Zabezpečení průmyslových počítačových sítí

Bc. Erik Vančo

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Erik Vančo**
Osobní číslo:	**A19417**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Zabezpečení průmyslových počítačových sítí**
Téma práce anglicky:	**Security of Industrial Computer Networks**

Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Popište bezpečnost průmyslových sítí – rizika, problémy, poruchovost, odolnost proti nechtěným zásahům na platformách LAN, MODBUS RTU over RS485 a MODBUS TCP/IP.
3. Zanalyzujte nynější stav zabezpečení průmyslové sítě.
4. Navrhněte řešení zabezpečení průmyslové sítě včetně přechodu z různých komunikačních protokolů, nastavení firewallů a L2 switchů, nastavení Active Directory a Windows Server Update Services.

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

Seznam doporučené literatury:

1. MATOUŠEK, P. *Síťové aplikace a jejich architektura*. Brno: VUTIUM, 2014. ISBN 978-80-2143-766-1.
2. BEASLEY, J. S. *Networking*. 2nd edition. Upper Saddle River: Prentice Hall, 2009. ISBN 978-0-13-135838-6.
3. DESMOND, B., RICBARDS, J., ALLEN, R. and A. G. LOWE-NORRIS. *Active Directory*. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 978-1-4493-2002-7.
4. ELAHI, A. and M. ELAHI. *Data, Network, & Internet Communications Technology.* 1st edition. Florence: Delmar Cengage Learning, 2005. ISBN 978-1-4018-7269-4.
5. MOSKOWITZ, J. *Group Policy: Fundamentals, Security and the Managed Desktop*. 2nd edition. Nashville: John Wiley & Sons, 2013. ISBN 978-1-118-28940-2.

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Jméno, příjmení: Erik Vančo

Název diplomové práce: Zabezpečení průmyslových počítačových sítí

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 26.5.2021

Erik Vančo, v. r.
podpis diplomanta

ABSTRAKT

Vzhledem k rozvíjející se kybernetické kriminalitě, která se aktivně rozšiřuje do průmyslových sfér, je nutno zavádět formy zabezpečení a bezpečnostních politik na úrovni průmyslových datových sběrnic. V rámci práce jsou rozebrány otázky zabezpečení komunikačních protokolů Modbus a průmyslových datových sběrnic. Poté je provedena analýza na úrovni průmyslové datové sítě a jsou navrženy soubory opatření, jež lze bezvýpadkovitě realizovat k zajištění alespoň základních stupňů zabezpečení proti poruše, nechtěným zásahům a výpadkům průmyslové datové sítě.

Klíčová slova: zabezpečení, rizika, zranitelnost, sběrnice, místní síť, Ethernet, model TCP/IP

ABSTRACT

Due to developing cybercrime which is spreading actively into industrial sections, it is necessary to introduce some forms of security and security policy at the level of industrial databus. Within a framework of the thesis, the issue of Modbus communication protocols and industrial databus is analysed. Then an analysis at the industrial data network level is implemented and sets of measures are proposed, that can be implemented without any blackout for a provision of at least basic security stages against failure, accidental intervention and industrial data network outage.

Keywords: Security, risks, vulnerability, databus, local area network, Ethernet, TCP/IP model

Děkuji Ing. Miroslavu Matýskovi, Ph.D. za systémovou pomoc a vedení diplomové práce. Dále děkuji panu Ing. Josefovi Frydrýškovi vzhledem k jeho přínosným podnětům k tématu.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická, nahraná do IS/STAG, jsou totožné.

OBSAH

ÚVOD

Vlivem stále se rozšiřujících požadavků na efektivitu výroby, získávání dat z výroby a zásahy do řízení výroby bylo nutno stanovit takové podmínky pro spojování technologií a zařízení, které by umožňovaly propojit tato zařízení a umožnit komunikaci mezi nimi. Proto bylo nutno zřizovat datové sběrnice v průmyslu a spojovat je do komunikačních celků.

V průmyslu je primární požadavek na plynulost a bezporuchovost výroby, a proto byly datové sběrnice často konstruovány s výchozím cílem zajistit přenos dat mezi zařízeními za každou cenu, což vedlo k potlačování požadavků na bezpečnost přenosu dat. V průmyslu se začaly objevovat sériové sběrnice, které již umožňovaly robustní přenos dat na delší vzdálenosti. Jednalo se o sběrnice typu RS485. Nad těmito sběrnicemi byly vytvořeny komunikační protokoly, příkladem je komunikační protokol Modbus RTU.

Kolem roku 2000 se do průmyslu začíná postupně dostávat řešení komunikací na úrovni komunikačního standardu Ethernet spolu s požadavky na jeho komunikační sběrnice. V té době byl již standard Ethernet rozšířen v komerční sféře a začaly se objevovat první náznaky zneužití rizik spojených s touto komunikační platformou. Do té doby byly v průmyslu téměř výhradně využívány sběrnice typu RS485, jež neumožňovaly tak snadné napadení z externích míst. Pokud došlo k poruše nebo k incidentu, bylo toto místo poměrně rychle odhaleno a opraveno. Navíc při poruše na jedné lince komunikace nebyly tímto stavem dotčeny linky jiné. Díky Ethernetu bylo docíleno částečné centralizace spojů a sběrnic, protože byly vzneseny požadavky na připojení co nejvyššího počtu zařízení do komunikačního standardu Ethernet. Zabezpečení komunikací platformy Ethernet bylo v počátcích své existence a nebylo tedy primárně nasazováno. Většina firem v průmyslu začala s nákupem nových technologií preferovat přenos dat na standardu Ethernet. Jednotlivé nové technologické celky byly spojovány do větších komunikačních celků, sběrnice pro přenos dat byly primárně uzpůsobeny pro komunikaci uvnitř technologických celků dle požadavků na danou technologii, což s sebou neslo nekoncepčnost řešení a minimální požadavky na bezpečnost a zabezpečení. Mezitím se v komerční sféře stále více rozvíjelo páchání kybernetické kriminality a bylo jen otázkou času, kdy tento trend zasáhne do průmyslové sféry. Objevily se první programy pro páchání kybernetické kriminality, jejichž cílem bylo generovat zisk pro útočníky, nebo byly cíleně napadány společnosti s cílem ochromit jejich výrobu.

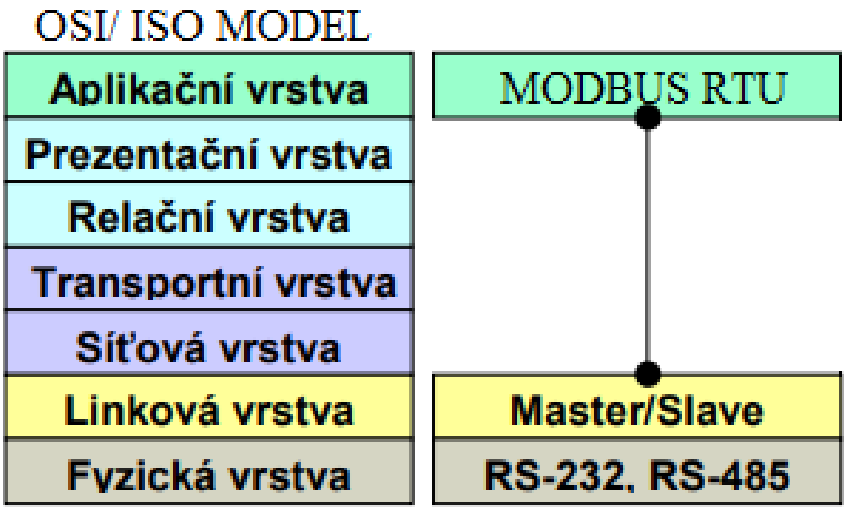
I. TEORETICKÁ ČÁST

1 BEZPEČNOST PRŮMYSLOVÝCH DATOVÝCH SÍTÍ

Bezpečnost průmyslových datových sítí je dána především požadavky na bezproblémový přenos dat mezi zařízeními nehledě na platformu, která zprostředkovává přenos dat. Poté jsou brány v potaz náklady na navržená řešení a až v poslední řadě je brán zřetel na bezpečnost a zabezpečení komunikačních platforem. Vzhledem k rozmanitosti komunikačních protokolů a sběrnic budou v rámci práce rozebrány nejrozšířenější otevřené komunikační protokoly a jejich sběrnice.

1.1 Modbus RTU

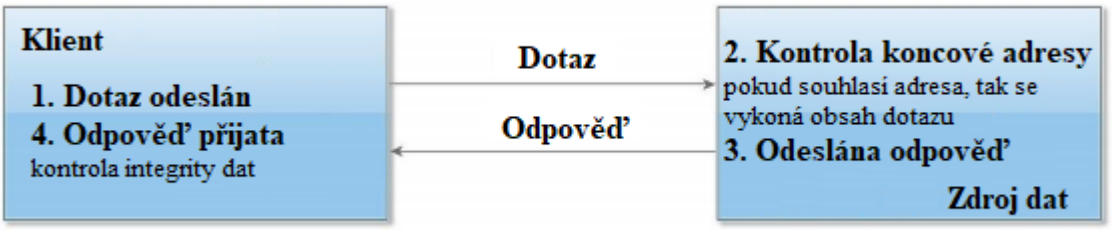
Jedná se o otevřený komunikační protokol, využívaný více než čtyři dekády, jenž byl vytvořen a představen v roce 1979 firmou Modicon. Protokol Modbus RTU bývá využíván převážně pro komunikaci v SCADA (Supervisory Control And Data Acquisition) aplikacích, kde jsou komunikovány údaje z čidel, částí polní instrumentace a dalších průmyslových komponentů, nebo je používán pro komunikaci mezi průmyslovými systémy. Protokol Modbus RTU je definován na úrovni aplikační vrstvy v modelu OSI/ISO (Open System Interconnection/ International Organization for Standardization) – viz Obr. 1 [1].



Obr. 1 Modbus RTU ve struktuře referenčního modelu OSI/ISO [1]

Komunikační protokol se vyznačuje vyžádanou komunikací typu klient–server, kde v rámci komunikačního protokolu může být zastoupen jeden klient a až 247 serverů připojených k jednomu klientovi, které jsou vždy adresovány. Vyžádanou komunikací se rozumí

komunikace, která je inicializována klientem, může být označen jako master, a serverem, tedy zdrojem dat označovaných jako slave. Server sám o sobě nikdy neposkytuje data, vždy pouze odpovídá nebo reaguje na dotazy, jež jsou mu zaslány. Klient může inicializovat komunikaci mezi sebou a jednotlivými servery nebo může využívat takzvaný multidotaz, na který servery jednotlivě odpovídají, dotaz je složen ze čtyř částí. V první části dotazu je zaznamenána adresa serveru, se kterým je inicializována komunikace, ve druhé části dotazu je zanesena informace, co má server vykonat. Ve třetí části dotazu jsou poskytována data ze serveru nebo data o vykonání požadovaného úkonu. Čtvrtou částí dotazu je přenášena informace o konzistenci dat. Jako kontrola konzistence dat je u komunikačního protokolu Modbus RTU využito kontrolního mechanismu řešeného pomocí cyklické redundantní kontroly, jedná se o jedinou možnost, jak ověřit, zda přenesená data jsou konzistentní, a nejsou tedy znehodnocena [2].



Obr. 2 Příklad Modbus RTU komunikace [2]

Pro bezpečný přenos informace z jednoho zařízení do druhého je nutné zabezpečit správnou implementaci komunikačního protokolu do zařízení a správnou instalaci komunikačního média. V komunikačním protokolu Modbus RTU nejsou implementovány žádné prvky bezpečnosti. S ohledem na zabezpečení přenosu dat, která mohou být zneužita, lze definovat možná rizika a problémy [2].

1.1.1 Zranitelnosti protokolu Modbus RTU

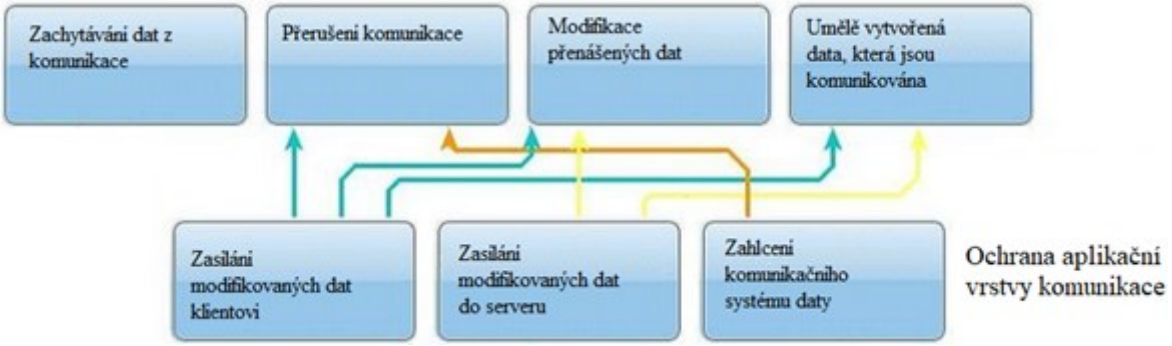
Z pohledu přenášených dat lze definovat čtyři základní stupně rizik pro komunikační protokol, a sice zachytávání dat, přerušení komunikace, modifikace přenášených dat a vysílání plně podvržených dat [3].

Zachytávání provozních dat umožňuje útočníkovi zjistit, jaká data jsou přenášena, jaká zařízení jsou pomocí komunikačního protokolu obhospodařována. Jedná se především o monitorování komunikace, která je přenášena. Tímto krokem útočník monitoruje stav sítě a dostává ucelenou představu, kolik zařízení je připojených k dané síti a v jakém časovém horizontu jsou odesílány požadavky na komunikaci a její obsah [2].

Dalším bodem může být snaha útočníka přerušit komunikaci nebo ji zpomalit natolik, aby byl systém komunikace vyhodnocen jako problematický. K takovéto kompromitaci systému může dojít jeho přetížením. Například lze systém vybavený komunikačním rozhraním Modbus RTU přetížit neustálým požadováním odpovědí nebo provedením úkonů, které vykonávají servery, a tím zapříčinit zahlcení a nefunkčnost komunikace. Následně může dojít k nestandardní situaci, poruše a škodám na majetku [3].

Neopomenutelným rizikem je možnost modifikovat přenášená data. Ta mohou být modifikována dvojím způsobem. Jako první můžeme zmínit modifikaci dat, která způsobí vyhodnocení chybné integrity přijatých dat u klienta, což zapříčiní, že data nejsou dále zpracována. Klient tedy zasílá nový požadavek na data a ta opět přijdou poškozena, výsledkem je zahlcení sběrnice a nefunkčnost systému. V druhém případě můžou být data podvržena způsobem, že kontrola dat na klientské straně proběhne v pořádku, v tomto případě jsou data zpracována a komunikace probíhá nadále beze změny. Takto podvržená data mohou být prezentována do nadřazených systémů, které mohou řídit technologie. V tomto případě nejde útočníkovi o okamžitou nefunkčnost systému, ale je cíleno na celkovou technologii. Důsledkem modifikace dat může být zvýšená kazivost výrobků, vyšší spotřeba energií, vyšší opotřebení technologie a další. Výsledkem je vyšší ekonomická náročnost technologie [4].

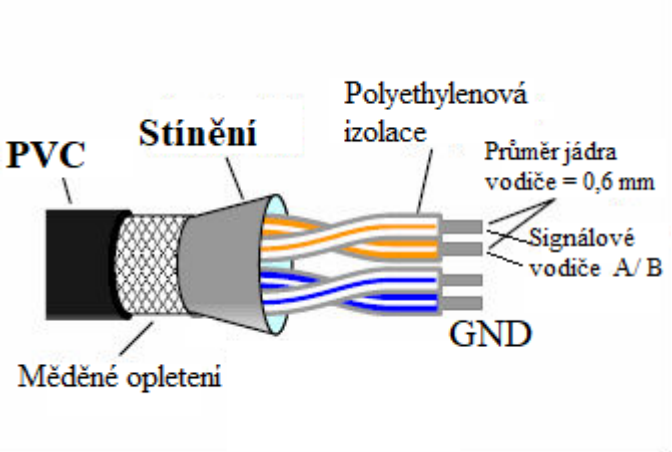
Další možností, jak kompromitovat komunikaci, je vysílat data, která nejsou modifikována, nýbrž jsou plně uměle vytvořena útočníkem. Ten je maskován jako součást komunikačního systému a odpovídá na dotazy vysílané klientem. Útočník dotaz přijme, zpracuje a pošle odpověď. Vzhledem k tomu, že útočník je plně integrován do komunikačního řetězce, mohou být přenášená data plně kompromitována. Klient v takovémto případě vyhodnotí kontrolu integrity (zda je v pořádku), data předá dále, nebo je zpracuje. Takovéto kompromitace může být využito například při vývoji technologie, kdy je útočníkem trvale sabotován vývoj [4].



Obr. 3 Bezpečnostní rizika komunikačního protokolu Modbus RTU [2]

Výše uvedená rizika představují možný bezpečnostní problém při použití komunikačního protokolu Modbus RTU. Nicméně komunikační protokol potřebuje ke své funkci přenosové prostředí, které je vytvořeno na úrovni fyzické vrstvy ve struktuře OSI/ISO, viz Obr. 1. Proniknutí útočníka do komunikace musí být nejdříve realizováno připojením dalšího zařízení do přenosové sběrnice. Jedná se především o sériové linky typu RS232, RS422 a RS485. V průmyslovém prostředí je nevíce zastoupena komunikace pomocí sériové diferenční sběrnice poloduplexního charakteru, tedy sběrnice RS485.

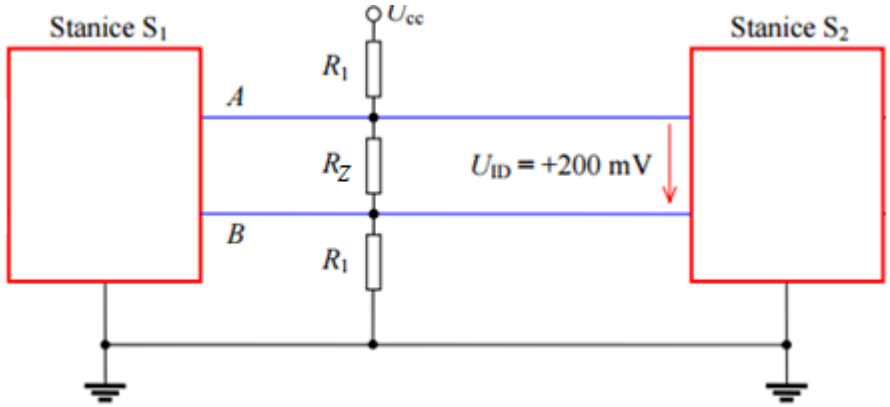
Sběrnice RS485 podléhají standardu EIA485 (Electronic Industries Alliance) (ISO 8482), kde jsou definovány parametry obvodů pro tyto sběrnice. Dle zmíněných standardů jsou definovány hodnoty vstupních impedancí R_i obvodů pro sběrnici RS485, zapojení terminačních (ukončovacích) rezistorů R_t na konci vedení, rozsah komunikačního napětí a hodnoty proudů protékajících komunikačními linkami A a B. Vlivem toho, že standard RS485 není závazný, jednotliví výrobci zařízení, která používají ke komunikaci sběrnici RS485, si tuto sběrnici různě modifikují a přizpůsobují [5].



Obr. 4 Doporučený kabel pro sběrnici RS485 [6]

Sběrnice typu RS485 je realizována pomocí kabelů (viz Obr. 4), které se vyznačují dvěma páry kroucených vodičů, sloužících k propojení jednotlivých zařízení. Jeden pár vodičů je využit pro datový přenos a druhý pár je pro distribuci jednotného potenciálu v rámci sběrnice. Zařízení určená pro komunikaci po sběrnici RS485 jsou vybavena pomocí sestavy vysílače a přijímače, které umožňují obousměrnou komunikaci. Funkce vysílače je řešena jako zapojení diferenciálního zesilovače, který je zapojen svým výstupem na sběrnici, kdežto u přijímače jsou zapojeny komunikační vodiče do vstupů operačního zesilovače. Z takového zapojení vyplývá hlavní přednost komunikační sběrnice, a tím je diferenciální přenos dat, kdy fyzikálně přenášená data jsou vyhodnocována pomocí diference, tedy rozdílu potenciálů mezi datovými vodiči, čímž je zajištěna vysoká odolnost sběrnice proti zarušení cizím elektromagnetickým polem [5].

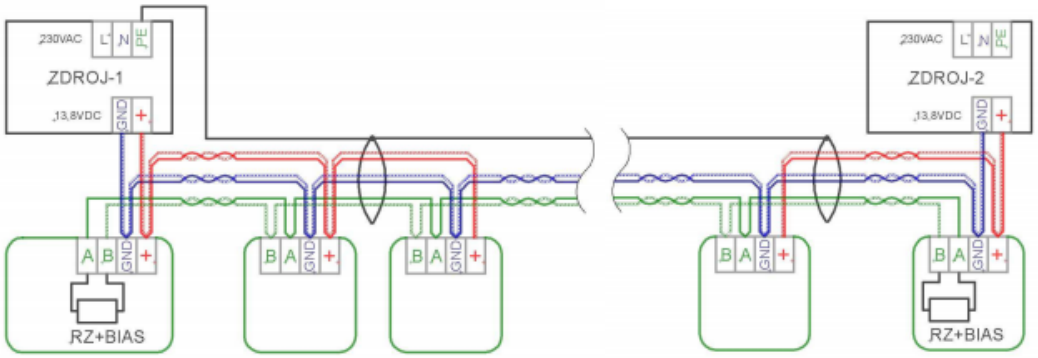
Pro úspěšný přenos informace musí být dodržena podmínka rozdílu potenciálů mezi vodiči A a B v minimálním rozsahu 200 mV. Sběrnice tedy zajišťuje sdílenou platformu pro vysílání a příjem dat. Při využití komunikačního protokolu Modbus RTU je nutno na sběrnici stanovit vysílací pravidla, a to pomocí zařízení, které se označuje jako master. Ostatní zařízení jsou označena jako slave. Master jednotka řídí procesy komunikace na sběrnici a zajišťuje, aby na sběrnici nevznikaly kolize. Pokud nejsou požadavky na vysílání a příjem dat, vysílací části zařízení jsou neaktivní. Sběrnice funguje de facto jako anténa, na sběrnici mohou tedy elektromagnetickou indukcí vznikat nežádoucí rušivá napětí, jež mohou být vyhodnocena jako korektní stavy. Pro vymezení nežádoucích stavů na sběrnici RS485 jsou definovány takzvané klidové stavy sběrnice RS485. Definovány jsou odporovým děličem sestaveným z odporů R_1, R_Z – viz Obr. 5 [7].



Obr. 5 Definice klidových stavů na sběrnici [5]

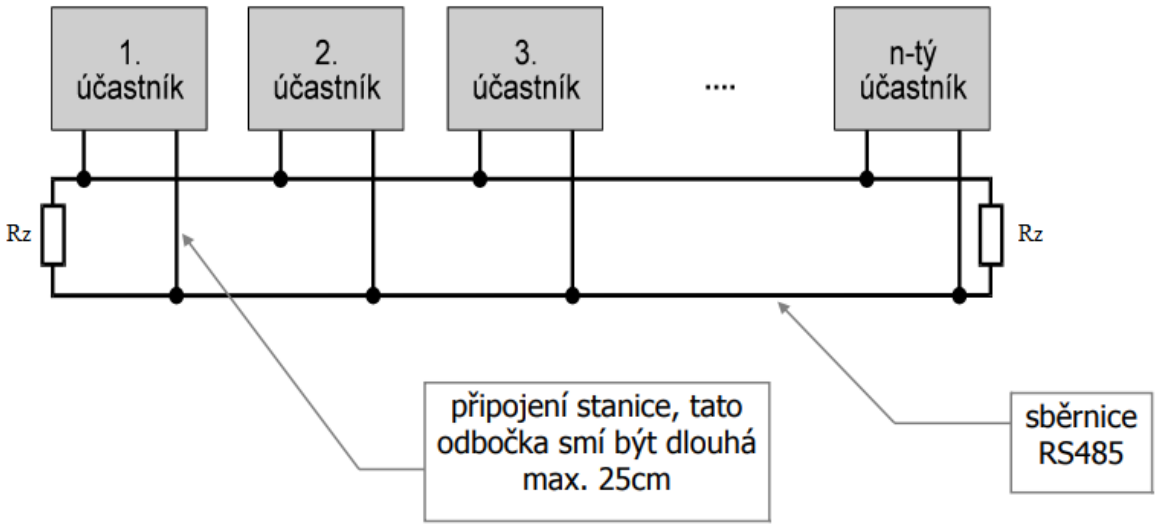
Rezistory R_Z jsou připojovány na konce sběrnice pro eliminaci odrazů a jejich jmenovitá velikost by měla reflektovat impedanci sběrnice. Sběrnice je omezena na připojení maximálního počtu 32 zařízení. Vlastností sběrnice RS485 je dosti úzká závislost délky vedení na rychlosti komunikace, při délkách sběrnice kolem 10 m může rychlost komunikace dosahovat hodnot atakujících 10 Mb/s, avšak při maximální délce sběrnice 1200 m se rychlost komunikace pohybuje kolem 30 kb/s. Pro konkrétní výrobce se jednotlivé vazby rychlosti na vzdálenost značně liší [7].

