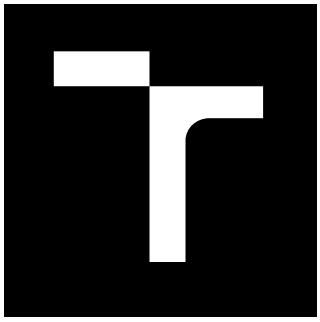


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

VYTVOŘENÍ PRŮMYSLOVÉHO SCÉNÁŘE S VYUŽITÍM WINCC UNIFIED

CREATING AN INDUSTRIAL SCENARIO USING WINCC UNIFIED

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Bohuslav Šotola**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Ondřej Pospíšil**

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Bohuslav Šotola ***ID:*** 220362

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Vytvoření průmyslového scénáře s využitím WinCC Unified

POKYNY PRO VYPRACOVÁNÍ:

V teoretické části se student zaměří na popis možností vizualizace pomocí WinCC Unified. Dále se zaměří na vzdálené ovládání procesů a popis možností komunikace za použití tohoto řešení. V návaznosti na to popíše možné bezpečnostní slabiny a jejich možná řešení. V praktické části student ověří funkčnost uváděnou výrobcem na konkrétním příkladě, který si sám zvolí. Vytvoří vlastní knihovnu HMI pro animaci a ovládání standardních funkčních bloků používaných v běžné průmyslové aplikaci (motor, ventil, analogové měření, digitální měření). Použije techniku tzv. faceplate – vyskakovacích oken, ve kterém budou vhodně sdruženy funkce pro animaci stavu zařízení, nastavení potřebných parametrů, zobrazení trendu a alarmů. Provede také analýzu zatížení komunikace mezi HMI a PLC (rychlost odezvy HMI) v závislosti na počtu animovaných objektů na HMI obrazovce. Implementuje do svého řešení také možnost vzdálené komunikace a provede detailní rozbor celé komunikace. Nakonec provede zachycení komunikace a následnou analýzu.

DOPORUČENÁ LITERATURA:

[1] DUNNING, Gary. Introduction to programmable logic controllers. 3rd ed. Clifton Park, NY: Thomson/Delmar Learning, c2006. ISBN 1401884261.

[2] STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, 2011, 800.82: 16-16

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 31.5.2022

Vedoucí práce: Ing. Ondřej Pospíšil

Konzultant: Ing. Martin Mierva

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Tato práce se věnuje tématu Vytvoření průmyslového scénáře s využitím WinCC Unified. WinCC Unified je vizualizační nástroj podporující vzdálený přístup přes web bez nutnosti instalace softwarů. Nutnost používání této technologie plyne zejména ze zavádění digitalizace a s tím spojeného zjednodušení průmyslových procesů.
Nejprve je probrána problematika vzdálené komunikace, po které následuje popis základních funkcí WinCC Unified. Následně jsou zpracovány různé scénáře komunikace, které jsou spolu s vytvořením HMI knihovny hlavním cílem bakalářské práce. Práce je ukončena tématem analýzy zatížení komunikace mezi HMI a PLC v závislosti na počtu animovaných objektů na HMI obrazovce.

KLÍČOVÁ SLOVA

WinCC Unified, ICS, HMI, PLC, analýza zatížení komunikace

ABSTRACT

This bachelor thesis is devoted to the Creation of industrial scenario by means of using WinCC Unified. WinCC Unified is a visualization tool supporting remote access via the web without the necessity to install softwares. The urgency for using this technology results in particular from the introduction of digitization and the associated simplification of industrial processes.
The issue of remote communication is discussed at first which is followed by a description of the basic functions of WinCC Unified. Then various communication scenarios are processed which are the main target of the bachelor's thesis together with the creation of the HMI library. The work is ended by the topic of analysis of communication load between HMI and PLC depending on the number of animated objects on the HMI screen.

KEYWORDS

WinCC Unified, ICS, HMI, PLC, analysis of communication load

Vysázeno pomocí balíčku `thesis` verze 4.07; `http://latex.feec.vutbr.cz`

ŠOTOLA, Bohuslav. *Vytvoření průmyslového scénáře s využitím WinCC Unified*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022, 110 s. Bakalářská práce. Vedoucí práce: Ing. Ondřej Pospíšil

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Bohuslav Šotola
VUT ID autora:	220362
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	Vytvoření průmyslového scénáře s využitím WinCC Unified

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Tímto bych chtěl poděkoval vedoucímu mé bakalářské práce panu Ing. Ondřeji Pospíšilovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Dále bych chtěl také poděkovat panu Ing. Martinu Miervovi za jeho věnovaný čas.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Tato bakalářská práce se zabývá vizualizačním nástrojem WinCC Unified, který podporuje vzdálený přístup přes web bez nutnosti instalace softwarů. Poprvé se objevil ve verzi 16 v programu Tia Portal.

Poté, co byla vydána druhá verze v17, je předpoklad, že jsou odladěny základní chyby. Tento nástroj si dává za cíl vzdálené ovládání podnikových strojů pomocí technologie HTML a JavaScript, tzn. že oprávněný uživatel bude smět ovládat stroje či konkrétní zařízení z jakéhokoliv místa na světě s dostupným internetovým připojením. I když tato technologie není zatím široké veřejnosti příliš známá, je zde velký předpoklad jejího využití pro mobilní zařízení, tablet či dokonce chytré hodinky. Pokud má být tato technologie úspěšná, bude nutné této oblasti věnovat velké úsilí.

Cílem bakalářské práce bylo ověřit funkčnost technologie WinCC Unified. Na jednoduchou úlohu naprogramovanou v programu Tia Portal v17 byly aplikovány dostupné metody a prvky. Dále byla vytvořena HMI knihovna pro animaci a ovládání standardních funkčních bloků používaných v běžné průmyslové aplikaci a také provedena analýza zatížení komunikace mezi HMI a PLC v závislosti na počtu tagů na HMI obrazovce.

Dalším cílem bylo provedení detailního rozboru celé komunikace prostřednictvím OPC UA servru. Limitujícími prvky práce je použití pouze dvou PC klientů, tedy nastává otázka, jak bude OPC UA sever reagovat na požadavky od více klientů. Dále není vyřešena otázka optimalizace vizualizací na chytré hodinky či mobilní telefony.

Hlavní cílem je nasazení WinCC Unified v průmyslové praxi. S tímto bodem úzce souvisí analýza komunikace mezi PLC a HMI, která si dává za cíl udržení spolehlivé komunikace v případě použití většího počtu animovaných objektů na HMI obrazovce. K uvedení WinCC Unified napomáhá vytvoření HMI knihovny, která má za úkol poskytovat operátorům informace o stavech zařízení.

Práce je složena z pěti kapitol. V první kapitole se pojednává o automatizační pyramidě a jejích úrovních. Následně je popsáno fungování SCADA systému v rámci podniku i mimo něj. Druhá kapitola obsahuje shrnutí zranitelnosti průmyslové sítě, možných útocích, které se mohou objevit a také o tom, co útokům předchází. Ve třetí kapitole je popsána bezpečnost a způsoby zabezpečení komunikace, vzdálená komunikace prostřednictvím VPN, cloudu a OPC UA a také je zde zmínka o šesti faktorech bezpečného použití OPC UA v průmyslové komunikaci. Čtvrtá kapitola se věnuje vizualizačnímu nástroji WinCC Unified a jeho rozdělení do tří platforem. V páté části Výsledky jsou prezentovány výsledky práce, kterých bylo dosaženo.

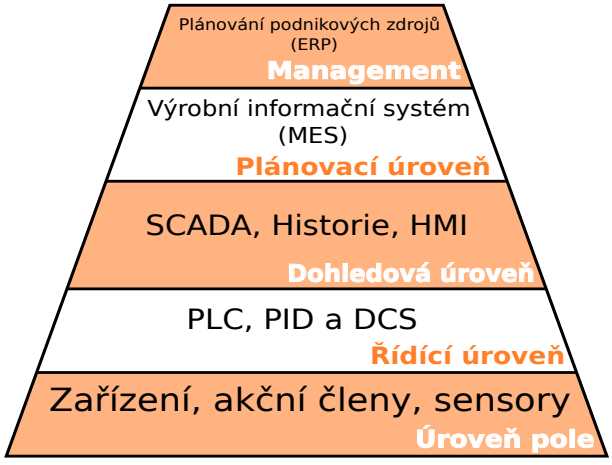
1 Úvod do průmyslových sítí a průmyslové komunikace

V dnešní době je průmyslová komunikace zásadním tématem pro zavádění Průmyslu 4.0, jehož cílem je propojení různých částí komunikace, zlepšení efektivity i dostupnosti strojů a dat, čímž je zvýšena konkurenceschopnost. Pracuje s předpokladem, že každý rok se zdvojnásobí propojení strojů a tím vzroste i objem přenášených dat a bude to znamenat enormní tlak na jejich zabezpečení. Pojmy průmyslová komunikace či průmyslové sítě můžeme shrnout jedním pojmem digitalizace. Ta nabízí spoustu nových příležitostí ve všech průmyslových odvětvích. Moderní a spolehlivé průmyslové komunikační sítě jsou předpokladem pro využití jejího velkého potenciálu, který bude možný pouze v kombinaci s výkonnou datovou komunikací. [33]

S digitalizací úzce souvisí systém WinCC Unified, kterému se tato práce věnuje především. Jedná se o vizualizační nástroj, který napomáhá digitalizaci a mezi jeho hlavní přednosti lze zařadit zejména škálovatelnost, jednoduchost nebo přístup odkudkoliv. [28]

1.1 Pyramida automatizace, průmyslový řídící systém

WinCC Unified je provázán s tzv. pyramidou automatizace, která je znázorněna na obr. 1.1. Pyramida automatizace slouží jako názorný příklad začlenění technologií do průmyslu [77].



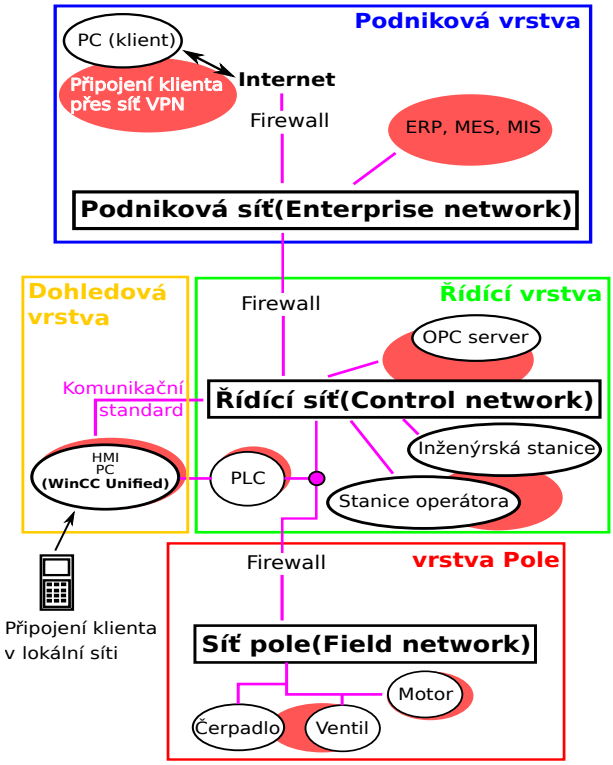
Obr. 1.1: Pyramida automatizace [78].

Automatizační pyramida je složena z pěti úrovní:

- 1. úroveň (nejnižší) – představuje úrověň pole, která je tvořena akčními zařízeními (např. ventily, čerpadla) a protokoly, které komunikují s řídící úrovní,

- 2. úroveň (řídící) – je tvořena programovatelnými logickými automaty (Programmable Logic Controller – PLC), ale v případě, kdy se jedná o složitější procesy, lze využít distribuovaný řídící systém (Distributed control system – DCS),
- 3. úroveň (dohledová) – slouží pro sběr dat, do této vrstvy je zařazen systém WinCC Unified,
- 4. (plánovací úroveň) – zahrnuje výrobní informační systém (Manufacturing Execution Systems – MES) poskytující přehled o stavu výroby či zaměstnancích,
- 5. úroveň (management) – plánování podnikových zdrojů (Enterprise Resource Planning – ERP), který sleduje zásoby, nákup, finance. [34]

Na obr. 1.2 je znázorněno obecné schéma průmyslového řídícího systému, sítě, která je aplikována v podnicích. Toto schéma je popsáno v podkapitolách níže.



Obr. 1.2: Průmyslový řídící systém.

Průmyslové řídící systémy (Industrial Control System – ICS) jsou široký pojem zahrnující systémy dohledové kontroly a získávání dat (Supervisory Control And Data Acquisition – SCADA), DCS, v neposlední řadě také PLC, průmyslovou automatizaci či řídící systémy (Industrial Automation and Control Systems – IACS) [5].

1.1.1 Úroveň pole a řídící

PLC bylo původně navrženo pro řízení jednotlivých strojů [15]. ICS může být založeno na více PLC, propojených dohromady za účelem předávání informací a dosažení centralizovaného řízení i monitorování. PLC funguje jako samotný řídicí systém a v případě jejich vzájemného propojení mohou v různých průmyslových odvětvích nahrazovat DCS. [5]

DCS byl navržen pro řízení mnoha strojů v továrně. Tím se odlišuje od PLC, kdy každé PLC řídí svůj vlastní stroj a v systému DCS jsou tyto stroje vzájemně propojeny. DCS lze integrovat s PLC na konkrétní proces jako např. rafinace ropy. I když se hranice mezi PLC a DCS stále více smazávají, tak jsou mezi nimi tyto zásadní rozdíly:

- DCS má delší dobu odezvy na změny,
- DCS zvládne několik tisíc IO bodů,
- DCS se používá v kritické infrastruktuře z důvodu redundance (záložní napájení) a také pro složitější aplikace, které vyžadují pokročilé řízení procesů. [15]

IACS představuje systém, který obsahuje bezpečnou infrastrukturu pro usnadnění komunikace, přenosu informací a chytrých zařízení pro sběr informací. IACS využívá kombinaci senzorů, hardwaru a softwaru k převedení informací ze senzorů na uživatelsky vhodné informace a jeho velkou předností je mimo jiné i schopnost zlepšení výroby nebo průmyslových procesů. [5]

1.1.2 Dohledová úroveň

SCADA je systém, který je schopen shromažďovat a zpracovávat data na velké vzdálenosti. Jeho velkou výhodou je schopnost hlásit informace na konkrétní místo, kde je vysoká šance úspěšného vyřešení. [5]

Rozvoj SCADA systémů přišel v průmyslově rozvinutých zemích v 60. letech 20. století. SCADA systém prochází již čtvrtou generací vývoje, kdy se izolované jednoúčelové systémy s vývojem počítačových sítí postupně transformovaly do podoby propojených stanic. V současné době probíhá tzv. generace internetu věcí (Internet of Things – IoT), kdy je pomocí internetu propojováno téměř vše. Zároveň lze pozorovat nástup cloudových služeb. [71]

Průmyslové organizace používají systémy SCADA k řízení, udržování efektivity anebo distribuci dat pro efektivnější rozhodování o problémech systému. SCADA systémy jsou používány v energetice (elektrárny), v oblasti potravin nebo segmentu ropy a plynu. Základní architektura SCADA koresponduje s obr. 1.2, ale kromě PLC smí být v architektuře použita i vzdálená jednotka terminálu (Remote Terminal Unit – RTU). Oba tyto prvky komunikují se senzory a HMI a následně informace směřují

do počítačů, kde je nainstalován software SCADA, který zpracovává a zobrazuje data, čímž pomáhá zaměstnancům data analyzovat a činit tak důležitá rozhodnutí. [69]

RTU je ve SCADA systému implementována na vzdáleném místě, kde se stará o sběr dat. Data jsou následně kódována do formátu vhodného pro přenos do systému. Pod pojmem HMI si lze představit například vizualizační software, který zobrazuje informace o procesech a umožňuje je ovládat buď z aplikace na PC či terminálu na stanovišti anebo také vzdáleně z okna webového prohlížeče na operátorské stanici. [70]

Průmyslové řídící systémy lze nakonfigurovat tak, aby fungovaly v režimu s otevřenou či uzavřenou smyčkou nebo v režimu manuálním. V případě, že je použit systém s otevřenou smyčkou, je výstup řízen pouze vstupem, tedy výstup nemá na chod systému žádný vliv. Jestliže je provedena konfigurace systému s uzavřenou smyčkou, tak výstup má schopnost měnit vstup. Systém v manuálním režimu je ovládán lidmi. Řídící systémy se používají v mnoha průmyslových odvětvích např. ve výrobě, distribuci anebo dopravě. [14]

Obecné komunikace průmyslového řídícího systému mohou probíhat tak, že senzor, zařízení měřící určitou veličinu, ji posílá kontroléru neboli PLC. PLC interpretuje signály a převádí je na odpovídající hodnoty, kterými následně řídí zařízení (motory, čerpadla či ventily). S PLC je propojeno rozhraní k monitorování a konfiguraci nastavených hodnot. Jedná se např. o SCADA systémy nebo HMI panely. [14]

Mezi SCADA systémy lze zařadit operátorskou a inženýrskou stanici. Jelikož se tato práce zabývá WinCC Unified, byl do schématu zakomponován i tento systém, který zároveň nahrazuje HMI panel. Rozdíl mezi operátorskou stanicí a stanicí inženýra je v míře oprávnění provádět změny systému, tedy inženýrská stanice má větší oprávnění než operátor. V obecném schématu se objevuje pojem OPC UA server/komunikace. Jedná se o komunikaci mezi PLC a WinCC Unified, ale tato problematika bude podrobněji popsána v kapitole nazvané Komunikace WinCC Unified prostřednictvím protokolů. Nad úrovní SCADA systémů potažmo WinCC Unified se nachází tzv. výrobní informační systém.

1.1.3 Plánovací úroveň

Do plánovací úrovně patří systém MES. Jedná se o softwarové řešení, které zvyšuje efektivitu nastolených procesů, monitoruje a synchronizuje výrobní procesy v jednotlivých závodech, které také propojuje. MES dále pomáhá eliminovat lidské chyby a tím dochází k pozitivnímu vlivu na kvalitu výrobků. Tento systém se využívá pro výrobu polovodičů, elektroniky nebo ve zdravotnictví. [65]

1.1.4 Management

Podle pyramidy automatizace lze použít i další nástroj a tím je ERP. ERP představuje rovněž software, který se stará o firemní finance, dodavatelský řetězec nebo provoz podniku na základě rad umělé inteligence. [66]

1.1.5 Rozdílnost ERP a MES

Rozdíly mezi ERP a MES lze pozorovat již v jejich samotných funkcích. ERP se zaměřuje na plánování a kvantitativní analýzu, kdežto MES se zabývá řízením výrobního procesu linky. Rozdíly mezi těmito nástroji lze spatřovat i v způsobu poskytování přehledů. ERP informuje uživatele až po určitém časovém období, MES poskytuje přehledy ihned. ERP není, na rozdíl od MES, integrováno přímo do podnikového stroje. [67]

1.2 Problematika vzdálené komunikace v průmyslových sítích

Pokud by se jednalo o vzdálenou komunikaci v rámci ICS, mluvíme většinou o SCADA systémech. Aplikování SCADA systémů v průmyslových sítích může být pojato ve dvou různých variantách. První variantou je, že SCADA bude fungovat pouze v rámci podniku. Druhou variantou je myšleno například propojení různých provozů sekcí podniků nebo připojování klientů ze vzdálených míst.

1.2.1 Fungování SCADA systému v rámci podniku

Fungování SCADA systému v rámci podniku si lze představit na tomto modelovém příkladu. Firma je rozdělena na několik oblastí (buněk) a každá oblast se zabývá různou formou výroby produktů. Poblíž každé oblasti je operátor, který dohlíží na správné fungování běžících procesů. Operátor může procesy ovládat buď pomocí HMI panelu, který se nachází hned vedle zařízení např. linky na míchání surovin anebo na stanici operátora. Nad množstvím stanic operátora jsou umístěny inženýrské stanice, které shromažďují a vyhodnocují informace ze stanic operátorů.

K tomu, aby operátoři a inženýři mohli ovládat spuštěné procesy, je nutné mít software, který bude prostřednictvím komunikačních protokolů komunikovat s PLC zařízeními potažmo akčními členy. To, který software bude vybrán, závisí na vybraném hardwaru, jelikož každá firma vyvíjí vlastní software k tomu, aby bez problémů fungoval na jejich hardwaru.

Firma SIEMENS, na jejíž produkt je tato práce zaměřena, nabízí pro ovládání hardwaru systém WinCC Unified ve verzích v16 a v17. Jelikož je WinCC Unified webová technologie, tak procesy jsou ovládány pomocí webového prohlížeče.

Na trhu jsou dostupné ale i jiné softwary např. PROMOTIC, MERVIS SCADA. PROMOTIC je zdarma ke stažení, ale maximální velikost naprogramované aplikace je 30 proměnných. Její využití je např. v energetice, klimatizaci či vytápění. [72]

Mervis SCADA je software, který umožňuje uživateli udržovat celkový přehled o stavu systému. Používá se u řídících jednotek Unipi. Mervis SCADA zajišťuje všechny nástroje pro vývoj a správu bezplatně, SCADA projekt lze vytvořit i bez hlubších znalostí. Je zde také možnost sledování a řízení provozu pomocí mobilní aplikace zdarma. [73]

1.2.2 Fungování SCADA systému i mimo prostředí podniku

Obecně SCADA systémy prostřednictvím příslušných softwarů (MERVIS SCADA, PROMOTIC, WinCC Unified) umožňují klientům vzdálené ovládání strojů a to i mimo prostory podniku. V praxi to může vypadat tak, že např. na inženýrské stanici bude vytvořen VPN sever a mimo prostory podniku se bude moci zákazník připojit jako VPN klient. Dále je možné využití softwaru UltraVNC, díky kterému se lze připojit na vzdálený počítač.

V průmyslu se čím dál více prosazuje vzdálená komunikace a to z důvodů několika faktorů. Jedním z nich je udržení provozu v chodu díky ochraně klíčových pracovníků. Pozitivem vzdálené komunikace může být i snižování provozních nákladů podniku nebo provádění technické podpory a servisu. Naopak nevýhodou vzdáleného připojení je, že pracovník nemusí mít k dispozici přístup ke všem hodnotám a parametrům. Další nevýhodou může být absence vzájemné komunikace lidí. Dále se objevuje otázka hrozeb hackerských útoků s využitím vzdálených přístupových bodů. I u sebelepšího systému nelze zaručit, že nedojde k závažným incidentům ohrožující data firmy. Jako optimální se jeví kombinace vzdáleného i fyzického přístupu, zvláště pak v oblasti revizí a kontrol. [25]

2 Zranitelnosti průmyslových sítí

Poté, co se zvedá povědomí o SCADA systémech, narůstá jejich náchylnost ke kybernetickým útokům. Zařízení v minulosti nebyla připojována k síti a v případě, že dojde k jejich masivnímu propojení, stávají se náchylnými k útokům. [12]

Obecně jsou rozlišovány dvě kategorie bezpečnostních rizik. První kategorie je tvořena cílenými útoky z vnějšího prostředí, kde největší slabinou je absence šifrovaného spojení. [13]

Útočník může využívat útoků jako je např. odepření přístupu (Denial of Service – DoS), který dokáže přetížit síť a v případě nedostatečně výkonného firewallu dochází ke zpomalení komunikace [12].

Nedostatečně zabezpečené sítě mohou být využity útočníky k zašifrování komunikace s následným vymáháním výkupného. Pro lepší zabezpečení sítí můžeme využít nástroje monitorování datových toků. Tato technologie poskytuje informace o síťové komunikaci ve formě IP toků (kdo s kým komunikuje, kolik dat bylo přeneseno, na jakých portech komunikace probíhá). Z monitoringu datových toků je možné získat informace o infikované stanici, nežádoucího síťového provoz nebo podezřelé aktivity uživatelů. [13]

Druhá kategorie je tvořena tzv. útoky v budově. Může se jednat např. o útok zaměstnance, kdy může odcizit kritická data firmy. Jako řešení můžou být použity přístupy viz kapitola Zabezpečení závodu.

Pokud se jedná o absenci šifrovaného spojení, tak v případě WinCC Unified je šifrování řešeno protokolem TLS 1.2, ECDHE RSA s P-384 a AES 256 GCM.

