Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

ZABEZPEČENÍ AUTOMATIZACE ŘÍZENÍ INTELIGENTNÍCH PRŮMYSLOVÝCH ZAŘÍZENÍ

Bakalářská práce

Autor: Miloš Etlík
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Mgr. Josef Horálek Ph. D

Hradec Králové Březen 2021

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

Miloš Etlík

V Hradci Králové dne 19.4.2021

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, své rodině a pracovnímu kolektivu za podporu během celého studia.

Anotace

Cílem bakalářské práce je návrh zabezpečení automatizace řízení inteligentních průmyslových zařízen. Realizovaná zabezpečení budou implementována na vznikající průmyslové síti pro společnost Freudenberg Sealing Technologies s.r.o. Úvodní část práce je zaměřena na popis prvků, které se momentálně nachází ve společnosti Freudenberg Sealing Technologies s.r.o.
a na prvky, které budou použity pro praktické připojení do průmyslové sítě za účelem kontroly a nasezeni systému SCADA. Práce se zaobírá protokoly, které jsou momentálně ve společnosti na strojích používány a které je nutné do sítě zakomponovat. Závěrečná část práce je věnována praktickému návrhu bezpečnostních opatření. V práci je uvedeno, jak by se mělo postupovat při zabezpečení sítě a jak by měl probíhat budoucí návrh takové sítě. Tento návrh bude součástí bakalářské práce.

Annotation

The aim of the bachelor's thesis is to design the automation of the management of intelligent industrial devices. Realized security will be implemented on the emerging industrial network for Freudenberg Sealing Technologies s.r.o. The initial part of the work focuses on the description of the elements currently in the company Freudenberg Sealing Technologies s.r.o. and on the elements that will be used for practical connection to the industrial network in order to control and find the SCADA system. The work looks at the protocols currently in use in society on machines, which need to be integrated into the network. The final part of the work is devoted to the practical design of security measures. The work outlines how network security should be handled and how the future design of such a network should be handled. This proposal will be part of the bachelor's thesis.

Klíčová slova:

Profinet, Profibus , Průmyslová síť, zabezpečení, kybernetický útok

Keywords:

Profinet, Profibus, Industrial Network, security, cyber attack

Obsah

Seznam tabulek

Seznam obrázků

1 Úvod

V nastupujícím trendu pro průmysl 4.0 jsou hojně nasazovány systémy SCADA (Supervisory Control And Data Acquisition) v mnoha moderních průmyslových odvětvích, jako výroba, doprava, energetika a jiná. SCADA systém propojuje více technologií k zajištění monitorování, zpracování a shromažďování dat, stejně jako vzdálené ovládání technologií. SCADA software slouží k monitorování a ovládání automatizovaných procesů, nejedná se o kontrolní systém, ale spíše o úroveň dohledu. Jde o softwarový balíček, který je umístěn na vrcholu hardwaru, a který je propojen na PLC nebo jiný komerčních hardwarový modul, jedná se o vývojové prostředí, které umožňuje vývoj pro vizualizaci řízení či sběr dat. SCADA systém dnes nalezneme na řadě míst prakticky kdekoliv (elektrárny, řízení dopravy, úpravny vod, supermarkety, domov a jiné). Základem každého systému SCADA je rozhraní HMI (Human Machine Interface – rozhraní mezi strojem a člověkem), který umožňuje uživatelům ovládání stroje a zařízení. SCADA software získává informace převážně pomocí OPC serveru, který dostává informace například z PLC (Programmable Logic Controller). [1][2][3]

Vzhledem ke komunikaci systémů SCADA pomocí protokolů TCP/IP, a propojení na podnikové komunikační sítě je důležité zabezpečení těchto systémů a komunikačních protokolů. Možnost ovládání SCADA za využití vzdáleného přístupu je nutné a velmi důležité tyto systémy chránit proti kybernetickým útokům, a to jak ze strany přístupu uvnitř průmyslové sítě, ať už úmyslného či neúmyslného případného poškození, tak zejména z vnější strany průmyslové sítě proti kybernetickému útoku k ovládání zmíněného SCADA systému či odcizení citlivých dat. [2][3]

Moje bakalářská práce se zabývá problematikou Profinet sítě a jejím zabezpečením, která je jedním z hlavních komunikačních sběrnic určená pro řídicí systémy v oblasti průmyslové automatizace. Profinet standard je vystaven na základech průmyslového Ethernetu. Tato technologie je podporována řadou výrobců a využívána v řadě průmyslových odvětví, jako je např. automobilový průmysl, strojírenství nebo potravinářský průmysl.

2 Systémy SCADA

2.1 Systém SCADA

SCADA (Supervisory Control And Data Acquisition) je vizualizační systém, který je schopen zajišťovat sběr dat, zpracování a prezentaci dat během procesů. Systém pracuje v reálném čase, kde získaná data posílá na centrální PC pro jejich zobrazení a následné zpracování. SCADA není plnohodnotný řídící systém, jedná se spíše o dohled nad daty. Systém funguje nad řídícím systémem například PLC (logický automat) nebo jiného hardwarového zařízení. Systém za pomoci komunikačních sítí je možné ovládat vzdáleně prakticky odkudkoliv (notebook, telefon). Tyto funkce usnadňují řízení rozsáhlých systémů například elektráren či jiných odvětví, kde operátor může reagovat na vzniklé situace. SCADA systém sbírá informace z různých zdrojů jako například databází, informačních systémů, snímačů, PLC a jiných. Systém SCADA se skládá z těchto částí: [7][6][5]

- Centrální SCADA
- Komunikační síť
- RTU (Remote Terminal Units)
- Čidla a akční členy

2.2 Vývoj SCADA

SCADA (Supervisory Control And Data Acquisition) ve většině publikací se autoři odkazují na 60. léta jako počátky používání systémů SCADA. V této době začalo být žádoucí sledování a řízení průmyslových a jiných procesů, což vedlo k hledání řešení, jak tyto požadavky splnit. SCADA systém je obecně monitorovací a kontrolní zařízení v různých oblastech průmyslu jako například kontrola vodního a odpadového hospodářství, energetických rozvoden a elektráren, rafinérií a jiných systémů.

1. Generace – ostrovní systémy
   - Izolované jednoúčelové
   - Centrální podnikové
2. Generace – distribuované systémy
   - Propojení větších počtů menších stanic (uzavřené)
   - Stanice mají specifické funkce

3. Generace – síťové systémy
    - Použití otevřených standardizovaných komunikačních protokolů
    - Propojení stanic
4. Generace – „internet of things“
    - V síti internet propojení takřka všeho
    - Cloudové služby

V prvních fázích systémů SCADA, před objevem tranzistorů, bylo klíčem pro komunikaci mezi vzdálenými systémy (například úpravny vod atd. telefonní vedení). Na základě vývoje telefonních reléových systémů a kódovacích schémat koncem 50. let bylo umožněno Westinghouse and North Electric Company vyvinout kontrolní systém Visicode, což je považováno za začátek systémů SCADA. [4].

Další milník ve vývoji systémů SCADA byl spjat s vývojem polovodičových součástek, kdy se začaly používat minipočítače využívající 8bit nebo 16bit procesory. To vedlo vývoj k možnosti provádění operací, které byly do té doby prováděny z ovládacích panelů. Tyto systémy umožnily funkce jako skenování dat, sledování stavů, alarmové hlášení a i zobrazení dat. [5]

S vývojem prvního PLC, které vyvinula společnost Bedford Associates a který měl označení 084 nebo Modicon, se vývoj systémů SCADA rozšířil o různé další funkce dohledové kontroly, které mohly pracovat v reálném čase, více efektivně a spolehlivě.[5][4]

Třetí generace systémů SCADA přišla s vývojem síťových systémů, která byla velmi podobná druhé generaci s rozdílem umožňujícím komunikaci a orientaci systémů SCADA na otevřenou architekturu oproti prodejci upřednostňované uzavřené a chráněné prostředí komunikačních možností systému. Komunikace byla založena na otevřených protokolech namísto uzavřených LAN. [4][5][6]

2.3 Využití SCADA

SCADA systémy jsou využívány ve všech sektorech, kde je nutno sbírat data a dohlížet na správný průběh dějů, jako jsou: energetika (elektrárny, teplárny, rozvodny, výměníkové stanice a jiné), výroba (výrobní linky, hutě, chemické provozy, balící linky, skladové systémy), technologie budov (vzduchotechnika, zabezpečení, docházkové systémy), ekologie (emisní monitoring, čističky odpadních vod) a mnoha dalších.

SCADA systémy jsou dnes mnohem dostupnější než v minulosti, a proto pronikají také do dalších oblastí mimo průmysl – například do rodinných domů a stávají se také nástrojem technologických nadšenců z různých oborů.[6][7]

2.3.1 Příklady systémů SCADA

Je mnoho firem a softwarů, které se vizualizací a sběrem dat zabývají. V průmyslu 4.0 je vizualizace procesu nezbytná, což otevírá cesty pro další výrobce.

2.3.1.1 InTouch software

Systém InTouch je produktem skupiny Wonderware s názvem FactorySuite. Podle informací v [10] jde o software, který používá jedna třetina všech průmyslových světových zařízení pracujících se systémy typu SCADA. Jde o uživatelsky přívětivé prostředí s velkým množstvím grafických prvků a jejich snadnou implementaci do provozu. Běží na všech platformách od Windows 7, včetně MS Windows Server 2008 a vyšší a je možné jej připojit k jakémukoliv průmyslovému automatizačnímu řídícímu zařízení. [9]

Software InTouch disponuje rozsáhlou nabídkou propojení s OPC servery, PLC a RTU od skoro všech největších distributorů na světě. Nevýhodou softwaru InTouch je, že jde o placený software. [10]

2.3.1.2 Control Web

SCADA systém Control Web je od české společnosti Moravské přístroje a.s. Control Web v7 verze disponuje jednoduchým prostředím pro vývoj aplikačních programů a současně se také snaží o snadný přístup k automatizační technologii. Síla designérových programů je v detailnosti vykreslování procesu i ve 3D. Jsou tedy názorněji vidět například poruchy a alarmy. Dále jsou podporovány internetové protokoly IPv6 a IPv4. Control web obsahuje nástroj, který umožňuje volbu mezi dvěma odlišnými způsoby běhu aplikace. První aplikace jsou aplikace reálného času, což je hlavní princip SCADA. Další jsou ale aplikace, které jsou řízené změnou dat (Data driven). V data driven aplikaci systém sám aktivuje přístroje, pokud se změní datové elementy, které přístroj používá. [11]

2.3.1.3 Simatic WinCC

WinCC je založeno na kooperaci s databází (MS SQL Server), do nichž se ukládají konfigurační i archivní data. K datům lze přistupovat metodami ODBC (Open Data-Base Connectivity) a SQL (Structured Query Language). Jako skriptovací jazyk je zde použit jazyk C, nově doplněný

o VisualBasic. Lze za pomocí nadstavby WinCC/WebUX, využít možnost vzdáleného přístupu k aplikaci vytvořené ve WinCC. Zpřístupnění aplikace na dálku je využito u mobilních telefonů, tabletů, ale i PC. Tato aplikace pracuje v prostředí webového prohlížeče využívajícího HTML5. Pro sledování efektivity výroby je vytvořena nadstavba WinCC/Perfomance Monitor. Pro potřebu dlouhodobě uložených dat, má společnost nadstavbu Simatic Process Historian. Simatic Process Historian je databáze přímo vytvořená od Siemens. Tato nadstavba umožňuje sběr obrovského množství dat z několika projektů WinCC najednou a současně jejich dlouhodobé uložení. [12, 13]

2.3.1.4 Iconics

SCADA software Iconics je znám, pod názvem GENESIS64, síla tohoto software spočívá v grafické stránce vizualizačních oken. Je zde podporována grafika ve 2D i ve 3D. Iconics nabízí balíčky
pro analýzu dat, pro sledování alarmů a další standartní balíčky. Pro celosvětové společnosti je nabízeno rozšíření EarthWorXTM, jedná se o real-time vizualizaci zařízení rozprostřených po světě. Rozšíření zvané FDDWorXTM je určeno pro analýzu dat pomocí prediktivní analýzy. Tato analýza slouží k zabránění poškození zařízení nebo k ušetření výrobních nákladů. Když už k poruše systému dojde, je situace srovnána se situacemi, které nastaly v minulosti, což umožňuje rychlejší opravu chyb. Díky úzké spolupráci s Microsoft a síti uživatelů po celém světě, patří firma Iconics mezi hlavní distributory SCADA na světě. [14, 15]

2.3.1.5 TIRS.NET

SCADA systém od společnosti CORAL s.r.o. je využíván napříč Českou republikou. Umožňuje standartní funkce SCADA, jako je komunikace a sledování technologie, získávání dat, zpětné zapisování a řízení technologie. Obsahuje uživatelsky přívětivou vizualizaci, zobrazování alarmů, trendů, ukládání dat do databází a export obrázků, grafů a tabulek. Tento systém SCADA má vlastní komunikační protokol s příslušnou technologií implementovánu přímo v sobě. Veškeré komunikační možnosti a funkce jsou plně v režii tvůrců SCADA systému. [16]

2.3.1.6 Ignition SCADA

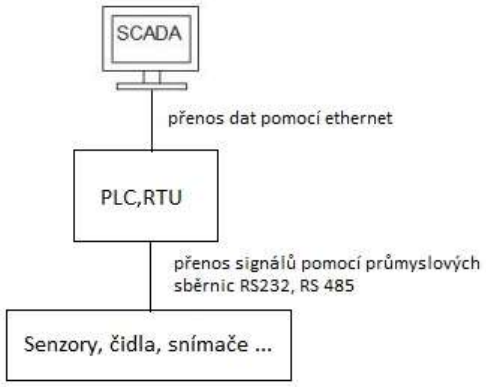
Ignition SCADA software je od společnosti Inductive automation. Mezi hlavní přednosti tohoto systému oproti konkurentům patří cena. Software Ignition je první skutečně univerzální platformou průmyslových aplikací pro připojení všech dat, návrh a nasazení průmyslových aplikací v rámci podniku bez omezení. Skládá se z platformy Ignition a modulů Ignition, které přidávají výkonnou funkcionalitu a umožňují vytváření prakticky

jakéhokoli druhu průmyslové aplikace včetně SCADA, MES, IoT, hlášení, alarmování a dalších. Ignition lze rozšířit přidáním plně integrovaných softwarových modulů, protože Ignition je modulární platforma. Všechny moduly jsou připojitelné za provozu, takže je lze instalovat, odebírat a upgradovat, aniž by to jakkoli ovlivnilo provoz.

Ignition je kompatibilní s více platformami, může běžet na Windows 10 a Windows Server 2016 a 2019 i na Linuxu a macOS. Ignition může běžet na jakémkoli zařízení včetně počítačů, notebooků, serverů, tabletů, smartphonů, vzdálených polních zařízení, a dokonce i Raspberry Pi.

