejména informací).

1.1 Základní pojmy

Jelikož se v oblasti bezpečnosti informací setkáváme s mnoha pojmy, které nemusí být pro každého úplně zřejmé, bude se tato kapitola věnovat právě vysvětlením základních pojmů.

Data

Často dochází k zkreslení představy o tom, jaký je rozdíl mezi pojmem data a informace. Data jsou získávána měřením, generováním, výpočtem či měřením. Jde o holá fakt v podobě čísel nebo textu, bez jakéhokoliv významu. Tyto data jsou pak základním předpokladem pro vznik informace (1).

Informace

Informace nám vnikají poté, co přidáme datům určitou souvislost. Základem informace jsou tedy samotné data. Jde tedy o poznatek, který má pro daného příjemce nějakou informační hodnotu či je jinak užitečná. To znamená, že informace může být považovaná za data, ale data bez přidané hodnoty se informací nestanou (1).

Informační systém (IS - Information system)

Existuje celá řada definicí informačního systému. Obecně se dá říci, že informační systém představuje systém vzájemně propojených informací a procesů, které tyto informace zpracovávají (2).

Informační technologie (IT - Information Technology)

Pokud mluvíme o informačních technologiích, máme na mysli hardwarovou a softwarovou část, která nám umožňuje získávat, uchovávat a následně zpracovávat data za účelem distribuce informací pro potřeby uživatele (3).

Informační a komunikační technologie (ICT - Information and Communication Technology)

Jak už z názvu plyne, jedná se o informační technologie s využitím komunikačních technologií, které nabízí specifickou množinu technických prostředků pro odesílání a přijímání informaci tj. komunikaci.

Dostupnost (Availability)

Zajištění přístupnosti k informaci oprávněnému uživateli v požadovaném okamžiku (2).

Důvěrnost (Confidentiality)

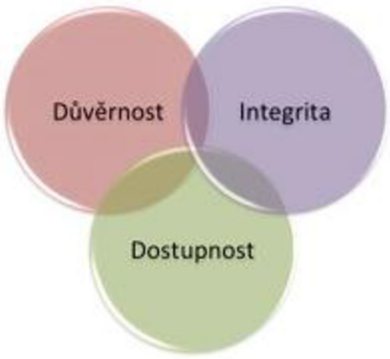
Zajištění přístupnosti k informaci pouze oprávněnému uživateli (2).

Integrita (Integrity)

Zajištění správnosti a úplnosti informace (2).

Bezpečnost informací (Information Security)

Bezpečnost informací řeší ochranu informací ve třech posledně zmíněných aspektech. Ochrana je tedy zaměřena na zachování integrity, zajištění dostupnosti a důvěrnosti informací.



Obrázek č. 1: Princip bezpečnosti informací. Zdroj: (4)

Bezpečnost informací je ve vzájemném vztahu s pojmy bezpečnosti organizace a bezpečnosti IS/ICT. Nejvýše postavená je logicky bezpečnost celé organizace, která má za úkol zajistit bezpečnost objektu a tím také majetek organizace, z čehož vyplívá, že napomáhá k bezpečnosti informační i bezpečnosti IS/ICT. Důležité je zmínit, že ochranou informací rozumíme i ochranu dat, která se nevyskytují pouze v digitální formě, ale i ve formě nedigitální (smlouvy, dokumentace,..). Bezpečnost IS/ICT má pak za úkol chránit pouze aktiva, která jsou přímo součástí informačních systému zajištěny informačními a komunikačními technologiemi (2).

Obrázek č. 2: Vzájemné vztahy bezpečností organizace. Upraveno dle: (2)

Pro bezpečnost nejen informací je pak tedy nutné vytvořit bezpečnostní zásady, politiky, postupy na vícero úrovních.

Aktivum (Asset)

Aktiva představují statky, které mají pro organizaci nějakou hodnotu. Aktiva můžeme rozdělit do dvou skupin.

- Hmotná aktiva - představují především technické prostředky výpočetní techniky (počítače, aktivní a pasivní prvky počítačové sítě, tiskárny, servery apod.);
- Nehmotná aktiva - nehmotná aktiva mohou mít formu důležitých dat, programového vybavení organizace, různých pracovních postupů v oblasti IS/ICT či jiných služeb (5).

Hrozba (Threat)

Potenciální příčina (skutečnost, událost) nechtěné bezpečnostní události, jejímž výsledkem může být poškození, zničení, ztráta důvěry nebo hodnoty aktiva. Hrozba

vzniká zneužitím zranitelnosti a může ohrozit bezpečnost organizace. Jednotlivé hrozby mohou mít odlišné charaktery jako například hrozby přírodní, technické, lidské a podobně (5).

Zranitelnost (Vulnerability)
Zranitelnost představuje slabé místo aktiva nebo řízení, které může být využito hrozbou tak, že hodnota aktiva může být snížena nebo úplně zničena.

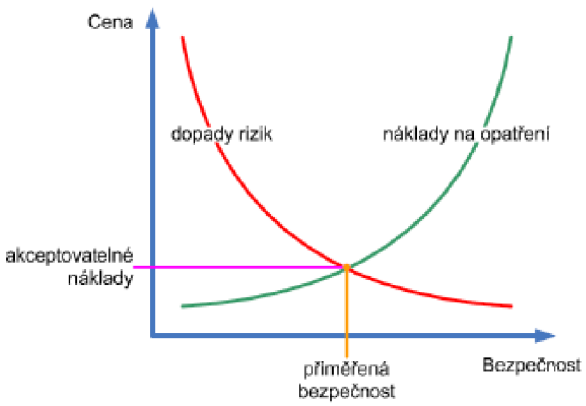
Dopad (Impact)
Dopadem se myslí možný vznik škody v důsledku působení hrozby. Dopady hrozeb se často převádějí na finanční hodnoty a porovnávají se s náklady na realizaci opatření.

Riziko (Risk)
Riziko je kombinace pravděpodobnosti události a jejího následku. Tato výsledná hodnota rizika se pak snižuje zavedením opatřeními pro dané hrozby a zranitelnosti (5).

Opatření (Countermeasure)
Opatření umožňuje snížit hodnotu hrozby nebo ji úplně eliminovat. Opatření mají nejčastěji formu zavedení určitých bezpečnostních politik.

Bezpečnostní incident (Security Incident)
Bezpečnostní incident je jakýkoliv útok neboli využití zranitelného místa s cílem krádeže nebo poškození určitého aktiva. Dále se jedná i o neúmyslnou akci, která může způsobit škodu na aktivech (1).

Přiměřená bezpečnost
Při investování úsilí a peněz do bezpečnosti by velikost této investice měla odpovídat hodnotě aktiv a míře možných rizik. Při zavádění systému informační bezpečnosti je tedy cílem najít přiměřenou úroveň bezpečnosti za akceptovatelné náklady.



Obrázek č. 3: Přiměřená bezpečnost za přijatelné náklady. Zdroj: (2)

ISMS (Information Security Management System)

Systém řízení informační bezpečnosti představuje část celkového systému řízení organizace. Skládá z pravidel, postupů, pokynů, souvisejících zdrojů a činností společně řízené organizací ve snaze o ochranu svých informačních aktiv.

1.2 Normy v oblasti ISMS

První norma pro oblast bezpečnosti informačních systémů vznikla ve Velké Británii v roce 1995 pod označením BS 7799. Tato norma položila první teoretický základ pro zavádění a implementaci managementu bezpečnosti informačních systémů. Byl to efektivní nástroj k hodnocení a aplikování bezpečnosti informací, který se rychle rozšířil po celém světě a dnes je k dostání v mnoha jazycích. Postupem času byla norma modernizována, kde v roce 1999 vznikla revize obsahující dva samostatné díly a v roce 2000 byla schválena jako mezinárodní standard ISO a uvedena pod označením ISO/IEC 17799:2000 (5).

1.2.1 Řada norem ISO/IEC 27000

Řada těchto norem vychází z výše zmiňovaných standardů BS 7799. Řada norem ISO/IEC vznikla v roce 2005 vydaná mezinárodní organizací pro normalizaci (ISO) a mezinárodní elektrotechnickou komisí (IEC). Tyto normy obsahují doporučení pro zavedení systému řízení bezpečnosti informací.

Normy řady ČSN ISO/IEC 27k obsahuje následující základní dokumenty (2):

- **ČSN ISO/IEC 27000** – Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Systémy managementu bezpečnosti informací – Přehled a slovník;
- **ČSN ISO/IEC 27001** – Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Požadavky;
- **ČSN ISO/IEC 27002** – Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Soubor postupů;
- **ČSN ISO/IEC 27003** – Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací;
- **ČSN ISO/IEC 27004** – Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací;
- **ČSN ISO/IEC 27005** – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací;
- **ČSN ISO/IEC 27006** – Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací;
- **ČSN ISO/IEC 27007** – Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací;

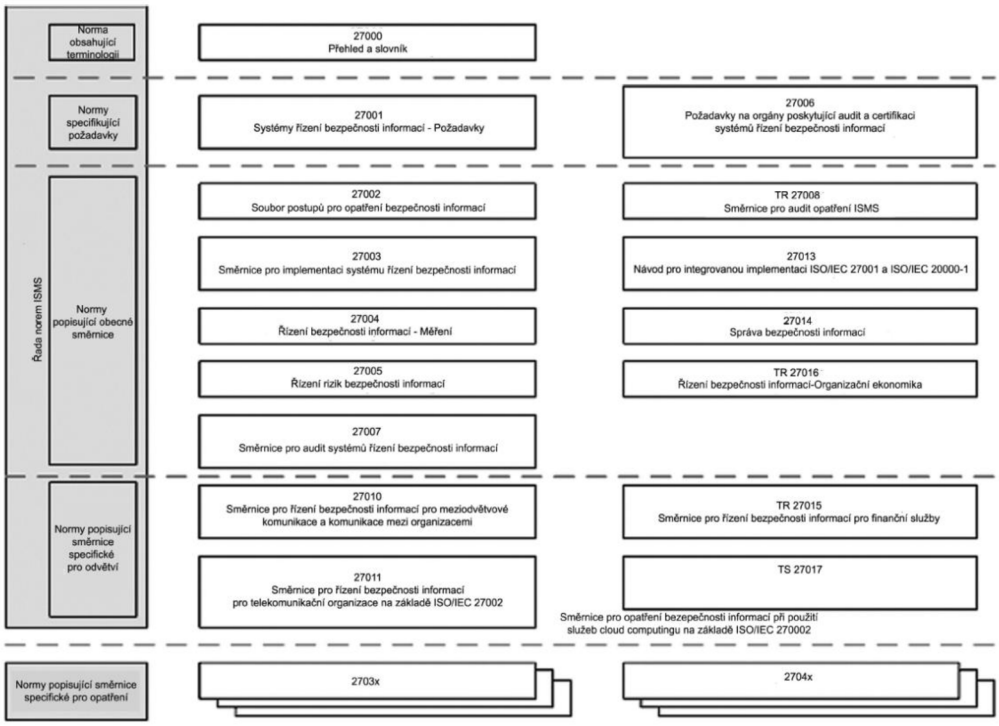
1.2.2 Norma ISO/IEC 27033

Tato norma představuje otevřený soubor norem s postupným vydáváním, poskytující podrobný návod na implementaci bezpečnostních mechanizmů, které jsou zmíněny v normě ISO/IEC 27002. Týkají se bezpečnosti zařízení připojených do sítě, síťových služeb, uživatelů přistupujících do sítě, informací přenášených po síti a také správy těchto bezpečnostních opatření (6). Norma se skládá z následujících částí (2):

- **ISO/IEC 27033-1:2009** *Network security overview and concepts* - Jedná se o revizi normy ISO/IEC 18028-1, která poskytuje celkový přehled principů a přístupů tohoto souboru norem;
- **ISO/IEC 27033-2:2012** *Guidelines for the design and implementation of network security* - Jedná se o revizi normy ISO/IEC 18028-2, která definuje bezpečnostní architekturu sítí;

- **ISO/IEC 27033-3:2010** *Reference networking scenarios -- threats, design techniques and control issues* - Definuje rizika, techniky návrhu a řešení problémů spjatých se správou sítí;
- **ISO/IEC 27033-4:2012** *Securing communications between networks using Virtual Private Networks (VPNs)* - Definuje rizika, techniky návrhu a řešení problémů spjatých se zabezpečením datových toků mezi jednotlivými sítěmi;
- **ISO/IEC 27033-5:2013** *Securing Virtual Private Networks (VPNs) - Risks, design techniques and control issues* - Jedná se o revizi normy ISO/IEC 18028-5, která definuje rizika , techniky návrju a řešení problémů spjatých se spojením pomocí VPN;

Vzájemné vztahy mezi normami řady ISMS jsou zobrazeny na obrázku 4.



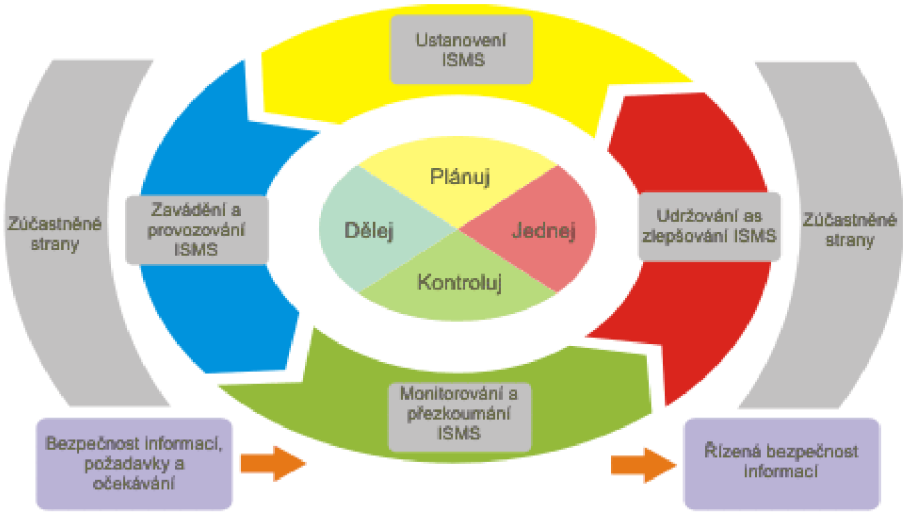
Obrázek č. 4: Vztahy mezi normami řady ISMS. Zdroj: (9)

1.3 Model PDCA

Model PDCA, taktéž známý jako Demingův model, poprvé použil ve svých prací W. Edwards Deming, Tento model představuje metodu postupného zlepšování například kvality výrobků, služeb, procesů, aplikací, dat, probíhající formou opakovaného provádění čtyř základních kroků.

- **plan (plánuj)** - naplánování zamýšleného zlepšení (záměr),
- **do (dělej)** - realizace plánu,
- **check (kontroluj)** - ověření výsledku realizace oproti očekávanému záměru,
- **act (jednej)** - úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe.

Tento přístup se stal základem nejen pro oblast řízení informační bezpečnosti, ale také pro mezinárodní standardy v oblasti integrovaných systémů řízení. Na obrázku 5 je PDCA model aplikovaný na procesy ISMS.



Obrázek č. 5: Životní cyklus ISMS. Zdroj: (7)

Celý životní cyklus je tedy postaven na čtyřech etapách:

Plánuj (ustanovení ISMS) - první etapa má za úkol stanovit politiku ISMS, cílů, procesů a postupů související s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace (5).

Dělej (zavádění a provozování ISMS) - v druhé etapě zavádíme stanovenou politiku ISMS a také všechny stanovené procesy a postupy (5).

Kontroluj (monitorování a přezkoumání ISMS) - ve třetí etapě se provádí posouzení včetně měření výkonu procesů vůči politice ISMS, stanoveným cílům a praktickým zkušenostem. Získané výsledky jsou následně předány vedení organizace ke kontrole (5).