Pro komunikaci pomocí sběrnice RS485 je stěžejní dodržení instalačních pokynů výrobce zařízení, pro které je sběrnice vytvářena.



Obr. 6 Příklad sběrnice firmy ESTELAR [8]

Zařízení připojená na sběrnici jsou identifikována pomocí unikátní adresy. Sběrnice může být provedena jako průběžná, kde je zapojení sběrnice vedeno ze stanice do stanice (viz Obr. 6), nebo může být řešena s aktivní odbočkou, či s pasivní odbočkou (viz Obr. 7).



Obr. 7 Sběrnice RS485 s pasivní odbočkou firmy TECO a.s. [9]

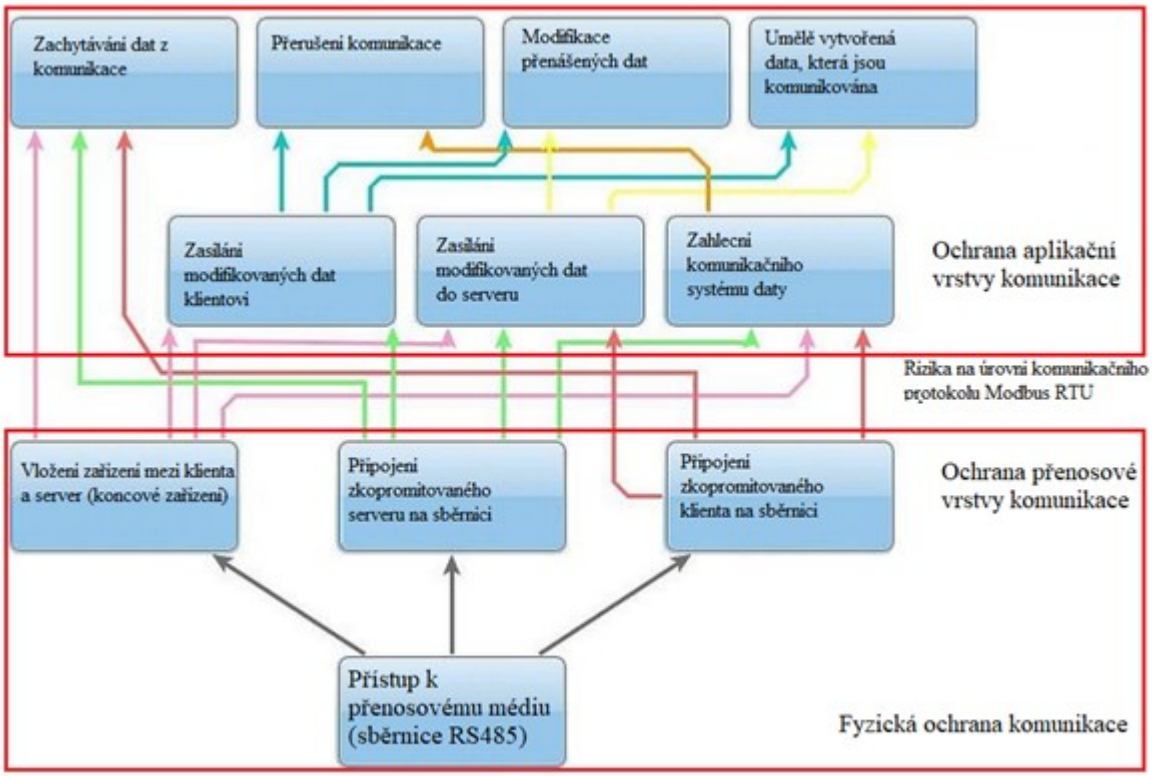
Možná rizika plynoucí z využívání přenosové sběrnice typu RS485 mohou představovat způsoby, jak kompromitovat data po ní přenášená. Z pohledu bezpečnosti může dojít ke čtyřem případům, jak kompromitovat přenos dat po sběrnici RS485.

Prvním příkladem může být plné rozpojení, tedy zničení přenosové cesty. Po takovémto zásahu sběrnice nemůže plnit svou roli a vlivem neodborného přerušení sběrnice může dojít až k poškození zařízení připojených na tuto sběrnici. Nicméně takto vzniklý incident je poměrně rychle odhalen a opraven.

Dalším rizikem může být vložení zařízení do sběrnice, kdy je sběrnice rozpojena a zařízení se stává její nedílnou součástí. Takovéto zařízení monitoruje veškeré dění na sběrnici, může zachytávat komunikaci, vyvolávat akce na serverech připojených ke sběrnici, odpovídat na dotazy klienta. Pomocí takového zařízení může útočník plně ovládnout komunikaci probíhající na sběrnici a může modifikovat přenášená data. Zařízení je obtížně detekovatelné, jelikož se stává plně integrovaným do sběrnice.

Pokud se útočníkovi nepodaří vložit zařízení přímo do sběrnice, může kompromitovat koncové zařízení (server). Pomocí kompromitovaného serveru je útočníkovi umožněno modifikovat odpovědi na dotazy klienta nebo upravovat reakce serveru na příkazy klienta.

Stejně lze kompromitovat i klienta. Útočníkem poté může být upravována komunikace, odesílány příkazy směrem k serverům, může být způsobeno zahlcení komunikace nebo může docházet k úpravě dat směrem do nadřazeného systému.



Obr. 8 Zranitelnosti sběrnice RS485 a komunikačního protokolu Modbus RTU

1.1.2 Odolnost komunikačního protokolu Modbus RTU

Odolnost je dána především schopností nosné sběrnice zajistit komunikační cestu pro protokol Modbus RTU i při nenadálých událostech nebo při zarušení sběrnice. Pokud je sběrnice zapojena jako průběžná (viz Obr. 6), pak při jakémkoliv jejím rozpojení dochází ke ztrátě komunikace se zařízeními, jež se vyskytují za místem rozpojení. Po opětovném připojení odpojené časti sběrnice dochází k téměř okamžitému obnovení komunikace. Při použití odbočky pro připojení zařízení na sběrnici jsou, při rozpojení na trase odbočky, zasažena pouze zařízení dislokovaná na této odbočce. Větší problém představuje chybně

zhotovená sběrnice, kdy je použito nesprávných typů kabelů a vlivem této skutečnosti může docházet k zarušení sběrnice kvůli elektromagnetické indukci, která působí na kabel. Proto je doporučeno používat pro vedení linek typu RS485 kroucené dvojlinky. Pokud je linka vedena v rámci více objektů, je zapotřebí používat zařízení s galvanicky oddělenými řadiči, které jsou připojeny na sériovou sběrnici, nebo zajistit distribuci stejného výchozího potencionálu pro všechna zařízení připojená na sběrnici. Dalším problémem je spojení obou komunikačních vodičů sériové linky nebo neosazení koncových terminačních rezistorů, což může způsobit odrazy na koncích sběrnice.

1.2 Místní sítě – LAN

Místní sítě, označované jako LAN (Local Area Network), jsou komunikační sběrnice sloužící k propojení jednotlivých geograficky blízkých zařízení nebo k propojení blízkých komunikačních celků. Sběrnice jsou tvořeny z fyzické a logické topologie. Fyzickou topologií je udáváno zapojení kabelů, spojení jednotlivých uzlů a způsob šíření signálu. Logická topologie vychází ze způsobu vzájemné komunikace. Zařízení připojená k logické sběrnici jsou unikátně identifikována v rámci konkrétního segmentu sběrnice. Po takto tvořených sběrnicích probíhá komunikace pomocí komunikačních protokolů. Dle zvoleného komunikačního standardu musí být přizpůsobeno tvoření sběrnice. Nejběžnějším typem komunikační sběrnice je v dnešní době sběrnice tvořená dle standardu Ethernet [10].

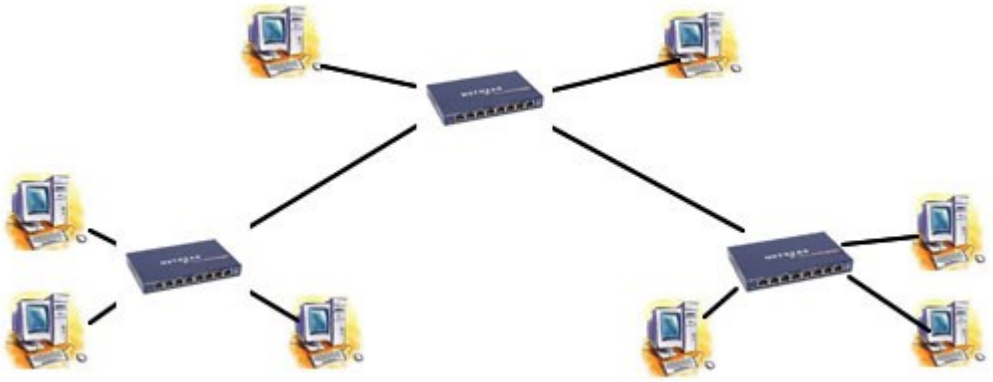
Obr. 9 Příklad místní sítě [11]

Pojem Ethernetu je definován jako standard s označením IEEE 802.3 (Institute of Electrical and Electronics Engineers). Sběrnice tvořeny dle standartu ethernet, používají pro řízení přístupu na sběrnici kontrolní protokol CSMA/CD (Carrier Sense Multiple Access with Collision Detection), který definuje algoritmus pro přístup a vysílání dat na sběrnici. Zařízení nejsou omezena v přístupu ke sběrnici a monitorují provoz na sběrnici, tedy naslouchají provozu na sběrnici. Pokud je kanál volný, dochází k vysílání dat. Stanice přitom kontroluje vysílaná data a naslouchá, zda nedošlo ke kolizi dat. Pokud je zjištěno, že nastala kolize dat, tak se vysílací stanice odmlčí. Interval odmlčení, si každá stanice, která detekovala kolizi, náhodně zvolí ze stanoveného intervalu. Pokud se situace opakuje, tak vysílací stanice zdvojnásobí původně zvolený časový interval odmlčení. Sběrnice může být rozdělena do segmentů a částí, tak aby se omezily přeslechy na sběrnici, omezila se kolize dat a došlo k separaci tranzitu na jednotlivých částech sběrnice. Takto rozdělená sběrnice (při správné segmentaci) může dosahovat vyšších přenosových rychlostí, dále je zajištěno, že primární provoz dat na sběrnici je soustředěn do jednoho segmentu sběrnice s minimálním dopadem do dalšího segmentu. Sběrnice může být realizována pomocí různých fyzických médií, jako jsou koaxiální kabel, kroucená dvojlinka, optické vlákno, nebo řešena pomocí bezdrátových technologií. V dnešní době jsou pro tvorbu místních sítí využívána fyzická média typu optického vlákna, kroucené dvojlinky a bezdrátových technologií pro přenos dat v topologiích hvězda, strom a v průmyslové sféře se používá topologie kruhu pro kritické komunikace v rámci infrastruktury výroby [10][12].

Sběrnice dle topologie hvězda jsou sestaveny z koncových zařízení a síťových přepínačů, propoje mezi nimi jsou v provedení strukturované kabeláže, buď metalickými propoji, nebo optickými vlákny. Data jsou přenášena z koncového zařízení do síťového prvku, nejčastěji síťového přepínače, odkud dále pokračují k dalšímu zařízení. V praxi to znamená, že síťový přepínač plní roli opakovače a zesilovače [10].

Obr. 10 Topologie hvězda [13]

Topologie typu strom je definována jako spojení více topologií typu hvězda do jednoho funkčního celku. Jednotlivé části sběrnice jsou spojeny do síťových přepínačů, které jsou poté mezi sebou vzájemně propojeny a tvoří páteřní datovou sběrnici. Síťové přepínače jsou obvykle vybaveny zvláštní sadou komunikačních portů, jež podporují vyšší přenosové rychlosti a jsou použity pro propoje mezi jednotlivými síťovými přepínači.

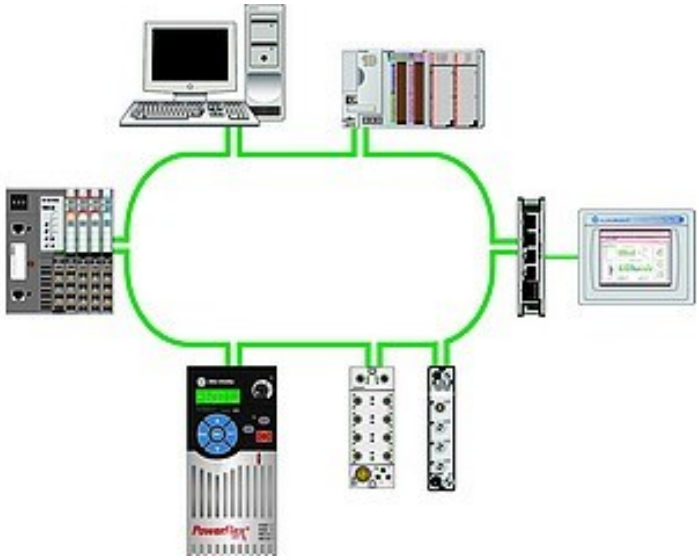


Obr. 11 Příklad stromové struktury [13]

V rámci vývoje byly postupně definovány standardy pro sběrnice, které jsou využívány pro přenos informace. V dnešní době je využíván především Fast Ethernet, používající pro přístup na sběrnici metodu CSMA/CD. Podporuje topologii hvězdy ve standardu 100BaseTX, kde se při přenosu informace uplatňuje strukturovaná kabeláž dle definice 100BaseTX. Zde je využito dvou vodičů v podobě dvou kroucených párů dvojlinky, přičemž jeden z dvojice je určen k detekci kolize na sběrnici a příjmu dat a druhý je využit pro datový přenos s přenosovou frekvencí 125 MHz. Přenášený signál je kódován, aby bylo docíleno

vyšší spolehlivosti přenosu, proto je propustnost přenášených dat redukována na 80 % kapacity přenosového média, tedy 100 MHz. Maximální délka přenosové cesty mezi dvěma body je omezena na 100 m kabelové trasy. Pro přenos dat pomocí optických vláken byl definován standard 100BaseFX, kde je jedno optické vlákno určeno pro detekci kolize a příjem dat a druhé pak pro přenos dat. Pro optický přenos dat je definována maximální vzdálenost 412 m mezi dvěma body. Pro větší datové přenosy jsou vymezeny standardy na úrovni gigabitového Ethernetu [14].

Kruhová topologie a její přenosový protokol byly vyvinuty firmou IBM, definovány jako standard IEEE 802.5 a jsou realizovány pomocí síťových prvků, jež tvoří uzavřený komunikační kruh a vynikají dokonalejším využitím přenosových kapacit sběrnice, jelikož je řízena komunikace i přístup zařízení na sběrnici. Řízení je realizováno pomocí předávání takzvaného tokenu, tedy práva na vysílání dat na sběrnici. Právo vysílat je časově omezeno, aby nedocházelo k nedefinovatelným prodlevám na sběrnici. Tím je zaručeno, že každému členu kruhu je umožněno komunikovat. Vlivem deterministického přístupu a přesně definovanému chování je nutno zvažovat i nejrůznější problémové a nahodilé stavy, jako jsou rozpojení kruhu, přidání zařízení do kruhu a disfunkce předávání práva na přístup na sběrnici. Kvůli takovým stavům je nutno v kruhu zřídit funkci monitoringu, kterou může plnit jedno zařízení připojené ke kruhu. Dále je třeba zajistit možnost komunikace z kruhu ven do dalších segmentů sítě. Je nutné zajistit, aby v rámci kruhu byl vždy pouze jeden monitorovací prvek, při výpadku nebo nefunkčnosti monitorovacího prvku musí být stanoveny takové priority a pravidla, aby byla monitorovací služba přiřazena na jiné funkční zařízení. Vlivem nemožnosti definice všech nahodilých stavů, které se mohou vyskytovat na sběrnici, jsou při poruchách sběrnice vysílány monitorovací rámce, jež mají za úkol shromažďovat informace o nahodilých stavech, jejich příčinách a možnostech vedoucích k vymezení těchto stavů. Výhodou topologie token ring je možnost implementace prioritizace vysílacích práv, kdy je jednoznačně stanoveno, jaká data mají být upřednostněna na úkor ostatních. Díky velmi robustnímu komunikačnímu mechanismu je síť v topologii kruhu využívána především v aplikacích, které mají vysoké nároky na spolehlivost komunikace [12] [14].



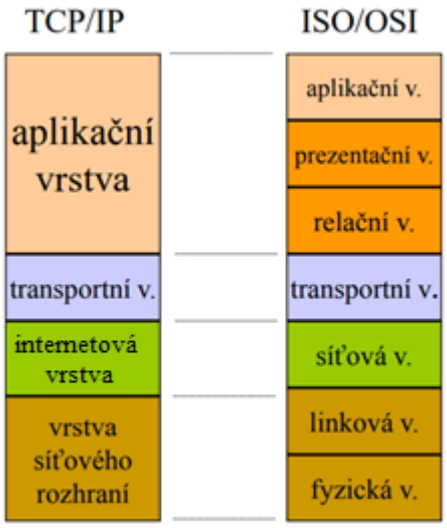
Obr. 12 Příklad komunikace na bázi kruhu od firmy Rockwell Automation [15]

1.2.1 Model TCP/IP

Referenční model OSI/ISO je koncipován jako sestava vrstev a úkonů, jež jsou v rámci jednotlivých vrstev řešeny. Jedná se o model sestavený k definování standardů pro komunikaci po sítích mezi zařízeními od různých výrobců [16]. Představuje výchozí model, dle kterého jsou koncipovány struktury novějších komunikačních protokolů. Referenční model OSI/ISO byl sestaven z definice sedmi po sobě jdoucích vrstev. V každé z nich jsou popsány postupy pro komunikaci mezi dvěma zařízeními pouze na úrovni této vrstvy. Každá vrstva referenčního modelu OSI/ISO jednoho zařízení vytváří komunikační spojení se stejnou vrstvou druhého zařízení. Mezi jednotlivými zařízeními se tak vytvoří komunikační kanál. Tento princip komunikace vyžaduje vysoké nároky na prvotní režii vytvoření spojení, ale omezuje režii potřebnou pro jednotlivý přenos dat mezi zařízeními. Tyto principy jsou většinou uplatňovány mimo místní sítě, jelikož jsou vhodnější pro přenášení velkých objemů dat [16].

Model TCP/IP (Transmission Control Protocol/ Internet Protocol) byl převzat z komunikačního modelu projektu Arpanet, vyvinutého v období studené války jakožto reakce na vypuštění sovětské vesmírné sondy v roce 1957 [16]. Pomocí projektu Arpanet měla být sestavena komunikační technologie, která by byla robustní, decentralizovaná, nezávislá na přenosovém médiu, v případě narušení fyzických vrstev měla být schopna přesměrovat datový tok jiným směrem a zajistit doručení dat do cíle. Vlivem tohoto snažení byl definován referenční model architektury TCP/IP, který je de facto přímo

převzat z architektury Arpanetu [16]. Architektura TCP/IP je proti referenčnímu modelu OSI/ISO značně zjednodušena (viz Obr. 13).



Obr. 13 Porovnání referenčního modelu OSI/ISO a TCP/IP [17]

Ve vrstvě internetového rozhraní je u modelu TCP/IP zahrnuta fyzická vrstva a linková vrstva modelu OSI/ISO. V rámci internetové vrstvy rozhraní modelu TCP/IP jsou definovány standardy pro komunikaci pomocí standardu Ethernet, Token Ring a další, jsou zde také zahrnuty definice přístupu k ovladačům síťových karet a přístupy k fyzickému přenosovému médiu [16]. Vrstva síťového rozhraní definuje fyzické a fyzikální vlastnosti linky. Jsou zde definovány úrovně napětí pro logické nuly a jedničky, počet připojených pinů a jejich pozice v portu a přenosová rychlost fyzického média. Linková vrstva je definována jako vrstva sloužící pro spojení dvou sousedních systémů, tedy systémů vzájemně spojených nebo připojených do jednoho síťového přepínače. Na úrovni této vrstvy dochází k faktickému propojení mezi jednotlivými účastníky komunikace, k vzájemné dohodě na parametrech, vytváří se zde rámce a adresování na linkové vrstvě. Na úrovni vrstvy síťového rozhraní je definováno zapouzdřování IP datagramů do rámců a jeho přenosu po fyzickém médiu [16].

Internetová vrstva modelu TCP/IP zajišťuje doručení vytvořených datagramů do cíle. Doručení dat do cílové destinace je řešeno pomocí takzvané best-efford delivery, což znamená doručení s největším úsilím. Internetová vrstva se snaží za každou cenu přenést data (pakety) od odesílatele k adresátovi, k tomu využívá nejvýhodnější přenosovou cestu.

Pokud dojde na takto definované cestě ke zpoždění, přeplnění vyrovnávací paměti na síťových prvcích nebo úplné degradaci cesty, pak je vysílací uzel informován o tomto problému pomocí zprávy protokolu ICMP (Internet Control Management Protocol) a odesílatel dat se snaží najít jinou cestu k doručení dat adresátovi. V této vrstvě jsou definovány protokoly IP (Internet Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), ICMP a IGMP (Internet Group Management Protocol), kde protokol IP představuje přenosový protokol, protokoly ARP a RARP slouží k přiřazení fyzických adres MAC (Media Access Control) k IP adresám. Protokol ICMP je použit pro řízení dostupnosti cest v rámci místní sítě, pro řízení toku dat a detekci nedosažitelných uzlů. Protokol IGMP je využit pro přihlašování do multicastových skupin. Výše uvedené protokoly musejí být implementovány v operačním systému v rámci modulu pro komunikaci na internetové vrstvě. V ní nedochází ke kontrole, zda byla data správně přenesena. Nedochází zde ani k opravě chybně přenesených dat [16].

Další vrstvou v protokolu TCP/IP je vrstva transportní, zajišťující přenos mezi aplikacemi, které spolu komunikují v rámci sítě, vytváří logické spojení komunikujících procesů a rozděluje data na menší celky (segmenty nebo datagramy), jež jsou posílány po síti. Transportní vrstva má primárně za úkol segmentizaci aplikačních dat do protokolů TCP a UDP. Jedná se o protokoly určené pro přenos dat, kde protokol TCP zajišťuje načítání dat z aplikace, jejich seskupení a spolehlivý přenos dat mezi jednotlivými zařízeními, na příjmové straně dochází vlivem protokolu TCP k sestavení dat, protokol UDP (User Datagram Protocol) zajišťuje rychlý přenos dat s minimálními požadavky na spolehlivost přenosu. Režie pro kontrolu dodání dat přebírá zdrojový uzel. Dále umožňuje přenos dat dle zvoleného typu na aplikační úrovni. Definuje přístup k posílání dat, buď jsou data posílána pomocí TCP spojení, kde je prvotně sestaven komunikační kanál mezi komunikujícími zařízeními, a poté jsou pomocí takto otevřeného kanálu přenášena a potvrzována data mezi systémy, což značně zvyšuje režijní náklady na přenos dat. Ověřování zařízení jsou řešena opět na aplikační úrovni modelu TCP/IP.

Dalším druhem přenosu je možnost data zasílat pomocí UDP spojení, kde jsou odeslána s určením adresáta a již není v rámci odesílatele udržována informace o stavu odeslaných dat. Tímto přístupem jsou minimalizovány režie potřebné pro spojení mezi jednotlivými zařízeními. Tento postup je výhodný pro komunikace typu klient–server, kde klientská část obsluhuje obrovské množství koncových zařízení [18].

Poslední vrstvou modelu TCP/IP je vrstva aplikační. Je tvořena procesy, které aplikacím umožňují přístup ke komunikačnímu systému. V rámci aplikační vrstvy je zajištěno zpracování dat na nejvyšší úrovni a jejich reprezentace společně s kódováním a řízením dialogu. Protokoly působící na aplikační vrstvě lze rozdělit do dvou kategorií: uživatelské protokoly a protokoly systémové. Jako uživatelské protokoly lze označit protokoly Telnet (Terminal Network), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) a jiné. Systémovými protokoly jsou pak protokoly zajišťující síťové funkce, a to jsou protokoly SNMP (Simple Network Management Protocol), BOOTP (Bootstrap Protocol) a DNS [19].

1.2.2 Zranitelnosti dle modelu TCP/IP

Rizika a problémy, které se vyskytují v místních sítích (LAN), kde je využíván komunikační standard typu Ethernet, se mohou dělit do skupin podle typu jejich výskytu, který je definován dle standardu TCP/IP.