Podporuje databáze SQL, programovací jazyk JAVA a skriptovací jazyk založený na PYTHON. Aplikace lze provozovat jako desktop aplikace nebo za pomocí webového prohlížeče s podporou HTML5.

2.4 Komunikace SCADA



Obrázek 1 : Hierarchie SCADA [Zdroj: Vlastní autorovo kreslení]

Komunikace v hierarchii SCADA je složitá a odlišná u různých výrobců. Můžeme ji rozdělit do dvou úrovní

- fyzická vrstva
- komunikační vrstva

Fyzická vrstva je průmyslová sběrnice. Na úrovni senzorů a PLC (RTU) se stále používají sběrnice RS-232, RS-485. [7] V případě RS-485 jde o kroucenou dvoulinku s vysokým dosahem až 1,2 km. Pro RS – 485 může být použita dvojlinka, druhým typem jsou dvě dvojlinky. Při použití dvojlinky je komunikace vedena v obou směrech a je nutné,

aby vysílač signálu věděl, jakým směrem a kdy může vysílat. Při použití dvou dvoulinek je komunikace zajištěna v každém směru zvlášť. U RS-232 je použita dvojlinka reprezentovaná napěťovými úrovněmi vzhledem k zemi. U tohoto zapojení signál vyžaduje společnou zem, z toho důvodu je omezen na délce max. 60 metrů. Spojení RS-232 je hlavně pro komunikaci lokálních zařízení. Tento typ linek se také používá z důvodu nízké náchylnosti k rušení v porovnání např. s Ethernetem. Využívá se hlavně při komunikaci PLC a akčních členů.[8] [17]

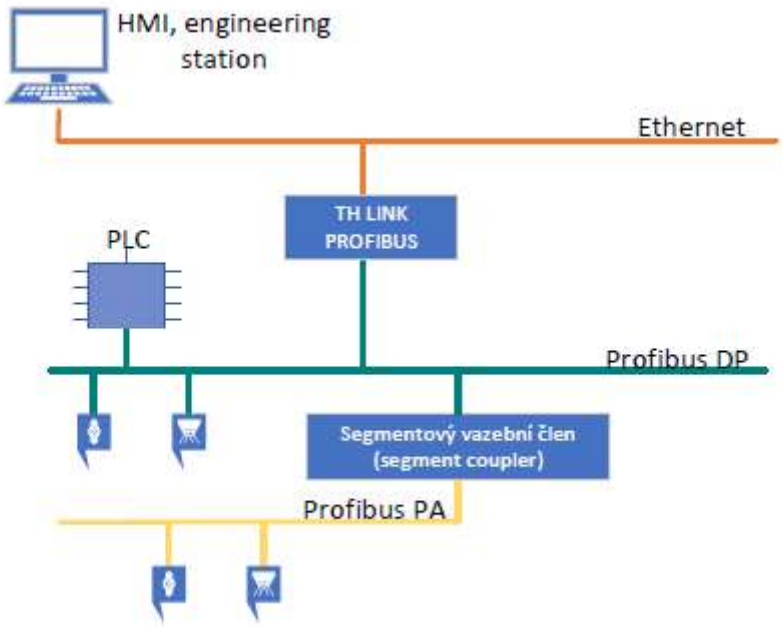
Průmyslový Ethernet se používá na úrovni SCADA tzn. komunikace mezi PLC-PC a dále pak mezi databázemi a dalšími zařízeními v síti. Od vzniku standartu průmyslový Ethernet, bylo vyvinuto více variant řešení jeho fyzické vrstvy. Původně koaxiální kabely byly nahrazeny kroucenými páry s vyšší přenosovou rychlostí, až 1000 Mb/s. Téměř většina níže popsaných komunikačních protokolů využívá standartu Ethernet. [7, 8]

2.5 Profibus

Profibus je standart pro komunikaci pomocí Fieldbus. Přenos probíhá pomocí sériové linky RS-485 nebo optickým vláknem. Profibus se dělí na dvě varianty a jeho použití je :

- **Profibus PA** – pro automatizaci procesů, monitorování zařízení prostřednictvím systému řízení procesů
- **Profibus DP –** pro decentralizované periférie, k ovládání senzorů a aktivních prvků pomocí centrálního PC

Na obrázku je standartní zapojení využívající Profibus DP a Profibus PA. K propojení Profibusu a Ethernetu je využito zařízení TH link Profibus jako převod mezi standardy.[25][1][26]



Obrázek 2 Zapojení Profibus DP a Profibus PA [Zdroj 25]

2.5.1 Bezpečnost

Pro řízení přístupu na linkovou vrstvu je použit FDL (Fieldbus Data Link), který používá hybridní metodu přístupu, možné schéma viz obr. 1.15, kombinující Master – Slave komunikaci a předávání tokenu. Token definuje, jaká stanice může obsadit sběrnici. Dále zajišťuje, že nedojde ke stavu, kdy komunikují dvě stanice současně. Tímto ovšem není zajištěna bezpečnost, může dojít k Traffic Injection, popřípadě DoS [1].

Na aplikační vrstvě jsou definovány tři vrstvy přístupu:

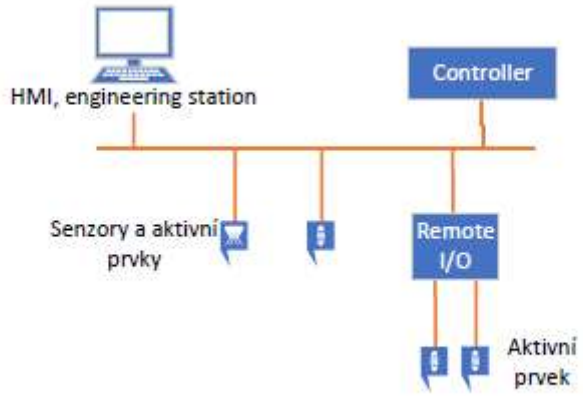
- DP-V0 – výměna periodických dat.
- DP-V1 – výměna komunikace bez pevné periodicity.
- DP-V2 – asynchronní komunikace prostřednictvím vysílání zpráv.

Dokumentace protokolu neuvádí na této vrstvě žádné přídavné zabezpečení, je nutné využít jiné mechanismy [20]. Pouze lze pro počáteční fázi přiřazení zařízení využít TCP jako transportní protokol. Pokud tím nebude dotčena činnost systému, lze použít přídavné prvky zabezpečení. Z důvodu absence autentizace a dostatečného zabezpečení protokolu je nutné, aby byl síťový provoz izolován od zbytku sítě.[33, 32, 31]

2.6 Profinet

Profinet je standard založený na Profibusu, který používá pro komunikaci fyzické rozhraní Ethernet. Má opakovací systém založený na předávání tokenů. Pro přenos dat nabízí stejné funkcionality jako TCP/IP, tím umožňuje využívat bezdrátové aplikace a vysokorychlostní

přenos dat. Zařízení podporující tento protokol jsou orientována na spolehlivost a komunikaci v reálném čase.



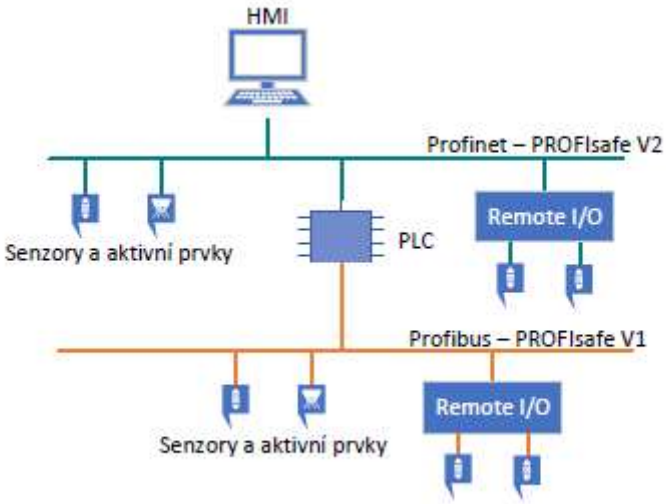
Obrázek 3 : Zapojení profinet [Zdroj 25]

2.6.1 Bezpečnost

Absence autentizace vyžaduje, aby veškerý provoz byl izolován od zbytku sítě. Dále je doporučeno provádět autentizaci veškerých zařízení v síti a využívání šifrované komunikace. Je doporučeno nastavit zabezpečení perimetru na nejstriktnější možné, za účelem zabránění neautorizovaného přístupu do sítě nebo podezřelého provozu. [33, 32, 31]

2.7 PROFISafe

PROFIsafe je bezpečnostní protokol popsán v normě IEC 61784-3. PROFIsafe lze označit za funkční bezpečnostní komunikační profil [21]. Existují dvě verze tohoto protokolu. První verze (V1) byla zaměřena pro provoz s protokolem Profibus. Druhá verze (V2) je rozšířená o funkcionality Profinet. Na obr. 1.17 je zobrazeno typické zapojení při využití PROFIsafe. Z důvodu, že se jedná o protokol pracující nad komunikačním protokolem Profibus/Profinet, tak je zapojení totožné v porovnání s těmito protokoly.



Obrázek 4 : Zapojení ProfiSafe [Zdroj 25]

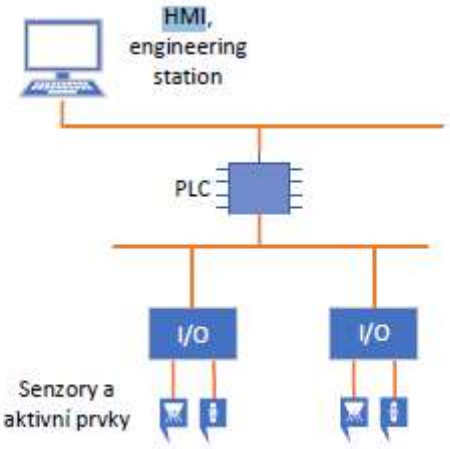
2.7.1 Bezpečnost

K přenosu datových jednotek jsou využívány kontejnery. Jeden kontejner je složen z dat o maximální délce 12/123 B, kontrolního bajtu a CRC2 o délce 3 B odpovídajících 12 B datové části, resp. o délce 4 B odpovídajících 123B datové části. Maximální délka závisí na vybraném operačním módu. Jeden Profinet rámec může obsahovat i více PROFIsafe kontejnerů. Cílem tohoto protokolu je především detekovat chyby v komunikaci. Je rozlišováno několik chyb (Corruption, Unintended repetition, Unacceptable delay, Incorrect sequence, Loss, Insertion, Masquerade, Addressing). CRC2 je generováno na základě CRC1, dat, statusu/kontrolního bajtu a pořadového čísla (Corresponding Consecutive Number). Pořadové číslo je využíváno jako měřítko pro řešení některých druhů chyb, je například používáno pro sledování zpoždění mezi přenosem a příjmem dat. [25][1][26]

2.8 PowerLink Ethernet

Ethernet Powerlink je protokol pro standardní Ethernet v reálném čase. Jedná se o otevřený protokol spravovaný skupinou Ethernet POWERLINK Standardization Group (EPSG). Představila ji rakouská automatizační společnost B&R v roce 2001.

Tento protokol nemá nic společného s distribucí napájení pomocí ethernetové kabeláže nebo napájení přes Ethernet (PoE), komunikace po elektrické síti nebo kabelu Bang & Olufsen PowerLink.



Obrázek 5: Zapojení PowerLink Ethernet [Zdroj 25]

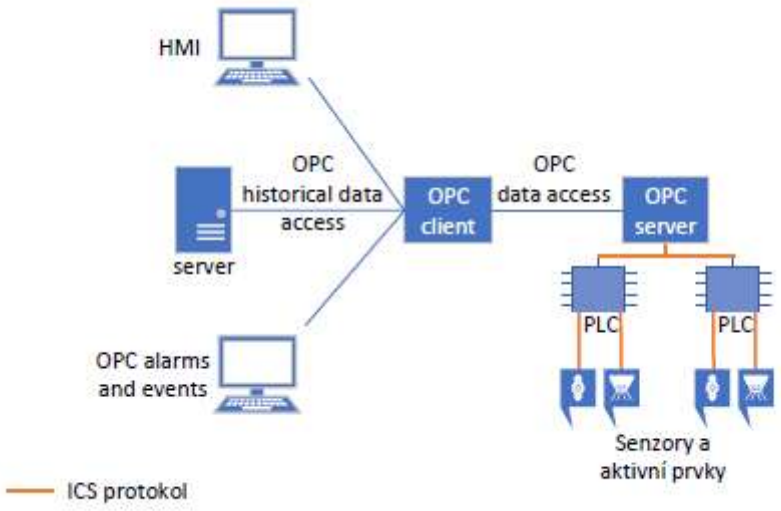
2.8.1 Bezpečnost

Mechanismy pro kontrolu autenticity zpráv a jednotlivých uzlů naprosto chybí. Každý prvek sice odpovídá ve stanoveném intervalu, který byl přidělen MN, ale není možnost, jak ověřit, že stanice, která odpověděla je skutečně ta, za kterou se označuje. Je zde možnost šířit nelegitimní provoz do sítě, popřípadě vyvolat DoS. Používání broadcastového šíření zpráv od CN umožňuje útočníkovi zachytit veškerou komunikaci, kterou zaslal [1, 22, 23]. SCNM, viz obr. 1.19, je náchylný na zpoždění, je tedy třeba jej oddělit od ostatních sítí, které využívají Ethernet. Je doporučeno nastavit bezpečnostní opatření perimetru tak, aby byla síť izolována a předcházelo se nežádoucímu provozu.

2.9 OLE for Proces Control (OPC)

OPC (OLE for Process Control), nejedná se o průmyslový protokol, ale o operační rámec pro komunikaci v systémech pro řízení procesů založených na Windows, které používají propojování a vkládání objektů (OLE). OLE jsou využívány komunikačními protokoly jako RPC (Remote Procedure Call). Jde tedy o sadu protokolů umožňující komunikaci systémů řízení procesů. Jednotlivé systémy založené na operačním systému Windows jsou spojeny prostřednictvím sady TCP/IP. OPC byl původně založen na DCOM (Distributed Component Object Model), který je stále využíván i přes existenci aktualizované verze OPC-UA (OPC Unified Architecture), která umožňuje použití SOAP (Simple Object Access Protocol) přes HTTPS [24, 25]. OPC specifikace popisuje OPC COM (Component Object Model) objekty a jejich rozhraní implementované OPC serverem. OPC klient je schopen spojení s OPC serverem poskytovaný jedním nebo více poskytovateli. Na nejnižší úrovni mohou OPC klienti získat nezpracovaná data z fyzických zařízení do SCADA, nebo ze systému SCADA do aplikace. Obr. 6 znázorňuje možné zapojení využívající operační rámec OPC. Vzhledem k tomu,

že se nejedná o skutečný průmyslový protokol, tak musí dojít k jeho kombinaci s průmyslovým protokolem. [35]



Obrázek 6 : Zapojení OPC [Zdroj 25]

2.9.1 Bezpečnost

Díky použití DCOM a RPC je OPC velice citlivý na útoky. Může být ovlivněn všemi zranitelnostmi vyskytujícími se v OLE. OPC je využíváno pouze na systémech Windows, tudíž mohou být využity všechny zranitelnosti i tohoto operačního systému. Kvůli obtížnému provádění záplat v průmyslových řídících systémech je stále mnoho objevených zranitelných míst bez záplaty. Pro dosažení větší úrovně bezpečnosti je doporučeno využívat OPC-UA [1, 24, 25]. OPC servery by měly mít zesílené zabezpečení, je doporučeno veškeré nepoužívané porty a služby vypnout. Měly by být sledovány všechny porty a služby, které přímo nenáleží OPC, ale jsou OPC serverem iniciovány. Také by měl být monitorován výskyt zranitelností spojených se systémy Windows, OPC, OLE RPC nebo DCOM. Ke zvýšení bezpečnosti by všechny OPC služby iniciované z neznámého OPC serveru, sledovány by měly být také veškeré neúspěšné pokusy o autentizaci.