V rámci internetu je TLS nejrozšířenějším protokolem. Poskytuje tzv. koncové zabezpečení proti aktivnímu útočníkovi. TLS je univerzální, tedy je možné jej použít na všechny druhy aplikací. Obsahuje protokol TLS Handshake, který je zodpovědný za ověření identity a dále protokol TLS Record, který implementuje klíče za účelem ochrany dat. [60]

Komunikace klient/server je inicializována klientem, který je připojen k serveru přes příslušný port a posílá mu tzv. TLS Client Hello. Poté, co je dokončen TLS Handshake, klient může iniciovat první http dotaz. Všechna http data jsou nadále posílána pod označením data aplikace (application data). V případě ukončení spojení TLS poskytuje možnosti pro bezpečné uzavření komunikace a tím je zajištěno, že nebudou přijímána data. Před samotným uzavřením komunikace je funkce MUST povinna vyslat upozornění. Poté funkce MAY uzavře komunikaci bez jakéhokoliv čekání na opověď serveru. [61]

P-384 je standardní eliptická křivka, která poskytuje 192 bitové zabezpečení. Její použití je zejména v oblasti výpočtu digitálních podpisů a protokolů pro dohodu o klíči. Kromě této eliptické křivky jsou známé P-192, P-224 a P-256. [62]

AES-256-GCM představuje komunikační standard s 256 bitovým klíčem. GCM je režim provozu, který slouží k vytvoření AEAD algoritmu. [63]

Pro prevenci případného útoku a k ochraně hlavních aktiv je také možné aplikovat vrstevnatou tzv. hloubkovou strategii ICS, která má základy ve vojenské strategii. K tomu, aby mohla být tato strategie aplikována, musíme mít povědomí o slabých místech sítě. Následující útoky a metody narušení systému mohou útočníkům bez aplikování hloubkové ochrany umožnit snadný přístup k datům a manipulaci s nimi. První hrozbou může být útok na zařízení připojené k síti přímo z internetu, také se může jednat o vyzrazení přihlašovacích údajů některým z pověřených zaměstnanců, v neposlední řadě mohou být provedeny útoky vložením infikovaného mobilního média do systému nebo zasláním podvodného emailu. Při aplikování hloubkové strategie je třeba brát v úvahu náklady s tím spojené, především náklady na zabezpečení starších systémů či náklady spojené s trendem připojování řídících systémů do podnikových sítí. Obranu do hloubky si lze představit jako kombinaci lidí, technologie, operací a povědomí o útočníkovi. Nutností je také upravování a zdokonalování ochrany před již známými, tak i novými hrozbami. Jsou proto doporučovány strategie, které jsou složeny z devíti celků. Jednat se může např. o tzv. Program řízení rizik, kam je možné zařadit např. systém identifikace hrozeb a jejich charakterizování či udržování inventáře aktiv. Dále je nutné zmínit strategii založenou na lidském elementu, kam je zařazeno školení zaměstnanců, aplikované postupy a opatření. [1]

2.1 Anatomie útoků na průmyslové systémy

Než se organizace rozhodne, jaký typ ochrany zvolí pro své prostředí ICS, je důležité porozumět metodám, které používají útočníci k útoku na systémy. Kybernetický útok je proveden poté, co útočník prozkoumá systém a odhalí jeho slabé stránky. [1]

Odhalování slabých stránek je prováděno na základě útočníkova průzkumu sítě, tzn. útočník zjišťuje, zda-li existuje firewall a nějaké otevřené komunikační porty. Cílem je najít jakékoliv slabé místo systému. Mohou být také získány veřejně dostupné informace např. jména a e-mailové adresy zaměstnanců či jejich fotografie. [1]

Pro provedení útoku jsou používány běžné metody, mezi které patří např. využívání slabého ověřování identit, metody síťového skenování, zneužití přístupového oprávnění či odesílání emailů vysoce postaveným zaměstnancům. [1]

Příkladem útoku pomocí emailů může být BlackEnergy, který je zaměřen na HMI systémy a využívá tzv. sociální inženýrství k tomu, aby uživatele přiměli otevřít e-mail nebo přílohu dokumentu, která vloží infikovaný spustitelný soubor na cílový počítač, což následně vede k instalaci škodlivého softwaru. [1]

Správa adres v síti je zásadní pro efektivní provoz. ARP protokol zaručuje správné směrování pomocí mapování sítě a při použití tabulek ARP je v síti zajištěno správné směrování provozu. Hlavním cílem útočníka je právě manipulace s tabulkami ARP, protože jejich otrava zajistí útočníkovi směrování veškerého síťového provozu na počítač, který byl útočníkem infikován. [1]

Jedním z možných řešení snížení rizika pro sítě a systémy může být antivirus, který ale nemusí vždy znamenat nejlepší řešení. Některé aplikace jsou velmi citlivé na časové zpoždění, uživatel tak tímto krokem může zabránit optimálnímu výkonu systému. [1]

Organizace při tvorbě zabezpečení mohou také využít řadu bezpečnostních a rizikových standardů či pokynů pro organizace. Normy se vztahují na organizaci v závislosti na sektoru kritické infrastruktury. [1]

3 Bezpečnost

Základem digitalizace je bezpečná výměna dat mezi provozní sítí (Operational Technology – OT) a sítí informační (Information Technology – IT) [24]. Provozní sítě představují větší bezpečnostní riziko, jelikož jejich bezpečnost byla postavena na tom, že nebyla součástí veřejné sítě [35]. Bezpečnost informačních sítí je zaměřena na pravost dat, přímé cloudové připojení, dynamickou komunikaci mezi serverem a klienty a také ochranu před útoky hackerů. Provozní sítě jsou zaměřeny na ochranu strojů a osob, založené na tzv. koncepci víceúrovňové ochrany, která je složena ze tří úrovní. [24]

První úrovní je integrita systému (SYSTEM integrity), tvořená např. rozdílností oprávnění mezi operátorem a klientem. Druhou úrovní je zabezpečení závodu (Plant security) např. přístup do budovy, video monitoring. Poslední úroveň představuje síťová ochrana (Network security), kam patří ochrana firewally a použití VPN sítí, která je popsána níže. [26]

3.1 Zabezpečení závodu

Jednou z možností, jak předejít neoprávněné manipulaci s daty či částmi zařízení, je kontrola přístupu osob do budovy. Zabezpečení může být na bázi čipů nebo karet. Jako ochranný prvek může posloužit i přítomnost kamer pro případné dohledání útočníka. Do kategorie *Zabezpečení závodu* můžeme zařadit i tzv. *Ochranu projektu (Project protection)*. Tato funkce je součástí Tia portálu verze 16, tak i verze 17. Project protection chrání projekt v Tia portálu před neoprávněnými úpravami projektu. Tuto možnost lze nastavit v záložce *Bezpečnostní nastavení (Security settings)*.

Dalším vhodným bezpečnostním nástrojem je archivace dat, která nám umožňuje uchovat citlivá data z hlediska dosažení potřebné kvality služeb.

3.2 Vzájemná komunikace zařízení

Pro vzájemnou komunikaci zařízení je nutné používat určité komunikační protokoly. Komunikace může být např. formou PLC – PLC, PLC – HMI, PLC – koncové prvky nebo také SCADA – PLC, jedná se tedy o vzdálenou komunikaci. V případě komunikace PLC – PLC je možné použít protokoly Profinet a Profibus. Poslední zmíněný bývá používán pro vysokorychlostní cyklickou datovou komunikaci [6].

Profibus začal být vyvíjen již v roce 1987 a o dva roky později byla představena jeho první verze Profibus FMS [11]. Postupným vývojem vznikla druhá verze nazvaná Profibus PA, která se používala pro oblast řízení spojitých technologických procesů, v průmyslových odvětvích např. pro úpravu vody, ropy, plynu, atd [6]. Dále

je na trhu i vysokorychlostní verze Profibus DP, která je používána pro automatizaci továren [6]. Protokol Profinet byl v 90. letech s rozšířením ethernetu do průmyslu [44].

Profinet je plně duplexní systém, ve kterém je využíváno zapojení hvězdicové topologie nebo zapojení několika hvězd připojených na kruhovou páteřní síť. Jeho výhodou oproti Profibus je mnohem vyšší přenosová rychlost. [6]

Délka propojovacího kabelu může dosahovat až sta metrů s téměř neomezeným množstvím stanic. Protokoly Profibus a Profinet se z ekonomického hlediska zásadně neliší, projektování a montáž jsou téměř stejné i použité komponenty jsou velmi podobné. [11]

Pro případnou komunikaci PLC – HMI je možné použít protokoly Ethernet/IT či Profibus. Pokud jde o srovnání Ethernet/IP a Profinet, tak Ethernet/IP je založen na protokolu CIP, kdežto Profinet vychází z Profibusu. Ethernet/IP se dle Knighta stává u uživatelů oblíbenější. [45]

Profinet je rychlejší než Ethernet/IP a nejčastěji je nasazován se standardním hardwarem. Ethernet/IP má lepší schopnost spolupráce, protože je založen na objektově orientovaném programování a spoléhá na komerční běžně dostupné komponenty. [46]

Ke komunikaci PLC – HMI je dále možné použít protokol Modbus, který je založen na architektuře klient/server a pracuje na bázi Ethernetu a mezi jeho výhody lze zařadit jednoduchost, rychlost a snadnou implementaci. Rovněž je schopný přenosu dat mezi zařízeními různých výrobců. [47]

Po nástupu Ethernetu byl Modbus přeřazen do relační vrstvy pod verzi Modbus/TCP [48]. Dalšími verzemi protokolu Modbus jsou Modbus RTU, Modbus ASCII, Modbus Plus [49].

Pro komunikaci PLC-koncová zařízení lze použít protokol DeviceNet, nekomunikující přímo s I/O moduly, ale komunikace probíhá prostřednictvím tzv. DeviceNet skeneru. DeviceNet se řídí modelem ISO/OSI, který používá sedm vrstev. Je založen na protokolu CIP využívajícím tři horní vrstvy CIP, tedy vrstvu relační, prezentační a aplikační. DeviceNet je schopen dosahovat přenosových rychlostí 125, 250 nebo 500 kilobitů za sekundu. Mezi výhody DeviceNetu lze zařadit nízké náklady, vysokou spolehlivost nebo efektivní využití šířky pásma sítě. Naopak jeho nevýhodou je omezená šířka pásma, omezená velikost zprávy a problémy způsobené kabeláží. [50]

Komunikace PLC – koncové zařízení může být postaveno také na protokolu IO-Link. Jde o obousměrný protokol typu bod-bod, fungující na krátké vzdálenosti. Koncová zařízení, akční členy nebo senzory jsou připojovány k nadřazenému zařízení IO-Link, které následně komunikuje s PLC. Spojení koncová zařízení – nadřazené IO-Link zařízení je navázáno prostřednictvím nestíněného třívodičového kabelu o délce do 20 metrů. [51]

Pro komunikaci SCADA – PLC můžeme využít předchozí protokoly např. Modbus, Profibus, Profinet či Ethernet/IP, nicméně v poslední době se do popředí dostává protokol OPC UA. OPC je komunikační standard pro aplikace, které jsou zaměřeny na monitorování a řízení procesů a jsou založeny na architektuře klient/-server. [52]

Úkolem OPC je zabránit závislosti softwaru (monitorování, řízení) na výrobci hardwaru. Standard OPC je vytvářen a udržován prostřednictvím volně přístupné technické dokumentací tzv. specifikací OPC. [53]

Existuje několik verzí protokolů OPC, mezi které patří OPC DA, OPC AE, OPC HDA a jsou zařazeny pod jedním názvem OPC Klasik. Dále je tu i nová verze OPC UA. V OPC Klasik jsou definovány přístupy k procesním datům (Open Platform Communications Data Access – OPC DA), historickým datům a alarmům (Open Platform Communications Alarms and Events – OPC AE). OPC UA definuje pouze formát předaných zpráv. [54]

OPC UA a OPC DA se neliší pouze ve verzi protokolu. OPC DA podporuje DCOM komunikaci (zajišťuje, že se uživatel bude moci připojit k serveru vzdáleně) pro propojení klienta a serveru, kde DCOM je závislý na operačním systému a podporuje pouze operační systém Windows. Dále disponuje nedostatečným zabezpečením, je náchylný na některé sofistikované viry a malware, přičemž tento bezpečnostní problém je řešen až v OPC UA a také přistupuje pouze k aktuálním datům, není schopen generovat alarmy, historické události, zatímco OPC UA tyto funkce podporuje. OPC UA je nezávislý na platformě Windows, ale také podporuje platformy jako Linux nebo Apple. [55]

OPC HDA (přístup k historickým datům OPC) je naopak používán k výměně archivovaných procesních dat. V kontrastu s přístupem OPC HDA je specifikace OPC DA, která se naopak zabývá daty v reálném čase. Jelikož je technologie OPC rovněž založena na architektuře server/klient, OPC klient je schopen pomocí OPC HDA získávat data z datového zdroje. [56]

Dalším standardem je OPC AE. Specifikace OPC AE řeší problematiku výměny alarmů a událostí v reálném čase za použití společného komunikačního standardu. Alarmy a data událostí v reálném čase obsahují stavy z akčních zařízení, operátoři následně mohou provádět řízení stroje, linky či podniku. [57]

3.3 Síťová ochrana

Jedna z cest jak zabezpečit komunikaci je nástroj *HMI spojení*, které se nachází v *HMI RT 2 -> Connection* viz obr. 3.1.

Obr. 3.1: Bezpečnost HMI spojení.

Cílem je zabezpečit komunikaci mezi počítačem a PLC. Pokud se útočníkovi podaří proniknout do komunikace, může manipulovat s daty.

Do oblasti síťové ochrany můžeme zařadit i hardwarové prostředky od firmy SIEMENS např. průmyslové routery kabelové i bezdrátové. Routery nám umožňují bezpečný vzdálený přístup a bezpečnost datových přenosů. [27]

3.3.1 Problematika vzdálené komunikace – VPN

VPN je technologie, která chrání uživatele na internetu [16]. VPN sítě mohou být vytvořeny za pomoci softwaru, hardwaru nebo jejich kombinací [17]. Umožňuje vytvářet zabezpečené připojení mezi dvěma počítači nebo mezi počítačem a sítí. Tato technologie znemožní útočníkům odposlouchávat vaši komunikaci či zamezí ztrátě dat. [16] Na VPN jsou kladeny bezpečnostní požadavky, mezi které lze zařadit např. ověření totožnosti účastníků komunikace, zda má uživatel oprávnění k uskutečnění operace nebo šifrování komunikace [17].

V sítích VPN se nejčastěji používají tunelové a šifrovací protokoly. U tunelování se využívá principu vložení původního paketu do nového, a tím se stane pro síť neviditelný. O proces vkládání a rozbalení se starají protokoly např. PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Lyer 2 Tunneling Protocol). [8]

PPTP protokol je rozšířením protokolu PPP a jeho šifrování zajišťuje šifrovací protokol MPPE (Microsoft Point-to-Point Encryption). Síťový protokol PPP je používán pro správu spojení klienta a serveru, také se stará o zapouzdření IP paketu do rámců PPP. [36]

Protokol L2F umožňuje, na rozdíl od PPTP protokolu, aplikování protokolů ATM a Frame Relay k sestavení tunelu. Poskytuje také autentizaci koncových bodů

tunelu. Další protokol L2TP vznikl spojením výhod protokolů PPTP a L2F. [8] Protokol L2TP je nejčastěji používán pro přenos paketů pomocí UDP protokolu a nabízí oproti PPTP vytváření vícenásobných tunelů mezi dvěma hostitelskými počítači. [37]

Poté co je vytvořen tunelovými protokoly tunel, je nutné použít šifrování k jejímu zabezpečení např. pomocí MPPE, IPSec šifrování či SSH šifrování. Pro zabezpečení sítě může být použito symetrické anebo asymetrické šifrování. [8] V symetrickém šifrování je k šifrování a dešifrování pouze jeden společný klíč [18]. Jednou z výhod symetrické kryptografie je menší výpočetní náročnost [38].

Nevýhodou je, že se klíč musí nějakým způsobem dostat k oběma stranám komunikace, pro přenos šifrovacího klíče je třeba použít zabezpečený přenos. Další nevýhodou je také to, že používaný klíč je bezpečný jen do té doby, dokud jej nevlastní nějaká třetí strana. [8]

V případě asymetrického šifrování je použit veřejný a privátní klíč. Veřejný klíč je přístupný všem komunikujícím, je však nutné, aby jej nebylo možné změnit. Privátní klíč májí pouze komunikující, nesmí být nikde zveřejněn. Výhodou je, že se nemusí přenášet klíč k dešifrování. Jeho nevýhodou může být větší časová náročnost. Odesílatel zprávu zašifruje prostřednictvím veřejného klíče tak, aby jí byl příjemce schopen dešifrovat pouze privátním klíčem. [18]

3.3.2 Problematika vzdálené komunikace – Cloud

K PLC se lze připojit i pomocí cloud technologií. Na trhu už jsou řešení připojení PLC na cloud a to pomocí cloud – VPN routerů. Cloudové služby jsou mnohdy v nabídce přímo od výrobců průmyslových zařízení, komponent nebo řídících jednotek, což zvyšuje důvěryhodnost v tuto službu. [25]

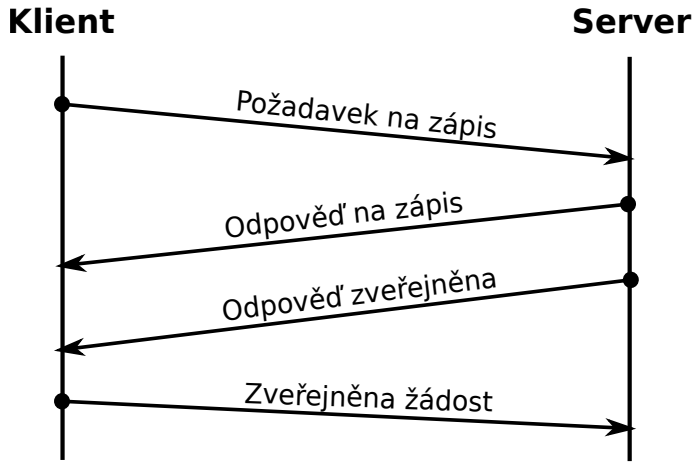
Výhody Cloudových uložišť jsou dostupnost dat na jakémkoliv místě v jakýkoliv čas, data jsou automaticky poskytována dle potřeb odběratelů a je zde možnost připojení pomocí standartních klientských platforem [39]. Nevýhodou cloudu je zahrnutí poskytovatele cloudových služeb do komunikace, za které je nutné průběžně platit [25]. Dále je zde možné omezení z hlediska předpisů a bezpečnosti [40].

3.3.3 Problematika vzdálené komunikace – OPC UA

OPC UA komunikace je založena na navazování spojení, zabezpečení komunikace a na předávání dat mezi OPC UA klientem a OPC UA serverem. OPC UA protokol je architektura orientovaná na služby, jsou v něm definovány služby, na které se klient může dotazovat a server na každý dotaz reaguje příslušnou odpovědí. [3]

Jeden z takových dotazů, které může klient požadovat je tzv. Požadavek na zápis (Write Request) viz obr. 3.2. Tento požadavek na server nastává tehdy, pokud

klient chce změnit hodnotu určitého tagu. Komunikace prostřednictvím protokolu OPC UA kromě změn určitého tagu obsahuje i další služby.



Obr. 3.2: Dotaz klienta, požadavek na zápis.

Otevření zabezpečeného kanálu

Služba *Otevření zabezpečeného kanálu (Open Secure Channel)* je používána pro otevření nebo obnovení zabezpečeného kanálu (Secure Channel) v průběhu komunikace. Každý zabezpečený kanál je charakterizován svou jedinečností pro konkrétní spojení uživatele (klienta) a serveru. Zabezpečený kanál obsahuje tzv. bezpečnostní symboly (Security tokens), které se starají o šifrování dat. Bezpečnostní symboly jsou však časově omezené a úzce spojeny s vypršením platnosti zabezpečeného kanálu, jelikož právě poslední symbol ukončí platnost zabezpečeného kanálu. Zabezpečený kanál může být také ukončen na žádost uživatele. Ke službě *Otevření zabezpečeného kanálu* lze zařadit zprávy *Žádost o otevření zabezpečeného kanálu (Open Secure Channel Request)* a *Odpověď o otevření zabezpečeného kanálu (Open Secure Channel Response)*. Obě tyto zprávy musí být podepsány soukromým klíčem odesílatele. Tento požadavek je platný pouze pro zabezpečené spojení, tudíž není použito nastavení *None*. [4]

Mezi hlavní parametry služby *Otevření zabezpečeného kanálu* lze zařadit ID zabezpečeného kanálu (SecureChannelId), který v případě nově vytvořeného Secure Channelu musí mít parametr roven nule. Dále je možné ze zachycené komunikace zjistit tzv. Request Header, který má rovněž hodnotu nula. Zásadní informaci poskytuje také tzv. Security Mode, která informuje o použitém stupni zabezpečení. Jedním ze stupňů zabezpečení může být *None*. [4]

Zavření zabezpečeného kanálu

Zavření zabezpečeného kanálu (Close Secure Channel) je použito pro ukončení služby *Zabezpečení kanálu* a tento požadavek musí mít stejný identifikátor kanálu jako při jejím navázání. Parametry u požadavku na *Zavření zabezpečeného kanálu (CloseSecureChannelRequest)* jsou např. RequestHeader, SecureChannelId. [4]

Vytvoření relace

CreateSession je použita klientem k vytvoření relace. Následně server odešle dva hlavní parametry a to sessionID a autentizační symbol. Relace ID je používána k identifikaci relace a autentizační symbol slouží k přidružení příchozího požadavku k relaci. [4]

K vytvoření relace dojde až po požádání uživatelem o službu Activate Session. Server může relace automaticky ukončit, jestliže uživatel nepožádá o službu serveru během časového limitu, který je uveden v paketu s názvem Create Session Response (jde o parametr Revised Session Timeout). Relaci může ukončit i uživatel pomocí služby Close Session. Pokud dojde k ukončení relace, nevyřízené požadavky budou přerušeny a uživateli budou zaslány stavové kódy. [4]

Achitektura OPC UA

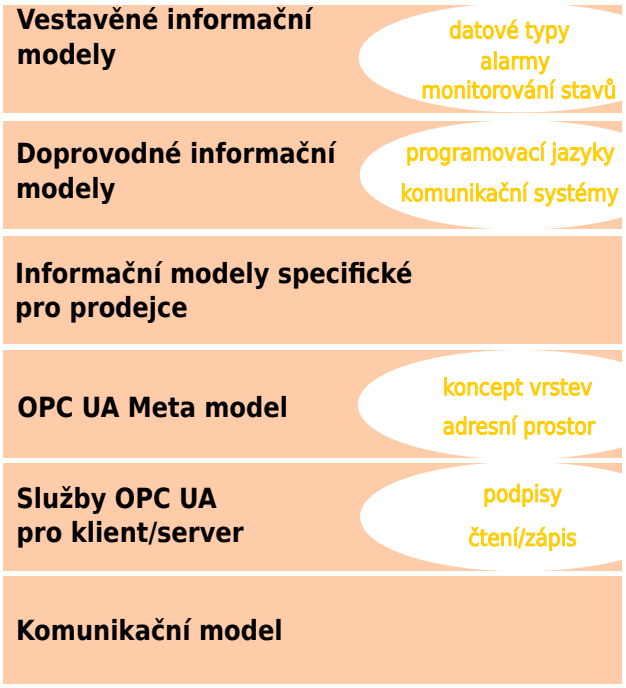
OPC UA Meta Model – je základním kamenem OPC UA informačního modelu, definuje koncept vrstev informačního modelu a pravidla, jak vystavět objektově orientovaný adresní prostor, který je složen z několika informačních modelů (např. informační model pro správu zařízení, pro funkčnost zařízení, model pro alarmy a stavy zařízení). [2]

Vestavěné informační modely – poskytují strukturu pro všechny informační modely využívající OPC UA, definuje např. typy objektů, datové typy nebo vstupní body adresního prostoru [2].

Doprovodné informační modely – jsou specifické pro konkrétní zařízení, definují např. programovací jazyky či komunikační systémy [2].

Informační modely specifické pro prodejce – jsou rozšířeny o specifické funkce prodejce, specifické funkce nepokrývají standardní model [2].

Služby OPC UA pro klient/server – představují možné interakce mezi aplikacemi klientskými a serverovými na základě komunikace typu žádostí/odpověď (např. čtení a zápis hodnot do tagů, dostupné nastavení zabezpečení) [2].



Obr. 3.3: Architektura OPC UA [2].

Komunikační model

Komunikace v OPC UA probíhá na základě komunikačního modelu, který je složen z transportní, komunikační a aplikační vrstvy [3].

Transportní vrstva – zajišťuje odesílání a příjem zpráv, používá šifrovací algoritmy a ověřovací mechanismy potřebné k zajištění bezpečnosti zprávy. Transportní vrstva je inicializována ihned po úspěšném navázání spojení. V této vrstvě jsou podporovány protokoly typu HTTP/SOAP, HTTPS nebo TCP/IP. [3]

Komunikační vrstva – funguje jako zabezpečený kanál mezi klientem a serverem. Zabezpečený kanál je vytvořen po navázání komunikace. Jakým způsobem je kanál vytvořen, závisí na použitém komunikačním protokolu. Následně je vytvořen identifikátor kanálu a bezpečnostní známka, kterými je kanál identifikován. Identifikátor kanálu je trvalý, známka má životnost omezenou a po jejím vypršení spojení končí. [3]

Aplikační vrstva – je zastoupena relacemi, ve kterých probíhá zpracování požadovaných služeb a volání. Relace jsou použity k identifikaci komunikace i autorizaci a při jejich vytváření předá klient serveru přihlašovací údaje. Následně server přidělí klientovi práva na vykonávání příkazů. Komunikačnímu kanálu může být přiřazena

maximálně jedna relace. Po vytvoření relace je třeba ji aktivovat. Relace se může uzavřít v případě určité doby nečinnosti. [3]

Důvod nasazení, výhody a problémy OPC UA

OPC UA je nasazováno pro tzv. komunikaci od stroje ke stroji, zvláště pak pro komunikaci od stroje ke cloudu [19]. Komunikací od stroje ke stroji si lze představit komunikaci koncového zařízení s aplikací. Jako příklad je možné uvést komunikaci motoru s WinCC Unified.

Jedním z důvodů vzniku OPC UA byla nezávislost na operačním systému, jak už bylo zmíněno dříve, jednodušší vzájemné propojení zařízení a bezpečnost dat. OPC UA se stává čím dál častějším artiklem, jeho použití nespadá pouze pod PLC systémy, nýbrž se začíná objevovat i u CNC systémů nebo routerů. [20]

Jednou z devíz OPC UA je navýšené množství přenášených dat, které jsou schopné si stroje mezi sebou vyměnit, tím dochází ušetření času a redukci nákladů. OPC UA lze implementovat na již zavedený průmyslový ethernet. Rovněž lze tímto protokolem propojit nejen různé typy komponent (PLC, HMI, RFID systém, SCADA), ale i např. průmyslové závody. [19]

Naproti tomu je zde nutné uvést častou příčinu s kompatibilitou OPC UA a starších verzí např. při převodu dat z OPC UA serveru do OPC DA klienta. Problémem je, že OPC UA se do zařízení dostává postupně a tak starší zařízení tento protokol nepodporují. Neznámou OPC UA protokolů může být reakce OPC UA serveru při velkém množství připojených klientů, tedy problém vypořádat se s velkým množstvím dotazů klientů. [20]

Aplikování technologie OPC UA

Digitalizace průmyslových systémů má za následek řešení bezpečnostních výzev, které je nutné řešit z důvodu zabránění potenciálních škod v podobě odcizení citlivých dat organizace. Za účelem dokumentování a informování o osvědčených postupech pro zabezpečenou komunikaci a pro lepší pochopení role OPC UA byla vytvořena skupina M2M Alliance a OPC Foundation, která vydala příručku dávající si za cíl zlepšení aplikování technologie OPC UA v průmyslových podnicích. Příručka například poskytuje přehled možných protiopatření, která jsou dostupná v OPC UA a dále popisuje situaci úrovně zabezpečení v době sestavení příručky. Například v roce 2015 Spolkový úřad pro informační bezpečnost provedl bezpečnostní analýzu OPC UA. Analýza ukázala, že OPC UA poskytuje vysokou úroveň zabezpečení, jelikož nebyly zjištěny žádné systematické chyby. Výsledky této analýzy pomohly vylepšit specifikaci OPC UA vydané skupinou M2M Alliance a OPC Foundation.

OPC UA se mimo jiné zabývá konceptem důvěryhodných informací (CIA triáda) nebo řízením přístupu (AAA rámec). [7]

CIA triáda

CIA triáda představuje důvěrnost, integritu a dostupnost. Tyto principy tvoří základní bezpečnostní infrastrukturu každé organizace. Důvěrnost představuje postup, jak udržet data v soukromí a zabránit jejich neoprávněnému prozrazení. Tímto postupem lze zařídit přiřazení oprávnění konkrétním osobám. Princip důvěrnosti může být narušen např. přímými útoky k získání neoprávněného přístupu, za účelem manipulace s daty. Dále může být použito skenování či odposlech sítě prostřednictvím útoku typu man in the middle. Důvěrnost lze ztratit i neúmyslnou lidskou chybou. Další částí CIA triády je již zmíněná integrita. Jedná se o zajištění pravosti dat, tzn. že s daty nebylo manipulováno a jsou tím pádem spolehlivé. I tento postup lze obejít, jednat se může především o manipulaci se systémy detekce narušení či o úpravu konfiguračních souborů. Jako protiopatření k těmto útokům lze použít šifrování hashování či digitální certifikáty. Poslední část je tvořena dostupností. Ta zajišťuje oprávněnému uživateli včasný a spolehlivý přístup ke zdrojům. Dostupnost může být ovlivněna životností hardwaru nebo selháním softwaru. Nejznámější útok provedený na dostupnost je útok typu odepření služby (denial of service), při kterém je úmyslně snížen výkon služby. Protiopatření zachovávající dostupnost je např. redundance, odolnost proti chybám hardwaru nebo pravidelné opravy softwaru.[68]

Řízení přístupu, monitorování aktivit uživatele

Řízení přístupu je složeno z autentizace pomocí jména a hesla nebo pomocí certifikátu X.509, dále z oprávnění ke čtení, zápisu hodnot podle práv a třetí složkou je monitorování aktivit. [7]

V případě autentizace se nemusí jednat jen o prokazování jménem, heslem či certifikátem, ale mohou být použity biometrické testy nebo přístupové karty[22].

