FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Demonstrace zabezpečení průmyslových řídicích systémů s protokolem CIP
Student:	Tomáš Plíhal
Vedoucí:	Ing. Jiří Buček, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	do konce letního semestru 2023/2024

Pokyny pro vypracování

Výuková stanice DS1 obsahuje programovatelný řídicí automat (PLC), modul displeje (HMI), digitální vstupy a výstupy (tlačítka, přepínače, kontrolky), z nichž některé jsou lokálně připojeny k PLC, a některé jsou připojeny přes síťový adaptér (AENTR). Výuková stanice obsahuje demonstrační aplikaci (např. simulace napouštění a vypouštění nádrže). Jednotlivé moduly jsou propojeny přes rozhraní Ethernet s protokolem CIP. Síťové prvky zahrnují Ethernetový switch, síťové bezpečnostní moduly CIP Security Proxy (CSP) a (volitelně) firewall.

Prostudujte protokol CIP se zaměřením na bezpečnostní aspekty (utajení, integrita zpráv). Prozkoumejte existující demonstrační aplikaci běžící na DS1 a demonstrujte nějaký typ útoku (odposlech, narušení integrity dat) na stávající konfiguraci.
Zvolte vhodné bezpečnostní opatření na zabezpečení komunikace mezi PLC a modulem AENTR nebo HMI pomocí bezpečnostních proxy CSP a demonstrujte jej na DS1.
Konkrétní typ útoku a bezpečnostní opatření budou zvoleny po konzultaci s vedoucím práce.

Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 20. února 2023 v Praze.

Bakalářská práce

DEMONSTRACE ZABEZPEČENÍ PRŮMYSLOVÝCH ŘÍDICÍCH SYSTÉMŮ S PROTOKOLEM CIP

Tomáš Plíhal

Fakulta informačních technologií
Katedra informační bezpečnosti
Vedoucí: Ing. Jiří Buček, Ph.D.
15. února 2024

Odkaz na tuto práci: Plíhal Tomáš. *Demonstrace zabezpečení průmyslových řídicích systémů s protokolem CIP*. Bakalářská práce. České vysoké učení technické v Praze, Fakulta informačních technologií, 2023.

Obsah

Seznam obrázků

Seznam tabulek

Rád bych vyjádřil svou vděčnost Ing. Jiřímu Bučkovi, Ph.D. za jeho cenné vedení během tvorby této bakalářské práce. Děkuji také mé rodině a kamarádům za neustálou podporu a povzbuzování.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 15. února 2024 .....

Abstrakt

Bakalářská práce je o kybernetické bezpečnosti síťové komunikace průmyslových řídících systémů využívajících protokol CIP. Obsahuje demonstraci zranitelnosti pomocí útoku na zranitelný systém (se zaměřením na integritu a utajení zpráv) a následné demonstrace možných zabezpečení. Konkrétní zařízení, na kterém útok a zabezpečení demonstruji je programovatelný řídící automat, síťový adaptér a ovládací panel, vyrobená firmou Rockwell Automation.

Klíčová slova zabezpečení průmyslových řídicích systémů, konfigurace CIP Security Proxy modulu, útoky na komunikaci CIP, zabezpečení komunikace mezi programovatelným řídícím automatem a síťovým adaptérem, CIP, CIP Security, MITM útok, odposlech komunikace

Abstract

The bachelor thesis is about cybersecurity of network communication of industrial control systems using CIP protocol. It includes a vulnerability demonstration using an attack on a vulnerable system (with a focus on integrity and confidentiality of messages), followed by a demonstration of security countermeasures. The specific devices on which I demonstrate the attack and security countermeasures are a programmable control PLC, network adapter, and control panel manufactured by Rockwell Automation.

Keywords industrial control system security, CIP Security Proxy module configuration, CIP communication attacks, communication security between programmable logic controller and network adapter, CIP, CIP Security, MITM attack, communication interception

Seznam zkratek

ACL	Access Control List
AENTR	Síťový adaptér
AES	Advanced Encryption Standard
API	Application Programming Interface
CIP	Common Industrial Protocol
CRC	Cyklický redundantní součet
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSP	CIP Security Proxy
CID	Connection Identifier
DS1	Demostanice pro testování kybernetické bezpečnosti
DTLS	Datagram Transport Layer Security
ECDHE	Elliptic-curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EtherNet/IP	EtherNet/Industrial Protocol
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HMAC	Keyed-hash Message Authentication Code
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ID	Identifier
IEC	International Electrotechnical Organization
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISA	International Society of Automation
MAC	Medium Access Control
MITM	Man in the Middle
ODVA	Open DeviceNet Vendors Association
OPC UA	Open Platform Communications Unified Architecture
OSI	Open System Interconnection
PLC	Programovatelný logický automat
PSK	Pre-shared Key
RFC	Request for Comments
SHA	Secure Hash Algorithms
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCMM	Unconnected Message Manager
UDP	User Datagram Protocol
USB	Universal Serial Bus
ČVUT	České vysoké učení technické v Praze

Úvod

Průmyslové řídicí systémy jsou kritickým prvkem v moderní průmyslové výrobě. Tyto systémy jsou běžně využívány k řízení a monitorování různých průmyslových procesů, včetně například výroby chemických látek, elektronických součástek a potravin. Bezpečnost těchto systémů je proto klíčová pro zajištění stability a bezpečnosti průmyslových procesů. Common Industrial Protocol (CIP) je jedním z nejčastěji používaných protokolů v průmyslových řídících systémech. Umožňuje komunikaci mezi různými prvky průmyslových sítí, jako jsou například programovatelné řídicí automaty (PLC), síťové adaptéry (AENTR) a modul displeje (HMI). Jeho hlavní výhoda je propojitelnost všech zařízení výrobního procesu pomocí jedné sítě. V této bakalářské práci se věnuji zabezpečení průmyslových řídicích systémů s protokolem CIP. Na výukové stanici DS1 nejprve demonstruji útok pro prokázání její zranitelnosti a následně ji vhodným způsobem zabezpečuji. Tato stanice mimo jiné obsahuje programovatelný řídicí automat (PLC) a síťový adaptér (AENTR), jejichž komunikaci zabezpečuji pomocí síťového bezpečnostního modulu CIP Security Proxy (CSP). Běží na ní aplikace, která simuluje řídicí systém pro napouštění a vypouštění nádrže.

V první části této práce se zabývám analýzou protokolu CIP. Vysvětluji základní principy této komunikace potřebné k porozumění mé práce. Také popisuji bezpečnostní prvky standardu CIP Security, který slouží pro zabezpečení CIP komunikace, a jeho implementaci pro zařízení výrobce Rockwell Automation.

Část druhá obsahuje praktickou demonstraci útoků provedených na již zmíněnou výukovou stanici. Nejprve odposlech komunikace a poté transformaci dat procházejících nezabezpečeným kanálem.

Ve třetí části popisuji doporučený způsob, jak tuto komunikaci zabezpečit. Vyberu bezpečnostní model vhodný pro zabezpečení komunikace výukové stanice a realizuji vybrané zabezpečení na výukové stanici.

Práce je určena především studentům školy, kteří budou na výukové stanici DS1 dále zkoumat zabezpečení průmyslových systémů. Také může být užitečná u potřeby zabezpečit obdobný průmyslový systém.

0.1 Cíle práce

Celkovým cílem této práce je ukázat, jak zabezpečit průmyslové řídicí systémy s protokolem CIP, minimalizovat riziko útoků na tyto systémy a upozornit, jak je jejich zabezpečení důležité. Což tedy zahrnuje: Seznámení čtenáře s protokolem CIP a jeho bezpečnostními aspekty, zejména utajení a integritu zpráv. Provedení demonstračního útoku na stávající konfiguraci DS1 (výuková stanice s řídícím systémem), například odposlech nebo narušení integrity dat. Navržení a zvolení vhodného bezpečnostního opatření pro zabezpečení komunikace mezi PLC a modulem

AENTR nebo HMI pomocí bezpečnostní proxy CSP. Demonstraci nového zabezpečeného řešení na výukové stanici DS1, s popisem použitých bezpečnostních principů.

Kapitola 1
Teoretická část

1.1 OSI model

V následujících částech této práce často používám při popisu protokolu CIP pojem OSI model. Proto považuji za důležité ho zde také krátce popsat.

OSI (Open Systems Interconnection) model je referenční model, který vytvořila společnost ISO (International Organization for Standardization) jako standard ISO 7498 pro propojování heterogenních počítačových systémů. Pokud se dodrží podmínky stanovené v tomto modelu, je umožněna spolehlivá komunikace po sériové sběrnici. OSI model se dělí na 7 vrstev, kde každá vrstva má přesně definovanou funkci a služby [1]. Jmenovitě je to vrstva fyzická, linková, síťová, transportní, relační, prezentační a aplikační.

Fyzická vrstva definuje propojení jednotlivých uzlů, konektory, médium datového přenosu (například koaxiální či datový kabel).

V linkové vrstvě se již řídí tok dat, synchronizují rámce a kontrolují chyby přenosu mezi uzly.

Síťová vrstva pomocí adresace a síťových protokolů určuje cestu, kudy se data dopraví k cílovému zařízení.

Transportní vrstva segmentuje odesílaná data, zajišťuje přenos a kontrolu dat, zda dorazila nepoškozená.

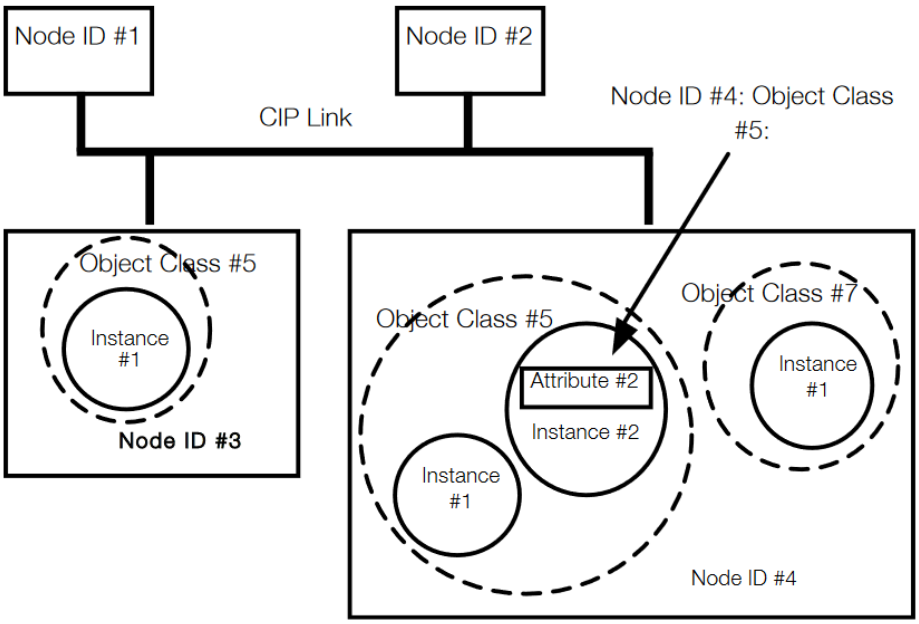
Relační vrstva určuje přístupová práva, zabezpečení a navazování spojení.

Prezenční vrstva definuje, jakým způsobem jednotlivé uzly komunikace kódují, šifrují, formátují data.

Aplikační vrstva definuje způsob komunikace s koncovou aplikací.

1.2 Common Industrial Protocol

Zpočátku funkci řídících systémů zprostředkovával člověk, který měl k dispozici jednoduché přepínače a indikátory, se kterými spouštěl, kontroloval a ovládal chod výrobního procesu. Tato metoda řízení se s rostoucí komplexitou výrobního procesu stávala stále méně použitelná. Proto se začala používat digitální komunikace, pomocí které se mohly řídit jednotlivá zařízení. Pro každý výrobní proces se tedy použila na míru vytvořená síť, po které zařízení komunikovala. To ale stále není vždy ideální řešení. Firmy, které mají více různorodých výrobních procesů či technologií pak vytvářely mnoho sítí pro jednotlivé účely. To vedlo ke zvýšené režii a nákladům na výrobu. Snaha o sjednocení celé podnikové infrastruktury pod jednou firemní sítí, zajištění bezpečné komunikace a kompatibilitu napříč mnoha technologiemi pak vedla k vytvoření protokolu CIP.



Obrázek 1.1 Příklad adresního schématu objektů[2]

Common Industrial Protocol je objektově orientovaný protokol spravovaný společností ODVA (Open DeviceNet Vendors Association) [2, 3]. V OSI (Open System Interconnection) modelu zastupuje protokol CIP vrstvu relační, prezentační a aplikační [4]. Mezi jeho hlavní služby patří sběr informací pro aplikace zajišťující automatizaci, konfiguraci, synchronizaci zařízení v síti a bezpečnost komunikace.

Informace týkající se protokolu CIP jsem čerpal z veřejně dostupných dokumentů přímo od společnosti ODVA [2, 4].

Protokol CIP poskytuje možnost využití několika síťových technologií zajišťujících vrstvu transportní, síťovou, linkovou a fyzickou z OSI modelu. Hlavní čtyři jsou EtherNet/IP™, CompoNet™, ControlNet™ a DeviceNet™ [4]. Tato práce se zaměřuje na typ EtherNet/IP, jenž je použit na demonstrační výukové stanici. Ten adaptuje protokol CIP na technologii Ethernetu TCP/UDP/IP, který se používá ve většině síťových architektur [5]. EtherNet/IP tedy zvládá koexistovat s ostatními protokoly a lze jej zapojit k běžnému internetu bez speciálních síťových prvků.

1.2.1 Modelování objektů

Každý uzel v síti CIP je tvořen skupinou objektů, které abstraktně reprezentují jeho jednotlivé komponenty a funkce. Cokoliv, co není popsáno takovými objekty, je pro síť CIP neviditelné. Tyto abstraktní objekty jsou pak reprezentovány třídami, instancemi tříd a atributy. Objekty a jejich komponenty jsou pak adresovány pomocí sjednoceného adresního schématu. Příklad adresního schématu objektů je na Obr. 1.1.

Adresa uzlu je přiřazena každému uzlu CIP sítě. V případě, kdy je použita technologie EtherNet/IP, je adresa uzlu přímo IP adresa. Následují identifikátory tříd, instancí a atributů. Tzv. Service Code je číselná hodnota přiřazena přímo k nějaké akci. Ta se využívá u explicitního spojení, kde si komunikující strana může od druhé vyžádat akci na základě jejího Service Code.

CIP objekty se dají rozdělit do tří kategorií – obecné objekty, aplikační objekty a síťové

objekty. Obecné objekty jsou užívány napříč různými zařízeními a jsou jimi například objekty na konfiguraci připojení, či objekty zastupující soubor. Aplikační objekty jsou pro použití voleny uživatelem na základě potřeb jím vyvíjené aplikace. Síťové objekty zahrnují síťové prvky – například objekt Ethernetového spojení, či objekt přepínače.

1.2.2 Komunikační protokol

Komunikace protokolu CIP funguje na principu producent-konzument [2]. To je řízeno pomocí identifikátorů přiřazených k jednotlivým spojením. Producent tedy vytvoří zprávu a odešle ji s předem domluveným identifikátorem spojení – dále jen CID (connection identifier). Ostatní zařízení v síti se pak na základě tohoto identifikátoru rozhodnou, zda mají, či nemají zprávu zkonzumovat. Takový způsob komunikace je mnohem efektivnější, než posílat každému příjemci stejnou zprávu zvlášť jako v modelu zdroj-cíl. Pokud je třeba vytvořit obousměrnou komunikaci, je potřeba CID pro každý směr komunikace (tedy dva). Principem producent-konzument je velmi jednoduše zařízena multicast komunikace (kdy se zpráva zasílá více příjemcům najednou).

1.2.2.1 Navázání spojení

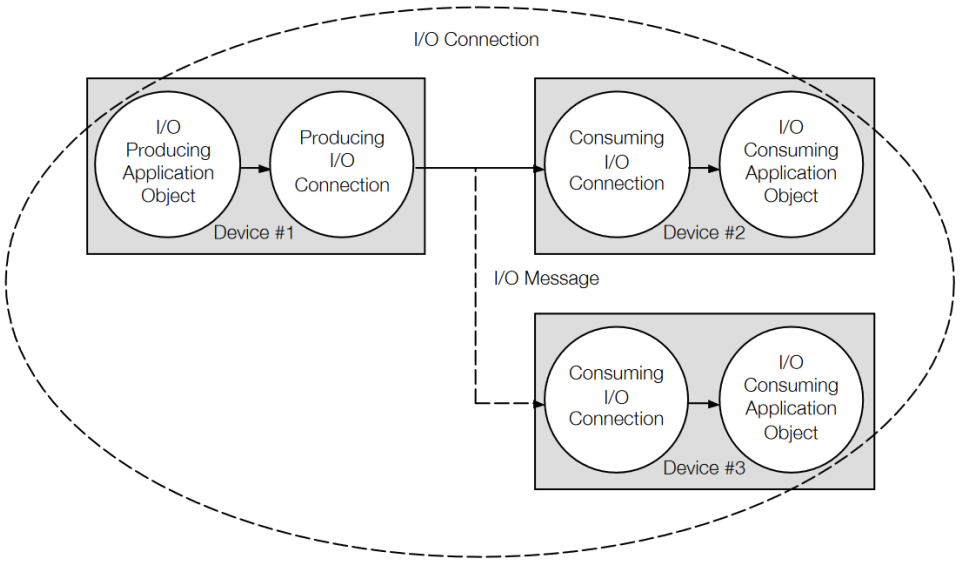
Většina komunikace v CIP sítích probíhá přes tato spojení a proto byl definován proces UCMM (unconnected message manager), který má za úkol vytvořit spojení mezi zatím nepropojenými zařízeními. CIP spojení se vytváří zasláním zprávy s požadavkem na službu `UCMM Forward_Open`. Tuto službu musí poskytovat všechna zařízení v síti CIP využívající technologii EtherNet/IP. Zpráva s požadavkem na vytvoření spojení obsahuje níže popsané informace potřebné k vytvoření spojení.

Obsah zprávy pro vytvoření CIP spojení[2]:

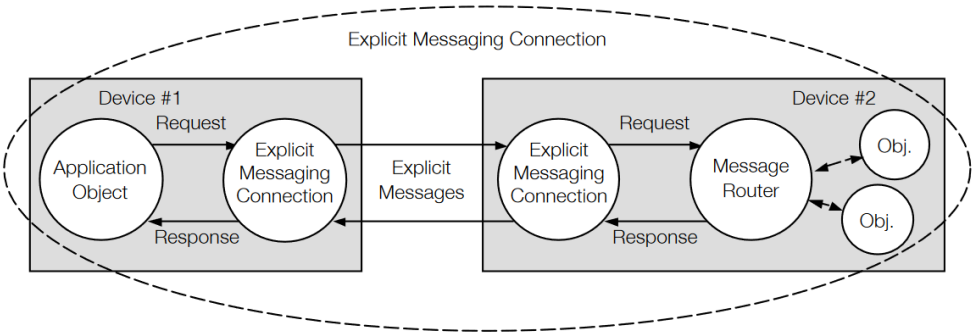
1. Informace o časovém limitu pro spojení.
2. CID pro spojení od odesilatele k cíli.
3. CID pro spojení od cíle k odesilateli.
4. Informace o identitě odesilatele (sériové číslo a ID výrobce).
5. Maximální velikost zprávy v tomto spojení.
6. Jestli je spojení typu multicast nebo unicast.
7. Vyvolávací mechanismy (například cyklický, změna stavu).
8. Volitelně elektronický klíč, aby mohl cílový uzel ověřit, zda je uzel odesilatele správný.
9. Cesta připojení pro data objektu aplikace v uzlu, který bude produkovat a konzumovat.
10. Volitelně segment dat obsahující konfigurační informace pro uzel.
11. A nakonec, také volitelně, směrovací informace pro případ propojení napříč více síťovými technologiemi CIP (například EtherNet/IP a ControlNet).

1.2.2.2 I/O a explicitní spojení v CIP sítích

Veškerá komunikace probíhající v síti CIP se dá rozdělit na dvě kategorie. První je I/O spojení, kde se vytvoří speciální kanály mezi producentem a konzumenty a po těchto kanálech se posílají data specifická pro komunikující aplikace. Také se mu říká implicitní spojení, jelikož význam dat se dá určit pouze z identifikátoru spojení (počítá se s tím, že aplikace konzumující data už ví, o co se jedná). Tímto způsobem se posílají I/O (vstupní a výstupní) data ve formátu vhodném



Obrázek 1.2 Znázornění CIP I/O spojení[2]



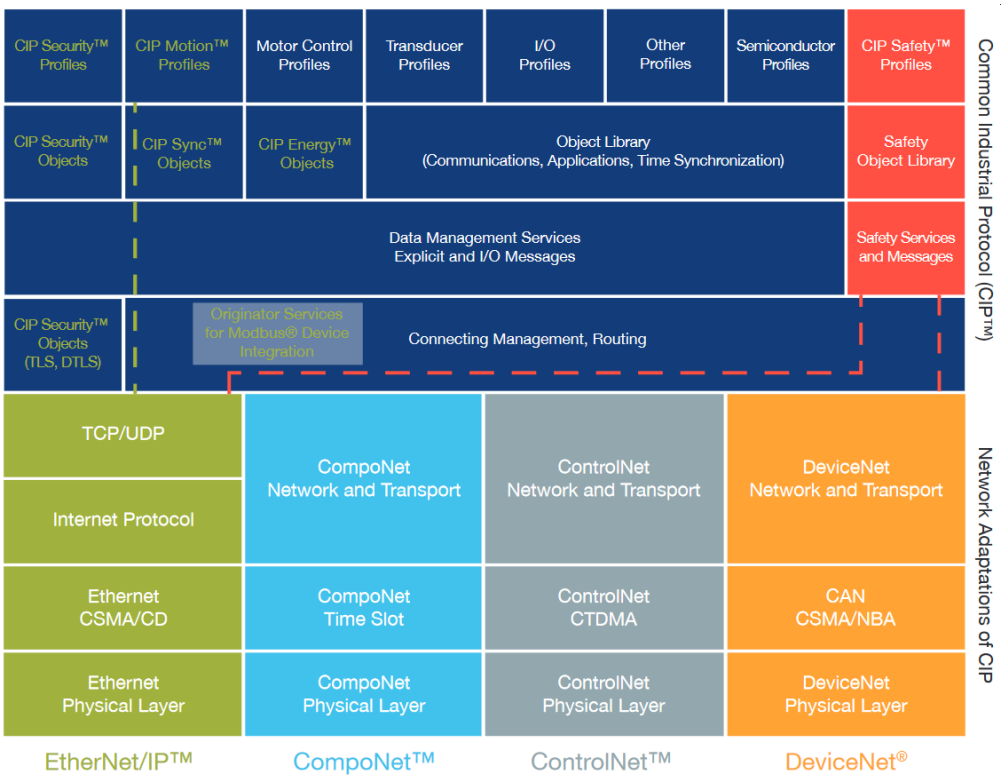
Obrázek 1.3 Znázornění CIP explicitního spojení[2]

pro specifické potřeby. Například pokud se vstupní a výstupní data zasílají cyklicky, je třeba rozlišovat správné pořadí přijmutých paketů. Toho se může docílit čítačem, který se umístí na začátek posílaných dat [2].

Druhá kategorie je explicitní spojení. V tom se vytvoří víceúčelové kanály, které jsou vždy mezi jen dvěma zařízeními. Má komunikaci typu dotaz/odpověď (z anglického request/response). V těchto zprávách se specificky požadují přesně určená data, proto název explicitní spojení. Tyto zprávy obsahují pouze Service Code (popsaný v kapitole Modelování objektů), informace o cestě k požadovanému objektu a případná data [2].

1.2.3 EtherNet/IP™

Technologie EtherNet/IP™, která zastává funkce vrstvy transportní a nižších z OSI modelu, má oproti alternativám tyto výhody. Je možné naráz získávat, konfigurovat a řídit data pomocí pouze jedné sítě či použít jednu síť pro komunikaci více nezávislých CIP sítí. Je kompatibilní se standardními internetovými protokoly (například HTTP, FTP) a standardními průmyslovými



Obrázek 1.4 EtherNet/IP™ jako část CIP OSI modelu[4]

protokoly pro sdílení a výměnu dat (OPC UA). Podporuje fyzické vrstvy standardů IEEE, což poskytuje uživatelům výběr různých rychlostí internetu, či tvořit flexibilní síťové architektury kabelové i bezdrátové s mnoha možnostmi topologií (hvězda, kruh) [4].

Na obrázku číslo 1.4 je znázorněno začlenění technologie EtherNet/IP do OSI modelu a jaké prostředky k tomu využívá. Pro tuto práci je potřebná znalost prostředků použitých pro přenos, proto je v následující části jejich stručný popis [4].

1.2.3.1 Ethernet

Technologie Ethernet v modelu zastává funkce vrstvy fyzické a linkové. Specifikace obou vrstev Ethernetu je vydána ve standardu IEEE 802.3.

Ve fyzické vrstvě jsou data přenášena po datových rámcích, jehož formát je znázorněn v tabulce 1.1. Tento rámec je bit po bitu přenášen mezi komunikačními uzly. Komunikace začíná startovací posloupností, která se používá pro synchronizaci vysílací stanice se všemi přijímacími. Poté následuje cílová adresa a zdrojová adresa a typ které jsou důležité pro vyšší (linkovou) vrstvu Ethernetu. V datovém poli jsou zapouzdřená samotná přenášená data a data potřebná pro správnou funkci vyšších vrstev. Datové pole má minimální délku. Pokud je posíláno méně dat, než je dáno minimální délkou, je datové pole na minimální délku doplněno. Rámec je zakončen kontrolním součtem CRC pro kontrolu správného přenosu. Příjemce si vypočítá vlastní kontrolní součet a pokud se neshoduje s přijatým, je detekována chyba a rámec je vyřazen (bez informování vysílače) [1].

Kvůli požadavku propojitelnosti zařízení od různých výrobců, je každé ethernetové rozhraní opatřeno unikátní MAC (medium access control) adresou. MAC adresa je šest bajtů velká, z nichž první tři bajty jsou kód výrobce a následující tři výrobní číslo samotného rozhraní. V linkové vrstvě se zajišťuje transport dat právě podle MAC adresy. Data v tabulce označená jako typ

Tabulka 1.1 Datový rámec v síti Ethernet

startovací posloupnost	cílová adresa	typ	zdrojová adresa	datové pole	kontrolní součet
8 B	6 B	6 B	2 B	46 až 1500 B	4 B

Tabulka 1.2 Struktura datagramu IPv4[1]

bit:				
0	4	8	16	24
verze	délka hlavičky	typ služby	celková délka	
identifikace			příznaky	číslo fragmentu
životnost		protokol	kontrolní součet hlavičky	
zdrojová adresa IP (4 bajty)				
cílová adresa IP (4 bajty)				
data (maximálně 64 kB)				

obsahuje buď velikost datového pole, nebo takzvaný EtherType, který určuje, jaký protokol je užit v datovém poli. Těchto 16 bitů označuje velikost datového pole, pokud je hodnota menší, než 0x0600 a v opačném případě označují daný EtherType. EtherType byl přidán až do standardu Ethernet II. Ethernet II je plně kompatibilní s předchozím standardem.

Další funkcí linkové vrstvy Ethernetu je kontrola správného přenosu rámce. To zastává metoda CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Při použití této metody zařízení nejprve poslouchají, zda je médium volné, a pokud ano, mohou začít odesílat data. V případě detekce kolize zařízení zastaví odesílání, čekají náhodnou dobu a pokusí se data znovu odeslat.

1.2.3.2 Internet protocol

Síťová vrstva je reprezentována protokolem IP. Ten má více verzí, ale pro tuto práci je zásadní pouze protokol IPv4 s adresovacím prostorem čtyř bajtů. Jeho hlavním účelem je zajistit směrování mezi sítěmi Ethernet. Adresy (tzv. IP adresy) slouží k unikátnímu označení jak sítě, tak koncového zařízení. IP adresy se dělí na veřejné a soukromé. Přidělování veřejných IP adres řídí centrálně úřad IANA (Internet Assigned Numbers Autority). Soukromé IP adresy jsou unikátní pouze v rámci sítě [1].

V tabulce 1.2 je graficky znázorněna datová struktura IPv4. Následuje stručný popis částí, které jsou důležité pro tuto práci.

Identifikace je šestnáctibitová část, kde odesílatel označí každou zprávu unikátním identifikátorem. Identifikátor je užitečný například, pokud bylo zprávu třeba fragmentovat. Každý fragment jedné zprávy pak má stejný identifikátor.

Kontrolní součet hlavičky kontroluje pouze, zda data hlavičky nebyla při přenosu poškozena. Pokud hlavička poškozena byla, je zpráva zahozena.

Zdrojové a cílové adresy IP označují již zmíněné IP adresy odesílatele a příjemce zprávy. Některé IP adresy mají speciální funkce, například pro poslání zprávy na zařízení, ze kterého je odesláno (tzv. loopback). Výčet speciálních IP adres se dá najít ve specifikaci RFC 6890.

Poslední částí jsou přenášená data, v čemž jsou zahrnuty i další protokoly, ve kterých jsou data zapouzdřena.

1.2.3.3 Transmission control protocol

TCP zajišťuje transportní vrstvu OSI modelu. Realizuje spojení pro uživatelské počítačové programy. V komunikaci využívající TCP se klade velký důraz na zabezpečený přenos (tzn. bez

Tabulka 1.3 Datagram UDP[6]

zdrojový port	cílový port	délka	kontrolní součet	datové pole
2 B	2 B	2 B	2 B	

ztráty dat při komunikaci). Bezchybný přenos je kontrolován vysílací stanicí pomocí potvrzovacích zpráv o přijetí zasílaných od příjemce [1]. Díky tomu se dá detekovat, ale i odstranit zasláním ztracené zprávy opakovaně. Tato komunikace má oproti níže popsané alternativě UDP menší ztrátovost dat, ale klade větší zátěž na síť kvůli kontrolním zprávám. V sítích CIP se TCP komunikace používá pro vytváření spojení a konfigurace pro následný přesun na komunikaci pomocí UDP [4].

1.2.3.4 User datagam protocol

UDP je alternativou TCP a také zajišťuje transportní vrstvu OSI modelu. Klade nižší zátěž na síť, ale neposkytuje spolehlivost přenosu, ani kontrolu chyb [6]. Protokol je díky absenci kontroly kratší a přenos rychlejší. Díky rychlejšímu přenosu se používá v situacích, kdy je třeba získávat data cyklicky a v reálném čase [1]. V CIP sítích je využíván přesně v tomto případě při zasílání I/O zpráv.

V tabulce 1.3 je graficky znázorněna struktura UDP paketu. Následuje stručný popis jednotlivých jeho částí.

Zdrojový a cílový port slouží jako přídavná adresace procesů odesilatele a příjemce.

Délka označuje velikost celého paketu v bajtech, tedy hlavičky UDP a velikost dat v části datové pole. Minimální délka je tedy 8 (délka hlavičky UDP). Maximální délka bývá omezena strukturami v nižších vrstvách modelu OSI (IPv4).

Kontrolní součet slouží k odhalení případné chyby při přenosu dat.

Datové pole je část, která nese doručovanou informaci a případně další protokoly vyšších vrstev modelu OSI.

1.2.4 CIP rozšíření

Společnost ODVA vytvořila několik dodatečných rozšíření k CIP na základě potřeb průmyslových sítí. Mezi těmito službami je CIP Motion pro přesné ovládání motorů, úhlu otočení a dalších mechanických zařízení. CIP Sync je užitá u aplikací, které jsou řízeny v reálném čase s důrazem na rychlou responzivitu. CIP Energy slouží pro mapování energetických toků a případnou úsporu energie. CIP Safety, které poskytuje spolehlivou komunikaci mezi bezpečnostními zařízeními (nouzový vypínač). A pro tuto práci nejdůležitější CIP Security jako implementaci kybernetické bezpečnosti do sítí CIP.

1.3 Bezpečnost komunikace v sítích CIP

Dříve byla komunikace v průmyslových systémech využívající EtherNet/IP™ nezabezpečená, jelikož se počítalo s fyzickou izolací systému od okolní sítě i neoprávněného přístupu (takovou bariérou mohly být například zamčené dveře) [7]. Postupem času ale narůstala potřeba mít i digitální přístup do těchto sítí z důvodu šetření nákladů, decentralizace pracoviště, efektivitě práce i sdílení informací. S takovým připojením ale přichází i bezpečností rizika, se kterými tento systém zatím nepočítal.

Proto začala společnost ODVA vyvíjet technologii CIP Security. Zařízení, které tuto technologii podporuje by mělo být schopné kontrolovat integritu dat a odmítat data, která byla neoprávněně změněna. Dále ověřovat autentizaci a odmítat data, která nejsou od důvěryhodného zařízení. A na závěr zamítnout akce, na které nemá autentizované zařízení práva, autorizovat.

Primárním zdrojem pro tuto kapitolu jsou veřejně dostupné dokumenty přímo od společnosti ODVA [7, 8].

1.3.1 CIP Security

Bezpečnostní rozšíření CIP Security je nyní dostupné pouze pro sítě využívající technologii EtherNet/IP.

Pro kvalitní zabezpečení systému a vývoj bezpečnostních opatření je důležité znát bezpečností hrozby, kterým je systém vystaven. K jejich identifikaci se užívají různé metodologie. Při vývoji CIP Security použila pro identifikaci hrozeb v sítích CIP společnost ODVA metodologii modelu STRIDE.

1.3.1.1 STRIDE

STRIDE je metodologie používaná v oblasti kybernetické bezpečnosti pro identifikaci a klasifikaci potenciálních hrozeb v informačních systémech. Jedná se o akronym, který reprezentuje šest hlavních hrozeb, které mohou ohrozit bezpečnost informačních systémů. Tato metoda byla vyvinuta společností Microsoft jako nástroj pro hodnocení bezpečnosti softwaru. Každé písmeno v názvu STRIDE představuje jednu z těchto hrozeb:

Spoofing (podvržení identity) označuje hrozbu, kdy útočník může získat a zneužít identitu někoho (či něčeho) jiného. Jednoduchým příkladem je získání a následné použití cizích přihlašovacích údajů.

Tampering (manipulace) je hrozba, kdy data mohou být neoprávněně upravována nebo měněna. To může zahrnovat manipulaci s daty během komunikace nebo na úložišti.

Repudiation (popírání) představuje akce, kdy je v systému, který nevede záznamy o provedených operacích použita zakázaná operace.

Information disclosure (odhalení informací) představuje hrozbu nechtěného úniku informací – ať už přečtení souboru, ke kterému by útočník neměl mít přístup či odposlouchávání nezabezpečené síťové komunikace.

Denial of Service (odepření služby) je zranitelnost, kdy útočník může odepřít přístup ke službě validním uživatelům.

Elevation of privilege (zvýšení oprávnění) zastupuje možnost, že útočník může získat vyšší oprávnění, než mu byla původně přidělena [9].

1.3.1.2 Kybernetické hrozby v sítích CIP

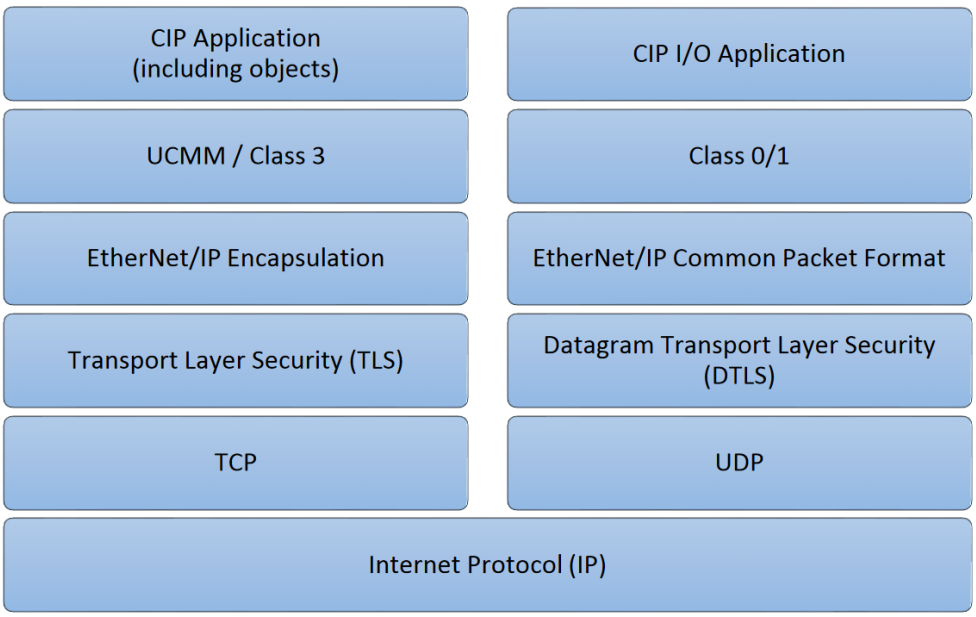
Podle hrozeb modelu STRIDE byly identifikovány hrozby týkající se zařízení používajících CIP. V následující části je stručný popis hrozeb, které společnost ODVA odhalila u sítí CIP mapována na model STRIDE. Tyto informace jsou získány přímo z dokumentu společnosti ODVA[7].

Typy útoků odpovídající sekci spoofing (podvržení identity) jsou neautorizovaná spojení (unauthorized session). Zde je útočník schopen vytvořit spojení s cílovým zařízením a zasílat mu uměle vytvořené CIP pakety. Ukradení spojení (session hijacking), kde útočník napadne již existující spojení. Znovupoužití zpráv (message replay), což znamená, že útočník odposlechne komunikaci a získá nezávadné pakety. Ty později a v jiném kontextu odešle znovu pro vyvolání závadné akce. Poslední je útok typu rogue server, kdy je útočník schopen podvrhnout identitu platného serveru a přijímat zprávy od nevědomého klienta.

V sekci tampering (manipulace) byla identifikována hrozba úpravy zpráv. Útočník je schopen pozastavit a upravit či zahodit data v MITM (man in the middle) útoku.

Hrozba repudiation (popírání) je změna záznamů. Útočník je schopen měnit staré záznamy a mazat je. Validní uživatel později nemá prostředky pro vystopování útočníka.

Útok využívající information disclosure (odhalení informací) je odposlouchávání komunikace CIP mezi komunikujícími stranami. Útočník je schopen číst a porozumět obsahu těchto zpráv.



Obrázek 1.5 Vrstvení protokolů technologie EtherNet/IP a CIP s rozšířením CIP Security (TLS a DTLS)[8]

Mezi útoky typu Denial of Service (odepření služby) se řadí již zmíněné útoky neautorizované spojení, ukradení spojení, úprava zpráv a znovupoužití zpráv.

Poslední typ útoku je Elevation of privilege (zvýšení oprávnění). Zde je zásadní problém v celkové absenci autorizace a autentizace. Kdokoliv kdo se tedy připojí, má již plná práva.

1.3.1.3 Bezpečnostní opatření CIP Security proti uvedeným hrozbám

Cílem CIP Security je umožnit zařízení připojenému k síti CIP, aby se samo bránilo před škodlivou CIP komunikací. Plně samoobranné zařízení CIP by mělo být schopno odmítnout data, která byla narušena (zajištění integrity), odmítnout zprávy odeslané nedůvěryhodnými subjekty nebo zařízeními (zajištění autenticity) a odmítnout zprávy, které požadují akce, které nejsou povoleny (zajištění autorizace).

CIP Security zabezpečuje CIP komunikaci pomocí často používaného standardu TLS (transport layer security). Koncept je stejný jako u zabezpečení HTTP (hypertext transfer protocol) pomocí TLS ze kterého vzniklo známé HTTPS. Vrstvení protokolů je zobrazeno na Obr. 1.5

Standardy protokolů IETF TLS (RFC 5246) a DTLS (RFC 6347) pro zabezpečení komunikace EtherNet/IP poskytuje CIP Security následující tři vlastnosti [10].

Identitu zařízení a autentizaci. Výměnou certifikátů či pomocí předem získaného tajného klíče si mohou zařízení dokazovat pravost své identity. Na základě identity se pak zařízení mohou rozhodnout, zda povolit, či nepovolit komunikaci.

Integrita dat a autentizace. Schopnost ověřit, zda data nebyla při přenosu pozměněna, či podvržena pomocí TLS HMAC.

Důvěrnost dat. Ta je dosáhnuta pomocí šifrování, které zabraňuje neoprávněným zařízením číst důvěrná data.

Tabulka 1.4 Šifrové sady podporované CIP Security[8]

Šifrové sady:
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_NULL_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_PSK_WITH_NULL_SHA256
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256

1.3.1.4 TLS 1.2 a DTLS 1.2 v CIP Security

Transport layer security (TLS) je kryptografický protokol navržený k poskytnutí bezpečné a šifrované komunikace na internetu. Předchůdcem TLS byl Secure Sockets Layer (SSL), ale kvůli několika bezpečnostním zranitelnostem byla vyvinuta nová verze, tj. TLS. Jedná se o protokol pracující na transportní vrstvě síťové architektury, což znamená, že jeho hlavním cílem je zajištění bezpečnosti komunikace mezi dvěma koncovými body.

Pro zajištění bezpečnosti komunikace poskytuje protokol TLS mnoho možností tzv. šifrových sad. Šifrové sady oznamují specifické principy, pomocí kterých je řízena výměna klíčů, šifrování zpráv a kontrolována integrita zpráv. Samotná bezpečnost komunikace je závislá na použité šifrové sadě. Seznam podporovaných šifrových sad v protokolu TLS verze 1.2 je v specifikaci RFC 5246[11]. CIP Security nepodporuje celý tento rozsáhlý list, ale pouze 8 vybraných šifrových sad (jejich seznam je v tabulce 1.4). Ty jsou vybrány na základě těchto požadavků. Možnost využití předem dohodnutého klíče, nebo X.509 certifikátů. Možnost použití asymetrického šifrování RSA i eliptických křivek pro výměnu klíčů. A možnosti zabezpečit komunikaci jak šifrováním dat včetně kontroly integrity dat, tak i umožnit posílat data nešifrovaná a kontrolovat pouze integritu. Výběr menšího počtu podporovaných šifrových sad byl proveden především, aby nebyla kladena nadměrná zátěž na implementace CIP Security a byla zajištěna interoperabilita mezi EtherNet/IP zařízeními [8].

V CIP Security je TLS používáno pro zabezpečení explicitního spojení, tedy pro komunikaci využívající především protokol TCP. Pro I/O CIP spojení využívající protokol UDP je třeba použít jiný bezpečnostní protokol a to datagram transport layer security verze 1.2 (DTLS). Ten je založen na protokolu TLS a poskytuje ekvivalentní bezpečnostní záruky [12]. DTLS 1.2 je detailně popsán ve specifikaci RFC 6347.

Komunikace TLS a DTLS se dá rozdělit na dvě hlavní části – na tzv. handshake (pozdrav) a následnou výměnu samotných šifrovaných dat.

V části handshake se obě strany dohodnou na použití konkrétní šifrové sady, provedou výměnu klíčů a autentizují se pomocí certifikátu, nebo předem sdíleného klíče.

V druhé části, na základě šifrové sady a společného klíče domluveného ve fázi handshake, zahájí šifrovanou komunikaci.

1.3.2 Metody autentizace v CIP Security

CIP Security nabízí podporu dvěma různými způsoby. V následující části jsou popsány jejich zásadní rysy a rozdíly. Je třeba uvést, že principy zde popisuji velmi zjednodušeně pro základní uvedení do problematiky, jelikož detailní principy nejsou pro tuto práci nutné.

1.3.2.1 Předem sdílený klíč

Mezi zařízení je zpočátku třeba distribuovat tajný společný klíč. To se nedoporučuje provádět po nezabezpečeném komunikačním kanále a přenos s sebou přináší riziko odposlechu společného klíče. Šifrové sady, které jsou podporovány CIP Security, nabízí použití předem sdíleného klíče pouze v kombinaci s Diffie-Hellmanovým schématem a kryptografii na základě eliptických křivek. Komunikující strany nejprve provedou výměnu veřejných klíčů a poté na základě veřejných klíčů a předem sdíleného klíče obě strany vypočítají společný tajný klíč. Ten pro správnou komunikaci musí být stejný pro obě strany, jelikož protokol TLS po navázání komunikace využívá symetrické šifry. Tím je tedy dosáhnuto samotné autentizace, jelikož pokud jedna strana nemá správný předem sdílený klíč, dostane pak nesprávný společný tajný klíč použitý pro šifrování dat a komunikace neproběhne.

Protokol TLS podporuje i variantu, kde je komunikace symetrické šifry založena okamžitě na předem sdíleném klíči. To je ovšem z hlediska bezpečnosti horší varianta, jelikož kód pro symetrickou šifru je napříč veškerou komunikací stále stejný. Kdyby došlo k prolomení šifry a útočník by získal předem sdílený klíč, měl by pak přístup k veškeré proběhlé komunikaci. Ve variantě s Diffie-Hellmanovým schématem je pro každé nové spojení vytvořen unikátní klíč. Když dojde k prolomení tohoto klíče, útočník má přístup pouze k této komunikaci a stále není schopen dešifrovat komunikaci dříve probíhající.

Autentizace pomocí předem sdíleného klíče obecně s sebou nese velké riziko ve zvolení slabého sdíleného klíče. Pokud je sdílený klíč generován na základě hesla od uživatele, přináší tato metoda riziko zranitelnosti proti slovníkovým útokům a dalším způsobům uhádnutí hesla. Proto se doporučuje heslo vytvářet pomocí náhodných generátorů.

1.3.2.2 Certifikát

Digitální certifikát je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč. Formát, ve kterém se v CIP Security certifikát uchovává je X.509, kde jsou k veřejnému klíči přidány další informace, což jsou například informace o tvůrci digitálního podpisu (certifikační autoritě), platnost certifikátu, algoritmus pro elektronický podpis a jiné. Budování důvěry mezi zařízeními zde obstarává certifikační autorita. Ta podepisuje důvěryhodným klientům jejich certifikáty pomocí svého soukromého klíče. Klienti pak na základě důvěry certifikační autoritě důvěřují i ostatním klientům, kteří poskytují svůj certifikát podepsaný od certifikační autority. Pravost podpisu se ověřuje veřejným klíčem certifikační autority.

Proces výměny certifikátů klade nepatrně vyšší nároky na rychlost navázání komunikace a použitý hardware. Při zabezpečování industriální sítě CIP se ale doporučuje použít autentizaci pomocí certifikátů. Certifikáty dovolují vytvořit složitější schéma bezpečnostních modelů a používá se u nich delší klíč, než v případě předem sdíleného klíče [10]. Delší klíč je pak obtížněji prolomitelný útokem hrubou silou (z anglického brute-force attack) založeném na postupném zkoušení možných hodnot klíčů.

1.3.3 Metody šifrování v CIP Security

CIP Security nabízí, nepočítaje také nabízenou variantu bez šifrování, pouze jeden způsob šifrování. Tím je často používaná symetrická šifra AES (Advanced Encryption Standard). Advanced encryption standard podporuje tři velikosti klíčů – 128 bitů, 192 bitů a 256 bitů. CIP Security ale podporuje pouze verzi 128 a 256. Data jsou šifrována po 128 bitových blocích. Pro šifrování více bloků dat je v CIP Security použita metoda CBC (Cipher Block Chaining). Pro šifrování to pak (zjednodušeně) znamená, že bloky otevřeného textu jsou xorovány s předchozím šifrovaným blokem před zašifrováním. Ve výsledku každý blok závisí na všech předchozích blocích, což zajišťuje ještě obtížnější prolamování šifry.

1.3.4 Integrita dat v CIP Security

Ověření, že data nebyla po cestě komunikačním kanálem upravena (ověření integrity dat), je zajištěno pomocí metody HMAC (Keyed-Hash Message Authentication Code) definováné ve standardu FIPS-PUB-198. V následující části je metoda HMAC zjednodušeně popsána.

Tato metoda ověřování je založena na hašovací funkci. Hašovací funkce vytvoří ze vstupu řetězec fixní délky. Tento řetězec se pak nazývá haš daného vstupu. Hašovací funkce generuje pro stejný vstup vždy stejný výstupní řetězec. Z výstupního řetězce je u hašovací funkce výpočetně neschůdné odvodit vstupní řetězec.

V metodě HMAC je ke každé přenášené zprávě přidán i haš zprávy a sdíleného tajného klíče. Příjemce zprávy pak může vytvořit vlastní haš (z příchozí zprávy a sdíleného klíče) a porovnat ho s hašem, který byl připojen k přenášené zprávě. Pokud haše nejsou stejné, došlo k narušení integrity dat.

V CIP Security jsou jako hašovací funkce používány SHA-1 , SHA256 a SHA384. U posledních dvou je číslo označení velikosti výstupního řetězce (v bitech) dané hašovací funkce, první vytváří řetězec o velikosti 160 bitů.

1.4 Zařízení Rockwell Automation a CIP Security

Výrobce Rockwell Automation se pro kybernetické zabezpečení svých zařízení rozhodl využít standard CIP Security spolu s mezinárodním standardem ISA/IEC 62443, což je standard určující požadavky a procesy pro implementování a udržování kyberneticky bezpečné industriální automatizace a kontrolních systémů [10, 13]. Konkrétně se zaměřují na sekce ISA/IEC 62443-3-2 a 3-3 popisující požadavky na systémové úrovni.

Architektura kybernetické bezpečnosti zařízení Rockwell Automation s CIP Security je založena na logické segmentaci odpovídající modelu zón a spojů (z anglického zones and conduits) dle ISA/IEC 62443-3-2. Ta je založena na rozdělení zařízení do skupin, s podobnou funkcí a stejnými bezpečnostními požadavky a následném budování důvěry pouze v menších skupinách. Pro tyto skupiny se vytváří zóny s odpovídající konfigurací kybernetické bezpečnosti. Spoje pak slouží pro komunikaci mezi zónami.

Sekce ISA/IEC 62443-3-3 je pak věnována systémovým požadavkům kybernetické bezpečnosti. Je založena na sedmi základních požadavcích, mezi nimiž je například požadavek kontroly identifikace a autentizace, požadavek důvěrnosti dat a jiné [10].

1.5 Související práce

Podobné úloze, kterou řeší tato práce, se věnuje diplomová práce, kterou napsal Bc. Milan Šindelek na téma CIP Safety [14]. V této práci se zaměřuje na bezpečnostní opatření proti poškození strojů či ublížení na zdraví uživatelů průmyslových sítí. Mé práci, která je věnována také bezpečnosti, ale kybernetické, je tedy podobná jen společným zaměřením na průmyslové systémy a protokol CIP.

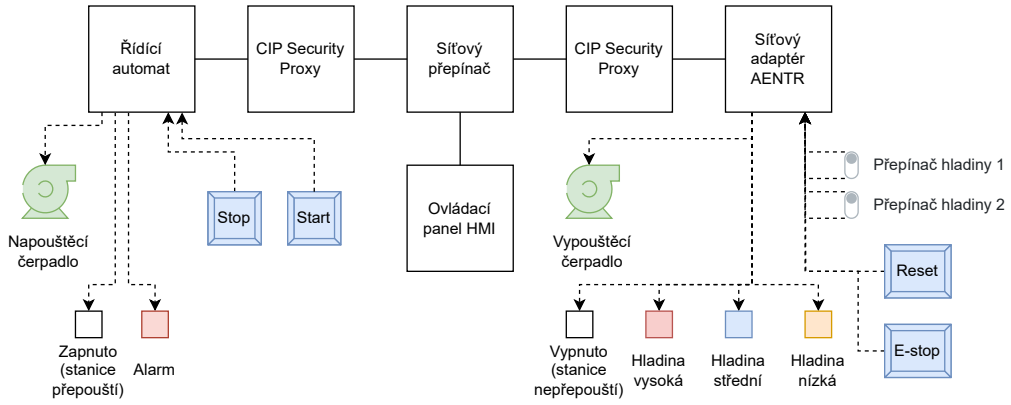
Primárním zdrojem informací pro tuto práci jsou dokumenty přímo od společností ODVA a Rockwell Automation. Společnost ODVA se věnuje popisu principů komunikace CIP a bezpečnostních praktik použitých v CIP Security [2, 4, 7, 8]. Rockwell Automation zase poskytuje manuály pro zavedení a zabezpečení komunikace CIP na jejich zařízeních [15, 16, 17].

Kapitola 2
Praktická část

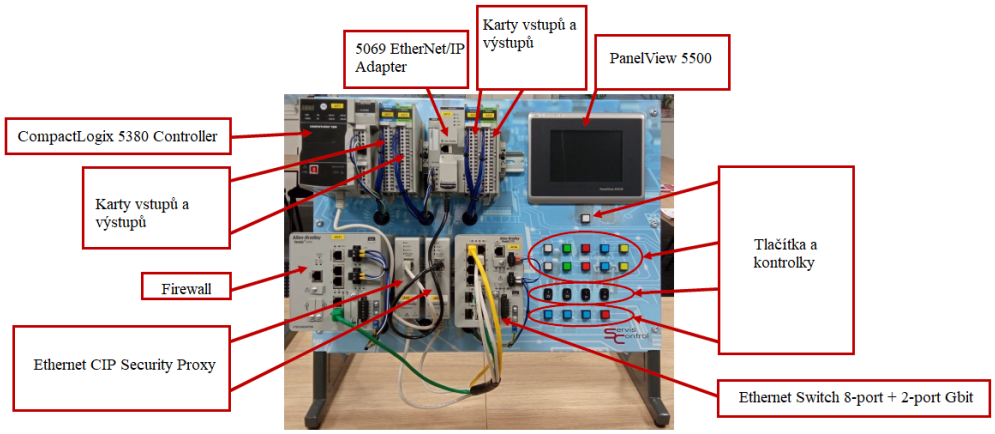
2.1 Popis výukové stanice DS1

V této práci se pro demonstraci útoků a následného zabezpečení používá výuková stanice DS1 pro testování kybernetické bezpečnosti sestavena společností ServisControl s.r.o. Obsahuje zařízení značky Allen-Bradley. Doprovodná fotografie z manuálu této stanice s popisky zařízení stanice je přiložena jako Obr. 2.2. Pro tuto práci je nejdůležitější programovatelný řídící automat (PLC) „CompactLogix 5380 Controller“ a síťový adaptér (AENTR) „5069 EtherNet/IP Adapter“. K těmto zařízením jsou připojeny rozšiřující moduly – karty vstupů a výstupů. Dále jsou na stanici síťové prvky – Ethernetový přepínač „Ethernet Switch 8-port + 2-port Gbit“, přes který mezi sebou jednotlivá zařízení komunikují a firewall, který v této práci není využit. Další důležitý prvek jsou dva bezpečnostní moduly „Ethernet CIP Security Proxy“ (CSP) pomocí kterých síť v další části práce zabezpečím. Z nich jeden je připojen mezi přepínačem a programovatelným řídícím automatem a druhý mezi přepínačem a síťovým adaptérem. Dále obsahuje sadu tlačítek a kontrolek, ke kterým jsou připojeny vstupy a výstupy síťového adaptéru a řídícího automatu. Obsahuje také modul displeje (HMI), který je také připojen k přepínači a jeho prostřednictvím komunikuje s ostatními zařízeními [18]. Na Obr. 2.1 je znázorněno síťové propojení jednotlivých zařízení a jejich periferie.

Na stanici je připravena aplikace zařízení, které ovládá napouštění a vypouštění nádrže. Samotná nádrž a zařízení, která ji monitorují, či ovládají jsou simulovaná pomocí přepínačů a tlačítek.



Obrázek 2.1 Model výchozího zapojení výukové stanice DS1[19]



Obrázek 2.2 Výuková stanice DS1[19]

2.1.1 Programovatelný řídící automat

Hlavní funkční částí celé desky je programovatelný řídící automat CompactLogix 5380 Controller. Na tom je nahrána samotná aplikace na řízení chodu simulované přepouštěcí stanice a jsou zde vykonávány všechny logické operace pro její chod potřebné. K automatu jsou připojeny karty digitálních vstupů a výstupů. Skrze tyto karty je automat připojen k periferiím – tlačítkům, přepínačům a světelným kontrolkám.

Jmenovitě je skrz kartu digitálních výstupů automat připojen ke světelným kontrolkám označujícím, zda je zapnuto přepouštění stanice (bílá), zda se přepouštěcí nádrž napouští, což simuluje propojení s napouštěcím čerpadlem (zelená) a alarmové kontrolce (červená). Karta vstupů je připojena k tlačítkům stop, kterým se vypne čerpadlo i výpust přepouštěcí stanice, dokud se nespustí tlačítkem start (které stanici opět rozběhne). Dále ke dvěma přepínačům, pomocí kterých se pouze mění pozadí modulu displeje. Karty vstupů a periferie jsou propojeny pomocí proudových drátů (na modelu 2.1 čárkované spojení). Samotnou informaci získává karta vstupů na základě toho, zda drátem protéká či neprotéká proud. V případě výstupů zase karta samotná pouští do drátů proud, když je třeba. Karty vstupů i výstupů mají vedle konektorů pro proudové dráty užitečné světelné indikátory aktivity daného vstupu či výstupu.

V úvodní konfiguraci výukové stanice má PLC verzi firmware 32.014 a proto nepodporuje rozšíření CIP Security. CompactLogix 5380 Controller podporuje CIP Security až od verze 34.011. Bezpečnostní moduly CSP se pro zaštítění PLC také nedají použít (více v části o zabezpečení výukové stanice). Proto bylo pro zabezpečení komunikace mezi řídícím automatem a síťovým adaptérem AENTR třeba nahrát novou verzi firmware (35.011).

2.1.2 Síťový adaptér

Síťový adaptér 5069 EtherNet/IP Adapter v praxi slouží pro řízení skupiny zařízení, které jsou příliš daleko od samotného řídícího automatu na to, aby se pro každý vstup a výstup přivedl jednotlivý kabel. Mnoho kabelů zde nahrazuje pouze jeden kroucené dvojlinky. Na této konkrétní stanici by bylo použití síťového modulu v praktickém použití zbytečné, jelikož zařízení, která ovládají jsou všechna blízko řídícímu automatu. Tato stanice ale slouží k testování bezpečnosti, a připojení vzdálených zařízení pomocí síťového adaptéru tedy simuluje.

K adaptéru jsou také připojeny karty vstupů a výstupů. Karta výstupů je připojena k těmto periferiím (schéma na Obr. 2.1). Světelná kontrolka, zda je aplikace pozastavena (bílá), zda běží vypouštěcí čerpadlo (které kontrolka zastupuje)(zelená) a třem kontrolkám popisujících stav vody v nádrži – vysoká, střední a nízká (červená, modrá a žlutá). Vstupní periferie jsou dva přepínače,

které simulují hladinový senzor v přepouštěcí stanici a tlačítka reset (modré) a e-stop (červené), kde první slouží pro vynulování chyby zastavující chod aplikace a druhé pro nouzové zastavení čerpadel.

Toto zařízení také nepodporuje rozšíření CIP Security. Pro zabezpečení jeho komunikace s řídícím automatem je třeba použít modul CSP.

2.1.3 Bezpečnostní moduly

Bezpečnostní moduly Ethernet CIP Security Proxy jsou zařízení, která slouží k zabezpečení komunikace probíhající po síti. K bezpečné komunikaci v CIP síti je třeba použít rozšíření CIP Security. Bohužel ne každé zařízení toto rozšíření podporuje a proto bylo vytvořeno CIP Security Proxy (dále jen CSP). To je schopné zaštítit zranitelné zařízení nepodporující CIP security a samo pomocí CIP security komunikaci zabezpečit. Je to samostatně funkční zařízení a připojuje se mezi chráněné zařízení a nedůvěryhodnou síť. Toto řešení má nedostatek v tom, že komunikace mezi zabezpečovaným zařízením a CSP zůstává nezabezpečená. Jeho výchozí nastavení je značně benevolentní a jednoduše propouští všechnu komunikaci. Toto chování se změní až po přidání zařízení do bezpečnostního modelu a jeho konfiguraci [16].

2.1.4 Modul displeje

Modul displeje je grafický terminál, který slouží pro zobrazování, ale i správu průmyslových zařízení. Obsahuje dotykový displej a do sítě je připojen ethernetovým kabelem přes přepínač. V tomto případě je pro bezpečnost komunikace toto zařízení problematické, jelikož nepodporuje CIP Security[15], ani není možné ho zabezpečit pomocí CSP[16].

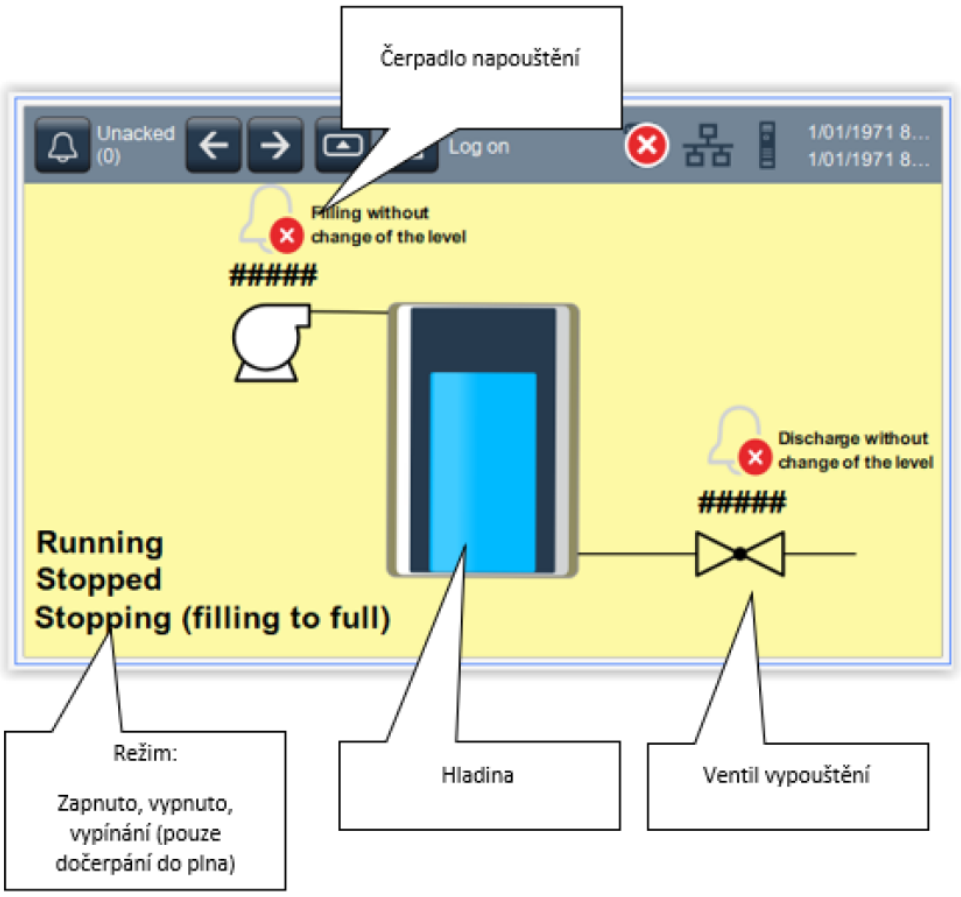
2.1.5 Aplikace běžící na stanici DS1

Tato aplikace řídí simulovanou přepouštěcí stanici. Celé simulované prostředí je názorně zobrazeno na modulu displaye HMI (Obr. 2.3). Zde je vidět přepouštěcí nádrž, čerpadlo čerpající tekutinu do nádrže a ventil vypouštění. Aplikace ovládá pouze dvě zařízení – napouštěcí čerpadlo a ventil vypouštění. Pro správné řízení také potřebuje informaci ze snímače hladiny v nádrži. Pokud je zařízení plněno a po 60 sekund se nemění hladina, nastane chyba, čerpadla se zastaví a začne blikat kontrolka alarm. Alarm se obdobně spustí i při neměnné hladině u vypouštění. Nastalá chyba je znázorněna i na displeji (například hlášení „Filling without change of level“).

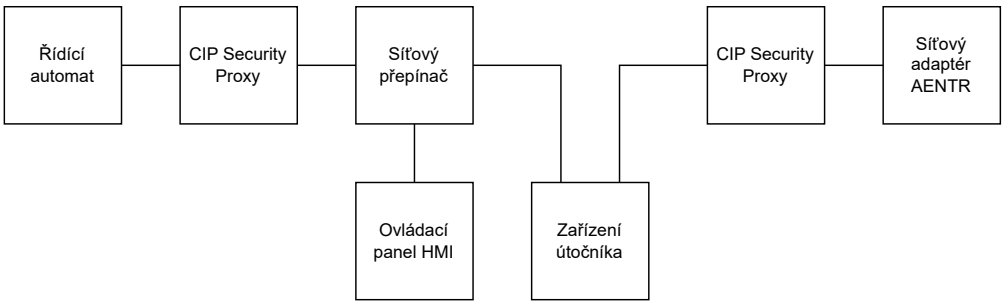
2.2 Útoky na stanici DS1

Samotné demonstrační útoky mířím na komunikaci mezi řídícím automatem PLC a síťovým adaptérem AENTR. Tato zařízení jsou propojena na linkové vrstvě přes přepínač. Útočník se k síti připojí jako tzv. Man-in-the-middle a to přímo na síťový kabel kroucené dvojlinky, po kterém probíhá komunikace mezi napadenými zařízeními. V tomto případě je zařízení útočníka připojeno mezi přepínač a síťový adaptér AENTR. Útočník se ale může připojit v kterékoliv části komunikace. Toto místo bylo zvoleno, jelikož síťový adaptér AENTR slouží k získání vzdálených vstupů a výstupů. Z toho se dá předpokládat, že v praxi je k propojení síťového adaptéru a PLC použit složitější síťový model sloužící i pro jiné účely, než propojení průmyslových zařízení spravujících chod přehrady. Důvod, proč používat sdílený komunikační kanál může být úspora financí či rychlejší uvedení do provozu. Uvažovaný útočník pak zneužívá přístupu ke sdílenému kanálu.

Moduly CSP jsou zapojeny již při útocích, ale stále jsou ve výchozím (továrním) nastavení. To dle manuálu znamená, že propouští veškerou komunikaci. Proto nejsou moduly CSP pro útok důležité a můžeme uvažovat zapojení bez nich.



Obrázek 2.3 Aplikace běžící na HMI displeji[19]



Obrázek 2.4 Schéma ukazující zapojení zařízení útočníka do sítě průmyslových zařízení

Jako útočné zařízení je použit notebook s operačním systémem Windows 10 a jedním síťovým adaptérem. Jelikož jsou pro tento typ útoku potřeba dva síťové adaptéry, bylo třeba použít externí síťovou kartu připojenou pomocí USB. Kvůli podobnosti pojmů síťový adaptér jako rozhraní počítače pro komunikaci se sítí a síťový adaptér jako název průmyslového zařízení pro vzdálené připojení vstupů a výstupů k řídícímu automatu, budu v práci dále označovat síťový adaptér 5069 EtherNet/IP Adapter vždy s doplněním AENTR (síťový adaptér AENTR).

2.2.1 Software použitý k útokům

K realizaci útoků jsem použil tyto aplikace, nástroje a knihovny.

2.2.1.1 Wireshark

Wireshark je open-source nástroj pro analýzu síťového provozu a protokolů. Jeho hlavním účelem je zachytávat a zobrazovat pakety, které putují po síti, což umožňuje uživatelům podrobně analyzovat komunikaci mezi různými počítači a zařízeními v sítích. Wireshark umožňuje uživatelům zachytávat pakety v reálném čase nebo načítat data ze souborů, což je užitečné pro pozdější analýzu. Wireshark poskytuje podporu protokolu CIP. Není ale schopen detailně rozebrat všechna data paketů CIP – například CIP I/O komunikaci, která hraje zásadní roli v úniku dat.

2.2.1.2 Npcap

Npcap je knihovna pro zachycování síťové komunikace na operačním systému Windows. Npcap poskytuje implementaci API na zachytávání síťového provozu (pcap). Pomocí této API je Wireshark schopen zachycovat komunikaci na operačním systému Windows [20].

2.2.1.3 Python

Jako základní programovací jazyk pro psaní útočných programů jsem zvolil Python. Jazyk Python je díky jeho lehké čitelnosti ideální pro vytváření názorných kódů na útok a díky jeho flexibilitě a podpoře mnoha knihoven umožňuje rychlý vývoj útočných programů. Jeho slabší stránky, jako je menší rychlost interpretovaných jazyků oproti kompilovaným, zásadně neovlivnily průběh útoku a výkon bohatě stačil.

2.2.1.4 ScaPy

Scapy je Python knihovna a nástroj pro manipulaci s pakety v počítačových sítích. Tato knihovna umožňuje vytvářet, odesílat a analyzovat síťové pakety na různých vrstvách síťového modelu. Scapy bylo navrženo tak, aby bylo schopné pracovat s různými protokoly a poskytovalo uživatelům širokou škálu funkcí pro manipulaci s datovými toky v síti.

Uživatelé zde mohou vytvářet vlastní síťové pakety na různých vrstvách modelu OSI a odesílat je na cílovou adresu. Také umožňuje provádět analýzu příchozích paketů. Pro tuto práci nabízí podporu různých síťových protokolů včetně IPv4, TCP, UDP. ScaPy ale nenabízí podporu pro protokoly CIP.

Knihovna ScaPy vyžaduje při její instalaci na systému Windows mít nainstalovanou i knihovnu Npcap. Využívá ji pro zachycování i odesílání paketů na síť.

2.2.2 Odposlech komunikace

Společnost ODVA, která nyní vyvíjí protokol CIP, neposkytuje podrobný popis této komunikace široké veřejnosti (jejich specifikace [3, 4] poskytují jen obecné informace). Proto je mým prvním krokem v útoku analýza probíhající komunikace pomocí programu Wireshark.

V tomto případě stačilo vytvořit síťový most mezi adaptéry přímo v nastavení systému Windows. Síťový most přeposílá pakety z jednoho adaptéru na druhý.

Na Obr. 2.5 je zobrazen záznam začátku komunikace mezi řídícím automatem a síťovým adaptérem. Nejprve se pomocí protokolu TCP navazuje spojení a posílají se konfigurační informace pro navázání obousměrného I/O spojení. Zprávy nejsou nijak šifrovány ani zabezpečeny. Zde se dozvídáme CID pro oba směry komunikace, výrobce zařízení, sériové číslo zařízení a další.

Hladina vody může mít v simulaci čtyři hodnoty, a to nádrž je prázdná, nádrž je plná a dvě střední naplnění nádrže. To se na stanici DS1 nastavuje pomocí dvou přepínačů.

Zajímavější informace ale získáme až ze samotné I/O komunikace. Po té se přenáší informace týkající se chodu přepouštěcí stanice. Síťový adaptér AENTR posílá řídícímu automatu informace o stavu hladiny vody a řídící automat zase posílá síťovému adaptéru AENTR pokyny, jaký výstup má zapnout či vypnout – mezi nimi nejdůležitější ventil vypouštění. Na Obr. 2.6 je zobrazen paket, který zaslal síťový adaptér AENTR řídícímu automatu. V tuto chvíli mezi oběma stanicemi neprobíhá žádná jiná komunikace než tato I/O komunikace dokonce i při změně stavu přepouštěcí stanice. Tento paket tedy musí nést informaci minimálně o aktuálních stavech vstupů síťového adaptéru AENTR, tedy například o stavu hladiny. Komunikace CIP I/O je implicitní – s daty se neposílá jejich přímý popis.

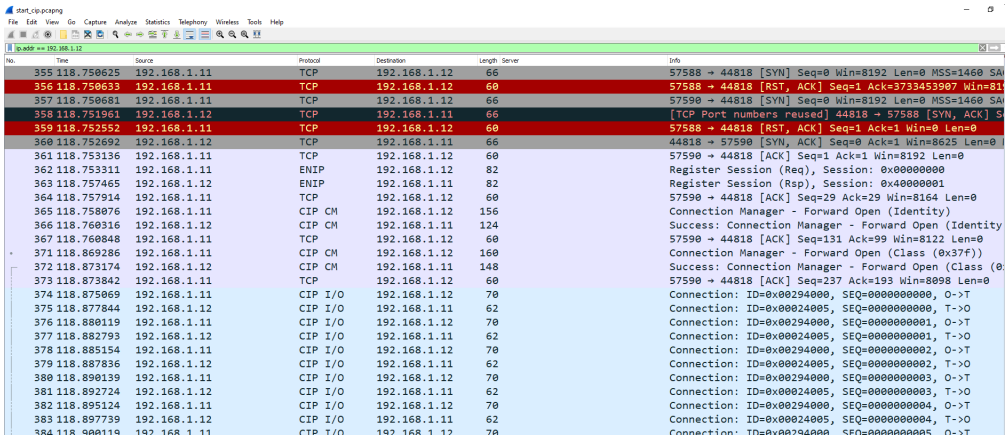
Já jsem měl oproti uvažovanému útočníkovi tu výhodu, že jsem mohl ovládat stav hladiny a sledovat, jak se změna projeví na samotném paketu komunikace. Na paketu je již na první pohled podezřelá část skládající se pouze z bajtů nul a jedniček. Ty mohou představovat binární hodnoty vstupů a výstupů. Po provedeném pozorování bylo téměř jisté, že bajty představují hodnoty vstupů a výstupů a byl jsem schopen přiřadit jednotlivé pozice těchto bajtů k jednotlivým vstupům a výstupům. K tomu mi pomohly i světelné kontrolky znázorňující, zda je daný vstup, či výstup zrovna aktivní. Z toho jsem také zjistil, že síťový adaptér posílá nejen informace ohledně vstupů, ale i výstupů. Vše je znázorněno na Obr. 2.7.

Jeden způsob odposlechu je tedy pozorovat tyto pakety přímo pomocí programu Wireshark. To je ale nepraktické a proto jsem vytvořil program, který z paketů vybírá pouze bajty vstupů a výstupů. Program `scan_io.py`, dostupný v externí příloze této práce, poskytuje konzolové výpisy vstupů a výstupů získaných z odposlechnutých paketů v reálném čase. Pro vytvoření programu jsem použil programovací jazyk Python s knihovnou ScaPy. Zásadní roli hrála funkce sniff ze ScaPy knihovny, která je schopna odposlouchávat pakety z daných síťových adaptérů a poskytnout je programu k dalšímu zpracování.

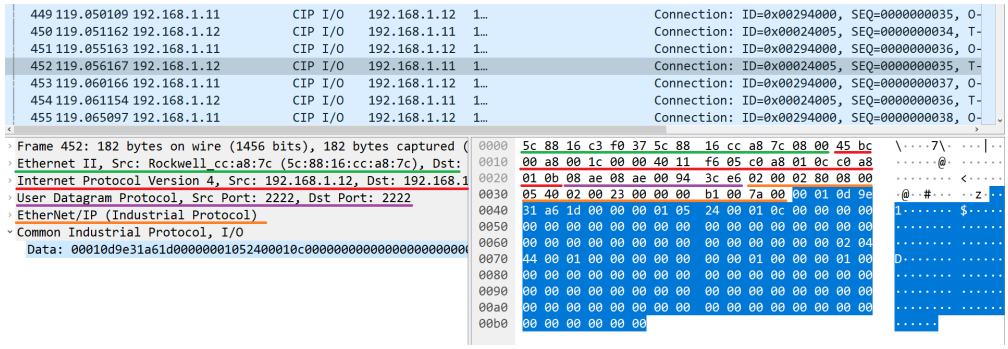
Při prozkoumání paketů odeslaných z řídícího automatu je formát obdobný. Hlavní rozdíl je v tom, že automat posílá pouze informace potřebné pro ovládání výstupů síťového adaptéru.

2.2.3 MITM útok

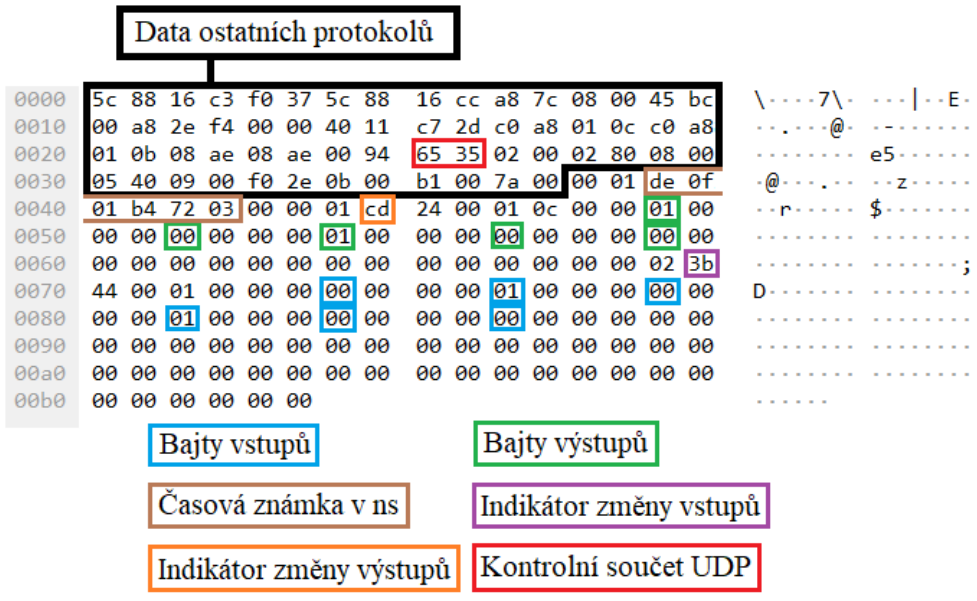
V tomto útoku je provedena modifikace probíhajících paketů tak, aby bylo chování napadené aplikace na základě útoku změněno od původního chování. Toho bylo dosáhnuto nahrazením



Obrázek 2.5 Začátek komuniace



Obrázek 2.6 Paket CIP I/O poslaný ze síťového adaptéru



Obrázek 2.7 Rozbor paketu CIP I/O poslaného ze síťového adaptéru

bajtů vstupů v paketech, posílaných z AENTR do PLC, vlastními daty útočníka a doprovodných úprav s modifikací spjatých. Útok provádím až po navázání I/O spojení mezi automatem a síťovým adaptérem AENTR. Nejprve je třeba provést dodatečnou analýzu paketů.

Nejprve jsem objevil časovou známku označující dobu odeslání každého CIP I/O paketu. To, že se jedná o časovou známku jsem ověřil porovnáním s časem odposlechnutí paketu.

Další, pro útok důležitější, části paketů jsou indikátory změny vstupů a výstupů paketů. Na základě pozorování jejich chování jsem zjistil, že při každé jedné změně vstupu se tento indikátor zvýší o 2. Má velikost pouze jeden bajt a při přetečení maximální hodnoty bajtu dochází ke ztrátě nejvyšší cifry. Pokud se změní více vstupů naráz, indikátor se zvýší o 2 za každou takovou změnu. Indikátor změny výstupů se chová obdobně se změnami výstupů.

Při modifikaci je také nutné vzít v potaz kontrolní součty protokolů vyšších úrovní. Mezi nimi jsou pouze dva, které se počítají z dat CIP I/O paketu. Kontrolní součet protokolu Ethernet a kontrolní součet protokolu UDP. Ethernetový kontrolní součet je řešený na úrovní ovladače síťového adaptéru. Proto není ani vidět v odposlechnutých paketech v aplikaci Wireshark. Ten se automaticky přidá po odeslání ethernetového paketu z našeho zařízení. U kontrolního součtu UDP je ale třeba vypočítat kontrolní součet pro modifikovaná data nový. To ale není velký problém, jelikož vzorec pro výpočet kontrolního součtu UDP je standardizovaný a veřejně dostupný.

Z těchto poznatků lze vyvodit, že pro modifikaci CIP I/O paketů je třeba nejprve odposlechnutý paket zadržet, přepsat bajty odpovídající vstupům či výstupům vlastními daty, na základě počtu změn vstupů a výstupů upravit indikátory změny vstupů a výstupů a nakonec přepočítat kontrolní součet v hlavičce UDP.

Zadržení odposlechnutého paketu nelze provést s použitím síťového mostu systému Windows. Proto byl můj první krok vytvoření vlastního síťového mostu. K tomu jsem použil funkce knihovny ScaPy, které nabízí vedle již zmíněné funkce sniff i funkci sendp, která je schopná odeslat data přímo na linkové vrstvě. První verze programu pouze přeposlala každý odposlechnutý paket z jednoho síťového adaptéru na druhý. Tato verze ale nefungovala, jelikož odesílaný paket byl z druhého (odchodového) síťového adaptéru opět odposlechnut, zpracován a poslán zpět. To vytvářelo záplavu mostu i celé sítě těmito pakety. Pro spravení této vady jsem vytvořil obdobu CAM tabulky používaných v síťových přepínačích. K oběma síťovým adaptérům si ukládám MAC adresy zařízení, která odesílají Ethernetové pakety na tento síťový adaptér (zdrojové MAC adresy Ethernetových paketů, které přišly na toto rozhraní). K síťovému adaptéru přiřadím MAC adresu pouze pokud zatím není přiřazena k jinému síťovému adaptéru. Díky té mohu o daném paketu zjistit, zda je, či není zpracovaný. U každého odchyceného paketu nejprve zjistím, zda adaptér, na kterém byl paket odchycen, má k sobě přiřazenou MAC adresu shodnou se zdrojovou MAC adresou odchyceného paketu. Pokud tomu tak je, pak paket přeposílám na druhý síťový adaptér. Pokud tomu tak není, paket místo odeslání zahodím.

Pak už stačilo pakety pouze správně modifikovat. Nejprve zaměním hodnoty vstupů v CIP I/O paketu poslaného z AENTR za hodnoty zvolené uživatelem. Dále vypočítám hodnotu bajtů indikujících změnu podle následujícího vzorce.

$$m_{i+1} \coloneqq m_i + 2 \cdot \mathrm{HD}(A, B) \bmod 2^8,$$

kde m_i je původní hodnota bajtu indikujícího změnu,hodnoty vstupů jsou reprezentovány binárními řetězci A a B, kde A jsou hodnoty vstupů v odposlechnutém paketu a B jsou hodnoty vstupů zadané útočníkem, $\mathrm{HD}(A, B)$ je Hammingova vzdálenost řetězců vstupů (tj. počet rozdílných bajtů). Výsledek m_{i+1} je nová hodnota bajtu indikujícího změnu pro podvrhnutý paket.

Výše popsané principy používám v programu `modify_trafic_l2bridge.py` (také dostupným v externí příloze této práce) s jednoduchým konzolovým uživatelským rozhraním, který útok (úpravu paketů) realizuje.

Výsledkem útoku je, že útočník může měnit údaje o stavu hladiny v přepouštěcí nádrži na nepravdivé a ovlivňovat tím chod napouštěcího čerpadla i odtokového ventilu. Jednoduchý příklad je přepsání údaje o plné kapacitě nádrže za prázdnou. Útok stěžuje jen odpočet nezměněné hladiny (po minutě nezměněné hladiny při napouštění se spustí alarm a čerpadla se zastaví).

To se dá ale primitivně obejít periodickou změnou hladiny každých například 50 s a následnou změnou zpět. Aplikace neaktivuje alarm při nelogické změně hladiny ze stavu poloprázdná na prázdná, když se nádrž pouze napouští, a při každé takové změně obnoví časový odpočet do alarmu. Čerpadlo pak napouští již plnou nádrž a v reálném případě může dojít ke škodám jako je rozbití čerpadla, přetečení nádrže či poškození přepouštěcí nádrže.

2.3 Zabezpečení stanice DS1

V této části práce je popsán postup pro zabezpečení stanice DS1 pomocí CIP Security. To se skládá z navrhnutí bezpečnostního modelu a následného nahrání bezpečnostního modelu na stanici DS1.

2.3.1 Software použitý k zabezpečení

Zde je základní seznámení s jednotlivými programy a aplikacemi, které byly v práci využity na zabezpečení výukové stanice DS1. Byly vytvořeny firmou Rockwell Automation právě pro správu průmyslových zařízení.

2.3.1.1 Studio 5000

Studio 5000 je nástroj pro programování, konfiguraci a diagnostiku průmyslových řídicích systémů. Prostředí Studia 5000 je rozděleno na několik částí.

Pro tuto práci je nejdůležitější jeho část s názvem Logix Designer, pomocí kterého se programují řídící automaty PLC. Logix Designer podporuje více způsobů psaní programu pro PLC. Aplikace na výukové desce DS1 je napsaná v žebříkové logice. Logix Designer poskytuje uživatelské rozhraní pro nahrávání programu na PLC, získávání programu z PLC, sledování chodu programu v reálném čase, psaní a upravování těchto programů a dokonce i prostředek pro aktualizování firmware PLC. Rockwel Automation vydala mnoho verzí tohoto programu, kde postupně programu přidávala funkce. Aby se dal Logix designer použít pro správu PLC, musí mít firmware PLC a Logix Designer kompatibilní verzi.

V této práci jsem zprvu pracoval s Logix Designer verzí 32.02.01, jelikož byla kompatibilní s původní verzí firmware PLC (32.014). Pak jsem ale musel kvůli kompatibilitě s CIP Security aktualizovat firmware PLC. Proto jsem přešel na novější verzi Logix Designer verze 35.00.00, pomocí kterého jsem změnil i firmware PLC na verzi 35.011 podporující CIP Security.

Další část Studia 5000 je například View Designer, což je prostředí pro vývoj ovládacích panelů HMI. Logix Emulate pro testování kódu bez potřeby fyzických zařízení a jiné.

Pro užívání Studia 5000 je třeba mít zakoupenou licenci. Rockwell Automation nabízí několik variant licence, kde každá varianta poskytuje různé části Studia 5000.

2.3.1.2 FactoryTalk System Services

FactoryTalk System Services poskytují certifikační autoritu, službu pro správu bezpečnostních politik a služby pro aplikování bezpečnostních modelů na fyzická zařízení. Tuto sadu služeb využívá především FactoryTalk Policy Manager, což je grafické uživatelské rozhraní pro konfiguraci bezpečnostních politik v CIP sítích.

V této práci byla použita verze 6.31.00 FactoryTalk System Services.

2.3.1.3 FactoryTalk Policy Manager

FactoryTalk Policy Manager je nástroj, pomocí kterého oprávněný uživatel vytváří a spravuje bezpečnostní model sítě CIP. Pro vytváření bezpečnostních modelů využívá tři základní kompo-

nenty – zóny (skupiny zařízení), zařízení (počítače, PLC, HMI atd.) a spoje (komunikační cesty mezi předchozími komponenty) [21].

FactoryTalk Policy Manager je závislý na službách, které poskytuje FactoryTalk System Services a nemůže bez nich samostatně fungovat. V této práci byla použita verze FactoryTalk Policy Manager 6.30.00.

2.3.1.4 FactoryTalk Linx

FactoryTalk Linx je server běžící na pracovních stanicích, přes který komunikují ostatní aplikace přímo s fyzickými zařízeními (PLC a další). Podporuje CIP Security a zařízení, na kterém běží server FactoryTalk Linx se dá přidávat do bezpečnostních modelů stejně jako ostatní průmyslová zařízení podporující CIP Security.

Součástí FactoryTalk Linx je také prohledávač sítě (FactoryTalk Linx Network Browser). Ten je schopen identifikovat zařízení připojená k síti a poskytnout jejich základní správu a informace, jako je například běžící verze firmware, změna IP adresy či zda je zařízení zabezpečeno s CIP Security.

V této práci byla použita verze FactoryTalk Linx 6.31.00.

2.3.1.5 FactoryTalk Administration Console

FactoryTalk Administration Console je aplikace sloužící pro konfiguraci FactoryTalk Directory. V té jsou vedle jiného uloženy i uživatelské účty, jejich přihlašovací údaje a oprávnění, která jsou správcem sítě udělena. FactoryTalk Directory se dělí na dva hlavní adresáře. První je lokální adresář sloužící pro správu oprávnění uživatelských účtů přímo v počítači. Druhý je síťový adresář, který je sdílený napříč více počítači. Síťový adresář je na serveru síťového adresáře, který je v ideálním případě k síti připojen stále (aby mohla probíhat autentizace a autorizace uživatelů). Úprava síťového adresáře serveru může být provedena (pokud má na danou úpravu přihlášený uživatel práva) jak přímo na serveru, tak na klientských počítačích k serveru připojených. FactoryTalk Administration Console umožňuje vytvářet uživatelské účty a udělovat jim oprávnění (například povolit uživateli správu bezpečnosti sítě pomocí FactoryTalk Policy Manager). Dále se zde dají vytvářet skupiny uživatelů s podobnými právy pro snazší správu uživatelů.

V této práci byla použita verze FactoryTalk Administration Console 6.31.00.

2.3.2 Kompatibilita s CIP Security

Dle zadání mám zabezpečit komunikaci mezi PLC a modulem AENTR nebo HMI pomocí bezpečnostních proxy CSP. Původní zapojení desky obsahuje dvě zařízení CSP – jedno pro zabezpečení síťového adaptéru AENTR a druhé pro zabezpečení řídícího automatu. Po důkladném prozkoumání manuálu CIP Security Proxy (s katalogovým číslem 1783-CSP) jsem se ale dočetl, že řídící automat CompactLogix 5380 Controller se dá zabezpečit pomocí CSP pouze pro komunikaci s pracovní stanicí (počítač, přes který se řídící automat programuje). Ochranu komunikace mezi PLC a modulem AENTR není možné provést pomocí dvou bezpečnostních modulů CSP, jelikož CSP nemůže otevřít kyberneticky bezpečné spojení s I/O zařízeními [16, 15]. Podrobnější informace v dokumentu neuváděli. Společnosti Rockwell Automation bych vytkl nedostatečné zdůraznění této informace v jejich manuálech a příručkách. Rockwell Automation manuál pro zabezpečení sítě pomocí CIP Security uvádí, že CompactLogix 5380 Controller je kompatibilní s CSP proxy a důležitou informaci o omezení této kompatibility uvádí malým písmem v záhlaví tabulky. V manuálu CSP je v sekci o kompatibilitě řečeno pouze, že CompactLogix 5380 Controller je s CSP kompatibilní omezeně (a zmiňují ochranu komunikace mezi PLC a pracovní stanicí). Samotná informace, že PLC se takto zapojit nedá je až v sekci „nepodporované topologie“ v popisku nákresu propojeného PLC a CSP.

Zprvu jsem se při zabezpečení stanice snažil použít obě zařízení CSP. V takovém případě proběhne aplikování bezpečnostních politik bez jakýchkoliv systémových upozornění, či chyb. Řídící systém ale není schopen chodu, jelikož CSP není schopno navázat spojení se síťovým adaptérem AENTR, ani ovládacím panelem HMI. Při prozkoumávání komunikace po síti pomocí programu Wireshark jsem zjistil, že CSP nepropouští k řídícímu automatu žádné pakety, ale propouští pakety od řídícího automatu ven. Dokonce je možné navázat jednosměrné spojení s ovládacím panelem HMI tak, že se pro navázání komunikace připojil řídící automat bez modulu CSP a modul CSP se připojil až po navázání komunikace.

O ovládacích panelech HMI dokumenty hovoří jasně, že nemohou být zaštítěny pomocí CSP (opět kvůli neschopnosti CSP otevřít kyberneticky bezpečné spojení) [16].

Problém s nekompatibilním CSP se ale dá vyřešit aktualizací firmware PLC. CompactLogix 5380 Controller totiž od verze 34.011 podporuje CIP Security samostatně [15]. Proto je třeba změnit topologii síťového zapojení tak, že se odpojí jedno zařízení CSP zaštiťující řídící automat PLC.

Prvním krokem zabezpečení výukové stanice DS1 je tedy aktualizace verze firmware z 32.014, která CIP Security nepodporuje na verzi 35.011, která CIP Security podporuje. To jsem provedl pomocí Logix Designeru. Při aktualizaci firmware ale doporučuji nejprve provést tvrdý restart řídícího automatu PLC a až poté nahrát novou verzi firmware, protože při aktualizaci bez tvrdého restartu se na PLC nejspíš nahrála skrytá chyba, která znemožňovala nahrání bezpečnostního modelu (aplikace pro chod nádrže fungovala).

Jakmile je aktualizovaný firmware PLC, je třeba převést do novější verze i program pro PLC. Při aktualizaci firmware se program z PLC smaže. Program se převede jednoduše otevřením staré verze programu v nové verzi Logix Designeru. Logix Designer vytvoří vedle aktualizovaného programu i zálohu předchozí verze.

Nová verze programu se již dá nahrát na PLC s aktualizovaným firmware. Toho se docílí v Logix Designeru neobvykle popsaným tlačítkem „download“.

2.3.3 Identifikace hrozeb

Bezpečnostní model, který je vhodný pro zabezpečení výukové stanice DS1, je silně závislý na okolnostech spjatých s použitím systému v reálném případě. Například výuková stanice DS1 není nijak připojena k nedůvěryhodné síti, což znamená, že útočník nemá do sítě žádný přístupový bod a stanici není třeba zabezpečit. Proto je třeba vytvořit model použití daného systému a bezpečnostní model vytvořit na základě tohoto modelu. V takovém modelu určuji část sítě, která je nedůvěryhodná a je zdrojem potenciálních útoků.

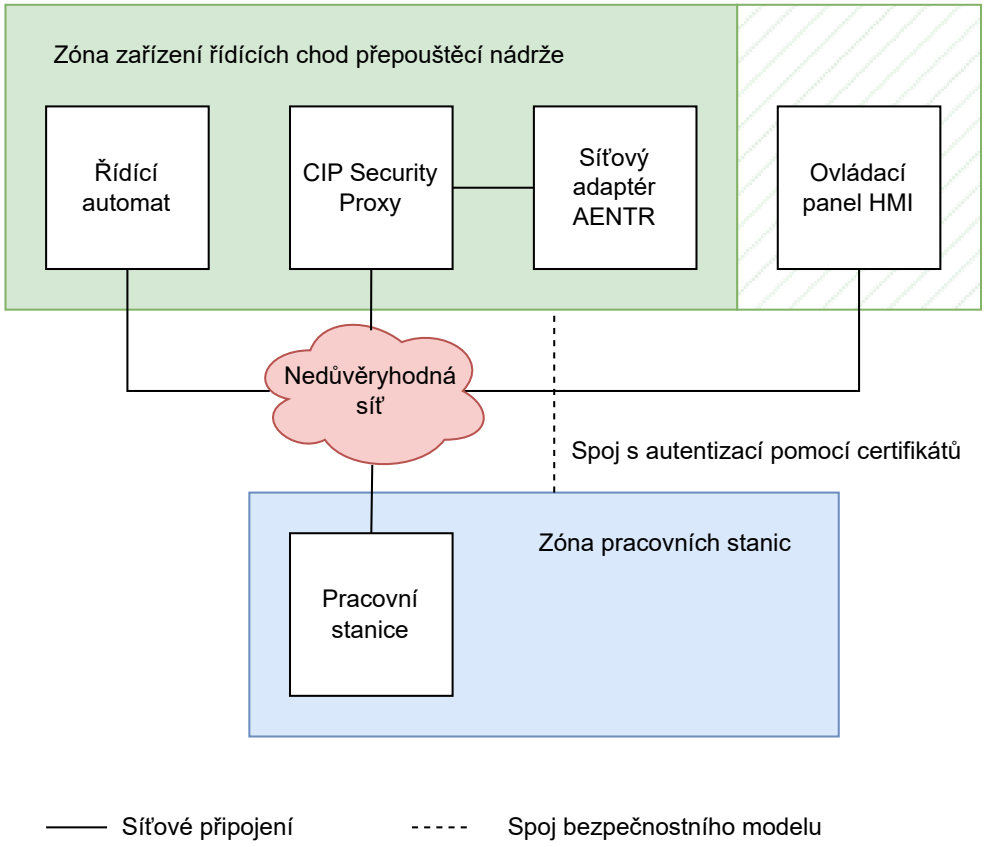
Nejprve uvažuji model, kde je řídící automat, bezpečnostní modul CSP zaštitující síťový adaptér AENTR a ovládací panel HMI přímo připojen do nedůvěryhodné sítě (znázorněno na Obr. 2.8). Ideální bezpečnostní model by pak byl schopen zabezpečit zařízení vůči všem útokům z nedůvěryhodné sítě.

V modelu předpokládám, že je přístup k zařízením, i propojujícím kabelům mimo nedůvěryhodnou síť fyzicky omezen (například zamknutými dveřmi).

2.3.4 Autentizace a autorizace správců a uživatelů

Pro chod industriálních společností a vývoj složitých aplikací pro řídící automaty je třeba rozdělování práce mezi více zaměstnanců. Tito zaměstnanci mají různé funkce a pracovní zaměření. Pro co největší potlačení hrozby útoku z řad vlastních zaměstnanců je třeba jim přidělit různá oprávnění. To je v industriálních sítích se zařízeními a softwarem Rockwell Automation dosáhnuto pomocí uživatelských účtů a k nim přiděleným oprávněním.

Pro správu uživatelských účtů a autentizace více pracovních stanic je potřeba mít k síti připojený server, ve kterém jsou centralizovaně uloženy jejich přístupová práva. V úvodní konfiguraci má přístup pro správu tohoto serveru každé zařízení s FactoryTalk softwarem. Nejprve je tedy



Obrázek 2.8 Model znázorňující zapojení průmyslových zařízení k nezabezpečené síti a navrhnutý bezpečnostní model

třeba server konfigurovat v uzavřeném prostředí pro nutnost autentizace a až poté server připojit k síti průmyslových zařízení [17].

Správa uživatelů se provádí v aplikaci FactoryTalk Administration Console. V tom se vytváří účty buď na základě existujících účtů operačního systému Windows, nebo se dá vytvořit kompletně nový účet přímo pro Rockwell Automation software.

Pro zabezpečení komunikace mezi řídícím automatem a síťovým adaptérem AENTR jsem využil pouze jednu pracovní stanici a centrální server tedy nebyl třeba.

2.3.5 Navrh bezpečnostního modelu

V produktech Rockwell Automation se bezpečnostní model vytváří pomocí aplikace FactoryTalk Policy Manager. Ta k modelování poskytuje dva základní prvky – zóny a spoje. Připojená zařízení se dají přiřazovat do různých zón. Mezi zařízeními ve stejné zóně je povolena komunikace. Spoje pak slouží k vytvoření komunikačních kanálů mezi zónami.

Zařízení se mají rozdělovat do zón podle několika faktorů. První je společná funkce zařízení a s ní spjatá potřeba komunikace. Druhý faktor je potřeba stejné úrovně zabezpečení více zařízení.

Pro stanici DS1 jsem tedy pomocí těchto komponent vytvořil model, který má 2 zóny a jeden spoj. První zóna v sobě obsahuje všechna průmyslová zařízení řídící chod přepouštěcí nádrže. Druhá zóna obsahuje pracovní stanice, které slouží pro vývoj aplikací a správu průmyslových zařízení (v tomto případě je pracovní stanice pouze jedna a to můj počítač). Tyto zóny jsou propojeny spojem, který slouží jako komunikační kanál mezi pracovními stanicemi a průmyslovými zařízeními. Tento bezpečnostní model je znázorněn na Obr. 2.8.

Tento model jsem vytvořil na základě dříve jmenovaných faktorů a faktu, že velmi podobné modely jsou v manuálech pro zabezpečení sítě pomocí CIP Security [15, 10]. Proto bude sloužit jako vhodný demonstrační model.

2.3.6 Nahrání bezpečnostního modelu na DS1

Výuková stanice DS1 se nachází ve stavu, kdy bezpečnost na stanici zatím nebyla konfigurována. V tomto případě přijme bezpečnostní konfiguraci od prvního zařízení, které se na ni bezpečnostní konfiguraci pokusí nahrát. To je takzvaný TOFU model (Trust On First Use) [10].

V předchozí kapitole popsaný model jsem nejprve musel vytvořit v aplikaci FactoryTalk Policy Manager. Poté, co jsem vytvořil zóny a spoj, bylo třeba do zón přiřadit jednotlivá zařízení. Zařízení se do zón dají přidávat manuálně, kde se vyberou ze seznamu Rockwell Automation produktů, zadá se jejich IP adresa a verze firmware (manuální přidání se dá provádět bez připojení do průmyslové sítě). Nebo to zařídí automatický vyhledávač průmyslových zařízení v síti FactoryTalk Linx Network Browser. Pracovní stanice musí mít zapnutou službu FactoryTalk Linx, jinak není nalezena automatickým vyhledávačem.

Další krok je nastavit bezpečnostní požadavky jednotlivým zónám. To zahrnuje nastavení typu autentizace, nastavení integrity a důvěrnosti dat pro I/O spojení i pro explicitní spojení, zvolit, zda zakázat port HTTP (80) a nakonec nastavit pravidla pro CIP přemostění komunikace.

Typy autentizace máme na výběr dva – autentizace pomocí předem sdíleného klíče a pomocí certifikátů (což odpovídá standardu CIP Security). Autentizace pomocí předem sdíleného klíče ale přináší v aktuální verzi systému zásadní nedostatek, že není možné propojovat takto autentizované zóny pomocí zabezpečených spojů. Pro náš model jsem pro obě zóny zvolil více doporučovanou variantu autentizace certifikáty. FactoryTalk Policy Manager v tomto případě slouží jako certifikační autorita.

Nastavení integrity a důvěrnosti spočívá ve zvolení, zda kontrolovat pouze integritu dat, nebo kontrolovat integritu a zároveň data šifrovat. To se volí zvlášť pro CIP I/O spojení a explicitní spojení. V našem případě považujeme všechnu komunikaci za důvěrnou a vyžadujeme i ochranu proti úniku informací v nedůvěryhodné síti. Zvolil jsem tedy kontrolu integrity a šifrování dat

jak pro I/O spojení, tak i pro spojení explicitní. Kontrola integrity a šifrování dat je esenciální pro ochranu proti útokům prezentovaných v kapitole 2.2.

Přes port HTTP (80) lze s některými zařízeními navázat diagnostickou komunikaci. V případě desky DS1 tuto službu poskytují pouze bezpečnostní moduly CSP. Uživatel jednoduše zadá IP adresu do svého prohlížeče a není-li port HTTP zablokovaný, ukážou se mu informace o průchodnosti paketů, navázaných síťových spojení a další. To představuje potenciální riziko úniku důvěrných informací, proto jsem port HTTP zakázal v zóně průmyslových zařízení. U pracovních stanic port HTTP zakázat nelze a ani to není žádoucí.

CIP přemostění komunikace je potřeba pouze při vytváření síťového spojení mezi různými CIP technologiemi (například EtherNet/IP a DeviceNet). Některá zařízení jsou schopna taková spojení vytvořit a pouze těchto zařízení se týká nastavení CIP přemostění. U výukové stanice DS1 je veškerá komunikace prováděna přes technologii EtherNet, a proto nejsou CIP přemostění komunikace potřeba a je vhodné ho zakázat. CIP Security je vyvinuté pouze pro technologii EtherNet/IP a povolení přemostění komunikace do nezabezpečené technologie je bezpečnostní riziko.

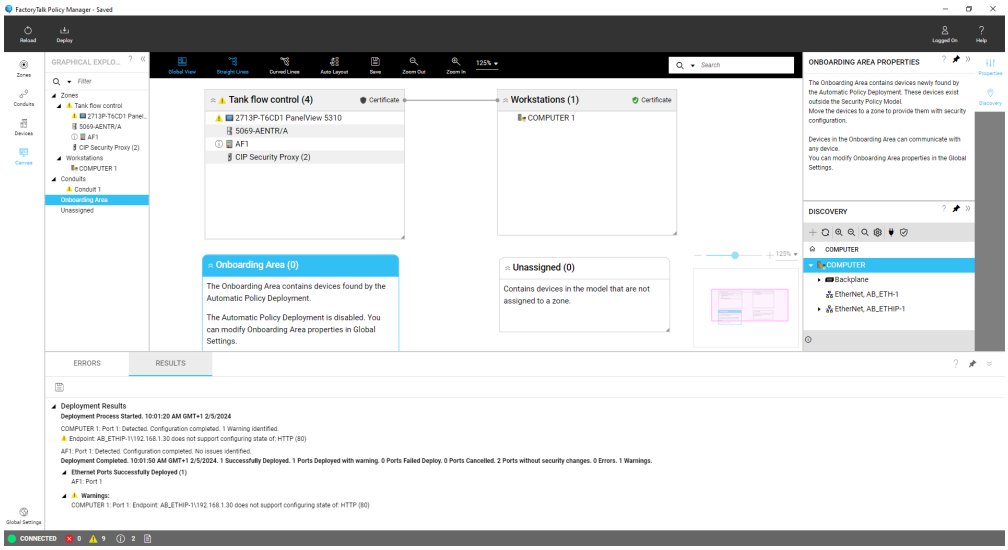
Po nastavení zón, je třeba zvolit bezpečnostní opatření i ve spoji. U toho se nastavuje pouze způsob autentizace a nastavení integrity a důvěrnosti dat pro CIP I/O a explicitní spojení.

V možnostech autentizace jsou na výběr dvě varianty. Autentizace na základě důvěrné IP adresy a na základě certifikátu. Autentizace na základě důvěrné IP adresy je ale velmi slabé bezpečnostní opatření a IP adresa může být lehce podvrhnuta. Toto spojení slouží k připojení zastaralých zařízení nepodporujících CIP Security a propojení zón s autentizací pomocí předem sdíleného klíče. Zvolil jsem tedy variantu autentizace pomocí certifikátu.

Nastavení integrity a důvěrnosti dat je obdobné nastavení u zón. Spojení mezi pracovní stanicí může přenášet důvěrné informace například jako výrobní tajemství nahrávaného programu. Zvolil jsem tedy variantu kontroly integrity a šifrování dat.

Již po nastavení bezpečnostních požadavků zón je v aplikaci FactoryTalk Policy Manager zobrazeno varovné hlášení týkající se ovládacího panelu HMI. Jak už jsem několikrát zmínil, HMI nepodporuje CIP Security a proto nemůže sdílet bezpečnostní nastavení zóny. Rockwell Automation dovoluje připojit zastaralá zařízení pomocí důvěryhodné IP adresy. Takové připojení ale představuje závažné bezpečnostní riziko. Mezi útoky, proti kterým je tato komunikace zranitelná je zajmutí IP adresy a odposlech nešifrovaných paketů. Samotný výrobce Rockwell Automation v manuálech pro zabezpečení průmyslových systémů prohlašuje, že zastaralá zařízení (nepodporující CIP Security) doporučují přidávat do bezpečnostního modelu, pouze pokud uživatel přijímá s tím spjatý risk [15]. Proto doporučuji pro zabezpečení výukové desky ovládací panel HMI vůbec nepoužít. V tomto případě je deska schopna plného chodu i bez ovládacího panelu. Informace o chodu přehrady jsou bez ovládacího panelu předávány uživateli pomocí světelných kontrolek a případně připojené pracovní stanice. Ovládací panel slouží na stanici DS1 jen jako zdroj informací a chod přepouštěcí nádrže přes něj není ovládán. Pro demonstraci zabezpečení jsem vytvořil a nahrál variantu bezpečnostního modelu s panelem HMI v zóně, jak prezentuje výrobce Rockvell Automation v manuálu[15] 2.9. Je možné, že výrobce Rockwell Automation v budoucnu implementuje podporu CIP Security i do ovládacích panelů HMI. V tom případě by byl tento model pro zabezpečení stanice DS1 nejvhodnější. Dále jsem vytvořil a nahrál i bezpečnostní model bez panelu HMI, který nemá zmíněnou zranitelnost 2.10. Z toho důvodu je také zóna v Obr. 2.8 rozdělena na dvě části – s plným pozadím a s šrafovaným pozadím. Šrafované pozadí pod panelem HMI znázorňuje možnost odebrání panelu HMI z bezpečnostního modelu.

S hotovým bezpečnostním modelem, a konfigurovanými bezpečnostními prvky jsem mohl přejít na nahrání bezpečnostního modelu na zařízení. To se provede stisknutím tlačítka deploy v aplikaci FactoryTalk Policy Manager. Aplikace pak sama nahraje na každé zařízení podepsané certifikáty a bezpečnostní politiky. Při nahrávání modelu jsem se setkal s několika chybovými hlášeními, že při konfiguraci bezpečnostního modulu CSP došlo k chybě, jelikož bezpečnostní modul je v tuto chvíli již konfigurován. Při následném zkoumání komunikace jsem ale zjistil, že komunikace je šifrována dle nastavení v bezpečnostním modelu a nějaká konfigurace bezpeč-



Obrázek 2.9 Bezpečnostní model s panelem HMI v aplikaci FactoryTalk Policy Manager

nostního modulu CSP tedy musela proběhnout. Vzhledem k povaze aplikace FactoryTalk Policy Manager, která poskytuje jen stručné chybové hlášení, jsem ale nemohl problém dále analyzovat. Pouze odhaduji, že se jedná o chybu samotného FactoryTalk Policy Manager, kdy se snažil nahrát bezpečnostní model jednak na zařízení zaštítěné (AENTR) a jednak na samotné CSP. Síťový adaptér AENTR ale nepodporuje CIP Security, tak byl místo něj podruhé konfigurován CSP modul. Po několika dalších pokusech o nahrání modelu se ale model nahrál již bez chybového hlášení. Přehledy modelů a prostředí aplikace FactoryTalk Policy Manager jsou na Obr. 2.9 a 2.10. Při nahrávání modelu se zobrazovalo i varovné hlášení, kde mě aplikace upozorňovala, že nelze konfigurovat HTTP port pracovní stanice. Důvod tohoto hlášení mi ale není zřejmý, jelikož je v zóně pracovních stanic nastaveno, že se HTTP port blokovat nemá. Na Obr. 2.10 je toto varovné hlášení vidět.

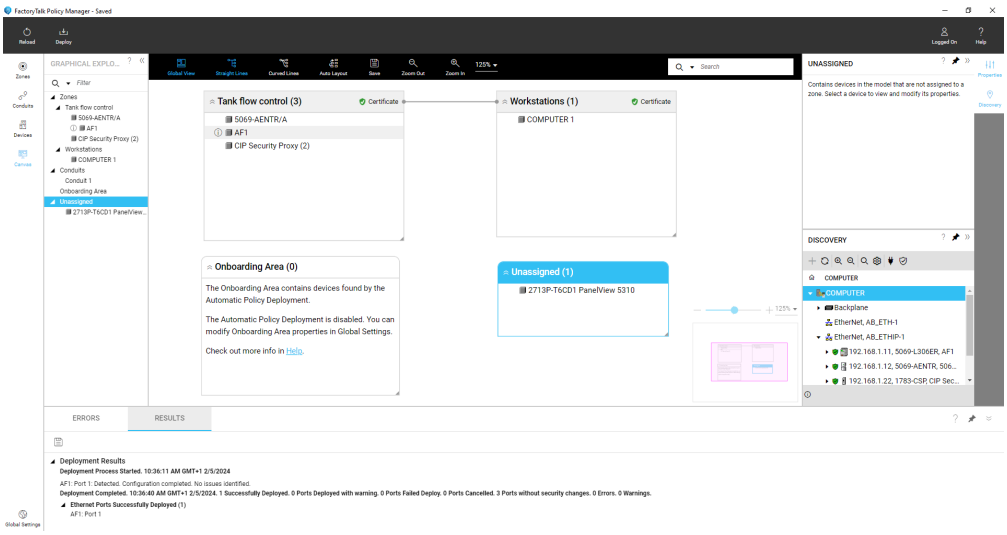
2.3.7 Analýza zabezpečené komunikace

Pro odchycení komunikace mezi řídícím automatem PLC a síťovým adaptérem AENTR jsem se připojil na síť stejně jako v při provádění útoků na nezabezpečenou CIP komunikaci (jako MITM). Poté jsem pomocí aplikace Wireshark odchytil navázání komunikačního spojení mezi PLC a AENTR.

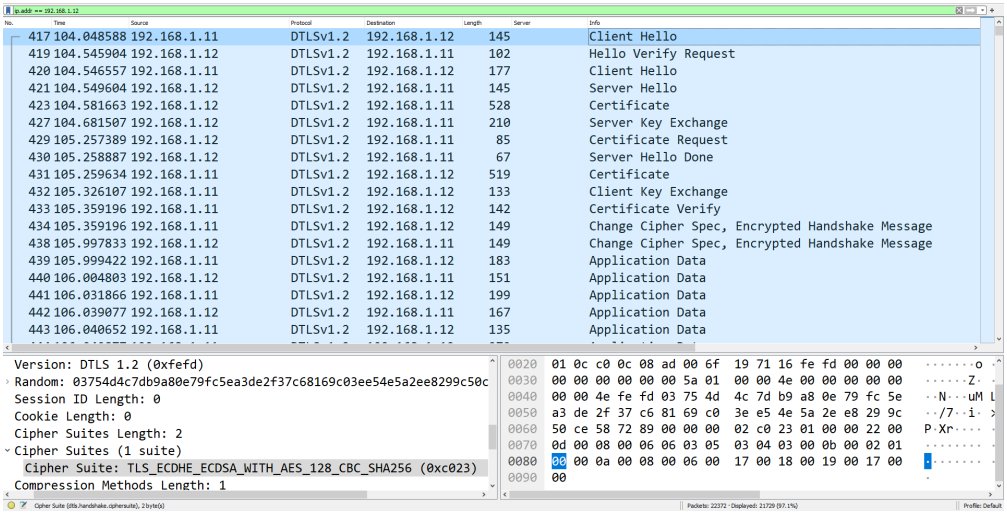
Jak je určeno standardem CIP Security, CIP I/O komunikace probíhá pomocí protokolu DTLS. Nejprve se domluví na použité šifrové sadě, poté si na základě šifrové sady vzájemně ověří podepsané certifikáty a vymění veřejné klíče. Šifrová sada, kterou k navázání spojení využili je `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`. To znamená, že je využita Diffie-Hellmanova metoda výměny klíčů používající eliptické křivky (zkratka ECDHE). Autorizace se provádí pomocí certifikátu s digitálním podpisem a podpis je vytvořen algoritmem ECDSA (také využívá eliptické křivky). Symetrické šifrování zastává bloková šifra AES s velikostí klíče 128 bitů. Pro šifrování více bloků dat je použita metoda CBC (cipher block chaining). Jako hašovací funkce pro kontrolu integrity dat je použita SHA256.

Ukázka navázání komunikace je prostřednictvím aplikace Wireshark prezentována na Obr. 2.11.

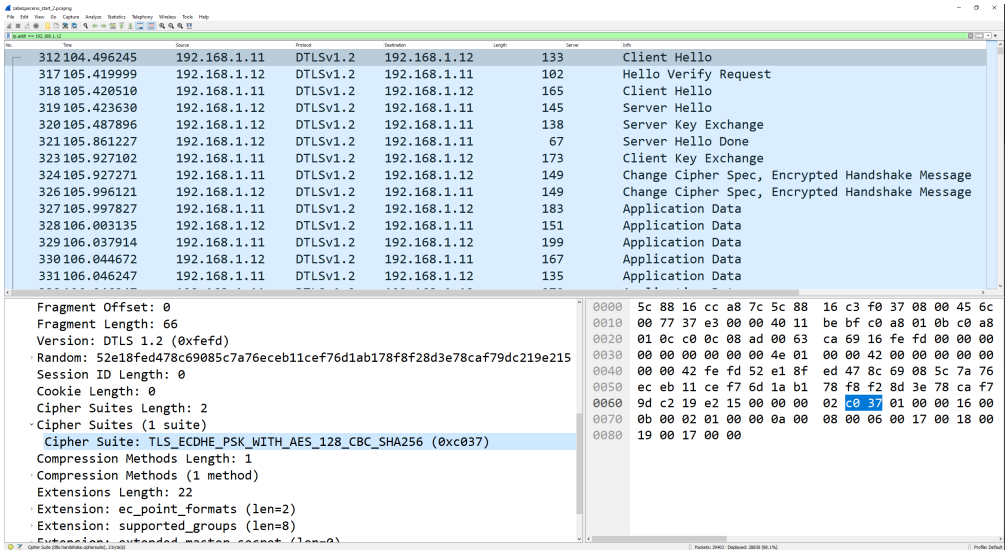
Pro demonstraci zabezpečení výukové stanice DS1 pomocí předem sdíleného klíče, jsem vytvořil a nahrál na výukovou stanici i model s tímto typem autentizace. U navázání spojení je



Obrázek 2.10 Bezpečnostní model bez panelu HMI v aplikaci FactoryTalk Policy Manager



Obrázek 2.11 Navázání komunikace mezi PLC a AENTR prostřednictvím protokolu DTLS a autentizací certifikáty



Obrázek 2.12 Navázání komunikace mezi PLC a AENTR prostřednictvím protokolu DTLS a autentizací typu předem sdílený klíč

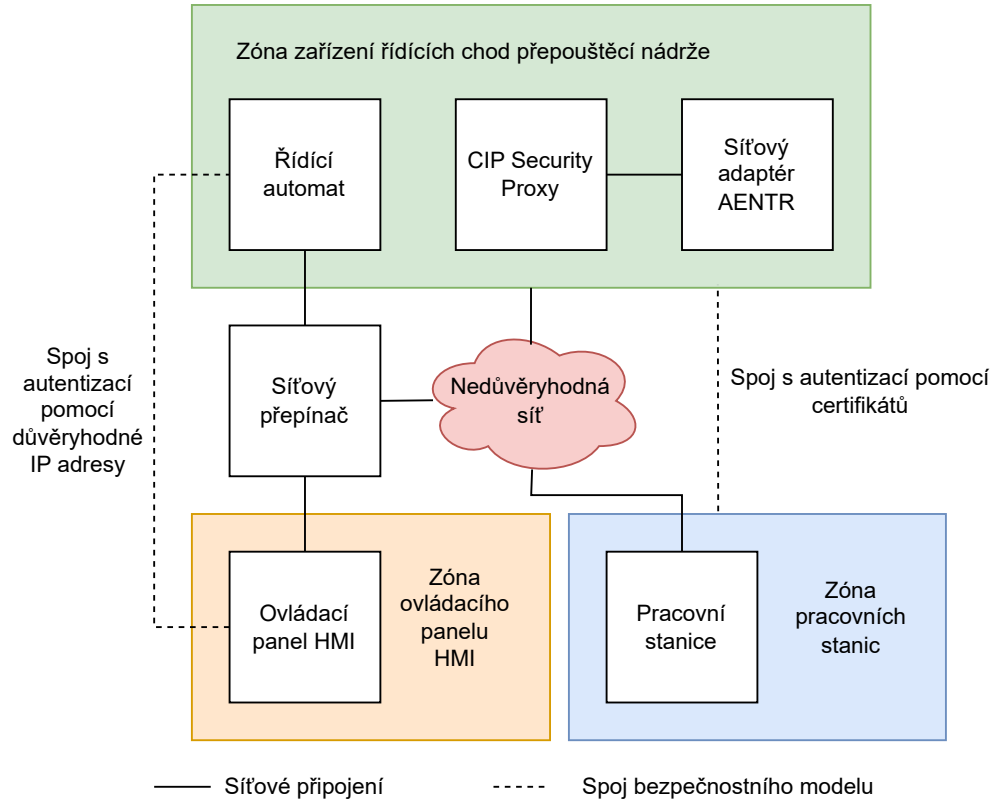
využita jiná šifrová sada a chybí výměna certifikátů. Ukázka navázání komunikace s autentizací pomocí předem sdíleného klíče je na Obr. 2.12

2.3.8 Zabezpečení ovládacího panelu HMI

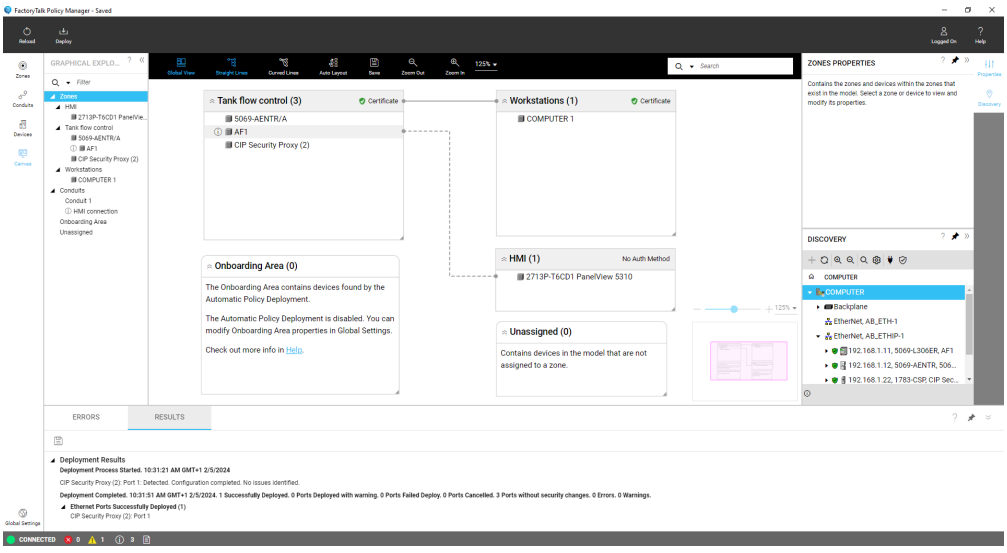
Zabezpečení ovládacího panelu HMI je třeba řešit odlišně, kvůli jeho nekompatibilitě s CIP Security. Výrobce průmyslových zařízení momentálně neposkytuje prostředky pro zabezpečení ovládacích panelů HMI na transportní vrstvě modelu OSI. Kdyby uživatel přesto vyžadoval zabezpečení této komunikace, musel by se spolehnout buď na zařízení od jiných výrobců, která jsou schopna vytvořit šifrovaný komunikační kanál, nebo na zabezpečení formou firewall, kde by se blokovala komunikace s konkrétní IP adresou. Vytvoření jednoduché firewall umožňuje na stanici DS1 například síťový přepínač. V síťovém přepínači se dá k síťovému adaptéru přiřadit access control list (ACL). ACL je seznam pravidel, který určuje, zda se komunikace povolí, či zamítne. ACL se nastavuje zvlášť pro příchozí pakety a odchozí pakety daného síťového adaptéru. V následující části popíši zabezpečení komunikace ve výukové stanici DS1 pomocí jednoduché firewall.

Nejprve je třeba do modelu zapojení k nedůvěryhodné síti přidat síťový přepínač. Nové zapojení je zobrazeno na Obr. 2.13. Upozorňuji, že fyzický přístup k zařízením a komunikačním kanálům, mimo nedůvěryhodnou síť, musí být povolen pouze oprávněným osobám.

Další krok je upravit bezpečnostní model tak, aby byla autentizace způsobem přednastavení důvěryhodné IP adresy aplikována pouze na dvě zařízení, kterých se komunikace týká – na řídící automat a ovládací panel HMI (mezi ovládacím panelem HMI a ostatními průmyslovými zařízeními nejsou navazována CIP spojení). Toho se dosáhne pomocí nového spoje s autentizací typu důvěryhodná IP adresa. Spojem se dají propojit přímo zařízení, ale zařízení musí být přiřazená do zóny, která není výchozí (v aplikaci FactoryTalk Policy Manager nelze vytvořit spoj se zařízením bez přiřazené zóny). Z toho důvodu do modelu přibyde i zóna pouze pro panel HMI. Tento bezpečnostní model je znázorněn na Obr. 2.13. Nastavení zóny pro panel HMI je vhodné ponechat výchozí, tedy bez konfigurace CIP Security. Jelikož panel HMI CIP Security nepodporuje, nastavení zóny není důležité a nemá na funkci vliv. Realizace modelu v aplikaci FactoryTalk Policy Manager je zobrazena na Obr. 2.14.



Obrázek 2.13 Model znázorňující zapojení průmyslových zařízení k nezabezpečené síti a navrhnutý bezpečnostní model pro zabezpečení komunikace s panelem HMI



Obrázek 2.14 Bezpečnostní model s panelem HMI, připojeným pomocí spoje, v aplikaci FactoryTalk Policy Manager

Po nahrání modelu je komunikace mezi řídícím automatem PLC a ovládacím panelem HMI stále bez autentizace a nešifrovaná. Proto je třeba zamezit úniku nezabezpečených dat z důvěryhodné sítě do nedůvěryhodné a přístupu zařízení z nedůvěryhodné sítě s podvrhnutou IP adresou k zařízením HMI a PLC. To se docílí nastavením ACL na síťové adaptéry, které propojují síťový přepínač s nedůvěryhodnou sítí. V ACL je třeba nastavit pravidla pro zamítnutí veškeré komunikace s IP adresou, která je používána pro autentizaci HMI. Také se musí nastavit ACL síťového adaptéru na vstupující (pro zamezení přístupu z nedůvěryhodné sítě), ale i vystupující pakety (pro zamezení úniku dat).

Takto zabezpečená síť má ale několik zásadních nedostatků. První je, že ovládací panel není možné konfigurovat pracovní stanicí připojenou přes nedůvěryhodnou síť, jelikož se všechna komunikace zamítne ve firewall. To je pro zabezpečení nutné chování kvůli absenci autentizace a autorizace HMI. Pro konfiguraci HMI je v takovém případě potřeba přístup přímo k ovládacímu panelu. Druhá nevýhoda je v potřebě mít fyzicky zabezpečený celý komunikační kanál mezi PLC a HMI. To může být v některých reálných aplikacích takřka nemožné (například při potřebě mít HMI velmi daleko od PLC).

Kapitola 3
Závěr

V této bakalářské práci jsem se zaměřil na zabezpečení výukové stanice DS1. Tuto stanici sestavila firma ServisControl a použila při tom zařízení značky Allen-Bradley od firmy Rockwell Automation. Na stanici běží aplikace, která řídí chod simulované přehrady.

Cíl seznámit čtenáře s protokolem CIP a jeho bezpečnostními aspekty jsem vypracoval v teoretické části práce. Zde popisuji funkce a principy využité při komunikaci CIP, jeho rozšíření CIP Security pro kybernetickou bezpečnost a vlastnosti implementace CIP Security v zařízeních firmy Rockwell Automation.

Pro demonstraci nedostatečné zabezpečenosti jsem provedl dva útoky na komunikaci mezi zařízeními této stanice se zaměřením na utajení a integritu zpráv. Zaměřil jsem se na komunikaci mezi programovatelným řídícím automatem a síťovým adaptérem AENTR. Konkrétně jsem provedl útoky odposlech komunikace, kde unikly informace týkající se chodu simulované přehrady, a úpravu komunikace, vedoucí k nežádoucímu chování průmyslového systému. Dosažené nežádoucí chování průmyslového systému je například napouštění přehrady přes maximální objem.

Pro demonstraci zabezpečení výukové stanice DS1 jsem v práci prezentoval různé typy bezpečnostních modelů pro různé případy použití průmyslového systému výukové desky DS1. K zabezpečení CIP komunikace jsem použil prostředky od firmy Rockwell Automation, což je konfigurační software a zařízení podporující zabezpečení pomocí CIP Security (PLC a CSP). Tyto prostředky slouží k implementaci standardu CIP Security v průmyslových systémech řečené firmy.

Výsledkem je funkční a zabezpečená komunikace mezi řídícím automatem a síťovým adaptérem, která je odolná proti demonstrovaným útokům.

Útok odposlechu komunikace jsem již prezentoval na dni otevřených dveří pro bakalářské studium na Fakultě informačních technologií ČVUT. Zde budou sloužit výukové stanice DS1 pro výuku studentů specializace informační bezpečnost.

Demonstrovaná zabezpečení a způsoby jsou jediným výrobci podporovaným způsobem zabezpečení CIP komunikace průmyslových zařízení od firmy Rockwell Automation. Tato technologie je poměrně nová (první Rockwell Automation zařízení podporující CIP Security byla představena až v roce 2018 [22]). Společnost již vydala několik verzí systému pro správu CIP Security, ale systém stále není dokonalý. Při vypracování práce jsem se velmi často potýkal s problémy s kompatibilitou a neprůhledným systémem, který poskytuje jen stručné a nejednoznačné chybové a varovné hlášky. Zásadní nevýhoda je nekompatibilita ovládacího panelu HMI s CIP Security. Panely HMI jsou součástí mnoha industriálních řídících systémů, o čemž vypovídá rozsáhlá nabídka HMI produktů na webových stránkách Rockwell Automation, a stále u nich není možnost zabezpečit síťovou komunikaci na transportní vrstvě. Jejich integrace do systému již zabezpečeného pomocí CIP Security, vede k vážným bezpečnostním rizikům celého systému.

Na tuto práci se dá navázat vytvořením dalších bezpečnostních opatření, jako je například konfigurace zařízení firewall. Zjistit způsob a bezpečnostní aspekty způsobu generování komunikačních klíčů. Více rozebrat způsob autentizace a autorizace správců a uživatelů řídícího systému. Dále se může prozkoumat ukládání důvěrných informací přímo v průmyslových zařízeních bez zaměření na síťovou komunikaci.

Bibliografie

1. ZELUZKA, František; HYNČICA, Ondřej. Průmyslový Ethernet II: Referenční model ISO/OSI. In: *AUTOMA* [online]. Praha: FCC Public, 2007, s. 60 [cit. 2023-01-15]. Dostupné z: `http://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-ii-referencni-model-iso/osi-2007_03_34209_3890/`.
2. SCHIFFER, Viktor. Common Industrial Protocol (CIP™) and the Family of CIP Networks. In: *Industrial Communication Technology Handbook*. CRC Press, 2017, s. 1–9.
3. ODVA. About ODVA | Industrial Automation | Communication Technologies. In: [online]. 2023 [cit. 2023-05-26]. Dostupné z: `https://www.odva.org/about/structure/`.
4. ODVA. EtherNet/IP™ – CIP on Ethernet Technology. In: *Technology overview series* [online]. 1999-2021 ODVA, Inc., 2021, s. 3. PUB00138R7 [cit. 2023-05-27]. Dostupné z: `https://www.odva.org/wp-content/uploads/2021/05/PUB00138R7_Tech-Series-EtherNetIP.pdf`.
5. ZELUZKA, František; HYNČICA, Ondřej. Průmyslový Ethernet IX: EtherNet/IP, EtherCAT. In: *AUTOMA* [online]. 2008, s. 86–90 [cit. 2023-05-27]. Dostupné z: `http://www.odbornecasopisy.cz/res/pdf/37910.pdf`.
6. DIERKS, Tim; RESCORLA, Eric. RFC 768: User datagram protocol. In: Internet Engineering Task Force, 1980. Dostupné z DOI: `10.17487/RFC0768`.
7. ODVA. OVERVIEW OF CIP SECURITY™. In: *Technology overview series* [online]. [B.r.], s. 4–7. PUB00319R1 [cit. 2023-05-27]. Dostupné z: `https://www.odva.org/wp-content/uploads/2020/05/PUB00319R1_CIP-Security-At-a-Glance.pdf`.
8. BATKE, Brian; WIBERG, Joakim; DUBÉ, Dennis. CIP Security Phase 1 Secure Transport for EtherNet/IP. In: [online]. 2015, s. 4–7 [cit. 2023-05-27]. Dostupné z: `https://icscsi.org/library/Documents/ICS_Protocols/ODVA%20-%20CIP%20Security%20Phase%201%20Secure%20Transport%20for%20EtherNetIP.pdf`.
9. CONKLIN, Larry. CIP Security Proxy Catalog Number 1783-CSP. In: OWASP Foundation, Inc., 2023. Dostupné také z: `https://owasp.org/www-community/Threat_Modeling_Process#stride-threat-list`. Spolupracovníci: Victoria Drake, Sven strittmatter, Zoe Braiterman.
10. Deploying CIP Security within a Converged Plantwide Ethernet Architecture. In: *Design Guide*. Cisco Systems, Inc., Panduit Corp., a Rockwell Automation, Inc., 2021, s. 3, 27. ENET-TD022A-EN-P. Dostupné také z: `https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/CIP_Security/DIG/CPwE_CIPSec_CVD.pdf`.
11. POSTEL, Jon. The Transport Layer Security (TLS) Protocol Version 1.2. In: Internet Engineering Task Force, 1980. Dostupné také z: `https://datatracker.ietf.org/doc/html/rfc768`.

12. RESCORLA, Eric; MODADUGU, Nagendra. Datagram Transport Layer Security Version 1.2. In: Internet Engineering Task Force, 2008. Dostupné také z: https://www.rfc-editor.org/rfc/rfc6347.
13. THE INTERNATIONAL SOCIETY OF AUTOMATION. ISA/IEC 62443 Series of Standards. In: [online]. [B.r.] [cit. 2023-05-26]. Dostupné z: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
14. ŠINDELEK, Milan. CIP Safety. In: [online]. Brno, 2016 [cit. 2023-05-27]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/58781/final-thesis.pdf?sequence=-1&isAllowed=y.
15. ROCKWELL AUTOMATION. CIP Security with Rockwell Automation Products. In: Rockwell Automation, Inc., 2022, s. 43, 47, 111–112. ECURE-AT001D-EN-P - December 2023. Dostupné také z: https://literature.rockwellautomation.com/idc/groups/literature/documents/at/secure-at001_-en-p.pdf.
16. ROCKWELL AUTOMATION. CIP Security Proxy Catalog Number 1783-CSP. In: Rockwell Automation, Inc., 2022, s. 11, 47, 49, 56. 1783-UM013C-EN-P - June 2022. Dostupné také z: https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um013_-en-p.pdf.
17. ROCKWELL AUTOMATION. System Security Design Guidelines. In: Rockwell Automation, Inc., 2022, s. 7, 13. SECURE-RM001F-EN-P - June 2022. Dostupné také z: https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/secure-rm001_-en-p.pdf.
18. LICHNOVSKÝ, Petr. Elektrodokumentace demostanice DS1. In: Ovčáry 299: ServisControl s.r.o, 2021.
19. *DEMOSTANICE DS1 pro testování kybernetické bezpečnosti: NÁVOD K OBSLUZE*. Ovčáry 299: ServisControl s.r.o, [b.r.].
20. LYON, Gordon. *Npcap: Packet capture library for Windows*. Dostupné také z: https://npcap.com/.
21. ROCKWELL AUTOMATION. FactoryTalk Policy Manager Getting Results Guide. In: Rockwell Automation, Inc., 2022, s. 45, 77. TALK-GR001C-EN-E, June 2022. Dostupné také z: https://literature.rockwellautomation.com/idc/groups/literature/documents/gr/ftalk-gr001_-en-e.pdf.
22. LUDWIG, Steve; HANSON, Leanne. Rockwell Automation Introduces First Industrial Control Devices to Support CIP Security. *Press Release*. 2018. Dostupné také z: https://www.rockwellautomation.com/en-cz/company/news/press-releases/Rockwell-Automation-Introduces-First-Industrial-Control-Devices-to-Support-CIP-Security.html.