3 Analýza hrozeb systémů pro průmyslová zařízení

U hrozeb systému pro průmyslová zařízení musíme mít vymezené pojmy „safety“ a „security“. Pojmem „safety“ se rozumí „funkční bezpečnost“, např.: ochrana před úrazem (bezpečnost práce) případně ochrana životního prostředí nebo požární ochrana apod.

Druhým pojmem „security“ se rozumí „kyberbezpečnost“, popř. „bezpečnost v IT“.

Komunikace na bázi Ethernetu hraje klíčovou roli v automatizačním prostředí. Výhoda nasazení Ethernetu v tomto prostředí je především jedna – umožnění nasazení otevřených, standardizovaných IT technologií, které umožňují implementaci integrovaných sítí. Tato výhoda však zvyšuje riziko narušení přístupu, které je nutné posoudit a následně implementovat vhodné bezpečnostní koncepty. Tyto útoky nemusí nutně souviset s hackerským narušením. Může se jednat o narušení způsobené servisním technikem. Ten může navázat spojení s řídící sítí a poté jednoduše, spuštěním několika aplikací, může tento servisní technik zahltit síť do té míry, že některá automatizační zařízení selžou a tím se spustí úplné přerušení provozu. V kontextu automatizačních systémů lze tedy za bezpečnostní problém považovat jakékoliv provozní narušení, ať již záměrně či omylem. Zabezpečení sítě není věcí, kterou lze umístit na jedno místo. Všichni, kteří se podílí na instalaci a správě, musí být zahrnuti do tohoto konceptu. Může se jednat o oddělení IT, odborníky na PLC, bezpečnostní tým, dokonce i výrobce komponent je do tohoto procesu zahrnutý. [7]

Úspěšné útoky na komponenty průmyslových sítí mají obrovské dopady na celou řadu aspektů, dělící se na lokální dopad (dopad na provoz), regionální (okolní území) a globální (národní, nadnárodní):

- dopad na kvalitu výrobku,
- pověst společnosti,
- ztráta výroby,
- ztráta duševního vlastnictví,
- mikroekonomický dopad,
- dopad na životní prostředí,
- ztráty na životech,
- makroekonomický (hospodářský) dopad,

- obecná panika,
- rozsáhlá katastrofa čítající mnoho ztrát na životech a obrovský dopad na životní prostředí.

Výsledky průzkumu zveřejněné společností Positive Technologies jasně říkají, že průmyslové sítě jsou z hlediska kyberbezpečnosti špatně chráněné navzdory tomu, že jsou rozhodující pro provoz průmyslových zařízení (a tedy pro samotné průmyslové podniky). Podle zprávy má 73 % testovaných podnikových informačních systémů a sítí nedostatečnou perimetrickou ochranu před vnějšími útoky. Penetrační testeři získali přístup k podnikové síti a využili tento přístup k průniku do průmyslové sítě obsahující zařízení v 82 % testovaných sítí. V 67 % úspěšných případů průniku byly vektory útoku ohodnoceny jako triviální nebo malé. „Implementace těchto útočných vektorů by vyžadovala pouze využití stávajících konfiguračních nedostatků v zařízení a segmentaci sítě, jakož i zranitelnosti OS, pro které jsou exploitační nástroje dostupné i online.“ uvádí se ve zprávě. [24,20]

Bob Noel, ředitel strategických vztahů a marketingu společnosti Plixer, řekl: „Existuje dnes tolik útočných vektorů pro kyberzločince, že každá organizace, zejména kritická infrastruktura, musí předpokládat, že bude porušena. K posílení bezpečnostních strategií by měla být analýza síťového provozu implementována tak, aby hledala zneužití důvěryhodnosti, boční pohyby (tzv. lateral movement) a anomálie v protokolech a aplikacích. Jak bylo demonstrováno penetračními testery, jakmile kybernetičtí zločinci proniknou do sítě, jsou schopni obejít bránu mezi podnikovou sítí a sítí podporující průmyslové systémy“. [43]

Ethernet je velice využíván v aplikacích průmyslové automatizace a v kancelářských prostředích průmyslových firem. Díky tomuto je mnoho lidí přesvědčeno, že postupy zabezpečení, které jsou využívány v kancelářských prostředí lze snadno aplikovat na průmyslové sítě. Bohužel to není pravda, protože existuje několik významných rozdílů mezi průmyslovými a kancelářskými ethernetovými sítěmi.

3.1.1 Cíl ochrany

Zatímco kancelářské sítě se zabývají především zabezpečením dat (obsahují totiž všechny druhy vysoce citlivých dat jako jsou mzdy, příjmy, seznam zákazníků, marže apod.), největším problémem pro průmyslové sítě obecně je provozuschopnost. Ve většině aplikací kancelářských sítí lze tolerovat přerušení služeb na několik minut, případně na několik hodin

až dní (v případě svátků, víkendů apod.). Průmyslové sítě naopak nepřenáší data s touto úrovní citlivosti, avšak nepřetržitý provoz 24/7 je pro ně velice klíčový. [25,20]

3.1.2 Omezený přístup

Velké množství kancelářských systémů musí mít rozsáhlé propojení s okolním světem. Mzdové systémy jsou spojeny s bankovními systémy, prodavači na pobočkách musí mít přístup k informacím o zákazníkovi apod. Na rozdíl od průmyslových sítí, které mohou mít úzce regulovaný přístup, díky kterým lze realizovat určitá bezpečnostní opatření, která by v kancelářské síti nebyla praktická. Jedná se například o poskytnutí přístupu na základě požadavků určité osoby. [25]

3.1.3 Velikost a stabilita

Obecně jsou kancelářské sítě mnohem větší, do sítě se připojuje mnohem více počítačů, tabletů, chytrých telefonů a dalších zařízení. Oproti tomu k průmyslové síti je připojené omezené množství zařízení. Tyto zařízení jsou také mnohem statičtější – přidání dalšího stroje, jeho HMI nebo PLC, do výrobního systému obvykle není častým jevem (častější je spíše výměna za jiný) a je poměrně běžné, že síť průmyslové automatizace zůstává v podstatě stejná nebo hodně podobná celé roky.

Taktéž komunikace je mnohem statičtější u průmyslových automatizačních sítí, než je tomu u kancelářských sítí. Z tohoto důvodu lze snadněji detekovat jakékoliv odchylky od normálních vzorců, které by mohly naznačovat problém v síti nebo vniknutí útočníka. [25]

3.1.4 Hardware a Software

Kancelářské sítě propojují standardní hardware, jakou jsou počítače, tablety, tiskárny apod. Mnoho z těchto zařízení je vybaveno ethernetovými porty a komunikuje přes Ethernet IP a další standardní protokoly. Software, který běží na těchto zařízeních je taktéž vysoce standardizovaný (z hlediska síťové komunikace). Průmyslové sítě spojují rozhraní HMI, řadiče, motorové pohony a další proprietární a embedded zařízení. Většina těchto zařízení má ethernetový port, ostatní spolu komunikují jednoduššími metodami, jakou jako napěťové či proudové smyčky apod.[25]

3.1.5 Softwarové aktualizace

Obecně se kancelářské sítě a systémy neustále záplatují a inovují pomocí nejnovějších aktualizací softwaru díky čemuž mají poměrně dobrou reakci na různé nalezené hrozby a zranitelnosti. Průmyslové sítě jsou na rozdíl od kancelářských sítí těžkopádnější, protože se musí pečlivě otestovat každá změna softwaru tak, aby nedošlo k ovlivnění komunikace s ostatními zařízeními. Z tohoto důvodu mnoho správců sítě tyto aktualizace nenasazuje. Díky tomu jsou sice sítě průmyslové automatizace stabilnější, mají zvýšenou dobu provozu schopnosti než kancelářské sítě, ale pokud jde o samotné aktualizace software, tak jsou méně aktuální. Tento kompromis zapříčiní menší pružnost reakcí na nově nalezené hrozby a zranitelnosti.[25]

3.1 Posouzení rizik

Co je to riziko? Existuje celá řada definic, z nichž nejcitovanější a obecně neuznávanější je definice dle ISO, která definuje riziko jako „potenciál, který daná hrozba bude zneužívat zranitelnosti aktiva a tím poškodit organizaci“. [26] Z této definice vyplývá, že riziko se skládá ze tří modifikátorů:

- pravděpodobnost dané hrozby,
- potenciální zranitelnost aktiva,
- výsledné důsledky, které ovlivní provoz.

Základní koncept řízení rizik je takový, že můžeme snížit nebo zmírnit riziko zaměřením na jeden nebo na více výše zmíněných modifikátorů. Obecný názor říká, že nejjednodušší metoda snížení rizika je identifikace a eliminace zranitelných míst, která mohou být zneužita. Například zavedením systému správy patchů, které pravidelně aktualizuje software pro odstranění identifikovaných bezpečnostních nedostatků. Riziko lze také snížit omezením rozsahu škod. Tato metoda bývá často přehlížena, ačkoliv může být mnohem efektivnější a levnější ve srovnání s jinými metodami. [22][21]

Pro identifikaci rizik v IT bylo vyvinuto několik metod. Tabulka 1 uvádí ty nejčastěji používané. Provedení analýzy rizik je obtížný úkol, protože je nutné, aby bylo homogenní při posuzování všech rizik a situací, které mohou nastat. Aby tento proces byl co možná nejpřesnější, je nutné, aby metoda bylo složena z poměrně jednoduchých kroků. Tyto kroky se stávají především z inventarizace systému a na základě tohoto seznamu lze provést vyhodnocení se správně

definovaným měřítkem. Tyto seznamy mají také další funkci a to takovou, aby analytik nezapomněl opomenout důležité body zabezpečení.[21]

V závislosti na těchto metodách lze popsat kategorie komponent, hrozeb, zranitelnosti a možných dopadů. Tyto metody lze využít na různých úrovních společnosti – od zkoumání organizačních procesů ve společnosti až po technickou úroveň. [4]

Hodnocení rizik je činnost, která probíhá jako součást procesu řízení rizik. Jde však o činnost, která je iniciována pouze v pravidelných intervalech, nikoliv kontinuálně. Hodnocení rizik obvykle slouží k identifikaci a analýze možných zranitelností a hrozeb daného systém. To se provádí za účelem odhadu rizik, kterým může provozovatel čelit. Výstup této fáze je základem pro všechny ostatní činnosti v rámci řízení rizik tím, že vyvolává nové požadavky na bezpečnost, vyhodnocuje současné bezpečnostní politiky, posuzuje stávající ochranné mechanismy, pomáhá při výběru protiopatření apod. [20][21][25]

Výsledkem posouzení rizik je kvalitativní a kvantitativní hodnocení možných rizik, kterým je síť vystavena s přihlédnutím k pravděpodobným hrozbám a kontextu. [20]

3.2 Událost ohrožení

Událost ohrožení se sestává z několika součástí, které mohou výrazně ovlivnit riziko a které jsou následující:

- zdroj hrozby,
- vektor hrozeb,
- cíl hrozby.

Řešení jednoho nebo více těchto součástí může taktéž ovlivnit riziko. Vektory útoku jsou například nechráněné USB porty, nesprávně nakonfigurovaný firewall apod. Termín „zmenšení útočné plochy“ označuje metodu, která může zcela vyloučit jeden z vektorů útoku (např. zcela zakázat řadič USB). [19]

Zdroj hrozby (neboli lidský útočník) provede kybernetický útok, pokud útočník má následující tři vlastnosti:

- znalost provedení útoku,

• záměr způsobit škodu,

• příležitost k zahájení útoku.

Existuje mnoho nástrojů (komerčních i s otevřeným zdrojovým kódem), které umožní provést kybernetický útok s poměrně malou znalostí problematiky. Pro organizace je velmi obtížné snížit riziko vnějšího zdroje útoku, protože to není v jejich přímé kontrole. Pokud však útok vychází z vnitřního zdroje (případně vnější útočník získá oporu uvnitř), je hrozba zvládnutelnější. [19][21]

3.3 Identifikace fyzických a logických aktiv

Identifikace aktiv a charakterizace systému se provádí pomocí konceptu segmentů. Tento přístup umožňuje podívat se na architekturu sítě a vytvořit segment perimetru zvanou „hranice důvěryhodnosti“. [27]

Schéma obsahuje v zásadě pět typů aktiv – firewall, datový koncentrátor, klientské PC, PLC a síťové přepínače. Tyto vstupní body mohou být použity jako útočné vektory od potenciálních útočníků. Je nutné také zjistit, zda aktivum nemá skrytý útočný vektor (např. vestavěné bezdrátové funkce 802.11, Bluetooth apod.).

Jiný pohled na aktiva je z hlediska logického přístupu. Většina bezpečnostních kontrol chrání především logická aktiva spíše než fyzická. Je například dobré zvážit instalaci antivirových programů, které zabrání neoprávněnému spuštění škodlivého kódu.[34]

3.4 Sběr dat

Dokumentace aktiv je ověřována pomocí různých metod sběru dat. U hodnoceného systému bude snazší identifikovat kritická fyzická a logická aktiva, která tvoří základ softwarového a hardwarového vybavení sítě. Metody sběru dat nejenom ověřují a aktualizují existující inventář aktiv, ale hlavně mohou odhalit skrytá a nezdokumentovaná zařízení a přístroje, které by mohly významně zvyšovat riziko útoku (resp. zvýšit počet útočných vektorů). Online sběr dat poskytuje schopnost přesně identifikovat všechny otevřené komunikační porty, spuštěné aplikace a služby na konkrétním přístroji. Tyto informace se později používají k vyhodnocení potenciálních útočných vektorů v systému. [2]

Existuje celá řada skenovacích komerčních nástrojů s otevřeným zdrojovým kódem. Tyto nástroje však mohou mít kritické účinky na fungování sítě jako takové, takže by se neměly používat bez rozsáhlé přípravy „offline“ testování pro zjištění, jakým způsobem samotný sběr dat ovlivní síť jako takovou. V tomto ohledu jsou nejnebezpečnější nástroje ty, které provádí aktivní sběr dat dotazováním – měly by být používány pouze pokud je síť v offline režimu (např. při plánované odstávce výroby). [2]

Základní typy skenerů jsou určeny k identifikaci zařízení, identifikaci konkrétních aplikací a komunikaci určitých služeb dostupných na těchto zařízení. Jedním z nejoblíbenějších mapovačů je nmap, který je k dispozici pro většinu operačních systémů. Tento nástroj je otevřeným zdrojovým kódem a zahrnuje detekce hostitelských služeb, detekce operačních systémů, spoofing, vyhledávání hostitelů apod. Má navíc schopnost spouštět vlastní scripty pomocí Nmap Scripting Engine (NSE). [28] Nástroj nmap provádí veškerý sběr dat prostřednictvím síťové externí injekce paketů a následné analýzy. Tento nástroj je realistickou reprezentací toho, jak útočník provádí skenování v síti, avšak není ideálním nástroje pro identifikaci systémových aktiv.