Na vrstvě síťového rozhraní dochází ke galvanickému propojení jednotlivých částí prvků místní sítě, pokud jsou použity metalické propoje. Při galvanickém propojení všech prvků sítě mohou protékat mezi jednotlivými zařízeními takzvané vyrovnávací proudy a ty mohou přetěžovat vstupní ochrany portů na zařízeních. Tyto stavy mohou mít poté za následek destrukci zařízení, či nedostupnost zařízení na síti a rizika s tímto spojená. Jedná-li se o zařízení poskytující služby, pak samozřejmě dochází k nedostupnosti zmíněných služeb a s tím mohou být spojena rizika například ve výrobě, jako jsou špatné dávkování, neefektivnost výroby, potíže se zajištěním bezpečnosti a plynulosti provozu. Odolnost v rámci vrstvy síťového rozhraní se odvíjí především od schopnosti jednotlivých síťových rozhraní obnovit svoji činnost po nenadálé události, která může být zapříčiněna odpojením zařízení od sítě, reakcí ochrany v síťovém rozhraní zařízení a krátkodobým odpojením zařízení od sítě, porušením kabelové trasy, jež má poté za následek nové nastavení parametrů komunikační cesty, a tedy opět krátkodobou nedostupnost zařízení na síti [20].

IP Spoofing zranitelnost je cílena na protokol IP a lze ji využít k útoku na zařízení. Využívá možnosti skrýt IP adresu potencionálního útočníka, tak aby v důsledku této činnosti byla vygenerována chybná adresa zdroje dat. Útok je možno realizovat jako podvržení více adres a z těchto adres zasílat data na adresáta nebo odeslat podvrženou adresu adresáta a z ní poté odeslat požadavek na komunikaci jiným zařízením v síti. Výsledkem obou metod je zahlcení

adresáta požadavky na komunikaci a znemožnění jeho komunikace v rámci sítě, a tudíž nedostupnost poskytované služby [21].

Útok HTTP (Hypertext Transfer Protocol) flooding je realizován pomocí vysílání legitimních příkazů protokolu HTTP. Hlavním úkolem útoku je vytěžovat na maximum zdroje cíleného zařízení a znemožnit mu tím další legitimní komunikaci. Problém spočívá v jeho detekovatelnosti, jelikož útok využívá legitimních příkazů [21].

Dalším typem zranitelnosti protokolu IP, která může být zneužita k útoku na systém, je možnost extrakce dat z cílových služeb, jež jsou poskytovány napadeným zařízením. Těmito útoky mohou být postiženy například webové servery zařízení a útočník z nich může doslova těžit data. Ta poté mohou být využita k vytvoření falešných webových stránek a ke zmatení nebo cílenému zneužití uživatelů, kteří tyto webové stránky používají [21].

Protokoly ARP a RAP jsou důležitými prvky internetové vrstvy modelu TCP/IP. Pokud je sestavená tabulka pomocí protokolu napadena, získává útočník data o návaznosti IP adres a koncových fyzických adres zařízení. Vlivem této skutečnosti mohou být útočníkem přerušena spojení mezi koncovými body komunikace nebo může převzít kontrolu nad aktuálními datovými přenosy. Data mohou být přesměrována na jiné zařízení. Kvůli této zranitelnosti může útočník rovněž odchytávat pakety přenášené v datové cestě [22].

Zranitelnost protokolu ICMP je tunelování pomocí sestavení propojení realizované požadavky na odpověď na ICMP paket, kterou může být odpověď na ping. Této metody je využíváno, jelikož na tento typ datového přenosu nezareagují ochrany zařízení. Tuto techniku je možno využít pro zjištění prostupnosti z místní sítě do internetu, aniž by byla vzbuzena nežádoucí pozornost. V návaznosti na snahu zařízení odpovědět na všechny dotazy odesílatele je možno definovat útok typu Smurf, kde útočník zasílá oběti ohromné množství ICMP a tím zahlcuje linku oběti, čímž opět omezuje služby poskytované napadeným zařízením [22].

Transportní vrstva modelu TCP/IP využívá pro svou funkci protokoly TCP a UDP, které jsou využity pro komunikaci mezi účastníky datové komunikace. Zranitelnosti jsou především definovány pro protokol TCP, jako je Syn flood zranitelnosti, v které je využito cíleného zahlcení napadeného zařízení pomocí zasílání žádostí o připojení. Každá taková žádost je cílovým zařízením zpracována a je na ni odeslána odpověď s požadavkem na potvrzení doručení odpovědi. Potvrzení doručení ovšem nikdy nepřijde, jelikož v původním požadavku na navázání spojení je podvržen adresát. Výsledkem takového chování je alokace

prostředků pro zahájení komunikace mezi adresátem a zasaženým zařízením, kvůli tomu mohou být ostatní legitimní požadavky na spojení upozaděny a nevyřízeny. Opět dochází ke zpoždění odezvy zasaženého zařízení a může docházet k výpadkům komunikace a k neposkytování služeb. Potencionální zranitelnosti mohou být způsobeny otevřenými porty pro komunikaci pomocí TCP a UDP protokolů, které nejsou využívány. Útočník může pomocí pasivního skenování zařízení tyto porty odhalit a využít je k napadení zařízení. Pro komunikaci pomocí protokolu TCP je využíváno sekvence čísel, jež jsou zasílána v požadavku na komunikaci mezi zařízeními. Pomocí těchto sekvencí jsou účastníci schopni sledovat, zda jsou data komunikována. Komunikace může být odposlouchávána útočníkem a útočník může zachytit tuto sekvenci čísel, kterou může dekódovat a poté zasílat pakety původním účastníkům komunikace, aniž by původní účastníci komunikace cokoliv rozpoznali. Pro protokol UDP je možno definovat zranitelnost zařízení, jež mohou být zasažena útokem typu UDP flood. Jedná se o útok využívající zranitelnosti zařízení, které je zasaženo obrovským množstvím datagramů vysílaných na otevřený UDP port oběti. Takové chování může mít za následek zahlcení komunikační části dotčeného zařízení [21].

Poslední vrstvou modelu TCP/IP je vrstva aplikační, sloužící jako prostředek pro šifrování a dešifrování komunikačních dat, což vede k lepšímu zabezpečení. Vzhledem k definici protokolu TCP/IP je nutno veškeré zabezpečení definovat na aplikační vrstvě. Vrstvy vyskytující se pod aplikační vrstvou se mají starat pouze o spojení bodů a uzlů na síti a zajistit buď spolehlivý přenos dat, nebo rychlý přenos dat – podle toho, jak je aplikace konstruována. Zranitelnosti, které se vyskytují na aplikační vrstvě, opět závisejí na druhu protokolu, který je zde použit. Pro popis zranitelností jsou zvoleny dva zástupci. Protokol HTTP je využit ve většině aplikací a služeb vyskytujících se na místní síti, jako jsou webové stránky webových serverů. První ze zranitelností může být napadení právě probíhajícího spojení na webové stránky. Pokud není použito zabezpečení komunikace, tak může útočník použít program pro zachytávání paketů (Sniffer). Pomocí takto získaných dat, které obsahují identifikační údaje o probíhajícím spojení, může útočník získat kontrolu nad probíhající komunikací a vytěžit z ní například přihlašovací údaje k ovládnutí uživatelského účtu, se kterým právě probíhá komunikace. Dalším z možných problému je ukládání webových stránek do vnitřní paměti zařízení. Takto uložené stránky poté slouží ke zvýšení uživatelského komfortu prohlížených dat, jelikož obsah těchto stránek není nutno znovu stahovat ze sítě. Pokud není dbáno na zabezpečení přístupu k zařízení, tak útočník může z takto uložených stránek získat důležitá data o uživateli. Problémem jsou takzvané HTTP

cookies, což jsou data o malé velikosti, jež webové servery zasílají koncovému zařízení uživatele. Jsou uložena místně na zařízení uživatele, ze kterého je inicializována komunikace. Poté – při každém dalším spojení mezi těmito zařízeními – jsou data odesílána zpět webovému serveru a obsahují personifikované údaje o uživateli. Pomocí nich poté webový server může nabízet uživateli relevantnější data, jako jsou reklamy, různé nabídky a pobídky. V rámci cookies můžou být uložena i přihlašovací jména a hesla k webovým službám. Pokud se útočníkovi podaří tato data infikovat, může ovlivnit personifikaci prostředí a ovlivnit data nabízená uživateli nebo může vytěžené údaje využít přímo k prolomení zabezpečení a ovládnutí webových služeb, na které přistupuje uživatel. Cross-Site Scripting je další z mnoha zranitelností, které lze zneužít na aplikační vrstvě. Vlivem této slabiny je útočníkovi umožněno vložit škodlivý kód na nezabezpečené webové stránky. Poté co uživatel danou stránku navštíví, je škodlivý kód proveden na klientském zařízení. Opět je útok veden s cílem vytěžit z klientské stanice citlivá data. V rámci aplikační vrstvy je definován protokol DNS, jímž je zajišťován překlad doménových jmen na IP adresy a reverzní převody z IP adres na jmenné záznamy. Zranitelnosti protokolu DNS dávají útočníkovi možnost infikace této služby za cílem změnit koncové adresy v DNS záznamu a tím přesměrovat dotazy na jiné zařízení, než bylo původně v záznamu. Jednou z možností, jak DNS záznam podvrhnout, je infikace krátkodobé paměti DNS, kde jsou uloženy poslední záznamy o překladu adres. Záznamy se vyznačují takzvaným časem životnosti, který definuje, za jakou dobu dojde k automatickému obnovení záznamu v krátkodobé paměti. Díky tomu může útočník podvrhnout záznam v krátkodobé paměti DNS, a dokud nedojde k aktualizaci tohoto záznamu, jsou všechny dotazy směrovány na špatnou IP adresu. Pro sofistikovanější útok je využito změny adresy DNS serveru, která je uložena na koncovém zařízení. Tento údaj slouží k definici, na které IP adrese se DNS server v síti nachází a poskytuje služby. Pokud se útočníkovi podaří tento záznam změnit, pak veškerý provoz, který vyžaduje pro svou činnost služby DNS serveru, je v plné správě útočníka [21].

Většina z výše uvedených zranitelností vede k útoku typu DoS (Denial of service), tedy odepření služeb poskytovaných napadeným zařízením, popřípadě DDoS (Distributed Denieal of Service), kde je využito více útočících zařízení, která jsou nasměrována na jeden cíl a přímo na něj vysílají požadavky, tak aby zapříčinila jeho přehlcení a nedostupnost služeb na něm provozovaných. Nebo jsou útoky vedeny s cílem vytěžit citlivé údaje, které mohou být posléze zneužity [23].

1.2.3 Poruchovost a odolnost místních sítí

Problémy a poruchovost místních sítí jsou většinou způsobeny nesprávnými postupy při konstrukci místní sítě, jako jsou chybně zvolené kabelové trasy, nevhodně zvolené druhy kabeláže, nedodržení instalačních postupů a v neposlední řadě chybná konfigurace jednotlivých zařízení připojených k síti. Většina poruch tedy vzniká na úrovni vrstvy síťového rozhraní a lze je vymezit správnou instalací sběrnic a důsledností zhotovitelů. Zde je důležité, aby všechna připojená zařízení byla pospojována ke stejnému výchozímu potenciálu napětí. Je nutné, aby při návrhu a realizaci lokálních sítí byly respektovány požadavky na správné provedení metalických spojů a byly vybrány správné typy kabeláže. Typ kabelových propojů se odvíjí od požadavků na datovou kabeláž a místa, kde bude daná místní síť realizována. Pro prostory s nízkým rušením je možno realizovat místní sítě pomocí nestíněných kabelových propojů, tedy kabelů typu UTP (Unshielded Twisted Pair). Pokud se jedná o prostory, kde je předpoklad zarušení přenosové cesty, doporučuje se zvolit kabely stíněné, tedy kabely typu FTP (Foiled Twisted Pair). Dle požadavků na přenosovou rychlost, které vyplývají ze standardu Ethernetu, jsou definovány typy kabelů vhodných pro standard Fast Ethernet, Gigabit Ethernet a další. Samozřejmostí jsou i správně zvolená zakončení kabelových tras. Měla by být ukončena na obou stranách zásuvkami pro ethernetové konektory dle definovaného standardu, pro který je daná kabeláž zhotovena. Součástí takto provedené realizace sběrnic pro místí sítě je i vyhotovení protokolu o certifikovaném měření daných datových tras. Protokol je důkaz, že daná sběrnice odpovídá standardu, pro který je zhotovena.

Pro fyzické oddělení jednotlivých částí místní sítě jsou zřizovány datové trasy pomocí optických vláken, kde je zajištěno galvanické oddělení jednotlivých zařízení na sběrnici. Pro optickou sběrnici jsou definovány požadavky taktéž dle daného standardu, pro který je sběrnice zřizována. Optické sběrnice jsou používány především pro propojení jednotlivých objektů v rámci stromové struktury topologie nebo jsou použity pro velkokapacitní datové spoje mezi jednotlivými zařízeními v místní síti.

Pro detekci poruch na sběrnici je možno využívat nejrůznější verifikační a certifikační přístroje pro měření strukturované kabeláže. Chybná konfigurace může taktéž způsobit nedostupnost služeb zařízení na místní síti, nicméně tento druh poruch je detekován snáze, a i jejich odstranění probíhá v rychlejším tempu, než je tomu u poruch sběrnic.

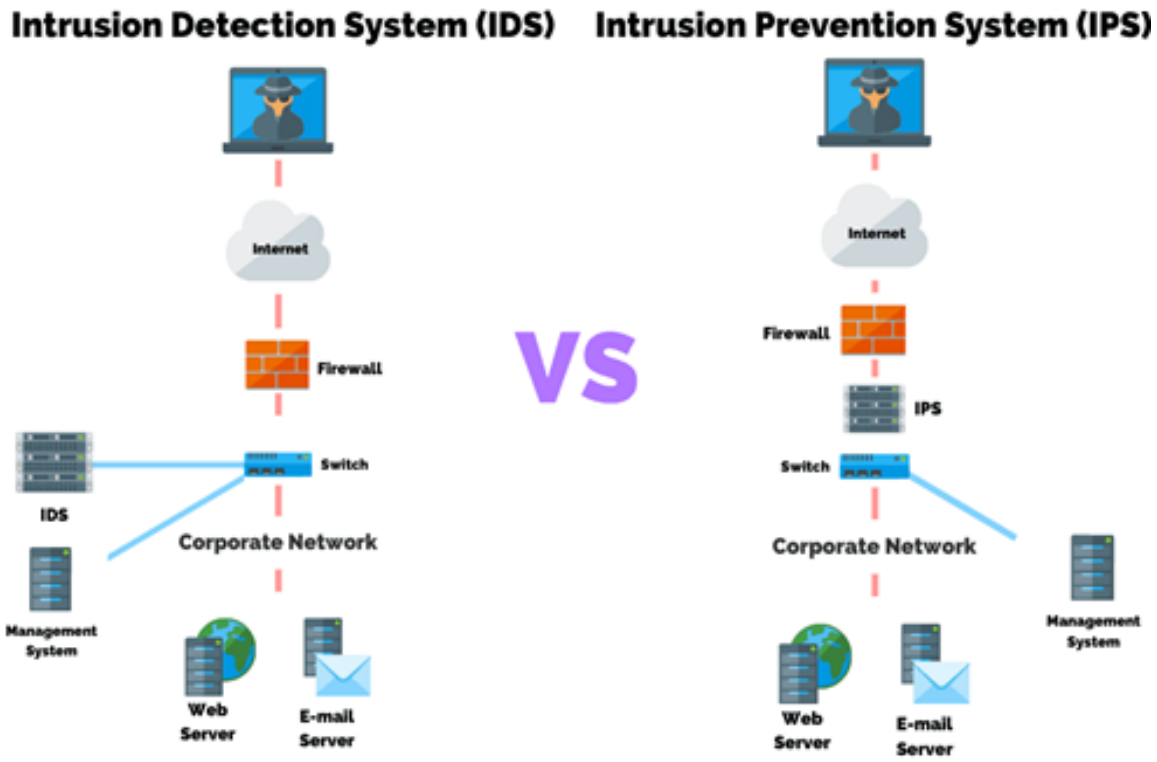
Odolnost místních sítí je možno definovat dvěma způsoby – jako odolnost proti fyzickým a fyzikálním vlivům a poté odolnost proti zranitelnostem na úrovni modelu TCP/IP. Pro fyzickou a fyzikální odolnost je nutné dodržovat standardy a doporučení pro zhotovení sběrnic pro komunikační standard Ethernet, jež jsou definovány v rámci norem a standardů IEEE 802.3u v implementaci pro kroucenou dvojlinku minimálně kategorie 5, umožňující přenosy až do frekvence 100 MHz. Je třeba dbát na správné zapojení konektorů a zásuvek. Nastane-li porucha na přenosové soustavě mezi dvěma body, jsou zjištěny výpadky v komunikaci a vrstva síťového rozhraní začne upravovat vlastnosti linky tak, aby bylo dosaženo bezproblémového přenosu i za cenu razantního snížení rychlosti. Spolu s tímto postupem nastane penalizace přenosové cesty pomocí protokolu ICMP. Pokud existuje náhradní přenosová trasa, pak je síťový přenos přesměrován do této náhradní trasy. Na uvedené skutečnosti reagují ochrany na portech jednotlivých síťových směrovačů a tyto události mohou být reportovány do nadřazených systémů. Odolnost místní sítě proti zranitelnostem na úrovni modelu TCP/IP je vázána na schopnost jednotlivých zařízení připojených do místní sítě zachytávat a filtrovat toto škodlivé chování. Odolnost a připravenost na jednotlivé zranitelnosti lze charakterizovat třemi stupni obrany, jsou to prevence, detekce a reakce na již známé stavy [24].

Pro potřeby prevence jsou v rámci místních sítí nastaveny vstupní filtry, které zamezují vstupu do sítě paketům opatřeným nelegitimní zdrojovou adresou. Takové pakety jsou vybaveny adresou, která nepochází ze stejné sítě, z níž je paket vyslán [25]. Výstupní filtry jsou kontrolovány odchozími pakety z místní sítě, opět jsou kontrolovány IP adresy zdrojů a porovnávány s adresním rozsahem dané sítě. Pokud se IP adresa obsažená v paketu neshoduje s adresami používanými v místní síti, je takový paket zablokován a zahozen [25]. Jako preventivní ochrana mohou být použity filtry, které trasují cestu paketů dle topologie použité v dané síti a hledají skutečný zdroj odesílaných paketů. Jsou-li zdroj a obsah paketu v pořádku, pakety jsou propuštěny dále. Filtry mohou taktéž využívat databázi historie IP spojení a dle ní vyhodnocovat IP adresy obsažené v paketech [25]. Zákaz nebo potlačení nepoužívaných služeb na zařízeních je taktéž formou prevence, útočník nemůže zařízení napadnout, pokud dané služby nejsou dostupné. V rámci sítě mohou být instalována takzvaná Honeypot zařízení, která jsou primárně určena k umělému zacílení útoku. Útočník se vždy snaží využít nejslabšího místa v systému nebo místní síti, a pokud je mu takovýto bod nabídnut, pak většinou své úsilí směřuje do něj. Výsledkem takového přístupu je větší šance k odhalení útoku a odklonění útočníka od rizikového zařízení. Spolu

s výše uvedenými preventivními úkony je nutno dbát na aplikaci a instalaci nejnovějších bezpečnostních záplat. Jestliže systém neumožňuje pružné záplatování, jelikož je provozován v režimu, který to neumožňuje, je nutno nastavit procesy tak, aby alespoň nejdůležitější záplaty byly aplikovány. Je-li systém ponechán bez záplat a zabezpečení, stává se z něj bezpečnostní riziko [26].

Detekce rizik na místní síti je směřována především na anomálie v chování zařízení, což můžou být náhlé zvýšení komunikace se zařízením, vytěžování systémových zdrojů zařízení a další anomálie v obvyklém chování. Detekování takových anomálií lze realizovat i podle již zmapovaných vzorců chování a dle toho je poté možné nastavit procesy o omezení nenormálního chování. Pro detekci lze použít sondy monitorující komunikace a vazby v rámci místních sítí, které při správném nastavení můžou upozorňovat na podezřelé aktivity a komunikace, tyto systémy monitorující dění na místních sítích jsou známy pod zkratkou IDS (Intrusion Detection System). Další formou detekce rizik a problémů se zabezpečením je možnost využití programů, které umožňují provést penetrační testy v rámci sítí. Penetračními testy se rozumí kontrola odolnosti zařízení na různé druhy definovaných komunikačních stavů. Výsledkem takových testů jsou podrobné informace o stavu zabezpečení v rámci místní sítě a zařízeních k této síti připojených [27].

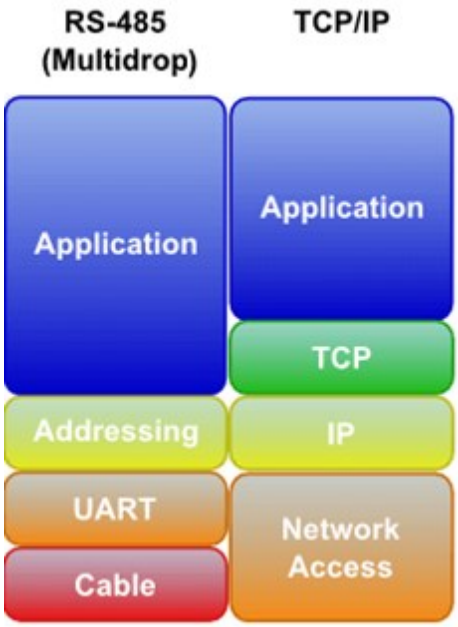
Poslední metodou obrany proti zranitelnostem je reakce na již detekovaný problém v síti, což mohou obstarávat systémy zabývající se monitoringem dění na síti a dle definovaných principů mohou aktivně zasahovat do nastavení síťových prvků a zařízení, čímž ovlivňují provoz na místních sítích a mohou zastavit detekovaný problém či anomálie, a to v úzkém segmentu sítě. Tyto systémy pro monitorování, detekci a aktivní ochranu místních sítí jsou na trhu uvedeny pod zkratkou IPS (Intrusion Prevention Systems) [28].



Obr. 14 Rozdíl mezi systémy IDS a IPS [29]

1.3 Modbus TCP

Stejně jako Modbus RTU je Modbus TCP/IP komunikační protokol využívaný především v průmyslové sféře. Jako přenosové médium komunikačního protokolu Modbus může být použito i strukturované kabeláže, která je součástí místní ethernetové komunikační sítě. Pro přenos informace je zde využíváno protokolu TCP/IP, kdy je klient připojen do stejného segmentu místní sítě jako server. Pro komunikaci zde není využito unikátních identifikačních čísel jako u verze komunikačního protokolu Modbus RTU, ale je zde využito IP adresy, přidělené každému zařízení, které je připojeno do komunikační sítě. Zabezpečení komunikace v rámci protokolu Modbus TCP/IP je tedy dáno úrovní zabezpečení na aplikační vrstvě [30].



Obr. 15 Modbus TCP v komunikačním modelu TCP/IP [31]

U komunikačního protokolu Modbus TCP jsou stejně jako v případě protokolu Modbus RTU hlavními bezpečnostními riziky chybějící ověření identity obou účastníků komunikace, nemožnost spravovat komunikační přístupy do zařízení a spravovat provádění přijatých povelů, nezašifrovaný přenos dat, zahlcení komunikace a možnost kompromitace přenášených dat [32].

Vzhledem k absenci ověření identity a přístupu do zařízení může potencionální útočník této zranitelnosti využít s cílem kompromitovat koncové zařízení. Může taktéž narušit jednotlivé části zařízení komunikující pomocí protokolu Modbus TCP, a tím zapříčinit ekonomické a technologické škody. Zařízení, s nímž je vedena komunikace, není schopno ověřit, zda je druhý účastník komunikace podvržené zařízení, či nikoliv [32].

Není zde řešena prioritizace povelů, potažmo seznam povolených a zakázaných povelů, které je zařízení schopno zpracovat.

Pokud útočníkem není přímo ovlivněna funkce jednotlivých komponentů, které komunikují pomocí protokolu Modbus, může být útočníkem odposlouchána komunikace vzhledem k absenci šifrování komunikace. Tato slabina může být zneužita rovněž ke kompromitaci přenášených dat. Takto získaná data mohou být podkladem k analýzám a přípravě mohutnějšího kybernetického napadení [32].

Komunikace pomocí protokolu Modbus TCP je plně závislá na prvních třech vrstvách standardu TCP/IP, tudíž je plně závislá na topologii a propustnosti místní sítě a na zranitelnostech plynoucích z místní sítě.

2 ZABEZPEČENÍ PRŮMYSLOVÉ DATOVÉ SÍTĚ

Zabezpečení průmyslových datových sítí je v dnešní době plně v gesci jednotlivých průmyslových společností. Jsou zpracovány studie a standardy, jako je standard IEC 62443 (International Electrotechnical Commission), který rozlišuje schopnost společnosti odolávat kybernetickým hrozbám do tří základních skupin označovaných jako stupně zabezpečení, a to od úrovně 1 až po úroveň 3 [33].