Jednej (udržování a zlepšování ISMS) - čtvrtá etapa se pak zabývá přijetím preventivních opatření včetně opatření nutná k nápravě, které vznikli na vyhodnocení vedení organizace, aby bylo dosáhnuté neustálé zlepšování ISMS (5).

1.4 Zavedení ISMS

1.4.1 Ustanovení ISMS

Etapa ustanovení je důležitou etapou zavedení ISMS, v které se definují základy celého systému řízení bezpečnosti. Výsledky této etapy pak mají vliv na další etapy, kde mají dlouhodobý charakter. V této etapě se formuluje definice rozsahu ISMS. Vzniká zde taktéž prohlášení o politice ISMS. Etapa ustanovení obsahuje i analýzu rizik a výběr vhodných bezpečnostních opatření pro snížení dopadů nalezených rizik. Etapa by zpravidla měla být zakončena souhlasem vedení se zavedením ISMS v rozsahu, v jakém to společnost potřebuje (5).

Rozsah a hranice ISMS

V této části jsou popsány dotčené části systému ISMS určené k implementaci. Rozsah a hranice ISMS se definují na základě posouzení specifických rysů činnosti společnosti, jejího uspořádání, organizační struktury, lokace a topologie, aktiv a technologií. Taktéž popisuje důvody, proč jsou některé oblasti z rozsahu ISMS vyjmuté (2).

Politika ISMS

Politika ISMS představuje důležitý dokument, který má charakter stručného dokumentu. Tento dokument musí být schválen vedením. Úkolem tohoto dokumentu je zpřesnit cíle ISMS při zohlednění požadavků a cílů celé společnosti. Politika by měla vytvořit potřebné vazby pro budování a údržbu ISMS. Dále by pak měla být definována kritéria pro popisování a hodnocení rizik (5).

Pravidla a postupy pro řízení rizik

Zde dochází k definování systematického přístupu k hodnocení rizik. Určuje metodiku hodnocení rizik, která vyhovuje ISMS a stanovené bezpečnosti informací. Na základě tohoto dokumentu se pak provádí analýza rizik včetně určení kritérií pro akceptaci rizik a pro definování jejich akceptační úrovně (2). Analýze rizik je blíže věnovaná kapitola 1.5.

Souhlas vedení se zavedením ISMS a se zbytkovými riziky

V této části vedení odsouhlasí návrh bezpečnostních opatření nutných pro snížení bezpečnostních rizik. Dále by mělo vzniknout vyjádření k existujícím zbytkovým rizikům a určit zda jsou pro chod organizace přijatelná. Pokud k souhlasu nedojde, je potřeba opatření upravit (5).

Prohlášení o aplikovatelnosti

Tento povinný dokument obsahuje souhrn rozhodnutí, jakým způsobem bude naloženo s identifikovanými riziky. Povinně musí být vysvětleny jednotlivá bezpečnostní opatření vybrané včetně jejich cílů a důvody pro jejich výběr. Obsahovat musí také vysvětlení důvodů vyřazení jednotlivých vyřazených bezpečnostních opatření (2).

1.4.2 Zavádění a provoz ISMS

Cílem této etapy je zavedení vybraných bezpečnostních opatření do chodu organizace.

Plán zvládaní rizik

Je důležitým dokumentem, který popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanovené cíle a priority těchto činností, omezující faktory a potřebné zdroje. Zapomenou se nesmí ani na definování odpovědnosti za

provádění jednotlivých činností. Plán je sestaven dle podkladů získaných při ustanovení ISMS a také dle podnětů získaných při pravidelném přehodnocování ISMS vedením společnosti (5).

Příručka bezpečnosti informací

Příručka bezpečnosti informací představuje souhrn dokumentů, kde dochází k stanovení bezpečnostních pravidel, principů, zásad a odpovědnosti. Při sestavování tohoto dokumentu je potřeba zpracovat několik provedení tak, aby každá cílová skupina měla přiřazena dokument určený přímo pro ni s konkrétní mírou podrobnosti. Dokument musí být pro cílové skupiny snadno pochopitelný a srozumitelný (5).

Prohlubování bezpečnostního povědomí

Jedná se o velmi důležitou činnost při rozvoji ISMS. Lidský faktor představuje v oblasti bezpečnosti nejslabší článek. Proto je nutné srozumitelně vysvětlovat bezpečnostní principy a pravidla včetně seznámí s bezpečnostními riziky. Tak se zvýší šance, že zaměstnanci budou schopni zvládat i situace, které nejsou v dokumentaci popsány. Tento úkol vyžaduje vysoké a systematické úsilí. Kvůli změnám, které vyžaduje rozvoj ISMS včetně pravidelné obměně pracovníků, je prohlubování bezpečnostního povědomí trvalý a nekonečný proces, který v mnoha případech rozhoduje o skutečné efektivitě zavedeného ISMS (5).

Měření provozu ISMS

Aby jsme zjistili efektivnost řízení bezpečnosti, je potřeba nějakým způsobem měřit účinnost zavedených bezpečnostních opatření. Jde o velmi důležitý proces, kdy je potřeba pravidelné sledování stanovených ukazatelů, které poskytují informace o skutečném fungování systému řízení bezpečnosti. Na základě těchto informací lze pak provádět důležitá rozhodnutí. Ukazatele pro měření bezpečnosti informací lze rozdělit do několika skupin dle předmětu měření:

- finanční,
- personální,
- technické - ukazatele provozu IS/ICT (5).

Řízení zdrojů, dokumentace a záznamů ISMS

Tento proces je posledním bodem etapy zavedení ISMS. Jako poslední krok vyžaduje provádění všech činností řízeným a dokumentovaným způsobem. Je tedy nutné o každém kroku shromažďovat podklady pro další fázi - monitorování. Pro umožnění kontroly fungování ISMS je podstatné vytvořit definovaná pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti. Současně je důležité vytvářet záznamy o všech provedených úkonech včetně identifikace osoby, která úkon provedla, kdy a kde byl realizován (5).

1.4.3 Monitorování a přezkoumání ISMS

Cílem třetí etapy je zajistit zpětnou vazbu při zavedení ISMS, kdy dochází k ověřování všech aplikovaných bezpečnostních opatření a jejich důsledek na ISMS.

Provádění kontrol

Pravidelné kontroly ze strany osob, které mají za fungování ISMS odpovědnost, jsou základní zpětnou vazbou, které jsou nezbytná pro fungování ISMS. Součástí kontrol musí být schopnost včasné detekce chyb a pokusů o narušení bezpečnosti stejně jako schopnost sledování bezpečnostních událostí a včasná detekce bezpečnostních incidentů. Podněty z těchto aktivit je nutné promítnout do příslušných dokumentů a plánů ISMS (5).

Interní audity ISMS

Interní audit zajišťuje zpětnou vazbu jako nezávislý pohled na fungování ISMS. Cílem auditu je stanovit rozsah, v jakém jsou splněna předem stanovená kritéria. Zaměření auditu by měl být rovnoměrně rozložen na celý rozsah ISMS. Audit by měl vždy prověřit jak dodržování procesních pravidel, tak fungování jednotlivých bezpečnostních opatření.

Přezkoumání ISMS vedením

Na základě podnětů a připomínek k fungováni ISMS získané během jeho monitorování by mělo pravidelně docházet k přezkoumání ISMS ze strany vedení organizace. Interval

tohoto přezkoumání by neměl přesahovat jeden rok. Výstupem tohoto přezkoumání bývá zpráva o stavu ISMS.

1.4.4 Udržování a zlepšování ISMS

Cílem poslední etapy při zavedení ISMS je jeho udržování a zlepšování na základě nedostatků, které se objevily v průběhu zavádění ISMS.

Soustavné zlepšování ISMS

Zpětná vazba, která je v systému zavedena, musí odhalovat nedostatky a jejich příčiny a na tyto podněty později reagovat. Podněty by měly pocházet od uživatelů na všech úrovních hierarchie. Důležitá je motivace pracovníků na účasti při všech činnostech spojených s ISMS (5).

Odstraňování nedostatků ISMS

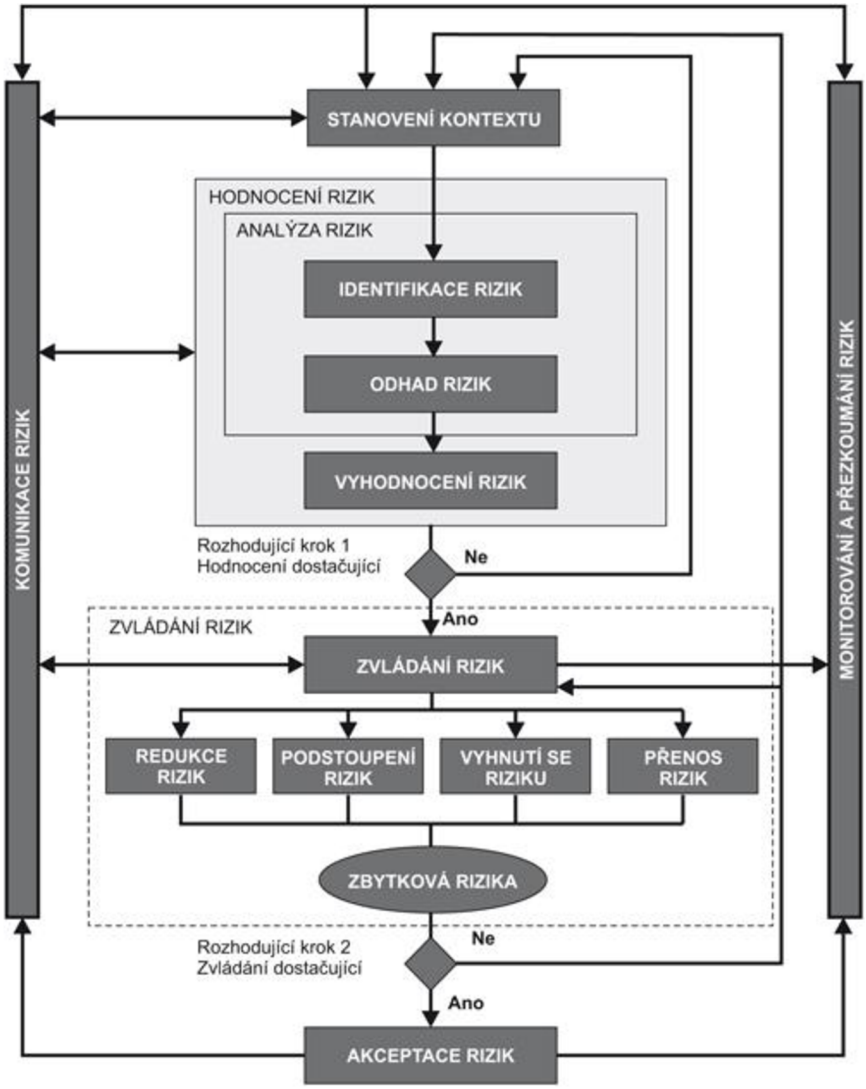
Jedno z řešení nedostatků ISMS je zajištění opatření k nápravě tohoto nedostatku, což představuje reaktivní formu řešení, kdy se tento nedostatek projevil a je potřeba na něj vhodným způsobem reagovat. Proaktivní forma řešení naopak představuje zavedení preventivního opatření, kdy se určitý nedostatek ještě neprojevil, ale pokud by se v budoucnu objevil, mohl by způsobit vážnější škody. Při odstraňování nedostatků je nutné vzít v úvahu všechny souvislosti a opatření realizovat tak, aby se omezily možnosti jejich opakování. Všechny postupy je nutné dokumentovat a po zavedení opatření přezkoumat, zda jsou účinná (5).

1.5 Analýza a řízení rizik

Řízení rizik představuje komplexní proces, jehož cílem je identifikace a kvantifikace rizik a následné rozhodnutí o vhodném způsobu zvládání těchto rizik.

Analýza rizik je první etapou procesu řízení rizik. Jedná se o klíčový nástroj systematického přístupu k zavádění a udržování bezpečnosti informací. Cílem analýzy rizik je identifikace zranitelných míst organizace. Znalost rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopná snížit negativní dopady rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní (2).

Obecný postup analýzy řízení je uveden na následujícím obrázku:



Obrázek č. 6: Proces řízení rizik. Zdroj: (10)

1.5.1 Metody analýzy rizik

V analýze rizik se pracuje s dvěma základními principy vyjádření veličin. Jde o kvantitativní a kvalitativní metody. Z těchto metod se může použít jedna z nich, jejich kombinace, nebo vlastní metoda sestavená na míru dané organizaci (11).

Kvantitativní metody - jsou metody využívající matematického a statistického výpočtu. Výsledky jsou velmi srozumitelné, jednoznačné a jdou jednoduše vyjádřit jako peněžní hodnoty. Tyto metody jsou velmi časově náročné a také často velmi nákladné na provedení (11).

Kvalitativní metody - jsou považovány za jednodušší a rychlejší metodu. Závisí na subjektivním posouzení. Tato metoda používá pro popis výše dopadu, hrozeb, zranitelnosti a konečného rizika nejčastěji hodnotící stupnice (například 1 až 5), nebo slovní popis (například nízké, střední, vysoké), případně hodnota pravděpodobnosti (0 až 1). U této metody nejsme schopni vyjádřit finanční hodnoty aktiv (11).

Vlastní metody - tyto metody mají možnost sestavit metodiku na základě znalostí daného prostředí přesně na míru dle mezinárodních norem a standardů (11).

1.5.2 Přístupy k analýze rizik

Norma ISO/EIC 27005 vysvětluje několik možností přístupů při sestavování analýzy rizik (12):

Základní přístup - používá se pro rychlé zavedení bezpečnostních opatření, kde o rychlé řešení s poměrně nízkými finančními náklady. Neprobíhá zde žádná podrobná analýza, takže nelze zajistit adekvátní bezpečnostní zajištění každého prvku. Vhodné pro organizace s menší závislostí na IS a nižší požadovanou úrovní informační bezpečnosti (11).

Neformální přístup - tento přístup využívá znalostí a zkušeností jednotlivců. Úroveň míry rizik je obvykle určována kvalifikovaným odhadem. Jedná se o poměrně rychlý finančně nenáročný přístup, kde ovšem může dojít k opomenutí důležitých detailů,

navíc může být do analýzy zanesena určitá míra subjektivity. Analýza se provádí bez dokumentace přesných postupů.

Detailní přístup - analýza je prováděna na základě standardními metodami. Analýza zahrnuje identifikaci a ohodnocení aktiv, identifikaci a ohodnocení hrozeb, identifikaci a ohodnocení zranitelností a stanovení jednotlivých rizik. Výsledkem je pak vztah mezi hodnotou rizika a hodnotou aktiva, hrozby a zranitelnosti. Následně se rizika vyhodnotí a jsou na ně aplikována odpovídající bezpečnostní opatření, tak aby byla dosažena požadovaná bezpečnost. Tento přístup vyžaduje značné úsilí a je velmi časově náročný a finančně dražší. Považuje se za nejpřesnější přístup (11).

Kombinovaný přístup - jedná se o přístup který kombinuje nejlepší vlastnosti základního přístupu a detailní analýzy rizik. Prvotní analýza je provedena pro všechny systémy a až následně detailně pro systémy, které jsou klíčové pro činnost společnosti. To má za následek minimalizaci časové náročnosti při zachování maximální finanční efektivnosti (11).