Pasivním a „přátelským“ (ve smyslu, že neohrožuje časově citlivou komunikaci mezi komponenty sítě) nástrojem je Network statistics neboli netstat. Užitečnost tohoto nástroje vychází ve schopnosti zobrazit počet síťových funkcí založených na hostiteli včetně aktivních a naslouchajících síťových připojení, mapování aplikací a přidružených služeb, identifikaci aktivních relací vzdálených hostitelů a služeb, které tito hostitelé používají (toto je obzvlášť důležitá informace při mapování toku dat v síti). [29]

3.5 Skenery zranitelnosti

Tyto skenery tvoří další typ běžně používaného vybavení pro zvýšení zabezpečení sítě. Existuje taktéž celá řada komerčních (Tenable Nessus, Core Impact) nástrojů s otevřeným zdrojovým kódem (OpenVAS). Tyto nástroje se specializují na identifikaci zranitelných míst, které porovnávají vůči své databázi zranitelností. Je tedy možné, že schopnost detekovat zranitelnosti se může u jednotlivých nástrojů značně lišit. [35] Zranitelnost není jen přítomnost neopatchovaného softwaru, ale také použití zbytečných aplikací a služeb, které nelze zjistit pouhým skenováním, nesprávné ověření, špatné řízení přístupu, nekonzistentní dokumentace apod. Fáze hodnocení závisí do značné míry

na automatizovaném skenování zranitelnosti softwaru – kontrola aplikace, hostitele a konfigurace sítě. [34]

3.6 Skenery síťového provozu sítě

Dalším typem skeneru, který se běžně používá pro zvýšení zabezpečení sítě jsou skenery síťového provozu. Tyto nástroje jsou určeny pro sběr surových síťových paketů, aby mohly být poskytnuty pro následnou analýzu, která zahrnuje identifikaci hostitele a datových toků, mohou být také použity pro vytvoření sady pravidel pro firewall. Nejznámějším nástrojem pro sběr je tcpdump pro Unixové systémy a windump pro Windows. Výše zmíněné nástroje opravdu pouze zachycují pakety a pro analýzu se používají jiné – nejznámější je Wireshark, který obsahuje GUI a je na něm tudíž analýza mnohem pohodlnější. Wireshark využívá protokol „disektorů“, takže protokoly používané v různých vrstvách ISO/OSI modelu lze rozdělit a prezentovat samostatně, což umožňuje rozebrat konkrétní podrobnosti protokolu v každé vrstvě. [30]

3.7 Analýza toku dat

Síťový provoz dat se vyhodnocuje na základě společných charakteristik paketů. Za datový tok považujeme provoz, který sdílí určité společné vlastnosti a přesouvá se z jednoho hostitele na druhého. Tok, jako takový, se neukládá, ukládají se pouze metadata paketů. Analýza provozních toků (toků dat) je založena na skupině protokolů, které umožňují implementovat procesy generování, přenosu, ukládání a předzpracování metadat. Existují dva protokoly, které představují dva různé přístupy k implementaci analýzy toku provoz – NetFlow a sFlow.[25]

3.8 Zdroje hrozeb

Mnoho vyvíjených metodik pro kybernetickou bezpečnost vychází z předpokladu, že největší zdroje hrozeb se nacházejí mimo organizaci. To vede společnosti k nasazení specifických bezpečnostních kontrol, které by měly zabránit těmto externím hrozbám. Dokumentované zprávy o bezpečnostních incidentech z několika zdrojů nicméně hovoří o tom, že většina incidentů měla původ v interním zdroji. Původ zdroje se rozlišuje na 4 různé typy: [31] [32]

• záměrný útočník z venku,

• náhodný útočník z venku,

• záměrný útočník zevnitř,

• náhodný útočník zevnitř.

3.9 Událost ohrožení

Neboli „threat event“ představuje podrobnosti o útoku, který provedl konkrétní zdroj hrozby. Níže tabulka číslo 1 ukazuje nejčastější události ohrožení.

Tabulka 1: Události ohrožení [Vlastní tvorba]

Události ohrožení
Provádění skenování/průzkumu sítě
Dodání škodlivého kódu do systému
Zaměstnanec s nekalými úmysly
Využití fyzického přístupu k zařízením organizace
Využití špatně nakonfigurované sítě
Využití známých chyb v zabezpečení
Využití nedávno objevených zranitelných míst
Prováděné útoky pomocí neautorizovaných portů, služeb a protokolů
Provedení DoS útoků
Provedení fyzických útoků na organizační zařízení
Provedení fyzických útoků na infrastrukturu
Útok na změnu síťového provozu
Útok typu man-in-the-middle
Útok s využitím sociálního inženýrství ve snaze získat informace
Získání neoprávněného přístupu
Útoky v dodavatelském řetězci
Způsobení zhoršení služeb
Způsobení ztráty integrity
Získání citlivých informací pomocí exfiltrace (vývoz dat)
VLAN hopping, MAC flooding, ARP spoofing
Koordinované útoky pomocí vnějších a vnitřních zdrojů hrozeb
Zavedení a využití zranitelností v SW produktech

3.10 Analýza zranitelností dle OSI modelu

Vzhledem ke komplexitě a velkého množství zranitelností v infrastruktuře průmyslové sítě lze zvolil rozdělení těchto zranitelností podle referenčního ISO modelu, který síť dělí do sedmi vrstev. [20] [36]

3.10.1 Fyzická vrstva

Vrstva 1 se týká fyzického aspektu sítí – jinými slovy kabeláže a infrastruktury používané pro komunikaci sítí. [22] [36]

3.10.2 Spojová vrstva

Spojová vrstva neboli vrstva datového spojení, zabývající se logickým přenosem mezi dvěma přímo připojenými uzly sítě. Nejčastější zranitelnosti na linkové vrstvě. [22]

- ARP poisoning – vydávání se za jiné zařízení v síti
- MAC spoofing – vydávání se za jiné zařízení v síti
- MAC flooding – zasílání citlivých informací do jiné části sítě
- STP útok – vložení dalšího switche do sítě
- Přetečení CAM tabulky – donucení přepínače chovat se jako rozbočovač
- VLAN hopping – umožní dostání se k více VLAN sítím
- Port stealing – Odcizení potu

3.10.3 Síťová vrstva

Síťová vrstva se stará o směrování v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítí. [22] [36] [18]

- IP adress spoofing – Vytvoření paketu s falešnou zdrojovou IP adresou.
- Ping flood – Zahlcení ICMP echo pakety.
- Network scanning – Pasivní útok mající za úkol získat informace o síti a zařízeních v něm.
- Smurf Attack – Zahlcení ICMP pakety.
- Teardrop Attack – Zahlcený fragmentovanými pakety.
- Packet Sniffing – Pasivní útok mající za úkol získat informace o síti a zařízeních v něm.
- Ping of death – Zaslání velkého paketu.

3.10.4 Transportní vrstva

Umožňuje adresovat přímo aplikace v protokolech TCP/IP pomocí portu, které v kombinaci s IP adresou dopravují data k dané aplikaci. Poskytuje transparentní

a spolehlivý přenos dat s požadovanou kvalitou. Provádí převod transportních adres na síťové, ale nestará se o směrování.[22] [36]

- SYN flooding – Útočník posílá posloupnost paketů SYN, ale pak už neodpovídá.
- Port knocking – Útočník skenuje, jaké porty jsou otevřené.
- TCP Session Hijacking – Útočník získá kontrolu nad relací.
- TCP sequence prediction – Útočník se snaží uhodnout sekvenční číslo, které má hostitel použít.
- TCP veto – Útočník odposlouchává a předpovídá velikost dalšího paketu, aby legitimní paket cíl označil jako duplikát.

3.10.5 Relační vrstva

Relační vrstva má za úkol vytvářet a řídit přenosy dat mezi uzly. Pro komunikaci jsou k dispozici tři režimy simplex, half-duplex a full-duplex. [22] [36]

- DNS poisoning
- Session hijacking
- Telnet DDoS

3.10.6 Prezentační

Prezenční vrstva je volána pro překlad dat při odesílání, a to na obecný formát, který není závislí na konkrétní platformě. Při přijímání dat probíhá překlad dat do formátu dané aplikace. Dále je tato vrstva zodpovědná za kompresy a šifrování dat. [22] [36]

- SSL MITM
- SSL DOS

3.10.7 Aplikační vrstva

Pomocí této vrstvy se vytváří rozhraní mezi aplikací a nižší sousední vrstvou. Využívá se v momentě, kdy aplikace požaduje komunikaci za použití protokolů. Nejčastější služby patří přístup k webovým stránkám, zasílání zpráv a přenos souborů. [22] [36]

- Viry, červy, trojské koně
- DNS spoofing
- SQL injection
- DDoS
- Phishing

4 Představení společnosti Freudenberg Sealing Technologies

Německá společnost, která byla založena před 171 lety Carlem Freudenbergem. Začínala jako koželužna. V roce 1850 získala první patent na kožedělnou výrobu. Kolem roku 1900 již zaměstnávala přes 500 zaměstnanců. Již od svého založení si společnost zakládá na vývoji. Za dobu svého působení se rozrostla do několika odvětví. Dnes vyrábí těsnění, výrobky pro domácnost Vileda, netkané textilie, čistící prostředky a jiné chemikálie, vyvíjí také nové technologie ve službách, co se týče hardwaru či softwaru. Své pobočky má na 555 místech po celém světě a zaměstnává více jak 40 000 zaměstnanců. Naše divize Freudenberg Sealing Technologies vznikla v roce 1929 a začala s výrobou kožených těsnění, v roce 1936 se již vyráběly těsnící hřídelové kroužky ze syntetického kaučuku Simmering – podle vývojáře Walthera Simmera.

4.1 Freudenberg Sealing Technologies s. r. o.

Středně velká firma sídlí v pardubickém kraji. Byla založena před 20 lety. Výroba se rozkládá na ploše 7000 m². Firma zaměstnává 200 dělníků a 50 THP pracovníků. Vyrábí pouze těsnící hřídelové kroužky – simmeringy. Ve společnosti se využívají především stroje BOY, ARBURG a FIM (LWB), jedná se o jednoúčelové stroje upravené pro lisování pryže. Dále jsou využívány zakladače, které jsou nadstavbou těchto strojů. Jedná se o dvouosé, popřípadě tříosé zakladače dílů do těchto strojů. V poslední době se společnost také věnuje možnosti robotických zakladačů. V současné době společnost disponuje dvěma druhy těchto robotů, hlavním pilířem je robot KAWASAKI a pro práci v blízkosti obsluhy se používá kolaborativní robot UR5e od společnosti UNIVERSAL ROBOTS.

4.2 Systémy jednotlivých strojů ve společnosti

4.2.1 Stroje BOY

Jedná se o vstřikovací stroj, který je upraven pro speciální potřeby společnosti. Zejména se jedná o úpravu pro gumárenskou výrobu. Jeho řízení je založeno na systému SIEMENS S7 300, který bude poskytovat data pro účely sběru dat. Stroj komunikuje s jednotlivými komponenty pomocí ProfiBus a umožnuje připojení ProfiNet, které bude využito pro připojení do nově vytvořené sítě pro účel sběru dat.

4.2.2 Stroje Arburg

Jsou vstřikovací lisy upravené pro gumárenskou výrobu obdobně jako stroje BOY a jejich systém, který bude poskytovat informace pro sběr dat, je SIEMENS S7 1200. Obsahuje komunikační modul ProfiBus a umožnuje komunikaci pomocí ProfiNet, která bude využita pro sběr dat a kterou společnost požaduje.

4.2.3 Stroje LWB

Jsou to taktéž vstřikovací stroje, které disponují dvěma systémy řízení, jeden pro hydraulické systémy a druhý pro zakladač na stroji. Hydraulické systémy jsou řízeny pomocí X20 od společnosti B&R, který disponuje komunikací Profibus, ten je vyžívám pro vzdálené vstupy, výstupy a servomotory. Profinet je využíván pro komunikaci s nadřazeným systémem, který komunikuje se zakladačem výrobků řízeným SIEMENS S7 300. Nadřazený systém a zároveň HMI zobrazení je realizováno pomocí PC od společnosti B&R, na kterém běží operační systém Windows 7. Software pro HMI je použit INTOUCH 9.0 od společnosti WONDERWARE. Tento systém bude poskytován pomocí OPC serveru dat, která jsou potřebná pro sběr dat ve společnosti.

4.3 Řízení strojů ve společnosti

4.3.1 PLC S7 300 SIEMENS

SIMATIC S7 300 je PLC „Programmable Logic Controller“ je modulární PLC pro nízké a střední rozsahy výkonu. Existuje celá řada CPU, které se používají a jejich výběr je v závislosti na dané aplikaci. U systému S7 – 300 je možné používat až 32 modulů různých I/O, kde nejčastěji jsou používány moduly digitálních vstupů a digitálních výstupů 24VDC, dále analogové vstupní moduly například pro měření teplot a analogové výstupní moduly například pro řízení topných článků za pomocí polovodičových relé, které oddělí vysoké napětí a proudy od analogových výstupů. Dále se často používají moduly pro interfacové připojení sběrnic a moduly funkční například PID regulace atd. S7 300 je od společnosti SIEMENS a jeho programování se provádí za pomocí softwaru STEP 7. Existují různí výrobci programovacích softwarů například S5/S7 For Windows od společnosti IBhsoftec a další. Jejich použití není nijak omezeno. Pro programování

se používá jazyk LAD, STL, FBD nebo GRAPH. Jedná se o normované jazyky pro programování PLC vyhovující normě EN 61131-3. Komunikaci zajišťují rozhraní, které jsou na výběr u PLC S7 300 a to MPI, Profibus – DP a ProfiNet. V našem případě bude použito rozhraní pro Profinet.