Stupeň 1 zahrnuje schopnost systému, využívající průmyslových sběrnic, ověřovat uživatele, kteří do systému přistupují. Ověření přístupu je možno buď pomocí fyzických přístupů, nebo pomocí autority, na které jsou vytvářeny uživatelské přístupy. Ověřováním pomocí centrální autority lze dosáhnout centralizovaného spravování přístupů, auditování přístupů, rozřazování oprávnění k těmto přístupům a v neposlední řadě možnost nastavit požadavky na složitosti a životní cyklus hesel. Dalším prvkem bezpečnosti na úrovni stupně jedna jsou požadavky na monitorování a omezování přístupů k systému z jiných sítí a systémů, což je zajištěno monitorováním a definicí přístupu, buď v rámci dotčených systémů, nebo použitím přídavného zařízení vloženého do komunikační cesty. Logování aktivit systému a aktivit uživatele je bráno jako esenciální pro naplnění zabezpečení stupně jedna. Důležitou součástí systému je tvoření provozních záloh řídicích a obslužných programů, zálohy nastavení komunikačních cest, síťových zařízení, implementace komunikačních bran, které jsou schopny řídit přístupy do systému v rámci povolených aplikací a protokolů, segmentace místních sítí a systémů dle provozního hlediska nebo dle návazností na jiné systémy [33].

Stupeň 2 v sobě implementuje zabezpečení na úrovni stupně 1 a navíc definuje další škálu zabezpečení, jako je implementace autorizačních certifikátů, ověřování přístupu z jiných sítí pomocí centrální autority, zřízení certifikační autority pro systémy řízení, mapování rolí z centrální autority přímo do systému řízení, zřízení systému pro detekci škodlivých kódů a anomálií IDS, jimiž je zajištěn dohled nad komunikačními přenosy v rámci místních sítí, implementace centrálního řešení pro řízení, které dohlíží nad výrobními procesy a provádí auditování jejich změn, ale také zajištění spolehlivého přenosu dat mezi kritickými systémy a prioritizace přenášených dat. Umístění forem zabezpečení stupně dva by mělo být co nejblíže zdrojům těchto dat, měly by být tedy umístěny co nejblíže řídicím systémům [33].

Zabezpečení úrovně 3 je definováno jako souhrn opatření, která jsou tvořena z vícefaktorové autentizace řídicích systémů a připojených zařízení. Doplněny jsou prvky certifikace

jednotlivých řídicích systémů, jež by měly v rámci svých procesů a komunikací provádět ověřování identit komunikujících zařízení a ověřování vznesených požadavků a postupů. Přístupy pro změnu v rámci řídicích systémů jsou omezeny a řízeny pomocí hardwarových mechanismů, které můžou být implementovány přímo v řídicích systémech, nebo jsou implementovány nad těmito řídicími systémy, a to jako systémy třetích stran. Zařízení a řídicí systémy reportují své stavy a nálezy do nadřazených systémů, do takzvaných SIEM (Securtiy Information and Event Managment) systémů. Pro synchronizaci dat a událostí je nutno dodat do systému zdroj jednotného časového údaje, k tomu může být použito zařízení využívající technologie GPS (Global Position System), které lze využít jako primární zdroj času. Takto definovaná časová známka je poté distribuována pomocí síťových služeb do jednotlivých systémů a umožňuje synchronizaci času napříč celou sítí. Komunikace na úrovni zabezpečení číslo 3 je šifrována a data jsou šifrována nebo jinak zabezpečena i v rámci systému řízení a přilehlé infrastruktury [33].

Ověřování uživatelů lze docílit implementací služby Active Directory, jež zahrnuje komplexní řešení správy počítačové sítě od firmy Microsoft. Jedná se o adresářovou strukturu, která v sobě zahrnuje objekty a služby vyskytující se v rámci sítě. Jsou do ní ukládány informace o těchto objektech a službách. Primární rolí AD (Active Directory) je schopnost poskytovat centralizované řešení autorizace a autentizace, definovaně distribuovat zásady zabezpečení a nastavení definované pomocí skupinových politik (Group Policy, zkráceně GP). Služba AD leží na doménovém kontroléru, který zabezpečuje chod domény pro technologickou síť, fungující na platformě operačního systému Windows Server. Do služeb AD jsou integrovány služby typu DNS. Vlivem centralizace těchto služeb je nutno zajistit, aby nedocházelo k výpadkům jejich poskytovatelů. Proto je nutné vytvořit více doménových kontrolérů a mezi nimi zřídit replikaci pro docílení stejného nastavení všech doménových kontrolérů [34] [35].

Omezování prostupů do systému a jejich monitoring lze realizovat pomocí zařízení označovaných jako firewally, která jsou vložena do komunikační cesty. Podle typu metody zpracování průchozích dat se firewally rozdělují na typy paketových filtrů, stavových firewallů a aplikačních firewallů. Firewally mohou být napojeny do nadstavbových systémů monitoringu sítě a mohou být těmito systémy ovládány, respektive tyto nadstavbové systémy mohou definovat definiční obory firewallu. Jedná se o systémy IDS a IPS. Aby mohly systémy IDS a IPS fungovat, je nutno zkoumané sítě vybavit zařízením, jež může sledovat

datový provoz na síti a poté může dle vlastního algoritmu definovat nastavení firewallu [29][36].

Paketový filtr

Díky paketovému filtru je možno přesně definovat průchodnost paketů přes firewall. Jako definiční obor paketového filtru slouží přesné určení, jaký typ paketů je zasílán, včetně zdrojové a cílové IP adresy. Paketový filtr pracuje s třetí a čtvrtou vrstvou modelu OSI/ISO. Data při průchodu paketovým filtrem nejsou podrobněji zkoumána, díky tomu paketový filtr vyniká především velmi rychlým přenosem dat. Značnou nevýhodou paketového filtru je nízká úroveň kontroly spojení, kdy paketový filtr neumožňuje detailnější kontrolu složitějších přenosových protokolů, jako jsou video, audio přenos, přenos souborů pomocí FTP, kdy dochází v rámci paketového filtru k otevření i dalších spojení a portů, jež mohou být využívány jinými protokoly. Paketové filtry mohou být nasazeny na centrálních přepínačích s dostatečným výkonem, který umožňuje hardwarové směrování mezi různými sítěmi, takto uzpůsobený směrovač je nazýván L3 směrovačem [37].

Stavový firewall

Stavový firewall je dalším typem používaného druhu zabezpečení. Umožňuje inspekci průchozích paketů, což znamená, že sleduje a udržuje všechny UDP a TCP spojení. Stavový firewall operuje na transportní vrstvě modelu OSI/ISO, rozlišuje různé stavy paketů v rámci spojení a propouští pouze definované pakety v rámci již povolených relací [37][38].

Aplikační firewall

Aplikační firewall funguje obdobně jako firewall stavový, pracuje na aplikační vrstvě modelu OSI/ISO. Aplikační firewall disponuje vnitřním algoritmem, který dokáže danou komunikaci zachytit, rozklíčovat ji a kontrolovat, zda komunikace odpovídá definicím, které jsou v rámci jeho algoritmu definovány. Aplikační firewall umožňuje definovat a vynucovat zásady komunikace, jež se vztahují k jednotlivým aplikacím, které jsou v rámci jeho definic povoleny. Lze prioritizovat komunikaci a dle takto definovaných podmínek je možné přiřazovat šířku pásma určitým typům komunikace. Jedna z funkcí aplikačního firewallu umožňuje definovat šířku přenosového pásma komunikace, které lze využít k omezování určitých typů komunikace v rámci pracovní doby, například lze omezovat pásmo pro přenos videa a zvuků. Aplikační firewall může tvořit zařízení, jež umí filtrovat komunikaci na svém datovém rozhraní. Takovým zařízením může být i řídicí

automat, který přes sebe nativně propustí pouze komunikaci, která je mu vlastní. O řídicím automatu lze hovořit jako o aplikační bráně [39].

Formy zabezpečení jsou definovány, ale jejich prosazování v rámci produkčního prostředí je stále postaveno proti ekonomickým zájmům jednotlivých subjektů. Většinou se jedná o subjekty s již rozvinutým stupněm rozvoje infrastruktury komunikačních sítí a nasazenými stupni automatizace, které neumožňují přímo implementaci jednotlivých stupňů zabezpečení nebo vyžadují celou reformaci procesů řízení a komunikací. V některých případech nelze aplikovat vyšší stupně zabezpečení z důvodu nekompatibility mezi jednotlivými zařízeními nebo vlivem absence jakýchkoliv forem možnosti integrace zabezpečení v systémech řízení a dalších podpůrných systémech. Nezřídka je možnost implementace stupňů zabezpečení podmíněna odstavením provozu, což většina průmyslových subjektů odmítá.

Většina implementací zabezpečení předpokládá, že firmy, u nichž se implementace dle výše uvedené problematiky nasazuje, již disponují základními prvky zabezpečení.

V průmyslové sféře je problematika zabezpečení upozaděna před bezproblémovým chodem výroby a strojů.

II. PRAKTICKÁ ČÁST

3 NÁVRH ZABEZPEČENÍ PRŮMYSLOVÉ DATOVÉ SÍTĚ

V rámci praktické části byly navrženy prvky zabezpečení, které mají za cíl zlepšit zabezpečení technologické sítě. Tato zabezpečení jsou navrhována s ohledem na komunikační model TCP/IP. Jsou zde popsány prvky zabezpečení, které již bylo možno implementovat. Jsou zde nastíněny postupy, jež teprve budou implementovány.

3.1 Stávající stav zabezpečení průmyslové datové sítě

Jednou z možností, jak provozovat jednotlivé průmyslové systémy, je úplná separace jejich sítí. V tomto případě nedochází k žádným možnostem ovlivňování ostatního síťového provozu. Není možno tyto sítě napadnout z vnějšího okruhu, a i pokud by se podařilo tyto sítě kompromitovat, vzniklé problémy by se vyskytovaly pouze v rámci vnitřních sítí těchto systémů, s omezenými možnostmi šířit se dále. Vlivem požadavků na sbírání dat z průmyslových systémů a požadavků na efektivní řízení zpravidla není takovýto přístup k průmyslovým datovým sítím využíván.

Průmyslové datové sítě jsou stavěny jako postupně se rozvíjející architektura stromu nebo hvězdy. Sítě jsou navrhovány jako součást technologií, kdy pro jeden technologický celek může existovat jedna technologická síť, která je poté propojena s ostatními technologickými celky, takový systém průmyslových sítí je decentralizován. Jednotliví správci technologií si spravují i své síťové celky, pravidla nastavená v rámci jednoho technologického celku nemusejí být aplikována do dalšího technologického celku. Výhodou takového řešení je přesné nastavení parametrů průmyslových sběrnic pro danou technologii a přesná definice stykových mít, kde jsou předávána data do dalších technologií, dalším výhodným faktorem je možnost minimálního ovlivňování technologických celků pomocí průmyslových sběrnic. Primárně jsou průmyslové sběrnice plně podřizovány potřebám technologických celků a jejich primárním cílem je podporovat bezvýpadkovou výrobu. Tato řešení jsou obvyklá pro výrobní linky, kde dochází k výrobě produktů, jež jsou poté dále zpracovávány dalšími technologickými celky, a není nutno, aby tyto celky mezi sebou komunikovaly.

Průmyslové sítě lze budovat jako centralizované, kde se jednotlivé technologické celky integrují do centralizovaného systému sítí. Připojované systémy jsou poté integrovány do celkového systému sběrnic a jsou na ně uplatňována pravidla definovaná správci infrastruktury. Při takovém řešení jsou pravidla, která mají být implementována do připojovaného systému, komunikována s dodavateli a poté jsou buď plně nasazena, nebo

jsou částečně změněna. Tyto změny jsou většinou způsobeny specifickými požadavky dodavatelů. Pokud nelze aplikovat globální pravidla do dodávaných systémů, přichází snaha tyto systémy uzavírat do vnitřních komunikačních celků, které jsou do centralizovaných systémů sítí připojovány přes komunikační brány. Ty filtrují užitečnou komunikaci, kterou propouštějí, a zároveň blokují komunikaci, která by mohla být problémová. Tímto způsobem lze efektivně docílit zabezpečeného přenosu dat.

Zabezpečení průmyslových datových sběrnic je sestaveno z dílčích prvků zabezpečení, které kopírují standard OSI/ISO, potažmo TCP/IP. Zaměřuje se především na zabezpečení datové cesty, která se skládá z koncových zařízení, síťových prvků a médií pro přenos dat. Nedílnou součástí zabezpečení datové cesty jsou taktéž různé formy přechodů z komunikačních protokolů na jiné komunikační protokoly. Lze zde využít formy zabezpečení komunikace na aplikační úrovni, například nativními protokoly, které jsou poskytovány výrobci průmyslových zařízení. Jako příklad lze uvést protokol CIP security (Common Industrial Protocol) od firmy Rockwell Automation. Ten má za úkol zabezpečit přenášená data a umožnit čtení z těchto dat pouze zařízením, jež mají takovýto bezpečnostní protokol integrován [40]. Pro zabezpečení celé datové cesty je nutno zabezpečit jednotlivé vrstvy dle modelu TCP/IP, jež představují vrstvu síťového rozhraní (fyzická vrstva a linková vrstva), internetovou vrstvu, transportní vrstvu a v neposlední řadě vrstvu aplikační. Firmy si stále vyvíjejí své vlastní algoritmy řízení pohybující se na úrovni aplikační vrstvy modelu TCP/IP. V takových případech je zabezpečení interpretováno jako součást systémů, nad kterými jsou tyto algoritmy vytvářeny. Vývojáři se často mylně domnívají, že za ně otázku zabezpečení a zabezpečeného přenosu dat řeší dodavatel systémů řízení. Dodavatelé systémů řízení poskytují zařízení, která jsou vybavena instrukčními sadami, vlastnostmi a možnostmi základní komunikace. Tato komunikace může být nezabezpečená, nebo zabezpečená. Volba typu komunikace a dalších forem zabezpečení je plně v rukou vývojáře. Bohužel tento úhel pohledu je většinou zavrhován a zodpovědnosti se mylně přisuzují správci síťové infrastruktury, popřípadě systémovým správcům.

Zabezpečení průmyslových datových sítí lze rozdělit do dvou rovin. První z nich je představována samotnou síťovou infrastrukturou a zařízeními do ní připojenými, zde je zabezpečení primárně zaměřeno na vrstvy síťového rozhraní, internetové a transportní z modelu TCP/IP. Druhá rovina je zaměřena na komunikaci na úrovni transportní a aplikační vrstvy modelu TCP/IP. První rovina pohledu připadá na správce síťové infrastruktury, kdežto druhá je plně v kompetenci vývojářů řídicích algoritmů.

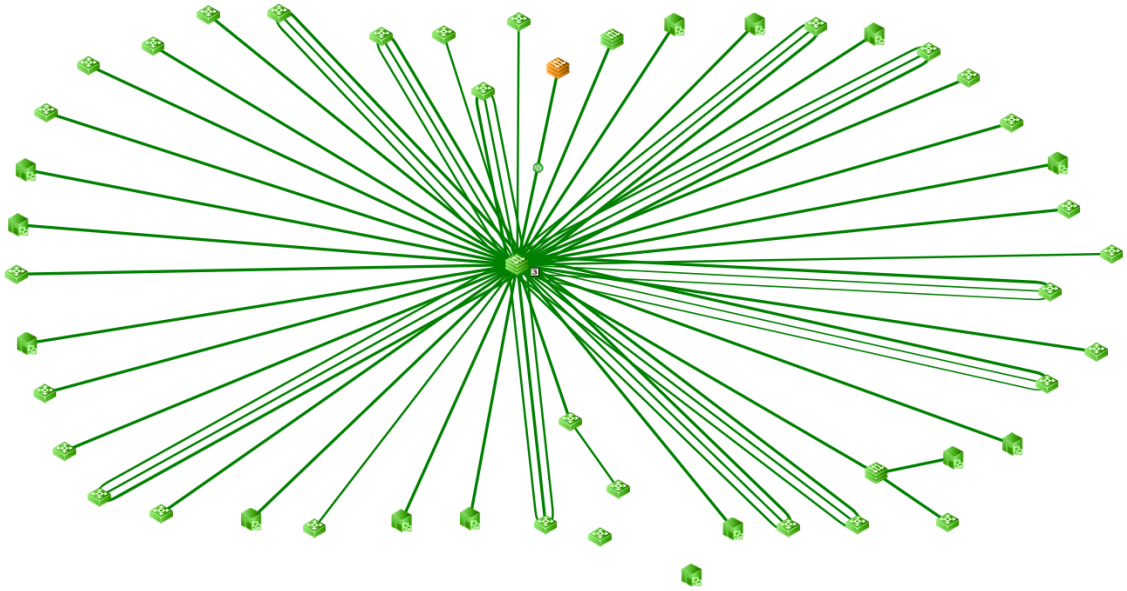
Další kritérium pro volbu a nastavení zabezpečení v rámci průmyslové datové sítě jsou systémy pro dohled výroby, sběr dat a další podpůrné systémy, které jsou ve většině případů provozovány na operačních systémech Windows server od firmy Microsoft. Zde se pohybujeme na úrovni správce sítě, potažmo na úrovni systémových, či aplikačních specialistů, kteří se zaměřují na nastavování jednotlivých systémů třetích stran, jejich komunikačních propojů a zabezpečení těchto systémů.

Neopomenutelnou součástí zabezpečení průmyslových datových sítí je instruování všech lidských zdrojů, jež mohou přijít do styku s jakýmkoliv zařízením připojeným do průmyslových sítí, ohledně povinností a chování v rámci podnikových sítí, ať už průmyslových, či administrativních.

Pro analýzu výchozího stavu průmyslové datové sítě (technologická síť) byla uvažována síť v architektuře hvězda s centrálním síťovým L3 přepínačem a koncovými síťovými přepínači, která využívá redundantních komunikačních cest mezi jednotlivými síťovými prvky. Pro zjištění míry zabezpečení byly uplatněny metody analýzy indukce a dedukce. Pro potvrzení zjištěných skutečností byl proveden pasivní sken technologické sítě.

Centrální L3 přepínač je ve správě hlavního správce síťové infrastruktury, který patří do struktur IT střediska. Koncové prvky a nastavení za tímto středem sítě jsou ve správě střediska řízení a regulace, spadají tedy do kompetencí systémového specialisty. Do jednotlivých koncových síťových prvků jsou připojeny průmyslové systémy, které jsou zdroji dat v rámci průmyslové datové sítě. Síť je využívána pro řízení výroby, sběr dat a kontrolu nad výrobním procesem. Jsou zde zastoupeny sériové komunikace na principu sběrnic RS485. Tyto sběrnice jsou již nedostačující pro dnešní požadavky na komunikaci, ale vlivem nemožnosti plného nahrazení sběrnic je nutné je integrovat do novodobých průmyslových sítí, řešených většinou na úrovni Ethernetu. Pro tuto integraci jsou využity převodníky, které jsou realizovány samostatnými jednoúčelovými zařízeními umožňujícími transparentní přístup na dané sériové linky, nebo pomocí programovatelných automatů pro řízení výroby. Programovatelné automaty se v rámci průmyslové sítě integrují od roku 2000, jsou zde tedy zastoupena i zařízení z dnešního pohledu zastaralá, na kterých není možno implementovat formy zabezpečení nad úrovní vrstvy síťového rozhraní modelu TCP/IP. Jsou zde i modely automatů, které již umožňují základní formy zabezpečení, a taktéž nejnovější modely automatů, které plně kopírují a nativně podporují nejnovější požadavky

na kyberbezpečnost. Síť je na základní úrovni segmentována v rámci čtyř rozsahů IP adres ve třídě C.



Obr. 16 Technologická síť

Formy stávajícího zabezpečení jsou tvořeny uzamykatelnými rozvaděči, jež disponují veřejně dostupnými klíči. Typ použitého klíče je definován výrobcem rozvaděče (například Rittal). Stejným stylem jsou umísťovány řídicí automaty, u kterých nejsou řešeny fyzické možnosti zabezpečení. Koncové síťové přepínače jsou řešeny pomocí již nepodporovaného zařízení, které je často na hraně své fyzické životnosti, primárně tato zařízení nejsou určena do provozu v průmyslovém prostředí.

Obr. 17 Původní koncový přepínač Cisco v technologické síti [41]

Řídicí automaty disponují základním nastavením zabezpečení, které je implementováno přímo od dodavatele. Není zde realizováno řízení přístupu do automatů a ani zde nejsou zaznamenávány auditní změny řídicího softwaru. Firmware v automatech není aktualizován.

Dohled řízení výroby je provozován na počítačích, které jsou primárně určeny pro administrativní prostředí, jsou zde provozovány nepodporované operační systémy. Počítače již nejsou pod podporou výrobce, nedisponují posledními záplatami operačních systémů, programy, jež umožňují dohled a řízení technologie, jsou spouštěny pod lokálním vestavěným účtem administrátora. Jsou zde potlačeny jakékoliv formy zabezpečení na úrovni operačního systému. Tyto počítače jsou plně otevřeny a vystaveny do sítě, je na nich povoleno sdílení místních disků a přístupy do systémových složek. U těchto stanic není řešena žádná forma programového nebo hardwarového zabezpečení pro připojení jiných zařízení, stanice jsou pouze umísťovány do uzamykatelných plechových boxů, které postrádají aktivní výměnu vzduchu. Plechové boxy disponují univerzálním klíčem, jejž opět definuje výrobce plechového boxu a jenž je pro všechny boxy stejný. Vzhledem k nemožnosti výměně vzduchu jsou počítače neustále provozovány na vyšších provozních teplotách, než je tomu v administrativní sféře. Při letních vysokých teplotách jsou plechové boxy otevřeny, aby se zabránilo poškození řídících počítačů přehřátím, vlivem toho aktu dochází k průniku prachových části do prostoru počítače a dochází k vytvoření prachové vrstvy, která poté znemožňuje efektivní chlazení. Kvůli otevření boxů je potlačena i základní fyzická ochrana zařízení. Počítače nedisponují žádným antivirovým programem. Po servisní stránce jsou v neuspokojivém stavu, náhradní díly prakticky nejsou k dispozici. Pokud některá z dohledových stanic přestane fungovat, její nahrazení je otázkou hodin a dnů. Na stanicích jsou provozovány služby vzdáleného dohledu, které nejsou nijak dále vyvíjeny a podporovány, tudíž zde vzniká možnost zneužití těchto služeb. Při servisním úkonu je třeba stanici vyčistit, provést kontroly a popřípadě celou stanici znovu instalovat. Provozní dohledové počítače jsou osazeny komunikačními kartami a jsou direktivně připojeny na sériové sběrnice standardu RS485. Slouží jako komunikační brány pro nadřazené systémy, jako jsou systémy sběru dat. Karty pro připojení do sériových linek nejsou již výrobcem podporovány, pro jejich chod je nutno instalovat neaktuální ovladače. Vlivem jejich velikosti nelze tyto karty osadit do průmyslových počítačů. V některých případech jsou tyto karty již na pokraji životnosti a narušují chod sériových sběrnic.

Obr. 18 SLC 5/05 – automat od firmy Rockwell Automation, uvedený na trh v roce 1991

Stanice používané pro vývoj algoritmů pro řízení jsou vybaveny neodpovídajícím neaktualizovaným operačním systémem, taktéž mimo podporu výrobce, program pro antivirovou kontrolu není přítomen. Jednotliví pracovníci nejsou v rámci technologické sítě nijak auditováni, autorizováni a jejich přístup do vývojových stanic je řešen pomocí jednoho typu virtuální vývojové pracovní stanice, která je rozklonována mezi několik vývojových pracovníků. V technologické síti jsou tyto stroje reprezentovány stejnou identitou, a nelze tedy určit, komu daný stroj náleží. Pro připojování k jednotlivým automatům jsou používány neaktuální verze vývojového programu. Není přítomna žádná politika hesel a definic přístupů do vývojových stanic.

Je nutno podotknout, že nepodporovaný operační systém musí být i nadále provozován, jelikož nelze ihned všechny struktury řízení přesunout na novější systémy pod podporou, a dále zde vzniká nekompatibilita mezi staršími automaty pro řízení provozu a novějšími operačními systémy.

Nejsou zde nastavena žádná omezení na straně komunikací z řídicích systémů, provozních a vývojových počítačů. Chybí zde konfigurace jednotné ověřovací autority na úrovni sítě, například služba Active Directory od firmy Microsoft. Jedná se o systém adresářových služeb, které se používají pro autentizaci a autorizaci uživatelů, počítačů a poskytování dalších služeb v rámci sítě. Pro autentizaci a autorizaci řídicích systémů není

implementována žádná autorita a ani žádné jiné dílčí ověřování. Služba Active Directory je sice v rámci technologické sítě přítomna, ale není nijak rozvíjena.