1.5.3 Obecný postup analýzy rizik

- **Stanovení hranic revize** - stanovuje, která aktiva budou do analýzy zahrnuta, abychom zabránili vynakládání zdrojů na zbytečné činnosti.
- **Identifikace aktiv** - vytváříme seznam všech aktiv ležících uvnitř hranic analýzy rizik. Může se jedna o fyzická aktiva, softwarová aktiva nebo informační aktiva. V ideálním případě by tento krok měli provádět interní zaměstnanci, protože mají o firemních aktivech nejlepší přehled.
- **Ohodnocení aktiv** - k vytvořenému seznamu aktiv je nutné přiřadit hodnoty, které reprezentují význam aktiv pro činnost organizace. Hodnota aktiv nemusí být určena finančním ohodnocením, ale například z hlediska nepříznivých dopadů na činnost organizace, plynoucí ze ztráty důvěrnosti, integrity, dostupnosti, individuální odpovědnosti, autenticity a spolehlivosti (2).
- **Identifikace hrozeb** - hroby mohou mít přírodní charakter nebo lidský původ, taktéž mohou být úmyslné nebo náhodné. Pro identifikaci hrozeb lze využít seznam uvedený v normě ČSN ISO/IEC TR 13335-3 v příloze C (2).

- **Odhad zranitelnosti** - tento odhad nám odhaluje slabá místa v různých oblastech organizace (fyzické prostředí, postupy, personál apod.), která mohou být využita zdrojem hrozby a způsobit tak škodu na aktivech (2).
- **Stanovení výsledné míry rizika** - výše rizika je odvozena z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. Matematicky lze riziko vyjádřit několika způsoby. Tří faktorový přístup je definován jako: $R = A \times H \times Z$, kde R je míra rizika, A hodnota aktiva, H pravděpodobnost hrozby, Z zranitelnost. Dvou faktorový přístup je pak definován jako $R = PI \times D$, kde R je míra rizika, RI pravděpodobnost incidentu, D dopad (2).

1.5.4 Zvládání rizik

Závěrečnou etapou řízení rizik je proces výběru a přijímání opatření pro změnu rizik. Po zjištění bezpečnostních potřeb a stanovení jejich priorit je nutné vybrat bezpečnostní opatření, která umožní zjištěná rizika efektivně snižovat. K výběru těchto opatření se nejčastěji využívá katalog opatření definovaný normou ISO/IEC 27002, který poskytuje doporučení a návod pro zavedení nejlepších praktik pro podporu opatření uvedených v příloze A normy ISO/IEC 27001. Následný návrh bezpečnostních opatření musí být odsouhlaseno vedením organizace. Důležitou částí zvládání rizik je akceptace zbytkových rizik vedením. Zbytkové rizika představují rizika, která zůstávají po eliminaci pomocí bezpečnostního opatření. Tyto rizika jsou většinou pro organizaci přijatelné a není nutné podnikat další postupy k jeho snižování. Akceptace těchto rizik zase musí být odsouhlaseno vedením organizace (11).

Způsoby zvládání rizik

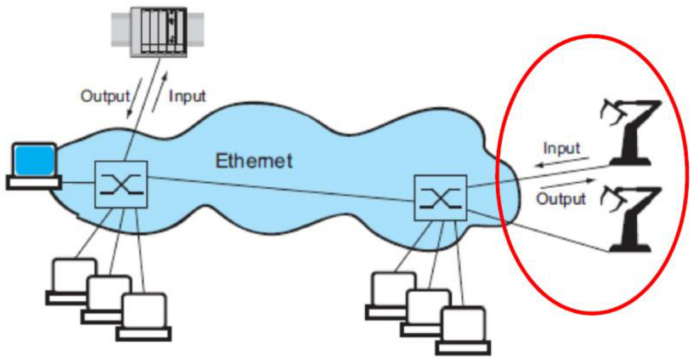
Před rozhodnutím způsobu zvládání rizika by měla být stanovena kritéria, na jejichž základě bude určováno, zda-li je riziko pro organizace akceptovatelné či nikoliv. Akceptace rizika může být zvolena z důvodu, že se jedná o nízké riziko nebo z důvodu, kdy náklady na zvládání tohoto rizika jsou pro organizace cenově neúnosné. U rizik středních až kritických by se pak mělo usilovat o jejich snížení (11).

Existuje několik metod zvládání rizik (11):

- **Akceptace rizika** - jedná se o vědomou a objektivní akceptaci rizika, kdy dopad na aktivum je téměř zanedbatelný. Nejpoužívanější metoda v případě zanedbatelných rizik.
- **Redukce rizika** - spočívá ve snížení rizika na požadovanou hodnotu vhodným opatřením.
- **Pojištění proti riziku** - tento způsob zvládání rizik nesnižuje riziko, ale snižuje pouze dopad. Používá se v případě, že výskyt bezpečnostního incidentu není pravděpodobný, ale pokud by k němu došlo, představoval by kritický vliv na chod organizace.
- **Transfer rizika -** jde o přenos rizika na jiný subjekt formou outsourcingu nebo společného partnera.
- **Vyhnutí se riziku -** je způsob, který je pro řešení mnoha rizik zcela nevyhovující. Dochází k zamezení činností, které jsou příčinou zniku rizika.
- **Ignorování rizika -** nejbezpečnější způsob zvládání rizik. Ignorování (retence) rizika může být vědomá či nevědomá.

1.6 Průmyslová bezpečnost

Neustálý rozvoj průmyslové automatizace a regulace má za následek zvyšující se požadavky na rychlost dat a dochází tak k integraci současných průmyslových sběrnic s nadřazenými počítačovými systémy. Jednou z možností, jak lze tyto nové požadavky realizovat, je využití technologie Ethernet v průmyslovém prostředí (13).



Obrázek č. 7: Příklad průmyslové komunikace. Zdroj: (14)

V průmyslovém prostředí je bezpečnost provozu ICT klíčovým prvkem a je dosahována maximálními možnostmi aplikovaných doporučených bezpečnostních doporučení.

Jeden z hlavních parametrů průmyslových aplikací je práce v reálném čase. Právě proto jsou požadavky na průmyslovou infrastrukturu tak specifické, že také splňují požadavky na sítě s maximální dostupností (MCN - Mission Critical Network) (2).

S průmyslovým prostředím je pak spojena i problematika **ICS (Industrial Control System)**. Jedná se tedy o průmyslové řídící systémy, které zahrnují několik typů řídících systémů, používaných v průmyslovém prostředí. Tyto systémy zahrnují SCADA (Supervisovy control and Data Acquisition) systémy, distribuované řídící systémy (DCS) a další menší systémy konfigurované jako jsou například programovatelné automaty (PLC).

1.6.1 Klíčové komponenty ICS

Průmyslové řídící systémy využívají komponenty, které můžeme rozdělit do dvou kategorií (15):

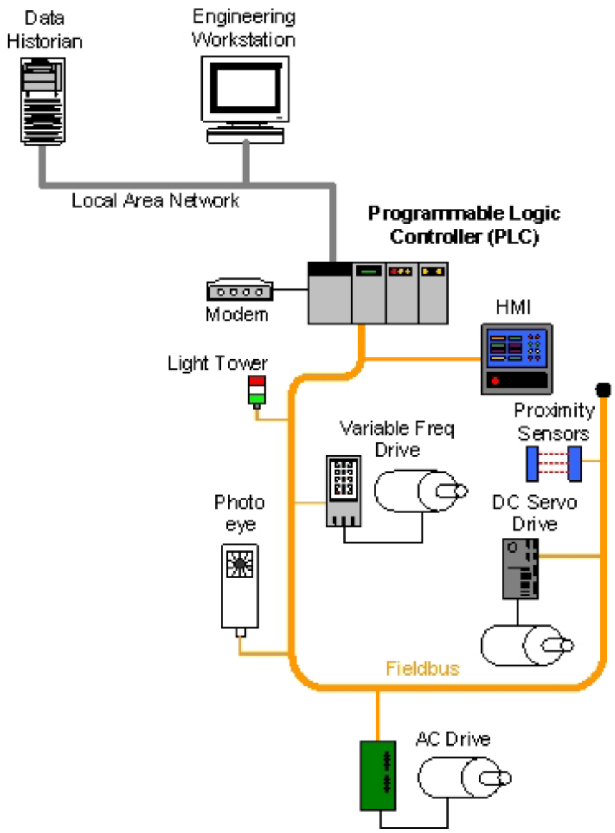
1.6.1.1 Řídící komponenty

- **Řídící server** (Control Server) **-** jedná se o server, který komunikuje s inteligentními jednotkami, které řídí jednotlivé výrobní procesy.
- **SCADA Server** (či MTU - Master Terminal Unit) - je řídící jednotka ve SCADA systému, který provádí dohled nad výrobními procesy.
- **Remote Terminal Unit** (RTU) - tato vzdálená telemetrická datová jednotka je určená k podpoře SCADA vzdálených stanic. Někdy je také funkce RTU převzata PLC zařízením, které je univerzálnější.
- **Programmable Logic Controller** (PLC) - zařízení ve formě malého průmyslového počítače určeného k řízení elektrických komponentů výrobních procesů.
- **Intelligent Electronic Devices** (IED) - jedná se o senzor, kde je vestavěna základní inteligence. Kombinuje tak analogový vstupní senzor s analogovým výstupem základního řízení, komunikačním modulem a programovatelným zařízením v jednom.
- **Human-machine Interface** (HMI) - představuje HW a SW, který umožňuje operátorovi monitorovat stav výrobního procesu, editovat řídící nastavení nebo manuálně převzít automaticky řízené operace.
- **Data Historian** - je centrální databáze pro protokolování informací o všech procesů v ICS infrastruktuře. Slouží k následným analýzám, statistikám procesů v ICS.
- **Input/Output (IO) Server -** je komponenta sloužící ke komunikaci s ICS zařízením (PLC, RTU a IED) a k připojení zařízení HMI a řídícího serveru.

1.6.1.2 Síťové komponenty

- **Výrobní síť** (Fieldbus Network) - Tato síť slouží k napojení senzorů a dalších výrobních zařízení k PLC. Sběrnicové řešení nahrazuje přímé napojení řídících jednotek s každým zařízením a komunikuje na základě různých protokolů.

- **Řídící síť** (Control Network) - řídící síť umožňuje propojení dohledové úrovně s kontrolními moduly typu PLC.
- **Komunikační router** (Communications Routers) - zajišťuje komunikaci mezi dvěma sítěmi. Nejčastěji jde o komunikaci LAN a WAN. Používá se také ke vzdálenému připojení RTU k MTU na delší a velké vzdálenosti pro SCADA komunikaci.
- **Firewall** (FW) - slouží k ochraně sítě a k filtrování komunikačních paketů podle nastavených politik. Taktéž se používají pro oddělení zón v ICS sítích.
- **Modem** - je zařízení, které se používá pro převod sériových dat na data, která jsou schopna být přenášena skrze komunikačních linkách (telefonních) na větší vzdálenosti.
- **Vzdálený přístup** (Remote Access Point) - vzdálený přístup je používaný pro vzdálenou konfiguraci řídícího systému nebo přístup k datům (PDA, tablety, apod.).



Obrázek č. 8: Příklad výrobního procesu využitím PLC. Zdroj: (15)

1.6.2 Porovnání ICS a IT systémů

Z počátku byly systémy ICS od IT systémů zcela odlišné, kdy ICS systémy představovaly izolované systémy běžící na jedinečných protokolech využívající speciální hardware a software. Avšak tyto specifické řešení jsou v dnešní době nahrazovány zařízeními využívající široce dostupné protokoly a služby. Tím s sebou nesou také možné zranitelnosti, na které se nesmí zapomínat. Je stále potřeba vnímat rozdíly mezi těmito systémy a odlišovat jejich požadavky (15).

ICS patří do časově kritických systémů, které nevyžadují vysokou průchodnost, ale vyžadují práci v reálném čase - velice nízké odezvy. Naproti tomu IT systémy obvykle vyžadují vysokou průchodnost a nepotřebují takovou úroveň odezvy. Požadavky na dostupnost u ICS systému jsou vysoké. Neočekávané výpadky systémů, které řídí výrobní procesy jsou nepřijatelné. Výpadky jsou plánovány dny až týdny předem. Pro tento požadavek je obecně nutno použít redundantní topologii. V typickém IT systému jsou primárním cílem zajistit důvěrnost a integritu dat. V ICS je prioritou dostupnost, která je spjata s ochranou jednotlivých procesů. Odlišnost v komunikaci u jednotlivých systému najdeme u požívání komunikačních protokolů, kde mimo standardní protokoly jsou v ICS využity i protokoly další. Podobně je to tak u operačních systémů. V ICS potřebujeme složitější systémy pro kontrolu a řízení, v IT systémech si vystačíme se standardními operačními systémy. Doporučen je výběr jednotné platformy u ICS. Poslední odlišnost pak najdeme v životnosti jednotlivých komponentů (15).

Požadavky	ICT	ICS
Požadavky na výkonnost	mimo reálný čas	v reálném čase
odezva	konzistentní	okamžitá
průchodnost	vysoká	střední
Požadavky na dostupnost	se zpožděním	vysoká
redundance	není nutná	nutná
Požadavky na Mngmt rizik	důvěrnost a integrita	maximální dostupnost
Požadavky na bezpečnost	ochrana aktiv	ochrana procesů

Komunikace	standardní protokol	více protokolů
OS	standardní	speciální
Doporučená technická podpora	různá	jeden dodavatel
Životnost komponentů	3-5 let	15 - 20 let

Tabulka č. 1: Shrnutí odlišností ICS a IT systémů. Zdroj: vlastní

1.6.3 Požadavky průmyslové síťové infrastruktury

Použití komerční infrastruktury Ethernetu není vhodná pro průmyslové prostory a to zejména proto, že nesplňují požadavky pro průmyslového prostředí. Tyto požadavky mohou být následující (16):

- **Větší rozsah pracovních teplot** - požadován může být rozsah až -40°C do +70°C. V některých případech může být požadavek i odolnosti proti rychlému cyklickému kolísání teploty (v extrémech od dolní až po horní teplotní hranici).
- **Vysoká odolnost proti vlivům prostředí**
  - prašnost (až velmi vysoká prašnost)
  - vibrace (až velké otřesy), rázy a údery
  - ultrazvuk
  - rentgenové nebo radiační zařízení
  - sluneční záření, UV záření, IF záření
- **Vysoká odolnost proti chemickým vlivům**
  - vlhkost, voda
  - olej, benzin, odmašťovadla
  - působení různých chemikálií
- **Další požadované vlastnosti**
  - odolnost proti EMI (elektromagnetické rušení)
  - přísné limity na elektromagnetické vyzařování
  - odolnost proti přepětí a podpětí
  - odolnost proti elektrostatickému náboji
  - provedení do výbušného prostředí

Všechny tyto požadavky se projevují na konstrukci jednotlivých komponentů (jak u pasivní vrstvy - kabeláže, tak aktivních prvků).

Prvky pasivní vrstvy (metalické i optické kabely) používají zodolněné, speciální či pancéřované plášťování. Konektory se zde používají v odolném provedení (krytí) nebo jsou použity speciální konektory (M12). U datového rozvaděče se počítá nejen s klasickou 19“ montáží, ale také s montáží DIN. Pro zarušené prostředí z pohledu EMC je také častá potřeba použít speciálního převodníku (konvertor), který je schopen převádět metalickou síť na optickou a naopak.

Obrázek č. 9: Metalický pancéřovaný kabel. Zdroj: (14)

Obrázek č. 10: Příklad průmyslových konektorů. Zdroj: (14)

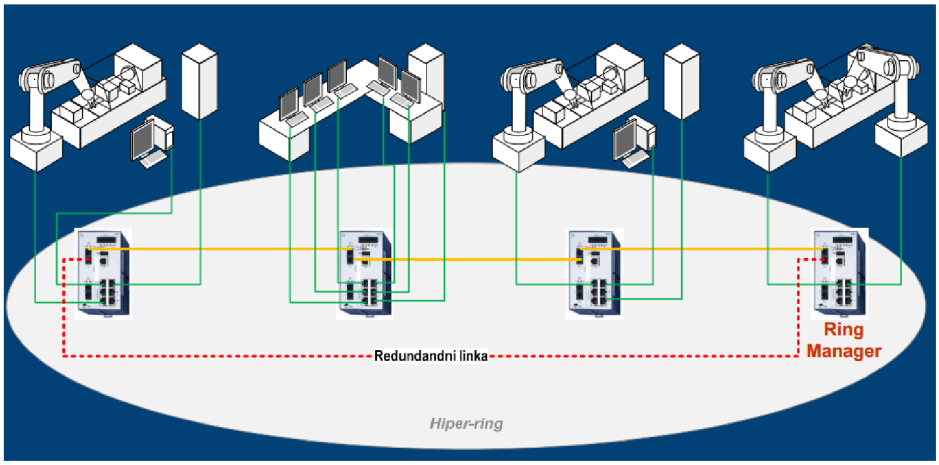
U aktivních prvcích jsou požadovány řešení v provedení pro montáž na DIN lišty, dále se požadují bezventilátorové provedení s pasivním chlazením. Vyžadují se, aby zařízení

poskytovali vysokou životnost (10-30 let). Chybět opět nesmí odolnosti vůči vlivům prostředí (koroze).

1.6.4 Topologie

Topologie v průmyslovém prostředí byla dána zařízeními, které komunikovali s dohledovým pracovištěm nejprve pomocí sériové komunikace (k propojení těchto zařízení byla používána topologie sběrnicová), poté přišel Ethernet/IP pro průmyslové použití (nejprve v topologii hvězda), na závěr při požadavku na redundanci vzniká kruhová (ring) topologie (2).

V současnosti je standardní průmyslová topologie řešena zpravidla kruhovou topologií. Koncept kruhové topologie umožňuje konstrukci sítě s vysokou dostupností prostředků síťové struktury. Pomocí funkce Ring Managera (RM) jsou oba konce páteřní lineární struktury propojeny v redundantní kruh. Úkolem Ring Managera je udržovat redundantní linku uzavřenou, pokud je struktura vedení hlavní trasy neporušena. Pokud se avšak některý segment stane nefunkčním, RM okamžitě zpřístupní redundantní linku a lineární struktura je opět funkční (16).



Obrázek č. 11: Příklad kruhové topologie s využitím RM. Zdroj:(14)

Toto řešení, lze pak rozšiřovat několika způsoby. Rozšířením topologie dosáhneme napojováním dalších kruhů (Sub-Ring) na zařízení v hlavním kruhu, napojováním kruhů pomocí linek v redundandním provedení (Couplink) nebo se v některých případech používají typické hvězdy při napojení na koncové přepínače (2).

2 ANALÝZA SOUČASNÉ SITUACE

2.1 Základní údaje společnosti

Obrázek č.12: Logo společnosti. Zdroj: (17)

Název společnosti:	AB Komponenty s.r.o.
Sídlo společnosti:	Vídeňská 101/119
	619 00 Brno
	Česká republika
IČ:	26269015
DIČ:	CZ26269015
Právní forma:	společnost s ručením omezeným

2.2 Všeobecný popis společnosti

Společnost AB Komponenty s.r.o. vznikla v roce 2001, kdy její úspěch byl založen na dlouhodobé tradici výroby komponent pro montážní linku výroby rozvaděčů společnosti ABB s.r.o. dříve známý jako EJF a.s. Nyní se společnost zabývá výrobou dílců a komponent v oblasti strojírenské výroby a elektrotechnického průmyslu. Díky různorodosti strojního vybavení poskytuje zákazníkům nejen kompletní služby v oblasti CNC obrábění kovů, ale i zpracování plechů včetně povrchových úprav. Aby si společnost udržela pozici spolehlivého dodavatele, je potřeba neustále držet krok s nejnovějšími trendy a výrobními technologiemi, stejně jak jako zefektivnit všechny

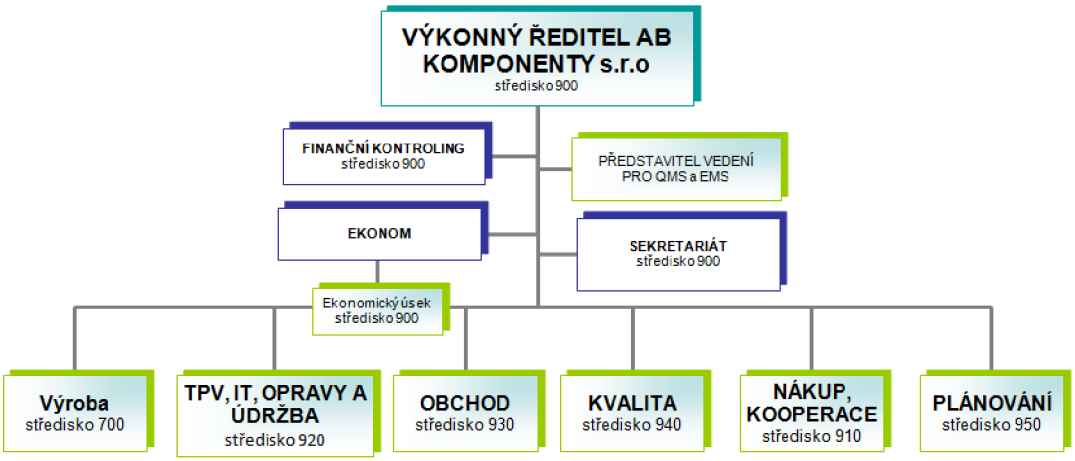
procesy pro řízení zakázek. Proto došlo k obnově výrobního parku, přechodu na nový informační systém a v roce 2003 se podařilo společnosti získat certifikaci ISO 14001 a ISO 9001. Tentýž rok začalo úspěšně fungovat i exportní oddělení a v současné době je AB Komponenty s.r.o. společností, která dokáže uspokojit zákazníky jak v České republice, tak i ve světě (17).

2.2.1 Poskytované služby

- **Obrábění** - Technicky náročné výrobky s vysokými požadavky na přesnost se vyrábí na NC a CNC obráběcích strojích. Klasické techniky jako jsou univerzální soustruhy, frézky atd. jsou vhodné pro jednoduché dílce s nižšími nároky na přesnost (17).
- **Tváření a laserové řezání** - NC technika zajišťuje i v oblasti tváření velkou přesnost. Na laserovém řezacím stroji se vyrábí tvarově složité dílce, zatím co děrovací centrum je vhodnější pro různé panely a kryty. CNC ohraňovací lisy zaručují přesnost i pro nejsložitější ohyby. Některé požadavky zákazníků je vhodnější řešit klasickými technologiemi a i v této oblasti je nabídka společnosti pestrá (17).
- **Svařování a spojování materiálu** - Kromě klasického svařování společnost nabízí bodové svařování a hydraulické nýtování. Nadstandardní nároky na kvalitu a rychlost se řeší pomocí svařovacího robota (17).
- **Povrchové úpravy** - Lakování probíhá na práškové lakovně Ideal Line. Součástí procesu lakování je i antikorozní předúprava, oplach zinečnatým fosfátem. Jelikož firma spolupracuje s několika dodavateli, v kooperaci je možné zajistit veškeré galvanické povrchové úpravy, žárové zinkování, nebo šopování (17).

2.3 Organizační struktura společnosti

Společnost je rozdělena na několik hlavních středisek (TPV, výroba, kvalita, plánování, obchod, kvalita, nákup a kooperace), které jsou organizovány do liniové organizační struktury. Hlavní zodpovědnost za vedení společnosti přejímá výkonný ředitel. Další pravomoci jsou poté delegovány na nižší úrovně organizační struktury.



Obrázek č. 13: Schéma organizační struktury společnosti. Zdroj: (18)

Každé středisko se skládá z několika podstředisek, kde jsou pak delegovány pravomoce a odpovědnost za svou činnost při dosahování firemních cílů. Pokud by jsme se bavili kupříkladu o středisku výroby, její podststřediska jsou obrobna, lakovna, NC technologie, a další. Nejvíce zaměstnanců najdeme logicky ve výrobním středisku, kde pracuje zhruba kolem 100 pracovníků. Celkový počet zaměstnanců se pak pohybuje kolem 180.

2.4 Analýza ICT společnosti

Firma ke své činnosti využívá kolem 75 počítačů připojených do sítě, z toho zhruba 30% představují notebooky. Na většině z těchto počítačů je nainstalován operační systém Windows 7. Kvůli nutné kompatibilitě s některými službami, bylo na některých počítačích potřeba starší operační systémy Windows XP. Pro potřebu práce s

dokumenty a především výkresy, společnost disponuje pěti sálovými tiskárnami, kolem desítky lokálních a s jednou plotr tiskárnou, která je využívána právě pro velkoformátový tisk. Největší množství připojených zařízení se nachází ve výrobní hale. Mimo počítače a tiskárny jsou zde připojené jednotlivé výrobní stroje. Převážně se jedná o CNC stroje, lasery a děrovací lisy. V hale také najdeme několik kamer, které jsou do sítě zapojeny. Tyto kamery sledují vnitřní i vnější prostory haly. Internet je zajištěn poskytovatelem GTS, jehož zařízení (GTS Gateway) se nachází přímo v serverovně. Do firemní sítě je taktéž možno přistupovat pomocí VPN.

2.4.1 Technická místnost (serverovna)

Samozřejmě nesmíme zapomenou na další důležité prvky zapojené do sítí - servery. Společnost využívá několik serverů, kde na každém z nich běží jedna nebo více služeb.

Mezi ten nejdůležitější server patří server pro ERP systém MS Dynamics AX. Tento ERP systém pak dále komunikuje s odděleným MS SQL Serverem.
Dalším důležitým serverem je doménový server, na kterém běží prostředí Active Directory. Active Directory je adresářová služba, která pomocí Group Policy řídí přístup jednotlivých uživatelů k různým informacím. Kvůli své důležitosti je tedy nutné, aby tento server byl duplicitně jištěn.
Jelikož je potřeba občas nějaká data sdílet s ostatními, ať už s kolegy nebo s jiným oddělením, byl pro tyto potřeby vytvořen „File server“, kam se tyto sdílená data nahrávají. Opět je zde řízen přístup skrze AD. Ostatní servery pak slouží pro služby jako DNS, DHCP, firewall apod.

Proti nečekaným výpadkům elektrické energie jsou servery zajištěny UPS záložním zdrojem. Zálohy serverů jsou spravovány formou outsourcingu.

2.4.2 Softwarové vybavení

2.4.2.1 ERP systém

Jak již výše zaznělo, hlavním informačním systémem je EPR systém Microsoft Dynamics AX. Tento software byl původně vyvíjen v Dánsku pod názvem Axapta.

Později byly společnosti vyvíjející tento produkt koupeny společností Microsoft Corporation.

Microsoft Dynamics AX je ERP systém určený pro středně velké až velké podniky. Jedná se o velice škálovatelný a funkčně bohatý produkt pro plánování všech podnikových procesů. Umožňuje optimalizaci vícestupňové výroby v několika lokacích, distribuci, řízení projektů, řízení dodavatelského řetězce, řízení vztahů se zákazníky, realizaci obchodních analýz a prodeje. Nabízí rozsáhlé funkce pro automatizaci účetních a finančních operací (19).

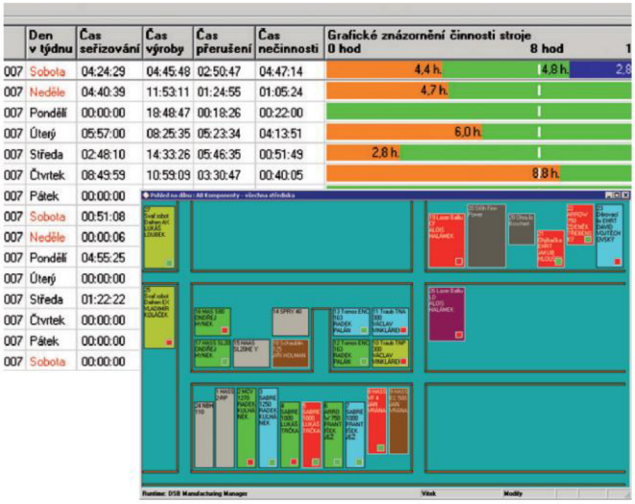
Systém je navržen tak, aby vycházel vstříc měnícím se a rozšiřujícím se obchodním a technologickým potřebám organizace. Nabízí se i možnost softwarových vylepšení a úpravy pro splnění specifických požadavků specifických obchodních procesů, pro pokrytí zvláštních požadavků společností i pro jiné účely, vždy ale s plnou izolací modifikací a kontrolou doplňků (21).

2.4.2.2 Systém pro online sběr dat a řízení výroby a skladu

Dodavatelem těchto systémů je firma Data Software Brno s.r.o. Ta se zabývá vývojem, implementací a technickou podporou informačních systémů pro řízení dodavatelského řetězce se zaměřením na skladování a výrobu (20).

DSB Logistic Manager představuje komplexní systém řízení skladů zboží a materiálu, kdy umožňuje mít kontrolu nad expiračními lhůtami, zabránit chybám či záměnám při manipulaci se zbožím a materiálem. Taktéž jako zajistit dohledatelnost původu produktů a efektivní využití skladovacích kapacit (20).

DSB Manufacturing Manager je komplexní řešení pro řízení výrobních procesů, který poskytuje kompletní dohled nad výrobním procesem a jeho optimalizaci. Monitoruje výrobní procesy v reálném čase. Umožňuje sledovat vytíženost jednotlivých strojů, porovnávat ji s plánem a statisticky vyhodnocovat, spočítat a graficky prezentovat OEE, vytvářet výrobní normy a následně sledovat plnění těchto norem (20).



Obrázek č. 14: Ukázka prostředí DSB Manufacturing Manager. Zdroj: (20)

2.4.2.3 Docházkový a mzdový systém

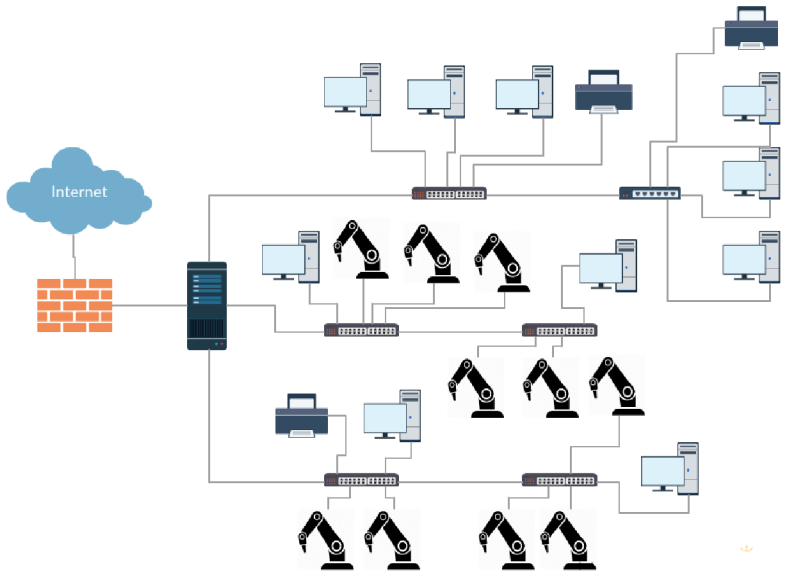
Společnost si pořídila docházkový a mzdový systém od společnosti Vema a.s. Tato softwarová společnost patří mezi přední dodavatele personálních informačních systémů v České a Slovenské republice.

2.4.2.4 Ostatní software

Jak již bylo výše zmíněno, společnost využívá operačních systému od společnosti Microsoft, jak u uživatelských stanic, tak i na serverech. Dále od společnosti Microsoft firma využívá kancelářského balíku Microsoft Office, kde je pravděpodobně nejvíce využitý program Microsoft Excel. Dále využívá software pro 3D modelování a nesmí chybět ani antivirový program. Společnost používá také několik opensourcových nástrojů.

2.4.3 ICT infrastruktura

Centrální místem celé ICT infrastruktury je serverovna. Odtud vedou tři hlavní optické trasy. Jedna z těchto tras vede do kancelářských prostor, kde se nachází jednotlivé oddělení organizace včetně technologické přípravy výroby. Od tohoto rozvaděče jsou dále taženy metalické trasy do všech místností ukončeny zásuvky RJ45. Další dvě trasy potom vedou přímo do výrobní haly, kde mimo počítačů a tiskáren jsou do sítě zapojeny i jednotlivé stroje.



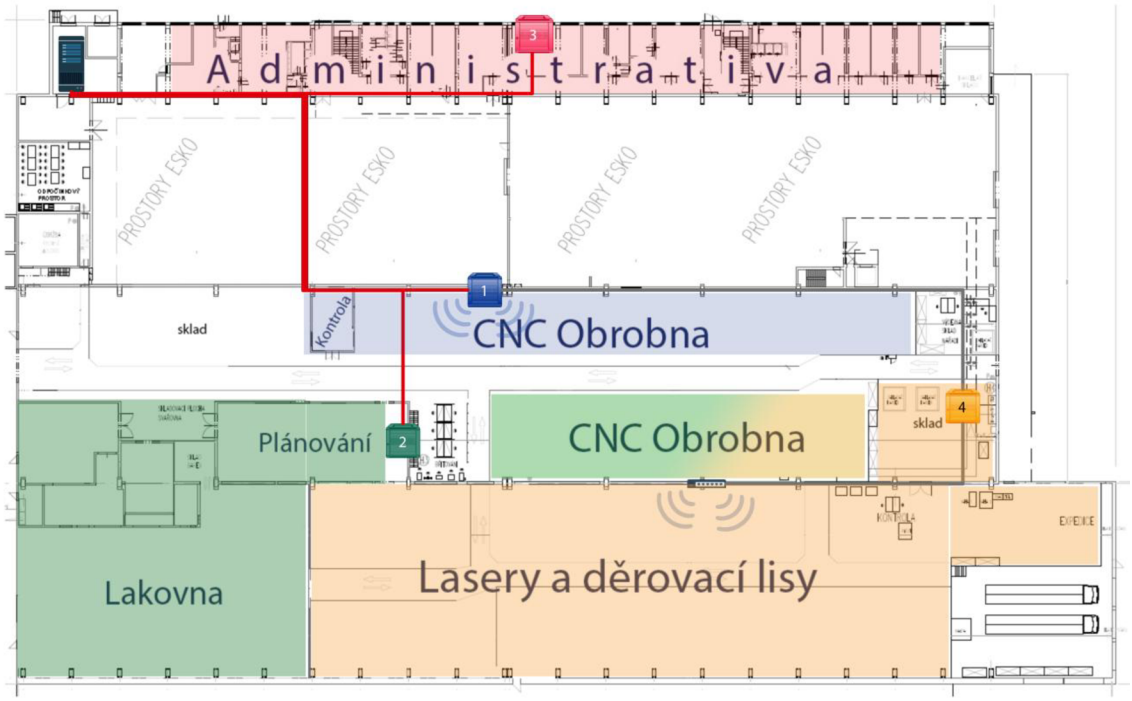
Obrázek č. 15: Schéma centrální sítě. Zdroj: vlastní

Jelikož je zde zvolena topologie sítě typu hvězda, nenajdeme tu žádné redundantní trasy.

Při stěhování do nové haly zařídit konektivitu v administrativním úseku problém ani tak nebyl, určila se místnost pro server, byla natažena optická trasa a pomocí metalických tras se zajistila konektivita rovnoměrně ve všech kanceláří. Ve výrobní hale to bylo složitější. Bylo jasné, že je potřeba zajistit konektivitu i na dílně. Avšak co se ještě moc nevědělo bylo, kde budou jednotlivé stroje umístěné a kolik těchto strojů vůbec v jednotlivých částech haly bude. To znamenalo, že navrhnout optimální vedení kabeláže bylo dosti obtížné.

Situace byla řešena tak, že kolem předpokládaných míst, kde se budou nacházet stroje, byly postaveny nosné sloupky ve výšce dvou až tří metrů, ve které je tažena silová kabeláž a pod ní, v plechovém nosníku, metalická kabeláž. Z tohoto nosníku je vždy po několika metrech vyveden datový výstup ve formě zásuvek RJ45.

Jak již zaznělo, využito je třech optických tras, které jsou na obrázku níže zvýrazněny červenou barvou. Z toho dvě z těchto tras vedou skrze prostory společnosti Esko. A právě v těchto místech by jakékoliv porušení kabelů mohlo způsobit vážné problémy pro chod celé sítě.



Obrázek č. 16: Přehled jednotlivých částí objektu a tra. Zdroj: vlastní

Z obou hlavních rozvaděčů (1,2) je pak zajištěna konektivita k určitým částem dílny. K rozvaděči 1 jsou připojeny stroje a počítače z kontroly a CNC obrobny (modrá část), rozvaděč č.2 pak poskytuje konektivitu pro plánovače, lakovnu a druhou část CNC obrobny (zelená část). Celkově se dá říci, že nejvíce zatíženými oblastmi jsou především prostory CNC obrobny. Právě proto jsou obě části CNC obroben připojený k různým rozvaděčům jinou větví optické trasy, aby se předešlo nerovnoměrnému vytížení, také bylo nutné rozšířit tuto větev o další switch. Dále je zde z rozvaděče č.1

prodloužena trasa metalickým kabelem do rozvaděče č.4, ke které jsou připojeny počítače na skladě a stroje jako lasery a děrovací lisy (oranžová část).

Většina kabeláže v hale je stavěna na stínění kabelů kvůli různým druhu rušení. Hlavní aktivní prvky jsou vybaveny záložními zdroji UPS. Hala je z větší části pokryta wi-fi signálem pro potřebu čteček čárových kódů nebo pro notebooky či tablety manažerů.

Co se týká samotných rozvaděčů, jedná se o komerční provedení, jde tedy o neklimatizované a ventilátorové rozvaděče, která slouží především jako ochrana proti mechanickému poškození.

Stejně tak jsou použity komerční provedení u aktivní prvky. Všechny důležitější prvky sice nabízejí vlastní management včetně například grafickému znázornění obsazenosti portů, ale neposkytují žádnou zvýšenou odolnost vůči prostředí.

3 VLASTNÍ NÁVRHY A ŘEŠENÍ

Cílem této kapitoly je navrhnout opatření pro minimalizaci těch nejvýznamnějších rizik. Tyto rizika zjistíme pomocí analýzy rizik. V prvním kroku je tedy nutné tuto analýzu provést. Následně bude vytvořen návrh na změnu, kterou bude nutné podstoupit k snížení jednotlivých rizik. Po návrhu potřebných změn bude pak vypracován finanční přehled ve formě rozpočtu.

3.1 Analýza rizik

Analýza rizik se sklává z několika částí - identifikace a hodnocení aktiv, identifikace a hodnocení hrozeb, vytvoření matice zranitelnosti a následné matice rizik. Metodika analýzy rizik vychází z doporučení normy ISO/IEC 27005.

3.1.1 Identifikace a hodnocení aktiv

Začneme tedy identifikací a hodnocením aktiv společnosti. Aktivum přestavuje hmotný i nehmotný majetek, který má pro společnost nějakou hodnotu.

Při hodnocení aktiv se bere v úvahu hlavně míra závažnosti možných dopadů při porušení dostupnosti, důvěrnosti či integrity daného aktiva. Pro hodnocení aktiv byla zvolena stupnice 1-5, kdy každá úroveň přestavuje jinou hodnotu (váhu) aktiv.

Hodnota aktiva	Hodnocení dopadu
1 - Velmi nízká	žádný dopad na společnost
2 - Nízká	zanedbatelný dopad na společnost
3 - Střední	potíže či finanční ztráta
4 - Vysoká	vážné potíže či podstatné finanční ztráty
5 - Velmi vysoká	existenční potíže

Tabulka č. 2: Stupnice pro hodnocení aktiv. Zdroj: vlastní

Při identifikaci aktiv určitě nejsou vybrána všechny aktiva, ale jsou vybrána ta aktiva, která jsou nejdůležitější pro společnost. Tyto aktiva můžeme rozčlenit na jednotlivé skupiny. V našem případě aktiva rozlišíme na aktiva typu dat, hardwaru, softwaru, služeb a dalších. V následující tabulce jsou pak vyobrazena ohodnocená aktiva společnosti.

Kategorie	Aktivum	Hodnota aktiva
Data	Databáze IS	3
	Osobní údaje zaměstnanců	3
	Účetnictví	3
	Zálohy dat	3
Hardware	Server	3
	ICT infrastruktura	4
	Pracovní stanice (PC)	3
Software	MS dynamics AX	4
	Výrobní IS (DSB MM)	4
Služby	Vzdálený přístup	2
	Připojení k internetu	2
Další	Budova	5
	Stroje	4

Tabulka č. 3: Ohodnocení aktiv společnosti. Zdroj: vlastní

3.1.2 Identifikace hrozeb a zranitelností

Dalším krokem je identifikace hrozeb, které mohou nepříznivě působit na aktiva společnosti. Jednotlivé hrozby se mohou vázat k jednomu nebo více aktivům. Opět je potřeba ohodnotit jednotlivé pravděpodobnosti výskytu těchto hrozeb na stupnici 1-5.

Hodnota	Pravděpodobnost výskytu hrozby
1	velmi nepravděpodobný
2	málo pravděpodobný
3	pravděpodobný
4	velmi pravděpodobný
5	téměř jistý

Tabulka č. 4: Stupnice pro hodnocení výskytu hrozby. Zdroj: vlastní

V následují tabulce je výčet jednotlivých možných hrozeb rozdělených do několika kategorií.

Hrozby	Pravděpodobnost výskytu
Přírodní hrozby	
Poškození vodou	1
Poškození požárem	2
Fyzické zničení	3
Prach, koroze	2
Dostupnost základních služeb	
Přerušení dodávky elektřiny	1
Výpadek síťových služeb	3
Výpadek serverových služeb a informačního systému	2
Výpadek internetového připojení	2
Informace	
Neoprávněný přístup do IS	2
Vnější útok	2
Zneužití přístupových práv	2
Únik důvěrných dat	2
Technická selhání	
Selhání ICT infrastruktury	4
Selhání HW	2
Přetížení některé části sítě	3

Tabulka č. 5: Ohodnocení identifikovaných hrozeb. Zdroj: vlastní

3.1.3 Matice zranitelnosti

Matice zranitelnosti přestavuje aktiva a hrozby z předchozích tabulek, kde stanovuje úroveň zranitelnosti mezi aktivem a hrozbou. Hrozba nemusí ovlivňovat všechna aktiva, ovlivňovat může jen některé a to v různých měřítkách.Stupnice zranitelnosti může nabývat hodnot od 1 do 5 (čím vyšší hodnota, tím větší zranitelnost).

V Zranitelnost	Popis aktiva	Databáze IS	Osobní údaje zaměstnanců	Účetnictví	Zálohy dat	Server	ICT infrastruktura	Pracovní stanice (PC)	MS dynamics AX	Výrobní IS (DSB MM)	Vzdálený přístup	Připojení k internetu	Budova	Stroje
	A	3	3	3	3	4	4	3	4	4	2	3	5	4
Popis hrozby	T													
Přírodní hrozby														
Poškození vodou	1				4	4	2	4					1	2
Poškození požárem	2				3	3	4	4					2	2
Fyzické zničení	3				2	2	4	3					1	2
Prach, koroze	3					1	3	2						1
Dostupnost základních služeb														
Přerušení dodávky elektřiny	1					5	5	5					2	5
Výpadek síťových služeb	3	2			2	3	4	2	4	4	5	3		2
Výpadek serverových služeb a informačního systému	2	4			2	4			4	4				3
Výpadek internetového připojení	2				2	1		3			5	5		
Informace														
Neoprávněný přístup do IS	2	3	4	3					3	4				
Vnější útok	2	3	3	3	3	4	2	3	3	3	3	4		
Zneužití přístupových práv	2	3	2	3	3	3	2	3	2	2	1		1	
Únik důvěrných dat	2	1	2	4	2				3	3	2		1	
Technická selhání														
Selhání ICT infrastruktury	4					5	4	3	4	4	4			3
Selhání HW	3					5	5	5						3
Přetížení některé části sítě	3	1				4	4				4			

Tabulka č. 6: Matice zranitelnosti. Zdroj: vlastní

3.1.4 Matice rizik

Pro výpočet míry rizika byla použita maticová metoda se třemi parametry. Výpočet se prováděl pomocí vztahu:

$$\boldsymbol{R = T \times A \times V}$$

kde **R** představuje míru rizika, **T** pravděpodobnost vzniku hrozby, **A** hodnotu aktiva a **V** zranitelnost. Před vyhotovením matice si nejdříve stanovíme hranice rizik, která určují o jak vážné riziko se jedná.

Hranice	Stupeň rizika
0 až 10	bezvýznamné riziko
11 až 20	akceptovatelné riziko
20 až 30	mírné riziko
30 až 60	nežádoucí riziko
60 a více	nepřijatelné riziko

Tabulka č. 7: Ohodnocení míry rizik. Zdroj: vlastní

Nyní nám nic nebrání v sestavení matice rizik.

V Zranitelnost	Popis aktiva	Databáze IS	Osobní údaje zaměstnanců	Účetnictví	Zálohy dat	Server	ICT infrastruktura	Pracovní stanice (PC)	MS dynamics AX	Výrobní IS (DSB MM)	Vzdálený přístup	Připojení k internetu	Budova	Stroje
	A	3	3	3	3	3	4	3	4	3	2	2	5	4
Popis hrozby	T													
Přírodní hrozby														
Poškození vodou	1	0	0	0	12	12	8	12	0	0	0	0	5	8
Poškození požárem	2	0	0	0	18	18	32	24	0	0	0	0	20	16
Fyzické zničení	3	0	0	0	18	18	48	27	0	0	0	0	15	24
Prach, koroze	2	0	0	0	0	6	24	12	0	0	0	0	0	8
Dostupnost základních služeb														
Přerušení dodávky elektřiny	1	0	0	0	0	15	20	15	0	0	0	0	10	20
Výpadek síťových služeb	3	18	0	0	18	27	48	18	48	36	30	18	0	24
Výpadek serverových služeb a informačního systému	2	24	0	0	12	24	0	0	32	24	0	0	0	24
Výpadek internetového připojení	2	0	0	0	12	6	0	18	0	0	20	20	0	0
Informace														
Neoprávněný přístup do IS	2	18	24	18	0	0	0	0	24	24	0	0	0	0
Vnější útok	2	18	18	18	18	24	16	18	24	18	12	16	0	0
Zneužití přístupových práv	2	18	12	18	18	18	16	18	16	12	4	0	10	0

Únik důvěrných dat	2	6	12	24	12	0	0	0	24	18	8	0	10	0
Technická selhání														
Selhání ICT infrastruktury	4	0	0	0	0	60	64	36	64	48	32	0	0	48
Selhání HW	2	0	0	0	0	30	40	30	0	0	0	0	0	24
Přetížení některé části sítě	3	9	0	0	0	36	48	0	0	0	24	0	0	0

Tabulka č. 8: Matice rizik. Zdroj: vlastní

3.1.5 Vyhodnocení rizik

Podle vypočtených hodnot v matici rizik vidíme, že největší slabinou jsou zejména slabiny spojené s dostupností síťových služeb a s síťovou infrastrukturou. Je tedy zřejmé, že je nutné se zaměřit především na infrastrukturu ICT. Vhodné tedy bude navrhnout takovou infrastrukturu, která poskytne co maximální dostupnost dle doporučení ISMS.

Dodávka elektrické energie je pro výrobu velmi důležitá, nicméně společnost sídlí v průmyslové oblasti, kde k výpadku velice ojediněle. Když už se nějaký výpadek objeví, jde zpravidla o plánovaný výpadek. Proto může společnost toho riziko akceptovat bez jakéhokoliv opatření. Stejně tak to platí s akceptací rizika, že se někteří zaměstnanci dostanou někam, kam by neměli a to právě díky správnému rozdělení uživatelů pomocí Group Policy v prostředí Active Directory.

3.2 Návrh infrastruktury ICS

Úkolem tedy bude navrhnout vyhovující ICS infrastrukturu s maximální dostupností, která již bude obsahovat základní bezpečnostní prvky.

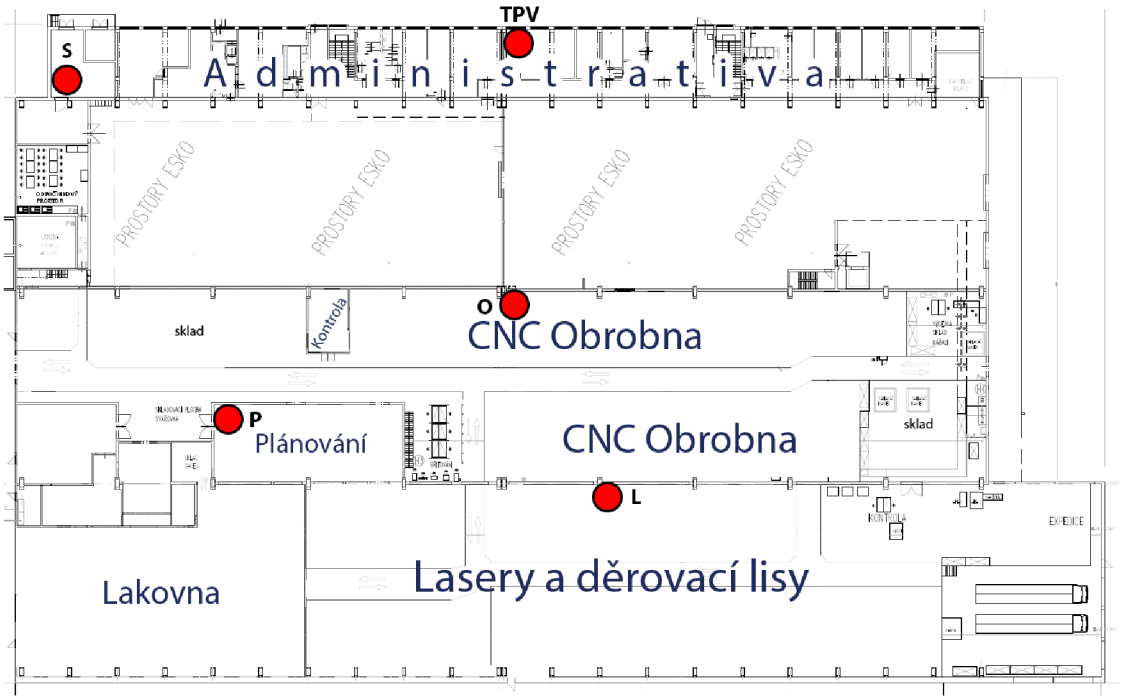
Důležitý bude výběr jednotné platformy a to včetně softwarového balíku, který bude zajišťovat centrální dohled nad celou síťovou infrastrukturou. Taktéž bude nutno zvolit správnou topologii sítě, která umožňuje zajistit redundanci včetně volby redundantních protokolů. Celý návrh se bude opírat o doporučení normy ČSN EN 50173-3, která specifikuje univerzální kabelážní systémy pro průmyslové prostory.

Je zřejmé, že společnost si nemůže dovolit na několik týdnů pozastavit výrobu „pouze“ kvůli realizaci nové infrastruktury, proto bude nutné implementovat celý projekt po etapách. To znamená, že se postupně zajistí konektivita pro každou část výrobní haly zvlášť a až ve finále, po propojení všech páteřních bodů, vznikne kruhová topologie.

3.2.1 Určení páteřních bodů

Prvním krokem návrhu tohoto řešení je volba páteřních bodů. Páteřním bodům zjednodušeně rozumíme jako místu, kde se nám dále rozvětvuje topologie sítě. Páteřní body je potřeba zvolit tak, aby k nim páteřní trasy byly realizovatelné a dostupné.

V tomto případě jsme zvolili celkem 5 páteřních bodů, z čeho 3 z nich jsou rozmístěny přímo na dílně. Všechny tyto body byli jednoduše pojmenovány pro lepší výstižnost a následují potřebu identifikace. Označením S je nazván páteřní bod serverovny, která bude středem celé topologie. Následně je v navrhnut další páteřní bod v administrativní části pod zkratkou TPV (technologická příprava výroby). Zbytek páteřních bodů se nachází na dílně pod názvy vystihující jednotlivé části výrobní haly. Písmeno O představuje obrobnu, písmeno L lasery a páteřní bod, kde se nachází mistři a jsou zde vytvářeny výrobní plány, je pojmenován písmenem P.



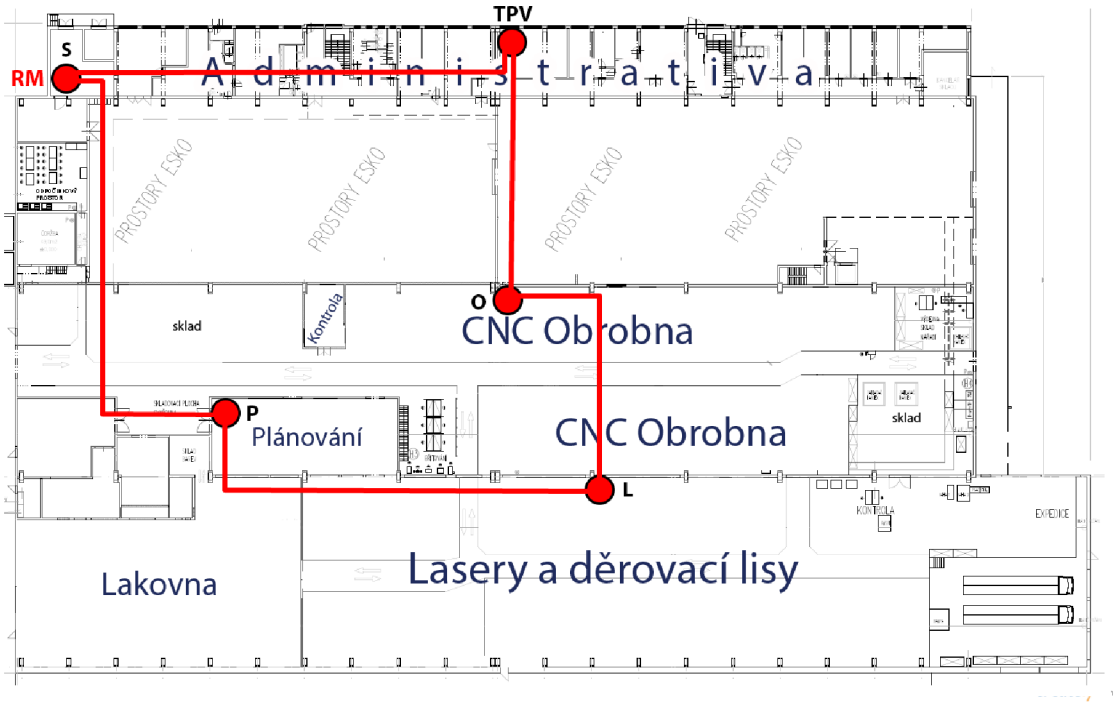
Obrázek č. 17: Určení páteřních bodů. Zdroj: vlastní

3.2.2 Návrh optických tras

Pro páteřní topologii se používá zásadně topologie kruhová, kde vzniká takzvaná topologická redundance. Pro páteřní trasy je silně doporučeno použít optické kabely. Kruhová topologie, která vznikne propojením jednotlivých páteřních bodů bude navržena tedy na optické páteři pro rychlost 1 Gb/s. V průmyslu v této době sice takovou rychlost není třeba, ale zde je hlavně potřeba uvažovat s nadhledem do budoucna, kdy může být tato rychlost využita.

Také je vhodné stanovit, kterému páteřnímu bodu bude přiřazena role Ring Managera, který pomocí watchdog paket hlídá integritu celé sítě. Logicky bude nejlepší Ring Managera zvolit v serverovně, která se nachází nedaleko od kanceláří IT oddělení.

Na obrázku níže jsou vyobrazeny jednotlivé páteřní trasy.



Obrázek č. 18: Návrh optických tras. Zdroj: vlastní

Co se týče počtu vláken a volby optického kabelu, vychází především z požadavků funkcionality. Jelikož by z již zmíněných důvodů realizace musela být zaváděna po etapách, bude v prvních stádiích dočasně řešena topologie hvězdy. A až tehdy, kdy bude

připojen i poslední páteřní segment, bude možný přechod z hvězdicové topologie na kruhovou. To znamená, že nejdříve budeme připojovat 4 segmenty.

Při určení počtu vláken pro optické trasy vycházíme z výpočtu:

$$počet\ segmentů\ \times počet\ vláken\ na\ segment + \%\ požadované\ redundance = počet\ vláken$$

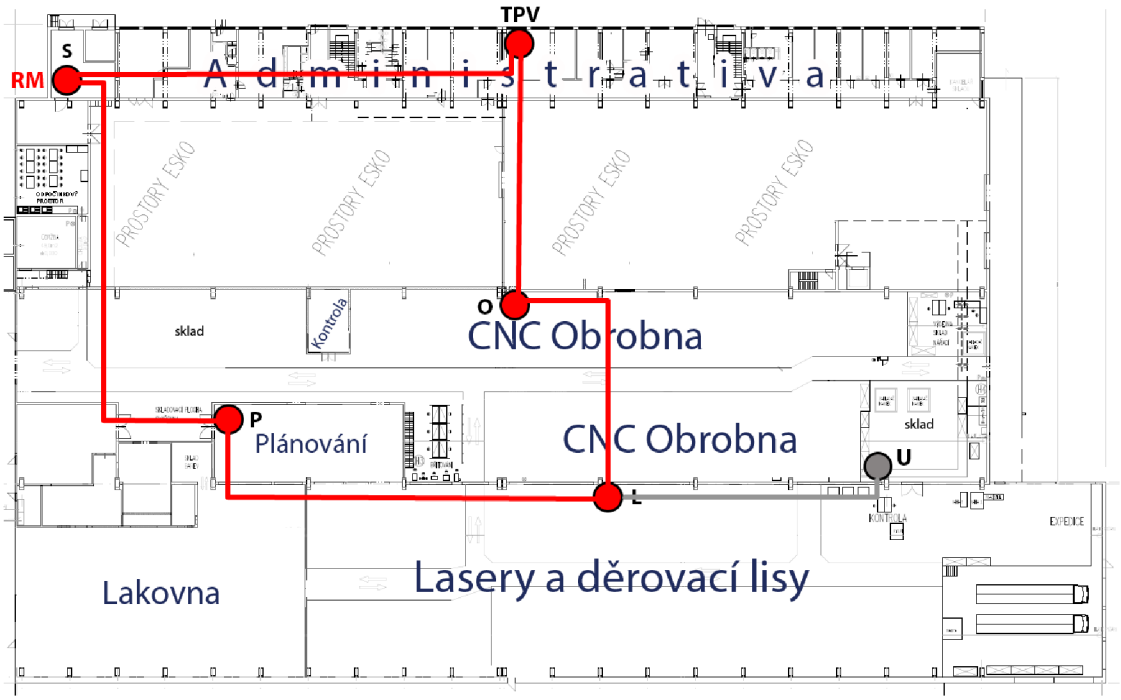
V našem případě jsou to 4 segmenty, 2 vlákna na segment a 50% redundance. Ve finále to pak vychází na 12 vláken. Jelikož nepotřebujeme zajistit rychlost větší než 1 Gb/s, vybereme univerzální multimodový kabel 12vl.50/125 v provedení OM2, který bude dostatečně stačit pro předpokládané délky segmentu. Při tažení samotné kabeláže by měly být kabely chráněné proti mechanickému poškození. To lze buď to pomocí speciálního pancéřovaného obalu a nebo pomocí různých kovových roštů či chraničeк. Jelikož by se speciálně chráněné kabely mohli dosti prodražit a očekává se, že kabely budou umístěny v dostatečné výšce, zvolila se již zmíněná druhá možnost ochrany. Umístění kabeláže může být zařízeno například pomocí využití již existujících registrů tras napájecích rozvodů a montáže optických tras k nim nebo se mohou využít například některé systémy pro vedení optických tras. Tyto systémy nabízí například firma Panduit (viz obrázek č.20).

Obrázek č. 19: Kovová chránička. Zdroj: (22)

Obrázek č. 20: Systém pro vedení kabelů. Zdroj: (23)

3.2.3 Uzlové body

Nyní se nacházíme ve stádiu, kdy jsme si navrhli páteřní body spojené optickou páteří. To byly ty nejdůležitější body, které bylo nutné připojit. Nicméně tyto body nejsou schopny pokrýt celé prostory, tudíž je potřeba navrhnout uzlové body, které budou k dispozici pro mimopáteřní požadavky. V těchto bodech budou použity stejné rozvaděče jako jsou využity v páteřních bodech.



Obrázek č. 21: Návrh uzlového bodu. Zdroj: vlastní

Z obrázku výše vidíme, že v našem případě stačilo navrhnout uzlový bod pouze jeden. Ten je umístěn v pravé části haly pod písmenem U.

Logicky je tento uzlový bod nutné připojit k páteřnímu bodu L. Předpokládá se, že v této trase bude využita rychlost o řád nižší a to znamená 100 Mb/s. K připojení můžeme použít stejný typ kabelu jako u páteřních rozvodů s rozdílem počtu vláken. Zde nám s přehledem vystačí čtyři vlákna. Bude se tedy jednat o optický kabel typu MM 4vl.50/125 (OM2). Opět se využije stejného chránění jako u páteřního rozvodu.

Požadavky na datové rozvaděče

Při výběru jednotlivých rozvaděčů je nutno počítat s tím, že se nacházíme v průmyslovém prostředí, tudíž je nutné zvolit speciální rozvaděče pro průmysl. Tyto provedení jsou odolné hlavně proti mechanickému poškození, ale je zde i zvýšená odolnost proti vodě a prachu. Díky výběru typizovaného řešení pak budou rozvaděče páteřních bodů prakticky identické s rozvaděčem uzlovým.

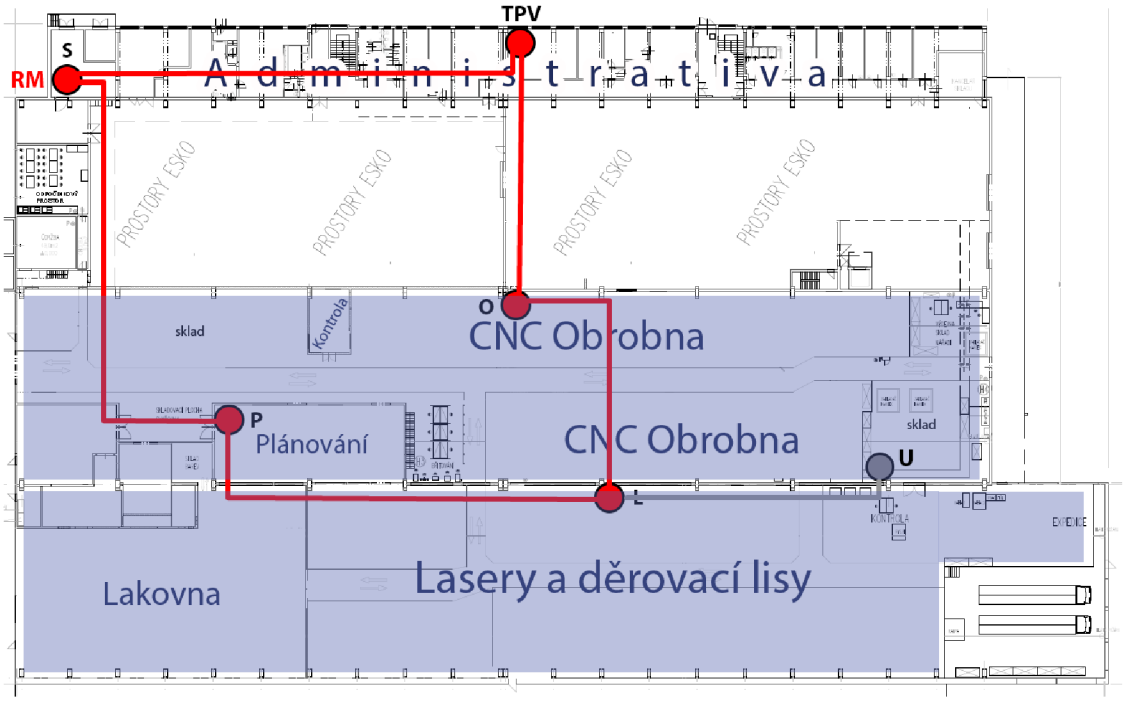
V páteřních rozvaděčích pak bude využita 19ti palcová montáž pro metalické rozvody použitím patch panelů, páteřní prvek a průmyslové záložní zdroje UPS. Dále bude také použita DIN montáž pro optický modulární rozvaděč, aktivní prvek PoE potřebný pro bezdrátové spoje a napájecí zdroj pro tento prvek.

V podružném rozvaděči budou pak stejně jako v předchozím případě připojeny metalické rozvody, průmyslový záložní zdroj UPS. Stejně tak bude využito modulárního optického rozvaděče v DIN provedení. Pokud bude potřeba, bude obsahovat i aktivní prvek PoE pro WiFi včetně napájecího zdroje.

Obrázek č. 22: Příklad průmyslového rozvaděče. Zdroj: (24)

3.2.4 Bezdrátové pokrytí (WiFi)

V dalším kroku je potřeba splnit požadavek na pokrytí WiFi technologií. Na následujícím obrázku jsou pak znázorněna místa, která jsou nutné pokrýt.



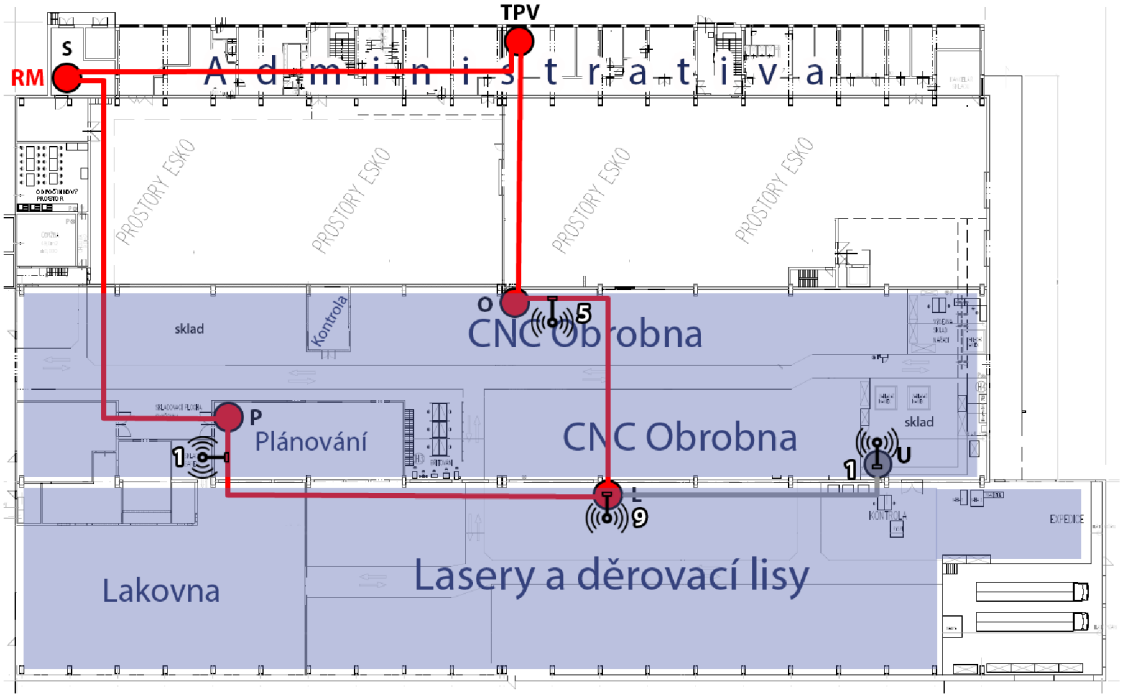
Obrázek č. 23: Vyznačení požadované plochy pokrytí. Zdroj: vlastní

Tyto plochy potřebuje mít společnost pokryta hlavně z důvodu logistiky a skladového hospodářství, kdy se pro tyto účely používají různé bezdrátové čtečky čárových kódů. Alternativně jsou bezdrátové sítě využity pro připojení zařízení manažerů jako jsou tablety a notebooky.

V první řade je potřeba určit počet a rozmístění WiFi zařízení v hale. To bude vycházet především z velikosti požadované plochy k pokrytí. K pokrytí prakticky celé výrobní haly nám bude bohatě stačit čtyři zařízení. To znamená, že umístění musí být vhodně rozvrženo.

Následně je nutné nastavit kanálové řešení u každého zařízení. Kanály je nutné nastavit tak, aby nenastal takový problém, kdy se zařízení mezi sebou „hádají“.

Proto je využito třech různých kanálu (1,5,9) rozvržených tak, aby se například kanál 1 „nepotkal“ s kanálem 1. To můžeme vidět i na obrázku, kde jsou zařízení s kanály 1 na opačné straně haly.



Obrázek č. 24: Umístění WiFi zařízení. Zdroj: vlastní

Po umístnění je pak potřeba zkontrolovat průchodnosti zařízení a někdy je také k dispozici možnost nastavení vyzařovacího výkonu. Předpokládá se, že u některých zařízení bude stačit nižší vyzařovací výkon než u ostatních.

Mezi hlavní požadavky pro výběr bezdrátových zařízení patří možnost napájení PoE. Avšak při použití tohoto prvku již nemůžeme použít optický kabel. Právě proto při připojení zařízení ať už k páteřním či uzlovým bodům použijeme metalický stíněný kabel. Opět je doporučeno využít kovové chráničky pro tyto metalické trasy. Jak je vidět na obrázku č.24, tyto trasy budou ve většině případů opravdu krátké, jelikož se zařízení nebudou nacházet daleko od páteřních či uzlových bodů. Vhodné je využít i speciální konektory. Dále je pak potřeba dodržet odstupy těchto logických vedení od silového vedení, kvůli elektromagnetickému rušení.

3.2.5 Výběr potřebných aktivních prvků

Jak již bylo zmíněno cílem celého návrhu bude vymyslet typizovaného řešení stavěné na jednotné platformě. Tento fakt se nám odrazí právě a hlavně v následující části, kdy budeme volit konkrétní aktivní prvky sítě. Je tedy potřeba vybrat dodavatele, který nabízí velké portfolio produktů. A právě takto velké portfolio nám nabízí společnost Hirschmann.

3.2.5.1 Páteřní switche

Výběr páteřních switchů vychází z několika požadavků. Je potřeba použít switch, který nabízí dostatečný počet metalických a optických portů. Dalším požadavkem bude 19ti palcové provedení. Obsahovat by měl taktéž management a podporu redundantní topologie.

Jelikož bude třeba připojit velký počet zařízení do páteřních switchů, volil se switch MACH104-20TX-F-4PoE. Ten nabízí 24 portů pro rychlost 1Gb/s, z toho jsou čtyři z těchto portů tzn. combo porty, které mohou být využity jak pro metaliku, tak pro optiku. Vybrána byla verze s PoE porty, které se můžou hodit pro bezdrátové zařízení či kamerový systémy.

Obrázek č. 25: Páteřní switch MACH104-20TX-F-4PoE. Zdroj: (25)

Tento páteřní switch je tedy v námi požadovaném 19" provedení podporuje kruhovou topologii a nabízí taktéž software pro management.

3.2.5.2 Podružný switch

Další místo, kde bude potřeba switch, je uzlový bod. Zde již nebudeme potřebovat takový počet portů jako u páteřních switchů. Z návrhu tras víme, že z páteřního bodu nám povede trasa k uzlovému bodu taktéž pomocí optického kabelu. Také bylo zmíněno, že rychlost trasy k tomuto bodu bude o řád nižší než je 1 Gb/s. Z toho

vychází, že budeme hledat aktivní prvek s optický porty pro rychlost 100 Mb/s. Nejdůležitější věc u tohoto prvku je požadavek na PoE porty, pro bezdrátové zařízení. Opět je vyžadována podpora managementu.

Obrázek č. 26: Switch RS22 s PoE porty. Zdroj: (26)

Produkt byl vybrán z řady RS22, která splňuje naše požadavky. Bohužel se mi nepodařilo najít prvek s menším počtem portů, který zároveň splňuje podmínky. Prvek je v provedení DIN a podporuje maximální rychlost 100 Mb/s.

3.2.5.3 Zařízení pro bezdrátové spoje

Dále je potřeba vybrat prvek, který bude poskytovat bezdrátové připojení. Samozřejmě základním požadavkem je opět podpora PoE napájení.

Obrázek č. 27: Zařízení BAT-R. Zdroj: (29)

Zařízení BAT-R podporuje jak pásmo 2,4 GHz, tak pásmo 5 Ghz. Jelikož se jedná o jednorádiové řešení, je potřeba si vybrat na jakém z těchto dvou pásmech bezdrátová síť poběží. Management je opět samozřejmostí.

3.2.5.4 Spider 1TX/1FX jako převodník

Pozor si musíme dávat na přechod rychlostí u optických tras. Páteřní rozvod je postavený na rychlosti větší než rychlost trasa z páteřního do uzlového bodu. To znamená, že také použita jiná vlnová délka. Tento problém se řeší pomocí převodníku a to tak, že z páteřního switche natáhneme metalický kabel do převodníku, který se postará o převod z metaliky zpět na optiku, ale už v rychlosti pouze 100 Mb/s.

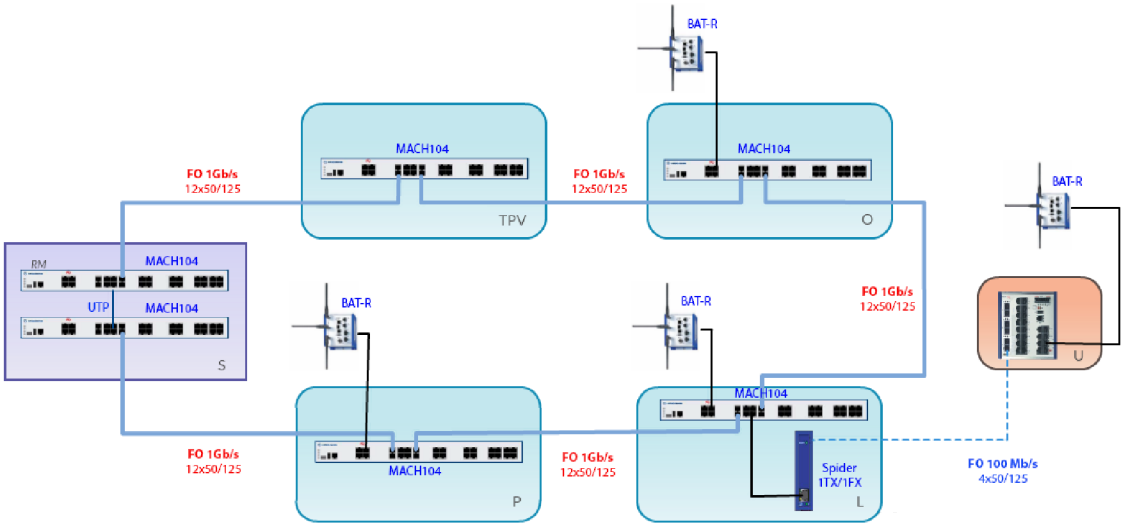
Jelikož se může stát, že převodník není schopen v nějakém případě poslat všechny pakety, ale může dojít k nějaké ztrátě, používají se jednoduché switche jako převodníky, u kterých toto riziko nehrozí.

Proto byl vybrán produkt Spider 1TX/1FX, kde jak už značení naznačuje, jeden port je určen pro metaliku a druhý pro optiku.

Obrázek č. 28: Switch Spider 1TX/1FX. Zdroj: (30)

3.2.6 Blokové schéma výsledného řešení

Dostali jsme se do bodu, kde máme úspěšně za sebou návrh páteřních, uzlových tras včetně výběru potřebných aktivních prvků, kterých bude pro potřeba pro výsledné řešení. Nyní jsme teda schopni sestavit schéma zapojení aktivních prvků.



Obrázek č. 29: Blokové schéma výsledné topologie. Zdroj: vlastní

Jak vidíme na obrázku č.18 centrem celé kruhové topologie je serverovna, kde jsou umístěny dva páteřní switche MACH104 a kde je nastavena role Ring Managera (RM).

Postupně jsou pak napojovány samostatné rozvaděče, z čehož se čtyři z nich nacházejí na páteři. Páteřní linka využívá optickou linku s rychlostí 1Gb/s. V každém páteřním rozvaděči je umístěný tedy jeden páteřní switch, který nabízí 4 PoE porty. Tyto porty jsou využity pro zařízení poskytující bezdrátové připojení ve výrobní hale. Připojení těchto zařízení je realizováno již pomocí metalických kabelů.

Navržen byl také jeden uzlový bod. Pro připojení tohoto uzlu k páteřnímu uzlu se musel použít převodník ve formě switche Spider 1TX/FX. Díky němu jsme pak schopni převést rychlost 1Gb/s na rychlost 100MB/s.

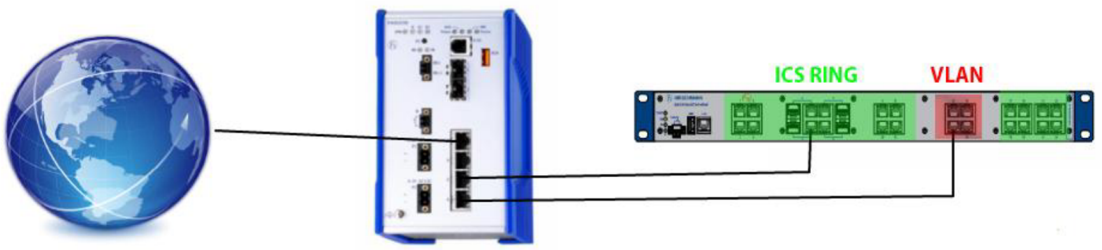
3.2.7 Logické oddělení sítí

Pokud již máme navrhnutou ICS infrastrukturu s aktivními prvky, které nabízí bohatý management, můžeme využít různé funkcionality jako je například oddělení sítí.

Oddělení sítí můžeme docílit pomocí nastavení virtuálních sítí (VLAN). To znamená, že staticky můžeme u každého portu samostatně nastavit do jakého VLANu spadá. To se může využít například v administrativní části, kde se vyberou klienti, kteří budou odděleni od průmyslové části. Touto metodou by se taktéž dala vytvořit oddělená sít, kde budou logicky napojené například pouze stroje. Využití VLANu je také možné využít pro oddělení kamerového systému.

Obrázek č. 30: EAGLE 30. Zdroj: (27)

K oddělení sítí také můžeme docílit využitím routeru na 3.vrstvě. A to například tak, že použijeme router EAGLE 30, který bude směřovat pakety do několika virtuálních sítí. To umožní i oddělení adresních prostorů s vlastním DHCP.



Obrázek č. 31: Příklad oddělení sítí na 3. vrstvě. Zdroj: vlastní

3.2.8 Management software

Velmi důležitou částí návrhové části je výběr softwarového řešení, které umožní řídit a monitorovat celou síť. Ten fakt, že máme celý návrh vyřešen pomocí jedné platformy, nám v této části obrovsky prospěje.

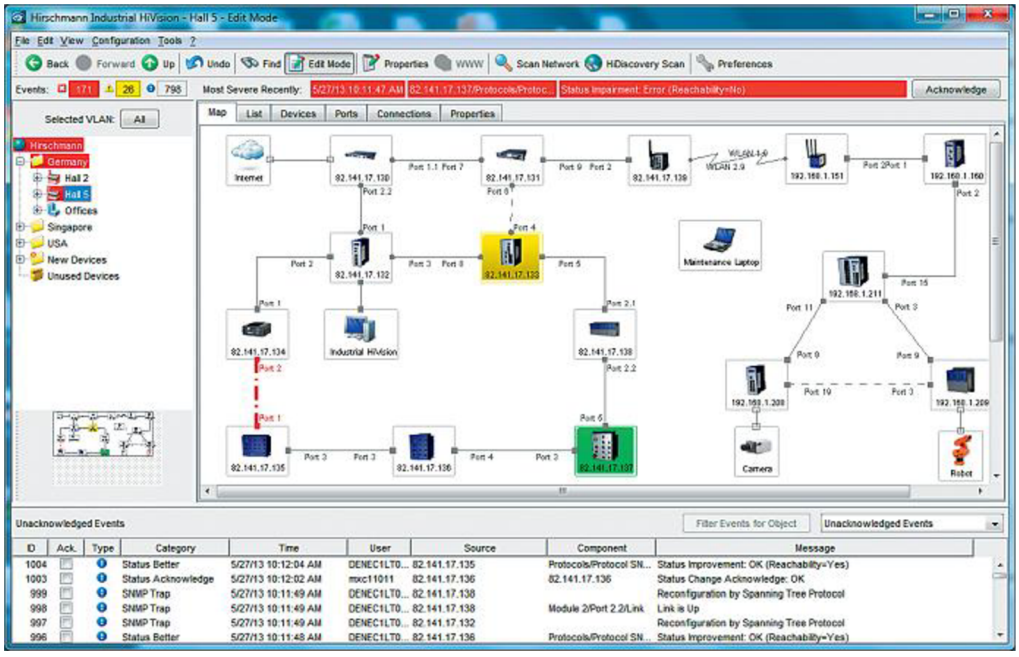
Jak již bylo zmíněno, portfolio společnosti Hirschmann je opravdu velké, takže nechybí ani produkty softwarového řešení pro management. K dispozici nabízí několik produktů:

- **HiDiscovery** - software, který umožňuje detekovat veškerý zařízení Hirschmann v sítí. Tento produkt je poskytnut volně ke stažení.
- **HiView** - tento software slouží jako jednoduchá cesta k různým grafickým zobrazením. Opět se jedná o volně dostupný software.
- **HiVision** - představuje ucelený systém pro správu a monitorování sítě a to na různých úrovních. Poskytuje celou řadu funkcí.
- **HiFusion** - umožňuje integrovat MIB databáze zařízeních třetích stran do prostředí HiVision.
- **HiMobile** - jedná se o podpůrnou záležitost, která umožňuje zobrazit různé stavy sítě na mobilním zařízení.

Logicky pak, pokud se bavíme o požadavku na nutné řízení a monitorování sítě, vybereme produkt HiVision.

Ten nabízí širokou škálu funkcionalit. Jedna z nich je funkce skenu celé sítě, kdy najde všechna připojená zařízení v sítí (včetně zařízení třetích stran) a zobrazí topologii sítě. Dokonce je u každého zařízení vidět i port pomocí kterého je zařízení připojeno k jinému. Samozřejmě celá topologie se dá následně upravovat podle potřeb, kdy je možné přidat další zařízení, barevně odlišit prvky, odlišit jednotlivé trasy dle rychlosti a podobně. HiVision nabízí opravdu mnoho vizuálních možností.

Jednotlivé události na sítí se ukládají jako event logy, které je následně možné i exportovat. HiVision nabízí i takzvaný event reporting, což znamená, že při problému na sítí se automaticky odešle email, pošle se SMS zpráva či se pouze na monitoru objeví vyskakující okno s upozorněním na problém. Zapomenout by jsme neměli ani na možnost statistických výstupy ve formě různých grafů například vytížení jednotlivých tras.



Obrázek č. 32: Prostředí HiVision. Zdroj: (28)

3.3 Ekonomické zhodnocení

V závěru by bylo vhodné sestavit jakýsi hrubý odhad rozpočtu pro celý návrh tohoto řešení. Mimo nutné komponenty, které je třeba pořídit, nesmíme zapomenout na softwarové řešení a co je obzvlášť důležité - instalační práce. Instalační práce v ICS je často největší resp. nejdražší položkou. Zahrnuje fyzické nastavení prvků, logické nastavení sítě a síťových služeb a nastavení zabezpečení ICS infrastruktury a další.

Výčet hrubého rozpočtu pak můžeme vidět v níže uvedené tabulce, kde jsou jednotlivé položky logicky rozděleny do jednotlivých skupin.

Název položky	Množství	Cena za mj	Cena celkem
Komponenty ICS infrastruktury			
Komponenty pasivní vrstvy			
Optický kabel OM2 12 vláken	260 m	45,-	11 700,-
Optický kabel OM2 4 vlákna	40 m	29,-	1 160,-
Kovová chránička	185 m	98,-	18 130,-
Odolné optické konektory	12 ks	499,-	5 988,-
Odolné RJ-45 konektory	20ks	366,-	7 320,-
Datový rozvaděč uzlových bodů	5 ks	9670,-	48 350,-
STP Cat 5	15 m	18,-	270,-
Kabelové trasy ARKYS 50x50 mm	300 m	106,-	31 800,-
Optická vana 19"/1U	6 ks	2890,-	17 340,-
Kabelový organizer 2U	5 ks	1090,-	5 450,-
Komponenty aktivní vrstvy			
Páteřní switch Mach 104 Poe	6 ks	69890,-	419 340,-
Switch RS 22	1 ks	34770,-	34 770,-
Wi-Fi prvek BAT-R	4 ks	34330,-	137 320,-
Switch SPIDER 1TX/1FX	1 ks	2990,-	2 990,-
Router Eagle One	1 ks	23950,-	23 950,-
Management software			
HiView	1 ks	zdarma	0,-
HiVision 16 nodes	1 ks	42300,-	42 300,-
HiFusion	1 ks	zdarma	0,-

Práce a instalace		
Projekt	*(5% NN)*	40 409,-
Instalace HW	*(50% NN)*	404 089,-
Instalace sítě	*(30% NN)*	242 453,-
∑ Suma		**1 495 129,-**

ceny jsou uvedené bez dph

Tabulka č. 9: Hrubý rozpočet. Zdroj: vlastní

Hrubý odhad rozpočtu pro realizaci tohoto návrhu řešení tedy celkem činí 1 495 129,- Kč. Z tabulky vidíme, že téměř polovinu rozpočtu tvoří komponenty aktivní vrstvy, kde nejdražší položkou jsou páteřní switche. S velmi podobnou částkou je pak potřeba počítat i u instalačních prací, kde je tato cena, zejména v ICS, dosti vysoká. Jelikož se předpokládá, že realizace bude probíhat po etapách, nebude tato částka potřeba nárazově, ale bude postupně rozdělena v závislosti na počtu jednotlivých etap a jejich obsahu.

ZÁVĚR

Cílem této diplomové práce bylo navrhnout průmyslové řešení ISMS ve společnosti AB Komponenty s.r.o.

V první části byly nejprve popsány základní pojmy a procesy používaní v oblasti bezpečnosti informačních systémů. Následně byl vytvořen přehled důležitých norem spjatých s problematikou ISMS. Následně byla vysvětlena provázanost modelu PDCA při zavádění ISMS. Po vysvětlení jednotlivých etapách zavedení ISMS následovala důležitá část celého procesu, tedy řízení rizik. Zde byl proveden důkladný popis obecných postupů a používaných metod. Teoretická část byla zakončena pojmem průmyslová bezpečnost, kde byla vysvětlena problematika ICS včetně jejich specifik a odlišností od IT systémů.

V druhé části byla představena společnost AB Komponenty s.r.o., kde byly uvedeny důležité informace a milníky společnosti. Následně byla provedena analýza ICT včetně analýzy infrastruktury, která nám nastínila způsoby vedení kabelážních systémů ve společnosti.

V praktické části byla nejdříve potřeba provést analýza rizik. Analýza rizik byla řešena pomocí kvalitativních metod. Nejdříve bylo nutné identifikovat a ohodnotiv aktiva, hrozby a zranitelnosti. Po sestavení rizik a hodnocení rizik bylo identifikováno nejvíce rizik spojené se síťovou infrastrukturou. Výběr opatření byl tedy zřejmý - navrhnout ICS infrastrukturu. Začalo se určením páteřních bodů a páteřních cest mezi těmito body. Po určení uzlového bodu a návrhu bezdrátového pokrytí se došlo v výběru vhodných aktivních prvků. Předběžně došlo i k návrhu logického oddělení sítí a výběru softwarového řešení pro řízení a monitorování sítě. Ve finále bylo potřeba ekonomicky zhodnotit celý návrh řešení ve formě hrubého rozpočtu.

Bylo tedy navrhnuté typizované ICS řešení stavěné na jedné platformě. Vznikla tak síť s maximální dostupností s kruhovou topologií. Návrh umožnil centrální správu nad sítí včetně diagnostické výbavy (logging, alarm,..). Celkové řešení využívá prvky specifické pro průmyslové prostředí. Cíle práce tedy byly splněny.

SEZNAM POUŽITÉ LITERATURY

(1) POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. 2005. 309 s. ISBN 80-86898-38-5.

(2) ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

(3) BÉBR, R. a P. DOUCEK. *Informační systémy pro podporu manažerské práce*.1. vyd. Praha: Professional Publishing, 2005. ISBN 80-86419-79-7.

(4) LA TAUPE. Informace a bezpečnost. *vlastnicesta.cz* [online]. 2011 [cit. 2016-05-25]. Dostupné z: http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/

(5) DOUCEK, P., NOVÁK, L., NEDOMOVÁ, L., SVATÁ, V., *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8

(6) SEDLÁK, Petr. *Normy ISO/IEC 27033: Bezpečnost síťové infrastruktury* [online]. Brno, 2013 [cit. 2016-05-25]. Dostupné z: http://www.vutbr.cz/www_base/priloha.php?dpid=75252

(7) E-ISO. ISO 27001. *eISO.cz* [online]. 2006 [cit. 2016-05-25]. Dostupné z: http://www.eiso.cz/poradenstvi/zavadeni-systemu/ISO-27001/

(8) NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. *CyberSecurity.cz - Kybernetická bezpečnost* [online]. [cit. 2016-05-25]. Dostupné z: http://*www.cybersecurity.cz/data/SRIB.pdf.*

(9) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: Český normalizační institut, 2014.

(10) CZECHTRADE. Jak volit nástroje pro snižování rizika. *BusinessInfo.cz* [online]. 2014 [cit. 2016-05-25]. Dostupné z: http://www.businessinfo.cz/cs/clanky/metody-snizovani-rizika-52919.html

(11) ČERMÁK, M., Řízení informačních rizik v praxi. 1. vyd. Brno: Tribun EU, 2009. 134s. ISBN 978-80-7399-731-1.

(12) ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009.

(13) JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů I: univerzální kabelážní systémy*. Druhé, rozšířené vydání. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5115-5.

(14) SEDLÁK, Petr. IE – Industrial Ethernet a průmyslová bezpečnost [online]. Brno, 2014 [cit. 2016-05-25]. Dostupné z: https://www.vutbr.cz/www_base/priloha.php?dpid=91602

(15) NIST. Special Publication 800-82: *Guide to Industrial Control Systems (ICS) Security. csrc.nist.gov* [online]. 2011 [cit. 2016-05-25]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

(16) JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů II: kritické aplikace*. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

(17) AB KOMPONENTY s.r.o. *AB Komponenty [online].* ©2005 [cit. 2016-05-22]. Dostupný z: http://www.abkomponenty.cz/

(18) KULHÁNEK, R. *Analytické služby Business Intelligence ve výrobní společnosti.* Brno, 2014. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky.

(19) SOFTWARE ADVICE. Microsoft Dynamics AX Software. *SoftwareAdvice.com* [online]. ©2006-2016 [cit. 2016-05-25]. Dostupné z: http://www.softwareadvice.com/accounting/microsoft-dynamics-ax-profile/

(20) DATA SOFTWARE BRNO s.r.o. DATA SOFTWARE BRNO – informační systémy pro řízení dodavatelských řetězců. *Dsb.cz [online].* ©2007-2014 [cit. 2014-05-22]. Dostupný z: http://www.dsb.cz/

(21) MAFRA. Microsoft Dynamics AX (AXAPTA). *TOPkontakt.cz*[online]. ©1999-2016 [cit. 2016-05-25]. Dostupné z: http://produkty.topkontakt.idnes.cz/p/microsoft-dynamics-ax-axapta/26729279/

(22) GUMEX. Kovové chráničky pro kabelové rozvody. *GUMEX.cz* [online]. ©2015 [cit. 2016-05-25]. Dostupné z: https://www.gumex.cz/kabelove-chranicky-a-konektory/kovove-chranicky-pro-kabelove-rozvody/

(23) PANDUIT. Fiber Routing Systems. *Panduit.com* [online]. 2015 [cit. 2016-05-25]. Dostupné z: http://goo.gl/XW2FvG

(24) KASSEX. Industrial EtherNet Cabling. *Kassex.cz* [online]. ©1995-2009 [cit. 2016-05-25]. Dostupné z: http://www.kassex.cz/produkty/panduit/industrial-ethernet-cabling

(25) BELDEN. MACH 104 Mouting Instuction. *Beldensolutions.com* [online]. 2014 [cit. 2016-05-25]. Dostupné z: https://www.e-catalog.beldensolutions.com/download/managed/pim/6b905baf-bc07-45f7-b5b5-08adecf2d882/Anl_MACH104_07_0714_en.pdf?type=attachment

(26) BELDEN. Compact OpenRail Fast Ethernet PoE switch 8-25 ports. *Beldensolutions.com* [online]. 2015 [cit. 2016-05-25]. Dostupné z: https://goo.gl/b22YyL

(27) BELDEN. Configurable Gigabit Industrial Firewall System. *Beldensolutions.com* [online]. 2015 [cit. 2016-05-25]. Dostupné z: https://goo.gl/z176wE

(28) GAE. Hirschmann Industrial HiVision Network Management System. *Gae.co* [online]. 2013 [cit. 2016-05-25]. Dostupné z: http://www.gae.co.id/detail/hirschmann-industrial-hivision-network-management-system-507

(29) BELDEN. Compact OpenBAT-R. *Beldensolutions.com* [online]. 2015 [cit. 2016-05-25]. Dostupné z: https://goo.gl/lti0NU

(30) BELDEN. Spider 1TX/1FX. *Beldensolutions.com* [online]. 2015 [cit. 2016-05-25]. Dostupné z: https://goo.gl/xmlbZX

SEZNAM OBRÁZKŮ

SEZNAM TABULEK