4.3.2 PLC S7 1200 SIEMENS

Systém S7-1200 má tři různé výkonosti procesoru, a to řady 1211C , 1212C a 1214C. Jedná se o obdobný systém PLC jako předchozí verze S7 300, kde se jedná o modulový systém, ke kterému je možno připojovat I/O rozšíření a komunikační rozhraní. Stejně jako u systému S7 300 se jedná o cyklické provádění programu, který je programovatelný softwarem TIA portál, dnes je již ve verzi 16. Režimy PLC se shodují se systémem S7 300 a to STOP, STARTUP a RUN. Systém S7 1200 má zabudovaný jako základní komunikační rozhraní PROFINET. Pokud uživatel do dané aplikace potřebuje komunikační rozhraní jiné, například PROFIBUS – DP, je nutné toto řešit pomocí přídavného modulu. K CPU 1214C lze připojit až tři komunikační moduly.

4.4 Počítačová síť

Společnost v současném stavu využívá místní počítačovou síť střední velikosti, která je využívána hlavně pro kancelářské účely. Zejména pro emailovou komunikaci,sdílení souborů a ukládání důležitých výrobních dat na místní uložiště. Sít je nazvána FST a je naznačena na obrázku topologie sítě. Společnost disponuje jednou serverovou místností, která je uzamykatelná a disponuje systémem pro kontrolu přístupů pomocí systému přístupových práv na elektronickém zámku. Serverová místnost obsahuje záložní UPS pro zajištění funkčnosti při výpadku energie a elektrický přívod je zajištěn pomocí dieselagregátu, který v případě výpadku energie startuje do cca 30 s. Tímto je zajištěn bezproblémový provoz při výpadku energií. Celá místnost je chráněna proti přehřátí, a to dvěma klimatizačními jednotkami.

5 Navržení průmyslové sítě a její zabezpečení

5.1 Základní požadavky pro průmyslovou síť

Průmyslová síť bude muset být schopna obsloužit cca 60 strojových zařízení a dále cca 60 tabletových zařízení, na kterých bude spuštěna aplikace MES určená pro zadávání dat operátorem do systému.

Komunikace do strojových zařízení bude probíhat pomocí OPC UA, protokolu Siemens TCP/IP Ethernet pro S7 1200 a S7 300. Tato komunikace probíhá pomocí portu 102 v případě komunikačního protokolu Siemens TCP/IP a za pomocí portu 4842 , 4880 a 4840 v případě komunikačního protokolu OPC UA.

5.2 Architektura průmyslové sítě a zabezpečení

Jako návrh topologie bude využit koncept bezpečnostních segmentů mající velký vliv na bezpečnost průmyslové sítě. Princip tohoto návrhu vychází z izolování aktiv do segmentů a ovládáním veškerého komunikačního toku uvnitř a mezi segmenty bude útočná plocha v daném segmentu minimální v rámci svého segmentu. Segmenty budou definovány jak z fyzického, tak logického hlediska. Segmenty fyzického hlediska jsou definovány dle jejich polohy a logické segmenty jsou virtuálního charakteru seskupeny na základě konkrétních funkcí.

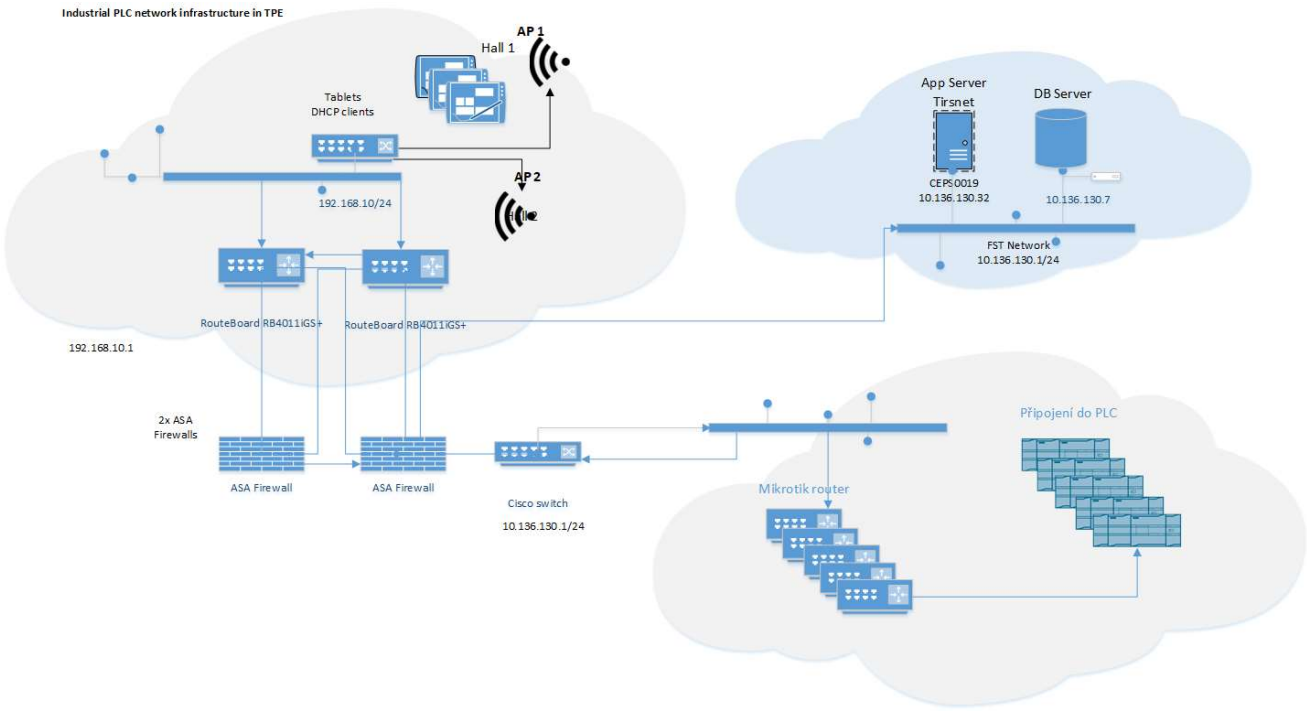
Při správném návrhu a definici segmentů je komunikace omezena jen na nutnou komunikační strukturu prvků a jejich bezpečnost je tak zvýšena správným návrhem a implementací sítě. Toto rozvržení architektury podporuje zásady kybernetické bezpečnosti jako je zásada nejmenšího oprávnění.

Návrh segmentů je na obrázku 3 pro provoz tabletů pro MES aplikace, dále na segment pevného připojení pro sběr dat z PLC a segment sítě FST pro server, který bude stávající s napojením na desktopové stanice. Jednotlivé stanice PLC jsou připojeny pomocí routeru MikroTik RB750Gr3, který zajišťuje překlápění IP adres a portů do vnitřní sítě stroje, a to za pomocí nastavení NAT na vnitřním firewallu zařízení MikroTik, která je mnohdy tvořena více zařízeními. Toto řešení je z důvodu stejných IP rozsahů u stejných strojů jednoho výrobce. Jejich přenastavení by znamenalo zásah do stroje, který u některých zařízení není možný

z důvodu pozáručního servisu. Router MikroTik má pevnou IP adresu v rozsahu 10.136.130. 1/24, kterou pomocí NAT překlápí na vnitřní adresu PLC či průmyslového PC, která je většinou v rozsahu 192.168.0.1 /24. Dále router disponuje unikátní MAC adresou a síťovým názvem.

Tento router je z bezpečnostních důvodů nastaven pouze na první port a port WAN a to pouze pro přístup ze serverové IP adresy a portu, který je potřeba pro dané PLC potřebný ke komunikaci například port 102 pro Siemens TCP/IP. Nastavení firewallu na daném routeru bude jakoukoliv jinou komunikaci ignorovat.

Tyto routery MikroTik jsou připojeny do RACKu dané haly viz schéma topologie místní sítě. Komunikaci na segment FST zajišťuje Cisco switch Cisco Catalyst 9200 24 PoE, který komunikuje skrze Firewall ASC (redundantní Firewall) a dále do virtuálního serveru (Windows server 2016) s OPC Kepware. Segment ze strany tabletů funguje obdobným způsobem za pomocí WIFI nastavené jako AP1 – AP3, který je přes Switch (Unifi Switch 16 Gigabit POE) propojen do Routeru MikroTik (CRS112-8G-45-IN), který pracuje jako DHCP server. Vnitřní pravidlo nastavení možné komunikace je nastavené obdobně jako u segmentu pro PLC a to tak, že je povolena nejnutnější komunikace na portech a pro konkrétní přednastavené zařízení.



Obrázek 7 – Hierarchie průmyslové sítě

5.2.1 Navržená zabezpečení sítě

5.2.1.1 Fyzická ochrana

Ochrana na hraně perimetru zabraňuje neoprávněnému vstupu a lze pro ni využít tyto opatření.

- Přírodní překážky, zdi, ploty, vnější stěny budovy.
- Systémy detekce vniknutí, bezpečnostní agenturu a podobné.
- Okna, dveře, řízení přístupu do budovy či místností závodů.
- Kamerový systém, identifikace osob pomocí RFID karet, pohybové a jiné senzory.

5.2.1.2 Linková vrstva a její ochrana

Pro ochranu linkové vrstvy je doporučeno použít monitorovacího programu ARP watch, který monitoruje aktivitu v Ethernetové síti a udržuje databázi párování MAC adres a IP adres, které označuje časovým razítkem.

Dále použití protokolu 802.1x, který v případě připojení klienta do sítě vyžaduje autentizaci a jeho komunikace bez autentizace je blokována přepínačem.

Dalším z opatření je zabezpečení portů samotných přepínačů. Přepínače budou mít povoleny pouze omezený počet MAC adres, které lze zjistit na portech připojených ke koncovým stanicím. To znamená, že síťový přepínač kontroluje MAC adresu na příchozích rámcích a pokud je MAC odlišná od povolené, přepínač tento rámec blokuje, případně vypne port. Všechny porty, které budou připojené ke koncovým zařízením budou v modů acces, ve kterém nebude možné pro útočníka imitovat přepínač pro přístup ke komunikaci na VLAN.

Dále pro zamezení útoku VLAN hopping (Při útoku napodobuje útočící hostitel trunkový přepínač používaných při údržbě VLAN. Provoz pro více sítí VLAN je poté přístupný útočícímu hostiteli.) budou odebrány přístupové body z výchozí VLAN 1

5.2.1.3 Síťová vrstva a její ochrana

Síťová vrstva (network layer) je název třetí vrstvy síťové architektury referenčního modelu ISO/OSI. Tato vrstva se stará o směrování v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích. Nejznámější protokol, který pracuje na této vrstvě, je protokol Internet Protocol (IP).

- Filtrování paketů je technika brány firewall, která slouží k řízení přístupu k síti sledováním odchozích a příchozích paketů a umožňuje na základě zdrojové a cílové adres a portů internetového protokolu tyto pakety zastavovat nebo předávat dále.
- VPN Tunel, mezi jednotlivými bezpečnostními zónami je vhodné použít vyhrazené virtuální sítě VPN. Jedná se tedy o tunelové spojení dvou sítí (resp. dvou bezpečnostních zón).

5.2.1.4 Transportní vrstva a její ochrana

Transportní vrstva je název čtvrté vrstvy modelu vrstvové síťové architektury (OSI). V originále se nazývá Transport Layer. Umožňuje adresovat přímo aplikace (například v protokolech TCP/IP pomocí čísel portů). Poskytuje transparentní a spolehlivý přenos dat s požadovanou kvalitou. Vyrovnává různé vlastnosti a kvalitu přenosových sítí. Provádí převod transportních adres na síťové, ale nestará se o směrování.

- Zvýšení fronty nevyřízených paketů – Jedna z reakcí na velké objemy SYN paketů je zvýšit maximální počet možných pootevřených spojení, které operační systém umožní. Aby bylo toto možné provést, je nutné, aby OS vyhradil další paměťové prostředky, aby se zabývaly všemi novými požadavky. Tato fronta SYN paketů může narazit na limit, který nebude schopná vyřídit. V určitých případech je nicméně toto lepší než, aby OS službu rovnou odmítl.
- Uzavření nejstaršího polootevřeného spojení – Lze definovat strategie, která uzavře nejstarší polootevřené spojení tak, že díky tomu se uvolní prostředky a bude možné nastávající žádosti o spojení začít vyřizovat. Toto řešení pouze částečné z důvodu, že pokud útočník zvětší objem útoku, problém zůstane stejný.

5.2.2 Aktualizace softwaru

Dalším zásadním opatřením bude včasné nasazení a aktualizace softwaru pro komponenty jako jsou servery, pracovní stanice, firewall, aplikace apod., které jsou součástí průmyslové sítě. Průmyslové sítě jsou sestaveny z velkého počtu komponent včetně serverů, pracovních stanic, síťových zařízení, PLC a podobně. Kde všechna tyto zařízení mají CPU, která vykonává kód, formu operačního systému a místního úložiště. Toto je potenciál zranitelnosti, který musí být opraven a jednou z možností je udržování aktuálního software a firmware. Takto je možné síťovou infrastrukturu neohrozit z důvodu jedné zranitelnosti, a proto by měla být také síťová

zařízení zahrnuta do správy oprav, stejně tak i servery, pracovní stanice apod. Správa aktualizací se definuje do několika fází jako je příprava, dodání, instalace a validace. Na průmyslovou síť se klade vysoký požadavek dostupnosti (která je běžně 99,99 %, což znamená 15 minut nedostupnosti za rok). U takovéto dostupnosti jsou měsíční restarty vyžadovaný k aktivaci „hotfix“ oprav apod. nepřijatelné.

Z tohoto důvodu se průmyslové sítě vybavují redundantními komponentami, ale i při této možnosti je riziko výpadku sítě při aktualizaci softwaru a je potřeba vzít ho v úvahu.

V praxi se používá CVE Common Vulnerabilities and Exposures, jedná se o volně dostupné databáze pro zranitelnost komponent z hlediska kybernetické bezpečnosti. Tyto databáze obsahují konkrétní informace o minimálně jednom bodu zranitelnosti, který může být cílem vedení útoku.

5.3 Softwarové vybavení

5.3.1 Server

Server, na který se připojuje průmyslová síť, je Windows Server 2016 64-bit, x64-procesor Intel Xeon CPU E5-2650 2.2GHz (4 procesory) 8GB RAM. Instalace je provedena jako Datacenter, která oproti Standard instalaci nabízí lepší možnosti a rozšíření jako je například network Controller a jiné podrobnosti jsou k dispozici v detailním popisu instalace serveru na webu Microsoft.

Páteřní síť je instalována v drátěných žlabech v prostorech pod stropem – ochrana polohou proti případnému narušení. Jednotlivé switche se nacházejí ve skříních RACK, které jsou chráněny proti přístupu mechanickým zámkem. Samotný server se nachází v serverové místnosti zabezpečený kamerovým systémem a identifikací pro přístup pomocí RFID.