Jak bylo zmíněno výše, tak autentizaci lze provést pomocí certifikátu X.509. Jedná se o certifikát s vlastním popisem, tedy certifikát vytvořený a podepsaný samotným uživatelem. X.509 definuje standard, tedy jaký formát bude mít certifikát. Certifikát je tvořen veřejným klíčem, informací o identitě osoby a dále také i dobu platnosti. Veřejný klíč zde má za úkol podepisování a šifrování komunikace se vzdálenou stranou. [7]

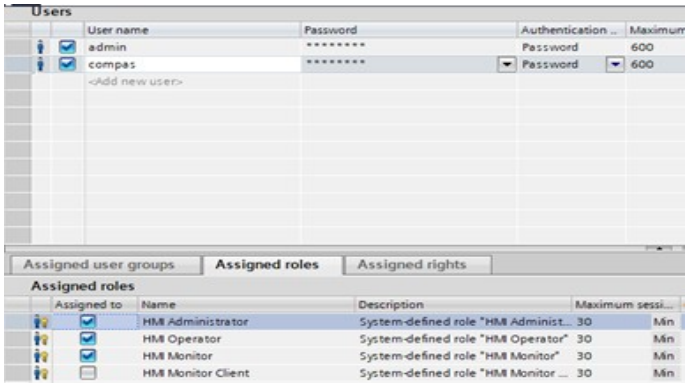
Pokud se jedná o monitorování aktivit, té je možné dosáhnout pomocí např. správy bezpečnostních informací a událostí. Na základě znalostí, k jakým souborům uživatel přistupuje, může být následně upraveno jeho oprávnění. [22]

Šest faktorů bezpečného použití OPC UA

Výstupem již zmíněné příručky je tzv. šest faktorů bezpečného použití OPC UA v průmyslové komunikaci. Jako první faktor je zmíněn tzv. bezpečnostní mód (Security mode). Bezpečnostní mód je použit z důvodu ochrany integrity a důvěrnosti dat. Zde je doporučován režim podpisu (Sign) nebo režim podpis a šifrování (SignandEncrypt). Druhým a třetím faktorem jsou výběr kryptografických algoritmů a tzv. autentizace uživatele. Při výběru kryptografických algoritmů by měla být minimální bezpečnostní politika 'Basic256Sha256', ale pouze pokud je tato politika podporována jak klientem, tak i serverem. U autentizace uživatele je zmiňován tzv. anonymní identifikátor, který by se měl používat pouze pro přístup k nekritickým zdrojům dat, jelikož nejde vysledovat osobu, která je zodpovědná za změnu dat nebo konfigurace. Čtvrtým faktorem je úložiště certifikátů a soukromých klíčů. Tady je zmiňováno nebezpečí ukládání soukromých certifikátů v nešifrovaném systému souborů. Dalším faktorem je použití certifikátů. V této oblasti je kladen důraz na neakceptování připojení, pokud se nejedná o důvěryhodné certifikáty. Posledním faktorem je správa a údržba certifikátů, tím je myšleno, že seznamy důvěryhodných certifikátů by měli vlastnit pouze osoby pověřené. Seznamy je nutné dále aktualizovat. [7]

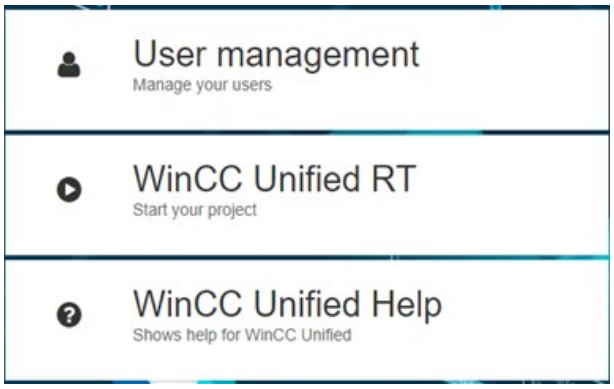
3.4 Integrita systému

Do této oblasti je zařazeno například oprávnění uživatelů. V Tia Portálu je možnost přiřazení práv konkrétnímu uživateli.

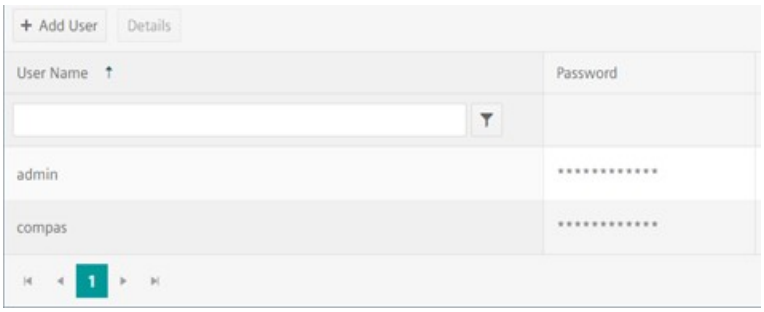


Obr. 3.4: Přístupová práva.

Program umožňuje čtyři přístupové role, konkrétně se jedná o HMI Administrátor, HMI Operátor, HMI Monitor, HMI Monitor Klient. Uživatele je možné přidávat jednak pomocí záložky *Nastavení zabezpečení (Security settings) -> Uživatelé a role (Users and roles)* viz obr.3.4 nebo pomocí *Správy uživatelů (User management)* viz obr.3.5, 3.6.

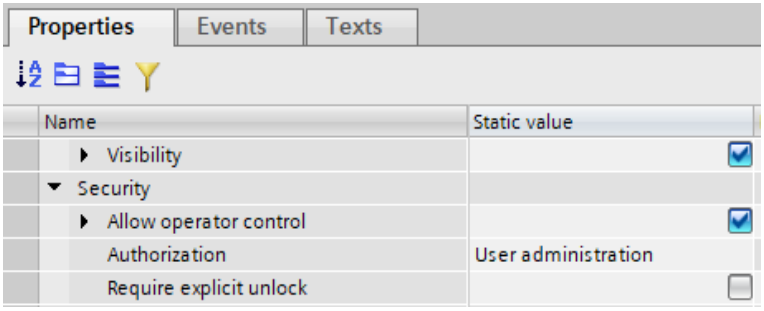


Obr. 3.5: User management.



Obr. 3.6: Přidání uživatelů.

S přístupovými právy souvisí funkce (vlastnost) nazvaná Autorizace viz obr.3.7. Ta dovoluje specifikovat, kteří uživatelé smí ovládat konkrétní prvek (tlačítko, I/O pole) ve vizualizaci. Pokud přiřadíme tlačítku autorizaci nazvanou Správce uživatelů (User administration), uživatelé s nižšími oprávněními jako HMI Operátor, HMI Monitor, HMI Monitor Klient nemohou tlačítko používat a tím pádem nemohou dávat povely zařízení. Aby bylo možné prvek ovládat, je nutné povolit řízení operátorem (Allow operator control).



Obr. 3.7: Aplikování přístupových práv prvku.

3.5 Možnosti připojení klienta

Systém WinCC Unified je založen na přístupu odkudkoliv, což je také jeho největší výhoda oproti předcházejícím systémům. Přístup je možný z PC, tabletu, telefonu a v dnešní době i z chytrých hodinek. Klient může k projektu přistupovat různými způsoby v závislosti na poloze. Prvním způsobem je přístup v rámci lokální sítě, kdy stačí zadat do vyhledávače https://ip adresa počítače (serveru) a následně zadat přístupové jméno a heslo. Pokud bychom se chtěli připojit z jiného místa, tak je potřeba využít VPN připojení. Výhoda přístupu k projektům je v tom, že u klienta nejsou požadovány další aplikace k propojení s počítačem.

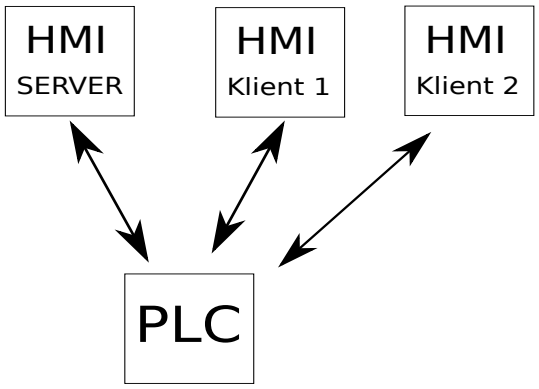
3.6 Doporučené prohlížeče

Mezi doporučované prohlížeče jsou zařazeny Google Chrome pro Microsoft Windows a Android, naopak v případě iOS a Mac je doporučován prohlížeč Safari [21].

4 WinCC Unified

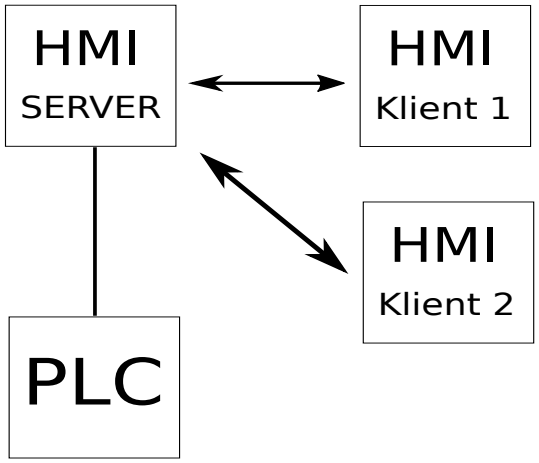
WinCC Unified je vizualizační nástroj podporující škálovatelnost, vzdálený přístup přes web bez nutnosti instalace softwarů a nové technologie. WinCC Unified je založen na technologiích HTML 5, SVG a JavaScript. [28] Poprvé se objevil v programu Tia Portal ve verzi 16.

Na obr. 4.1 je zobrazena komunikace PLC s HMI. Jedná se o komunikaci, kde je klient nucen se připojovat přímo na PLC a tím dochází k jeho zatěžování a případně k zahlcení. V tomto ohledu nabízí WinCC Unified zlepšení.



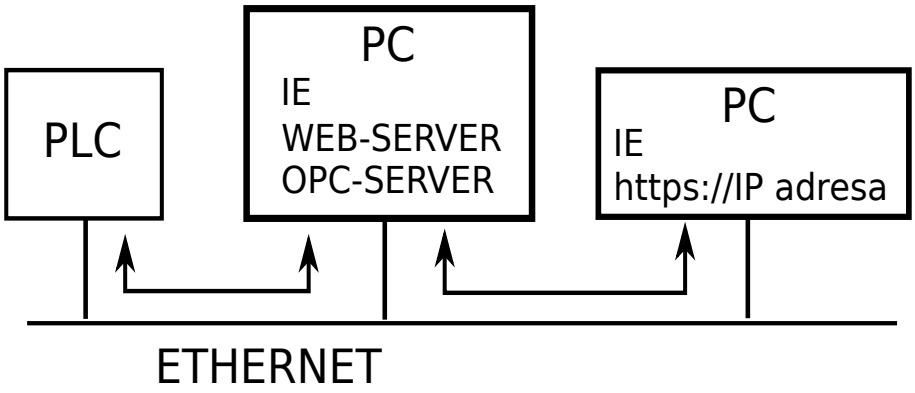
Obr. 4.1: Komunikace PLC-HMI.

Na obrázku 4.2 lze vidět, že koncoví uživatelé (operátoři, klienti) nejsou připojeni přímo na PLC, ale na HMI server, tedy na zařízení, kde je uložen projekt.



Obr. 4.2: Komunikace WinCC Unified.

Na obr. 4.3 lze pozorovat, že server může být přítomen kromě HMI panelu i na PC stanici, na kterou se pomocí webového serveru mohou připojovat ostatní zařízení. Ve WinCC Unified je kromě PC zařízení možnost používání tabletu či mobilního telefonu.



Obr. 4.3: Komunikace WinCC Unified s PC.

Na trhu existuje kromě WinCC Unified mnoho dalších verzí WinCC, kterými jsou WinCC OA (Open Architecture), WinCC Comfort, WinCC Basic, WinCC Advanced a WinCC Professional [9].

4.1 Srovnání WinCC Unified s předchozími verzemi

Prostřednictvím WinCC OA lze vytvářet internetové SCADA systémy. Pro konfiguraci panelů Siemens Basic postačí verze WinCC Basic. Pomocí WinCC Comfort lze kromě základních panelů vytvářet aplikace pro panely Comfort a Mobile, které disponují pokročilejšími funkcemi např. faceplaty a skripty. Ve WinCC Advanced lze kromě panelů vytvořit také jednouživatelské PC velíny. WinCC Professional již nabízí také víceuživatelské PC velíny a případně SCADA systémy. [9]

WinCC Unified je software, který se začal používat v roce 2019. Pomocí WinCC Unified lze konfigurovat HMI Unified Comfort panely, které jsou všestrannější i výkonnější a obsahují funkci „multitouch“, což znamená, že panely umí rozpoznat několik dotykových bodů a jsou vhodné především pro prostředí továrny, jelikož umožňují detekovat kontakt přes pracovní rukavice. [9]

WinCC Unified je oproti předchozím verzím (WinCC Professional, WinCC Comfort) založen na webových technologiích HTML5, SVG nebo JavaScript. Tento systém umožňuje uživatelům volně designovat uživatelské rozhraní s velkou škálou grafických funkcí a znuvupoužitelností všech prvků. HTML5 podporuje návrh grafického designu na PC, řídících strojích či mobilních zařízení. Dále WinCC Unified podporuje globální přístup správy i ovládaní systémů. Oproti předcházejícím verzím nabízí společný vzhled prvků např. struktury obrazovek, grafů a dalších ovládacích prvků na všech zařízení. Je zde možnost přístupu dat z kterékoliv platformy. [21]

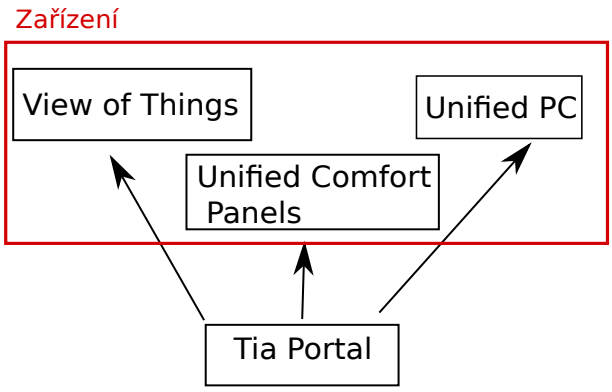
U WinCC Unified v17 jsou vyžadovány náročnější hardwarové požadavky. Např. u procesoru Intel ® Core ™ i3-6100U, 2.3 GHz, RAM minimálně 8 GB, rozlišení 1024

x 768 px a mít volné alespoň 20 GB paměti [42].

V případě WinCC Professional je nutné mít procesor Intel® Celeron™ DualCore 2.2 GHz, nejméně 4 GB RAM s rozlišením 1024 x 768 px [43].

4.2 WinCC Unified – Platformy

Systém WinCC Unified pro Tia Portál je složen ze tří platforem: Wiew of Things, Unified Comfort Panels a WinCC Unified PC [10].



Obr. 4.4: Platformy-WinCC Unified System.

4.2.1 HMI Unified Comfort Panel

HMI Unified Comfort Panel obsahuje tři vzdálené klienty, kteří vyžadují licence. Tito klienti mají možnost tzv. asynchronního přístupu, tzn. že uživatel může aktivně ovládat HMI panel a nevidí pouze to, co je na obrazovce. HMI panel obsahuje zdarma jednoho klienta pro potřeby odzkoušení vytvořeného projektu. Další možností je tzv. synchronní přístup, který je možný pouze prostřednictvím VNC (Virtual Network Computing). [10]

4.2.2 Unified PC systém

Unified PC systém, kterým se zabývám v této práci, nabízí jednoho lokálního klienta. V rámci tohoto systému je také k dispozici jeden tzv. *Řídící klient*. Tento klient má možnost čtení a zápisu, nicméně záleží na roli, která mu bude přidělena. V nabídce je i tzv. klient *Monitor*. Jedná se o klienta, který má omezenou možnost zápisu, tudíž nemůže zadávat např. proměnné. [10]

4.2.3 WinCC Unified – Pohled na věci, porovnání s ostatními

WinCC Unified - Pohled na věci je navržen za účelem jednoduché webové vizualizace. Z tabulky 4.1 je možné zjistit, že Pohled na věci (View of Things) podporuje volby vstupně/výstupních polí, tlačítka, do vizualizace lze také vkládat dynamické SVG, práce s obrazovkami jako např. vyskakovací okna (Pop-up screens). V případě, že má uživatel náročnější požadavky na webovou vizualizaci, je doporučováno použít WinCC Unified PC nebo Unified Comfort Panels, kde je umožněna sofistikovanější práce. [41]

	Pohled na věci	Comfort panel	Unified PC
Základní objekty	✓	✓	✓
Grafika	✓	✓	✓
Obrazovky	✓	✓	✓
Vytváření prototypu objektů (faceplate)	✓	✓	✓
Alarmy		✓	✓
Archivování		✓	✓
Ovládání parametrů		✓	✓
Spolupráce (Collaboration)		✓	✓
Inteligenční možnosti závodu			✓

Tab. 4.1: Srovnání Unified PC, Pohled věcí a Comfort panelu [41].

Pro aplikaci tohoto systému je nutné splňovat předpoklady, a to jak licencí (je vyžadována WinCC Inženýrská licence), tak verzí PLC (SIMATIC S7-1500) [10]. Je také uplatněno omezení počtu deseti vytvořených obrazovek a maximálního počtu sto tagů. Na rozdíl od Unified PC a Comfort panelu je zachována funkce *Změna (Change)*. Není nutné spouštět Runtime na PLC, vše běží na webu. U tohoto systému je použit stejný editor obrazovky. [64]

4.3 WinCC Unified – Funkce

4.3.1 Toolbox

Toolbox je sada nástrojů, která uživateli umožňuje vizualizovat procesy a je složen z několika oddílů. Prvním oddílem jsou *Základní objekty (Basic Objects)*. Uživateli je nabídnuta možnost kreslení čar, mnohoúhelníků, elips nebo vytvářet textová pole. Další oddíl je pod názvem *Elementy*. V Elementech lze nalézt I/O pole, přepínače, zaškrtávací pole, tlačítka či měřiče, které mají kromě zobrazení hodnot pozitivní dopad na vzhled aplikace. Ve WinCC Unified lze také aplikovat prvky např. zobrazení

zaznamenaných alarmů, okno obrazovky (Screen window) nebo trendová okna, kde má uživatel možnost sledovat průběhy hodnot procesů např. v podobě spojnicových grafů.

4.3.2 Vlastnosti objektů

Vlastnosti objektů (prvků) lze přidělit dvěma způsoby. Je možné použít dvojklik levým tlačítkem myši na vybraný objekt nebo kliknout na objekt pravým tlačítkem myši a vybrat položku vlastnosti. Vlastnosti jednotlivých objektů se liší v závislosti na typu objektu. Objektům lze ale obecně nastavovat barvy, konkrétně barvu ohraničení či barvu výplně. Za jejich společný markant lze ještě považovat jejich velikost a umístění na obrazovce. Ve vlastnostech objektů je možné nastavovat také jejich dynamizace, tzn. že v případě určité události dojde např. ke změně barvy tlačítka.

4.3.3 Události (Events)

Pod pojmem událost si lze představit situaci, kdy po kliknutí uživatelem na objekt levým tlačítkem myši dochází k provedení (vyvolání) požadované akce. K té nemusí dojít pouze po kliknutí levým tlačítkem myši, ale také při tzv. stisku (Pressu), tzn. že se událost vyvolá nejen po stisku levého i pravého tlačítka myši, ale i středního kolečka myši. Dále existují i další způsoby, jak vyvolat akce, možnosti volby však závisí na použité verzi softwaru.

4.3.4 Faceplate

Faceplate je skupina objektů, která uživateli zjednodušuje práci. Lze jej vytvořit v Tia Portalu. Uživatel po kliknutí pravým tlačítkem myši kdekoliv na obrazovce následně vybere položku *Vytvořit faceplate*. Otevře se okno, kde má uživatel možnost vybrat z Toolboxu libovolné objekty, které bude chtít sloučit k sobě. K tomu, aby byl uživatel schopen svůj Faceplate použít, musí kliknout na *Vydat verzi (Release the Version)*. Zjednodušení práce uživatele je v tom, že uživatel vytvoří faceplate z několika objektů, které nemusí pracně vytvářet znovu, ale může je zkopírovat.

4.3.5 Vyskakovací okna (pop-up)

Pop-up obrazovky úzce souvisí s faceplaty i s událostmi. Pop-up obrazovky lze využít k ovládání faceplatu. Pop-up okna je možné vytvořit jako novou obrazovku s modifikovanou velikostí uzpůsobenou počtu prvků. Jako příklad lze uvést faceplate, který bude simulovat motor. Faceplatu se následně přidá událost v podobě metody

Otevřít obrazovku v pop-up (Open Screen In Popup). V této metodě bude jako parametr figurovat uživatelem vytvořená pop-up obrazovka motoru. V pop-up obrazovce motoru je žádoucí mít definované funkce jako je zapnutí/vypnutí motoru, příp. nastavení otáček. Metodu *Open Screen In Popup* lze spustit až po spuštění Runtimu.

4.3.6 Simulace

Simulaci lze pojmout dvěma způsoby. V prvním případě uživatel nemá fyzicky žádné akční zařízení (servo motor, ventil, atd.) ani PLC. Tím pádem musí použít simulátor PLCSIM, příp. vylepšenou verzi PLCSIM Advanced. Druhým způsobem je, že uživatel vlastní PLC s určitým akčním zařízením a tedy není nutné použít jakýkoliv simulátor, jelikož PLC komunikuje s PC zařízením klienta pomocí Ethernet/Profinet. U obou výše zmíněných verzí nyní stačí spustit simulaci v Tia Portalu nebo v SIMATIC Runitime Manageru a následně otevřít webový prohlížeč a do vyhledávače napsat jméno počítače příp. IP adresu PC stanice, na kterém je licence TIA Portálu. Doposud byla řeč pouze o klientovi, který vlastní licenci TIA Portálu v17. Pokud by chtěl mít další uživatel možnost ovlivňovat procesy, které byly naprogramovány pomocí funkčních bloků, postačí mu pouze webový prohlížeč, kde uvede již známé parametry počítače (IP adresa, jméno PC stanice) s licencí.

4.3.7 Simulace na smartphonu

Simulaci lze ovládat nejen pomocí PC stanice, ale i pomocí mobilního telefonu či tabletu. Zobrazení simulace (vizualizovaného projektu) lze přizpůsobit velikosti displeje bez ztráty kvality zobrazení jednotlivých prvků.

Bezztrátovost kvality je zajištěna použitím SVG grafiky. Jedná se o škálovatelnou vektorovou grafiku, založenou na jazyce XML. Tzn. že objekt není popsán pixel po pixelu, ale pomocí čar, křivek a dalších tvarů, což umožňuje objekt zvětšovat a to bez zhoršení kvality. [76]

4.3.8 Certifikáty

Certifikáty, přesněji SSL certifikáty, jsou v případě přístupu k simulaci z mnoha různých zařízení, používány pro udržení bezpečnosti. Pro vytváření certifikátů existuje program WinCC jednotný správce certifikátů (WinCC Unified Certificate Manager), kde lze vytvářet certifikáty typu Webserver, OPC UA nebo Runtime Collaboration. [9]

SSL certifikát je nutný pro zabezpečení přenosu dat na internetu. Zajišťuje ochranu přenášených dat a také umožňuje identifikaci provozovatele webových stránek. SSL certifikáty byly rozšířeny po roce 2014, kdy bylo Googlem oznámeno, že

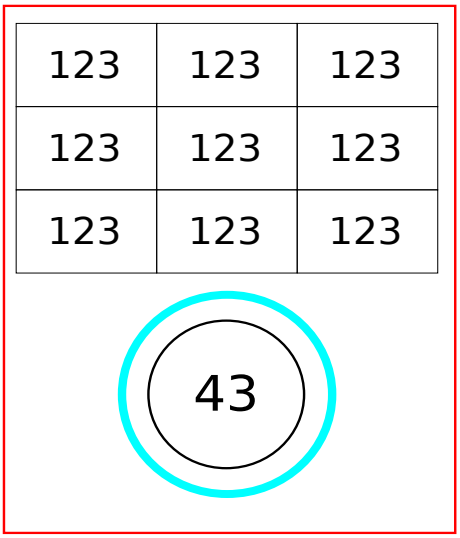
stránky s adresou HTTPS budou mít oproti HTTP ve vyhledávání prioritu. V případě, že webové stránky nemají SSL certifikát, jsou v prohlížeči Chrome označovány *Nezabezpečeno* tedy *Not secure*. [74]

SSL certifikát by měl být používán těmi majiteli webových stránek, kteří požadují od svých uživatelů údaje ve formulářích např. přihlašovací údaje. Naprostou samozřejmostí by také mělo být používání SSL certifikátů u e-shopů, bank nebo sociálních sítí. [75]

4.4 Rozšíření systému WinCC Unified o nové funkce

4.4.1 Sada HMI šablon

Sada HMI šablon (HMI template suite) je využita jako pomocník pro systém WinCC Unified, ale pouze pro verzi 16. Zjednodušuje tvorbu designu projektu. Sada HMI šablon nabízí široké množství šablon, obrázků a objektů, jak pro Unified Comfort Panel, tak i pro Unified PC. Unified Comfort Panel nabízí celkem šest možností volby rozlišení. Maximální velikost panelu, kterou můžeme používat, je 21,5 palců (1920 x 1080 px). Pro PC systémy je můžeme vybírat ze čtyř velikostí a to s maximální velikostí 1920 x 1080 px. Aplikace slibuje vytvoření rychlé, jednoduché a sjednocené vizualizace. Šablonu lze samozřejmě měnit podle přání uživatele. Od této aplikace se slibuje také jednoduší úprava projektu např. změna barvy. [29]



Obr. 4.5: HMI template suite šablona.

Základní myšlenkou je, že lidé nejsou schopni přijmout v jeden okamžik tolik informací, proto je HMI šablona založena na jednoduchosti a prezentování nejdůležitějších hodnot. Základním požadavkem pro práci se šablonami je být členem

skupiny *Siemens TIA Openness*. HMI template suite si zakládá na tzv. Flat designu. Flat design znamená, že nejsou použity trojrozměrné efekty jako např. stíny či textury. Pro HMI objekty je použita sada barev, kterou tvoří např. světle šedá, která je používána pro pozadí hlavního okna anebo modrá barva používaná pro aktivní tlačítka. Další sada barev je použita pro zobrazování stavu např. barva červená pro zobrazení alarmů. Existuje přehled rozložení, který obsahuje šest částí viz obr. 4.6.

Obr. 4.6: Přehled rozložení [23].