Není zde implementován systém řízeného poskytování aktualizačních balíčků pro nosné operační systémy a taktéž není aktualizováno programové vybavení, které je provozováno. Přechod mezi komunikačními sběrnicemi je řešen pomocí operátorských stanic, využívaných i k dohledu a monitorování technologie, tudíž při jakémkoliv výpadku této stanice je odstaven komunikační kanál do starších systémů sběrnic.

Výsledkem popsaného stavu zabezpečení jsou možnosti přímého přístupu do systémů dohledu a řízení, možnosti nekontrolovatelného připojování vývojových pracovníků do systémů řízení. Dohledovým pracovníkům je umožněn plný nekontrolovaný přístup do technologické sítě. Kdokoliv může připojovat cizí neověřená zařízení do pracovních stanic, do technologické sítě nebo může použít lokálních portů k připojení do systémů řízení. Stanice provozované v technologické síti jsou neaktualizovány a není na nich prováděna periodická údržba, což má za následek nespolehlivost a výpadky zařízení na dohledových pracovištích. Není možno nahradit dohledová zařízení novějšími vlivem nekompatibility hardwaru a softwaru, který je zde provozován. Z pohledu administrace sítě nelze spárovat identitu vývojového stroje a jeho uživatele, jelikož všechny vývojové stanice mají totožnou identitu. Programové vybavení vývojových stanic není aktualizováno a kvůli tomu nejsou aktualizovány verze programového vybavení systémů řízení.

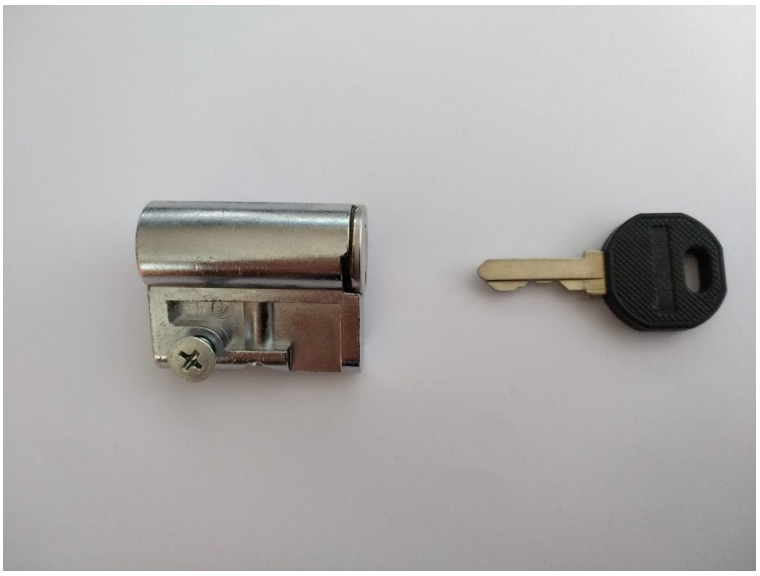
Koncepce technologické sítě a řízení je řešena pouze pro zajištění přenosu dat. Pokud by došlo k závadě na zařízení, která by generovala nekontrolovatelné množství všesměrových komunikací, zahltil by tento provoz celý segment sítě a ohrozil by chod ostatních zařízení.

Vlivem nepoužívání centrální autority ověřování a centrální správy skupinových politik nelze zaručit stejné nastavení všech stanic v rámci technologické sítě.

Provedení pasivního skenu bylo realizováno externí firmou, která provedla sken technologické sítě, zaměřený na kontrolu stability koncových zařízení. Kontrolovány byly otevřené porty na zařízeních a poskytované služby zařízeními v rámci technologické sítě. Do technologické sítě bylo připojeno zařízení externí firmy, byly zřízeny prostupy do technologické sítě, u kterých byly potlačeny základní stupně ochrany – přesně dle požadavků na protiplnění. Při pasivním skenu byly pozorovány výpadky v datových komunikacích. Pomocí skenu byly ověřeny a doplněny zjištěné skutečnosti. Výsledky pasivního skenu nebylo možno šířeji prezentovat.

3.2 Zabezpečení na úrovni vrstvy síťového rozhraní

Je kladen důraz především na fyzické zabezpečení prvků, jež spolu komunikují nebo které slouží ke komunikaci. Jednotlivé části infrastruktury by neměly být veřejně přístupné. Pro omezení přístupu k jednotlivým částem komunikační infrastruktury lze tyto prvky umísťovat do uzamykatelných místností, do racků nebo rozvaděčů, které jsou vybaveny systémy neveřejného jednotného klíče. Pro zmíněné systémy jednotného klíče je veden seznam vlastníků klíče, je tedy možno určit, kdo je daným klíčem vybaven.



Obr. 19 Systém neveřejného jednotného klíče

Problémem mechanického zabezpečení pomocí systému jednotného klíče je nemožnost zjistit, kdo do místnosti k zařízení přistoupil a v jakou dobu. Systém jednotného klíče může být vybaven kamerovým dohledem jednotlivých míst, kde se nacházejí prvky infrastruktury, nicméně monitorovat tímto stylem všechny vstupní body do síťové architektury by bylo značně nákladné. Pro omezení možnosti připojení cizích zařízení do sítě bylo navrženo použití mechanických záslepek do nevyužitých portů koncových síťových přepínačů. Podobný systém záslepek je doporučeno použít pro nevyužité USB porty na operátorských stanicích.

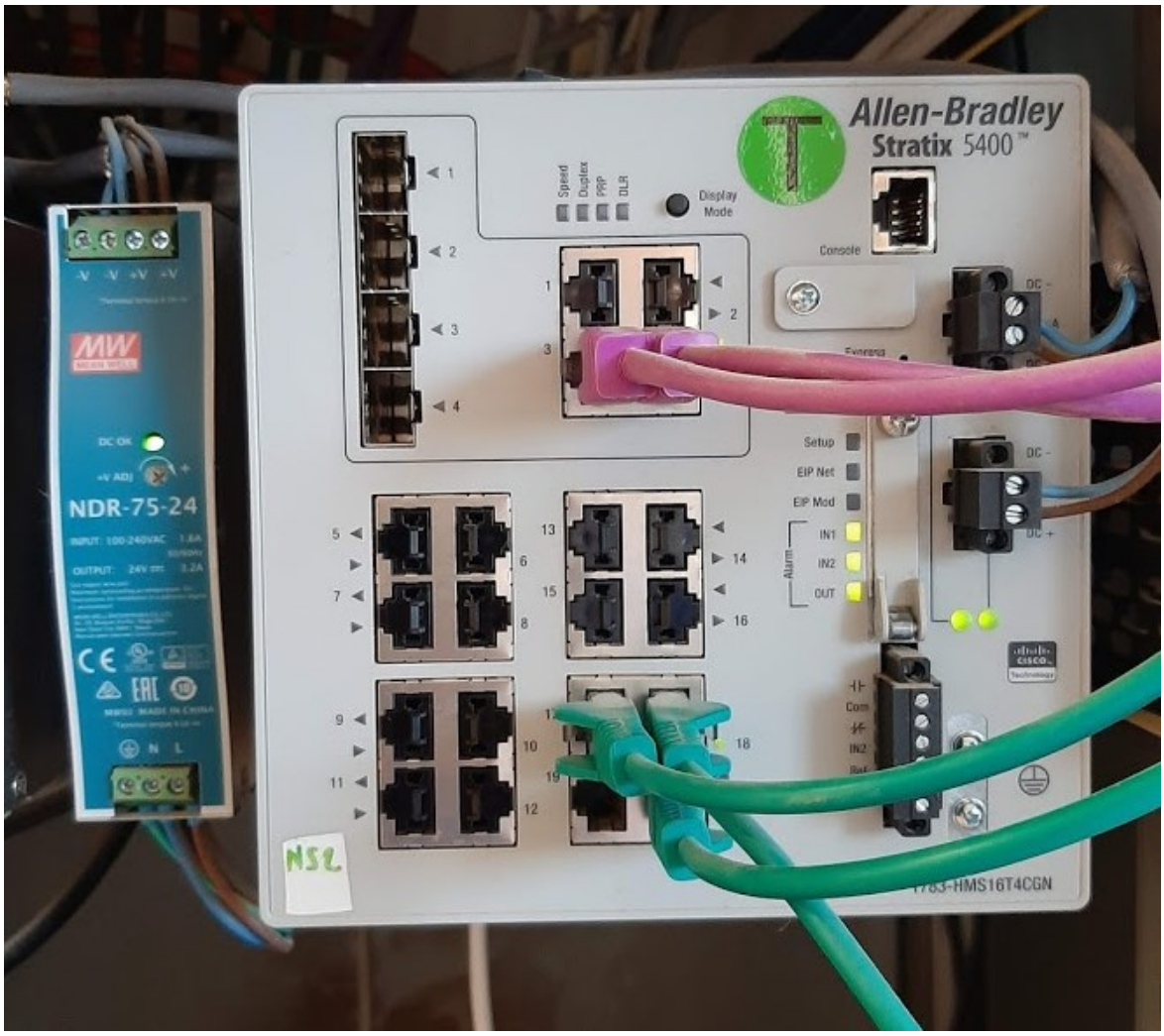
Obr. 20 Systém záslepek do USB portů [42]

Pro propojování technologií a koncových síťových přepínačů je důležité dbát na použití správných typů komunikačních kabelů a komunikační kabely ukončovat v patch panelech. Propojení mezi patch panely a koncovými síťovými přepínači je dále realizováno pomocí nestíněných originálně lisovaných datových propojů (patch kabelů). Každé takto realizované přípojné místo bude poté fotograficky zaznamenáno a bude uzamknuto systémem neveřejného jednotného klíče (viz Obr. 19).

Jednotlivé síťové přepínače z rodiny Cisco jsou vyměněny za síťové přepínače z rodiny Stratix řady 5000 od firmy Rockwell Automation, která je rovněž dodavatelem automatů řídících výrobu (viz Obr. 21).

Z pohledu nastavení jednotlivých síťových přepínačů je důležité nastavit vazbu mezi jednotlivými MAC adresami zařízení připojených na porty na koncovém přepínači. Toto nastavení lze realizovat dvěma způsoby. Prvním z nich je fixace daných MAC adres na porty síťového koncového přepínače, druhou možností je omezit maximální počet MAC adres na jednotlivé porty. U druhé varianty je třeba zvolit čas expirace jednotlivých adres, tedy pokud je do portu připojeno nové zařízení, kdy má stará MAC adresa uvolnit pozici v tomto pravidle. Pokud je využito přepínačů, jež patří do architektury řídicích systémů, jako jsou například síťové přepínače Stratix řady 5000, je možno monitorovat jejich stav a zobrazovat tato data na operátorských stanicích. Další možností nastavení zabezpečení u přepínačů z rodiny Stratix řady 5000 je možnost monitorování výskytu jedné MAC adresy na různých portech síťového přepínače (Flapping MAC adres). Je-li pravidlo zavedeno, pak při tomto jevu dochází k firmwarové blokaci jednotlivých portů. Pro nynější potřeby

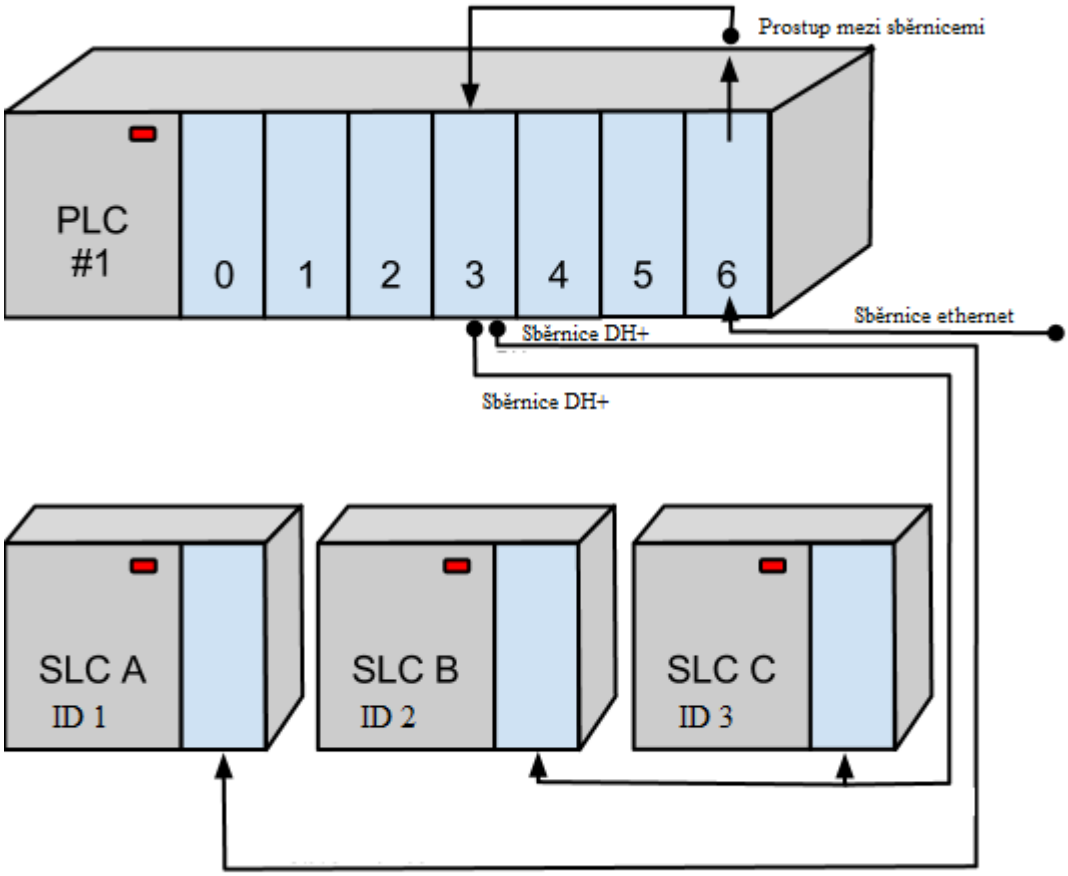
zabezpečení bude použito mechanismu pro omezení počtu dvou MAC adres na jeden port koncového síťového přepínače s časem expirace neaktivní MAC adresy jedna minuta. Síťové přepínače Stratix budou implementovány do struktur řízení, jež budou umožňovat poskytování diagnostických dat do nadřazených systémů. Nadřazené systémy řízení budou provádět aktivní monitoring síťových přepínačů, čímž bude docíleno alespoň základního online monitoringu chodu datové sítě. Data o chodu a diagnostice budou zpracována v dohledovém softwaru a budou i separátně ukládána v rámci logů dohledového softwaru.



Obr. 21 Nově nasazený prvek Stratix 5400

Pro zabezpečení starších sériových sběrnic na bázi standardu EIA485 je důležité používat definovaná přenosová média. Pro platformu komunikací firmy Rockwell Automation jsou to sběrnice DH+ (Data Highway Plus) a DH485 (Data Highway 485) a je nutno u nich používat výrobcem definované konektory a realizovat trasy sběrnic, které budou

zabezpečeny polohou, budou tedy umísťovány mimo dosah lidských zdrojů. Sběrnice budou zavedeny do přípojných míst, jež budou v uzamykatelných rozvaděčích. Ty budou vybaveny systémem jednotného neveřejného klíče. Sběrnice budou ukončeny odpovídajícím impedančním přizpůsobením a jejich připojení bude pravidelně kontrolováno. Zařízení na těchto sítích budou mít fixně definována identifikační označení. Fyzické datové prostupy budou realizovány výhradně převodníky k tomu určenými. Jako převodníky mohou být osazeny řídicí automaty s rozhraním standardu typu Ethernet a přídavným rozhraním pro sériové komunikace na bázi standardu EIA485 nebo jednoúčelové převodníky třetích stran.



Obr. 22 Blokové schéma řídicího systému komunikujícího přes více sběrnic [43]

Jako formu fyzické ochrany je nutno zabezpečit základní lokální přístupy do řídicích automatů? Tato forma ochrany bude realizována jako omezení přístupu do řídicího automatu formou zaheslování vnitřního programu a potlačení jiných forem přístupu k automatu, jako jsou vypnutí USB (Universal Seriál Bus) portů, vypnutí vstupně výstupních sériových linek

a požadování vyšších forem ověřování přístupu k automatu. Tyto formy budou vztaženy k centrální autoritě pro ověřování, která je pro platformu Rockwell Automation řešena pomocí služby FactoryTalk Directory (FTD) a definovaných oprávnění na úrovni aplikace. FactoryTalk Directory patří do rodiny aplikací a služeb nazvaných FactoryTalk. Umožňují aplikační zabezpečení a zprostředkovávají komunikaci mezi zařízeními na platformě výrobků Rockwel Automation. Je nutno pravidelně kontrolovat novější verze firmwaru automatů a postupně je nasazovat. Dalším prvkem bezpečnosti je kontrola nejnovějších zranitelností automatů a implementace ochran [44].

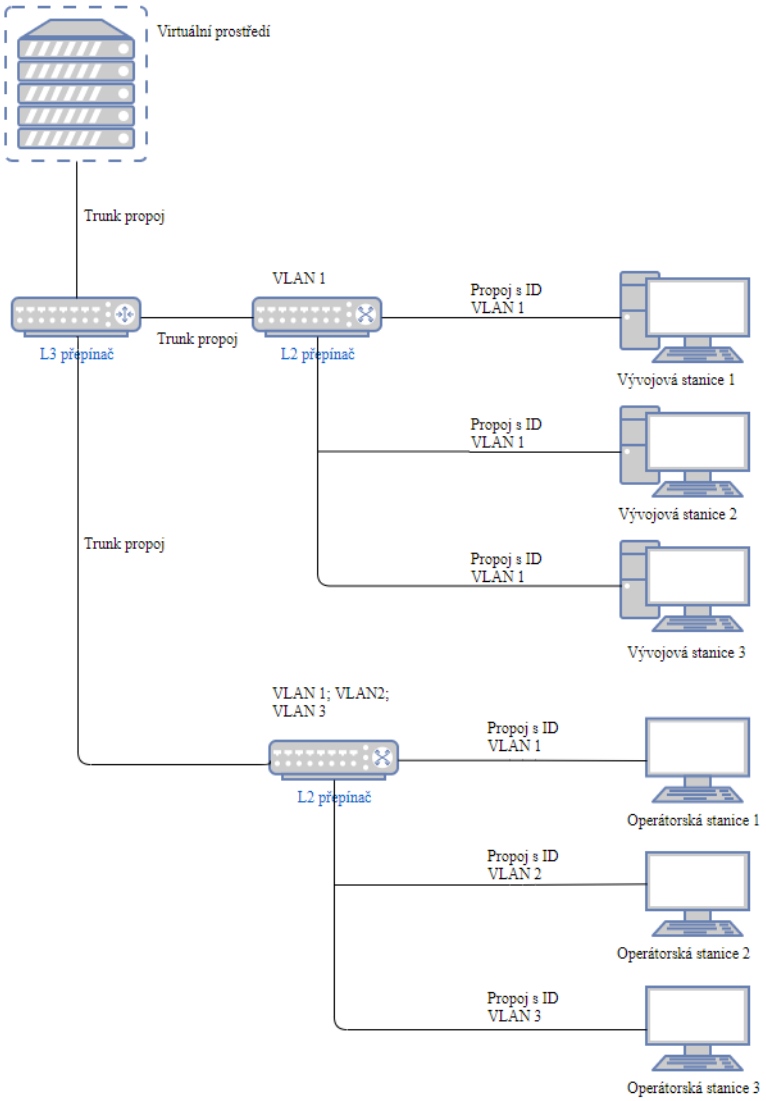
3.3 Internetová vrstva a její zabezpečení

Zabezpečení na úrovni síťové vrstvy je řešeno již primárně na úrovni nastavení definic zabezpečení v rámci jednotlivých síťových přepínačů, na úrovni IP adres a protokolu ICMP a ARP. Na této vrstvě dochází k fixnímu spojení MAC adres a IP adres jednotlivých komunikujících zařízení, tyto ARP tabulky vznikají na úrovni L3 síťových přepínačů. Dle výše uvedené topologie a původního nastavení technologické sítě je přistoupeno k segmentaci sítě pomocí VLAN (Virtual Local Area Network), což jsou virtuální sítě vytvořené na již fungující platformě technologické sítě (nosná síť). Virtuální sítě sdílejí s nosnou sítí síťový hardware, používají stejná fyzická datová média pro přenos informací. Zařízení komunikující v rámci jednotlivých virtuálních sítí generují komunikační rámce, jež jsou poté značeny dle jednotlivých VLAN a přenášeny nosnou infrastrukturou do centrálního L3 přepínače, kde dochází k jejich přesměrování do místa určení a přeznačení do patřičné VLAN. Takovéto architektuře musejí odpovídat i síťové prvky využívané pro komunikaci, je tedy nutno použít prvky umožňující management, který dovoluje nastavení jednotlivých portů na síťovém koncovém prvku. Pro takzvané uplinkové porty, což jsou porty spojující síťový střed s koncovými prvky, je nastavení definováno jako trunk, označující, že daný port propouští veškerou komunikaci z definovaných VLAN v rámci koncového prvku. Přiřazení odpovídající VLANy jednotlivým zařízením je definováno na úrovni přístupového portu na koncovém prvku, který je definován v režimu přístupu (Access mode) a je mu přiřazena patřičná identifikace VLAN. Pakety generované zařízeními lze označovat pomocí identifikačních znaků VLAN i na úrovni programové, čemuž odpovídá funkce označování VLAN (takzvané tagování paketů). Ty je možno konfigurovat na úrovni síťové karty na operačním systému Windows Server [45].

Hlavní devizou takto vytvořených struktur je omezení možnosti interakce mezi jednotlivými částmi technologie, a tedy i vymezení možných chybových stavů do ohraničených komunikačních zón a zároveň zachování možnosti komunikace mezi zařízeními v rozdílných virtuálních sítích. Pro takto vytvořené VLAN jsou definovány vlastní IP rozsahy, dle počtu zařízení je jeden IP rozsah třídy C rozsegmentován od čtyř nezávislých VLAN, definovaných vlastními branami a vlastní adresní maskou. Tímto je docíleno i omezení všesměrových komunikací (broadcastů) mimo takto ohraničené celky. Mezi zmíněnými komunikačními bloky je možno vytvářet přístupové listy. Ty jsou definovány na centrálním L3 přepínači. Nevýhodou takto řešené segmentace sítí je nemožnost komunikace mezi virtuálními sítěmi v případě výpadku centrálního L3 přepínače.

Pro zabezpečení je zde použito definic přístupových matic, které jsou derivátem z komunikačních map, jež tvoří vývojáři řídicích aplikací na aplikační úrovni modelu TCP/IP. Tyto matice sestavené z IP adres jednotlivých komunikujících zařízení jsou poté definovány v centrálních prvcích jako přístupové listy (Access listy), tento typ zabezpečení bývá označován jako White list (seznam povolených zařízení, adres a služeb), prostupy jsou tedy povoleny pouze těm IP adresám, které se vyskytují v tomto definičním seznamu.

Potlačení komunikace na bázi protokolu ICMP není implementováno, jelikož jeho jednotlivé dílčí části jsou využívány pro prvotní diagnostiku zařízení. Pro tyto účely je používáno příkazu ping, směřovaného na zjišťované zařízení. Pokud dané zařízení aktivně odpovídá na žádost o echo, tedy odezvu na ping, je možné usuzovat, že zařízení je aktivní [46].



Obr. 23 Schematické uspořádání stanic v rámci technologické sítě

3.4 Opatření zvyšující zabezpečení na úrovni transportní vrstvy

Pro průmyslové sítě je možno využít přenosy dat pomocí TCP i UDP spojení. Je ovšem nutno ještě před přenosem stanovit důležitost dat. Pokud jsou data velmi důležitá a jsou pomocí nich řešeny vyšší formy řízení, doporučuje se data přenášet pomocí TCP spojení. Pro přenosy pomocí TCP spojení je nutno na aplikační vrstvě programu, který inicializuje přenos dat, vyřešit problematiku vypršení spojení, například při násilném přerušení komunikace, aby nedocházelo k zahlcení komunikujících zařízení. Přenos dat pomocí UDP spojení je doporučen pro data, která mají nízkou prioritu a slouží většinou k informativním účelům, nebo se jedná o velmi pomalu měnící se data.

Princip přenosu je plně v rukou vývojáře aplikací, jelikož ten jediný může nastavit prioritizaci dat s ohledem na stupně řízení provozu.

3.5 Soubor opatření na aplikační vrstvě

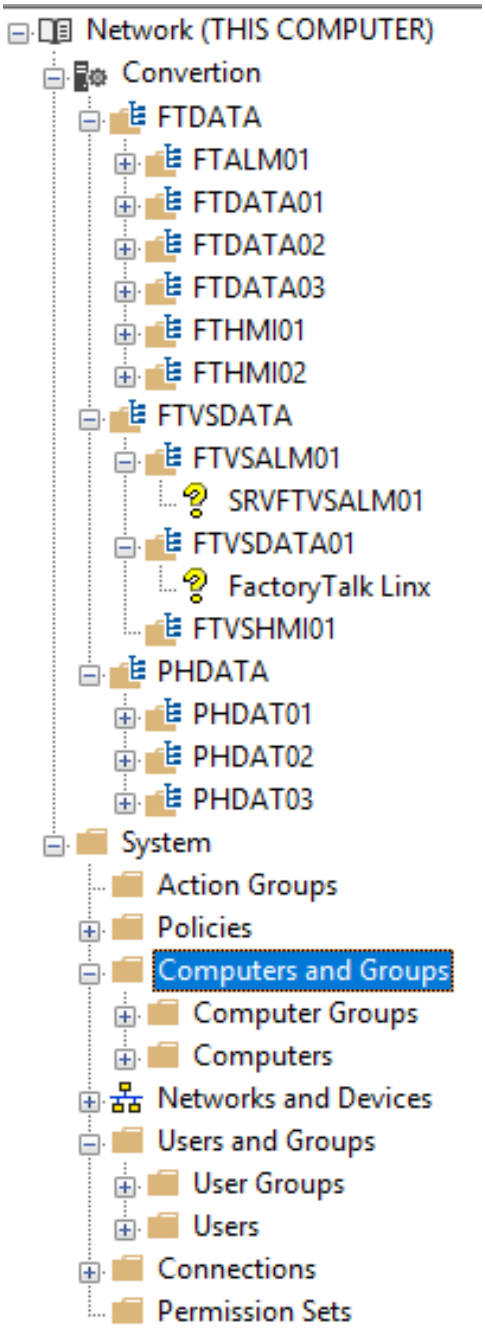
Aplikační vrstva představuje oblast, v níž působí většina vývojových pracovníků, kteří používají pro provoz svých aplikací hardware třetích stran. Zpravidla se jedná o zakoupená zařízení, vybavená nativními způsoby zabezpečení na vrstvách síťového rozhraní a transportní vrstvy. U vrstvy aplikační se jedná o soubor doporučení a možností, jak definovat řízenou komunikaci. Z pohledu zabezpečení sítí a dostupnosti služeb je nastavení stanoveno tak, že co není využíváno, je zakázáno. Pokud přijde požadavek na poskytování služby, je nutno zvolit zabezpečený typ komunikace. Pro koncová zařízení typu automat od firmy Rockwell Automation se jedná především o služby webových serverů, tedy protokolů HTTP/HTTPS, SNMP protokolů ve verzi jedna a dva. Pokud je použit protokol SNMP pro získávání informací o stavu zařízení, pak bude provozován ve verzi tři s patřičným uživatelským jménem a heslem se zapnutým šifrováním. Komunikace s řídicími automaty probíhá pomocí komunikace na úrovni CIP protokolu nativního aplikačního protokolu od firmy Rockwell Automation nezávislého na typu použité sběrnice. Výhodou této formy komunikace je definování komunikační obálky a komunikačního protokolu, které jsou pro ostatní zařízení na síti nečitelné, za předpokladu, že zde není veden útok typu man in the middle a odposlouchávací zařízení není nakonfigurováno pro odpovídající typ komunikace [47].

Do souboru opatření posilujících zabezpečení je nutno zařadit ověřování jednotlivých účastníků komunikace, ty je možno definovat aplikačním listem s definicí komunikačních přístupů, kdy jsou umožněny komunikace pouze v rámci přesně definovaných typů zařízení a jejich firmwarů. Tento typ zabezpečení je dodáván jako vestavěný volitelný v zařízeních od firmy Rockwell Automation. Při využití zabezpečené komunikace pomocí CIP security protokolu jsou data zabezpečena při přenosu. Tento typ komunikace vyžaduje, aby oba účastníci komunikace disponovali stejnou implementací CIP security protokolu. Vlivem různorodosti použitých řídicích systémů není možno tento protokol implementovat v rámci návrhu zabezpečení zkoumané technologické sítě, proto jedinou formou autorizace a ověřování komunikace mezi jednotlivými zařízeními je verifikace účastníků komunikace pomocí ověřování IP adresy, verze firmwaru a časového razítka. Pro komunikace mezi řídicími automaty a nadřazenými systémy, což jsou dohledové vizualizace a sběr dat,

popřípadě programovací prostředí, je použito ověřování pomocí rodiny nativních služeb fungujícího v rámci platformy FactoryTalk, jejíž součástí je i adresářová struktura FactoryTalk Directory (FTD), průmyslová obdoba služeb Active Directory [38].

Do adresářové služby FTD jsou připojena všechna zařízení z rodiny Rockwell Automation umožňující přímý přístup z technologické sítě. V rámci FTD jsou pro každé takové zařízení vytvořeny objekty, pro počítače a server jsou to objekty počítačů, pro uživatele to jsou buď objekty uživatelského typu v úrovni FTD, nebo zde mohou být začleněni uživatelé z Active Directory, pro řídicí automaty jsou zde vytvořeni zástupci s definovanou cestou k danému automatu. Aplikace, které jsou vytvořeny nad touto strukturou, používají výhradně komunikační struktury balíčku FactoryTalk.

Z Obr. 24 je patrné, že každý objekt vyskytující se na platformě FTD je zanořen do adresářové struktury. Díky tomuto stylu rozřazení lze pomocí oprávnění nad jednotlivými adresáři docílit přesného zacílení zabezpečení jednotlivých oprávnění k přístupům k jednotlivým objektům.



Obr. 24 FactoryTalk Directory

3.6 Přenos dat mezi sběrnicemi a přenosovými protokoly

Přenos dat v rámci různých protokolů je jistá forma ochrany, jelikož přenášená data jsou nucena projít transformací z různých komunikačních sběrnic, tedy na jedné straně z komunikační sběrnice standardu Ethernet a na druhé straně se jedná o sběrnice na bázi standardu EIA485. Při použití řídicích automatů jako převodníku dochází ke kontrole

přenášených dat. Data do automatu vstupují přes kartu ethernetového komunikačního rozhraní zajišťující komunikaci v rámci struktur Ethernetu. Data dále pokračují po vnitřní sběrnici automatu do procesoru automatu, kde jsou kontrolována. Poté jsou data poslána po vnitřní sběrnici automatu karty, jenž zprostředkovává komunikaci se sériovou sběrnicí. Díky tomu dochází k filtraci dat na aplikační úrovni, kterou zajišťuje vstupní ethernetová karta. Výhodou této přenosové struktury je možnost rozdělení režií nutných pro zpracování přenášených dat. Režie pro příjem a filtraci dat je soustředěna do vnitřních struktur ethernetové karty. Režie pro kontrolu dat je soustředěna do procesoru automatu a režie pro přenos dat do sériových sběrnic je záležitostí karty pro sériové komunikace. Výsledkem tohoto přístupu k datům je, že automat přijme pouze výrobní data. Tento typ přenosu informace byl zvolen jako jediný možný pro komunikace procházející z prostředí technologické sítě na platformě Ethernet na sběrnice sériového charakteru, na kterých je využíváno k přenosu informace pomocí protokolu Modbus RTU.

Převodníky fungují pro transparentní přenos dat, jedná se o jednoúčelová zařízení, jež jsou vybavena možností uložení konfigurace v místní paměti. Při poruše je místní paměť vyjmuta a vložena do nového převodníku, na vnitřní paměti je uložena plná konfigurace převodníku. Při přechodu ze sběrnic fungujících na standardu Ethernet jsou data transformována na jiný typ přenosového protokolu. Problém při použití transparentního přenosu dat je nemožnost zajistit rozdělení režií pro kontrolu a transformaci v rámci přenosových protokolů a sběrnic. Procesor převodníků zpracovává veškerou síťovou komunikaci a konverzi užitečných dat mezi sběrnicemi a komunikačními protokoly. Problém nastává v rychlosti zpracování dat, kde dochází k zahlcení převodníku. Řešením tohoto problému je převodníky umisťovat až za zařízení umožňující filtraci datového provozu. Takovým zařízením můžou být jednoduché automaty, které nedisponují možností rozšíření o jiné typy komunikací, než je Ethernet, nebo nasazení aplikačních firewallů.

3.7 Problematika stanic připojených do průmyslové datové sítě

Pro zabezpečení operátorských přístupů do technologické sítě a taktéž pro vymezení nepodporovaného hardwaru a softwaru operátorských dohledových stanic jsou nasazena terminálová řešení přístupu k dohledovým vizualizacím pomocí platformy Wyse od společnosti DELL a vytvořeny odpovídající protikusy virtuálních stanic. Terminály jsou vybaveny firmwarem a operačním systémem platformy Linux, který je upraven pro potřeby terminálového přístupu pomocí protokolu vzdáleného přístupu. Pro produkty firmy

Microsoft je tento protokol nazván jako Připojení ke vzdálené ploše. Pro potřeby správy a nastavení oprávnění a zabezpečení terminálů je nasazena centrální správa, do které jsou tyto terminály připojeny, a přejímají vytvořené politiky. V rámci těchto politik jsou potlačeny třídy vstupních zařízení mimo třídy pro klávesnice a myši, jsou definovány požadavky na zobrazovací rozlišení, požadavky na aktualizační cyklus operačního systému terminálu a zajištění automatického přihlášení [48].

Spouštění odpovídajícího softwaru na virtuální stanici je řešeno tak, aby byly minimalizovány úkony operátora potřebné ke spuštění dohledové aplikace. Terminály pro připojení na virtuální stanice používají systém autorizace buď na úrovni Active Directory, nebo na úrovni lokální autentizace a autorizace. Systém přihlašovacích jmen je pro každý velín technologie jiný a přihlašovací hesla jsou taktéž diverzifikována s ohledem na velíny, kde je tento terminálový přístup zřízen. Politika hesel a uživatelských účtů je definována s ohledem na požadavky přejaté z Active Directory.

Obr. 25 Terminál Wyse 3040 [48]

Obrovskou výhodou uvedených terminálů je rozdělení paměti na sekce pro uložení operačního systému s omezenými právy pro zápis, další část paměti je definována jako operační, kde je poskytnuta pro běžící aplikace, a poslední část paměti je určena pro běh samotného operačního systému. Tudíž ani při napadení není možno přímo zapsat škodlivý kód do paměti určené pro uložení operačního systému. Terminály jsou periodicky kontrolovány centrální správou a je možno kontrolovat neoprávněné pokusy o přístup, pokusy o připojování dalších zařízení do terminálů. Při použití digitálního přenosu dat do

zobrazovacího zařízení je terminál schopen logovat připojení a odpojení zobrazovacích zařízení a tyto informace po vyžádání zaslat do centrální správy.

V rámci virtualizace operátorských dohledových stanic jsou na stanicích aplikovány politiky pro potlačení třídy zařízení, které jsou mapovány z terminálových stanic do virtuálních, mimo třídy obsahující definice klávesnice a myši, tedy obslužných periferií. Přístupy do dohledového obslužného softwaru jsou diverzifikovány dle oprávnění, jež jsou specifikována místními technology. Přístupy budou zaheslovány a požadavky na parametry hesla budou přejaty z nastavených doménových politik. Na operátorských stanicích jsou zapnuty ochrany v podobě firewallu a instalován antivirový software firmy Symantec. Operátorské stanice jsou pravidelně podrobeny aktualizačnímu cyklu a jsou pravidelně restartovány. Obslužný dohledový software je spouštěn pod účty lokálních uživatelů a aplikace, které jsou potřebné pro jeho chod a jsou spouštěny v režimu služby. Omezení přístupu na pracovní plochu je řešeno pomocí aplikace DeskLock od firmy Rockwell Automation, která znemožňuje uživateli přístup k jiným aplikacím a službám, než jsou v rámci jejího nastavení povoleny. Přístup na virtuální dohledová pracoviště je řešen pouze pomocí služeb připojení ke vzdálené ploše. Administrativní přístup pro modifikace vizualizací na dohledových pracovištích je řešen pomocí služeb vzdálené plochy, kdy jednotlivým vývojovým pracovníkům je umožněn přístup do těchto stanic na základě doménových politik definovaných v rámci Active Directory. Firewally na operátorských stanicích jsou nastaveny v režimu vše, co není povoleno, je zakázáno. Výjimky tvoří pouze aplikace nutné pro chod dohledových softwarů. Zabezpečení na úrovni operátorských stanic jsou definována jako soubor opatření, jež mají za úkol minimalizovat možnost infiltrace aplikací, znesnadnit možnosti modifikace běžících aplikací a služeb a znemožnit přístup do technologické sítě [49].

Servery poskytující služby v rámci technologické sítě jsou vytvořeny taktéž jako virtuální a jsou tvořeny dle pravidla jeden server, jedna instalace aplikace. Pro serverové možnosti vizualizace řízení výroby je vytvořena struktura serverů, které poskytují přístup k řídicím automatům, tedy datové servery, dále jsou vytvořeny servery pro poskytování obrazovek pro dohled výroby, jako samostatné servery jsou vytvořeny alarmové, kde probíhá vyhodnocení stavů technologie. Tyto stavy jsou reportovány do operátorských stanic. Přístup k těmto aplikacím je řízen pomocí politik na úrovni Active Directory a na úrovni FTD. Veškeré komunikace v rámci serverů jsou řešeny pomocí ethernetového rozhraní a jednotlivé aplikace jsou proti sobě autorizovány pomocí struktur FTD, potažmo AD. Výhodou tohoto

přístupu k tvoření platforem dohledu řízení je možnost provozovat aplikace na rozdílných operačních systémech s různými formami zabezpečení, jelikož komunikace je vždy vedena po standardu Ethernet a v rámci jednoho komunikačního protokolu FactoryTalk [49].

Pro ukládání logů ze stanic z platformy FactoryTalk je použito databázového serveru, do něhož jsou v desetiminutových intervalech importována diagnostická data z dohledových stanic, dále jsou ukládány jednotlivé úkony vývojových pracovníků na úrovni aplikačního přístupu k vývojovým programům. Do stejného databázového serveru jsou ukládány datalogy z vizualizačních serverů. Každý datalog je unikátně pojmenován podle stanice, kde byla data vytvořena. Pro autorizaci a autentizaci spojení jsou použity lokální účty, příprava pro doménovou autorizaci je vytvořena, prozatím není nasazena z důvodu nedostatečného odzkoušení se staršími typy dohledových softwarů.

3.8 Nastavení koncových přepínačů

Pro eliminaci problémů, které mohou narušit chod sítě, je vhodné začlenit prvky zabezpečení co nejblíže místům, kde by mohlo dojít k výskytu nežádoucích stavů. Proto jsou definice zabezpečení sítě implementovány na koncových síťových přepínačích. Zařízení z rodiny Stratix 5000 umožňují implementaci definic zabezpečení do svých operačních systémů. Definice zabezpečení jsou vztaženy k ochraně přístupu do jednotlivých přepínačů a jejich nastavení. Pro nastavení přístupu do přepínačů jsou definovány dva uživatelské účty, které slouží k administrátorské úrovni přístupu do prvků. Jeden účet je stanoven pro administrátora IT zařízení a druhý pro systémového specialistu z oddělení měření a regulace. Součástí konfigurace koncových přepínačů jsou definice úrovní logování událostí, nastavení adres poskytovatelů časové známky, nastavení adres serverů pro překlad síťových adres a nastavení zotavení systému po výskytu chyby.

Dále jsou zde definice parametrů sítě, jako jsou definice spanning tree, včetně definice všech VLAN, jež se vyskytují v rámci technologické sítě, včetně těch VLAN, které mají být poskytovány na jednotlivých portech síťového přepínače. Jedním z bodů nastavení zabezpečení na úrovni koncových přepínačů je možnost omezení pro přenos kořene protokolu spanning-tree, který určuje ohodnocení datových cest v síti, toto hodnocení poté definuje datové toky v rámci sítě. Jedná se o protokol vymezující vznik smyček na úrovni vrstvy síťového rozhraní modelu TCP/IP. Protokol spanning-tree neustále monitoruje jednotlivá propojení v rámci síťové infrastruktury a oceňuje si jednotlivé propoje dle vlastního klíče. Protokol zasílá jednotlivým zařízením sítě zprávy, takzvané BPDU (Bridge

Protocol Data Units) zprávy, dle kterých poté dochází k informování jednotlivých zařízení o tom, kdo je centrálním středem sítě, informace ohledně konfigurace jednotlivých instancí stromu a informace o časových parametrech komunikací pomocí BPDU. Ochrany na jednotlivých koncových zařízeních omezují možnost nechtěné komunikace pomocí BPDU paketů ze strany přístupových portů. Po vyhodnocení komunikačních tras pomocí protokolu spanning-tree je možné určit, které porty a komunikační trasy z infrastruktury je nutno potlačit, aby nedocházelo k vytvoření smyček a zahlcení datové infrastruktury.

Nastavení zabezpečení sítě je vztaženo ke vstupním bodům do sítě, což představují u koncových přepínačů jednotlivé síťové porty. Ty na síťovém přepínači jsou nastaveny v přístupovém módu a k jednotlivým portům jsou přiřazeny odpovídající VLANy. Pro přístupové porty jsou nastavena omezení pro posílání paketů typu unicast (posílání paketů jednomu cíli), multicast (zasílání paketů skupině cílů) a broadcast (typ komunikace, kdy jedno zařízení posílá informaci všem ostatním zařízením v rámci sítě). Nastavení potlačení protokolů LLDP (Link Layer Discovery protokol) a CDP (Cisco Discovery Protokol) neumožňuje zjišťovat uzly sítě z rozhraní přístupových portů. Na prvcích jsou nastavena omezení pro počet připojených hostů v rámci jednoho portu, tedy počet připojených aktivních MAC adres na jednom portu. Tímto omezením se předchází možnosti zařazení dalšího síťového prvku s více zařízeními nebo vymezení zařízení, kterému se mění MAC adresa, například vlivem chyby na zařízení. Součástí nastavení ochrany je definice času, kdy dochází k zapomenutí neaktivních MAC adres. V návaznosti na toto nastavení je nutno specifikovat druh omezení, jež bude vykonáno, pokud dojde ke splnění podmínky maximálního počtu připojených zařízení do jednoho portu. Další část nastavení specifikuje parametry, za kterých je neaktivní MAC adresa zapomenuta. Dalším krokem bude implementace centrální správy pro ověřování MAC adres proti centrální autoritě. Bude disponovat databází definic buď absolutních MAC adres, nebo definicí, dle kterých bude možno určit, jestli daná MAC adresa patří zařízení, kterému má být umožněno připojení do technologické sítě. Tímto je posílena ochrana na vrstvě síťového rozhraní a internetové vrstvě modelu TCP/IP [50].

```
interface FastEthernet1/2
 switchport access vlan 601
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 16
 switchport port-security
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 storm-control broadcast level pps 1k
 storm-control multicast level pps 1k
 storm-control unicast level pps 16k
 storm-control action shutdown
 storm-control action trap
 no lldp transmit
 no lldp receive
 no cdp enable
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 100
```

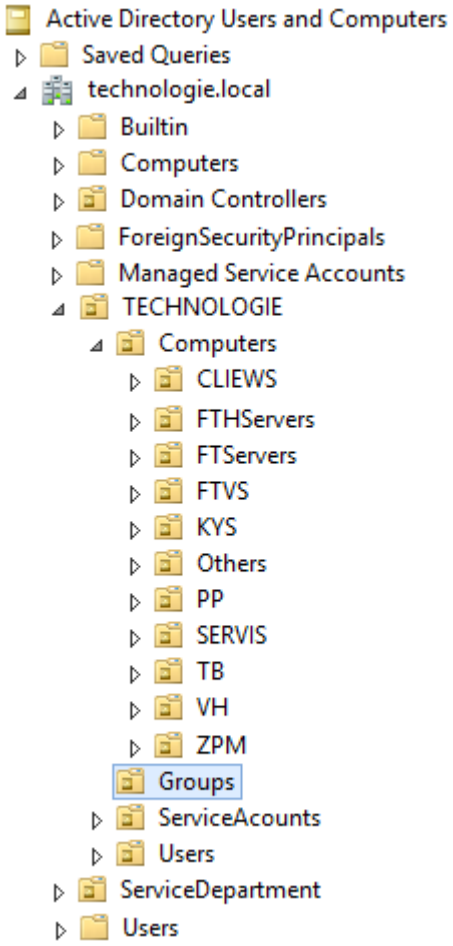
Obr. 26 Ukázka nastavení koncového přepínače typu Stratix 5400

Každému koncovému přepínači je přiřazena IP adresa, která poté umožňuje vzdálené nastavení. Ověřování účtu a hesla je prozatím řešeno na lokální úrovni. Pro přístupy do síťových přepínačů budou sestaveny seznamy IP adres, kterým bude povolen přístup. Pokud přepínač má dedikovaný management port umožňující připojení do místní sítě, bude tento port připojen do privátní virtuální sítě. Pro eliminaci neoprávněného přístupu do zařízení bude port pro připojení lokální konzole zaslepen pomocí záslepky, kterou lze vyjmout pouze nástrojem.

3.9 Active Directory

V případě uvedeném v této práci se bude jednat o již implementované řešení, které čítá tři doménové kontroléry. V rámci zabezpečení je nutno naplnit struktury AD definicemi skupinových politik, uživatelských účtů, zaregistrovat všechna zařízení umožňující interakci s doménou, vytvořit odpovídající skupiny uživatelů a nad nimi definovat oprávnění. Je vytvořena adresářová struktura, inspirovaná označením průmyslových výrob v rámci zabezpečované technologické sítě. Do jednotlivých adresářů (Organization Unit) jsou vloženy objekty počítačů. Pro uživatele jsou vytvořeny skupiny odpovídající jejich

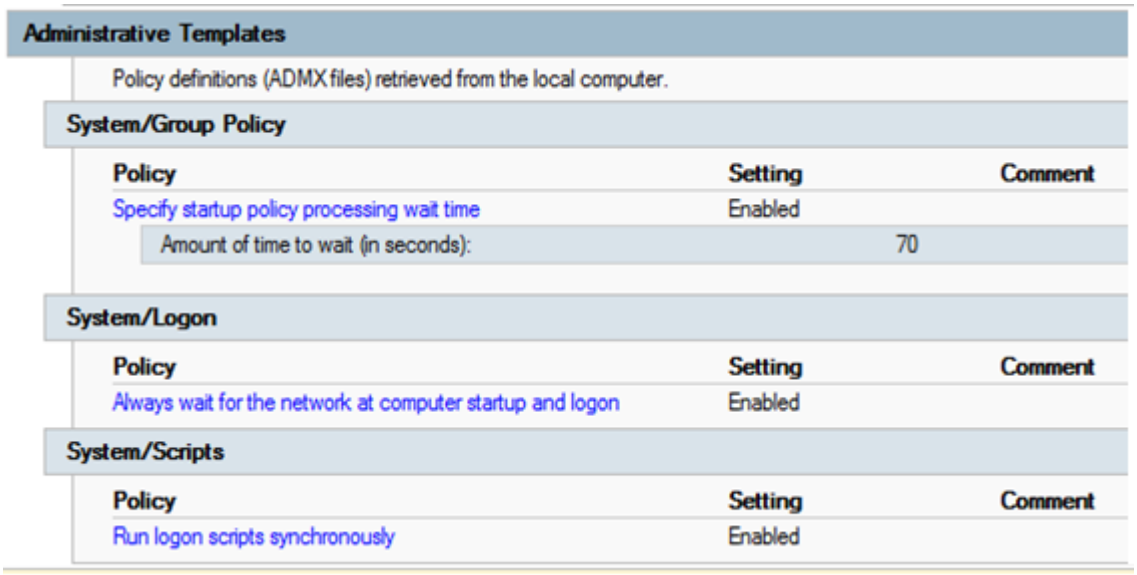
profesnímu zařazení. Vytvořené doménové politiky jsou poté směrovány buď do kořene domény, nebo je lze vnořit do adresářové struktury. V definici skupinových politik mohou být zahrnuty zásady pro změnu nastavení aplikací, požadavků na jednotlivá zabezpečení operačních systémů, mohou zde být vloženy sekvence, které se mají vykonat po spuštění operačních systémů, upravování záznamů v registrech, firewally a jiné. Je možné – pomocí Active Directory – cíleně distribuovat instalační balíčky aplikací, které mohou být centrálně spravovány. Jednotlivé aplikace provozované v rámci technologické sítě umožňují interakci s doménou, tedy přejímání definic přístupů a oprávnění do svých aplikačních politik. Pro uživatele je vytvořena centrální identita, jež mu umožňuje přístup do jednotlivých aplikací v technologické síti. Pro systémového specialistu se jedná o odlehčení agendy správy nad jednotlivými aplikacemi, jelikož veškerá oprávnění jsou stanovena v centrální autoritě domény [34][35].



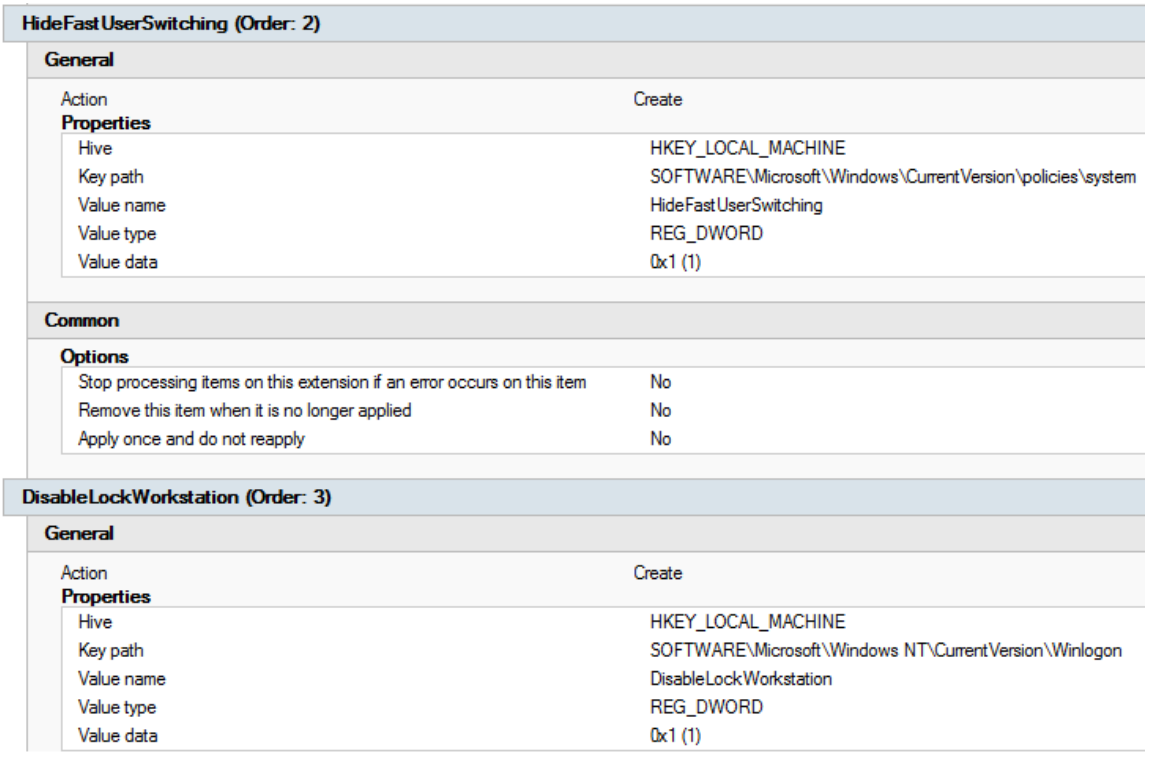
Obr. 27 Struktura Active Directory

Na úrovni domény jsou specifikovány požadavky na složitosti a struktury hesel, jsou zde definovány politiky pro aktualizační cyklus operačních systémů. Uživatelské účty a skupiny jsou poskytnuty do struktur platformy FactoryTalk, kde jsou jednotlivá oprávnění upravována a cílena přímo pro průmyslovou sféru a kde jsou omezována práva na úrovni aplikací. Veškeré politiky jsou tvořeny nad objektem uživatelské skupiny, která obsahuje jednotlivé účty uživatelů v technologické síti. Nastavení firewallů operátorských stanic je řešeno na úrovni AD a je potlačena možnost upravování politik na úrovni lokálních stanic. V rámci politik jsou vytvořena nastavení schémat napájení, jež jsou dále distribuována. Politiky distribuované z AD jsou nositeli nastavení omezujícího přihlašování uživatelů na konkrétní stanice integrované do domény, výjimku tvoří pouze skupina vývojových pracovníků. Pro skupinu vývojových pracovníků je vytvořena politika, která jim definuje oprávnění lokálních administrátorů na jednotlivých operátorských stanicích. Dalším nastavením nad skupinou vývojářských pracovníků je automatické mapování souborů ze souborového serveru oboru měření a regulace do síťových disků. Tento přístup k datům je nezbytný, jelikož je tím dosaženo sdílení jednotlivých vyvíjených programů v rámci kolektivu pracovníků. Jsou vytvořeny politiky pro jednotlivé externí společnosti, přistupující do technologické sítě striktně pomocí doménových účtů, politiky omezující, na které počítače mohou být externí firmy přihlášeny a do jakých systémů mohou zasahovat [34][35].

Vzhledem k nutnosti využívat na některých místech provozu plnohodnotné počítače v průmyslovém provedení jsou na úrovni politik v rámci AD stanoveny zásady a pravidla, která jsou implementována do těchto počítačů. Pravidla definují například nemožnost operátorů přepnout počítač do režimu spánku, použít funkce přepnutí uživatele, vymezují funkci tlačítka hibernace, umožňují použití služeb vzdálené plochy, zakazují správce úlohy při vyvolání kontextového menu. Pro správné spouštění skriptů při startu operačního systému je uměle vytvořeno okno pomocí politik. Skripty jsou spouštěny po sobě a jejich primárním cílem je umožnit operačnímu systému správnou identifikaci druhu připojené ethernetové sítě, tak aby vždy byly aplikovány správné zásady zabezpečení. Vlivem existence těchto strojů je nutno v rámci politik vytvořit zásady zabezpečení pro potlačení přejímání fyzicky připojených zařízení do virtuálních stanic [35].



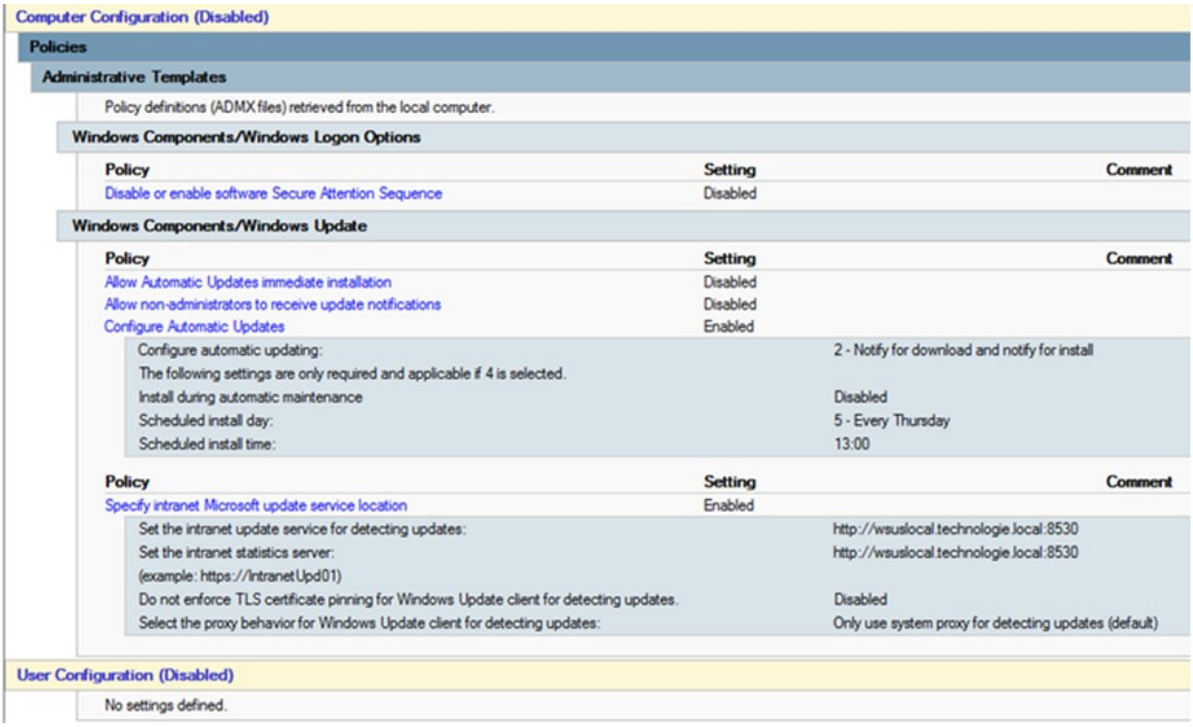
Obr. 28 Doménová politika pro synchronní spouštění operačního systému



Obr. 29 Doménová politika potlačující možnost přepínání uživatelů

Skupinové politiky umožňují definovat cestu k aktualizačnímu serveru v rámci technologické sítě a nastavení parametrů aktualizační služby na jednotlivých stanicích. Vzhledem k možnosti cílit skupinové politiky na konkrétní stanice lze vytvořit různé politiky na implementované aplikace. Vzhledem k povaze aplikací jsou definovány požadavky na

aktualizační cykly dodavatelem aplikací nebo dodavatelem zařízení, jež jsou propojena s aplikacemi na stanicích v technologické síti.



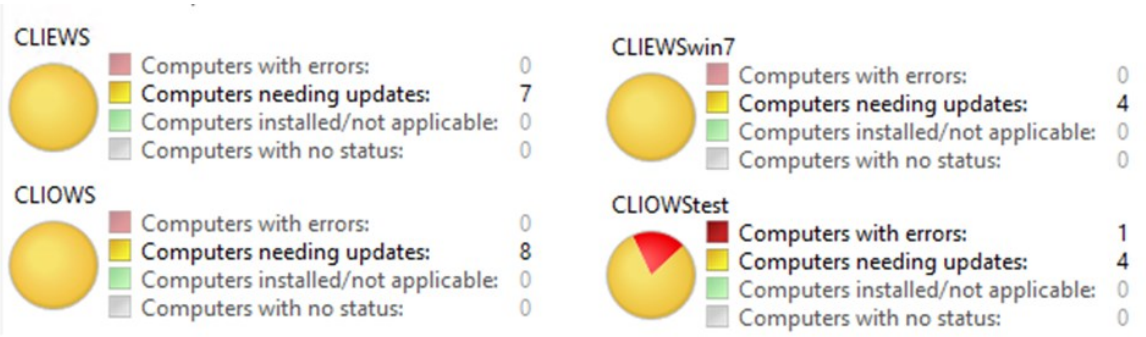
Obr. 30 Doménová politika s definicí cesty k centrálnímu aktualizačnímu serveru

Pomocí doménových politik lze definovat přístupy a povolení pro přihlášení do jednotlivých stanic v rámci domény. Tímto lze zajistit, že do stanic určených pro vývoj aplikací jsou přístupy povoleny pouze definovaným uživatelům. Stejným principem jsou řešeny přístupy servisních techniků do technologické sítě a do struktur FactoryTalk.

3.10 Windows Server Update Services

Pod názvem Windows Server Update Services (WSUS) se skrývá služba umožňující správci sítě, administrátorovi IT systémů nebo systémovému specialistovi centrálně ovlivňovat aktualizační cyklus a jeho obsah na úrovni průmyslové datové sítě. V rámci průmyslové datové sítě je využito místního řešení WSUS, které je napojeno na hlavní vnitropodnikový WSUS. K takovému řešení se přistoupilo kvůli snaze odlehčit přenos dat pomocí hlavního datového připojení do firmy. Díky této koncepci propojení jsou definice a aktualizace stahovány do hlavního aktualizačního serveru, jenž je poté poskytuje dále. V centrálním aktualizačním serveru jsou uchovávány informace o úspěšně

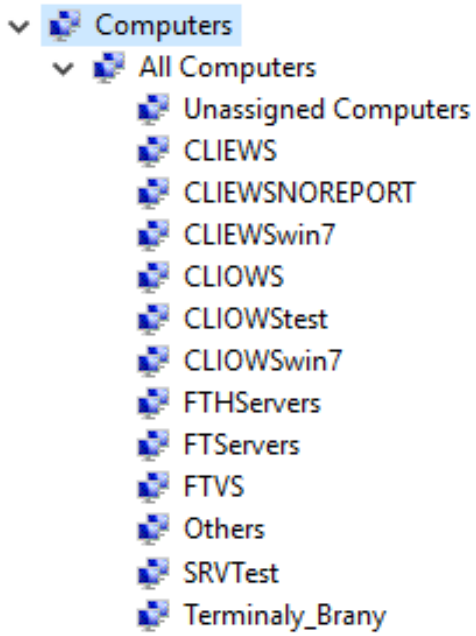
a neúspěšně aplikovaných aktualizacích, díky tomu je správce informován o stavu aktualizací napříč všemi stanicemi, které jsou do centrálního aktualizačního serveru směrovány [51].



Obr. 31 Informace o aktualizacích na stanicích v rámci technologické sítě

V rámci místního aktualizačního serveru jsou vytvořeny skupiny obsahující stanice a servery, každá skupina zahrnuje stanice a servery vztahující se k jednomu druhu aplikace. Jsou zde vytvořeny testovací skupiny. Pro větší míru kontroly vlivu aktualizací na běžící aplikace v rámci technologické sítě jsou definovány skupiny strojů, na které jsou aktualizace primárně instalovány, a je sledován dopad aktualizací na běžící aplikace. Koncept prvotního odzkoušení vlivu aktualizací je koncipován tak, aby nedocházelo k výpadkům aplikací v technologické síti. Definovaný přístup k cílenému nasazování aktualizací je kvitován dodavateli aplikací a dalších systémů v rámci technologické sítě, jelikož mohou být dodávány definiční soubory pro aktualizace a dle těchto definičních souborů je možno cíleně distribuovat aktualizace [51].

Dalším typem rozdělení koncových strojů do aktualizačních skupin je rozdělení dle jejich druhu. Jedna skupina sdružuje stanice s operačními systémy, jež jsou stále pod podporou výrobce, další skupina sdružuje stanice s operačními systémy s ukončenou podporou výrobce. V rámci tohoto rozdělení se stanice člení na vývojové, ke kterým je nutno volit speciální přístup z pohledu aktualizací, jelikož na sobě sdružují několik vývojových softwarů, a stanice operátorské, jež je nutno aktualizovat postupně, tak aby nedošlo k nemožnosti řídit výrobu.



Obr. 32 Struktura aktualizačního serveru

Vlivem centrálního systému distribuce aktualizací je možno snížit režie nutné k instalaci aktualizací a lze kontrolovat aktualizace jednotlivých aplikací a poté je dle doporučení výrobců aplikovat na již zaktualizované operační systémy. Díky tomuto přístupu nedochází k rozcházení verzí aplikací s verzemi operačních systémů.

Patřičně definovanými zásadami skupin na úrovni AD spolu se správným nastavením aktualizačního serveru je možno vymezit automatické instalování aktualizací v rámci technologické sítě. Toho faktu je hojně využíváno, jelikož dodavatelé průmyslových aplikací jsou defakto o dva až tři roky pozadu s vývojem kompatibilních systému vůči nejnovějším verzím operačních systémů. Tato skutečnost je dána především náročností vývoje průmyslových aplikací, které musí být vyvíjeny na bezvýpadkový a bezporuchový provoz a musejí být řádně odzkoušeny, než jsou podstoupeny zákazníkům.

3.11 Firewall

Pro posílení bezpečnosti bylo rozhodnuto, že v rámci technologické sítě budou instalována zařízení umožňující omezovat definované datové toky v rámci technologické sítě, firewally. V rámci technologické sítě bude definice paketového filtru využita pro přechody mezi jednotlivými virtuálními sítěmi a pro vstupně výstupní datové toky technologické sítě.

Vzhledem k možnosti nativní filtrace síťového provozu na vstupu do řídicích automatů bylo rozhodnuto, že tyto automaty budou plnit funkci aplikační brány. Budou definovány nejmenší možné komunikační okruhy, do kterých bude přistupováno výhradně přes definované aplikační brány. V rámci zabezpečení budou tyto brány zahrnuty do platformy FactoryTalk. Přistupovat do programovacího prostředí lze pouze pomocí ověřených účtů a ověřených aplikací v rámci FactoryTalk. Přístupy do aplikačních bran jsou monitorovány a ukládány do datalogů.

Pro řešení otázky zabezpečení na rozhraní sítě a stanic jsou určeny definice firewallu na úrovni operačních systémů dohledových a vývojových stanic. Firewall provozovaný na operačních systémech firmy Microsoft vychází z definice paketového filtru a stavového firewallu, tudíž je možné v rámci jeho nastavení vymezit definiční obory IP adres, jež budou paketovým filtrem propouštěny. Stavovou částí firewallu jsou shromažďovány informace o komunikacích procházejících přes firewall, v případě komunikace s dalším zařízením v rámci datové sítě pak stavový firewall umožní i zpětnou komunikaci. Pokud je ovšem komunikace inicializována z datové sítě a zdrojová IP adresa komunikace není definována v povolených adresách, je komunikace blokována. V rámci firewallu jsou definovány tři síťové profily, jimiž je určeno, do jakého typu sítě je operační systém připojen. Typy síťových profilů jsou doménový, privátní a veřejný profil. Doménový profil reprezentuje připojení systému do sítě, kde je definována doména a systém je do domény připojen. Privátní profil je definován pro připojení systému do sítí, kde není vyžadována doménová registrace systému, což mohou být privátní sítě. Veřejný profil je definován pro sítě, které jsou veřejně přístupné, počítá se tedy s tím, že je na nich aplikována malá množina zabezpečení. Nastavení firewallu stanic s operačními systémy je nastaveno do doménového profilu. Definice povolených aplikací je řešena na úrovni doménových politik s akceptací lokálních modifikací nastavení firewallu na stanicích. Nastavení pro zbývající dva profily firewallu je definováno jako zákaz průchodu všech příchozích a odchozích komunikací.

Definice povolených komunikujících IP adres není nasazena z důvodu roztříštěnosti komunikací mezi stanicemi a řídicími automaty.

Nastavení firewallu je řešeno dle pravidla, co není povoleno, je zakázáno. Tudíž jsou povoleny pouze ty typy komunikací, které využívají aplikace provozované na stanicích. Sdílení složek, sdílení tiskáren a zjišťování sítě je potlačeno. Pro připojení pomocí relace vzdálené plochy jsou povoleny s ověřováním na úrovni sítě. Aplikacemi instalovanými na stanice nacházející se v rámci technologické sítě jsou při jejich instalaci definována pravidla prostupů do firewallu. Tato pravidla zahrnují veškeré možné komunikační prostupy, jež aplikace mohou využívat ke komunikaci s ostatními zařízeními. Proto je nutné po kompletní instalaci všech aplikací zkontrolovat nastavení prostupů ve firewallu a potlačit nežádoucí prostupy, které nebudou využívány. V rámci technologické sítě se preferují komunikace definované v rámci platformy FactoryTalk.

Aplikacemi, jež jsou instalovány na jednotlivé stanice, jsou definována pravidla pro průchody dat přes firewall. Tato pravidla zahrnují veškeré prostupy firewallem, kterých je aplikace schopna využít, pro zvýšení zabezpečení jsou pravidla pro nepoužívané komunikační prostupy potlačena.

Na vstupu do technologické sítě bude realizován síťový firewall, který bude schopen kontrolovat meziaplikační komunikace. Paketový filtr bude realizován na úrovni centrálního L3 přepínače, který zároveň zajišťuje přestupy mezi jednotlivými virtuálními sítěmi. Pro komunikace do technologické sítě bude využíváno pouze relací vzdálené plochy, a to pouze z definovaných stanic z administrativní sítě.

ZÁVĚR

Cílem diplomové práce bylo navrhnutí opatření pro zvýšení zabezpečení průmyslové datové sítě. Pro návrh vhodných opatření byly v teoretické části práce popsány protokoly Modbus RTU, který je provozován na sběrnici RS485, Modbus TCP protokol provozovaný na místních datových sítích standardu Ethernet. Jednotlivé protokoly a sběrnice byly popsány s ohledem na jejich zranitelnosti, odolnost proti nechtěným zásahům, rizika zabezpečení a jejich poruchovost. Pro návrh zabezpečení byla vybrána průmyslová datová síť, na níž jsou již provozovány systémy řízení výroby a sběr dat. Nad touto sítí byla provedena analýza zabezpečení průmyslové datové sítě. Stav před implementací jednotlivých prvků a částí zabezpečení odpovídal řešení sítě, která se postupně rozvíjela, a na otázku zabezpečení byl dosud kladen minoritní důraz.

V návaznosti na provedenou analýzu jsou v praktické části práce navrženy sady opatření s primárním cílem ochránit datovou cestu a umožnit bezproblémový přenos dat, což jsou sady opatření reprezentující první tři vrstvy modelu TCP/IP. Opatření mají zamezit neoprávněnému fyzickému vniknutí do technologické sítě, omezit všesměrová vysílání a umožnit vznik přestupových bodů, na kterých je možno nasazovat další formy zabezpečení. V rámci definic transportní vrstvy je poukazováno na nutnost používat především TCP formy spojení. Sady opatření na aplikační vrstvě jsou definovány jako obecně platná doporučení, doplněná o konkrétní úkony, které již jsou, nebo v brzké době budou realizovány.

Jsou zde popsána řešená zabezpečení pomocí implementace terminálových přístupů pro operátorské dohledové stanice, pro vývojové stanice, kde je možno definovat zabezpečení na úrovni terminálů. Pro centralizovanou správu jsou definovány služby FactoryTalk a Active Directory, jež mají podobný základ a stejnou logiku definování zabezpečení a nastavení. Jejich primárním účelem je ověřování, verifikace a definování oprávnění pro jednotlivé uživatele, aplikace a stanice v rámci technologické sítě. V návaznosti na bezvýpadkový provoz je nutno se zaobírat otázkou aktualizací a navazujících opatření. Tuto problematiku ilustruje nasazení serveru pro centrální správu a distribuci aktualizačních balíčků. Pro možnosti připojení zařízení do technologické sítě byly vybrány přepínače z rodiny Stratix, v rámci definic nastavení přepínačů jsou realizovány základní formy ochrany na úrovni vrstvy síťového rozhraní modelu TCP/IP. Obrovskou devizou implementace těchto přepínačů je možnost plného integrování do platformy FactoryTalk.

Firewally jsou důležitou součástí zabezpečení vnitropodnikových sítí, vlivem nemožnosti implementovat aplikační firewally do struktur sítě bylo přistoupeno k řešení firewallu na úrovni stanic připojených do technologické sítě.

V rámci práce jsou reflektovány skutečnosti, jichž bylo prozatím docíleno a které bylo možno implementovat. Nelze se nezmínit o problémech mezi pojetím otázky bezpečnosti mezi okruhem aplikačního vývoje a správců sítě. Tento rozpor je dán především nepochopením podstaty otázky zabezpečení z pohledu aplikací a jejich návazností na další vrstvy modelu TCP/IP. Další podstatnou rovinou pohledu je překotný rozvoj kyberhrozeb, na který průmysl nebyl připraven, jelikož některé části řízení jsou projektovány na nepřetržitý chod v řádu roků až desetiletí a v době jejich vývoje nebyly podmínky zabezpečení řešeny natolik intenzivně jako v dnešní době.

Pro zlepšení zabezpečení jsou plánovány změny topologie technologické sítě. Ta bude rozdělena do menších komunikačních bloků, které budou realizovány na kruhové topologii. Jednotlivé kruhy budou mít přesně definovány vstupní aplikační brány, před nimi budou předsazeny aplikační firewally. Jednotlivé kruhy budou realizovány nad funkčními celky, jež spolu úzce komunikují. Jednoúčelová zařízení budou připojována do technologické sítě jako uzavřené komunikační celky, kdy vstupní bod do systému bude řešen aplikační bránou nebo firewallem. Budou sjednocovány systémy řízení a systémy pro zobrazování informací. Dohledové aplikace běžící na nepodporovaných operačních systémech budou migrovány na novější verze. Pro aplikace, jež nemohou být migrovány, bude vyčleněn speciální adresní prostor a na ten budou aplikovány speciální požadavky na zabezpečení, které budou diskutovány s oddělením vývoje. Systémy provozované na sběrnicích typu RS485 budou postupně odstavovány a nahrazovány novějšími systémy, umožňujícími napojení do sběrnic fungujících dle standardu Ethernet. Budou prováděny pravidelné vnitropodnikové a externí audity zabezpečení a dle výsledků auditů budou dále navrhována opatření posilující zabezpečení technologické sítě.

Pro příklad konfigurace koncového přepínače používaného uvnitř technologické sítě byl zvolen koncový přepínač umožňující přístup do technologické sítě z vývojového pracoviště. Konfigurace koncových přepínačů je z větší formy unifikovaná, proto v práci nejsou přiloženy další příklady konfigurací koncových přepínačů.

Práce reflektuje snahu doplnit zabezpečení do technologické sítě z pohledu jednotlivce, který je omezen pracovní dobou, a možností kooperace mezi útvary. Zabezpečení technologické

sítě se bude i nadále rozvíjet a budou se stále více omezovat služby a prostupy do technologické sítě. K tomuto postupu je dobré dodat, že stanovená omezení budou moci být aplikována pouze za předpokladu, že nebude omezen provoz výroby.

SEZNAM POUŽITÉ LITERATURY

[1] **REMEŠOVÁ, A.** *Přehled protokolu MODBUS*. [online]. Plzeň: Západočeská univerzita, 2005, [cit. 2021-02-21]. Dostupné z: http://home.zcu.cz/~ronesova/bastl/files/modbus.pdf

[2] **ÁDÁMKÓ, É. and JAKABÓCZKI, G.** *VULNERABILITIES OF MODBUS RTU PROTOCOL – A CASE STUDY*. ANNALS OF THE ORADEA UNIVERSITY [online]. Varšava: ANNALS OF THE ORADEA UNIVERSITY. Fascicle of Management and Technological Engineering., 2015, 2015(XXIV), 203-206 [cit. 2021-02-21]. ISSN 1583-0691. Dostupné z: doi:10.15660/AUOFMTE.2015-1.13111

[3] **ÁDÁMKÓ, E., JAKABÓCZKI, G. and SZEMES, P.** *Proposal of a secure modbus RTU communication with adi shamir's secret sharing method*. International Journal of Electronics and Telecommunications [online]. Varšava: Polish Academy of Sciences, 2018, 2018(64(2)), 107-114 [cit. 2021-02-21]. Dostupné z: doi:10.24425/119357

[4] **BYRES, E., FRANZ M. and MILLER D.** *The use of attack trees in assessing vulnerabilities in SCADA systems*. In IEEE Conf. International Infrastructure Survivability Workshop (IISW ’04) [online]. New Jersey: Institute for Electrical and Electronics Engineers, 2004, 2004 (January 2004), 1–10 [cit. 2021-02-21]. Dostupné z: https://www.researchgate.net/profile/Eric-Byres/publication/228952316_The_use_of_attack_trees_in_assessing_vulnerabilities_in_SCADA_systems/links/546cfaf10cf26e95bc3caabf/The-use-of-attack-trees-in-assessing-vulnerabilities-in-SCADA-systems.pdf

[5] **BURDA, K.** *Systémy elektronického zabezpečení pro integrovanou výuku VUT a VŠB-TUO* [online]. 1. Brno: VUT v Brně, 2014 [cit. 2021-02-21]. ISBN 978-80-214-5060-8. Dostupné z: https://databaze.op-vk.cz/Product/Detail/71725

[6] *Is CAT5 cable good enough for RS-485 vs “true” RS-485 cable*. Electrical Engineering [online]. New York: Stack Exchange, 2012 [cit. 2021-02-21]. Dostupné z: https://electronics.stackexchange.com/questions/33455/is-cat5-cable-good-enough-for-rs-485-vs-true-rs-485-cable

[7] *Vývoj.HW.cz: RS485 & 422. Vývoj.HW.cz:* Základní informace o rozhraní RS-485 [online]. Praha: HW server s.r.o, c 2014 [cit. 2021-02-21]. Dostupné z: https://vyvoj.hw.cz/teorie-a-praxe/dokumentace/rs-485-422.html

[8] *Pravidla pro instalaci sběrnice RS-485.* ACS-line – Docházkové a identifikační systémy [online]. Holešov: ESTELAR, 2016 [cit. 2021-02-21]. Dostupné z: http://www.acsline.cz/media/document/pravidla-pro-instalaci-sbernice-rs485.pdf

[9] *Teco Wiki: Základní informace o rozhraní RS-485*. Teco Wiki: Základní informace o rozhraní RS-485 [online]. Kolín: TECO, c 2021 [cit. 2021-02-21]. Dostupné z: https://wiki.tecomat.cz/clanek/341-zakladni-informace-o-rozhrani-rs-485

[10] **ELAHI, A. and ELAHI, M**. *Data, Network, & Internet Communications Technology*. Florence: Delamar Cengage Learning, 2005. ISBN 978-1-4018-7269-4.

[11] *D-link,Cisco LAN And WAN Solution Service, Lucknow Up*. Indiamart [online]. Noida: IndiaMART InterMESH, c 2021 [cit. 2021-02-22]. Dostupné z: https://www.indiamart.com/proddetail/lan-and-wan-solution-service-14518675391.html

[12] **STROLE, N. C.** *The IBM token-ring network — A functional overview*. IEEE Network [online]. 1987, **1**(1), 23-30 [cit. 2021-02-22]. ISSN 0890-8044. Dostupné z: doi:10.1109/MNET.1987.6434299

[13] **ZVONÍČEK, P.** *Topologie siti.* Počítačové sítě [online]. Praha: Pepa Zvonicek, c 2020 [cit. 2021-02-22]. Dostupné z: http://pepa.zvonicek.info/inf/topologie.html

[14] **PETERKA, J.** *Ethernet II vs. IEEE 802.3*. Jiri Peterka [online]. Praha: Jiří Peterka, c 2015 [cit. 2021-02-22]. Dostupné z: http://www.earchiv.cz/anovinky/ai2058.php3

[15] **SMITH, J.** *'DLR': raising functionality while lowering cost and complexity.* DPA Magazine the engineers guide to new products and design ideas [online]. Tonbridge: IML Group, c 2021 [cit. 2021-02-22]. Dostupné z: http://www.dpaonthenet.net/article/60193/-DLR-raising-functionality-while-lowering-cost-and-complexity.aspx

[16] **MATOUŠEK, P.** *Síťové aplikace a jejich architektura*. 1. Brno: VUTIUM, 2014. ISBN 978-80-214-3766-1.

[17] *Rodina protokolů TCP/IP*: Část 2: Architektura TCP/IP. *EArchiv.cz* [online]. Praha: Univerzita Karlova, 2011 [cit. 2021-4-30]. Dostupné z: https://www.earchiv.cz/l223/gifs/P2_27.pdf

[18] *Transport Layer. Transport Layer – an overview* | ScienceDirect Topics [online]. Amsterdam: Elsevier B.V., c 2021 [cit. 2021-02-22]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/transport-layer

[19] *What is application layer? The functions and examples of application layer.* Router-Switch [online]. HongKong: Router-switch, c 2021 [cit. 2021-02-22]. Dostupné z: https://www.router-switch.com/faq/what-is-application-layer-the-functions-and-examples-of-application-layer.html

[20] **PHILCOX, J**. *Solaris 9 network administrator*. 2003. Indianapolis: Que, c2004. ISBN 978-0-7897-2870-8.

[21] **PRABHAKER, M.** *Chapter 1 Security Issues in the TCP/IP Suite*. 2007. Dayton: Wright State University, c 2007. ISBN 978-981-270-807-6.

[22] *Ping Tunnel*. Ping Tunnel - Send TCP traffic over ICMP [online]. Oslo: Institutt for informatikk, 2011 [cit. 2021-4-30]. Dostupné z: http://www.cs.uit.no/~daniels/PingTunnel/

[23] **DAYANANDAM, G., RAO, T. V., BUJJI BABU, D. and NALINI DURGA, S.** *DDoS Attacks—Analysis and Prevention.* Innovations in Computer Science and Engineering [online]. Singapore: Springer Singapore, 2019, 2019-05-26, 2018(32), 1-10 [cit. 2021-4-30]. Lecture Notes in Networks and Systems. ISBN 978-981-10-8200-9. Dostupné z: doi:10.1007/978-981-10-8201-6_1

[24] *Doporučené požadavky na projekty a výstavbu slaboproudých rozvodů pro nově zřízená pracoviště obcí III.* MVCR [online]. Praha: Ministerstvo vnitra České republiky, c 2021 [cit. 2021-4-30]. Dostupné z: https://www.mvcr.cz/sluzba/docDetail.aspx?docid=11708&docType=ART&chnum=2

[25] **KESSLER, C. G.** *Defenses Against Distributed Denial of Service Attacks.* GIAC Cybersecurity Certifications [online]. GIAC: SANS, c 2022 [cit. 2021-4-30]. Dostupné z: https://www.giac.org/paper/gsec/236/defenses-distributed-denial-service-attacks/100755

[26] *What is a honeypot*? Kaspersky [online]. Moskva: Kaspersky Lab., c 2021 [cit. 2021-4-30]. Dostupné z: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

[27] **HUNG-JEN, L., CHUN-HUNG, L., YING-CHIH, L. and KUANG-YUAN, T.** *Intrusion detection system: A comprehensive review*. Journal of Network and Computer Applications [online]. Amsterdam: Elsevier B.V., 2013, **2013**(36), 16-24 [cit. 2021-4-30]. Lecture Notes in Networks and Systems. ISBN 978-981-10-8200-9. Dostupné z: doi:10.1016/j.jnca.2012.09.004

[28] **XINYOU, Z., CHENGZHONG, L. and WENBIN Z.** *Intrusion prevention system design.* In: The Fourth International Conference onComputer and Information Technology*, 2004. CIT '04* [online]. New Jersey: IEEE, 2004, s. 386-390 [cit. 2021-4-30]. ISBN 0-7695-2216-5. ISSN 8425031. Dostupné z: doi:10.1109/CIT.2004.1357226

[29] **SWANAGAN, M.** *What Is The Difference Between IDS And IPS?* Purplesec [online]. Vienna: Purplesec, c 2021 [cit. 2021-4-30]. Dostupné z: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

[30] **BAI, Q., JIN, B., WANG, D., WANG, Y. and LIU, X.** *Compact Modbus TCP/IP protocol for data acquisition systems based on limited hardware resources.* Journal of Instrumentation [online]. 2018, **13**(04), T04004-T04004 [cit. 2021-4-30]. ISSN 1748-0221. Dostupné z: doi:10.1088/1748-0221/13/04/T04004

[31] **JOHNSON, G.** *The OSI Model, Part 2.* Applied motion [online]. Shanghai: Applied Motion Products, c 2021 [cit. 2021-4-30]. Dostupné z: https://www.applied-motion.com/news/2015/10/osi-model-part-2

[32] *SCADA MODBUS Protocol Vulnerabilities*. Cyberbit [online]. Ra'anana: Cyberbit, C 2021 [cit. 2021-4-30]. Dostupné

z: https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/

[33] *Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications*. Schneider-Electric [online]. Rueil-Malmaison: Schneider Electric Software, c 2018 [cit. 2021-4-30]. Dostupné z: https://download.schneider-electric.com/files?p_Doc_Ref=998-20186845

[34] **BEASLEY, J. S**. *Networking*. 2nd Edition. Upper Saddle River: Prentice Hall Certification, 2008. ISBN 978-0-13-135838-6.

[35] **DESMOND, B., RICBARDS, J., ALLEN, R. and LOWE-NORRIS, A. G.** *Active Directory*. 5th Edition. Sebastopol: O'Reilly Media, 2013. ISBN 978-1-4493-2002-7.

[36] **REGAN, P.** *MCTS 70-642 Exam Cram: Windows Server 2008 Network Infrastructure, Configuring*. Hoboken: Pearson IT Certification, 2008. ISBN 978-0-7897-3818-9.

[37] *Network Security: Packet Filtering Firewall.* Science Direct [online]. Amsterdam: Elsevier B.V., c 2021 [cit. 2021-4-30]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/packet-filtering-firewall

[38] *Stateful vs. Stateless Firewall Differences*. Security [online]. Ottawa: N-able Solutions ULC and N-able Technologies, 2019 [cit. 2021-4-30]. Dostupné z: https://www.n-able.com/blog/stateful-vs-stateless-firewall-differences

[39] *Aplikační firewall se neomezuje na porty a protokoly.* Computerworld [online]. Praha: Internet Info DG, a.s, c 2008 [cit. 2021-4-30]. Dostupné z: https://computerworld.cz/securityworld/aplikacni-firewall-se-neomezuje-na-porty-a-protokoly-45322

[40] *What is CIP Security for EtherNet/IP?* Pyramid Solutions [online]. Bingham Farms: Pyramid Solutions, c 2021 [cit. 2021-4-30]. Dostupné z: https://pyramidsolutions.com/network-connectivity/blog-nc/what-is-cip-security-for-ethernet-ip/

[41] *Cisco Catalyst Switch 2960-24PC-L.* Ab-com [online]. Hradec Králové: AB COM CZECH, C 2021 [cit. 2021-4-30]. Dostupné z: https://www.ab-com.cz/cisco-catalyst-switch-2960-24pc-l/?gclid=Cj0KCQjw38-DBhDpARIsADJ3kjmwu_wJTnGAMqtOOKEMjx9_GHrVOJk6C9vO06z0Zgz5zPjvdRelIroaAjHAEALw_wcB

[42] *Renkforce zámek portu USB rf-USBBlocker-02 sada 10 ks stříbrná RF-4463019*. Conrad [online]. Praha: Conrad Electronic Česká republika, c 2020 [cit. 2021-4-30]. Dostupné z: https://www.conrad.cz/p/renkforce-zamek-portu-usb-rf-usbblocker-02-sada-10-ks-stribrna-rf-4463019-1487673

[43] *A DH+ Example*. Inductive automation [online]. Folson: Inductive Automation®, c 2021 [cit. 2021-4-30]. Dostupné z: https://docs.inductiveautomation.com/pages/viewpage.action?pageId=1704045

[44] *FactoryTalk Security System Configuration Guide*. Rockwell Automation [online]. Milwaukee: Rockwell Automation Publication, 2021 [cit. 2021-4-30]. Dostupné z: https://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-e.pdf

[45] **SCHIFFER, C.** *COMMON INDUSTRIAL PROTOCOL (CIP™) AND THE FAMILY OF CIP NETWORKS.* ODVA [online]. Ann Arbor: ODVA, c 2016 [cit. 2021-4-30]. Dostupné z: https://www.odva.org/wp-content/uploads/2020/06/PUB00123R1_Common-Industrial_Protocol_and_Family_of_CIP_Networks.pdf

[46] *Disabling ICMP and SNMP won't increase security, but will impact network monitoring*. Paessler [online]. Nürnberg: Paessler, 2021 [cit. 2021-4-30]. Dostupné z: https://blog.paessler.com/disabling-icmp-and-snmp-wont-increase-security-but-will-impact-network-monitoring

[47] *Co je VLAN.* Správa sítě [online]. Praha: Aira GROUP, c 2016 [cit. 2021-4-30]. Dostupné z: https://www.sprava-site.eu/vlan/

[48] *Dell Wyse 3040 Thin Client User Guide.* Dell Technologies [online]. Round Rock: DELL, c 2021 [cit. 2021-4-30]. Dostupné z: https://www.dell.com/support/manuals/cs-cz/wyse-3040-thin-client/3040_ug/welcome-to-dell-wyse-3040-thin-client?guid=guid-423f8ce2-8950-497f-88d3-22c2e1e3fe4a

[49] **MOSKOWITY, J**. *Group Policy: Fundamentals, Security, and the Managed Desktop*. 2nd Edition. Nashville: John Wiley, 2013. ISBN 978-1-118-28940-2.

[50] *Security Features on Switches.* Cisco Press [online]. Hoboken: Cisco Press, c 2021 [cit. 2021-4-30]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=12

[51] *Windows Server Update Services (WSUS).* Microsoft Docs [online]. Redmond: Microsoft, C 2021 [cit. 2021-4-30]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL	Access Control List
AD	Active Directory
ARP	Address Resolution Protocol
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Units
CDP	Cisco Discovery Protoko
CIP	Common Industrial Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DDOS	Distributed Denial of service
DH+	Data Highway Plus
DH485	Data Highway 485
DNS	Doman Name System
DoS	Denial of service
EIA	Electronic Industries Alliance
FTD	FactoryTalk Directory
FTD	FactoryTalk Directory
FTP	File Transfer Protocol
FTP	Foiled Twisted Pair
GND	Ground
GP	Group Policy
GPS	Global Position System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Management Protocol
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPS	Intrusion Prevention Systems
LAN	Local Area Network
LLDP	Link Layer Discovery protokol
MAC	Media Access Control
OSI/ISO	Open System Interconnection/ International organization od Standardization
PVC	Polyvinylchlorid
RARP	Reverse Address Resolution Protocol
SCADA	Supervisory Control And Data Acquisition
SIEM	Securtiy Information and Event Managment
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/ Internet protocol
Telnet	Terminal Network
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: NASTAVENÍ KONCOVÉHO PŘEPÍNAČE

version 15.0	
no service pad	*potlačení servisního protokolu*
service timestamps debug datetime msec	*nastavení časové známky pro režim debug*
service timestamps log datetime year	*nastavení časové známky záznamu v logu*
service password-encryption	*hesla ukládána v nereverzibilním šifrováním při výpisu konfigurace*
hostname RTechnologie	*systémový název koncového přepínače*
logging buffered 131071	*nastavení velikosti bufferu logu*
username root privilege 15 secret heslonove	*vytvoření uživatele a nastavení úrovně jeho oprávnění (15 = nejvyšší)*
no aaa new-model	*potlačení externího zdroje pro aaa (pro autentizaci, autorizaci a accounting)*
clock timezone CET 1 0	*nastavení časového pásma centrální Evropy (plus volitelně nastavení pro přepínání letní/zimní čas)*
system mtu routing 1500	*nastavení velikosti rámce MTU*
ptp mode e2etransparent	*nastavení precision time protocol (distribuce milisekundového přesného času)*
vtp domain TS	*centrální distribuce VLANů pro danou doménu*
vtp mode off	*vypnutí příjmu centrálně distribuovaných VLAN*

ip dhcp snooping vlan 1-4094
ip dhcp snooping information option allow-untrusted
ip dhcp snooping information option format remote-id string MAR-TS
ip dhcp snooping

technika pro ochranu před neautorizovanými dhcp servery formou definic důvěryhodných a nedůvěryhodných portů, do dhcp žádosti lez připojit doprovodné informace o původu žádosti

ip domain-name technologie.local	*jméno domény*
ip name-server 10.131.20.165	*ip adresa DNS*
ip name-server 10.131.20.167	*ip adresa DNS*
crypto pki trustpoint TP-self-signed-1184999936	*nastavení přístupových certifikátů*
enrollment selfsigned	*způsob vydávání certifikátu (zde podepsaný sám sebou)*
subject-name cn=IOS-Self-Signed-Certificate-1184999936	*předmět certifikátu*
revocation-check none	*kontrola odvolání*

rsakeypair TP-self-signed-1184999936	*název šifrovacího RSA klíče*
crypto pki certificate chain TP-self-signed-1184999936	*název certifikátu*
certificate self-signed 01 nvram:IOS-Self-Sig#2.cer	*cesta uložení certifikátu*
errdisable recovery cause all	*rozsah obnovení v případě chyby*
errdisable recovery interval 30	*nastavení intervalu obnovení 30s*
mac access-list extended PVSTfilter	*definice MAC white listu pro potlačení rámců PVST, při ochraně MST*
deny any host 0100.0ccc.cccd	*potlačení přístupu pro definovanou MAC (PVST paketů a framů)*
permit any any	*pravidlo pro povolení ostatních komunikaci*
no mac authentication	*vypnutí MAC autentizace*
mac authentication table version 0	*definice tabulky povolených adres*
spanning-tree mode mst	*definice typu STP*
spanning-tree loopguard default	*definice ochrany detekce smyčky na portech, pokud není uvedeno jinak*
spanning-tree portfast bpduguard default	*ochrana proti BPDU paketům na portfast portech, režim portguard*
spanning-tree portfast bpdufilter default	*ochrana proti BPDU paketům na portfast portech, režim filtru*
spanning-tree extend system-id	*lze použít čísla VLAN nad číslo 1005*
spanning-tree pathcost method long	*definice metody výpočtu ,,ceny“ datové cesty*
spanning-tree mst configuration	*konfigurace spanning tree protokolu*
name TSTR01	*název regionu MSTP protokolu*
revision 1610	*revize konfigurace protokolu*
instance 1 vlan 281-282	*přiřazení VLAN do jednotlivých instancí v daném MST regionu*
instance 2 vlan 283-284	
instance 3 vlan 291-292	
instance 4 vlan 293-294	
instance 5 vlan 301-302	
instance 6 vlan 303-304	
instance 7 vlan 311-312	
instance 8 vlan 313-314	
instance 9 vlan 321-322	
instance 10 vlan 323-324	
instance 11 vlan 331-332	
instance 12 vlan 333-334	
instance 13 vlan 341-342	

```
instance 14 vlan 343-344
instance 15 vlan 351-352
instance 16 vlan 353-354
instance 17 vlan 361-362
instance 18 vlan 363-364
instance 19 vlan 371-372
instance 20 vlan 373-374
instance 21 vlan 381-382
instance 22 vlan 383-384
instance 23 vlan 391-392
instance 24 vlan 393-394
instance 25 vlan 401-402
instance 26 vlan 403-404
instance 27 vlan 411-412
instance 28 vlan 413-414
instance 29 vlan 421-422
instance 30 vlan 1
```

alarm profile defaultPort	*definování alarmovacího profilu pro rozhraní*
vlan internal allocation policy ascending	*alokace VLAN pro interní použití od ID 1006*
vlan 321-324,331-334,341-344,371-374	*inicializace VLAN*
lldp run	*spuštění služby pro zjišťování sousedů*
interface range FastEthernet 1/5 - 20	*vybrání rozsahu portů 1/5 až 1/20 pro konfiguraci*
switchport mode access vlan 331	*přiřazení access portů do VLAN 331*
switchport nonegotiate	*potlačení DTP zpráv na portech*
switchport port-security maximum 2	*maximální počet MAC adres na port*
switchport port-security	*aktivace bezpečnostních prvků na portech*
switchport port-security aging time 1	*čas, kdy bude MAC zapomenuta*
switchport port-security violation restrict	*typ reakce bezpečnostních prvků na narušení*
switchport port-security aging type inactivity	*kritérium pro zapomenutí MAC adresy*
storm-control broadcast level pps 1k	*definice limit proti paketovým bouřím typu broadcast*
storm-control multicast level pps 1k	*definice limit proti paketovým bouřím typu multicast*
storm-control unicast level pps 16k	*definice limit proti paketovým bouřím typu unicast*
storm-control action shutdown	*reakce na paketové bouře (zde vypnutí portu)*
storm-control action trap	*generování SNMP při překročení nastavených limitů pro paketové bouře*

no lldp transmit	*vypnutí odesílání LLDP paketů na daném portu*
no lldp receive	*vypnutí přijímání LLDP paketů na daném portu*
no cdp enable	*vypnutí CDP*
spanning-tree bpdufilter enable	*zapnutí BPDU filtru na portu*
spanning-tree bpduguard enable	*zapnutí BPDU ochrany na portu*
ip dhcp snooping limit rate 100	*definování kolik DHCP žádostí lze přijmout za 1 s*
interface GigabitEthernet1/1	
description UPLINK Stratix5400	*popis portu na přepínači*
switchport mode trunk	*nastavení portu do módu Trunk*
switchport nonegotiate	*potlačení DTP zpráv na portech*
mac access-group PVSTfilter in	*aktivace MAC filtru*
spanning-tree guard loop	*ochrana před smyčkou v síti*
ip dhcp snooping trust	*povolení prostupů DHCP ACK paketů*
interface Vlan1	*aktivace L3 rozhraní pro VLAN1*
no ip address	*vypnutí IP adresy pro dané rozhraní*
shutdown	*vypnutí L3 rozhraní pro VLAN1*
interface Vlan431	*vytvoření L3 rozhraní pro konkrétní VLAN*
ip address 10.131.43.11 255.255.255.0	*přiřazení IP k L3 rozhraní*
no ip route-cache	vypnutí paměti pro směrování
no shutdown	*aktivace rozhraní*
ip default-gateway 10.131.43.1	*definice výchozí brány*
no ip http server	*vypnutí http serveru*
ip http authentication local	*nastavení ověřování pro http rozhraní*
ip http secure-server	*povolení https serveru*
ip http secure-ciphersuite 3des-ede-cbc-sha	*šifrovací algoritmus pro https rozhraní*
line con 0	*zapnutí místní RS232 konzole pro správu*
exec-timeout 60 0	*čas pro automatické odhlášení z rozhraní*
login local	*zdroj pro ověřování přihlášení (zde místní uživatelé)*
line vty 0 4	*zapnutí základních virtuálních konzolí pro vzdálený přístup*
access-class 10 in	*řízení přístup k rozhraní přes ACL*
exec-timeout 60 0	*čas pro automatické odhlášení z rozhraní*
login local	*zdroj pro ověřování přihlášení (zde místní uživatelé)*
length 0	*vypnutí stránkování na konzoli*
transport input ssh	*vymezení metody pro vzdálený přístup ke správě (zde zabezpečené SSH)*

line vty 5 15	*zapnutí základních virtuálních konzolí pro vzdálený přístup*
access-class 10 in	*řízení přístup k rozhraní přes ACL*
exec-timeout 60 0	*čas pro automatické odhlášení z rozhraní*
login local	*zdroj pro ověřování přihlášení (zde místní uživatelé)*
length 0	*vypnutí stránkování na konzoli*
transport input ssh	*vymezení metody pro vzdálený přístup ke správě (zde zabezpečené SSH)*
no ip domain-name technologie.local	odstranění domény z DNS názvu zařízení
ntp source Vlan431	*vymezení rozhraní pro komunikaci se zdrojem přesného času*
ntp server 10.131.43.1	*určení zdroje přesného času*
end	