5.3.2 Instalovaný software na serveru

Na stávajícím virtuálním serveru je instalován základní software pro komunikaci s PLC. Jedná se o OPC server Kepware v6.9.572.0 od společnosti Kepware, který zajišťuje základní

komunikaci mezi PLC a SQL databázovým serverem, ze kterého jsou následně data vyčítána do aplikací MES.

Aplikační softwarem MES je zvolen Ignition designer verze 8.0.16, jedná se o nástroj SCADA, který v sobě zahrnuje ostatní platformy pro MES aplikace jako jsou například alarmová hlášení, podpora HMI, reporting atd. Jedná se o ucelený nástroj na osvědčených technologiích jako jsou SQL, Python, OPC UA a MQTT. Celá aplikace vyvinutá v Ignition může pracovat jako desktopový program nebo může být distribuována na webové platformě, která zajišťuje mnoho výhod v rámci snadného přístupu ať už z PC nebo mobilních zařízení.

5.3.3 Software pro monitorování sítě

5.3.3.1 Simple Network Management Protocol (SNMP)

Protokol SNMP rozlišuje mezi stranou monitorovanou (hlídaný systém) a monitorovací (sběrna dat). Tyto strany mohou běžet, buď odděleně na různých fyzických strojích nebo v rámci jednoho stroje. Na monitorované straně je spuštěn agent a na straně monitorovací manager. Využívá architekturu založenou na modelu klient-server. SNMP je hojně používaný protokol aplikační vrstvy definovaný v RFC1157, slouží pro správu síťových zařízení. Klientem je většinou síťové zařízení, které má být spravované SNMP serverem, jako je např. klientské PC nebo síťové přepínače, směrovače, tiskárny apod.

Data využívaná SNMP jsou organizována do datového stromu. Datový strom se skládá z několika větví, které se nazývají „Management Information Base“ (MIB). Tyto tabulky seskupují konkrétní typy zařízení nebo jejich součásti. MIB má za cíl shromažďovat informace a organizovat je do hierarchického datového formátu. Správce SNMP používá informace z MIB k překladu a k interpretaci zpráv před jejich odesláním koncovému uzlu. Uvnitř těchto MIB tabulek se nachází datová reprezentace celé řady spravovaných objektů, které mohou mít odlišnou datovou reprezentaci – může se jednat o čítače, čísla, texty apod. Každý z těchto objektů se identifikuje pomocí identifikátoru objektu OID. Jedná se o posloupnost čísel, jež určují přesnou polohu datového objektu ve stromu MIB datové struktury.

5.3.3.2 Syslog

Syslog je standard pro zasílání logovacích zpráv, pomocí něhož může zařízení nebo aplikace odesílat logovací data o svém stavu, událostech, diagnostice apod. Komunikace probíhá prostřednictvím UDP portů 514 a 601.

Zprávy Syslogu mají vestavěnou úroveň závažnosti od 0, která je nejzávažnější (nouzový stav) až po úroveň 7, která je informativního (resp. debugového) charakteru. Pracuje podobně jako SNMP protokol s architekturou klient-server. Syslog server přijímá, ukládá a interpretuje zprávy Syslog.

Pro ukládání syslogových dat doporučuji MySQL server a pro samotnou interpretaci výše zmíněný otevřený nástroj „RRD Tool“. Ten lze navíc rozšířit o plugin syslog, který poskytuje další úroveň zpracování a reprezentaci dat (různé grafy, export zpráv ve formátu CSV, HTML a textové alarmy, podpora Native MySQL 5.1 apod.).

5.3.3.3 Wireshark

Tento grafický nástroj se příliš neliší od výše zmíněného TCPdumpu. Oba totiž dokážou využívat knihovnu „libcap“ pro zachycení „živého“ provozu nebo reprezentovat data uložená ve formátu PCAP. Hlavní rozdíl mezi těmito nástroji je v tom, že Wireshark se snaží poskytovat uživateli srozumitelnější a přehlednější reprezentaci dat na rozdíl od TCPdumpu, který vypisuje spíše strohá data paketů.

Data jsou ve Wiresharku zobrazována v nastavitelných oknech s barevně odlišenými pakety. Navíc filtry, které lze použít pro zobrazení požadovaných dat, jsou pestřejší, takže s nimi lze dosáhnout lepšího zobrazení dat. Navíc poskytuje další možnosti statistické analýzy dat, tvorby grafů
a vkládání volitelných pluginů a skriptů.

6 Testování sítě

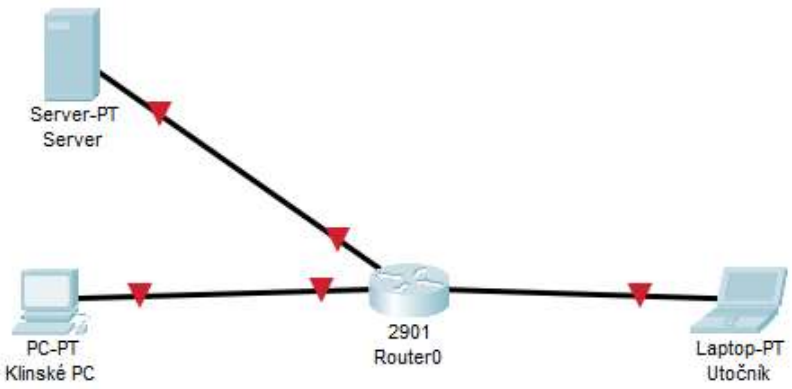
Cílem této kapitoly je popsání sítě pomocí nástrojů určených pro testování zranitelnosti a bezpečnosti sítě ve výše popisovaném modelu sítě.

Vzhledem k velkým rizikům a obavám provozovatele sítě Freudenberg Sealing Technologies s. r. o. Bylo potřeba testovat mnou navrhovanou síť v laboratorních podmínkách.
V laboratorních podmínkách se omezím na L2 a L3 vrstvu ISO OSI modelu. V laboratorním testování sítě se zaměřuji na dvě největší hrozby, které vyplívají z DREAD modelu. Jedná se o hrozbu DoS útoku a hrozbu Sniifing útoků.

Tyto dvě hrozby jsou simulovány pomocí nástrojů uvedených níže. Práce se zabývá nástroji a technologiemi, které tyto hrozby buď zcela zastaví a nebo minimalizují jejich riziko hrozby.

6.1 Testovací prostředí

Po konzultaci s místním správcem sítě byla použita simulace sítě, její model je patrný z obrázku 8.



Obrázek 8 : Schéma testovací sítě (autorova tvorba)

Pro samotné testování a virtuální PC byl použít Hyper-V instalovaný na Windows 10 Pro, na virtuálním serveru je instalován Windows server 2016 a dva virtuální stroje s operačním systémem Windows 10 Pro.

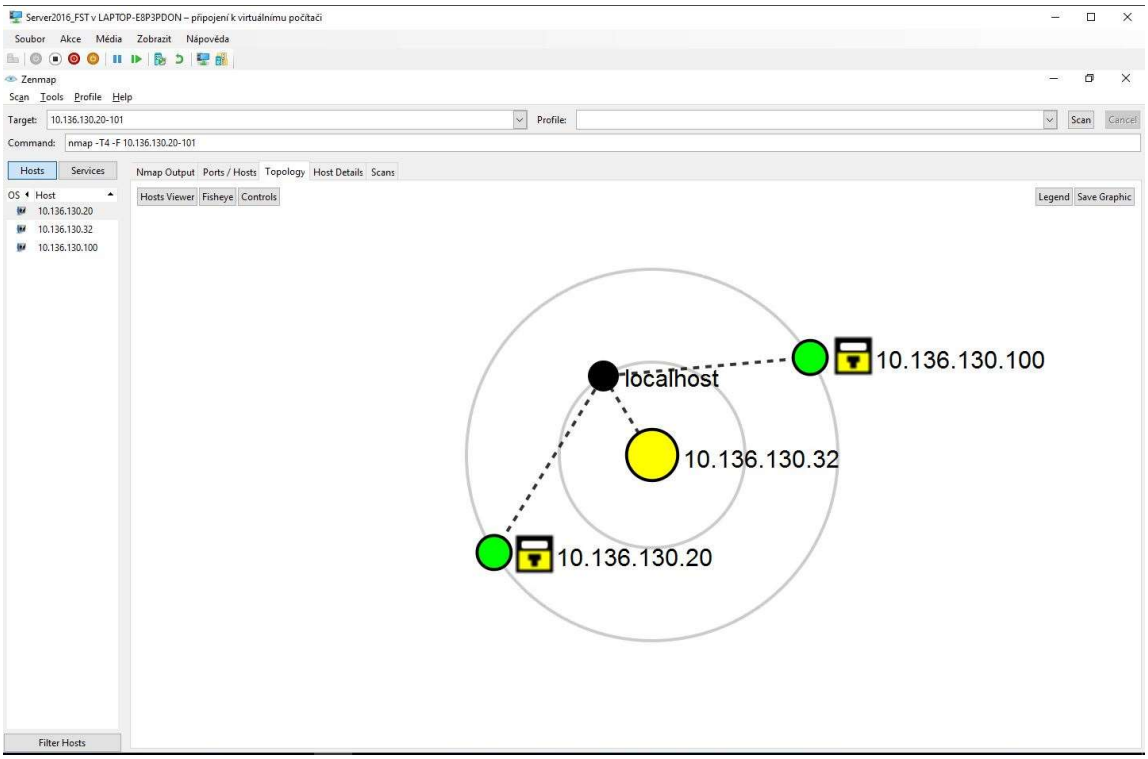
Seznam všech síťových prvků a stanic je uveden společně s IP adresami v tabulce. Samotná topologie sítě je zakreslena na obrázku 13.

Tabulka 2 : Tabulka prvků a adres testovací sítě

Zařízení	Popis	Operační systém	IP
Server	Hyper-v	Windows Server 2016	10.136.130.32/24
Klientské PC	Hyper-v	Windows 10	10.136.130.20
Útočník	Hyper-v	Windows 10	10.136.130.100

Simulace předpokládá základní prolomení fyzického přístupu k ethernetovému rozhraní přepínače umístěného v hale (tj. jedná se o prolomení vnějšího perimetru fyzického zabezpečení).

Pomocí programu zenmap, který je nadstavbou programu nmap a vytváří její grafické prostředí bylo provedeno skenování sítě. Tento program vytvořil model laboratorní sítě, která je použita pro testování. Do modelu jsou zahrnuty otevřené porty a IP adresy zařízení v síti.
Na obrázku je topologie sítě vytvořená pomocí programu zenmap.



Obrázek 9 : Screen z programu Zenmap

6.2 Detekce útoků

Pro detekování útoku DoS a Network scanning v prostředí laboratorní sítě byl použit program Wireshark (popsaný v kapitole 5.3.3.3) a program Suricata IDS pro prostředí Windows dostupné na stránkách výrobce Open Information Security Foundation. Jedná se o systém detekce průniku (IDS) a systém prevence průniku. Licence softwaru je GNU GPL, který je OpenSource.

Software Suricata pro funkčnost v operačním systému Windows, musí mít nainstalovaný WinPcap. Instalace začíná stažením instalačního souboru ze stránek softwaru Suricata. Pravidla se mohou konfigurovat ručně nebo se dají použít již vytvořená, která lze stáhnout ze zdroje : http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz.

Obsah se extrahuje do kořenového adresáře Suricaty. Archiv obsahuje adresář rules, kterým se nahradí stávající adresář z instalačního balíčku a umístí se do kořenové složky softwaru Suricata.

Konfigurace se provádí pomocí konfiguračního souboru surikata.yaml, který je nejdůležitější pro konfigurace programu Suricata. V tomto konfiguračním souboru se mimo jiné parametry zaměříme na parametr HOME_NET, který specifikuje interní síť a parametr EXTERNAL_NET,

který specifikuje externí síť. Dále je nutné přidat parametr se souborem pravidel nazvaným ruleScan, který se nachází v adresáři rules a obsahuje vložená pravidla.

```
alert icmp any any -> any any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev: 1;)
alert tcp any any -> any any (msg: "NMAP TCP Scan";sid:10000005; rev:2; )
alert tcp any any -> any any (msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1; )
alert tcp any any -> any any (msg:"Nmap FIN Scan"; flags:F; sid:1000008; rev:1;)
alert tcp any any -> any any (msg:"Nmap NULL Scan"; flags:0; sid:1000009; rev:1; )
alert udp any any -> any any ( msg:"Nmap UDP Scan"; sid:1000010; rev:1; )
```

Obrázek 10 : Výpis nastavení pravidel v programu Suricata

Způsoby práce s odchytaným provozem jsou následující:

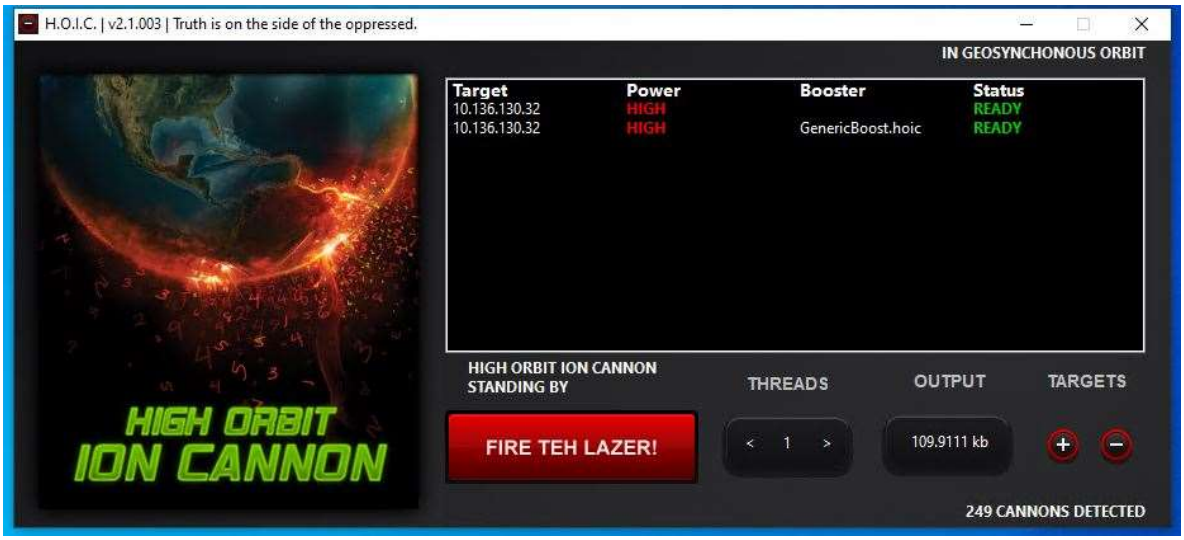
- Pass – provoz nebude kontrolován, jedná se v podstatě o tzv. „whitelist“;
- Drop – zahodí paket, odesílatel o této skutečnosti nebude informován;
- Reject – zahodí paket, odesílatel o této skutečnosti bude informován pomocí ICMP protokolu
- Alert – předá výstrahu do logu s definovanými metadaty

Popis nastavených pravidel :

- *alert* – pokud se pravidlo shoduje s datovým provozem, Suricata vytvoří výstrahu;
- *imcp* – určení kterého protokolu se pravidlo týká;
- *any -> $HOME_NET* – zdroj a cíl provozu (v našem případě proměnná $HOME_NET je nastavena na síť 10.136.130.32/24);
- *any -> any* – zdrojový a cílový port;
- *msg: “ Nmap FIN Scan“* – zpráva, která se zobrazí uživateli;

V tomto případě jsou nastavena pravidla na Alert, aby bylo demonstrováno odchycení samotného útoku.