Sekce *Titulní lišta (Title bar)* se stará o zobrazení názvu právě používané obrazovky nebo projektu. *Stavová lišta (Status bar)* slouží k zobrazení informací např. jména uživatele, který je právě zaregistrován či stavu stroje. *Hlavní okno (Main Window)* zajišťuje zobrazení procesních hodnot, které můžou být v podobě grafu. Do *hlavního okna* je zahrnuto menu s možností přepínání obrazovek a modulů. *Podnavigace (SubNavigation)* je navigační lišta na dolním okraji šablony. Jako poslední je tzv. *Navigace třetí úrovně (Thirdlevel-Navigation)*, která se využívá pro lepší strukturování informací. Další částí HMI template suite je knihovna s objekty obrazovky. Jedním z těchto objektů je tzv. faceplate, který slouží např. k ovládání motoru či ventilu. Dále knihovna obsahuje prvek *Schránka (Clipboard)*, který se stará o vizualizaci a stukturu prvků na obrazovce. Zásadním prvkem je tzv. přístrojová deska (Dashboard), která zobrazuje nejdůležitější informace o výrobě či příslušném stroji a také obsahuje odkazy na další obrazovky HMI. Knihovna dále obsahuje moduly strojů, které mohou zobrazovat jednotlivé stavy či chyby různých strojů. V sadě HMI šablon lze použít i tzv. *Pomocníka (Wizard)*, který slouží jako průvodce kroků, které má operátor provést. Z knihovny objektů obrazovky stojí za zmínku *Funkční panel (Function Panel)*, díky němuž může uživatel zakázat konkrétní funkce či části stroje. [23]

4.4.2 Inteligenční možnosti závodu v17

Inteligenční možnosti závodu v17 (PLANT Intelligence options v17) jsou schopné řídit pracovní dobu zařízení i linek a také dokáží měřit jejich efektivitu [32].

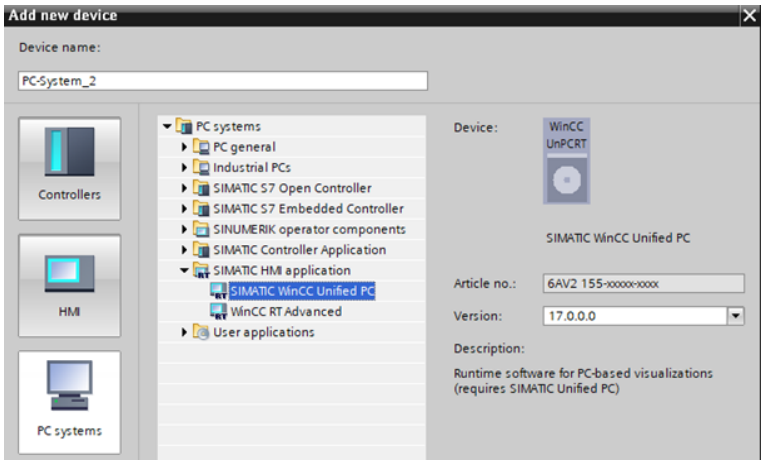
Inteligenční možnosti závodu jsou rozděleny do následujících čtyř oblastí: Přehled výkonu (Performance Insight), Kalendář (Calendar), Koordinace procesů (Line Coordination) a Sekvence (Sequence). Přehled výkonu zajišťuje např. zlepšení výkonu v Runtimu či doplnění chybějících hodnot. Funkce Kalendář zase zajišťuje plánování, konfiguraci a správu událostí či směn v kalendáři na základě zvolené pracovní doby. Pomocí Kalendáře (Calendar Control) může být získán přehled o tom, jak bylo nastaveno plánování směn pro stroj nebo celý závod a upravit tak plánování dle potřeby. Kalendář obsahuje funkce *Přejít na datum* a *Přejít na dnešek*, hlášení kalendáře či jednodušší zpracování akčních položek (úkoly, které musí být splněny). Koordinace procesů umožňuje uživatelům sledování procesů, kontrolu a řízení receptur, sledování zakázek pro výrobu různých produktů nebo škálování parametrů receptury v závislosti na objemu výroby. Poslední oblastí je *Sekvence*, která poskytuje import, export operací a řízení přístupu. Mezi výhody PLANT Intelligence jsou zmiňovány především výpočet ukazatelů, vytváření vzájemných vztahů, analýza dat v podobě grafů či tabulek, analýza poruch a informace o jejich frekvenci výskytu. Inteligenční možnosti jsou využívány v managementu nebo u aplikačních inženýrů. V Inteligenčních možnostech jsou vytvářeny aplikace Excel automaticky na základě událostí nebo času a jsou používány managementem pro analýzu a dokumentaci výroby. [31]

5 Výsledky

5.1 Vytvoření prostředí WinCC Unified

5.1.1 Přidání nových zařízení

Aby mohl být již naprogramovaný projekt vizualizován prostřednictvím systému WinCC Unified, je potřeba přidat nové zařízení *WinCC Unified PC* v záložce *PC systémy*, kde je zvolena položka *SIMATIC WinCC Unified PC* viz obr. 5.1. Aby PC stanice WinCC Unified mohla komunikovat s PLC, HMI panely a případně jinými zařízeními, je žádoucí přidat komunikační modul *IE general*, kterému bude přiřazena IP adresa.



Obr. 5.1: PC systémy, WinCC Unified PC.

5.1.2 Propojení WinCC Unified PC stanice s ostaními zařízeními

Pokud nebude vytvořeno HMI spojení, tak samotný modul IE general nebude s dalšími zařízeními komunikovat. Jednou z možností, jak vytvořit příslušné spojení, je přetáhnutí tagu z kteréhokoliv PLC datového bloku na WinCC Unified obrazovku. Další možností vytvoření HMI spojení je její manuální vytvoření, které je možné vytvořit v zobrazení *Zařízení a sítě*. Metoda manuálního vytvoření HMI spojení nemusí být stoprocentně funkční.

5.2 Zapojení scénářů pro simulaci a fyzické prvky

Pro demonstraci funkčnosti WinCC Unified systému byly použity dvě formy zapojení, a to zapojení jak s reálnými prvky (fyzický HMI Panel, PLC, . . .), tak proběhlo

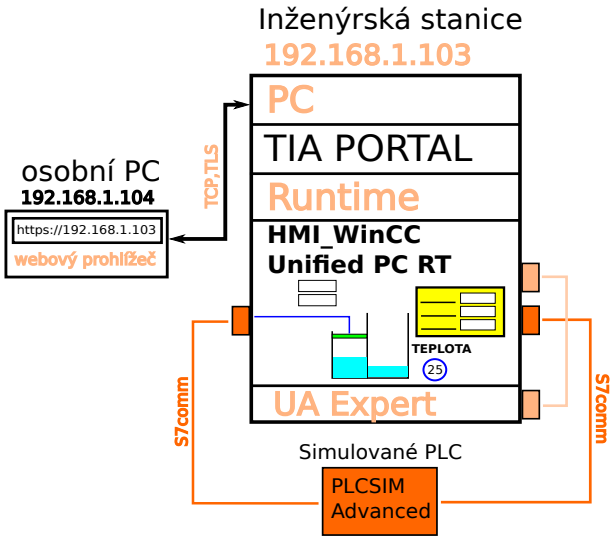
odzkoušení v rámci simulace systému (PLC, HMI jsou pouze simulovány v programu Tia Portal). V tab. 5.1 je seznam základních prvků, jež byly použity v obou typech zapojení pro ověření funkčnosti WinCC Unified.

Simulace	**Fyzické zapojení**
TIA Portal V17	KTP400Basic Panel
SIAMTIC Runtime Manager	SIMATIC S7-1200
UA Expert	Měnič SIMATIC V90
S7-PLCSIM Advanced V3.0	Servo motor
	SITOP PSU100L
	UA Expert
	SIAMTIC Runtime Manager
	TIA Portal V17

Tab. 5.1: Seznam použitých komponent v zapojení

5.2.1 Zapojení-simulace

Zapojení simulace je složeno ze dvou hlavních částí viz obr. 5.2, a to z inženýrské stanice a osobního PC. V inženýrské stanici je obsažen software jako např. Tia Portal a s ním spojený Runtime, díky kterému je možné spravovat vizualizaci. Dále je zde možné použít aplikaci UA Expert, která slouží k tomu, že uživatel se stane klientem, který se připojí na server (HMI WinCC Unified PC RT obrazovka v Tia Portalu) a je schopen jej pomocí OPC UA protokolu ovládat, tudíž má klient schopnost měnit hodnoty na HMI WinCC Unified PC RT obrazovce.

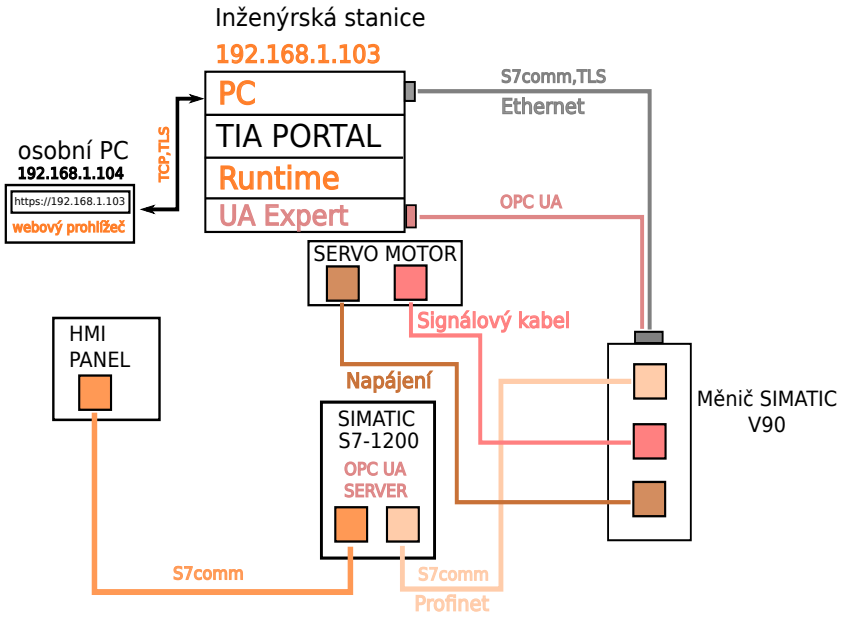


Obr. 5.2: Zapojení pracoviště-simulace.

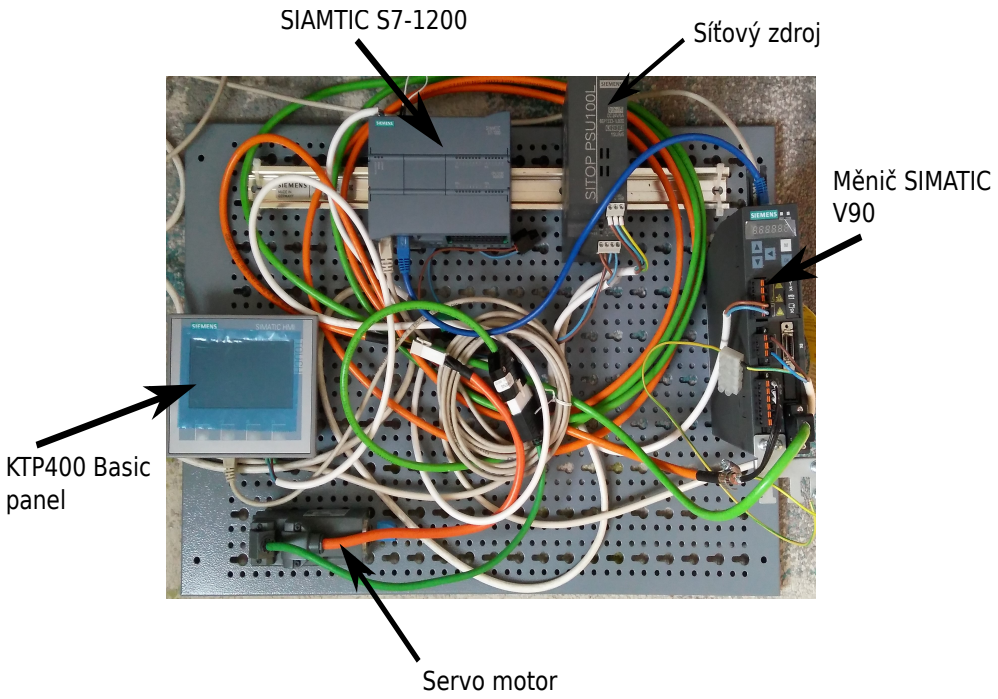
Na schématu je dále znázorněno PLCSIM Advanced. PLCSIM Advanced zde nahrazuje reálné PLC typu 1500 a slouží k odladění chyb před uvedením do provozu. Schéma zahrnuje i připojení osobního PC. Na osobním PC uživatel pouze otevře webový prohlížeč a napíše do něj IP adresu v tomto formátu: *https://192.168.1.103* a následně se pomocí uživatelského jména a hesla přihlásí.

5.2.2 Zapojení-reálné PLC

Koncepce inženýrské stanice a osobního PC je zde stejná, kromě jedné změny a tou je HMI Wincc Unified PC RT obrazovka, která je stále obsažena v rámci projektu v TIA Portalu. Namísto simulované obrazovky je použit SIMATIC HMI KTP400 Basic Panel, který komunikuje s PLC (SIMATIC S7-1200) v rámci protokolu S7-comm viz obr.5.3. Na PLC lze vytvořit OPC UA server. To je v tomto zapojení jediná možnost, jelikož HMI Basic Panely neumožňují vytvářet OPC UA server. PLC je přímo napojeno na Měnič SIMATIC V90, který umožňuje řízení Servo motoru.



Obr. 5.3: Zapojení pracoviště-fyzické PLC.



Obr. 5.4: Zapojení pracoviště.

5.3 HMI knihovna pro WinCC Unified

5.3.1 Práce s bloky, tagy

Nejprve je třeba si vytvořit v Tia Portalu novou funkci (FC), která je použita za účelem shromáždění funkčních bloků (FB) na jedno místo, tedy do organizačního bloku (OB) *Main* stačí již vložit jedno FC daného typu. K tomu, aby FC bylo provozuschopné, je nutné do něj vložit FB. Do FB se vkládají bloky/instrukce, jaké funkce bude mít komponenta (např. ventil, motor). Po vložení FB do FC se otevře okno pro vytvoření datového bloku (DB). Pro pojmenování DB se doporučuje jednotný postup, jelikož při dlouhodobé absenci práce na projektu by mohlo dojít k záměně bloků.

V této bakalářské práci jsou používány tři základní typy FB a těmi jsou: FBTIA (AQM, DQV, DQM,...), FBTIA WCC, FBTIA LOGOP. U prvního FB jsou v závorce uvedeny ostatní jména FB, jedná se o zkratky pojmenování analogového motoru, digitálního ventilu a digitálního motoru. Pojmenování dalších FB (FBTIA WCC, FBTIA LOGOP) je již neměnné, jsou aplikovatelné na všechny typ motorů a ventilů. Výše zmíněné tři základní typy FB jsou vloženy do již vytvořené FC. Po vkládání jednotlivých FB se vytvářejí DB. Pokud nedojde k vložení každého FC do *Mainu*, nebude naprogramovaný kód fungovat.

Po vytvoření DB je možné pracovat s tagy. Tagy z vytvořených DB se nacházejí

v levé liště Tia Portalu v sekci *Programové bloky* PLC zařízení. Z tohoto místa lze tagy kopírovat do HMI panelů. U systému WinCC Unified v17 je důležité kopírovat tagy do *HMI tagy -> Data zařízení (Device data)*. Kopírování tagů na jedno místo je zásadní pro chod aplikací, protože pokud by bylo na obrazovce více zařízení stejného druhu (např. tři motory), tak by nově vytvořený motor kopíroval veškeré chování již předešle vytvořeného motoru.

5.3.2 Tvorba Faceplatů pro HMI knihovnu

Tvorba faceplatů lze prostřednictvím záložky *Libraries -> Knihovna projektů (Project library) -> Typy -> Přidat nový typ*. Zde je možnost výběru mezi dvěma typy. První možnost představuje *Panels/WinCC Runtime Advanced*, druhou *Unified Comfort Panel/WinCC Unified PC*. Pro systém WinCC Unified je vybrána možnost druhá. Následně je spuštěno okno, kde je možné vytvořit si vlastní objekt, který je složen z mnoha elementů (elipsy, křivky,...). Tvorba faceplatů sebou přináší tzv. *možnost Rozhraní tagu (Tag Interface)*. Zde uživatel zadá libovolné názvy rozhraní, které budou následně ve vizualizaci propojení na reálné tagy z DB, které jsou již umístěny v HMI tazích, konkrétně v *Data zařízení (Device data)*.

Pro konkrétní elementy lze již při tvorbě faceplatů nastavovat události. Je třeba mít na mysli, že události nejsou viditelné na HMI obrazovce (není možné určit, jaká událost byla pro element použita), a tudíž je nelze ani upravovat. Jediná možnost úpravy událostí je v rámci editování typu.

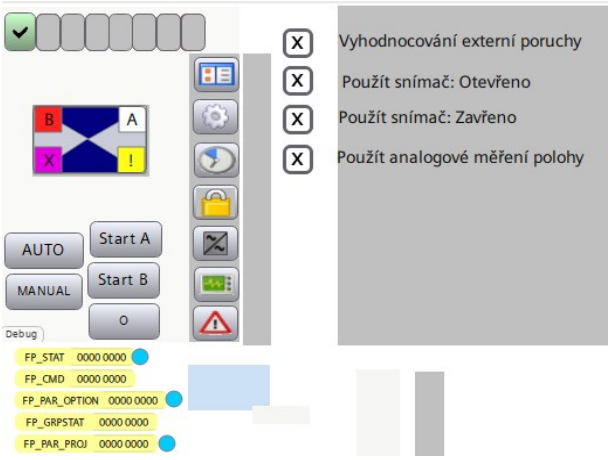
Pro tuto bakalářskou práci byla použita událost, která obsahuje tento JavaScript viz výpis. 5.1. Na tomto obrázku se jedná o kód, který přiřadí jméno konkrétního zařízení jako jméno vyskakovacího okna. To potom umožnuje uživateli rozlišit o jaké konkrétní zařízení se jedná.

```
1  if(HMIRuntime.Tags.Item("devicePopUpRequest").Read() == true)
2      {
3          HMIRuntime.Tags.Item("devicePopUpRequest").Write(false);
4      }
5      else
6      {
7          let p = HMIRuntime.Tags.Item("deviceName").Read();
8          HMIRuntime.Tags.Item("devicePopupRequestName").Write(p);
9          HMIRuntime.Tags.Item("devicePopUpRequest").Write(true);
10     }
```

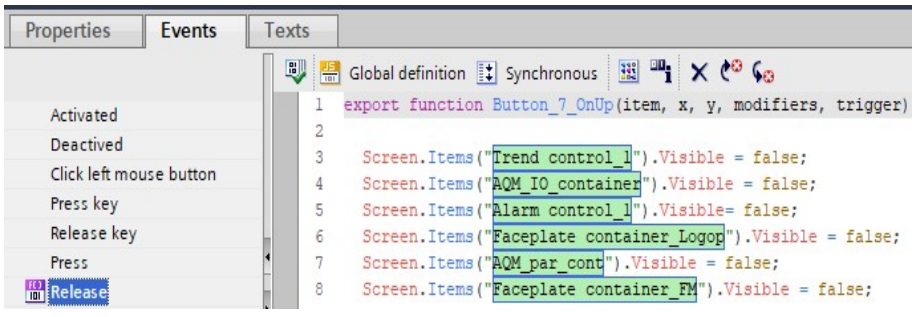
Výpis 5.1: Přiřazení jména vyskakovacího okna.

5.3.3 Vyskakovací okna

Vyskakovací okna nejsou vytvářena jako faceplate, nýbrž jako normální vizualizace, tedy prosté přesouvání elementů na obrazovku viz obr. 5.5. Důvodem, proč se vyskakovací okna nevytvářejí jako faceplate je, že vyskakovací okno je stejné pro všechny zařízení téhož druhu např. použiji stejné vyskakovací okno na čtyři motory. Vyskakovací okna jsou vytvářena prostřednictvím záložky *Rozložení (Layout)* -> *Vrstvy (Layers)*, která se nachází na pravé straně obrazovky. Layouty slouží pro skrývání elementů, se kterými momentálně uživatel nepracuje. Tím se ušetří prostor HMI obrazovky, jelikož i skryté prvky jsou plně funkční. Aby se konkrétní elementy zobrazily podle požadavku uživatele, lze zajistit přiřazením událostí konkrétnímu tlačítku viz obr. 5.6.



Obr. 5.5: Vyskakovací okno ventilu.



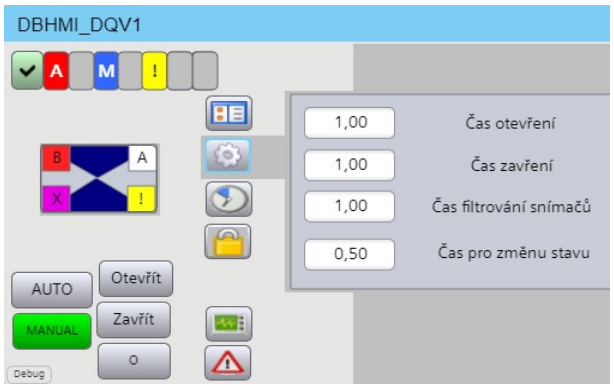
Obr. 5.6: Události tlačítka.

5.3.4 Přiřazení tagů rozhraní faceplatu, proces spouštění vyskakovacích oken

Přiřazení tagů se provede zobrazením vlastností daného objektu např. již zmíněného motoru. Dále je nutné vyhledat vlastnost rozhraní. Zde je možnost přiřazení konkrétního tagu k *Rozhraní* viz obr. 5.7, které se postará o předání informací na obrazovce v prohlížeči viz obr. 5.8.

Interface	
FP_STAT	DBHMI_DQV1_FP_STAT
devicePopUpRequest	popUpRequest
devicePopupRequestName	popUpRequestDeviceName
deviceName	DBHMI_DQV1_WCC_deviceName
Cycle_base	
PV	DBHMI_DQV1_POS_PV
FP_Option	DBHMI_DQV1_FP_PAR_OPTION

Obr. 5.7: Tagy pro faceplate.



Obr. 5.8: Vizualizace faceplatu.

K tomu, aby se vyskakovací okno na obrazovce prohlížeče objevilo, slouží skript viz výpis 5.2. Skript momentálně umožňuje otevřít vyskakovací okna digitálnímu ventilu a analogovému motoru.

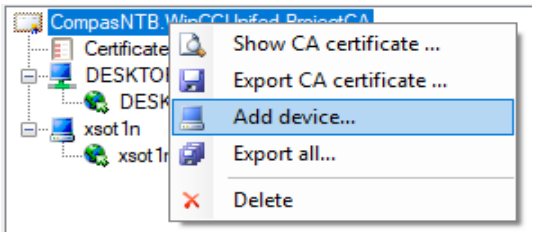
```
if(HMIRuntime.Tags.Item("popUpRequest").Read())
    {
        let device = HMIRuntime.Tags.Item("popUpRequestDeviceName")
    .Read();
        let pop_up;

    if (device.includes("DQV"))
        {
            pop_up = "DQV_pop";

        }

    if (device.includes("MOT"))
        {
            pop_up = "AQM_pop";

        }

    UI.SysFct.OpenScreenInPopup(device,pop_up,true,device,100,100,
    false);
    HMIRuntime.Tags.Item("popUpRequest").Write(false);
    }
```

Výpis 5.2: Skript na zobrazení vyskakovacích oken.

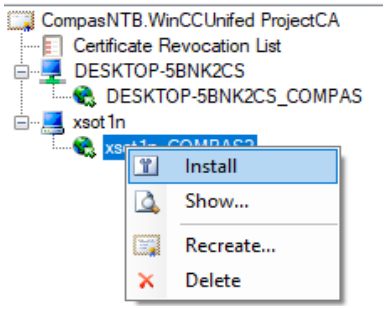
5.4 Připojení klienta k WinnCC Unified

Po vytvoření vizualizace ve WinnCC Unified přichází na řadu připojení klienta. Pro připojení klienta je nutné nejdříve vytvořit ve *Správci certifikátů (WinCC Unified Certificate Manager)* certifikační autoritu (certificate authority). Certifikační autorita se vytvoří kliknutím přes pravé tlačítko na položku *Není nakonfigurována žádná certifikační autorita (No certificate authority configured)* a s následným vybráním možnosti *Vytvořit novou certifikační autoritu (Create new certificate authority)*. Pro vytvoření nové certifikační autority je nutné vyplnit pole *Jméno autority (Authority Name), Organizaci, Životnost certifikátu (Lifetime)* a dále je nutné zadat *heslo*. Po vytvoření certifikační autority je zapotřebí přidat konkrétní zařízení, kterému bude povolen přístup k ovládání projektu, resp. jeho vizualizaci. Po označení certifikační autority a následným kliknutím pravým tlačítkem je vybrána položka *Přidat zařízení (Add device)* viz obr. 5.9. Nejdříve je nutné přidat *jméno počítače (Computer name)*. Je požadováno jméno počítače, ze kterého je spouštěn projekt. Dále je možnost zadat IP adresu, ale v případě, že zařízení je přiřazována IP adresa automaticky, je dostačující ponechat pouze jméno počítače. Poté, co zařízení bylo vytvořeno, je

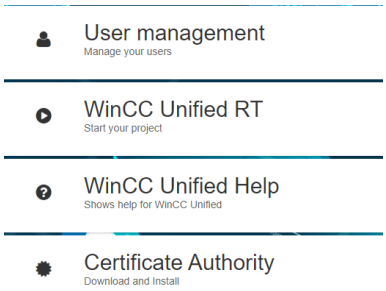
nutné mu přidat certifikát *Webserver (Add Webserver certificate)*. Zde postačí vyplnit jméno, organizaci a případně lze upravovat i dobu platnosti certifikátu. Pro fungování Webserver certifikátu je nutné jej nainstalovat viz obr. 5.10. Při následném připojení klienta je na obrazovce znázorněna položka *Certifikační autorita* viz obr. 5.11, kterou je potřeba nainstalovat do klientského počítače.



Obr. 5.9: Přidat zařízení.



Obr. 5.10: Instalování certifikátu.



Obr. 5.11: Certifikát - klient.

Aby byl klient schopen ovládat procesy zařízení, je nutné mu vytvořit uživatelské jméno, heslo a také oprávnění viz obr. 3.4. Výhodou připojení klienta ve WinCC Unified je to, že není třeba instalovat další aplikaci k připojení k serveru. Nevýhodou naopak může být nedostatečné zabezpečení komunikace. K lokálnímu připojení klienta je nutné znát pouze IP adresu serveru. Minimálním hardwarovým požadavkem je mít na zařízení možnost internetového připojení.

V případě klienta probíhá komunikace klient – server, která je založena na http protokolu a také na tzv. TCP příznacích, konkrétně PSH a ACK. Příznak PSH označuje, že příchozí data jsou předána přímo aplikaci, je vhodný pro aplikace a procesy citlivé na latenci a potlačuje zpoždění dané Nagleovým algoritmem nebo zpožděními způsobené potvrzeními, což způsobí, že data budou odesílána co nejrychleji. Příznak ACK se používá jako potvrzení, že datové pakety byly v pořádku přijaty. [58]

Následně je provedena komunikace SYN, SYN ACK, ACK tzv. třícestný handshake, který slouží jako pokus připojení klienta na server [59].

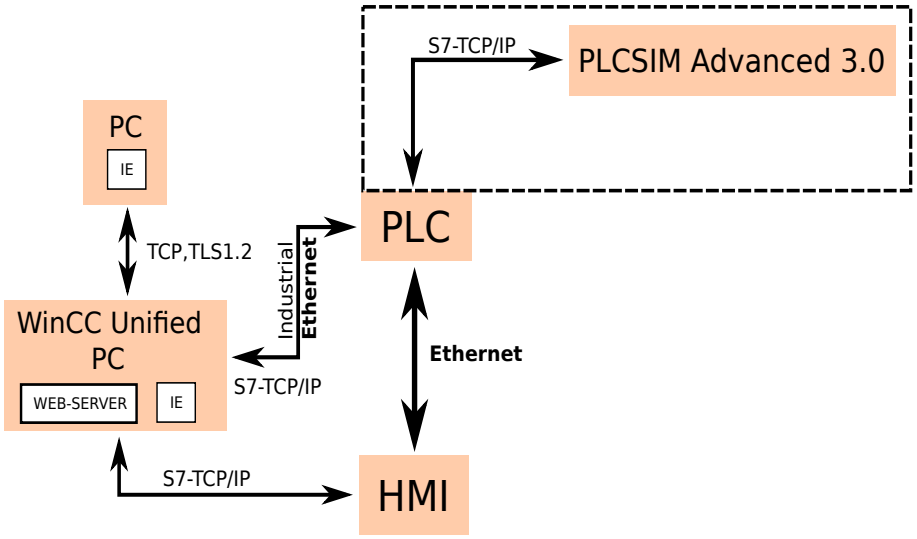
Pro vzdálené připojení klient – server může být použita síť VPN nebo program TeamViewer.

5.5 Komunikace WinCC Unified prostřednictvím protokolů

Implementace protokolů závisí především na hardwaru. V rámci výchozího nastavení je použita komunikace prostřednictvím tzv. protokolu S7-TCP/IP. Jako druhá možnost připadá v úvahu komunikace prostřednictvím protokolu OPC UA, kdy je po uživateli požadováno vytvoření OPC UA serveru.

5.5.1 Výchozí komunikace zařízení

Výchozí varianta komunikace systému WinCC Unified s ostatními zařízeními probíhá pomocí protokolu S7-TCP/IP. U výchozí varianty není požadováno, aby uživatel provedl nastavení zařízení buď jako server nebo klient. Pokud dojde k přidání nového zařízení k již stávajícím, tak nové zařízení opět funguje ve výchozím režimu. Na obr. 5.12 je znázorněno schéma komunikace. Komunikace probíhá na základě protokolu S7-TCP/IP, tedy mimo komunikace webového prohlížeče PC a WinCC Unified PC zařízení, ta probíhá pomocí protokolů TCP a TLS 1.2. Ve schématu se počítá jak se simulací zapojení, tedy použitím PLCSIM Advanced 3.0, tak i s reálným zapojením. V tomto případě komunikace nemusíme pracovat s HMI panelem, jelikož WinCC Unified PC zařízení HMI panel zastoupí.



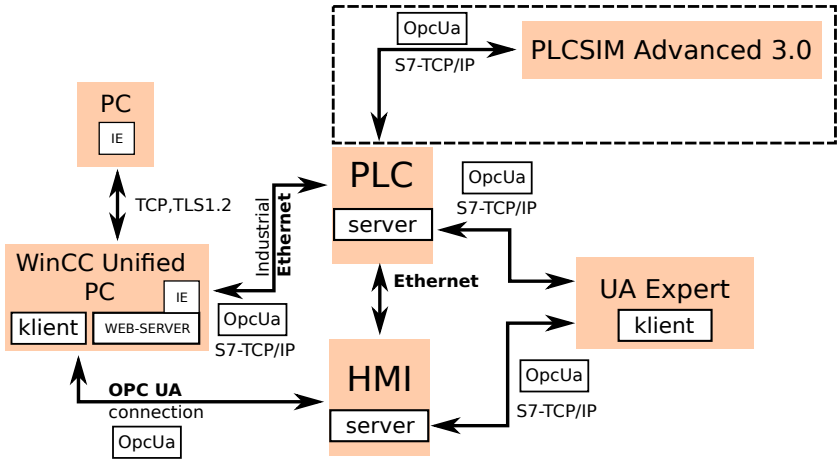
Obr. 5.12: Výchozí komunikace zařízení.

5.5.2 Komunikace server (PLC, HMI) - klient (aplikace UA Expert, WinCC Unified PC)

Na obr. 5.13 je nakresleno zjednodušené schéma komunikace jednotlivých prvků systému. OPC UA server je vytvořen jak na PLC, tak i na HMI panelu. Je nutné dodat, že se v tomto případě jedná o Comfort Panel, který vytvoření OPC UA serveru podporuje, ale např. na Basic Panelu OPC UA server nelze vytvořit.

Jako klient je zde použita aplikace UA Expert, pomocí které je možné ovládat uživatelem naprogramované procesy na základě OPC UA protokolu. V tomto případě je použit nezabezpečený OPC UA protokol, tedy v případě zachycení komunikace pomocí programu Wireshark lze jednoduše zjistit, které příkazy uživatel použil.

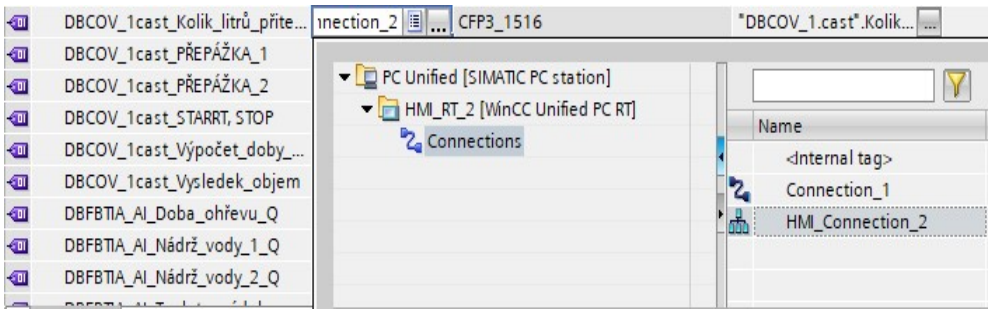
Na obr. 5.13 je dále znázorněna WinCC Unified PC stanice, která se chová rovněž jako klient. Dále obsahuje WEB-SERVER, pomocí kterého je možné připojení dalšího PC zařízení, mobilního telefonu či dokonce chytrých hodinek. K tomu, aby WinCC Unified PC stanice komunikovala prostřednictvím OPC UA protokolu, je nutné nastavit v programu Tia Portal *OPC UA Spojení (Connection)*. Pokud testujeme OPC UA komunikaci pomocí simulace, je nutné použít software PLCSIM Advanced 3.0, který simuluje fyzické PLC. V případě použití UA Experta bude probíhat komunikace PLCSIM Advanced 3.0 a PLC serveru prostřednictvím OPC UA protokolu.



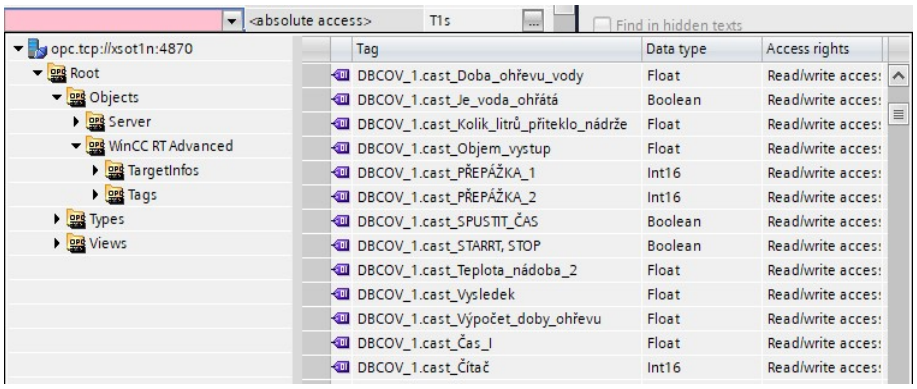
Obr. 5.13: Komunikace server (PLC, HMI) – klient (UA Expert, WinCC Unified PC).

Aby mohlo WinCC Unified pracovat jako klient, je potřeba nejdříve vytvořit OPC UA server na HMI panelu a následně ho přepnout do simulace. Dále je nutné vytvořit na WinCC Unified stanici *OPC UA spojení* a vybrat *lokální OPC UA server*. V položce HMI tagy je nutné změnit spojení z *HMI Spojení (HMI Connection 2)* na *Spojení 1* viz obr. 5.14 a odstranit *PLC jméno*. Posledním krokem je přidání odpovídající adresy tagu na straně serveru viz obr. 5.15.

Nastavení WinCC Unified stanice jako klient může vést ke ztrátě schopnosti zápisu hodnot tagů na straně klienta, tedy ve webovém prohlížeči uživatel není schopen provádět změny hodnot. Tento problém se netýká serveru.



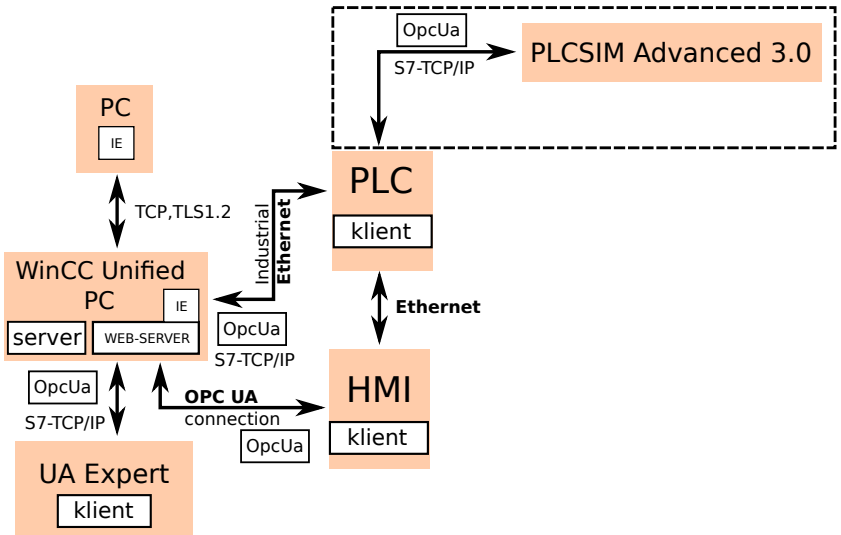
Obr. 5.14: Změna spojení u HMI tagů.



Obr. 5.15: Přiřazení tagů pro OPC UA spojení.

5.5.3 Komunikace server (WinCC Unified PC) - klient (aplikace UA Expert, HMI)

Další možností komunikace server – klient je, že OPC UA serverem je WinCC Unified PC stanice a klienti mohou být např. UA Expert, HMI Panel či dokonce PLC viz obr. 5.16. Stejně jako v předchozím případě, pokud má být WinCC Unified PC serverem a HMI Panel klientem, je nutné vytvořit *OPC UA spojení*, ale v opačném pořadí než v předchozím případě. K serveru se lze opět připojit pomocí UA Expertu, který se ale připojuje na adresu *opc.tcp:// jméno PC (IP adresa):4890*. Je třeba zmínit, že WinCC Unified PC server neumožňuje použít nezabezpečený přenos dat, tedy přihlašování k serveru prostřednictvím UA Expertu je z krátkodobého hlediska pohodlnější než vytvářet OPC UA spojení, certifikáty na HMI panelu.

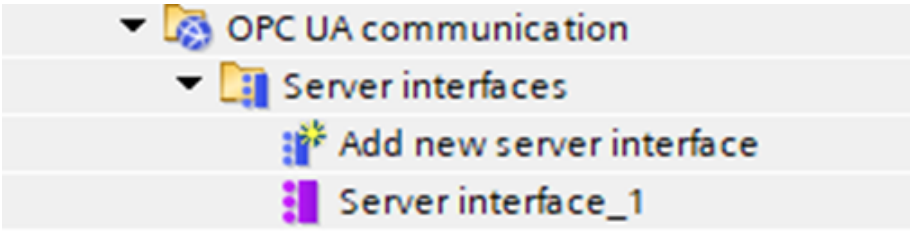


Obr. 5.16: Komunikace server (WinCC Unified PC) – klient (aplikace UA Expert, HMI).

5.6 Zachycení komunikace s následnou analýzou pomocí programu WIRESHARK

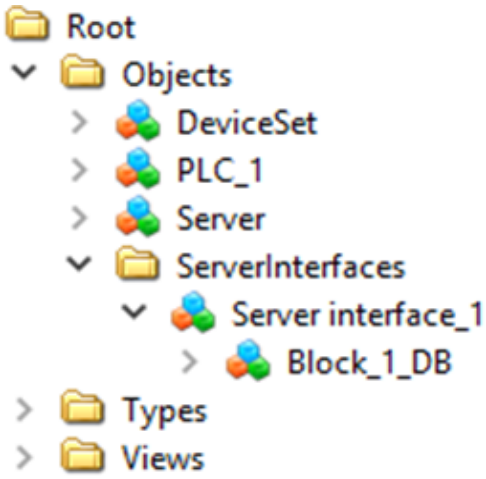
5.6.1 Zachycení komunikace u fyzického scénáře

Pro zachycení komunikace s následnou analýzou v programu Wireshark byl vytvořen OPC UA server na PLC typu 1215. Aby bylo možné zprovoznit OPC UA server na tomto typu PLC, je nutné mít nainstalovanou verzi firmwaru minimálně V4.4. V případě PLC použitého v bakalářské práci je použita verze V4.5. Kromě verze firmwaru je nezbytné vytvořit *Rozhraní serveru (Server interface)* viz obr. 5.17, kde je nutné vložit tagy, které uživatel bude chtít ovládat z aplikace UA Expert.



Obr. 5.17: Rozhraní OPC UA komunikace.

Server interface slouží k tomu, aby byly tagy viditelné pro OPC UA klienta viz obr. 5.18.



Obr. 5.18: Rozhraní OPC UA v aplikaci UA Expert.

Jako klient byl použit software UA Expert ve verzi 1.6.1. Pokud je zprovozněno v aplikaci UA Expert připojení k OPC serveru, je možné vložit tagy z *Server Interfaces* do tzv. okna *Zobrazení přístupu k datům (Data Access View)*. Na obr. 5.19 lze vidět

Číslo pořadí tagů, na kterém serveru běží tagy, dále následuje tzv. *Identifikace tagu (Node Id)*, *Hodnota proměnné* a nakonec *Datový typ*.

Data Access View

#	Server	Node Id	Display Name	Value	Datatype
1	SIMATIC.S7-120...	NS4|Numeric|4	axisEnable	false	Boolean
2	SIMATIC.S7-120...	NS4|Numeric|8	btnJogLeft	false	Boolean

Obr. 5.19: Zobrazení přístupu k datům u fyzického PLC.

Po zachycení komunikace mezi IP adresami 192.168.50.32 (IP síťové karty Ethernet) a 192.168.50.40 (PLC 1 [CPU 1215]) lze ve Wiresharku rozkliknout paket s názvem *Zapiš požadavek (WriteRequest)* viz obr. 5.20.

213	6.874630	192.168.50.32	50776	192.168.50.40	4840	OpcUa	135	UA Secure Conversation Message: WriteRequest
216	6.972195	192.168.50.40	4840	192.168.50.32	50776	OpcUa	118	UA Secure Conversation Message: WriteResponse
234	7.635591	192.168.50.40	4840	192.168.50.32	50776	OpcUa	183	UA Secure Conversation Message: PublishResponse
235	7.645412	192.168.50.32	50776	192.168.50.40	4840	OpcUa	128	UA Secure Conversation Message: PublishRequest

Obr. 5.20: Zachycení komunikace v programu Wireshark u fyzického PLC.

Po dalším rozbalení informací paketu je možné vyčíst hodnotu příkazu, která byla zadána uživatelem. O tom, o jaký tag se konkrétně jedná rozhoduje tzv. *Číselný identifikátor (Identifier Numeric)* viz obr. 5.21.

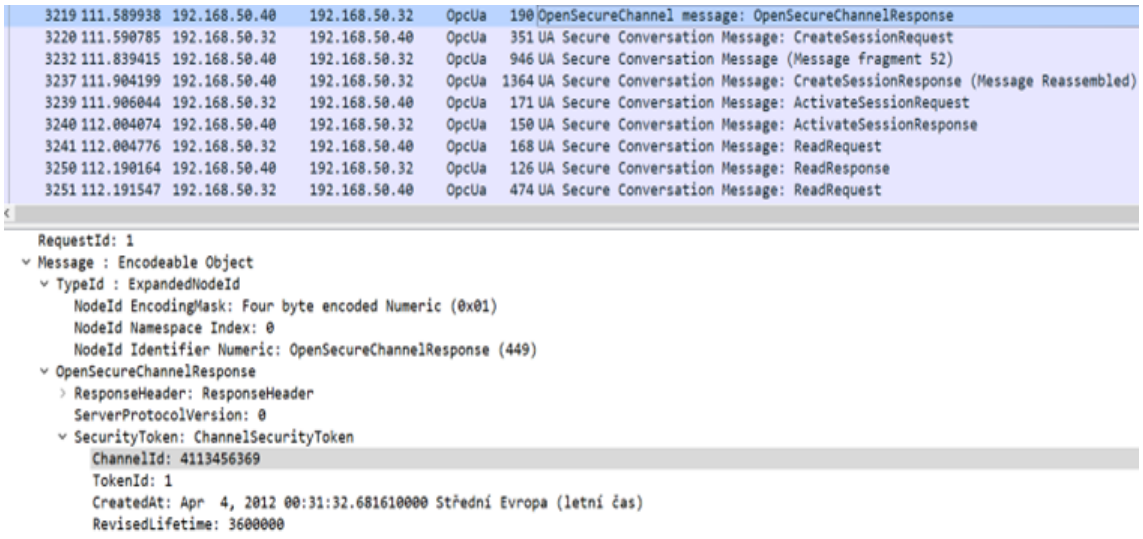
```
▼ [0]: WriteValue
  ▼ NodeId: NodeId
        .... 0001 = EncodingMask: Four byte encoded Numeric (0x1)
        Namespace Index: 4
        Identifier Numeric: 8
    AttributeId: Value (0x0000000d)
    IndexRange: [OpcUa Null String]
  ▼ Value: DataValue
    ▶ EncodingMask: 0x01, has value
    ▼ Value: Variant
        Variant Type: Boolean (0x01)
        Boolean: False
```

Obr. 5.21: Hodnota tagu v programu Wireshark u fyzického PLC.

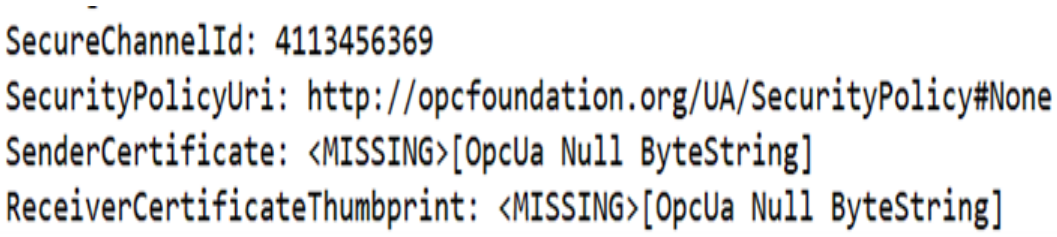
Konkrétně v tomto případě se jedná o *Číselný identifikátor 8*, ten v aplikaci UA Expert přísluší jménu *btnJoqLeft*. Důvodem, proč je ve Wiresharku možné takto říct, jaká hodnota byla zadána a o který tag se jedná, je použití nezabezpečené (None) OPC UA komunikace.

Otevření zabezpečeného kanálu

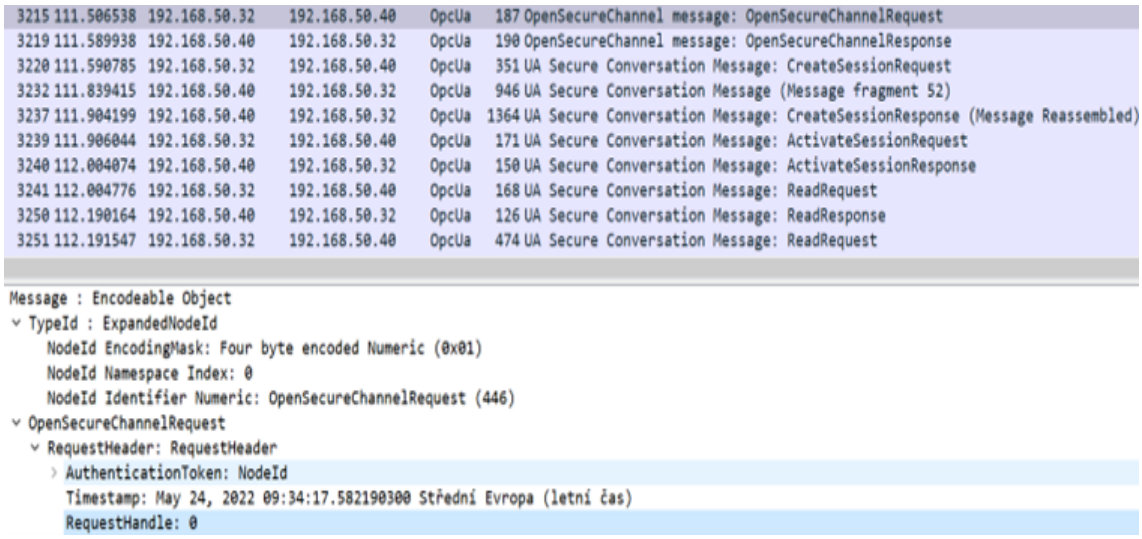
Ze zachycené komunikace lze také vypozorovat tzv. *Otevření zabezpečeného kanálu* viz obr. 5.22, který je charakterizován tzv. ID kanálem. Standardně má délku 190 B. Ze zachyceného paketu lze rovněž vypozorovat *časovou omezenost*, která je v tomto případě rovna 3 600 000 ms. Dále lze zjistit, že komunikace proběhla na základě nezabezpečeného spojení, a tudíž zde není použito certifikátu viz obr. 5.23. Z obr. 5.24 lze ověřit že parametr *Request Header* je roven nule.



Obr. 5.22: Otevření zabezpečeného kanálu, ID kanál.



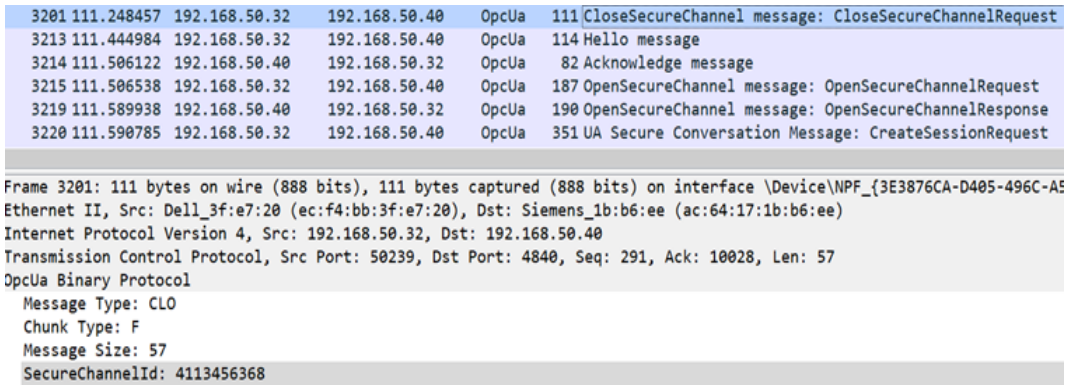
Obr. 5.23: Nezabezpečená komunikace, chybějící certifikát.



Obr. 5.24: Parametr Request Header.

Zavření zabezpečeného kanálu

Pro ověření shodného identifikátoru při *Otevření zabezpečeného kanálu*, tak i u *Zavření zabezpečeného kanálu* lze použít parametr *ID zabezpečeného kanálu* viz obr. 5.25. Tento parametr je shodný s parametrem paketu *Open Secure Channel Response*.



Obr. 5.25: ID zabezpečeného kanálu.

Vytvoření relace

Z paketu na straně serveru, tedy se jedná o paket *Create Session Response* lze zjistit dva parametry, a to tzv. *session ID* a *autentizační symbol* viz obr. 5.26. Po paketu *Create Session Response* následují pakety *Activate Session Request* a *Activate Session Response*.

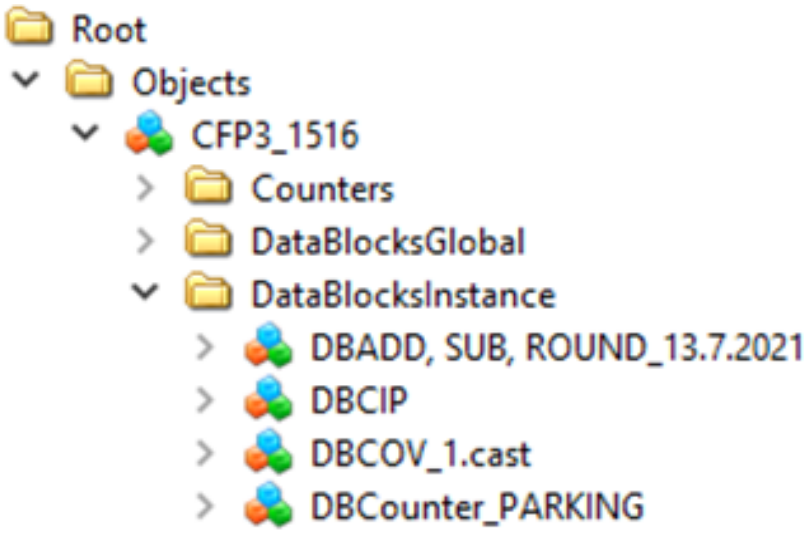
```
3237 111.904199  192.168.50.40   192.168.50.32   OpcUa  1364 UA Secure Conversation Message: CreateSessionResponse (Message Reassembled)
3239 111.906044  192.168.50.32   192.168.50.40   OpcUa   171 UA Secure Conversation Message: ActivateSessionRequest
3240 112.004074  192.168.50.40   192.168.50.32   OpcUa   150 UA Secure Conversation Message: ActivateSessionResponse
3241 112.004776  192.168.50.32   192.168.50.40   OpcUa   168 UA Secure Conversation Message: ReadRequest
3250 112.190164  192.168.50.40   192.168.50.32   OpcUa   126 UA Secure Conversation Message: ReadResponse
3251 112.191547  192.168.50.32   192.168.50.40   OpcUa   474 UA Secure Conversation Message: ReadRequest
3257 112.351349  192.168.50.40   192.168.50.32   OpcUa   406 UA Secure Conversation Message: ReadResponse
3258 112.374504  192.168.50.32   192.168.50.40   OpcUa   155 UA Secure Conversation Message: BrowseRequest
3261 112.463416  192.168.50.40   192.168.50.32   OpcUa  1352 UA Secure Conversation Message: BrowseResponse

  SessionId: NodeId
      .... 0010 = EncodingMask: Numeric of arbitrary length (0x2)
      Namespace Index: 1
      Identifier Numeric: 1897073021
  AuthenticationToken: NodeId
      .... 0010 = EncodingMask: Numeric of arbitrary length (0x2)
      Namespace Index: 0
      Identifier Numeric: 2725217319
    RevisedSessionTimeout: 30000
```

Obr. 5.26: Session ID a autentizační symbol.

5.6.2 Zachycení komunikace u simulace

Zde je zachycena komunikace, ale nyní již pro simulovaný PLC typu 1516, na kterém byl vytvořen OPC UA server. Aplikace UA Expert je zde opět OPC UA klientem.

V případě simulace PLC není nutné vytvářet *Server Interface*, tagy jsou v UA Expertu zobrazeny v *Instanci datových bloků (Data Blocks Instance)* viz obr. 5.27.



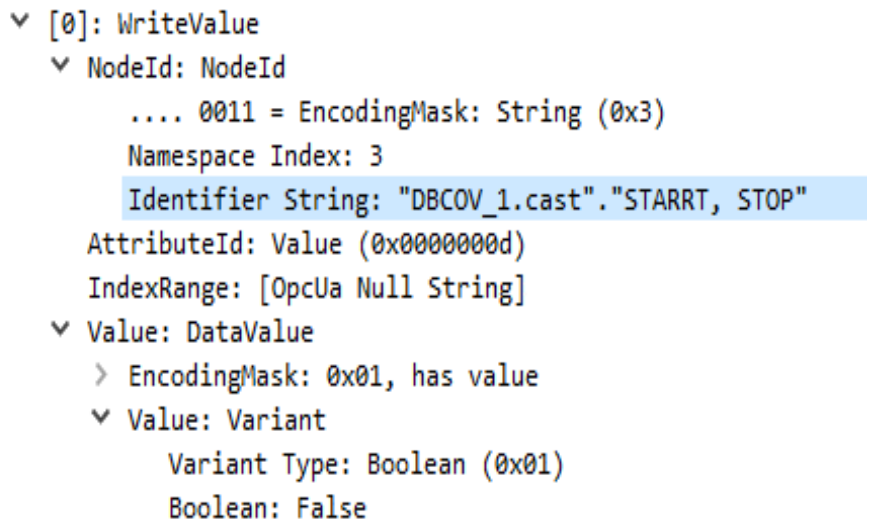
Obr. 5.27: Instance datového bloku po připojení k OPC UA serveru na simulovaném PLC.

Po přetáhnutí tagů do *Data Access View* se zobrazí oproti předchozímu případu i jméno tagů viz obr. 5.28. Ve Wiresharku je zachycena komunikace. Opět lze zobrazit detaily paketu viz obr. 5.29. Z paketu lze také určit hodnotu, která byla nastavena, je zde uvedeno i jméno tagu.

Data Access View

#	Server	Node Id	Display Name	Value	Datatype
1	SIMATIC.S7-120...	NS4|Numeric|4	axisEnable	false	Boolean
2	SIMATIC.S7-120...	NS4|Numeric|8	btnJogLeft	false	Boolean
3	SIMATIC.S7-150...	NS3|String|"DBCOV_1.cast"."STARRT, STOP"	STARRT, STOP	false	Boolean

Obr. 5.28: Zobrazení přístupu k datům u simulovaného PLC.



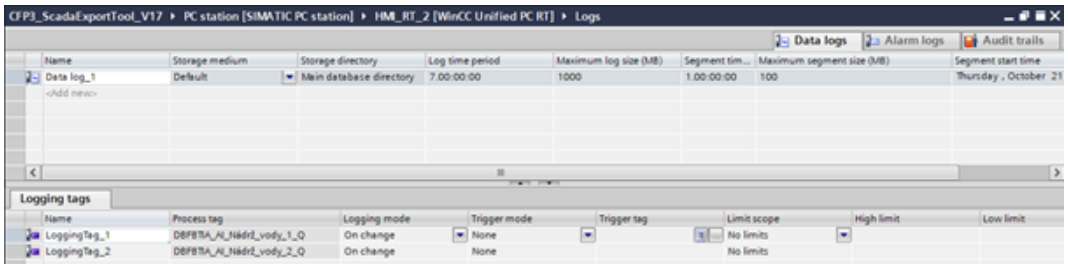
Obr. 5.29: Hodnota tagu v programu Wireshark u simulovaného PLC.

5.7 Práce s daty – Eport dat do tabulkového procesoru Microsoft Excel

WinCC Unified umožňuje pokročilou práci s daty. První možnou funkcí je tzv. *Trend Control*. Tato funkce dokáže vizualizovat data v podobě grafů viz obr. 5.30 s možným exportem dat do tabulkového procesoru Excel. Pro uchovávání dat je nutné definovat tzv. *Logging tags* viz obr. 5.31. V případě, že by toto nastavení nebylo provedeno, přichází se po každé aktualizaci vizualizace o předešlá data. Množství dat, které bude exportováno, záleží na nastavení parametru *Time-Selection*.

Jako doplněk k funkci *Trend Control* může být využit nástroj *Trend companion*, který dokáže poskytnout např. minimální, maximální i průměrnou hodnotu z určitého intervalu hodnot.

Obr. 5.30: Funkce - Řízení trendů.



Obr. 5.31: Nastavení tagů za účelem jejich exportu.

5.8 Analýza zatížení komunikace mezi WinCC Unified PC a PLC

Analýza komunikace mezi WinCC Unified PC a PLC byla provedena na základě těchto sledovaných parametrů: využívání paměti RAM aplikacemi Google Chrome (64 bitová verze) a TIA Portal V17, zatížení CPU aplikací Google Chrome (64 bitová verze). Výše zmíněné parametry byly sledovány z důvodů aplikování složitějších vizualizací v průmyslu.

Pro sledování a odečet výše uvedených parametrů byl použit nástroj Správce úloh a dále také výchozí nastavení komunikace zařízení v rámci simulace viz obr. 5.12.

Ve WinCC Unified PC zařízení byla použita jedna, případně dvě obrazovky s tagy typu Bool a ani jedna *Vyskakovací obrazovka*. Žádné další obrazovky nebyly v analýze použity.

5.8.1 Zatížení paměti RAM v závislosti na počtu tagů

Měření probíhalo metodou inkrementace tagů o dvojnásobnou hodnotu, na obrazovku WinCC Unified byly postupně přidávány tagy typu Bool. Po startu simulace byla aktualizována webová stránka localhost s tagy. Následně byl pro odečtení hodnot ve *Správci úloh* použit cca 15 s čekací interval, který zapříčinil ustálení hodnoty zatížení paměti RAM (16 GB DDR3), tedy hodnota byla téměř neměnná a byla použitelná pro analýzu komunikace.

Jedna Unified obrazovka, jeden PC uživatel

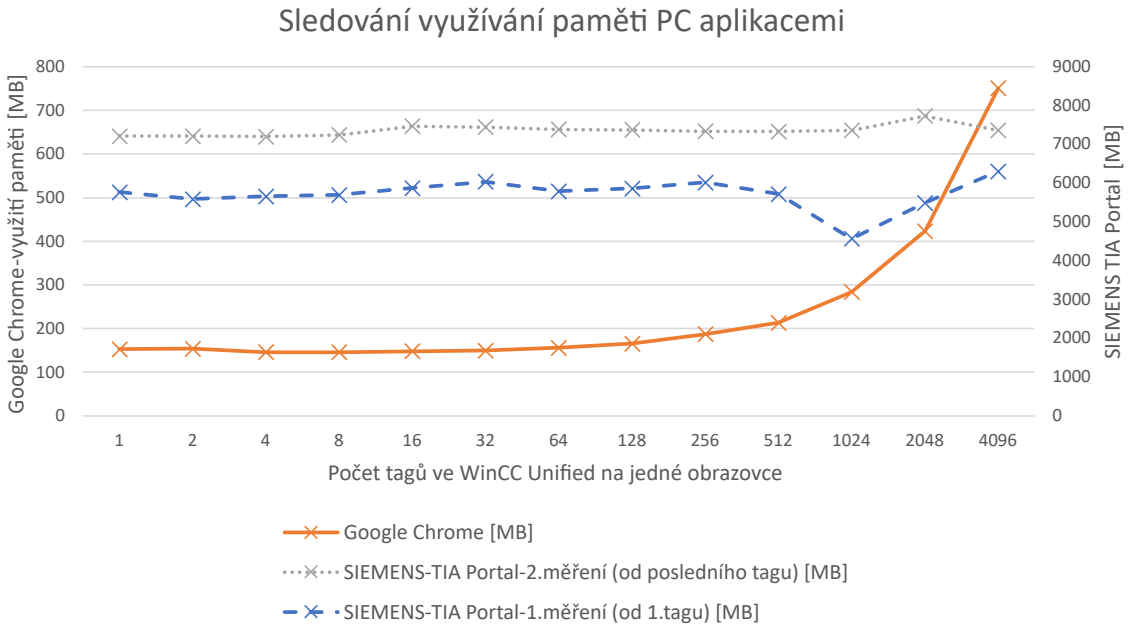
Jako první byla provedena zkouška zatížení paměti RAM při použití jednoho PC uživatele a tagy byly postupně přidávány pouze na jednu HMI obrazovku. Z tabulky 5.2 lze pozorovat dynamiku navyšování tagů, zatížení aplikací Google Chrome a Tia Portal na paměť RAM. V tabulce je zahrnuto dvoje měření zatížení, které představuje Tia Portal. První měření bylo provedeno zvyšováním tagů, tedy od prvního tagu do 4096 tagů. Druhé měření probíhalo formou snižování tagů.

Počet tagů	Google Chrome [MB]	SIEMENS-TIA Portal-2.měření [MB]	SIEMENS-TIA Portal-1.měření [MB]
1	152,9	7211,1	5763,6
2	153,8	7209,6	5587,9
4	145,8	7201,8	5660,9
8	146,1	7239,1	5696,6
16	148	7466,6	5872,7
32	149,7	7445,3	6035
64	155,7	7381,7	5787
128	165,4	7370	5863,1
256	187,3	7333,9	6018,2
512	213,4	7329	5720,5
1024	283,9	7361,4	4567,4
2048	423,2	7731,5	5491,7
4096	751,1	7357,5	6304,3

Tab. 5.2: Jedna HMI obrazovka, jeden PC uživatel

Graf 5.32 obsahuje osu x, na které je zobrazeno počet tagů na jedné obrazovce. Na hlavní ose y jsou vyneseny hodnoty zatížení RAM aplikací Google Chrome. Z hodnot lze vyčíst, že do počtu 128 tagů na jedné obrazovce je nárůst využité paměti RAM zcela minimální, ale po dalším zdvojnásobení tagů, tedy při 256 tazích lze pozorovat znatelnější nárůsty zatížení. Pro názornost lze zatížení aplikace Google Chrome přirovnat k zatížení, které představuje samotný Správce úloh. U Správce úloh se jedná o zatížení cca 30 MB, tedy přibližně o 10krát menší hodnotu než při běhu 1024 tagů typu Bool.

Na vedlejší ose y jsou vyznačeny hodnoty zatížení připadající aplikaci Tia Portal v17. Cílem tohoto měření bylo zjistit, jaký vliv bude mít počet tagů na chod aplikace či PC. Stejně jako u aplikace Google Chrome se jedná o ustálené hodnoty, tedy je třeba si uvědomit, že peakové hodnoty zatížení jsou mnohem vyšší. Bylo mimo jiné zjištěno, že při kopírování z 512 tagů na 1024 tagů dochází k přetížení Tia Portalu a přestává dočasně reagovat na požadavky klienta. Jak bylo uvedeno výše, provedl jsem dvojí měření z důvodu hledání případné závislosti zatížení na počtu tagů, bohužel se z měření nedá určit konkrétní závislosti. Měření se liší ve startovacích bodech i v dynamice růstu křivky zatížení. Tyto odlišnosti jsou způsobeny měřením v různých provozních podmínkách (došlo k vypnutí PC a následnému spuštění Tia Portalu).



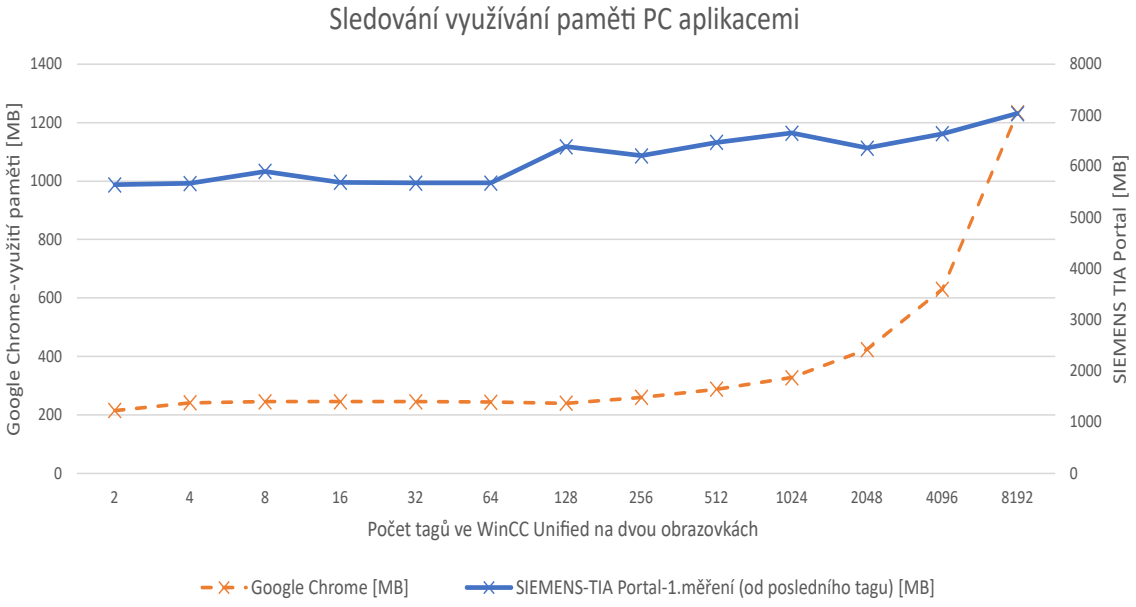
Obr. 5.32: Jedna HMI obrazovka, jeden PC uživatel.

Dvě Unified obrazovky, jeden PC uživatel

V tomto měření bylo žádoucí zjistit, zda-li při použití dvou obrazovek nedojde ke snížení zátěže aplikací Google Chrome či Tia Portalu. U Google Chromu můžeme pozorovat snížený nárůst zatížení oproti předchozímu měření s jednou obrazovkou. Používání dvou obrazovek u Tia Portalu zásadní význam na zatížení PC nepřináší. S přihlédnutím na předcházející měření zde nelze vysledovat dynamiku růstu zatížení programu na PC.

Počet tagů-1.obrazovka	Počet tagů-2.obrazovka	Celkem tagu	Google Chrome [MB]	SIEMENS-TIA Portal-1.měření (od posledního tagu) [MB]
1	1	2	214,7	5641,8
2	2	4	241,3	5669,9
4	4	8	245,1	5901,6
8	8	16	244,8	5691,2
16	16	32	245,5	5677,6
32	32	64	243,9	5674,8
64	64	128	239,6	6385,1
128	128	256	259,7	6208,8
256	256	512	287,7	6470,9
512	512	1024	327,1	6652,9
1024	1024	2048	423,9	6360,5
2048	2048	4096	629,8	6641,3
4096	4096	8192	1233,7	7035,5

Tab. 5.3: Dvě HMI obrazovky, jeden PC uživatel



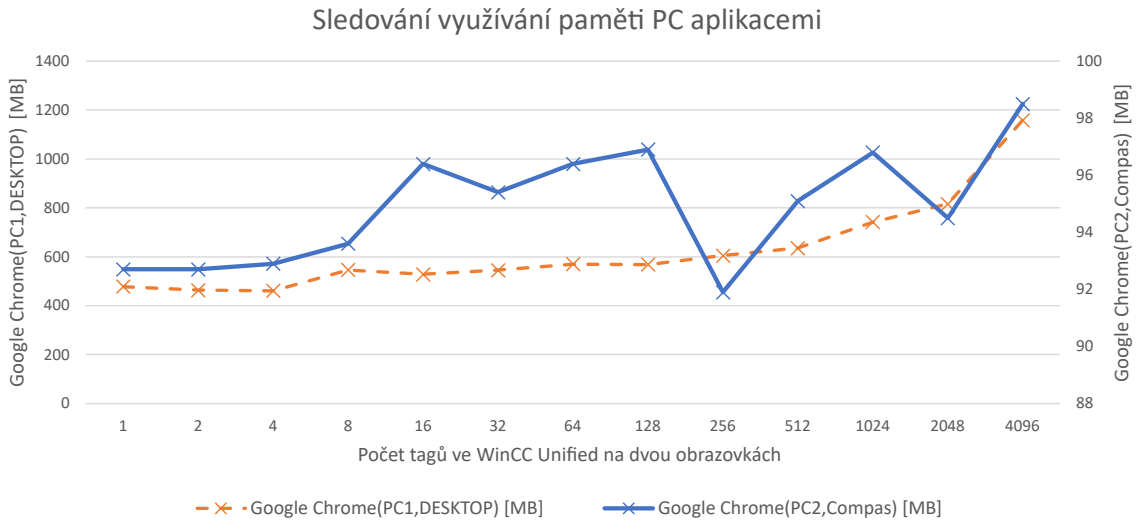
Obr. 5.33: Dvě HMI obrazovky, jeden PC uživatel.

Jedna Unified obrazovka, dva PC uživatelé

Cílem tohoto měření bylo zjistit, jak se projeví připojení druhého PC uživatele na zatížení PC. Bylo zjištěno, že hlavní zátěž aplikace Google Chrome byla přesunuta na druhého PC uživatele a zátěž na prvním PC uživateli (notebook Compas) se pohybovala od 92,7 po 98,5 MB. Oproti případu měření jedna Unified obrazovka, jeden PC uživatel zde nastala podstatná změna zatížení jak v nominálních hodnotách zatížení, tak dynamice jejího růstu.

Počet tagů-1.obrazovka	Google Chrome(PC1,DESKTOP) [MB]	Google Chrome(PC2,Compas) [MB]
1	478,3	92,7
2	463,2	92,7
4	460,9	92,9
8	546,2	93,6
16	528	96,4
32	545,5	95,4
64	569,8	96,4
128	568,5	96,9
256	605,2	91,9
512	635,8	95,1
1024	741,8	96,8
2048	815,7	94,5
4096	1158,6	98,5

Tab. 5.4: Jedna HMI obrazovka, dva PC uživatelé



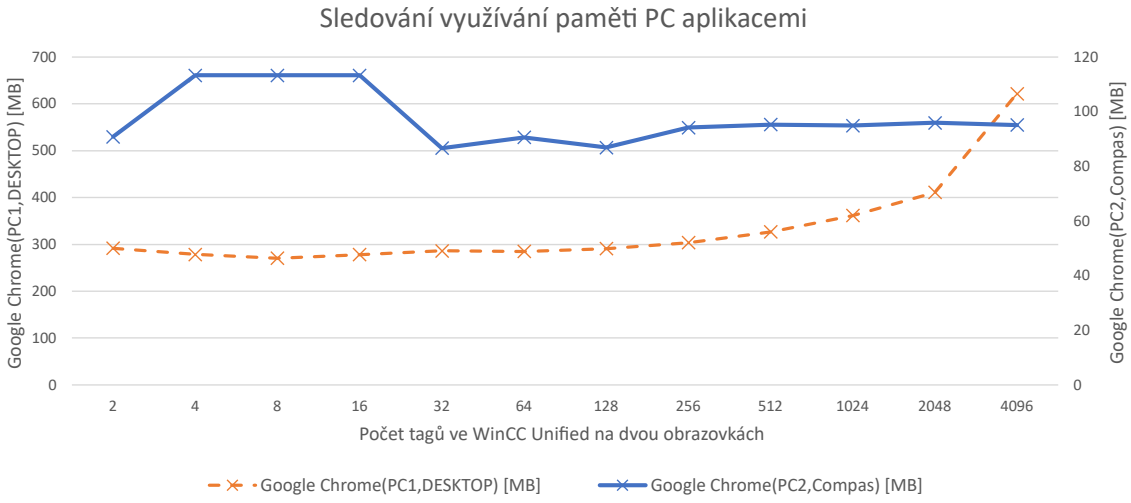
Obr. 5.34: Jedna HMI obrazovka, dva PC uživatelé.

Dvě Unified obrazovky, dva PC uživatelé

Dále byla zkoumána situace, kdy budou opět přítomni oba PC klienti, ale tagy se rozloží do dvou obrazovek. V porovnání s předcházejícím měřením *Dvě Unified obrazovky, jeden PC uživatel* zde došlo k mírné redukci zátěže, ale není pozorovatelný značný přínos redukce zatížení po připojení druhého PC uživatele.

Počet tagů-1.obrazovka	Počet tagů-2.obrazovka	Celkem tagu	Google Chrome(PC1,DESKTOP) [MB]	Google Chrome(PC2,Compas) [MB]
1	1	2	291,9	90,8
2	2	4	278,6	113,3
4	4	8	270,7	113,3
8	8	16	278,1	113,3
16	16	32	286,1	86,7
32	32	64	284,9	90,6
64	64	128	291,1	86,9
128	128	256	303,8	94,2
256	256	512	326,6	95,3
512	512	1024	361,5	94,9
1024	1024	2048	411,2	95,9
2048	2048	4096	621,7	95,1

Tab. 5.5: Dvě HMI obrazovky, dva PC uživatelé



Obr. 5.35: Dvě HMI obrazovky, dva PC uživatelé.

5.9 Zatížení CPU v závislosti na počtu tagů

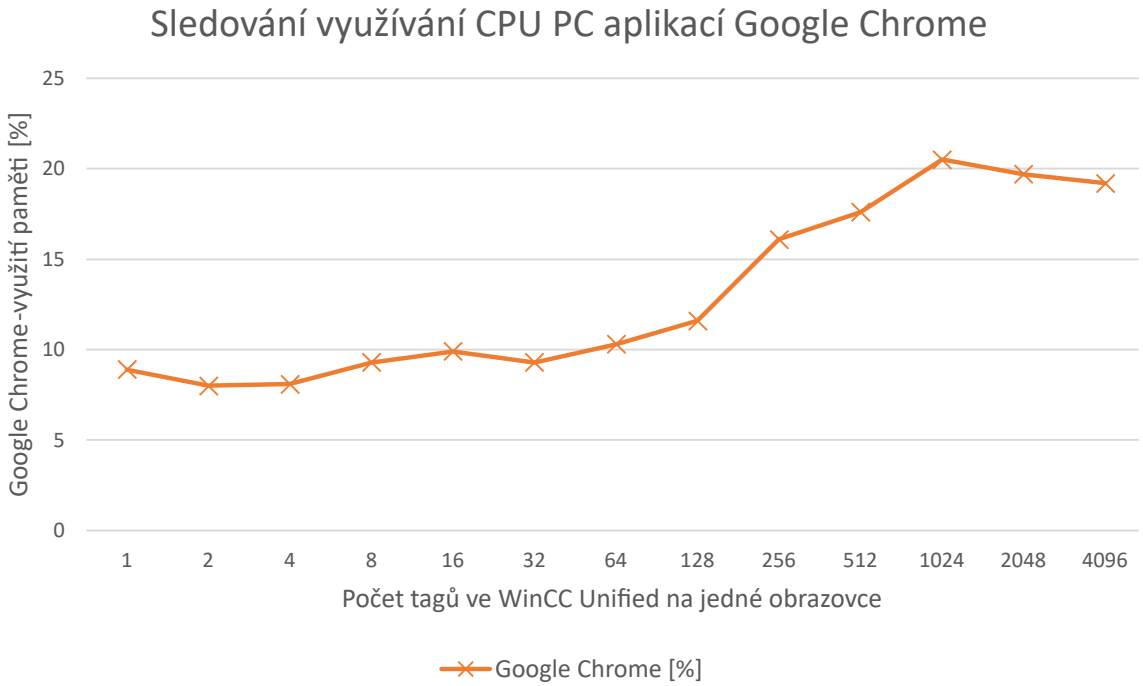
Tato část měření byla zaměřena na zatížení, které představuje aplikace Google Chrome na procesory Intel(R) Core™ i7-4800MQ CPU @ 2,70 GHz a Intel(R) Core™ i5-8300H CPU @ 2,30 GHz. Zatížení na procesoru bylo vybráno z důvodů toho, že paměť lze upgradovat, ale výkon procesoru zlepšit tak jednoduše nejde, resp. se dodatečný upgrade nevyplatí. Při měření se postupovalo obdobně jako u zátěže RAM, ale s tím rozdílem, že nebylo aplikováno 15 s zpoždění, ale hodnoty v grafech jsou maximální možné pro daný počet tagů. Pro zatížení byly zkoumány čtyři možnosti.

CPU – Jedna Unified obrazovka, jeden PC uživatel

Zde se podrobovala zkoušce pouze aplikace Google Chrome. Z grafu nelze predikovat/dopočítat, jaké zatížení by bylo pro jiný počet tagů. Nejvyšší procento zatížení je dosaženo při 1024 tazích, které se zde jeví spíše jako parazitní hodnota, jelikož nedává smysl, aby nejvyšší zátěž byla právě na 1024 tazích.

Počet tagů	Google Chrome [%]
1	8,9
2	8
4	8,1
8	9,3
16	9,9
32	9,3
64	10,3
128	11,6
256	16,1
512	17,6
1024	20,5
2048	19,7
4096	19,2

Tab. 5.6: CPU – Jedna HMI obrazovka, jeden PC uživatel



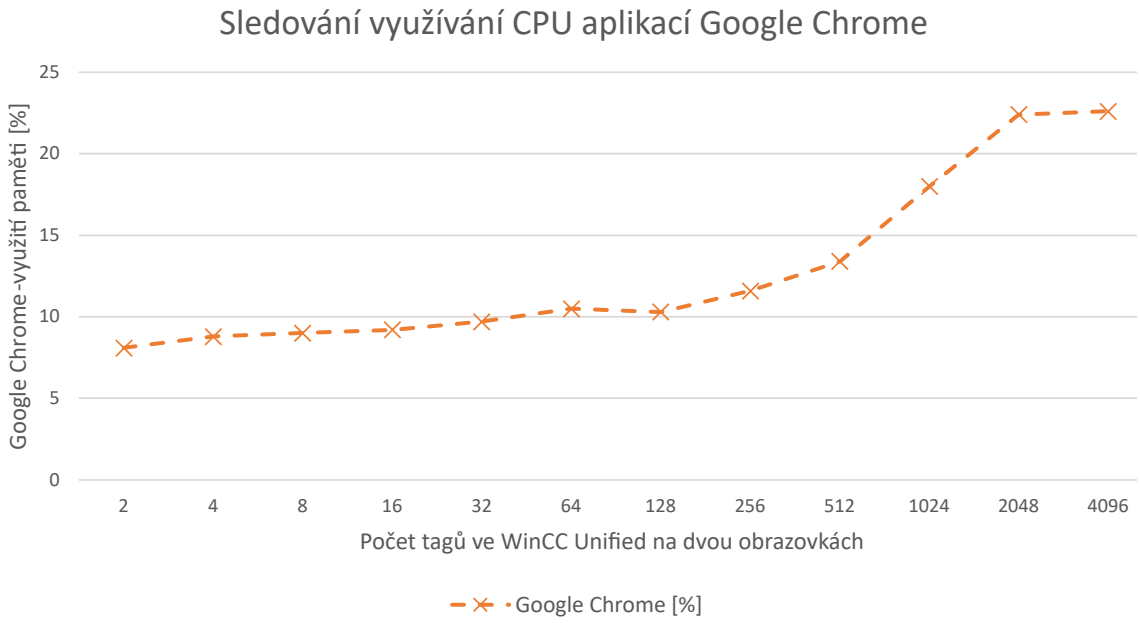
Obr. 5.36: CPU – Jedna HMI obrazovka, jeden PC uživatel.

CPU – Dvě Unified obrazovky, jeden PC uživatel

V případě použití dvou Unified obrazovek, kdy na každé z nich je 2048 tagů, je maximální zatížení 22,6 procent. V tomto měření nelze určit konkrétní závislost růstu na počtu tagů, růst má odlišnou dynamiku.

Počet tagů-1.obrazovka	Počet tagů-2.obrazovka	Celkem tagu	Google Chrome [%]
1	1	2	8,1
2	2	4	8,8
4	4	8	9
8	8	16	9,2
16	16	32	9,7
32	32	64	10,5
64	64	128	10,3
128	128	256	11,6
256	256	512	13,4
512	512	1024	18
1024	1024	2048	22,4
2048	2048	4096	22,6

Tab. 5.7: CPU – Dvě HMI obrazovky, jeden PC uživatel



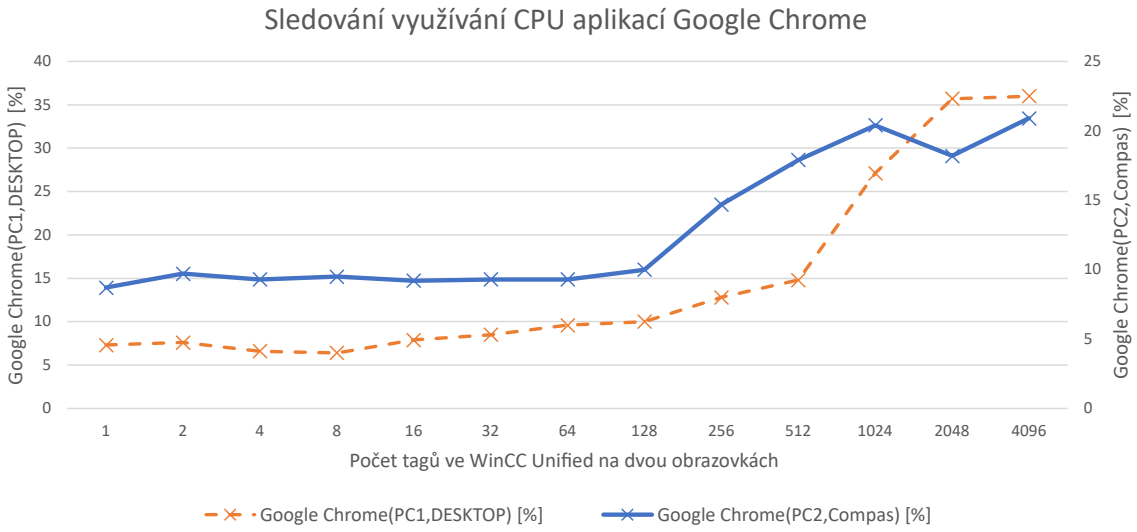
Obr. 5.37: CPU – Dvě HMI obrazovky, jeden PC uživatel.

CPU – Jedna Unified obrazovka, dva PC uživatelé

U uživatele č.1 (PC1) byl použit procesor Intel(R) Core™ i5-8300H CPU @ 2,30 GHz a u klienta č.2 (PC2) Intel(R) Core™ i7-4800MQ CPU @ 2,70 GHz. Křivka u uživatele č.1 se podobá křivce zatížení u měření *CPU – Dvě Unified obrazovky, jeden PC uživatel.*

Počet tagů-1.obrazovka	Google Chrome(PC1,DESKTOP) [%]	Google Chrome(PC2,Compas) [%]
1	7,3	8,7
2	7,6	9,7
4	6,6	9,3
8	6,4	9,5
16	7,9	9,2
32	8,5	9,3
64	9,6	9,3
128	10	10
256	12,8	14,7
512	14,8	17,9
1024	27,1	20,4
2048	35,7	18,2
4096	36	20,9

Tab. 5.8: CPU – Jedna HMI obrazovka, dva PC uživatelé



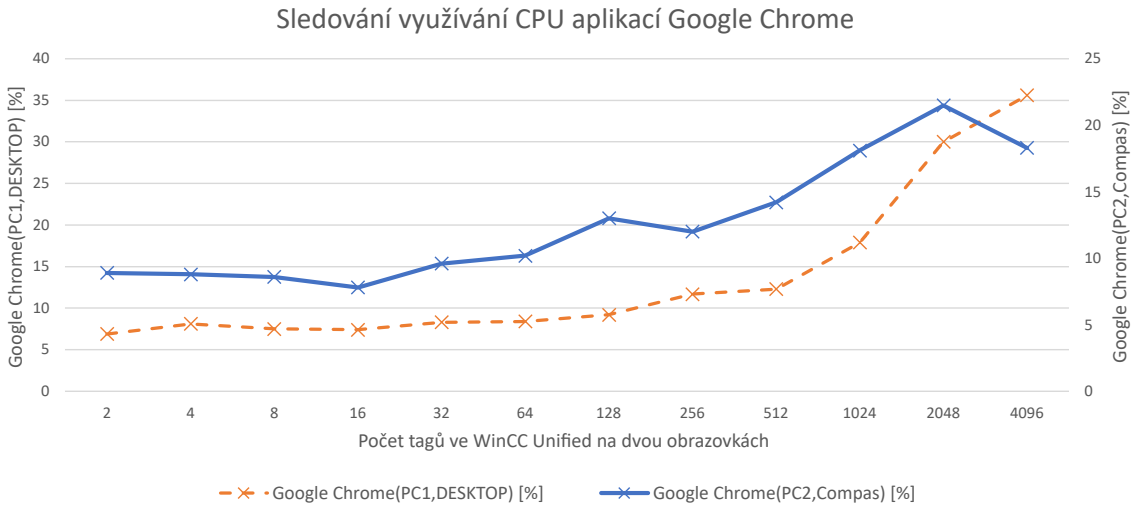
Obr. 5.38: CPU – Jedna HMI obrazovka, dva PC uživatelé.

CPU – Dvě Unified obrazovky, dva PC uživatelé

V tomto měření si lze všimnout u uživatele č.1 (PC1) jisté spojitosti s předcházejícím měřením. Od 512 tagu do 2048 tagu zde lze pozorovat mírnější nárůst zatížení.

Počet tagů-1.obrazovka	Počet tagů-2.obrazovka	Celkem tagu	Google Chrome(PC1,DESKTOP) [%]	Google Chrome(PC2,Compas) [%]
1	1	2	6,9	8,9
2	2	4	8,1	8,8
4	4	8	7,5	8,6
8	8	16	7,4	7,8
16	16	32	8,3	9,6
32	32	64	8,4	10,2
64	64	128	9,2	13
128	128	256	11,7	12
256	256	512	12,3	14,2
512	512	1024	17,9	18,1
1024	1024	2048	30	21,5
2048	2048	4096	35,6	18,3

Tab. 5.9: CPU-Dvě HMI obrazovky, dva PC uživatelé

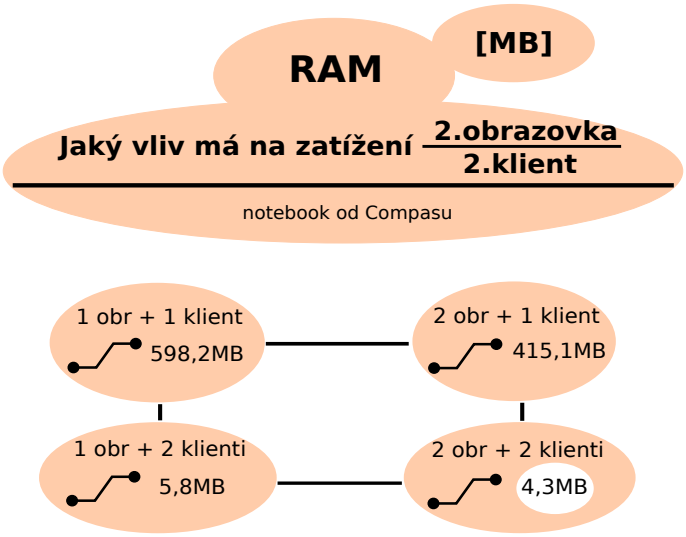


Obr. 5.39: CPU – Dvě HMI obrazovky, dva PC uživatelé.

5.10 Shrnutí výsledků měření zatížení

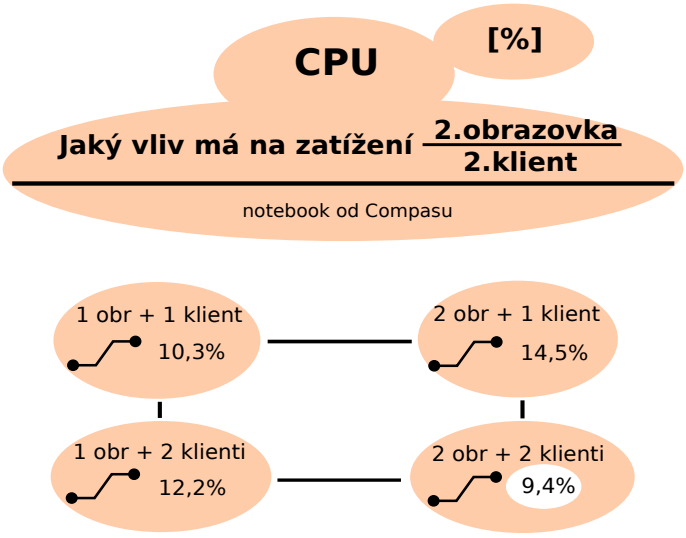
Pro přehlednost byla vypracována dvě schémata všech měření, které se týkaly zatížení RAM a CPU podle počtu tagů u aplikace Google Chrome. Hodnoty v elipsách jsou vždy výsledkem rozdílu hodnoty dosaženého zatížení u 4096 tagů a hodnoty zatížení u jednoho tagu pro notebook, kde je licencován Tia Portal a WinCC Unified. Např. pokud bylo u 4096 tagů naměřeno zatížení 95,1 MB a u jednoho tagu

zatížení 90,8 MB, tak výsledek je 4,3 MB. Z obrázku 5.40 lze zjistit, že nejvyššího rozdílu zatížení RAM je dosaženo při použití jedné HMI obrazovky a jednoho PC klienta. Naopak nejnižší rozdíl zatížení je při použití dvou HMI obrazovek a dvou PC klientů.



Obr. 5.40: Schéma zatížení RAM pro aplikaci Google Chrome.

Totéž schéma je aplikováno na zatížení CPU podle počtu tagů (obr. 5.41). Metoda výpočtů hodnot je stejná jako u zatížení RAM. Zde je patrný nejvyšší dosažený rozdíl zatížení u dvou obrazovek a jednoho PC klienta, nejnižší je opět při použití dvou obrazovek a dvou klientů.



Obr. 5.41: Schéma zatížení CPU pro aplikaci Google Chrome.

Závěr

Tato bakalářská práce Vytvoření průmyslového scénáře s využitím WinCC Unified se zabývala možnostmi vizualizace pomocí WinCC Unified, vzdáleným ovládáním procesů a možnostmi komunikace s návazností na popis bezpečnostních slabin systému. Praktická část obsahuje ověření funkčnosti uváděnou výrobcem, vytvoření HMI knihovny a analýzu zatížení komunikace mezi HMI a PLC.

Cílem prozkoumání možností vizualizace pomocí WinCC bylo zjistit, jaké prvky jsou pro uživatele k dispozici, jakou mají funkčnost a zda-li odpovídají deklaraci od výrobce. Možnosti vizualizace byly zkoumány na základě prostého zkoušení změn v nastavení základních prvků v simulačním prostředí. Je nutné dodat, že nebyly zkoumány všechny prvky a jejich funkce.

V oblasti vzdáleného ovládání procesů a popisu možností komunikace se pracovalo s výchozím nastavením komunikace, tedy v komunikaci nebyl použit OPC UA server ani klient. Dále byla použita tzv. komunikace server/klient, tzn. že na zařízení typu PLC, HMI byl vytvořen OPC UA server a WinCC Unified byl použit jako klient. Vytvoření komunikace server/klient bylo provedeno na základě vytvoření OPC UA spojení v programu Tia Portal s následným přiřazením adres konkrétním tagům. Do problematiky vzdáleného ovládání a komunikace lze rovněž zařadit vzdálenou komunikaci pomocí VPN, cloudu či OPC UA protokolu.

Při tvorbě HMI knihovny byla použita tzv. technika faceplate, ve které byly sdruženy funkce pro animaci a ovládání standardních funkčních bloků, nastavení potřebných parametrů a také zobrazení trendu a alarmů.

U analýzy zatížení komunikace mezi HMI a PLC v závislosti na počtu animovaných objektů bylo využito tagů typu Boolean, které byly postupně přidávány na HMI obrazovku. Analýza byla měřena Správcem úloh. Měření zatížení se týkalo aplikací Google Chrome, Tia Portal a jaký význam měly tyto aplikace na zatížení CPU a RAM paměti.

Jedním z výsledků bakalářské práce byla HMI knihovna. Aby mohla být aplikována v průmyslu, musí projít dalším vývojem, jelikož v ní chybí např. filtrace alarmů pro jednotlivá zařízení. Dílčím výsledkem je analýza zatížení komunikace na základě počtu animovaných objektů na HMI obrazovce. Analýza neprokázala, že by při použití až 4096 tagů docházelo k jakýmkoliv problémům s komunikací.

Do budoucna se jeví možnost použití WinCC Unified na mobilní telefony či chytré hodinky. Dále lze očekávat nástup nové verze WinnCC Unified a s tím spojená vylepšení.

Literatura

[1] HOMELAND SECURITY. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies.* [online]. 2016 [cit. 10. 12. 2021]. Dostupné z URL: <https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>.

[2] UNIFIED AUTOMATION. *OPC Unified Architecture Overview.* [online]. 2022 [cit. 24. 4. 2022]. Dostupné z URL: <https://documentation.unified-automation.com/uasdkcpp/1.7.3/html/L2OpcUaFundamentalsOverview.html>.

[3] VOJÁČEK, A. *Průmyslová komunikace OPC UA - 1.díl, popis protokolu.* [online]. 22.7.2020 [cit. 5. 12. 2021]. Dostupné z URL: <https://automatizace.hw.cz/prumyslova-komunikace-opc-ua-1dil-popis-protokolu.html>.

[4] OPC FOUNDATION. *OPC Unified Architecture Part 4: Services, Release 1.05.00.* [online]. 27.10.2021 [cit. 24. 5. 2022]. Dostupné z URL: <https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-4-services/>.

[5] BELDING, G. *Types of ICS.* [online]. 8.8.2019 [cit. 5. 12. 2021]. Dostupné z URL: <https://resources.infosecinstitute.com/topic/types-of-ics/>.

[6] PROCENTEC. *Profibus vs Profinet: what are the main differences?* [online]. 2021 [cit. 5. 12. 2021]. Dostupné z URL: <https://procentec.com/content/profibus-vs-profinet-what-are-the-main-differences/>.

[7] POHLMANN, U., SIKORA, A. *Practical Security Guidelines for Building OPC UA Applications.* [online]. 2018 [cit. 19. 2. 2022]. Dostupné z URL: <https://opcconnect.opcfoundation.org/2018/06/practical-security-guidelines-for-building-opc-ua-applications/>.

[8] KERCL, J. *Bezpečnost informačního systému: bakalářská práce.* Praha: České vysoké učení technické v Praze, Fakulta elektrotechnická, 2010. 52 stran. Vedoucí práce Ing. Josef Semrád.

[9] JOKI-HOLLANTI, O. *WinCC Unifiedin ja WinCC Professionalin Tuoteominaisuuksien Vertailu.* Finsko: Centria-Ammattikorkeakoulu, 2021. 28 stran. Vedoucí práce Hannu Ala-Pöntiö.

[10] AUTOMATION FAIR. *Simatic WinCC Unified V17.* [online]. 24.10.2021 [cit. 11. 12. 2021]. Dostupné z URL: <https://www.automation-fair.com/2021/10/24/simatic-wincc-unified-v17/>.

[11] MURRELEKTRONIK CZ, spol. s r. o. *Profinet versus Profibus.* [online]. Automa. 2012, no.5, s.69 [cit. 5. 12. 2021]. Dostupné z URL: <https://automa.cz/cz/casopis-clanky/profinet-versus-profibus-2012_05_0_9618/>.

[12] ELVAC, a.s. *Tři zranitelná místa v zabezpečení průmyslových sítí.* [online]. 2015 [cit. 21. 11. 2021]. Dostupné z URL: <http://automa.cz/Aton/FileRepository/pdf_articles/53408.pdf>.

[13] MINAŘÍK, P. *Bezpečnost průmyslovýchsítí a systémů SCADA/ICS.* [online]. 2018 [cit. 21. 11. 2021]. Dostupné z URL: <https://www.flowmon.com/Flowmon/media/content/it-systems-2018-09-13-strana-30-31.pdf>.

[14] STOUFFER, K., LIGHTMAN, S., PILLITTERI, V., ABRAMS, M., HAHN, A *Guide to Industrial Control Systems (ICS) Security.* [online]. 2014 [cit. 19. 2. 2022]. Dostupné z URL: <http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf>.

[15] REID, M. *PLC vs DCS - What's the difference?* [online]. 2021 [cit. 26. 2. 2022]. Dostupné z URL: <https://www.linkedin.com/pulse/plc-vs-dcs-whats-difference-mathew-reid>.

[16] ESET. *Proč používat VPN? 4 hlavní výhody virtuální privátní sítě.* [online]. 2021. [cit. 13. 11. 2021]. Dostupné z URL: <https://www.eset.com/cz/blog/prevence/proc-pouzivat-vpn-4-hlavni-vyhody-virtualni-privatni-site/>.

[17] ŠTEIDL, P. *Srovnání VPN realizací: diplomová práce.* Brno: Masarykova univerzita, Fakulta informatiky, 2007. 51 stran. Vedoucí práce RNDr. Radek Ošlejšek, Ph.D.

[18] INDRA, M. *Šifrovací algoritmy: bakalářská práce.* Pardubice: Univerzita Pardubice, Fakulta elektrotechniky a informatiky, 2014. 69 stran. Vedoucí práce Ing. Petr Veselý.

[19] SIEMENS, s.r.o. *OPC UA.* [online]. 2022 [cit. 19. 2. 2022]. Dostupné z URL: <https://new.siemens.com/cz/cs/products/automation/industrial-communication/opc-ua.html>.

[20] FOXON s.r.o. *OPC UA Vám zjednodušší život, ale...* [online]. 2019 [cit. 19. 2. 2022]. Dostupné z URL: <https://foxon.cz/blog/ostatni/454-opc-ua-vam-zjednodusi-zivot-ale?search=&gclid=Cj0KCQiAr5iQBhCsARIsAPcwROMnEyPbDHOddiTpmDy8Uf_fIpgMJpvgXYaZ8FXaSVYuqK0URQ4mu3oaApDSEALw_wcB>.

[21] SIEMENS, s.r.o. *SIMATIC WinCC Unified System, webinar presentation.* [online]. 2020. [cit. 5. 11. 2021]. Dostupné z URL: <https://assets.new.siemens.com/siemens/assets/api/uuid:cf0c75b3-32cb-4fdc-a226-2c1d379dfec7/simatic-wincc-unified-pc-webinar-110520.pdf>.

[22] BOWMAN, B. *The AAA Framework for Identity Access Security.* [online]. 2019 [cit. 19. 2. 2022]. Dostupné z URL: <https://securityboulevard.com/2019/03/the-aaa-framework-for-identity-access-security/>.

[23] SIEMENS, s.r.o. *SIEMENS HMI template suite.* [online]. 2021. [cit. 2. 11. 2021]. Dostupné z URL: <https://cache.industry.siemens.com/dl/files/767/91174767/att_1021068/v2/91174767_HMITemplateSuiteUnified_V10_DOC_en.pdf>.

[24] SIEMENS, s.r.o. *Perfect interaction between OT and IT networks.* [online]. 2021. [cit. 6. 11. 2021]. Dostupné z URL: <https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-network-solutions/ot-it-networks.html?gclid=CjwKCAjwz5iMBhAEEiwAMEAwGMXmOmPTItGGIgUWejNttuV1N3CMV4KpzQRcWjPR8clSSt1kBGYxDBoCAHsQAvD_BwE>.

[25] VOJÁČEK, A. *Vzdálená práce a přístup v průmyslu.* [online]. 2021 [cit. 17. 11. 2021]. Dostupné z URL: <https://automatizace.hw.cz/moznosti-vzdaleneho-pristupu-k-prumyslovym-systemum.html>.

[26] SIEMENS, s.r.o. *Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices.* [online]. 2020 [cit. 15. 10. 2021]. Dostupné z URL: <https://cache.industry.siemens.com/dl/files/300/109481300/att_1039769/v2/109481300_SecurityGuidelineUnified_V10_en.pdf>.

[27] SIEMENS, s.r.o. *SCALANCE M: industrial routers for IP-based networks.* [online]. 2021. [cit. 16. 10. 2021]. Dostupné z URL: <https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/remote-networks/scalance-m-industrial-routers-ip-based-networks.html>.

[28] SIEMENS, s.r.o. *Visualization with WinCC Unified, now even more flexible!* [online]. 2021. [cit. 16. 10. 2021]. Dostupné z URL: <https://new.siemens.com/global/en/products/automation/simatic-hmi/wincc-unified.html>.

[29] SIEMENS, s.r.o. *HMI template suite.* [online]. 2021. [cit. 2. 11. 2021]. Dostupné z URL: <https://new.siemens.com/global/en/products/automation/simatic-hmi/hmi-template-suite.html>.

[30] SIEMENS, s.r.o. *SIEMENS support request.* [online]. 2021. [cit. 2. 11. 2021]. Dostupné z URL: <https://support.industry.siemens.com/tf/bd/en/posts/using-winc c-unified-with-simulator/229741/?page=0&pageSize=10>.

[31] SIEMENS, s.r.o. *Delivery release SIMATIC WinCC Unified Plant Intelligence options V17.* [online]. 2021. [cit. 4. 11. 2021]. Dostupné z URL: <https://support.industry.siemens.com/cs/document/109792168/delivery-release-simatic-wincc-unified-plant-intelligence-options-v17?dti=0&lc=en-WW>.

[32] SIEMENS, s.r.o. *PCC The Future of SIMATIC HMI.* [online]. 2019. [cit. 4. 11. 2021]. Dostupné z URL: <https://www.pccweb.com/wp-content/uploads/2019/11/S1-2019_10_PCC_OKTOBERFEST_HMI_Future.pdf>.

[33] SIEMENS, s.r.o.: *Průmyslové komunikační sítě.* [online]. 2021. [cit. 5. 11. 2021]. Dostupné z URL: <https://new.siemens.com/cz/cs/reseni/digitalni-podnik/industrial-communication-networks.html>.

[34] MANTLE, J. *The 5 Layers of the Automation Pyramid and Manufacturing Operations Management.* [online]. 2019 [cit. 6. 11. 2021]. Dostupné z URL: <https://www.syspro.com/blog/erp-for-manufacturing/the-5-layers-of-the-automation-pyramid-and-manufacturing-operations-management/>.

[35] ICT BLOG. *IT a OT – postupné sbližování dvou světů.* [online]. 14.2.2021 [cit. 6. 11. 2021]. Dostupné z URL: <https://www.ictblog.cz/it-a-ot-postupne-sblizovani-dvou-svetu/>.

[36] PORUBOVA, A. *Vysokorychlostní virtuální privátní sítě: bakalářská práce.* Brno: Vysoké učení technické v Brně, Fakulta Elektrotechniky a komunikačních technologií, 2017. 45 stran, Vedoucí práce Ing. Lukáš Malina, Ph.D.

[37] VEŘMIŘOVSKÝ, R. *Virtuální privátní síť: diplomová práce.* Ostrava: VŠB - Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, 2010. 46 stran, 3 přílohy. Vedoucí práce Ing. Jaroslav Zdrálek, Ph.D.

[38] MILOŠ, J. *Kryptografické metody zabezpečení dat: bakalářská práce.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 43 stran. Vedoucí práce Ing. Petra Lambertová.

[39] VALENTA, M. *Cloudové řešení pro řízení týmových projektů: bakalářská práce.* Plzeň: Západočeská univerzita v Plzni, Fakulta strojní, 2019. 48 stran. Vedoucí práce doc. Ing. Milan Edl Ph.D.

[40] SEVERA, J. *Cloud computing v IT průmyslu: bakalářská práce.* Praha: Bankovní institut vysoká škola Praha, 2012. 49 stran. Vedoucí práce Ing. Bc. Jiří Rezler.

[41] SIEMENS, s.r.o. *Web visualization with WinCC Unified View of Things.* [online]. 2021 [cit. 21. 11. 2021]. Dostupné z URL: <https://new.siemens.com/global/en/products/automation/simatic-hmi/wincc-unified/view-of-things-web-hmi.html>.

[42] SIEMENS, s.r.o.: Industry online support. *Delivery Release SIMATIC WinCC Unified V17 ES and RT.* [online]. 2021 [cit. 28. 11. 2021]. Dostupné z URL: <https://support.industry.siemens.com/cs/document/109792165/delivery-release-simatic-wincc-unified-v17-es-rt?dti=0&lc=en-US>.

[43] SIEMENS, s.r.o.: Industry online support. *Delivery release SIMATIC WinCC V17.* [online]. 2021 [cit. 28. 11. 2021]. Dostupné z URL:

<https://support.industry.siemens.com/cs/document/109795525/delivery-release-simatic-wincc-v17?dti=0&lc=en-US>.

[44] SIEMENS, s.r.o. *Čas na změnu – přejděte z PROFIBUSu na PROFINET.* [online]. 2021 [cit. 5. 12. 2021]. Dostupné z URL: <https://new.siemens.com/cz/cs/products/automation/industrial-communication/profinet/pb-2-pn.html>.

[45] KNIGHT, J. *EtherNet/IP vs Profinet - a Comparison.* [online]. 2020 [cit. 5. 12. 2021]. Dostupné z URL: <https://eecoonline.com/ethernetip-vs-profinet-protocol-heavyweights/>.

[46] EITEL, L. *EtherNet/IP versus PROFINET.* [online]. 11.5.2020 [cit. 5. 12. 2021]. Dostupné z URL: <https://www.digikey.com/en/articles/ethernet-ip-versus-profinet>.

[47] DOMAT CONTROL SYSTEM s.r.o. *Komunikační protokol Modbus v kostce.* [online]. 23.5.2020 [cit. 5. 12. 2021]. Dostupné z URL: <https://elektro.tzb-info.cz/126361-komunikacni-protokol-modbus-v-kostce>.