Jako generátor pro útok DoS (Denial of service) je použit program HOIC (High Orbit Ion Cannon), který je Open source a slouží k zátěžovému testování sítě a útoku typu DoS. Program umožňuje útok až na 256 URL současně. Jedná se o program s grafickým rozhraním, který generuje odesílání požadavků http POST a GET na napadený počítač ve snaze přetížení cílové URL a k jejímu zahlcení.



Obrázek 11 : Screen programu H.O.I.C

Na uvedeném obrázku je ukázka z aplikace, kde byl testován útok DoS jako cíl (Target) je adresa serveru 10.136.130.32, další možnost Power má tři možné úrovně a to

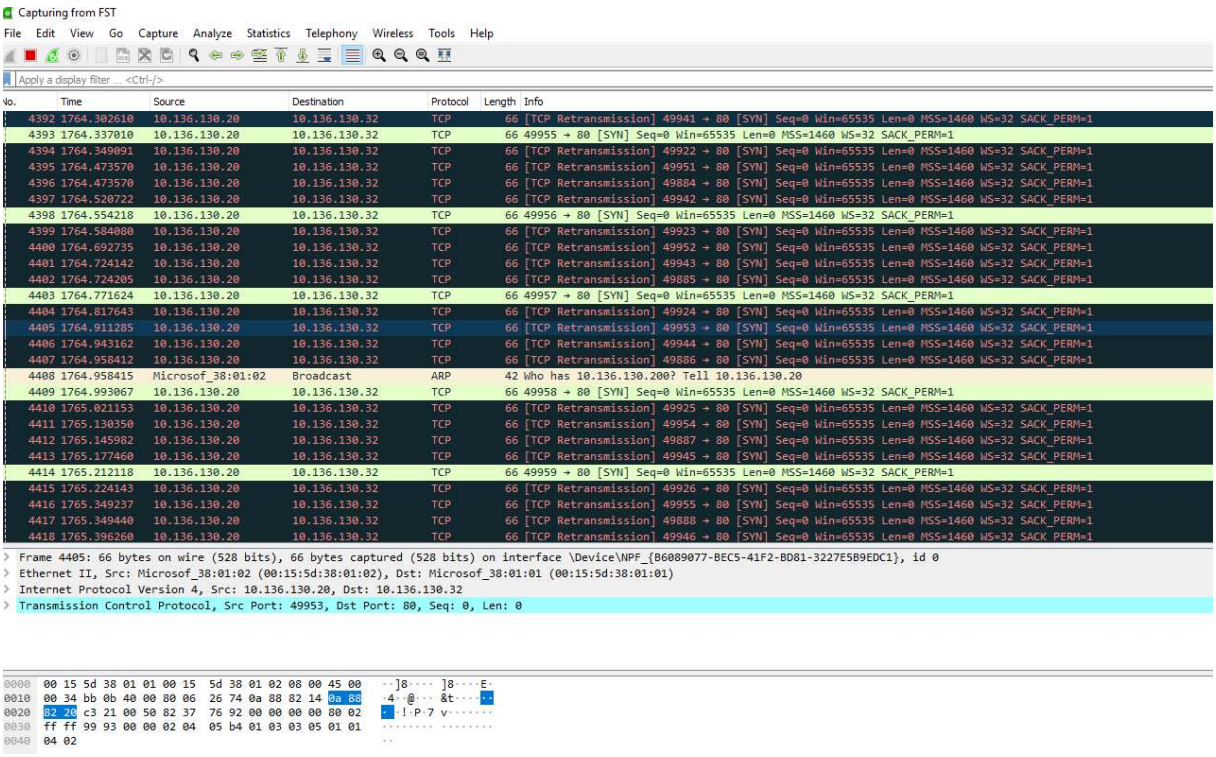
- Low - 2 request/sec
- Medium - 4 request/sec
- High - 8 request/sec

Tyto úrovně nastavují rychlost požadavku, a to na počet požadavků za jednu sekundu. Dále možnost Booster je volba konfiguračního scriptu, který definuje atributy dynamického požadavku.

6.3 Detekce útoku programem Wireshark

Program Wireshark obsahující knihovnu LibPcap byl inicializován na serveru Windows na síťové rozhraní LAN, kde detektor odposlouchával provoz na dané síti. Pomocí filtrů lze nastavit jaký provoz bude zachytáván, jde například o IP, kde se zachytávají pouze pakety protokolu IP, tcp nebo tcp port 80, kde se zachytávají pakety protokolu TCP popřípadě pakety protokolu TCP, které v záhlaví obsahují port 80 nebo například IP host 10.136.130.20, který zachytává pouze pakety, které v záhlaví IP obsahují IP 10.136.10.20.

Program spolehlivě odhalil potenciální simulovaný útok, jak je zřejmé z přiloženého obrázku.



Obrázek 12 : Screen programu Wireshark

Řádky černé barvy ukazují zachycený rámec s časovou známkou, zdrojem odeslaného rámce je v našem případě IP adresa 10.136.130.20, příjemcem daného rámce je IP adresa 10.136.130.32. Dále zde vidíme využitý protokol, jeho délku a informace.

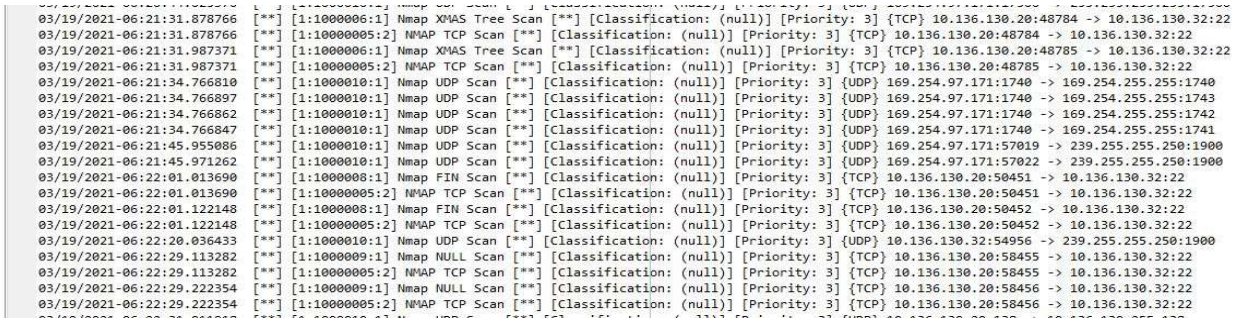
6.4 Detekce útoku programem Suricata

Program Suricata nám na obrázku z log souboru programu ukazuje zachycení útoku network scanning . Útok byl proveden z programu nmap a v naší testovací síti je prováděno skenování sítě s následujícím nástavním:

nmap -sN – jedná se o řadu TCP paketů, které obsahují pořadové číslo 0 a nemají žádné nastavené příznaky. Tento typ paketu může proniknout firewallem z důvodu absence filtrování paketů bez konkrétních příznaků. V případě uzavření portu cíl pošle paket RST. V případě otevření portu se paket zahodí a nepošle žádnou odpověď, tím se odhalí pro útočníka jeho stav.

nmap -sX – jedná se o skenování s názvem xmas tree scan, z důvodu obsahu v záhlaví. TCP nastavuje příznaky PSH, URG a FIN jako blikající žárovky. Operační systém na tyto „vánoční“ pakety reaguje odlišně, pomocí této vlastnosti lze odhalit informace o operačním systému cílového zařízení, stavech portů a další.

nmap -sF – TCP syn scan nechává na cílovém hostiteli otisky prstů a odhaluje tak identitu útočníka, běžně jsou IDS systémy nastaveny ke sledování SYN paketů. Z výše popsaných důvodů bylo využito FIN skenování, které inicializuje skenování pomocí paketu FIN. Protože mezi cílovým a zdrojovým hostitelem není žádná předchozí komunikace, cíl odpoví paketem RST a resetuje spojení a tím však odhalí svou přítomnost.



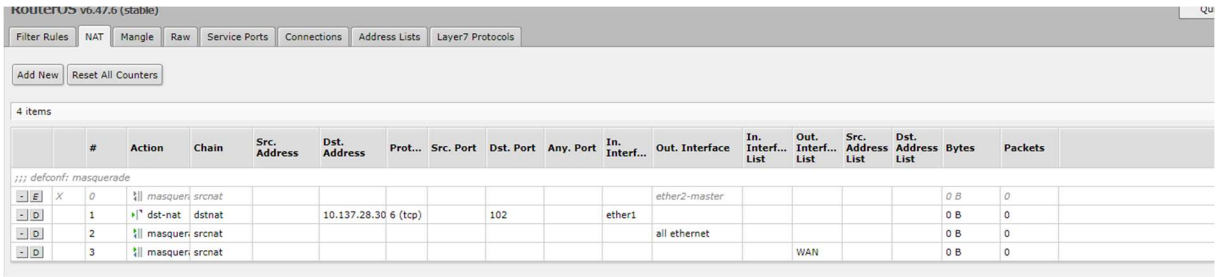
```
03/19/2021-06:21:31.878766  [**] [1:1000006:1] Nmap XMAS Tree Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:48784 -> 10.136.130.32:22
03/19/2021-06:21:31.878766  [**] [1:10000005:2] NMAP TCP Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:48784 -> 10.136.130.32:22
03/19/2021-06:21:31.987371  [**] [1:1000006:1] Nmap XMAS Tree Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:48785 -> 10.136.130.32:22
03/19/2021-06:21:31.987371  [**] [1:10000005:2] NMAP TCP Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:48785 -> 10.136.130.32:22
03/19/2021-06:21:34.766810  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 169.254.97.171:1740 -> 169.254.255.255:1740
03/19/2021-06:21:34.766897  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 169.254.97.171:1740 -> 169.254.255.255:1743
03/19/2021-06:21:34.766862  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 169.254.97.171:1740 -> 169.254.255.255:1742
03/19/2021-06:21:34.766847  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 169.254.97.171:1740 -> 169.254.255.255:1741
03/19/2021-06:21:45.955086  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 169.254.97.171:57019 -> 239.255.255.250:1900
03/19/2021-06:21:45.971262  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 169.254.97.171:57022 -> 239.255.255.250:1900
03/19/2021-06:22:01.013690  [**] [1:1000008:1] Nmap FIN Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:50451 -> 10.136.130.32:22
03/19/2021-06:22:01.013690  [**] [1:10000005:2] NMAP TCP Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:50451 -> 10.136.130.32:22
03/19/2021-06:22:01.122148  [**] [1:1000008:1] Nmap FIN Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:50452 -> 10.136.130.32:22
03/19/2021-06:22:01.122148  [**] [1:10000005:2] NMAP TCP Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:50452 -> 10.136.130.32:22
03/19/2021-06:22:20.036433  [**] [1:1000010:1] Nmap UDP Scan [**] [Classification: (null)] [Priority: 3] {UDP} 10.136.130.32:54956 -> 239.255.255.250:1900
03/19/2021-06:22:29.113282  [**] [1:1000009:1] Nmap NULL Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:58455 -> 10.136.130.32:22
03/19/2021-06:22:29.113282  [**] [1:10000005:2] NMAP TCP Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:58455 -> 10.136.130.32:22
03/19/2021-06:22:29.222354  [**] [1:1000009:1] Nmap NULL Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:58456 -> 10.136.130.32:22
03/19/2021-06:22:29.222354  [**] [1:10000005:2] NMAP TCP Scan [**] [Classification: (null)] [Priority: 3] {TCP} 10.136.130.20:58456 -> 10.136.130.32:22
```

Obrázek 13 : Screen z logu v programu Suricata

Na obrázku je vidět záznam z log souboru programu Suricata, který zachytil útok Network scanning. Detekce mají název NMAP FIN Scan , Nmap NULL Scan a Nmap XMAS Tree Scan. Pomocí nastavených pravidel v programu Suricata byl útok včas odhalen a lze podniknou další kroky k řešení této situace.

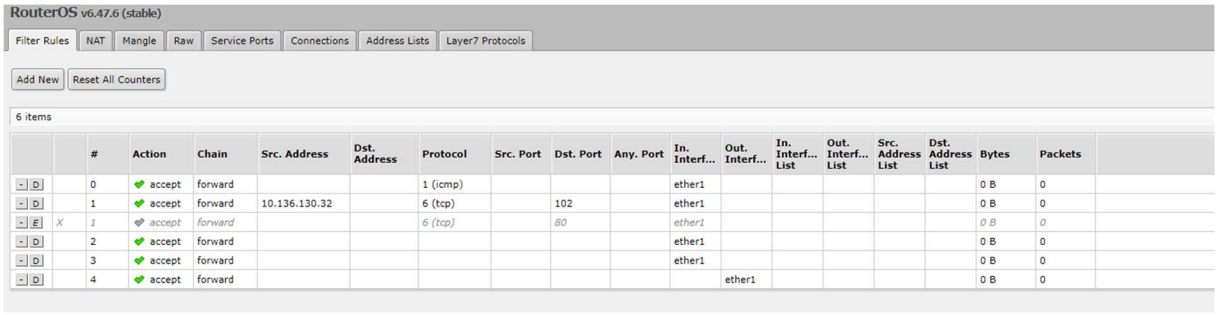
6.5 Zabezpečení portů

Na rozhraní klientů (PLC a jejich vnitřních sítí) je zde předřazen Mikrotik RouterBOARD RB750Gr3, který zajišťuje překlad IP adres pomocí NAT na adresu vnitřní sítě stroje většinou nastavenou v rozsahu 192.168.0.1/24 na adresu rozsahu průmyslové sítě v rozsahu 10.136.130.1/24 a to z výše důvodu jiného rozsahu IP stroje, které jsou na jednoúčelových strojích stejné a s takřka identickým nastavením vnitřních sítí.



Obrázek 14 : Screen z nastavení routeru MicrTik

No tomto RouterBOARDU jsou nastaveny pravidla, která povolují komunikaci pouze IP adrese serveru a to na určitém portu. Toto pravidlo a jeho nastavení je vidět na obrázku. Konkrétně se jedná o propustnost na portu 102 pro Siemens S7 a adresu serveru 10.136.130.40.