[48] HAVLE, O. *Jak na Modbus?* [online]. Automa. 2009, no.10, [cit. 5. 12. 2021]. Dostupné z URL: <https://automa.cz/cz/casopis-clanky/jak-na-modbus-2009_02_38594_5436/>.

[49] GASTREICH, W. *What is Modbus?* [online]. 3.12.2018 [cit. 5. 12. 2021]. Dostupné z URL: <https://realpars.com/modbus/>.

[50] DIXON, M. *What is DeviceNet?* [online]. 24.12.2018 [cit. 5. 12. 2021]. Dostupné z URL: <https://realpars.com/devicenet/>.

[51] JOWETT, J. *What is IO-Link?* [online]. 21.10.2019 [cit. 5. 12. 2021]. Dostupné z URL: <https://realpars.com/io-link/>.

[52] MICROSYS, spol. s.r.o. *Komunikace přes rozhraní OPC.* [online]. 2018 [cit. 5. 12. 2021]. Dostupné z URL: <https://www.promotic.eu/cz/pmdoc/Subsystems/Comm/OPC/OPC.htm>.

[53] STIANKO, PETERKA. *OPC v průmyslové komunikaci.* [online]. 2004 [cit. 5. 12. 2021]. č.6 Dostupné z URL: <https://automa.cz/cz/casopis-clanky/opc-v-prumyslove-komunikaci-2004_06_32378_2345/>.

[54] MICROSYS, spol. s.r.o. *Komunikace přes rozhraní OPC UA.* [online]. 2018 [cit. 5. 12. 2021]. Dostupné z URL: <https://www.promotic.eu/cz/pmdoc/Subsystems/Comm/OPC/OPCUA.htm>.

[55] THE AUTOMIZATION.COM. *OPC-UA vs DA.* [online]. 2019 [cit. 5. 12. 2021]. Dostupné z URL: <https://theautomization.com/opc-ua-vs-da/>.

[56] MATRIKON. *What is DA and HDA?* [online]. 15.7.2021 [cit. 5. 12. 2021]. Dostupné z URL: <https://honeywellprocess-community.force.com/opcsupport/s/article/What-is-DA-and-HDARef-KB-976>.

[57] EMERSON, DELTAV. *OPC Alarms and Events Overview.* [online]. 2016 [cit. 5. 12. 2021]. Dostupné z URL: <https://www.emerson.com/documents/automation/white-paper-opc-alarms-events-overview-deltav-en-56294.pdf>.

[58] HOWTOUSELINUX.COM. *Understanding PSH ACK TCP Flags* [online]. 29.11.2021 [cit. 5. 12. 2021]. Dostupné z URL: <https://www.howtouselinux.com/post/psh-ack-tcp-flags>.

[59] RAPID7. *Firewall Reporting Excessive SYN Packets? Check Rate of Connections.* [online]. 27.11.2017 [cit. 5. 12. 2021]. Dostupné z URL: <https://www.rapid7.com/blog/post/2017/11/27/firewall-reporting-excessive-syn-packets/>.

[60] KRAWCZYK, H., PATERSON, K.G., WEE, H. *On the Security of the TLS Protocol: A Systematic Analysis.* [online]. 2013 [cit. 10. 12. 2021]. Dostupné z URL: <https://link.springer.com/content/pdf/10.1007%2F978-3-642-40041-4_24.pdf>.

[61] RESCORLA, E. *HTTP Over TLS.* [online]. 2000 [cit. 10. 12. 2021]. Dostupné z URL: <https://www.hjp.at/doc/rfc/rfc2818.html#sec_2https://www.hjp.at/doc/rfc/rfc2818.html#sec_2>.

[62] HERNÁNDEZ, A. F., LÓPEZ, J. *Speeding up Elliptic Curve Cryptography on the P-384 Curve.* [online]. 2016 [cit. 10. 12. 2021]. Dostupné z URL: <https://www.researchgate.net/publication/322056853_Speeding_up_Elliptic_Curve_Cryptography_on_the_P-384_Curve>.

[63] DOLBEAU, R. *An hybrid AES 256 GCM implementation for NEON CPU CUDA GPU.* [online]. 2014 [cit. 10. 12. 2021]. Dostupné z URL: <https://www.researchgate.net/profile/Romain-Dolbeau/publication/326423568_An_hybrid_AES-256-GCM_implementation_for_NEON_CPU_CUDA_GPU/links/5b4cb06c0f7e9b240fe2d9f6/An-hybrid-AES-256-GCM-implementation-for-NEON-CPU-CUDA-GPU.pdf>.

[64] SIEMENS, s.r.o. *WinCC V17 Innovations and Unified Highlights.* [online]. 2021 [cit. 11. 12. 2021]. Dostupné z URL: <https://assets.new.siemens.com/siemens/assets/api/uuid:20246010-a0d7-4c88-82d6-afec019d5273/v17-launch-webnar-wincc-unified-v17-highlight-innvovations.pdf>.

[65] SIEMENS, s.r.o. *Výrobní informační systémy (MES).* [online]. 2022 [cit. 19. 2. 2022]. Dostupné z URL: <https://www.plm.automation.siemens.com/global/cz/our-story/glossary/manufacturing-execution-systems-mes/38072>.

[66] MICROSOFT. *Co je to ERP a proč ho potřebujete?* [online]. 2022 [cit. 19. 2. 2022]. Dostupné z URL: <https://dynamics.microsoft.com/cs-cz/erp/what-is-erp/>.

[67] PYRAMID SOLUTIONS. *3 Major Differences Between an MES and ERP System.* [online]. 2022 [cit. 19. 2. 2022]. Dostupné z URL: <https://pyramidsolutions.com/intelligent-manufacturing/blog-im/3-differences-between-mes-and-erp/>.

[68] WALKOWSKI, D. *What Is the CIA Triad?* [online]. 2019 [cit. 19. 2. 2022]. Dostupné z URL: <https://www.f5.com/labs/articles/education/what-is-the-cia-triad>.

[69] INDUCTIVE AUTOMATION. *What is SCADA?* [online]. 2018 [cit. 26. 2. 2022]. Dostupné z URL: <https://inductiveautomation.com/resources/article/what-is-scada>.

[70] BEER, J. *SCADA systémy pro průmyslové aplikace: bakalářská práce.* Plzeň: Západočeská Univerzita v Plzni, 2015. 46 stran. Vedoucí práce Ing. Martin Sirový Ph.D.

[71] MICROSYS, spol. s.r.o. *Co je to SCADA?* [online]. 2022 [cit. 26. 2. 2022]. Dostupné z URL: <https://www.promotic.eu/cz/pmdoc/WhatIsPromotic/WhatIsScada.htm>.

[72] MICROSYS, spol. s.r.o. *Vítejte na webovém portálu SCADA/HMI systému PROMOTIC.* [online]. 2022 [cit. 27. 2. 2022]. Dostupné z URL: <https://www.promotic.eu/cz/index.htm?gclid=CjwKCAiA9tyQBhAIEiwA6tdCrDMhiSykNyhPx4hB9RUbJnqM8M5COf-EBfKw0dcZnlWLkdM7BzcMyxoCahwQAvD_BwE>.

[73] UNIPI TECHNOLOGY, DCEŘINÁ SPOLEČNOST FASTER CZ spol. s r.o. *Mervis SCADA.* [online]. 2022 [cit. 27. 2. 2022]. Dostupné z URL: <https://www.unipi.technology/cs/produkty/mervis-scada-335>.

[74] SSLMENTOR.CZ. *SSL certifikát pro www stránky.* [online]. 2022 [cit. 7. 3. 2022]. Dostupné z URL: <https://www.sslmentor.cz/ssl/ssl-certifikaty>.

[75] COMES, spol. s.r.o. *SSL Certifikát.* [online]. 2022 [cit. 7. 3. 2022]. Dostupné z URL: <https://www.comes.cz/produkty/komunikace/ssl-certifikat/>.

[76] ŠTRÁFELDA, J. *SVG.* [online]. 2022 [cit. 7. 3. 2022]. Dostupné z URL: <https://www.strafelda.cz/svg>.

[77] COPE, K. *What is the automation pyramid?* [online]. 11.6.2018 [cit. 22. 5. 2022]. Dostupné z URL: <https://realpars.com/automation-pyramid/>.

[78] RAHMAN, M., FENTAYE, A., ZACCARIA, V., ASLANIDOU, I. *A Framework for Learning System for Complex Industrial Processes.* [online]. 2021 [cit. 22. 5. 2022]. Dostupné z URL: <https://www.researchgate.net/figure/The-automation-pyramid-of-a-typical-industrial-plant_fig2_349412387>.

Seznam symbolů a zkratek

ACK potvrzení – Acknowledgement

AEAD autentizované šifrování s přidruženými daty – Authenticated Encryption with Associated Data

AQM analogový motor

ARP protokol pro rozlišení adresy – Address Resolution Protocol

cca přibližně

CIP společný průmyslový protokol – Common Industrial Protocol

CNC počítačem řízený obráběcí stroj – Computer Numerical Control

DCS distribuovaný řídící systém – Distributed control system

DoS odepření přístupu – Denial of Service

DQM digitální motor

DQV digitální ventil

ERP plánování podnikových zdrojů – Enterprise Resource Planning

FB funkční blok

GCM galoisovský čítačový režim – Galois Counter Mode

HMI rozhraní mezi člověkem a strojem – Human Machine Interface

HTML hypertextový značkovací jazyk – Hypertext Markup Language

HTTP protokol používaný pro přenos HTML stránek – Hypertext Transfer Protocol

HTTPS protokol používaný pro zabezpečený přenos HTML stránek – Hypertext Transfer Protocol Secure

IACS průmyslová automatizace či řídící systémy – Industrial Automation and Control Systems

ICS průmyslové řídící systémy – Industrial Control System

IE průmyslový ethernet – Industrial Ethernet

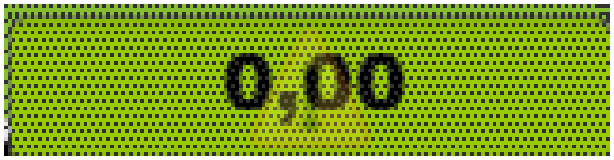
IoT	internet věcí – Internet of Things
IP	internetový protokol – Internet Protocol
IT	informační síť – Information Technology
MES	výrobní informační systém – Manufacturing Execution Systems
např.	například
OB	organizační blok
obr.	obrázek
OPC AE	přístup k historickým datům a alarmům – Open Platform Communications Alarms and Events
OPC DA	přístup k procesním datům – Open Platform Communications Data Access
OPC UA	otevřená platforma komunikace jednotné architektury – Open Platform Communications Unified Architecture
OT	provozní síť – Operational Technology
PC	osobní počítač
PLC	programovatelný logický automat – Programmable Logic Controller
příp.	případně
PSH	příchozí data jsou předána přímo aplikaci – Push
px	pixel
RAM	paměť s náhodným přístupem – Random Access Memory
resp.	respektive
RT	runtime
RTU	vzdálená jednotka terminálu – Remote Terminal Unit
SCADA	systémy dohledové kontroly a získávání dat – Supervisory Control And Data Acquisition
SSL	vrstva bezpečných socketů, zabezpečená šifrovaná komunikace – Secure Sockets Layer

SVG	škálovatelná vektorová grafika – Scalable Vector Graphic
tab.	tabulka
TCP	protokol kontroly přenosu – Transmission Control Protocol
Tia	plně integrovaný portál pro automatizaci – Totally Integrated Automation Portal
TLS	zabezpečení transportní vrstvy – Transport Layer Security
tzn.	to znamená
tzv.	tak zvaný
VNC	virtuální výpočetní síť – Virtual Network Computing
VPN	virtuální privátní síť – Virtual Private Network

A Příloha č.1–Problémy při tvorbě projektu

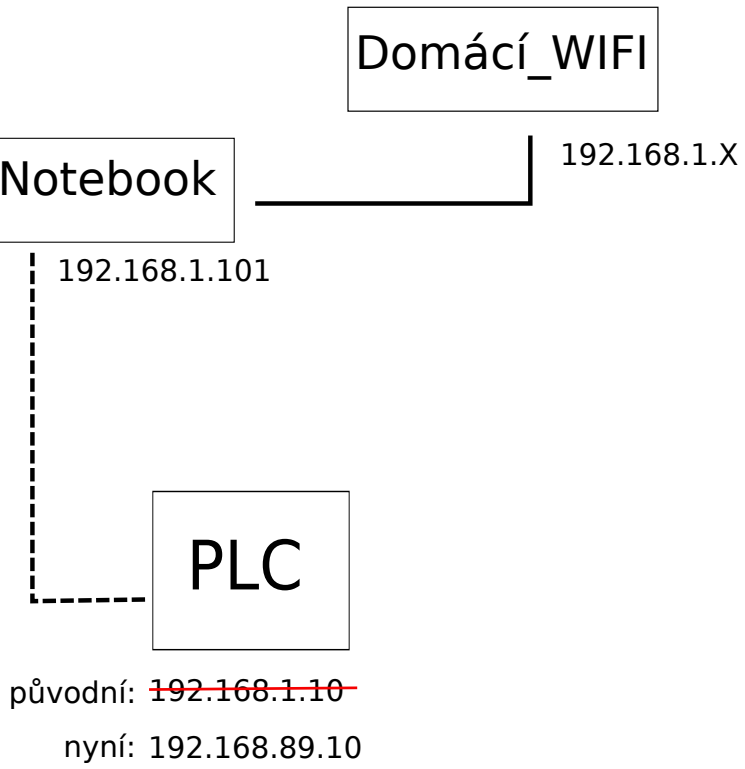
A.1 Nefunguje komunikace mezi simulací a PLC – žlutý vykřičník

Jeden z problémů, který může uživatele během vytváření projektu provázet, je nefungující komunikace mezi simulátorem a PLC. Tento problém je charakteristický žlutým vykřičníkem na obrazovce viz obr. A.1 a v SIMATIC RUNTIME Manageru se zobrazuje simulace jako tzv. *Partly Running*.



Obr. A.1: Problém v komunikaci.

Tento problém nastává, pokud zařízení (PC, notebook, ...) má stejnou adresu sítě jako PLC.



Obr. A.2: Znázornění přidělení IP adres.

Pokud poskytovatel internetového připojení přiděluje adresy v rozsahu *192.168.1.X.*, zařízení (např. PC) může být přidělena IP adresa 192.168.1.101. Problém s komunikací nastává až v případě, kdy je PLC zařízení přidělena adresa např. *192.168.1.10* a dochází ke kolizi. K nápravě je potřeba nahradit číslo jedna na číslo např. osmdesát devět.

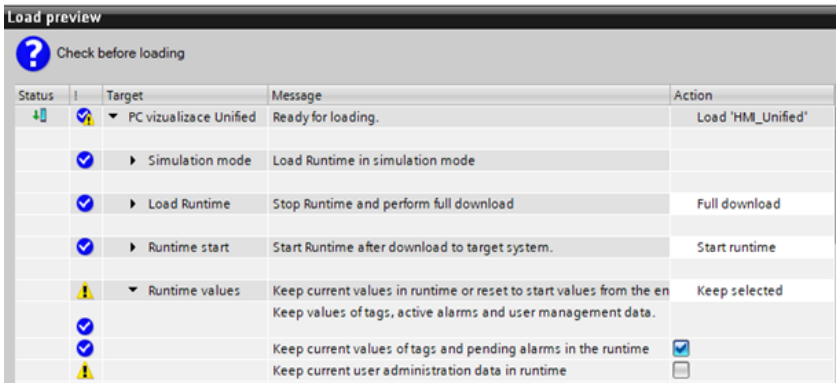
A.2 Použití PLCSIM nebo PLCSIM Advanced

V programu Tia Portal v17 je možné použít PLCSIM Advanced i simulátor PLCSIM, který umožňuje testovat simulaci systémů s komunikací PLC a HMI mezi sebou. To však neplatí pro Tia Portal v 16, kde musí být použit pouze PLCSIM Advanced. [30]

A.3 Ztráta schopnosti zápisu hodnot tagů na straně klienta

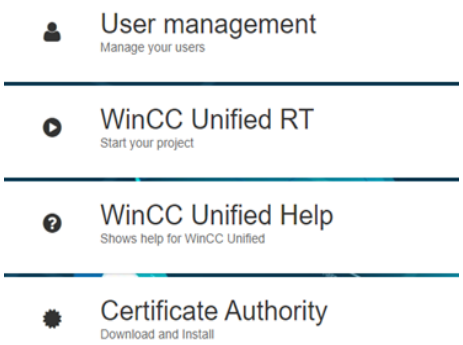
Tento problém může nastat při konfiguraci komunikace server (PLC, HMI) – klient (WinCC Unified). Tento problém v praxi znamená, že uživatel není schopen ve webovém prohlížeči měnit hodnoty tagů (animovaných objektů) a to i v případě, pokud je uživateli přiřazena role *HMI Administrátora* a tagy jsou tzv. *zapisovatelné a přístupné z HMI/OPC UA a aplikačního rozhraní*. Pokud uživatel změní hodnotu tagu na serveru např. na HMI panelu, změna hodnoty tagu se ve webovém prohlížeči ihned projeví.

Jako řešení tohoto problému lze použít druhého uživatele, kterého je nutné vytvořit v záložce *Uživatelé a role* a kterému bude přiřazena role HMI Administrátor. Při startu simulace je nutné zrušit volbu Držet aktuální data správy uživatelů viz obr. A.3. Tímto krokem je docíleno přidání nového uživatele do projektu.



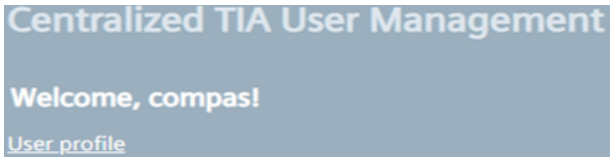
Obr. A.3: Přepsání stávajících uživatelů.

Další nutné úkony jsou prováděny již ve webovém prohlížeči v rámci základní nabídky možností viz obr. A.4.



Obr. A.4: Základní nabídka možností.

Zobrazení vizualizace lze dosáhnou dvěma způsoby. První způsob je reprezentován možností *WinCC Unified RT*, poté je po uživateli požadováno zadání uživatelského jména a hesla. Druhý způsob je veden přes tzv. *Správu uživatelů*, kde je také nutné opět zadat přihlašovací údaje. Po úspěšném přihlášení je načtena úvodní hláška viz obr. A.5. Toto okno lze již zavřít, dále je nutné opět přejít na základní nabídku možností a kliknout na možnost *WinCC Unified RT*. Po této sérii akcí by mělo dojít k zobrazení startovací obrazovky. V této chvíli je používán pomocný uživatel, toho je nutné odhlásit a poté zopakovat druhý způsob přihlašování pro již dříve vytvořeného uživatele, který byl vytvořen v Tia Portalu.



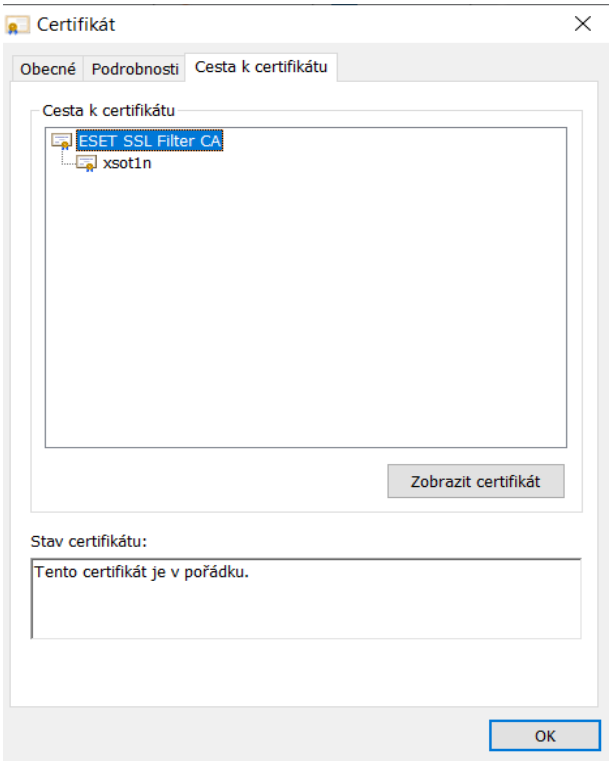
Obr. A.5: Úvodní hláška po úspěšném přihlášení.

Při dalších pokusech přihlašování již postačí používat první způsob přihlašování, tedy jen přes *WinCC Unified RT*.

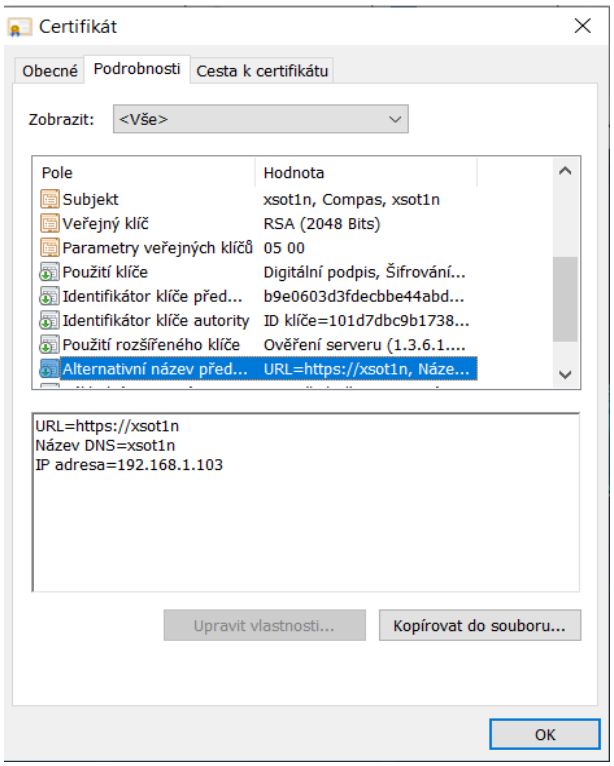
A.4 Nefunguje bezpečená komunikace – neshoda názvu

Tento případ nastane, pokud je certifikát nainstalován správně *(položka Stav certifikátu)* viz obr. A.6, ale stále je webovým prohlížečem zobrazován stav: *Vaše připojení není soukromé* s chybovou hláškou *NET:ERR CERT COMMON NAME INVALID*.

Řešení tohoto problému by mohlo souviset s nastavením parametrů *jméno počítače* a *IP adresa* volených v položce *Přidat zařízení* viz obr. 5.9. Pro zabezpečené připojení je nutné do webového prohlížeče zadávat jméno či IP adresu zařízení, které bylo uvedeno jako parametr certifikátu. Tedy pokud se uživatel připojí k projektu např. zadáním adresy *localhost*, dojde k chybě nastavením certifikátu a následným zobrazením hlášky *Vaše připojení není soukromé*. Jako příklad pro zabezpečené připojení je možné zadat DNS název např. *https://xsot1n* nebo IP adresu např. *https://192.168.1.103*. Zmíněný DNS název a IP adresa jsou zde použity pro názornost. Které parametry lze použít pro zabezpečené připojení lze zjistit ve webovém prohlížeči při rozkliknutí Podrobností certifikátu v poli *Alternativní název předmětu* viz obr. A.7.



Obr. A.6: Správnost certifikátu.



Obr. A.7: Alternativní název předmětu.

B Obsah elektronické přílohy

Odkaz na přílohu: `https://vutbr-my.sharepoint.com/:u:/g/personal/xsotol01_vutbr_cz/EeVizbBCnPdOjx4v2ULvVlABWbjPb9CRBBskMP2CLwD_vQ?e=SRDbTa`

- `/` ..... kořenový adresář přiloženého archivu
  - `přílohy` ..... hlavní složka
    - `CFP3_ScadaExportTool_V17`
      - `CFP3_ScadaExportTool_V17.ap17` ..... spustitelný hlavní soubor projektu, vytvořený v Tia Portal V17
    - `CFP3_ScadaExportTool_V17_OPC_UA_klient_2`
      - `CFP3_ScadaExportTool_V17_OPC_UA_klient_2.ap17` ... spustitelný hlavní soubor projektu, vytvořený v Tia Portal V17
    - `HMI knihovna`
      - `HMI knihovna.ap17` . spustitelný hlavní soubor HMI knihovny, vytvořený v Tia Portal V17
    - `Ovládání servo_motoru_OPC UA Server - UA Expert.pcapng`
    - `Ovládání START,STOP_OPC UA Server - UA Expert.pcapng`
    - `Zachyceni veskere komunikace OPC UA fyzicke zapojeni.pcapng`

B.1 CFP3_ScadaExportTool_V17

Základem projektu CFP3_ScadaExportTool_V17, HMI obrazovka *ČOV WinCC Unified*, která se nachází v záložce *PC stanice -> HMI_RT_2*. Na této obrazovce je vizualizován naprogramovaná simulace čištění odpadní vody. Simulace je složena z prvotního přítoku vody do první nádrže s následným ohřevem, které se provede v druhé nádrži. Hlavním ovládacím prvkem je START, STOP tlačítko, které zastaví přítok vody. Simulace dále obsahuje zobrazení trendů, tedy jsou vykresleny křivky v podobě grafu. Křivky zobrazují hodnoty, které byly zachyceny v obou nádržích v průběhu simulace.

B.2 CFP3 ScadaExportTool V17 OPC UA klient 2

Tento projekt je použit za účelem aplikování komunikace server/klient, kdy serverem je HMI Comfort Panel [TP1200 Comfort] a WinCC Unified představuje klienta. Komunikace server/klient byla aplikována na předešlý projekt s čištěním odpadních vod. Komunikace funguje na bázi vytvoření nového spojení OPC UA a přidělení nových adres ke stávajícím tagům.

B.3 HMI knihovna

Hlavním prvkem tohoto projektu jsou hlavní obrazovky např. HMI knihovna, Hlavní obrazovka, které jsou umístěny v záložce *PC vizualizace -> HMI_Unified -> Obrazovky* a také *vyskakovací okna*, které tvoří doplněk hlavních obrazovek. Na hlavních obrazovkách lze pozorovat analogové motory a ventily, kterým lze nastavovat určité parametry. Runtime, který je obsažen na obrazovce s názvem *HMI knihovna*, má za cíl otevřít vyskakovací okno, které přísluší danému zařízení.

B.4 Ovládání servo_motoru_OPC UA Server – UA Expert.pcapng

Zde je zachycena komunikace příkazů, které byly použity na ovládání servo motoru. Záchyt paketů navazuje na kapitolu *Zachycení komunikace u fyzického scénáře*. Komunikace byla zachycena pomocí programu Wireshark 3.4.9 64-bit na rozhraní Ethernet.

B.5 Ovládání START, STOP_OPC UA Server – UA Expert.pcapng

V tomto souboru se nachází zachycená komunikace pro simulační část. Komunikace je zachycena na rozhraní Ethernet 3. Hlavním prvkem je zachycení požadavků na ovládání *START, STOP tlačítka*. Komunikace byla rovněž zachycena programem Wireshark 3.4.9 64-bit.

B.6 Zachycení veškeré komunikace OPC UA fyzické zapojení.pcapng

Komunikace byla zachycena na rozhraní Ethernet. Kromě samotných požadavků na ovládání servo motoru byly také zachyceny pakety typu *Otevření zabezpečeného kanálu*.