Obrázek 15 : Screen z nastavení routeru MicrTik

Dále pomocí jednoduchých pravidel pro firewall lze nastavit MAC adresy, které mají povolený přístup do MikrotikBOARDu, které doporučuji jako jedno ze základních nastavení pro průmyslové sítě.

7 Závěr

V rámci bakalářské práce se snažím navrhnout řešení vnitřního zabezpečení průmyslové sítě pro společnost Freudenberg Sealing Technologies s.r.o. V rámci práce jsem zmapoval technologii, kterou společnost používá a požadavky na průmyslovou síť, která bude instalována ve společnosti a bude sloužit hlavně pro sběr dat do systému MES. V práci popisuji jednotlivé komunikační protokoly, které se nejčastěji používají v průmyslové síti. Dále se zaměřuji na protokol ProfiNet, na kterém je postavena komunikace průmyslové sítě ve společnosti Freudenberg Sealing Technologies s.r.o. Zaměřuji se na průmyslové vybavení společnosti a jejich PLC, které komunikují pomocí ProfiNet a OPC UA.

Veškeré stroje komunikují za pomocí OPC serveru KepWare, který je instalován na místním virtuálním serveru a následně jsou data distribuována do aplikace Ignition, kde jsou k dispozici pro uživatele, kteří s daty pracují.

V práci jsem navrhl řešení průmyslové sítě a její rozdělení do segmentů, které snižují možnou plochu potenciálního útoku na průmyslovou síť. Tyto segmenty jsou rozděleny na logické a fyzické, kde jejich dělení je uspořádáno s ohledem na jejich polohu. Logické segmenty jsou virtuálního charakteru a jsou seskupeny na základě konkrétních funkcí. Jednotlivé strojní zařízení, jejich PLC a PC jsou z důvodu obsahu vnitřních LAN a stejných IP adres mezi PLC a PC připojeny pomocí routeru MicroTik, který je nastaven jako NAT a překládá pakety přicházející ze serveru na IP do rozsahu vnitřní sítě LAN. Na routeru je nastavena pouze příchozí komunikace ze serveru a to pouze na daný port, na kterém komunikuje zařízení. Dále je zde nastaven vnitřní firewall pro komunikaci pouze pro IP adresy serveru a stroje a jejich MAC adres, ostatní komunikace je „zahazována“.

Ostatní routery, které se nachází v síti a jsou nastaveny obdobným způsobem a to na komunikaci pouze určitého zařízení se serverem, pouze na určeném portu a z povolené MAC adresy a IP adresy.

Tato opatření v nastavení sítě zajistí co nejmenší plochu možného útoku na daný segment a popřípadě na celou průmyslovou síť. Tato opatření jsou doplněna o sledování sítě a jejich automatickém logování, které zajistí případné upozornění správce sítě na podezřelé aktivity, jako je pokus o připojení z jiné IP či MAC, popřípadě pokusu o změnu MAC adresy zařízení.

Pro ochranu linkové vrstvy je doporučeno sledování provozu na síti programem ARP watch, který monitoruje aktivitu na Ethernetové síti a udržuje databázi párování MAC a IP adres, které označuje časovým razítkem.

Pro síťovou vrstvu je navrženo ochrana pro protokol Internet Protocol (IP) filtrování paketů pomocí Firerwall a dále použití VPN tunelu mezi bezpečnostními zónami sítě.

Ke čtvrté vrstvě modelu OSI (Transportní vrstvě) je jako ochrana proti SYN paketům použita zvýšená fronta nevyřízených paketů a dále uzavření nejstarších polootevřených spojení pro uvolnění prostředků.

Dalším z opatřeních je včasná aktualizace softwaru prvků sítě a zařízení připojených do sítě.

Software, který v závěru práce navrhuji pro používání monitoringu sítě, je zejména pro sledování sítě, jako osvědčený nástroj Suricata a podobné, které jsou dostupné jak pro platformu Windows tak Linux, a které dokážou logovat dle zadaných pravidel. Při jejich správném nastavení je detekce a upozornění správce sítě včasné.

Jednotlivá opatření jsou zaměřena na události ohrožení z kapitoly 3.9, na které jsem se snažil vytvořit protiopatření a eliminovat popřípadě minimalizovat riziko potenciálního útoku.

7. SEZNAM ZDROJŮ

[1] SCADA (supervisory control and data acquisition). TechTarget. [online]. © 1999- 2015 [cit. 2015-05-24]. Dostupné z:http://whatis.techtarget.com/definition/SCADAsupervisory-control-and-data-acquisition

[2] Co se skrývá pod označením PLC ?. Automatizace.hw.cz. [online]. 1997 [cit. 2015- 05-24]. Dostupné z: http://automatizace.hw.cz/co-se-skryva-pod-oznacenim-plc

[3] D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942-1976, thirdquarter 2020, doi: 10.1109/COMST.2020.2987688

[4] UJVAROSI, Alexandru. Evolution of SCADA systems. *Bulletin of the Transilvania University of Brasov. Engineering Sciences. Series I*, 2016, 9.1: 63.

[5] Russel, J.: A Brief History of SCADA/ EMS. Available at: http://www.Scada history.com/. Accessed: 21.04.2016.

[6] Office of the Manager NCS: Supervisory Control and Data Acquisition (SCADA) Systems. Communication Technologies Inc., 2004

[7] GRILL, David. *SCADA systém Control Web* [online]. Plzeň, 2012 [cit. 2020-11-01]. Dostupné z: https://otik.zcu.cz/bitstream/11025/4029/1/BP_SCADA.pdf. Bakalářská práce. Fakulta elektrotechniky Západočeská univerzita Plzeň. Vedoucí práce Ing. jiří Basl Ph.D.

[8] PRIMUS, Tomáš. *Systémy SCADA a nástroje pro sběr, vizualizaci a analýzu průmyslových dat* [online]. Praha, 2017 [cit. 2020-11-02]. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/70825/F2-BP-2017-Primus-Tomas-scada%20systemy_FINAL.pdf?sequence=1&isAllowed=y. Bakalářská práce. ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE FAKULTA STROJNÍ. Vedoucí práce Doc. Ing. Ivo Bukovský, Ph.D.

[9] 4 SCADA/HMI systémy [online]. [vid. 2017-02-02]. Dostupné z: http://homel.vsb.cz/~rep75/Predmety/Distrib_sys/Vytah/04.htm

[10] Wonderware InTouch HMI [online]. [vid. 2017-02-02]. Dostupné z: http://global.wonderware.com/DE/Pages/WonderwareInTouchHMI.aspx

[11] Představili jsme finální podobu nového systému Control Web v7 [online]. [vid. 2017- 05-13]. Dostupné z: http://www.mii.cz/art?id=822&cat=146&lang=405

[12] SIMATIC WinCC V13 - Digital Factory & Process Industries and Drives - Siemens [online]. [vid. 2017-05-15]. Dostupné z: http://www1.siemens.cz/ad/current/index.php?vw=0&ctxnh=d8746d77f6&ctxp=home

[13] PLACHÝ LADISLAV. Siemens představuje vizualizační software WinCC v rámci nové verze TIA Portal V14. Automa. nedatováno, 16(11).

[14] *Výrobní informační systémy & Obchodní vizualizační systémy* [online]. [vid. 2017-05-18]. Dostupné z: http://www.iconics.com/Home.aspx?lang=cs-CZ

[15] *Iconics* [online]. 2017 [vid. 2017-05-14]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Iconics&oldid=771492417

[16] TIRS.NET 6 - profesionální SCADA/HMI systém. *CORAL s.r.o.* [online]. [vid. 2017-05-17]. Dostupné z: http://www.coral.cz/scada-hmi-systemy-tirs/tirs-net-6-profesionalni-scadahmi-system/

[17] *Co je PROMOTIC* [online]. [vid. 2017-02-07]. Dostupné z: http://www.promotic.eu/cz/pmdoc/WhatIsPromotic/WhatIsPromotic.htm

[18] CHOLT, Milan. *Informační bezpečnost v malých a středních podnicích* [online]. Praha, 2019 [cit. 2020-10-15]. Dostupné z: https://is.ambis.cz/th/ffuax/BP_Cholt_Informacni_bezpecnost_v_malych_a_strednich_podnicich.pdf. Bakalářská práce. Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS. Vedoucí práce Ing. Vladimír Beneš, Ph.D.

[19] ISSAYEV, Jovkhar. *Ochrana přístupu do sítě* [online]. Pardubice, 2020 [cit. 2020-10-12]. Dostupné z: https://dk.upce.cz/handle/10195/76139. Bakalářská práce. Universita Pardubice Fakulta elektrotechniky a informatiky. Vedoucí práce Ing. Soňa Neradová, Ph.D.

[20] BARTONÍČEK, Bc. Tomáš. *Analýza zabezpečení sítí na L2* [online]. Hradec Králové, 2020 [cit. 2020-10-12]. Dostupné z: https://theses.cz/id/f6z2uc/STAG93241.pdf. Diplomová práce. Univerzita Hradec Králové Fakulta informatiky a managementu Katedra informačních technologií. Vedoucí práce Mgr. Josef Horálek, Ph.D.

[21] CECC 2019: Proceedings of the Third Central European Cybersecurity Conference November 2019 Articlehttps://www.researchgate.net/publication/336765682_Simulating_and_Detecting_Attacks_of_Untrusted_Clients_in_OPC_UA_Networks

[22] MINAŘÍK, Pavel. Bezpečnost průmyslových sítí a systémů SCADA/ICS: Klíčem je viditelnost. *SystemOnLine* [online]. Brno: CCB, 2018, 9/2018, 2018(9), 4 [cit. 2020-08-05]. ISSN 1802-615. Dostupné z: https://www.systemonline.cz/rizeni-vyroby/bezpecnost-prumyslovych-siti-a-systemu-scada-ics.htm

[23] CHIOCK, Mario a Del RODILLAS. AUTOMA: časopis pro automatizační techniku. *AUTOMA* [online]. Děčín, 2016, 04/2016, 2016(04), 12 [cit. 2020-08-05]. Dostupné z: https://automa.cz/cz/casopis-clanky/kyberneticka-bezpecnost-prumyslovych-ridicich-systemu-cast-2-2016_04_0_11059/

[24] *Industrial Network Security* [online]. České vysoké učení technické v Praze, 2020 [cit. 2020-09-26]. Dostupné z: https://dspace.cvut.cz/handle/10467/89820. Bakalářská práce. České vysoké učení technické v Praze ,Fakulta elektrotechnická. Vedoucí práce Doc. Ing Leoš Boháč, Ph.D.PŘÍLOHY

[25] *Vhodná strategie pro detekci bezpečnostních incidentů v průmyslových sítích* [online]. ČVUT, 2020 [cit. 2020-09-28]. Dostupné z: https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/189110/final-thesis.pdf?sequence=1&isAllowed=y Diplomová. České vysoké učení technické v Praze ,Fakulta elektrotechnická. Vedoucí práce Ing. Radek Fujdiak, Ph.D.

[26] KNAPP, Eric D. a Joel Thomas LANGILL. Industrial Network Protocols. *Industrial Network Security* [online]. Elsevier, 2015, 2015, , 121-169 [cit. 2020-05-28]. DOI: 10.1016/B978-0-12-420114-9.00006-X. ISBN 9780124201149.

[27] PIGAN, Raimond a Mark METTER. *Automating with PROFINET*. 2nd. Germany: Publicis Publishing, 2008. ISBN 9783895789502.

[28] Belai, Igor & Drahoš, Peter. (2009). THE INDUSTRIAL COMMUNICATION SYSTEMS PROFIBUS AND PROFInet. Applied Natural Sciences. Dostupné z : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.7320&rep=rep1&type=pdf

[29] PROFINET Communication Channels – PROFINET University. PROFINET University – PROFINET University [online]. Copyright © 2019 [cit. 05.01.2020]. Dostupné z: https://profinetuniversity.com/profinet-basics/profinet-communication-channels/

[30] PROFINET – Standard pro průmyslový Ethernet v automatizaci [online]. Praha: SIMATIC Guide, 2005, 2005(4) [cit. 2020-01-05]. Dostupné z:

http://stest1.etnetera.cz/ad/current/content/data_files/automatizacni_systemy/prumyslova_komunikace/profinet/profinet_04_2005_cz.pdf

[31] *PROFINET IO: PROFINET Unplugged – An introduction to PROFINET IO* [online]. [cit. 2020-01-05]. Dostupné z: https://www.rtautomation.com/technologies/profinet-io/

[32] DOVICA, Martin. *Testování implementace sběrnice PROFINET do systémů Simotion* [online]. Ostrava, 2010 [cit. 2020-01-05]. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava. Dostupné z: http://hdl.handle.net/10084/78634

[33] KROUPA, Jiří. *Návrh ovladače pro PROFINET bus coupler* [online]. Brno, 2015 [cit. 2020-01-05]. Diplomová práce. Vysoké učení technické v Brně, Fakulta strojního Dostupné z : https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=104778

[34] SHIMANUKI, Y. OLE for process control (OPC) for new industrial automation systems. *IEEE SMC'99 Conference Proceedings. 1999 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No.99CH37028)* [online].
IEEE, 1999, , 1048-1050 [cit. 2020-05-28]. DOI: 10.1109/ICSMC.1999.816721.
ISBN 0-7803-5731-0.

[35] Federal Office for Inform. Security, "OPC UA Security Analysis," 2017.Dostupné z : https://arxiv.org/abs/2003.12341

[36] KNYTL, Radek. *Simulace útoků na síťovou infrastrukturu* [online]. Universita Pardubice, 2014 [cit. 2021-01-25]. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/55701/KnytlR_SimulaceUtoku_SN_2014.pdf?sequence=4&isAllowed=y. Bakalářská práce. Universita Pardubice Katedra Informačních technologií. Vedoucí práce Ing. Soňa Neradová.

8 Zadání práce

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2019/2020

Studijní program: Aplikovaná informatika
Forma studia: Kombinovaná
Obor/kombinace: Aplikovaná informatika (ai3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Miloš Etlík**
Osobní číslo:	**I1800485**
Adresa:	Ladova 301, Čeperka, 53345 Opatovice nad Labem, Česká republika
Téma práce:	Návrh zabezpečení automatizace řízení inteligentních průmyslových zařízení
Téma práce anglicky:	Design of automation control for intelligent industrial devices.
Vedoucí práce:	Mgr. Josef Horálek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je analyzovat stávající stav a navrhnout řešení zabezpečení automatizace řízení inteligentních průmyslových zařízení za využití komunikačního protokolu Profinet a systémů řízení Scada.
V teoretické části práce provede rešerši možných řešení a analýzu stávajícího stavu v konkrétním průmyslovém prostředí. Na základě výsledků analýzy pak v praktické části navrhne a v maximální možné míře otestuje zabezpečení automatizace řízení inteligentních průmyslových zařízení.

Seznam doporučené literatury:

JI, Xiu. *PROFINET in Practice : Installation, Maintenance, Design and System Engineering*. Independently Published, 2019. ISBN 9780655327172.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: