Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Řešení pro centrální správu řídicích systémů SCADA

Bakalářská práce

Autor: Petr Hruška
Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2021

Prohlášení:

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

V Hradci Králové dne 29.4.2021 Petr Hruška

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefovi Horálkovi, Ph.D. za metodické vedení práce a cenné profesionální rady při zpracování. Dále bych chtěl poděkovat rodině za podporu během studia.

Anotace

Název: Řešení pro centrální správu řídicích systémů SCADA

Bakalářská práce se zabývá problematikou řešení pro systémy řízení založených na SCADA řešeních. Cílem je zmapovat, navrhnout a realizovat vhodné řešení využití tenkých klientů pro SCADA systémy. V teoretické části práce jsou zmapovány a popsány požadavky řídicích SCADA systémů na komunikační a systémové zdroje. Na základě této analýzy je představeno možné řešení přechodu z desktop řešení na serverově řízenou správu a vybráno technologicky, bezpečnostně a ekonomicky nejlepší řešení. V praktické části je podrobně popsaná a otestovaná tato implementace a efektivita.

Annotation

Title: Central administration of SCADA control systems

The bachelor thesis deals with the issue of solutions for control systems based on SCADA solutions. The goal is to map, design and implement a suitable solution for the use of thin clients for SCADA systems. The theoretical part of the thesis maps and describes the requirements of SCADA control systems for communication and system resources. Based on this analysis is presented a solution for the transition from a desktop solution to server-controlled management and chosen technologically, security and economically best solution. In the practical part, this implementation and effectiveness is described and tested in detail.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Předmětem bakalářské práce je navrhnout přechod z desktopového řízení systémů SCADA na řízení v režimu klient/server. Využívání počítačů se mění a společně s tím se mění i technologie. Vzhledem ke stáří současného hardwaru desktopových koncových stanic a jejich nepodporovanému operačnímu systému je nutno přistoupit k jejich obnově.

SCADA systémy lze provozovat i v režimu relací vzdálené plochy instalací na hostitele relací vzdálené plochy (terminálový server).

Na základě analýzy dosavadního desktopového řešení dojde k navržení možnosti řízení SCADA systémů pomocí terminálových serverů. Na serveru je pak možné provozovat více instancí vizualizačního softwaru InTouch. Klientské stanice (tenký klient) poté umožní uživatelům zobrazit vizualizační SCADA aplikaci. Tento princip zajišťuje Microsoft Remote Desktop Protocol. Protokol RDP přenáší ze serveru směrem ke klientům multimediální informace (obraz, zvuk, atd.) a od klienta směrem k serveru zajišťuje přenos interaktivních akcí (interakce myši, klávesnice, atd.)

2 Rešerše

K vypracování bakalářské práce byla použita doporučená literatura zabývající se konkrétními případy řešení řízení SCADA systémů. Zároveň bylo k vypracování použito odborných článků, které řešily dílčí části.

První část se zabývá popisem systémů SCADA a vizualizačního softwaru InTouch. Zde byl důležitým zdrojem článek "What is SCADA?", který zpracovali a vydali A. Daneels a W. Salter [2]. Článek popisuje, co jsou SCADA systémy obecně a jejich použití. Autoři říkají, že SCADA systémy se nejčastěji používají v průmyslových firmách a zaměřují se na úroveň dispečera. Dále pak popisují typickou hardwarovou architekturu systémů SCADA a rozdělují ji do dvou vrstev. První vrstva je „klientská“, kterou používá dispečer k ovládání technologických procesů. Druhá vrstva je „datová“, která zpracovává veškerá procesní data.

Pro část zabývající se vizualizačním programem byl použit článek, který zpracovali a vydali D. Gaushell a H. Darlington [3]. Zabývají se historií, alarmovým procesem, logováním a v neposlední řadě i databází. K definici vizualizačního softwaru InTouch sloužily DataSheet a TechNote od společnosti WonderWare a firmy Pantek [4]. K doplnění informací sloužily v neposlední řadě interní podnikové provozní předpisy.

Shankar [5] definuje komunikaci mezi SCADA a PLC, která může probíhat různými způsoby (pomocí sériového portu, po síti a podobně). Dále pak popisuje definici PLC a jak PLC pracuje. Říká, že základem funkce PLC je kontinuální skenování programu. Skenování zahrnuje tři základní kroky.

- Krok 1: Testování vstupu
- Krok 2: Provedení programu
- Krok 3: Kontrola a úprava výstupu

Komunikačním protokolem OPC, který má za úkol vytvořit rozhraní mezi hardware a software produkty průmyslové automatizace, se zabývá Hawkinson [6], který se zabývá i přenosem dat z pomocí OPC protokolu a jejich následné zobrazení v aplikaci.

Závěrečná část zabývající se terminálovými servery, tenkými klienty a softwarem ThinManager vycházela zejména z článku "An Investigation into Current Thin Client/Server Computing Technology and its Impact Upon PC based Industrial Control

and Supervisory Systems" od I. Williams [7], který se zabývá historií tenkých klientů a problematikou klient/server.

Podobně i Galea [8] se věnuje této problematice a také různým způsobům bootování tenkého klienta. Autor článku popisuje také přínosy topologie klient/server.

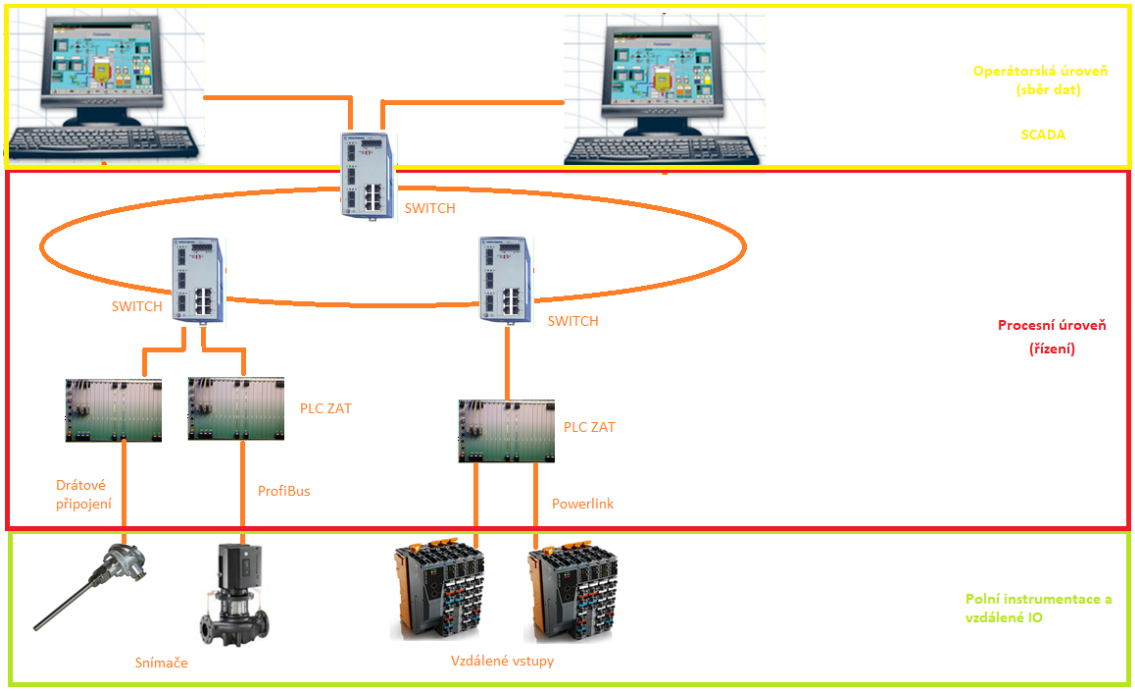
Poslední část se zabývá softwarem ThinManager, který slouží ke snadnému doručování obsahu na tenké klienty. Firma Pantek [9] říká, že ThinManager je software pro efektivní správu, provoz a flexibilitu architektur s tenkými klienty. Tento software pracuje na základě služeb vzdálené plochy a pomocí ní může doručovat aplikační obsah na operátorské stanice. Jak používat služby RDP pro tenké klienty popisuje v článku „Case studies in Thin Client acceptance“ Doyle [10].

3 SCADA/HMI

Scada (Supervisory Control and Data Acquisition) je supervizní řízení výrobních technologií a procesů. Zaměřuje se na úroveň supervizora (dispečer, technolog, manažer), aby mohl v reálném čase efektivně sledovat, ovládat a optimalizovat průběhy technologických procesů nebo výrobních operací a reagovat na ně. Základem SCADA systému je HMI (Human Machine Interface), které představuje rozhraní mezi zařízením a člověkem. Představuje také prostředky pro zobrazení a předání informace o stavu zařízení (stav, hodnoty) obsluze nebo operátorovi a zároveň poskytuje možnost k ovládání stroje a zadávání hodnot.

Software typu SCADA je tedy provozován nad skutečným řídicím systémem (PLC automat, I/O moduly, senzory, měřiče, apod.), který zprostředkovává konektivitu a sběr dat ze sledovaných technologických procesů. SCADA se skládá z:

- SCADA systém
- Komunikační síť
- PLC
- Akční členy, čidla. [2]



Obr. 1 - Schéma SCADA/HMI

3.1 Základní pojmy

Následující pojmy byly popsány na základě vlastních vědomostí a za použití interní podnikové normy (provozní předpis).

3.1.1 PLC

PLC (Programmable Logic Controller) je programovatelný logický automat. Jedná se o relativně malý průmyslový počítač řízený mikroprocesorem s vlastním operačním systémem. Je uzpůsoben pro potřeby řešení automatizačních úloh v reálném čase, s co nejkratší dobou odezvy. Tyto automaty zpracovávají své programy cyklicky. Pro komunikaci s okolím je PLC vybaven vstupními periferiemi, na které jsou přivedeny signály z řízeného procesu (například teplota, tlak). Na "opačné" straně jsou výstupní periferie, ke kterým jsou připojeny akční prvky řízeného procesu (například polohy regulačního ventilu).

Řídící logika PLC na základě stavu vstupů ovládá výstupy tak, aby bylo dosaženo žádaného nebo zadaného stavu celého zařízení. Jak bude PLC reagovat na změnu stavu vstupních signálů, určuje programátor vytvořením algoritmu. [5] [11]

3.1.2 Akční člen

Akční člen je základním prostředkem pro ovládání výrobního procesu. Jedná se vesměs o elektrické stroje (motory, servopohony, topná tělesa, zdroje napětí, ventily apod.), kterými řídíme výrobní proces. [11]

3.1.3 Čidla

Čidlo je základní prostředek pro získání informace o výrobním procesu. Pomocí čidel jsou měřeny fyzikální veličiny, jejichž měření je následně převedeno na elektrický signál. Tento signál je pak dále dopravován do řídícího automatu ke zpracování. Jedná se o oči a uši řídicího systému.

Čidla se dále podle druhu signálu dělí na analogová a binární, kde analogové signály mohou nabývat různé hodnoty od minimální do maximální měřené hodnoty. Binární signál může naopak nabývat pouze jedné ze dvou možných hodnot, které odpovídají stavu signálu (například Vypnuto/Zapnuto, 0/1). [11]

3.1.4 RDP

Remote Desktop Protocol, neboli protokol služeb vzdálené plochy, umožňuje ovládat vzdálený počítač pomocí využití počítačové sítě. Tento protokol pracuje na principu topologie klient/server. RDP provádí přenos obrazu a případně dalších medií (například zvuk) na klienta a přenos interaktivních informací od klienta na server v rámci režimu relace vzdálené plochy.

3.1.5 VLAN

Virtuální LAN, která je nezávislá na fyzickém uspořádání, slouží k virtuálnímu rozdělení sítě. Pomocí VLAN lze vytvořit dvě nebo více sítí, které jsou na sobě nezávislé. Jedná se tedy o segmentaci původní fyzické struktury sítě na menší sítě. Pokud je komunikace mezi sítěmi potřeba, lze komunikaci nastavit pomocí routování. To znamená pomocí administrátorem nastavených pravidel, jaká virtuálně oddělená síť může komunikovat s jinou oddělenou sítí.

3.2 Vizualizační software InTouch

Tento software je produktem firmy WonderWare a patří mezi světově nejpoužívanější. InTouch je software kategorie HMI/SCADA určený k vizualizaci, monitorovaní a operátorskému řízení technologických a výrobních procesů. Tento software nabízí jednoduchou tvorbu grafických symbolů jakýchkoliv výrobních technologií. Umožňuje je zobrazovat na monitoru počítače a pomocí těchto symbolů může operátor zasáhnout do výrobních procesů.

„Pro sběr dat z technologických procesů je k dispozici rozsáhlá nabídka komunikačních I/O serverů přímo od Wonderware nebo od nezávislých softwarových firem, podporována je samozřejmě i komunikace s OPC servery od libovolných dodavatelů. Kromě nástrojů pro snadné vytvoření grafických obrazovek zobrazujících aktuální stavy provozovaných technologií je součástí SCADA systému InTouch i správa distribuovaných historických dat umožňující i spolupráci s výkonnou historizační databází Wonderware Historian Server a správa distribuovaných alarmů (výstrah), které lze ukládat do databáze MS SQL.“ [3] [4]

3.2.1 Funkce

Software InTouch nabízí mnoho funkcí a s novými verzemi tohoto softwaru jich mnoho přibývá.

- **Sledování alarmů a událostí** – zde došlo k významnému zvýšení výkonosti a k různým možnostem filtrování a třídění pro větší pohodlnost práce s alarmy.
- **Grafické symboly ArchestraA** – možnost tvorby vlastních symbolů za použití grafického editoru nebo použití knihovny, která obsahuje mnoho profesionálně navržených symbolů.
- **Skriptový editor** – tento editor přináší rychlé a snadné psaní skriptů. Nově je zde funkce Auto-Complete, která vývojáři nabízí seznam vhodných možností. Tím dojde k minimalizování chyb (například různých překlepů).
- **Šablony** – ve starších verzích InTouch se nová aplikace vytvářela prázdná. Vytvořené symboly musel vývojář vytvářet znovu. Tato nová funkce pomáhá vývojáři vytvořit aplikaci ze šablony. Aplikace tak bude obsahovat prvky, které vývojář nebude muset vytvářet znovu.
- **Kompatibilita** – software je plně kompatibilní se staršími verzemi a umožňuje snadný převod vytvořených aplikací.

3.2.2 Komunikační protokoly

OPC Server

OPC (OLE for Process Control) je sada standardních rozhraní založených na technologii OLE/COM společnosti Microsoft. Použití těchto standardů umožňuje bezproblémovou komunikaci mezi hardware a software produkty průmyslové automatizace.

OPC je založen na topologii klient/server, kde OPC klient přijímá data z OPC serveru a tato data jsou následně zobrazena pomocí vizualizační aplikace. Příkladem topologie OPC klient/server může být aplikace na operátorské stanici, kde bude nainstalován OPC server i OPC klient. Tento systém se používá pro jednoúčelové aplikace. [6] [13]

SuiteLink

SuiteLink je protokol založený na standardu TCP/IP vyvinutý firmou Wonderware pro komunikaci mezi jejími produkty. Poskytuje tyto vlastnosti:

1. Value Time Quality (VTQ), tj. umístění časové značky a příznaku kvality do dat přenášených do připojených klientů.
2. Rozsáhlá možnost diagnostiky datové propustnosti, zatížení počítače a sítě je zpřístupněná přes „Performance monitor“ operačního systému.
3. Možnost práce s velkými objemy dat nezávisle na tom, zda jsou aplikace lokálně na jednom počítači nebo distribuované na velkém množství počítačů. [14]

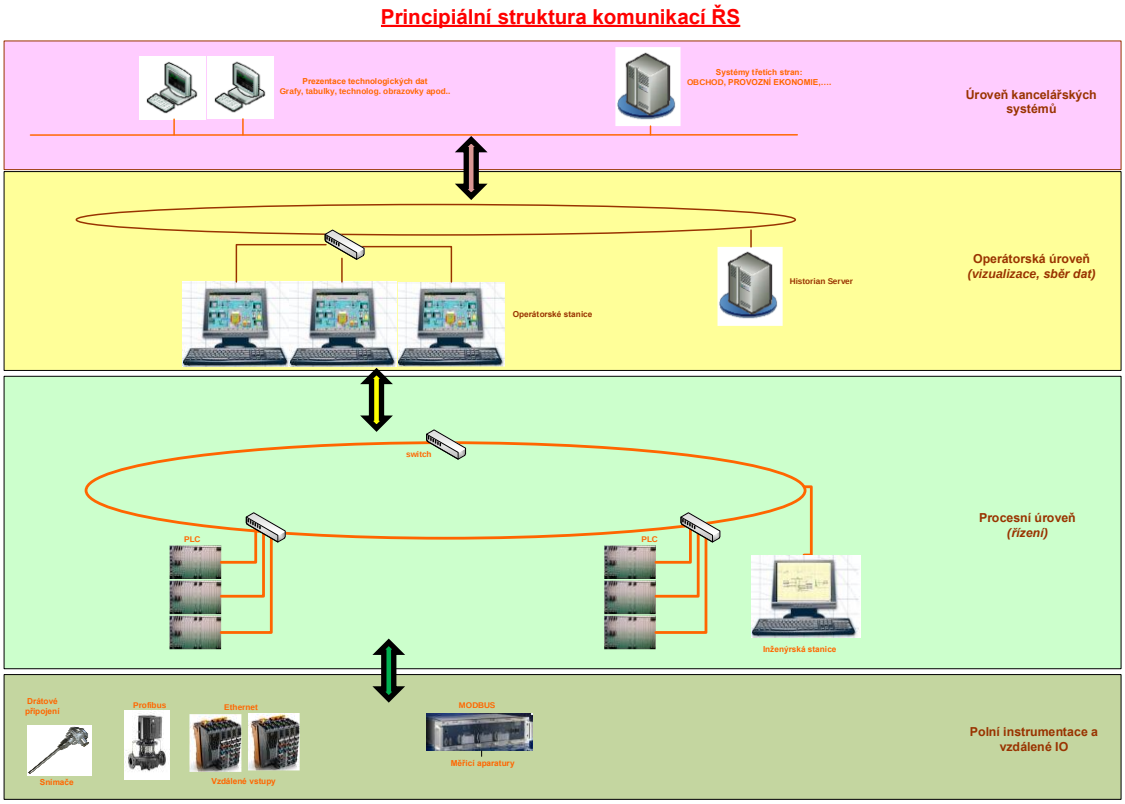
DDE

Komunikační protokol je vyvinutý firmou Microsoft, který umožňuje aplikacím v prostředí Windows posílat a přijímat data a instrukce mezi sebou. Tímto protokolem je realizována topologie klient/server mezi dvěma souběžně běžícími aplikacemi. Některé aplikace, např. InTouch a Microsoft Excel, mohou být zároveň server i klient.

Tento protokol se často využívá ke shromažďování a distribuci aktuálních dat. DDE je využíván pro jednorázové přesuny dat nebo pro výměny dat. Nová data se při výměnách posílají, jakmile jsou k dispozici. To znamená, že jakmile dojde ke spojení mezi aplikacemi, server může posílat data klientovi vždy, když dojde ke změně hodnot. Spojení mezi aplikacemi zůstává, dokud ho jedna z nich nepřeruší. [15]

4 Popis stávajícího stavu

V současné době jsou SCADA aplikace řízeny ze samostatných desktopů. Provoz jednotlivého desktopu není nijak závislý na dalších počítačích nebo serverech. Je na něm spuštěn operační systém Windows 7, antivirus, zálohovací klient, Scada vizualizační software a komunikační driver pro komunikaci s PLC. Je vybaven dvěma síťovými kartami. Jedna slouží pro komunikaci s PLC (procesní úroveň), druhá slouží pro sběr dat a management (operátorská úroveň).



Obr. 2 – Struktura komunikací ŘS

Úroveň kancelářských systémů spadá pod správu IT. Na této úrovni se nachází kancelářské počítače s různými aplikacemi. Z této úrovně jsou pro některé technické pracovníky povoleny přístupy k historickým datům pomocí aplikace Trend. Mezi provozní a IT síti jsou bezpečnostní prvky s definovanými pravidly přístupu. Procesní úroveň je určena programátorům PLC. Programátoři PLC využívají inženýrskou stanici, která komunikuje s touto úrovní a na které je nainstalován software pro správu PLC. Jestliže dojde ke změnám v softwaru PLC, je možné učinit pomocí této stanice beznárazové přehrání.

Některým servisním pracovníkům jsou povoleny notebooky, kterým je administrátorem přidělena IP adresa pro procesní úroveň a jsou jim povoleny některé porty na SWITCH, které bývají logovány.

Polní instrumentace se skládá z akčních členů a čidel, které jsou připojeny do PLC a ze kterých je potom možné pomocí vizualizační aplikace číst data.

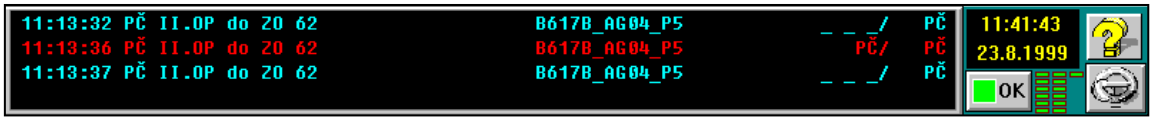
V operátorské úrovni se nacházejí operátorské stanice (dále koncové stanice), které jsou umístěny na příslušných velínech. Zbývající technologické koncové stanice jsou umístěny v rozvaděčích, v kabelových prostorech nebo v kancelářích. Tyto koncové stanice jsou slabým článkem z hlediska neoprávněného napadení systému.

Samotná správa tak velkého počtu koncových stanic je náročná. Vzhledem k technologickému provozu je nutné zabezpečení těchto stanic a zajištění provozuschopnosti a dostupnosti. Kvůli tomu se musí většina operací dělat přímo na místě, aby se administrátor přesvědčil (např. po instalaci bezpečnostních aktualizací), že vizualizační software funguje správně a korektně.

Hardware koncových stanic je měněn po 4 letech nepřetržitého provozu. S výměnou hardwaru se provádí i přechod na nejnovější operační systém a jemu odpovídající verzi vizualizačního softwaru. V současné době je na stanici instalován Windows 7, který přestal být od 01/2020 Microsoftem podporován.

4.1 Aplikační vizualizace

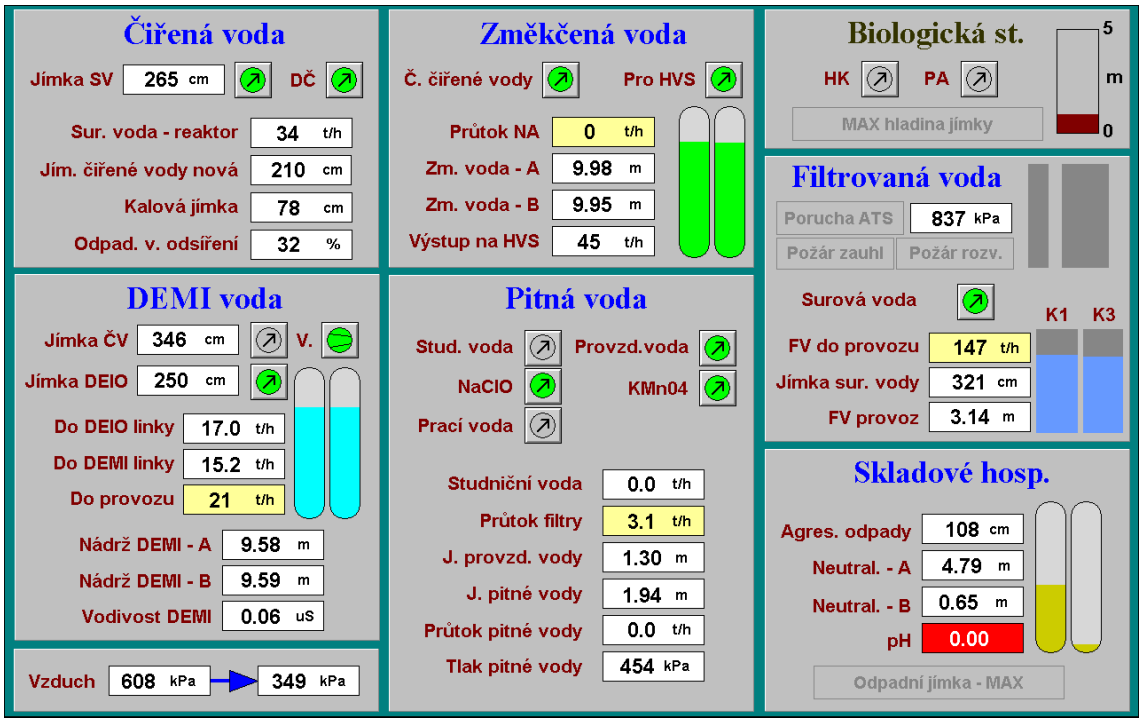
Každá desktopová stanice (operátorská stanice) má svou vlastní InTouch aplikaci. S její pomocí může operátor (dispečer) ovládat technologické zařízení, regulační akční členy, motory a podobně. Ovládacím prvkem stanice je běžná myš. Pohybem myší se pohybuje po obrazovce kurzor, kterým ukazujeme na jednotlivé prvky - objekty technologického snímku. Pokud je některý prvek „vybrán“ – ukazuje na něj kurzor a je možná nějaká akce (činnost stanice), prvek se orámuje. Kliknutím myší se potom akce provede (zobrazí vybraný snímek, panel, provede povel, vypíše identifikace prvku a podobně).



Obr. 3 – Horní okno InTouch

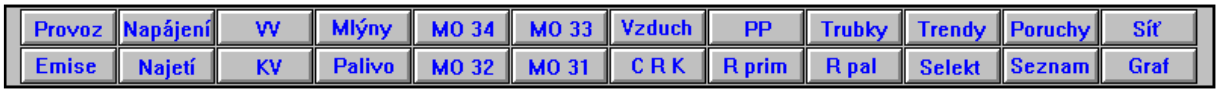
Grafika u všech operátorských stanic je rozdělena do tří hlavních částí. První část je horní okno, které obsahuje poslední čtyři řádky archivu alarmů, test komunikace s okolními automaty, kvitovací tlačítko a klíč pro přihlášení uživatele. Každý uživatel má po přihlášení administrátorem danou privilegovanost.

Druhá část aplikace je střední okno, které je tvořeno vlastními technologickými snímky. Tyto snímky se zobrazují na základě volby operátora a tvoří základ pro řízení technologického procesu. Toto okno má proměnlivý vzhled, podle momentálně operátorem vybraného technologického snímku.



Obr. 4 – Technologický snímek

Třetí část grafiky je spodní okno, které má vždy stejný vzhled. Obsahuje tlačítka se jmény nejčastěji používaných technologických snímků, které operátor může zvolit. Tyto snímky jsou zobrazeny ve druhé části grafiky. [11]



Obr. 5 – Spodní okno InTouch

4.1.1 Použitá symbolika pro vizualizaci

V rámci celého podniku je uplatněna interně vytvořená norma pro tvorbu snímků a animací jednotlivých komponentů. Všeobecně platí následující pravidla:

Pro zobrazení technologických schémat je použito těchto barev:

- Světle zelená - čistý kondenzát, napájecí voda
- Tmavě zelená - chladicí voda, topná voda
- Světle modrá - topný kondenzát, spalovací vzduch kotle
- Červená - pára, přehřátá pára
- Oranžová - spaliny kotle, mazací olej strojů
- Tmavě modrá - tlakový vzduch
- Hnědá - topný olej

Symbol motoru (čerpadla, ventilátoru a jiných točivých strojů) má při zobrazování tyto barvy:

- Vypnuto - tmavě šedý
- Zapnuto - zelený
- Zajištěno - bílý
- Chyba - fialový
- Not ready - žluté orámování symbolu
- Časová prodleva - symbol hodin u akčních členů
- Neovladatelnost - žluté N u symbolu akčních členů

Obr. 6 – Ventilátor, motor, čerpadlo

Symbol armatury mění barvu podle stavů:

- Zavřeno - černý
- Otevřeno - v barvě media
- Zavírá - bliká černě
- Otevírá - bliká v barvě media
- Mezipoloha, bez stavu - šedý
- Chyba, oba stavy - fialový
- Další stavy jsou hlášeny stejně jako u motorů, symboly N a hodin.

Obr. 7 – Vizualizace ventilu a klapky

U binárních signálů se používá zpravidla slovního popisu významu signálu v rámečku (např. „Ložiska.“). Pokud je signál neaktivní, je nápis proveden jako tmavošedý na šedém

pozadí (slabě viditelný). Pokud má charakter poruchy, svítí červeně s bílým textem, pokud má charakter potvrzení normálního provozního stavu, svítí zeleně s černým textem. Používají se také hlášení ve žlutočerné kombinaci a tato zpravidla znamenají signalizaci nebezpečného stavu.

Obr. 8 – vizualizace binárních signálů

Ovládání servopohonů

Kliknutím na symbol pohonu se objeví panel s identifikačními údaji příslušného akčního členu a třemi tlačítky.

ZAVŘÍT / OTEVŘÍT – kliknutím na tlačítko se akce provede,

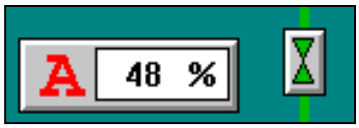
ZRUŠ – uzavře ovládací panel bez provedení jakékoliv akce.

Obr. 9 – Panely pro ovládání motoru, servopohonu

Ovládání regulačních akčních členů

Na technologických snímcích s regulačními obvody je vždy u příslušné regulačního obvodu umístěn panel obsahující údaje:

- stav obvodu automatického (A) nebo ručního (R) řízení
- ukazatel stavu otevření regulačního obvodu.



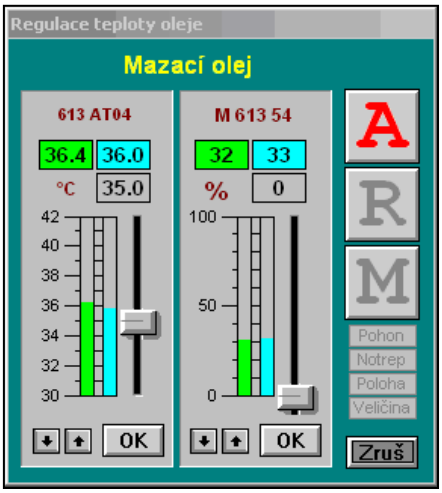
Obr. 10 – Regulační obvod

Kliknutím na tento panel se potom otevře vlastní panel pro řízení regulačního obvodu.

Každý panel regulačního obvodu má samostatnou část pro ovládání polohy akčního členu (vpravo) a zadávání žádané hodnoty (vlevo).

Zadání žádané hodnoty je zpravidla omezeno v určitém rozsahu.

Tlačítka „A/R“ přepínají způsob řízení a červený nápis signalizuje stav automaticky nebo ručně.



Obr. 11 – Regulační panel

A – poloha akčního členu je řízena automatem,

R – poloha je řízena podle polohy zadané šoupákem (operátorem),

M – poloha je řízena tlačítky z pultu operátora.

Zobrazení analogových veličin

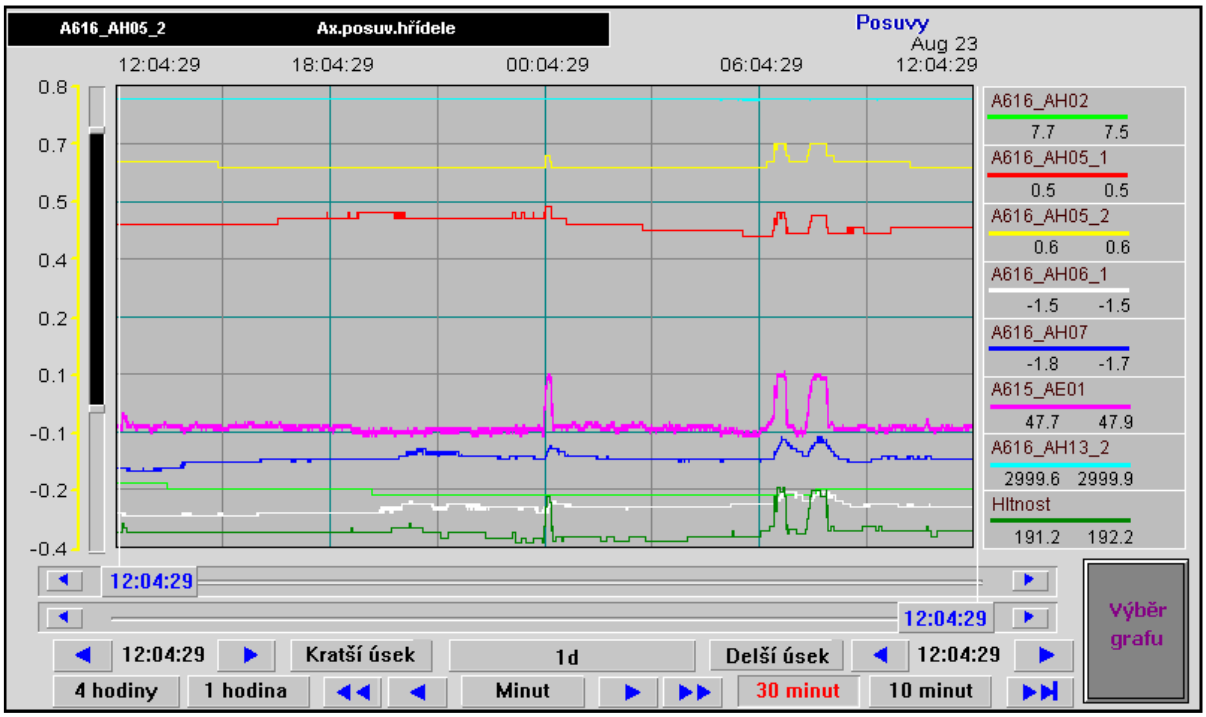
Analogové veličiny jsou zobrazovány v číslicové podobě včetně jejich atributů a fyzikální jednotky a jejich atributů. Atributy veličin jsou poruchy čidla nebo status překročení nastavitelných mezí. Zobrazení těchto veličin bývá často číslo na bílém podkladu. V případě měření se statusem poruchy čidla je veličina zobrazena jako bílé číslo na fialovém podkladu. Jestliže měření překročí některou z nastavitelných mezí, je číslo zobrazováno jako bílé číslo na červeném podkladu nebo černé číslo na žlutém podkladu.

V případě, že chce operátor vidět popis či rozsah měřené veličiny, může vyvolat okno „popis veličiny“, které vyvolá po kliknutí na zobrazovaný podklad. V tomto vyvolaném okně jsou zobrazeny i nastavitelné meze (Lo, LoLo, Hi, HiHi). Je zde také adresa veličiny v řídicím systému, ze které je tato veličina pomocí komunikačního protokolu čtena.

Obr. 12 – Okno popis veličiny

Ukládání veličin (logování)

Pomocí ukládání veličin neboli logování je v Intouch možné pomocí grafů (trendů) zobrazit historické data. Pro každou ukládanou veličinu je stanoveno pásmo necitlivosti (deadband). Pokud se veličina od poslední uložené hodnoty nezmění než o toto pásmo necitlivosti, veličina se neuloží. V případě, že toto pásmo překročí, dojde k uložení nové hodnoty a opět se čeká na další změnu. Tato data jsou uchována na pevném disku operátorské stanice v souborech LGH. Pokud jsou tyto soubory starší více než 21 dnů, dojde k jejich odmazání.



Obr. 13 – Zobrazení historických dat

Zároveň s tímto sběrem dat běží i sběr na Historian serveru. Na tomto serveru jsou data uchována pro dlouhodobější potřebu archivace. Data jsou uchována v tzv. „historických blokách“, které se vytváří automaticky na začátku dne. Jejich struktura a systém záznamu je odlišný od operátorské stanice a data jsou dostupná pro následnou analýzu v manažerské síti uživatelům se zpřístupněnou aplikací Trend. [11]

4.1.2 Komunikace operátorské stanice s okolím

Provozní síť ETHERNET

ETHERNET je síť, která propojuje kabelem jednotlivé operátorské stanice do jednotné informační sítě. Operátorské stanice tak mohou sdílet informace. Základní charakteristikou přenášených dat je jejich přenos v reálném čase. Jedná se o okamžité, skutečné údaje.

Řídící stanice PLC

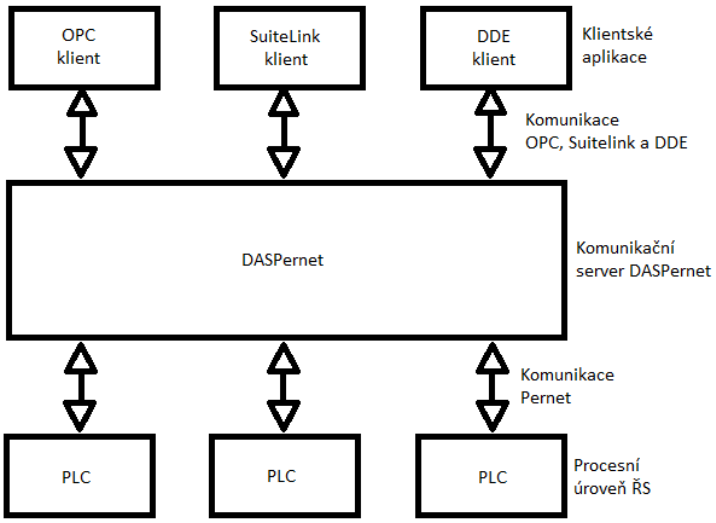
Řídící stanice PLC s názvem Sandra Z200 se používají pro realizaci algoritmů přímého řízení. Tyto algoritmy nejčastěji bývají v podobě regulačních smyček a logických funkcí. Stanice Z200 jsou určeny pro komunikaci s externími zařízeními a dále pak s operátorskou stanicí k doručování informací z těchto zařízení. Komunikace je založena na technologii ETHERNET a probíhá pomocí protokolu PERNET.

Operátorská stanice komunikuje s řídicím systémem a s ostatními operátorskými stanicemi. Stanice je vybavena dvěma kartami ETHERNET. Při komunikaci s ostatními operátorskými stanicemi se nepřenášejí žádné řídící povely. Tato komunikace slouží pouze k přenosu informací pro potřebu jednotlivých operátorů. K tomuto přenosu slouží první karta operátorské stanice. Pomocí této karty je zajištěno, že každá stanice dodává potřebná data do sítě a zároveň ze sítě data sbírá pro vlastní potřebu. Přenášená data jsou potom na operátorské stanici vizualizována prostřednictvím standartních (v celé síti stejných) snímků. Touto kartou komunikuje i s Historian serverem, který slouží pro sběr a ukládání dat do SQL databáze.

Druhá karta (dvouportová) slouží ke komunikaci s automaty příslušného technologického zařízení. Komunikace s automaty probíhá obousměrně a představuje hlavní tok dat a povelů pro řízení příslušného technologického zařízení. Dvouportová karta slouží k redundantnímu připojení do dvou SWITCHů na řídící stanice PERNET. Díky redundanci je zajištěna větší spolehlivost komunikace v případě výpadku například jednoho SWITCHe. [5] [11] [12]

4.2 Komunikační server DASPernet

Server DASPernet (Data Access Server Pernet) je aplikace běžící v operačním systému Microsoft Windows, která pracuje jako komunikační server. Umožňuje datové spojení



Obr. 14 – Komunikační server DASPernet

mezi klientskými aplikacemi spuštěnými v operačních systémech Microsoft Windows a mezi procesní částí řídicího systému. Klientským aplikacím server DASPernet poskytuje komunikační rozhraní s protokoly OPC, SuiteLink a DDE. Toto komunikační rozhraní může využívat více klientských aplikací současně. S řídícími stanicemi procesní části komunikuje server protokolem Pernet. Přestože server DASPernet je primárně určen pro použití s aplikací InTouch, může být využíván jakýmkoliv programem, který pracuje jako DDE, SuiteLink nebo OPC klient. [14]

4.3 Zabezpečení stanic

Nedílnou součástí bezpečnostní politiky je kontrola a ochrana koncových stanic. Jedná se asi o nejstarší a zároveň uživatelsky nejznámější část IT bezpečnosti. Na koncové stanici jsou vytvořeny dva účty. První účet je určen pro operátory a má práva na úrovni USER. Zároveň jsou pro tento účet upravena bezpečností pravidla tak, aby uživatel neměl možnost na koncové stanici instalovat, konfigurovat síť nebo upravovat nastavení počítače a podobně. Uživatelům jsou dále odepřeny přístupy přes USB porty a všechny jednotky (CD, diskety, apod.). Tím je zajištěno, že se do koncové stanice nedostane

škodlivý kód přes uživatele koncové stanice. Druhý účet je určen pro správce koncových stanic na úrovni ADMINISTRATOR. Tento účet je určený pro správu operátorské stanice. Pro zajištění větší bezpečnosti dochází na tomto účtu jednou za měsíc ke změně hesla.

Na všech stanicích je k zajištění bezpečnosti před škodlivými programy nainstalován antivirový program ESET. Tento program zajišťuje pravidelné kontroly stanice před případným nebezpečím. K provádění aktualizací modulů a detekčního jádra antivirového programu slouží server, který je nastaven jako mirror. Tento server je nastaven tak, aby ze serverů ESET stahoval aktuální aktualizace a tyto aktualizace distribuoval koncovým stanicím, které mají odepřen přístup k internetu. K oddělení tohoto serveru a koncových stanic slouží firewall. Ke stažení aktualizací komunikuje koncová stanice se serverem mirror prostřednictvím portu 2221, který je povolen na firewall. Kontrola antivirových aktualizací probíhá na koncových stanicích automaticky vždy jednou za den.

Firewall odděluje provozní síť od kancelářské sítě. Využívané servery, které mají přístup na internet a bývají zpravidla virtualizovány na serveru, který spadá pod správu IT, se nacházejí až za firewall (Historian, ESET Mirror, WSUS, licenční server). Jsou zde nastaveny jen ty nejzákladnější komunikační porty, které jsou nezbytně nutné pro bezpečnost a fungování operátorské stanice. Příkladem můžou být bezpečnostní aktualizace Windows, které se na stanicích provádějí prostřednictvím serveru WSUS.

Server WSUS (Windows Server Update Services) je lokálně spravovanou alternativou ke službě Windows Update a je používán převážně ve firemních sítích. Windows Update je služba, která zajišťuje aktualizace systému Windows ze serveru Microsoft. WSUS běží na virtuálním serveru v lokální síti s přístupem na internet. Ze serveru Windows Update pak dále stahuje aktualizace, které pak distribuuje na koncové stanice. Ke správě a distribuci aktualizací slouží role WSUS na operačním systému Windows Server. Ke stažení bezpečnostních aktualizací Windows je potřeba nakonfigurovat server WSUS na koncových stanicích pomocí úpravy registrů. Jakmile je server nakonfigurován na koncové stanice, mohou tyto stanice stahovat aktualizace ze serveru WSUS pomocí portu 8530, který je nastaven na firewallu. Instalací bezpečnostních aktualizací se zvyšuje zabezpečení stanice a zároveň snižuje rizika napadení.

Další zabezpečující složkou koncové stanice je pravidelné zálohování. Zálohování se provádí prostřednictvím aplikace Acronis. Aplikace nabízí management z inženýrské

stanice, ze které je potom možné nainstalovat agenty Acronis na koncové stanice. V případě, že je potřeba provést zálohu konkrétní koncové stanice, probudí se pomocí managementu agent, který zálohu provede. Jedná se o vytvoření obrazu disku se systémem, kde jsou důležité soubory pro obnovu v případě ztráty dat. Následně je záloha uložena na pevném disku stanice a poté je také uložena na inženýrské stanici. Z inženýrské stanice se zálohy kopírují na přenosné disky, aby bylo zajištěno větší bezpečí v případě ztráty dat. Tyto zálohy se provádějí každý měsíc vždy po nainstalování bezpečnostních aktualizací. Dále je pak zálohován adresář, kde se nachází složka s vizualizační aplikací InTouch a adresář s výpisy alarmových hlášení. Tyto adresáře jsou na všech stanicích zálohovány jednou týdně z důvodu neustálých úprav aplikací.

4.4 Technologická síť

Výsledná fyzická topologie sítě je kruhová struktura s logickou topologií linie. Technologická síť je na bázi paketového přenosu s nedeterministickým přístupem k médiu, což zajistí transparentní přenosovou cestu pro komunikující koncová zařízení. Síť zajišťuje kromě základní komunikační cesty i vysokou redundanci. K tomu slouží zdvojené aktivní prvky.

Dalším základním prvkem redundance sítě je výpočetní protokol RSTP (Rapid Spanning Tree Protocol), který pomocí standardních metod výpočtu cest v síti a pomocí blokování a definování různých stavů portů zajišťuje, že v každém okamžiku a za každé konfigurace sítě je síť ve stavu schopném přenášet data, a to necyklicky. Protokol zajistí redundanci na úrovni optické páteře, ale zároveň zajistí odolnost proti případným problémům, které by mohly vzniknout výskytem smyček v síti (například smyček, které vzniknou špatnou manipulací obsluhy). U každé cesty je pak stanovena váha cesty, která je podstatná pro rekonfiguraci. Optimální cesta je pak taková, která má nejnižší součet vah skrz celou cestu. Doba rekonfigurace je obvykle v řádu stovek milisekund. Síť je zároveň odolná proti výpadku jedné cesty (linky), výpadku jednoho uzlu (aktivního prvku) a také proti výpadku jednoho napájení.

Aktivní prvky komunikují na páteřních portech pomocí optické páteře, která je provozována v režimu 1000 Mbps FDX (plně duplexní přenos). Koncovým zařízení na metalických portech síť zajistí automatické vyjednání přenosové rychlosti (10, 100

Mbps), automatické vyjednání režimu přenosu, automatické vyjednání řízení toku dat a automatickou odolnost proti křížení kabelů.

Bezpečnost sítě je jeden z důležitých aspektů, na který je kladen velký důraz. Všechny aktivní prvky jsou pro konfiguraci chráněny bezpečnostním heslem. Jednotlivé porty jsou konfigurovány tak, aby umožnily připojení pouze definovaného koncového zařízení. Každá manipulace s portem je monitorována a následně zaznamenávaná do logů. Nepovolená manipulace vede k uzamčení portu do doby, než administrátor provede odblokování. Pro oddělení jednotlivých úrovní technologických sítí jsou použity VLAN (virtuálně oddělené sítě). Počítá se i se vzdálenými přístupy servisních pracovníků. Proto jsou v síti navrženy firewally, které určují, do které sítě má servisní pracovník přístup. Součástí je i logování pokusů o nekorektní komunikace a přístupy.

4.5 Nároky SCADA systémů na HW

Každá aplikace vyžaduje pro svůj provoz operátorský počítač s parametry odpovídajícími zatížení aplikace v plném provozu. Aby nedošlo k zaplnění pevného disku, je potřeba provádět pravidelnou údržbu a udržovat volné místo ve velikosti 20 % kapacity pevného disku. Požadavky na hardware počítače se liší v závislosti na velikosti aplikace. V případě malé SCADA aplikace (1 – 25 tisíc proměnných) jsou nároky na hardware minimální.

Aplikace	Nároky	Jádra CPU	RAM	HDD	Rychlost sítě
1 – 25 tisíc proměnných	Minimální	2	2 GB	100 GB	100 Mbps
	Požadované	4	4 GB	200 GB	100 Mbps

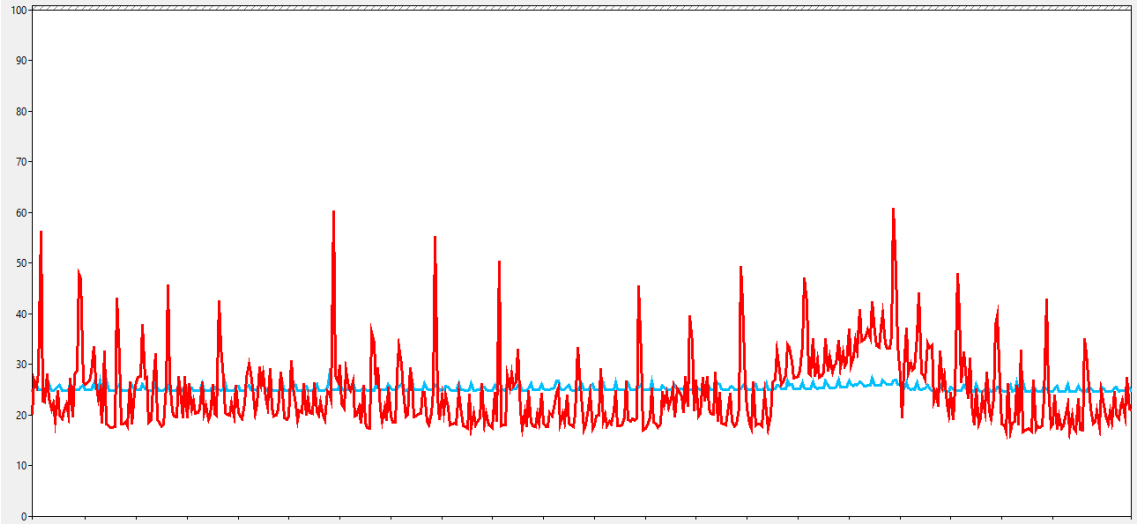
Tabulka 1 – HW na malé SCADA aplikace

V případě, že se jedná o obsáhlejší SCADA aplikaci (25 – 50 tisíc proměnných), bývá zatížení počítače vyšší. Je to způsobeno zejména SQL (alarmní DB), které je instalováno na každé operátorské stanici zvlášť. V tomto případě je do ní ukládáno velké množství dat. Zároveň je na počítači používané automatické ukládání dat do souboru. Tím je zajištěno, že operátor může v aplikaci sledovat historický vývoj jedné nebo více proměnných najednou. Ve velkých SCADA aplikacích, se ukládá velké množství proměnných a z toho důvodu je nárok na hardware vyšší.

Aplikace	Nároky	Jádra CPU	RAM	HDD	Rychlost sítě
25 – 50 tisíc proměnných	Minimální	4	8 GB	500 GB	100 Mbps
	Požadované	8	16 GB	500 GB	1000 Mbps

Tabulka 2 – HW na velké SCADA aplikace

Na následujícím obrázku je znázorněno celkové zatížení počítače při požadované konfiguraci z tabulky č. 1. Červené zvýraznění je pro procesorový čas v %, modré zvýraznění je pro RAM.



Obr. 15 – HW zatížení malé SCADA aplikace

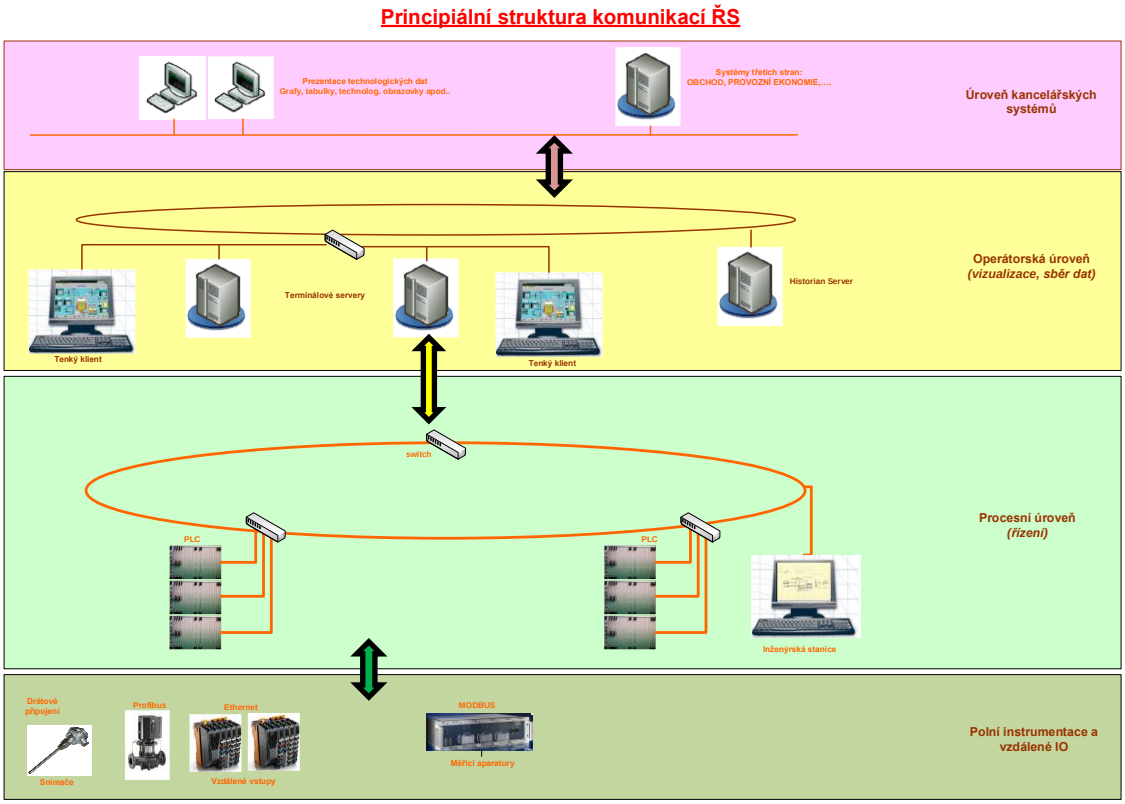
Z tohoto obrázku je patrné, že hardwarové požadavky, které jsou od společnosti WonderWare požadované, jsou plně dostačující pro provoz malé aplikace. Tabulky požadovaných nároků na hardware vycházejí z oficiálního doporučení od společnosti WonderWare. [16]

5 Popis návrhu nového řešení

Stávající vizualizační aplikace jsou spuštěny na jednotlivých desktopových zařízeních, kde je nainstalován operační systém Windows 7. Tento operační systém již není od 1. ledna 2020 společností Microsoft podporován, a verze vizualizační aplikace InTouch (2014 R2) není na novějších operačních systémech podporovaná. Z tohoto hlediska a zároveň i z hlediska stáří hardwaru desktopových stanic je nutné přistoupit k obnově těchto desktopů.

Obnova řešená instalací novějšího operačního systému Windows 10 neřeší bezpečnostní rizika z hlediska kybernetické bezpečnosti. Tato možnost obnovy bude zároveň klást ještě větší nároky na administraci systému například tím, že společnost Microsoft vydává každý rok nové, tak zvané „sestavení“ operačního systému. Může se stát, že v novém sestavení systému nemusí být vizualizace zcela kompatibilní a můžou se zde objevit chyby. Toto sestavení je tedy víceméně nová verze operačního systému, která musí být před nasazením do průmyslu důkladně otestována.

Z výše uvedených důvodů je navržena změna architektury operátorských stanic, kde vizualizační aplikace InTouch bude k dispozici na terminálovém serveru (redundantní pár). Terminálový server je výkonný stroj, který umožňuje spuštění více relací vizualizační aplikace InTouch a zároveň zajišťuje komunikaci jak na procesní (PLC), tak i na operátorskou úroveň. U operátora je namísto desktopových zařízení umístěn tenký klient, který je bez operačního systému, bez úložiště a rotačních prvků, jako jsou ventilátory a podobně. Tento tenký klient komunikuje s terminálovými servery pomocí RDP. Jakmile se tenký klient připojí k serveru, naváže s ním relaci. V této relaci, která je řízena serverem, si poté spustí všechny požadované aplikace. Na terminálovém serveru jsou tyto relace na sobě nezávislé a jsou zde všechny výpočetní činnosti. Tato komunikace bude probíhat po stávající technologické síti.



Obr. 16 – Nová struktura komunikací ŘS

Na těchto terminálových server bude nainstalován software ThinManager, který se používá pro správu a provoz tenkých klientů a umožňuje optimální rozložení zátěže terminálových serverů.

Toto navrhované řešení má výrazně vyšší kybernetickou bezpečnost, protože není třeba řešit zabezpečení přístupu na klientské straně. Operátorovi se doručuje pouze vizualizační aplikace a sám nemá přístup k ničemu jinému. Na tenkém klientovi nejsou ovladače USB a to znamená, že se škodlivý kód nemůže v případě vložení USB spustit. Veškerá správa tedy bude prováděna na terminálových serverech (Windows Update, antivirus, zálohování). Nebude třeba starat se o koncové tenké klienty. Ty administrátor nebo provozní mechanik v případě poruchy pouze vymění. [7]

5.1 Specifikace tenkých klientů

Tenký klient, který bude sloužit jako grafický výstup z terminálového serveru a bude z něj moct být ovládán daný technologický celek je jednou z důležitých částí. Nakonec došlo k nákupu 10 tenkých klientů značky NexCom NISE 105-E3845 s doplňující RAM pamětí 4 GB. [17]

CPU	Intel Atom E3845, Quad Core, 1.91GHz
RAM	1x 4GB DDR3L
Ethernet	2x Intel I210IT, podporující Teaming a PXE
Grafický výstup	1x DVI, 1x HDMI
Napájení	24V DC ze zálohovaného napájení
Chlazení	Pasivní

Tabulka 3 – Specifikace tenkého klienta

5.2 Specifikace terminálových serverů

Jednou z důležitých částí je návrh specifikace terminálových serverů. Z důvodu vyššího počtu relací InTouch, které na serverech budou probíhat, je nutné počítat s vyšším výkonem těchto strojů. Specifikace proto byla provedena na základě sledování výkonu desktopových operátorských stanic (obr. 15). Zároveň bylo postupováno tak, aby měl server při vyšším počtu relací dostatečný výkon pro vykonávání ostatních důležitých částí, které jsou potřeba pro plynulý chod tohoto návrhu.

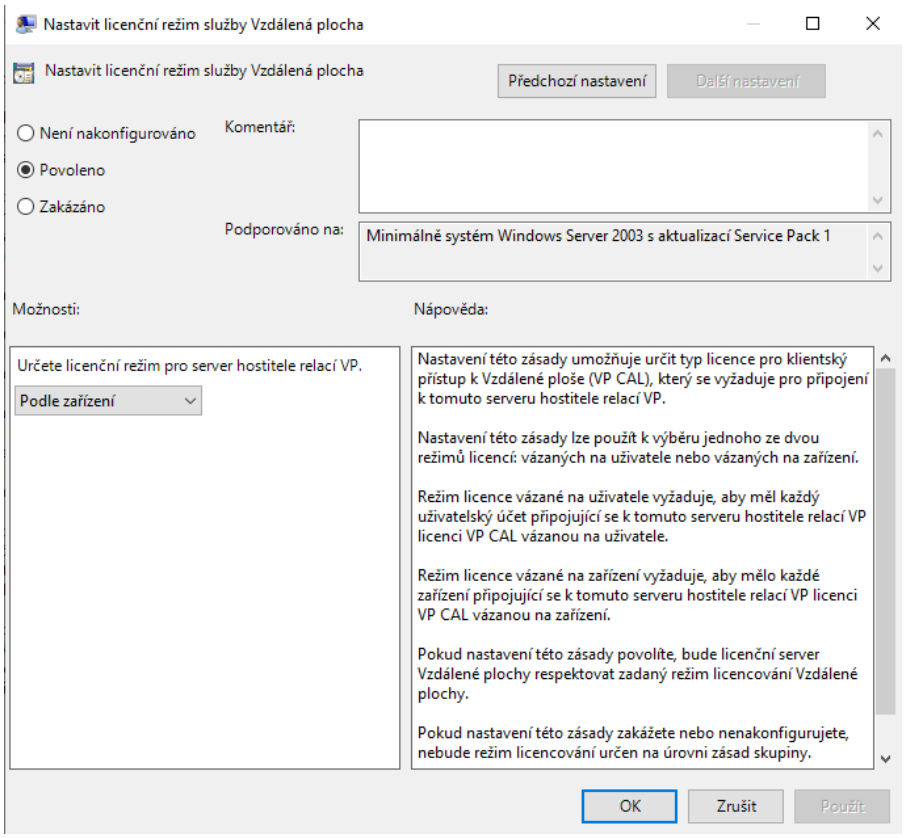
Specifikace HW terminálových serverů	
Operační systém	Windows Server 2019
CPU	2x Intel Xeon Silver 4216 2.1G, 16C/32T
RAM	4x 16GB RDIMM, 2666MT/s
Ethernet	3x Dual Port – 10/100/1000BASE-T
HDD	6x 600GB SAS 12Gbps 10k, Raid 10, Cache 2GB
Napájení	Redundantní napájecí zdroj, výkon napájecího zdroje doporučí výrobce tak, aby server byl schopen bez omezení být provozován na jeden zdroj

Tabulka 4 – Specifikace HW terminálových serverů

5.2.1 Konfigurace serverů

Nejprve je zapotřebí přidat role serverům, které slouží jako servery vzdálených služeb (terminálové servery). Role, které je potřeba na serverech nastavit, jsou Remote Desktop Session Host a Remote Desktop Licensing. RDSH (Remote Desktop Session Host) je role, která serveru umožňuje hostovat aplikaci v rámci vzdálené plochy. K tomuto účelu budou vytvořeny uživatelské účty, které se budou připojovat k RDSH serveru a následně tak mohou vzdáleně spustit aplikaci.

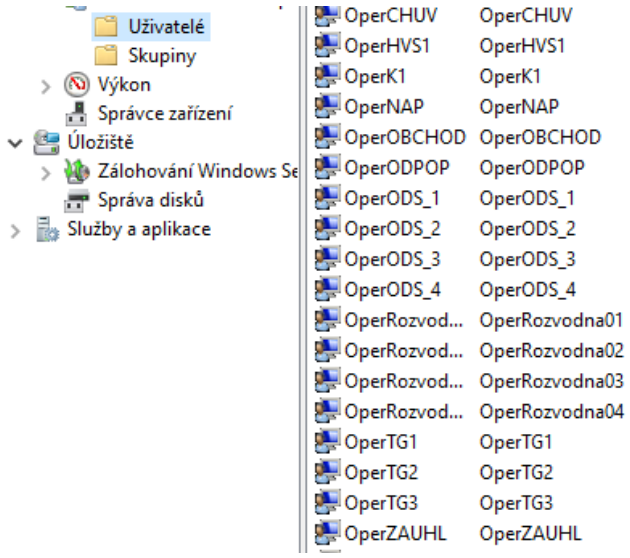
RDL (Remote Desktop Licensing) je role, která serveru umožňuje spravovat oprávnění pro RDS klienta. K oprávněnému připojení k relaci vzdálené plochy klienta je vyžadována licence RDS CAL, která je určena pro jednoho klienta. Z tohoto důvodu je potřeba mít licence RDS CAL pro každé zařízení, které bude navazovat relaci se serverem. Dále je potřeba nastavit pomocí „Group Policy Editor“ licenční režim služby vzdálená plocha, který může být pro uživatele nebo pro zařízení. V tomto případě jsou zakoupeny RDS CAL licence určené pro zařízení (Per Device). [18]



Obr. 17 – Nastavení RDS CAL podle zařízení

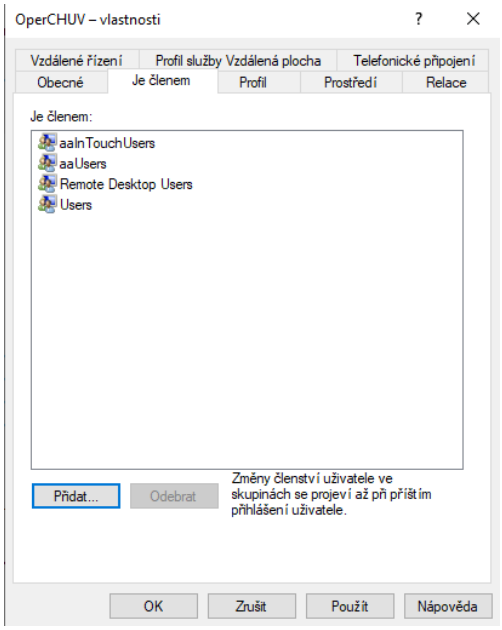
5.2.2 Konfigurace uživatelů

K tomu, aby klient dokázal navázat relaci, je potřeba na serverové straně nakonfigurovat uživatelé. Pro návrh nového řešení není potřeba doména, a tak budou uživatelé založeni na terminálových serverech. Tito uživatelé jsou vytvořeni pro dané operátorské stanoviště, například pro operátorské stanoviště „Chemická úprava vody“ je vytvořen účet OperCHUV. Tímto způsobem jsou vytvořeni i další uživatelé, kteří se serverem budou navazovat relace.



Obr. 18 – Vytvoření uživatelů

Po vytvoření daných uživatelů je pro navázání relace nutné určit oprávnění a přidat uživatele do skupin. Tito uživatelé jsou přidáni do skupiny „Users“ a dále pak do skupiny „Remote Desktop Users“, která zajistí vzdálený přístup k terminálovým serverům a naváže potřebnou relaci. V neposlední řadě jsou uživatelé přidáni do skupiny „aaUsers“ a „aaInTouchUsers“. Tyto skupiny mají práva pro čtení a zápis do adresáře InTouch a adresáře který je určen dané aplikaci InTouch. Bez těchto práv by daný uživatel nebyl schopný aplikaci spustit a ovládat, nebo ukládat nezbytně potřebná data pro běh aplikace InTouch.



Obr. 19 – Přidání uživatelů do skupin

5.3 ThinManager

Tento software pracuje na základě služeb vzdálené plochy a umožňuje doručování vizualizačních aplikací na tenké klienty. Veškeré aplikace, které budou potřeba doručit na tenkého klienta, jsou tedy nainstalovány na serveru a na tenkém klientovi je nainstalován pouze protokol určený ke komunikaci se serverem.

ThinManager zajišťuje bootování tenkých klientů, kde na základě MAC adresy tenkého klienta je mu přidělena IP adresa a následně jsou spuštěny nakonfigurované vizualizační aplikace. Tento software zároveň nabízí vysokou dostupnost aplikací, kde v případě výpadku jednoho serveru (například plánovaná údržba) dojde k automatickému přepnutí klientů na dostupný záložní server bez výpadku vizualizační aplikace. ThinManager umožňuje konfiguraci nastavení zobrazení na daném tenkém klientovi. Pomocí toho

mohou být klientovi se třemi monitory doručeny tři různé aplikace, které běží na každém monitoru zvlášť.

5.3.1 Základní nastavení ThinManager

Po nainstalování softwaru ThinManager a konfigurací serverů je možné přistoupit ke konfiguraci tohoto softwaru. Před konfigurací je ale potřeba povolit na firewall následující porty:

- UDP/4900 – používá se ke stažení firmwaru pomocí TFTP (protokol určený k přenosu souborů),
- TCP/2031 – slouží k předání konfigurace z ThinManager serveru k tenkému klientovi,
- UDP/67 – přiřazení IP adresy,
- UDP/69 – používá se serverem PXE (Preboot Execution Environment, používá se pro bootování tenkých klientů ze sítě),
- TCP/3389 – používá se protokolem RDP,
- TCP/5900 – používá se pro připojení k tenkému klientovi a umožnuje manipulaci s aplikací,
- TCP/3268 – používá protokol LDAP (Lightweight Directory Access Protocol), který slouží pro ukládání a přístup k datům na terminálovém serveru.

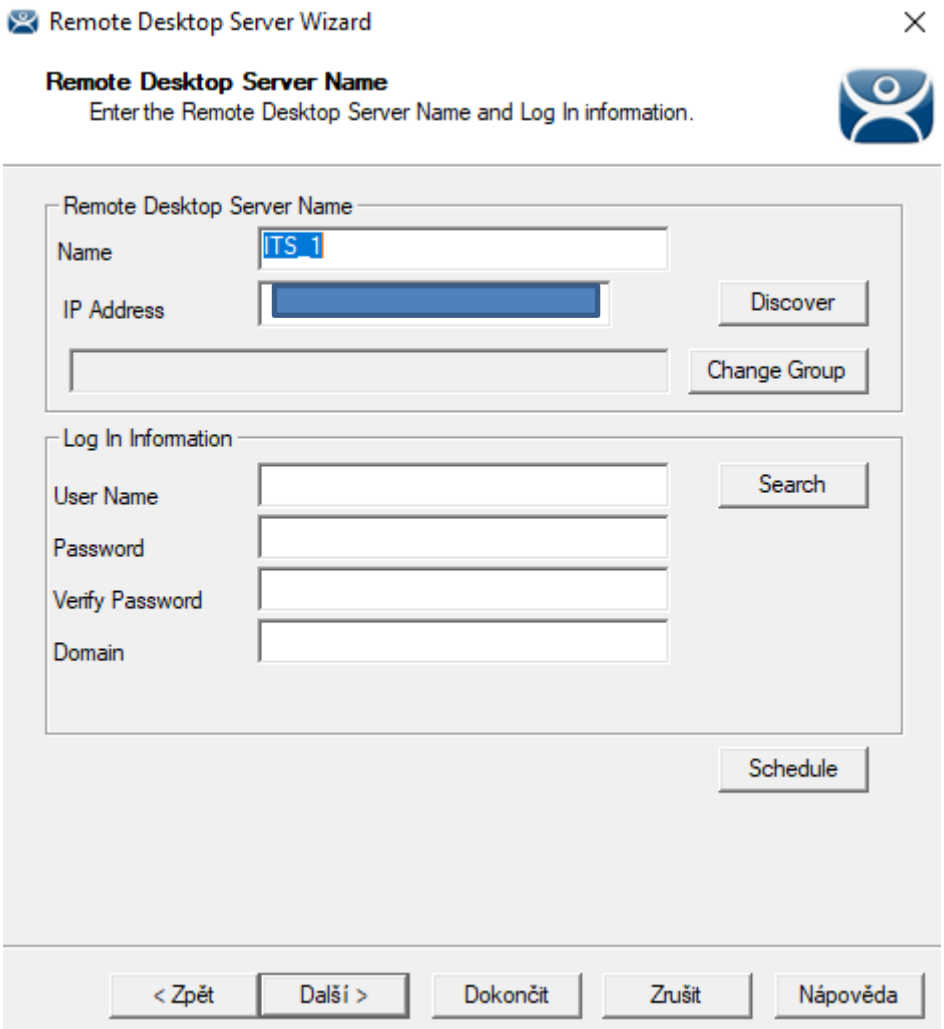
Po povolení těchto důležitých portů na firewall je možné přistoupit k samotné konfiguraci softwaru ThinManager. Grafické prostředí samotného softwaru je velice přehledné a práce s ním je snadná. Dělí se na různé sekce, které jsou potřeba nakonfigurovat pro správné fungování.

Obr. 20 – Sekce ThinManageru

V popisovaném nasazení jsou potřebné sekce „Display Servers“, „Display Clients“ a „Terminals“. Sekce „ThinManager Server“ zobrazuje pouze základní informace o běhu serveru a různé reporty a eventy, které se staly na klientech a zároveň kolik klientů je připojeno k hostitelskému serveru. Sekce „Users“ se používá pouze v tom případě, jestliže se pracuje s doménou, a tudíž se s touto sekcí nebude pracovat. [19]

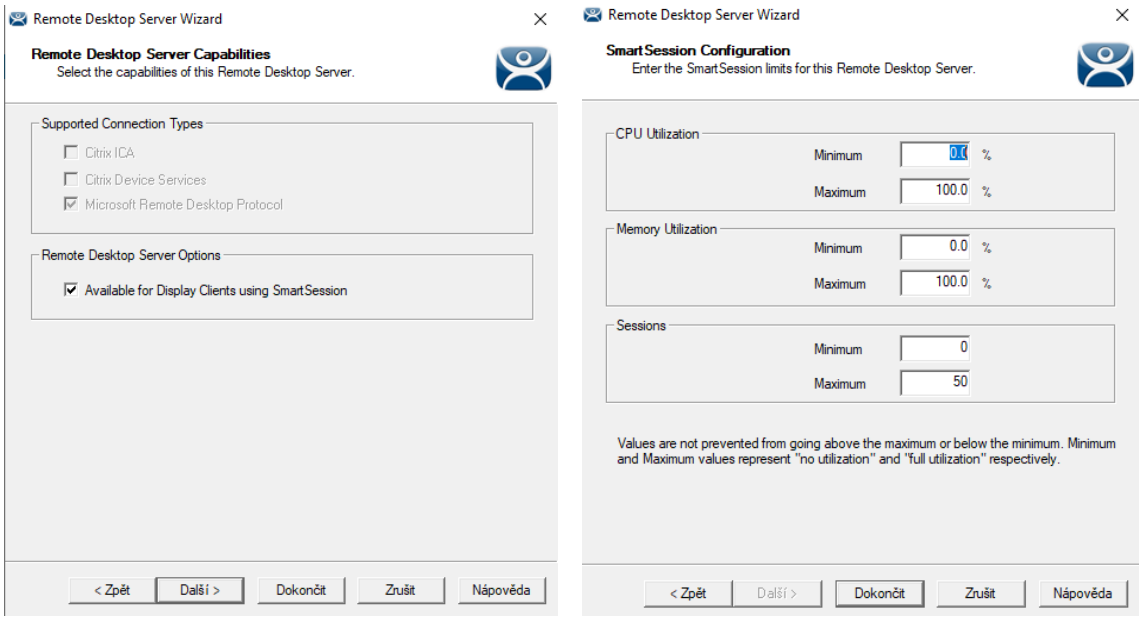
5.3.2 Přidání RDS serveru

Na začátku konfigurace je potřeba přidat do softwaru terminálové servery, jejichž úloha je být hostitelem relací tenkých klientů. Přidání se provádí v sekci „Display Servers“, kde po kliknutí pravým tlačítkem myši na „RDS Servers“ a vybráním možnosti „Add Remote Desktop Server“ se následně zobrazí okno pro konfiguraci RDS serveru, do kterého se zadá název serveru a jeho IP adresa.



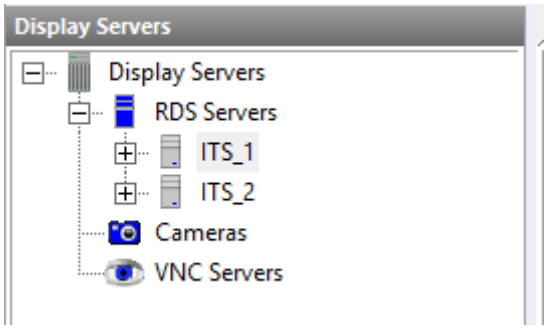
Obr. 21 – Přidání RDS serveru

V dalším kroku je potřeba zvolit, jakým typem protokolu se budou klienti připojovat k terminálovému serveru. Je zde možnost povolit SmartSession. SmartSession je relace, která se podle vytížení serveru rozhoduje, kde otevře další relace a zajistí tak efektivní provoz serverů.



Obr. 22 – Konfigurace protokolu a SmartSession

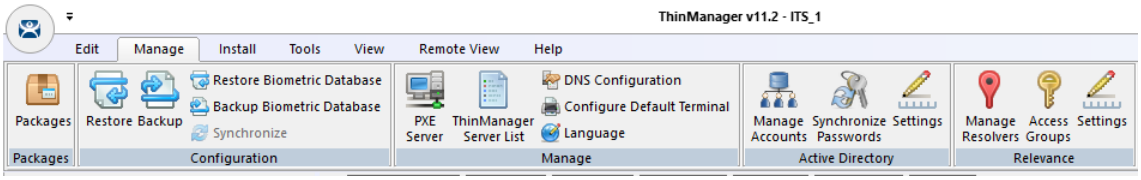
Po dokončení těchto kroků je stejným způsobem přidán stejně nakonfigurovaný redundantní server. Úspěšné přidání serverů lze ověřit v sekci „Display Servers“, kde je pod záložkou „RDS Servers“ možno vidět všechny přidané terminálové servery. [19]



Obr. 23 – Zobrazení serverů

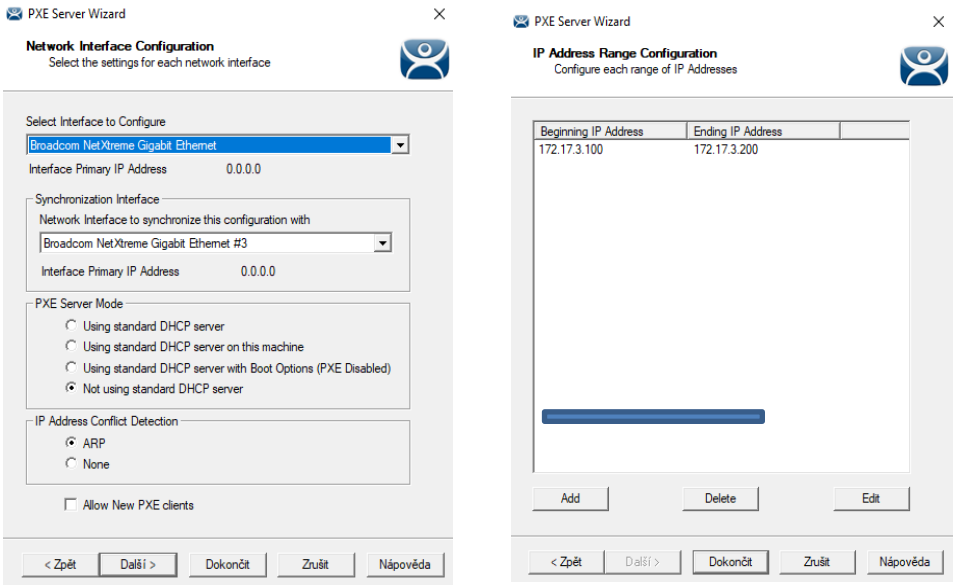
5.3.3 Konfigurace PXE

Jelikož provozní síť podniku nevyužívá DHCP server a adresy jsou vždy přiřazeny manuálně administrátorem, je v novém řešení využíván PXE server. PXE (Preboot Execution Environment) má za úkol bootování tenkých klientů z počítačové sítě. Konfigurace se vyvolá z hlavního okna ThinManageru, kde je potřeba stisknout možnost „PXE Server“.



Obr. 24 – Hlavní okno

PXE je v řešení nakonfigurováno na síťovou kartu, pomocí které se server dostane do operátorské VLAN. Dále je v konfiguraci adresní rozsah, ze kterého jsou poté přiřazeny IP adresy tenkým klientům.



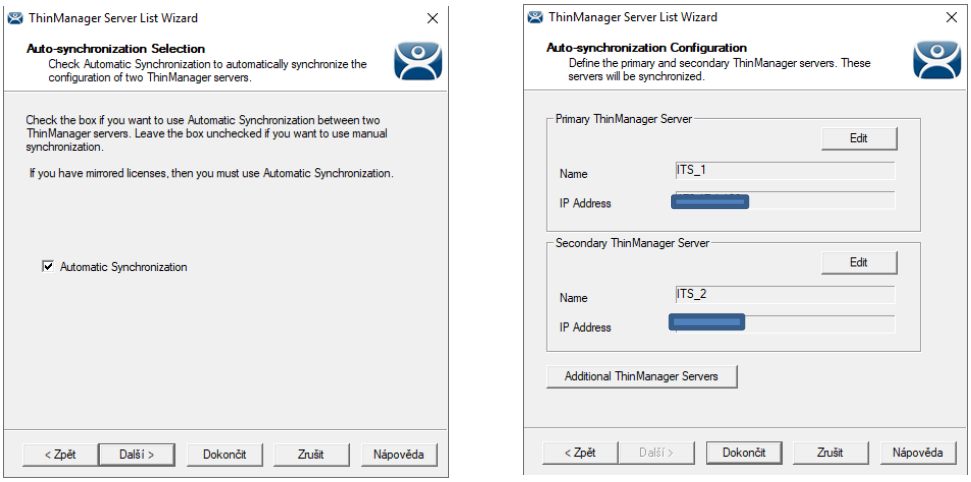
Obr. 25 – Konfigurace PXE

Pro zaručení funkčnosti komunikace mezi tenkým klientem a PXE serverem je nutné na tenkém klientovi v BIOS povolit bootování ze sítě. Poté zažádá tenký klient o přidělení základních údajů nutných pro komunikaci v síti. ThinManager server má v konfuguraci terminálu nastavené MAC adresy, na které má odpovídat. Jestliže byla nalezena tato MAC adresa, je tenkému klientovi odeslán balíček se základními údaji a tento balíček je poté stažen a načten do paměti RAM tenkého klienta. Zároveň s tím je mu zaslán i

bootovací balíček, pomocí kterého se zavede operační systém a spustí se dané nakonfigurované zobrazení. [19]

5.3.4 Synchronizace serverů

Synchronizace zajišťuje, že konfigurace provedené na jednom serveru se promítnou i na serveru druhém (redundantním serveru). To ulehčuje práci zejména v tom, že se nic nemusí konfigurovat dvakrát. Pomocí synchronizace zároveň získáme automaticky řízenou redundanci, kdy jeden ze serverů je „Master“ (hlavní server) a druhý je „Slave“ (sekundární server). Tato konfigurace se vyvolá pomocí hlavního okna ThinManageru (viz Obr. 24) stisknutím volby „ThinManager Server List“. Po stisknutí se vyvolá průvodce konfigurací. V této konfiguraci je zapotřebí povolit funkci „Automatic Synchronization“ a následně nastavit ThinManager servery, u kterých bude tato automatická synchronizace aplikována. [19]

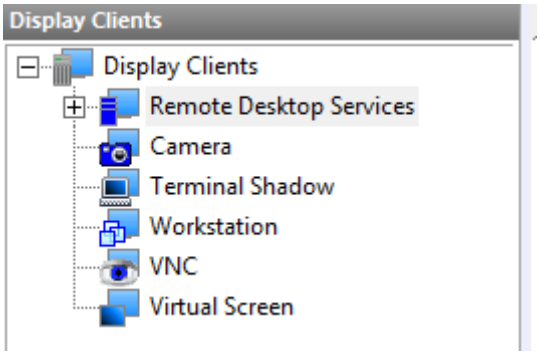


Obr. 26 – Nastavení synchronizace

5.3.5 Konfigurace zobrazení

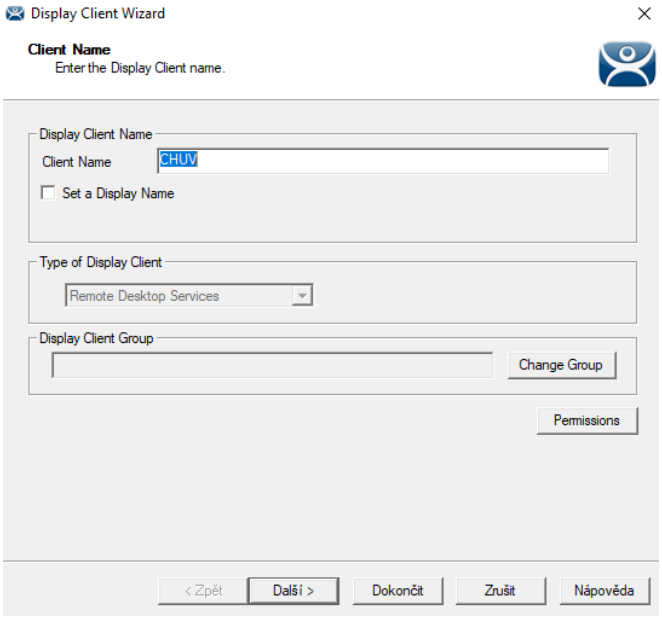
Po přidání terminálových serverů, které budou využívány, následuje konfigurace zobrazení na klientovi. K takovému nastavení a přidání daného zobrazení se využívá sekce „Display Clients“ v softwaru ThinManager. Toto zobrazení je poté určeno pro jednoho klienta, nebo je používáno větším počtem klientů. Tato konfigurace slouží k zobrazení grafického výstupu z RDS serverů. Může se jednat o klasickou relaci služby

vzdálené plochy nebo například o IP kamery, pracovní stanici, VNC (virtuální stroj) a v neposlední řadě virtuální obrazovku.



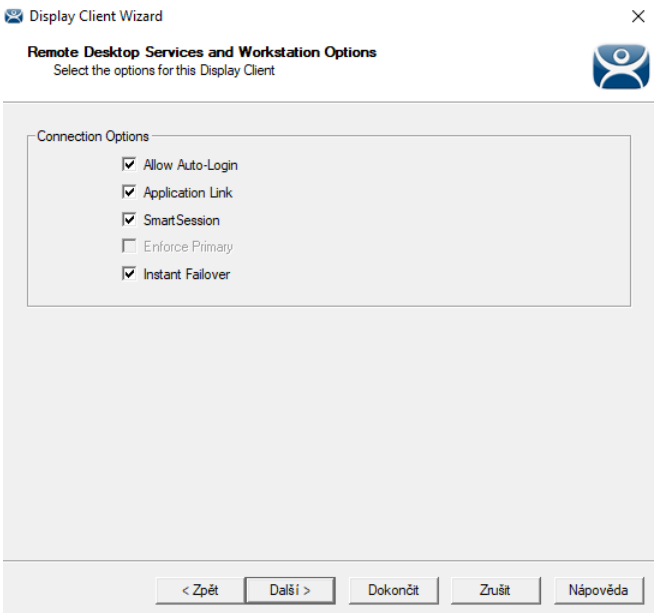
Obr. 27 – Sekce Display Clients

Jelikož IP kamery a ostatní relace nespadají v podniku pod správu provozní sítě, nebudou proto v řešení použity. V řešení bude použita pouze klasická relace služby vzdálené plochy. Vytvoření relace se zajistí kliknutím pravým tlačítkem myši na „Remote Desktop Services“ a vybráním možnosti „Add Display Clients“. Opět se zobrazí průvodce konfigurace, kde se zadá jméno zobrazení.



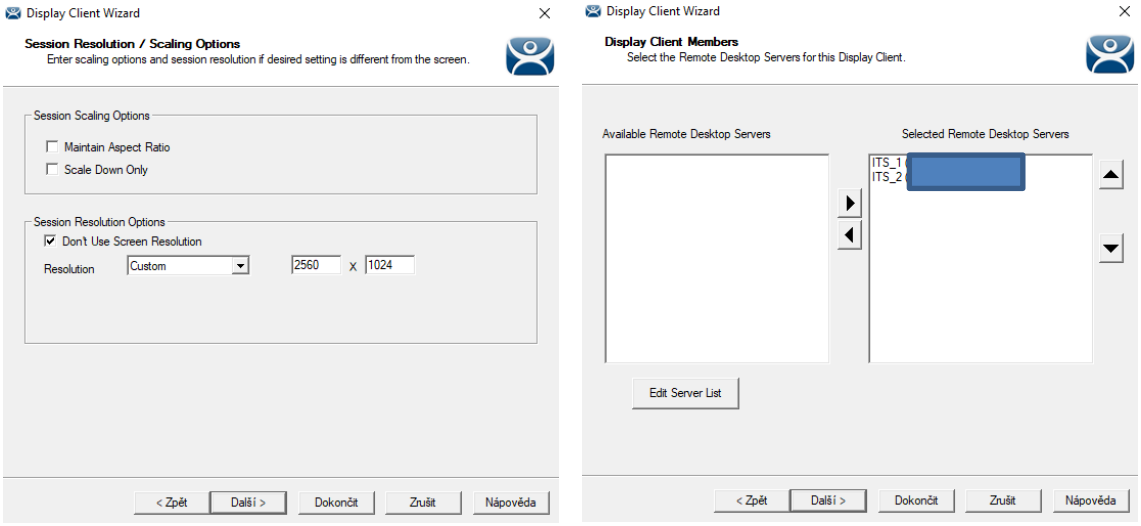
Obr. 28 – Přidání zobrazení

Po kliknutí na tlačítko „Další“ je na řadě nastavení, zdali se uživatel bude muset přihlašovat manuálně, nebo automaticky. V tomto případě je možnost „Allow Auto-Login“ povolena a tím je usnadněn operátorům přístup do aplikace. Možnost „Application Link“ slouží k doručení administrátorem vybrané aplikace na klienta. Tím je uživateli povolen přístup pouze do vybrané InTouch aplikace a také zabráněn jakýkoliv přístup uživatele do operačního systému. Tím, že se uživatel (operátor) nedostane do operačního systému, je ošetřeno úmyslné či neúmyslné spuštění škodlivého kódu ze strany uživatele. Další povolená možnost je „SmartSession“ určená k efektivnímu provozu serverů podle vytíženosti systému. A jako poslední povolená možnost je „Instant Failover“, která zajistí spuštění relace jak na primárním serveru, tak spuštění relace na sekundárním serveru (redundance). Touto možností je ošetřen výpadek jednoho serveru (například z důvodu plánované údržby), kdy se tenký klient automaticky přepne na sekundární server.



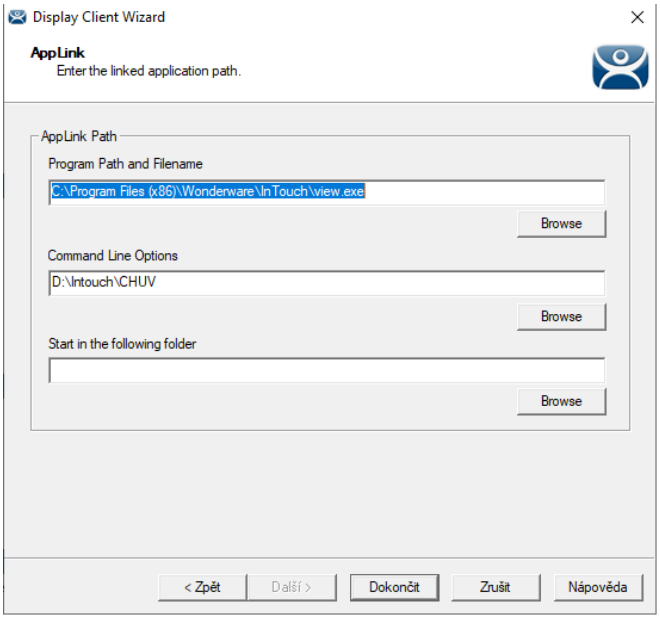
Obr. 29 – Konfigurace relace

Další důležitou částí nastavení zobrazení je konfigurace rozlišení relace a následné vybrání serverů, na kterých bude relace navázána. Podporované rozlišení softwaru je velké množství. Je možné nastavit i definovat vlastní rozlišení. V tomto případě je ale třeba vědět, jaké rozlišení je podporováno ze strany tenkého klienta. Pokud dojde k nastavení nepodporovaného rozlišení, pak tenký klient nabootoje, ale nebude schopný zobrazit obraz na monitoru.



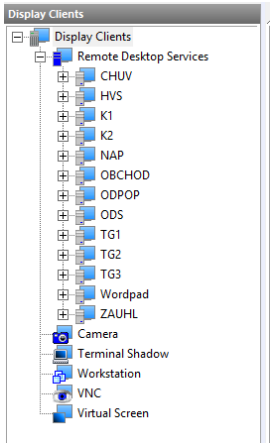
Obr. 30 – Nastavení rozlišení a serverů

Jako poslední nastavení, které je potřeba provést před dokončením konfigurace zobrazení, je nastavení aplikačního linku. Pomocí tohoto linku bude po automatickém přihlášení uživatele zajištěno, že se na tenkém klientovi spustí pouze tento nadefinovaný software. Z toho důvodu není potřeba řešit kybernetickou bezpečnost na koncových klientech. První link „Program Path and Filename“ je cesta k adresáři, kde je nainstalovaný vizualizační software InTouch. Vizualizační software InTouch ale nemůže být spuštěn bez definování, která aplikace má být spuštěna. K tomuto účelu slouží druhý link, což je cesta k adresáři s danou spouštěnou aplikací.



Obr. 31 – Aplikační link

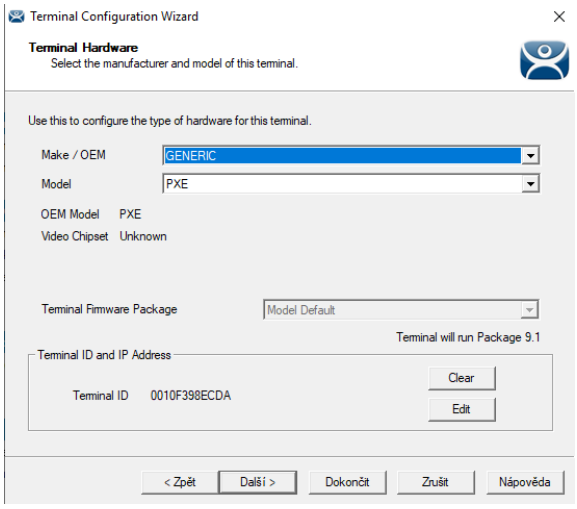
Stejným způsobem budou vytvořeny všechny zbývající konfigurace zobrazení, které budou pomocí ThinManageru doručené na tenké klienty. Lišit se budou pouze v aplikačním linku, protože je potřeba doručit na tenké klienty takové aplikace, které jim náleží. Zobrazení, která jsou v ThinManageru nadefinovaná lze vidět v přehledové sekci „Display Clients“. [19]



Obr. 32 - Zobrazení

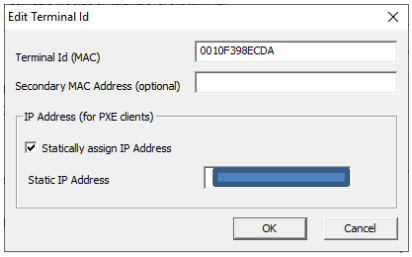
5.3.6 Konfigurace tenkých klientů

Při založení nového tenkého klienta se jedná o stejný postup jako u předchozích konfigurací. Konfigurační okno se vyvolá po stisknutí pravého tlačítka myši na „Terminals“ a zvolením volby „Add Terminal“. Po této akci přijde na řadu zadání názvu terminálu. Jakmile je zadán název terminálu, je nutné v konfiguračním okně vybrat, že se jedná o zaváděcího klienta PXE. V nabídce se tedy vybere možnost GENERIC/PXE.



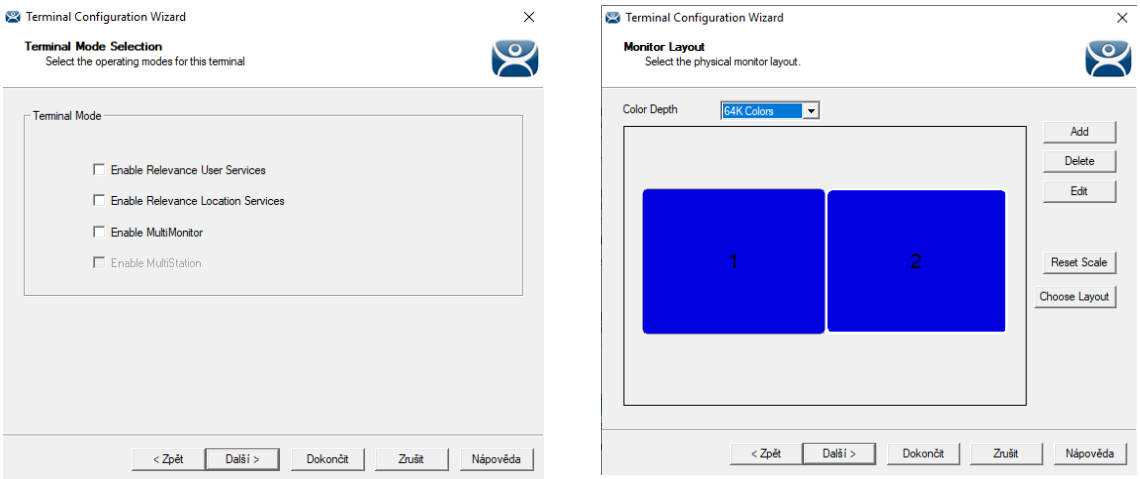
Obr. 33 – Konfigurace údajů pro klienta

Dalším krokem je přiřazení IP adresy na základě MAC adresy. Tento krok je dostupný z tlačítka „Edit“ v konfiguračním okně na obrázku 33. V následně vyvolaném okně se do části „Terminal Id (MAC)“ zadá MAC adresa tenkého klienta a následně se v části „IP Address (for PXE clients)“ povolí volba „Statically assign IP Address“ pro zadání IP adresy, která bude přidělena tenkému klientovi.



Obr. 34 – Konfigurace IP adresy

Při pokračování v konfiguraci je možné nastavit více monitorové zobrazení, pokud se používá více monitorů pomocí vybrání volby „Enable MultiMonitor“. Pomocí tlačítka „Add“ dojde k vyvolání nabídky s výběrem rozlišení monitoru a následně je možné monitor přidat do layoutu. Při kliknutí levým tlačítkem myši na plochu monitoru lze daný monitor odstranit („Delete“) nebo upravit pomocí tlačítka „Edit“, kde je možné upravit rozlišení či hloubku barev. Pomocí „Choose Layout“ je dále možný výběr polohy monitorů – vedle sebe či pod sebou.

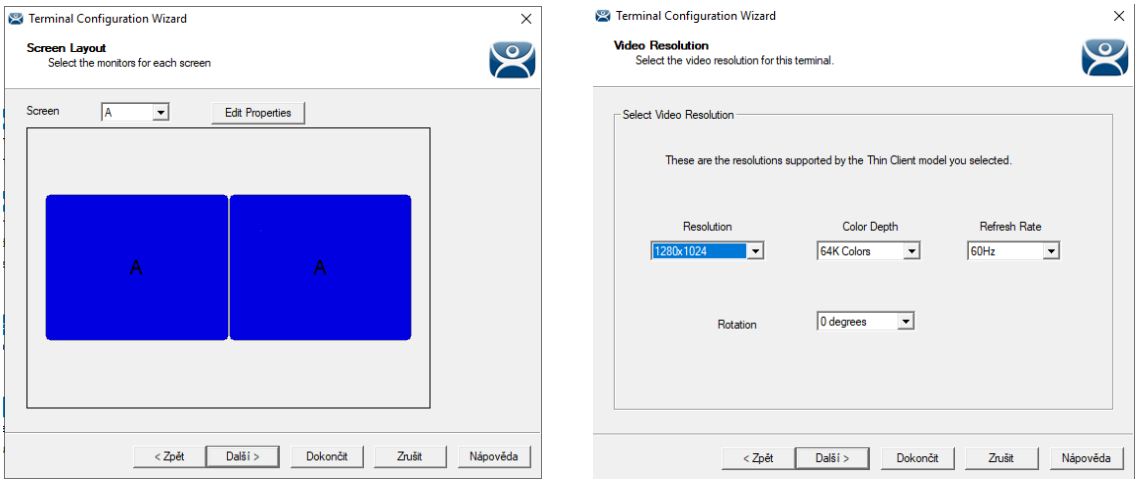


Obr. 35 – Konfigurace více monitorů

Po klepnutí na tlačítko „Další“ se konfigurace věnuje nastavení obrazovky. V tomto případě se obrazovka může nastavit jako koláž a tím se bude chovat jako jedna plocha

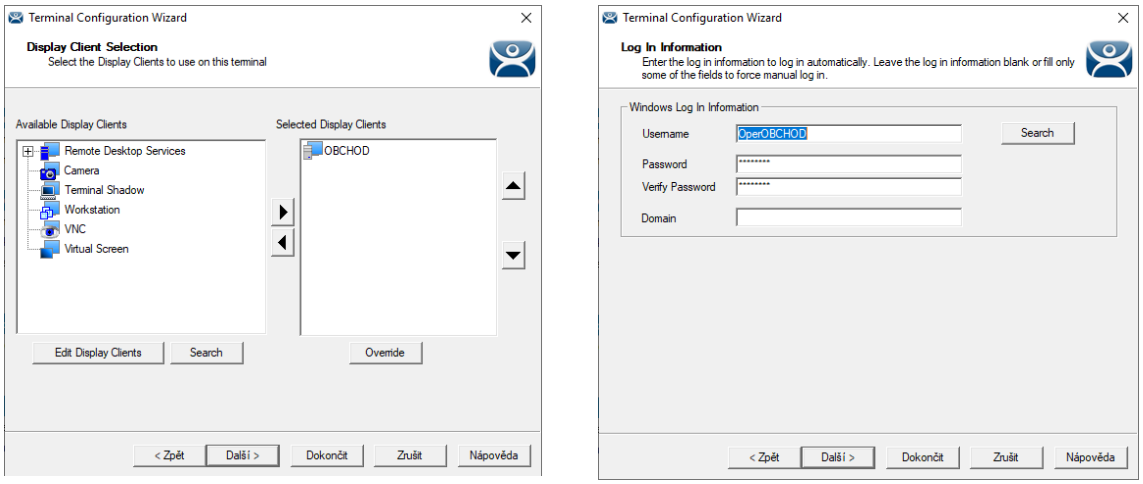
nebo je možné na každém monitoru spustit jinou aplikaci. Vše závisí na potřebách daného pracoviště a také na tom, co bude potřebovat operátor technologického celku.

Jestliže bude mít tenký klient k dispozici jen jeden monitor, pak se toto nastavení neřeší a volba „Enable MultiMonitor“ (viz Obr. 35) není povolena. V takovém případě se v konfiguraci nastaví rozlišení, barevná hloubka a podobně pro daný monitor.



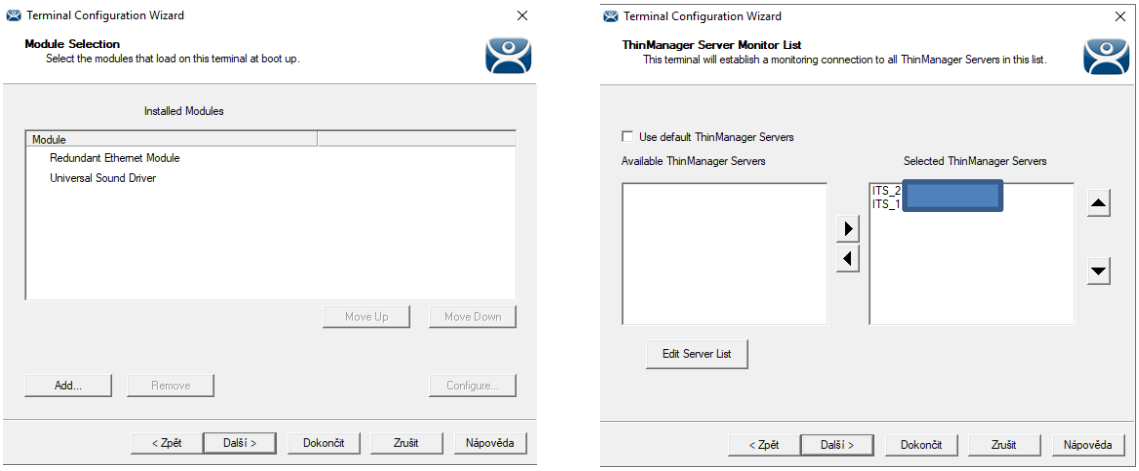
Obr. 36 – Konfigurace obrazovky

Pokračováním v konfiguraci nastává výběr aplikace, která bude spuštěna pomocí Remote Desktop Services na daném tenkém klientovi. Jedná se o předem nakonfigurovaného „Display Client“ (viz 5.2.3). Následně po výběru aplikace je potřeba zadat, pod kterým uživatelem bude RDS aplikace spuštěna. Zadaný musí být název uživatele a jeho přístupové heslo.



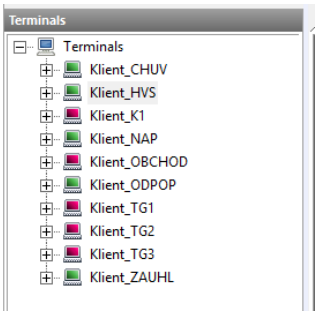
Obr. 37 – Nastavení aplikace a uživatele

Poslední kroky této konfigurace jsou moduly, kterými bude tenký klient disponovat. Jedná se o moduly například redundantní síťové karty, zvukový modul a mnoho jiných, které ThinManager nabízí. Pro popisované řešení plně postačí jmenované dva základní moduly. A jako poslední nastavení je přiřazení ThinManager serverů, na kterých budou relace navázané.



Obr. 38 – Konfigurace modulů

Po stisknutí tlačítka „Dokončit“ je konfigurace tenkého klienta hotová. Stejným způsobem probíhá konfigurace všech tenkých klientů, kteří jsou v řešení použiti. V sekci „Terminals“ pak jsou dostupní a viditelní všichni nakonfigurovaní klienti. Zelená barva znázorňuje spuštěného klienta, naopak červená barva znázorňuje vypnutého klienta. [19]

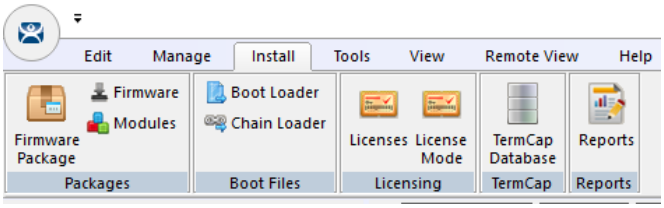


Obr. 39 - Klienti

5.3.7 Licencování

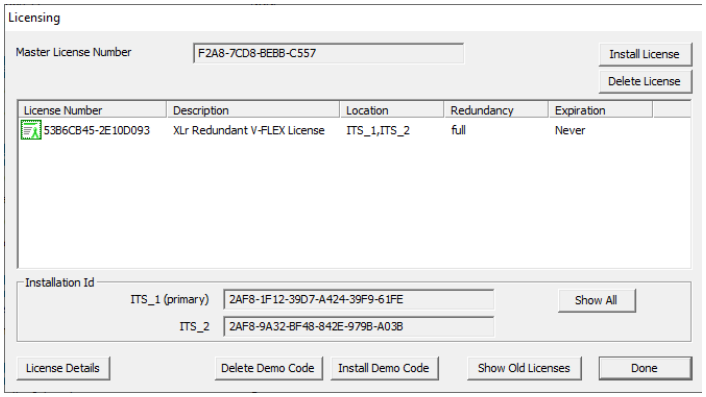
K tomu, aby byl software ThinManager používaný oprávněně, je potřeba vlastnit licenci. Tento software byl vyvinutý firmou Rockwell Automation, a proto i licencování probíhá na jejich straně. Nejprve je potřeba zažádat o licenci, která se dělí na různé části. Může se jednat o licenci Enterprise, kde ThinManager server může obsluhovat libovolný počet tenkých klientů. Tato licence je plně redundantní, proto není důvod kupovat licenci pro oba servery. Dále se může jednat o standartní licenci, kde je možné obsluhovat pouze určitý počet klientů (balíček pro 5, 10 nebo 25 klientů). V této licenci je potřeba zdůraznit, zdali se jedná o stand-alone ThinManager, nebo jestli se jedná o redundantní pár. Pro navrhované řešení plně postačuje standartní licence s obsluhou deseti klientů. Tato licence musí být zároveň plně redundantní.

Po obdržení licence je potřeba tuto licenci nainstalovat do softwaru. Instalace se vyvolá z hlavního okna (viz Obr. 24) pod záložkou „Install“, kde se po vyvolání volby „Install License“ otevře okno instalace.



Obr. 40 - Instalace

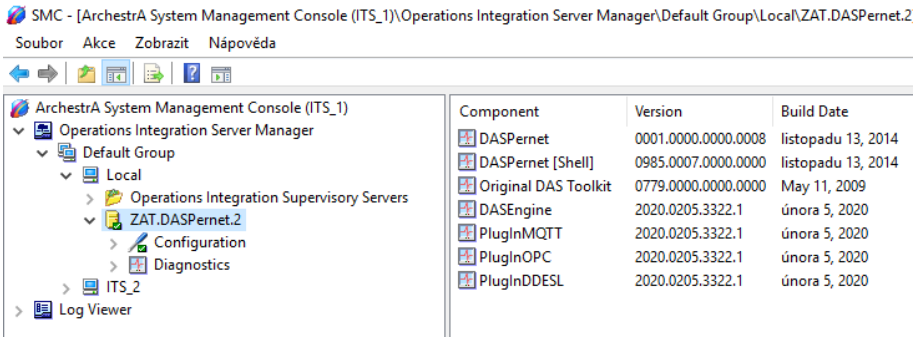
V tomto okně je důležitá možnost „Install License“, která po vyvolání otevře prohlížeč souborů Windows, kde je potřeba vybrat licenční soubor. Po výběru se následně v okně instalace zobrazí obdržená licence s informací redundance, či pro které ThinManager servery je licence určená. [19]



Obr. 41 – Licence

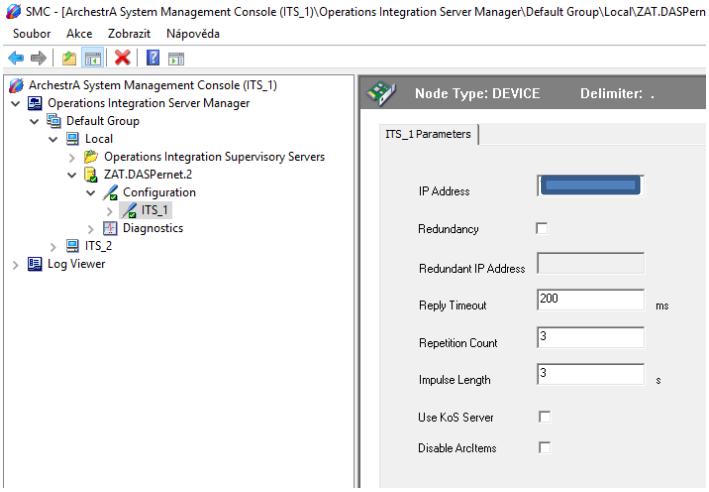
5.4 Konfigurace DASPernet

Konfigurací ThinManageru dostaneme vizualizaci technologického celku. K tomu, aby bylo možné ovládat danou technologii, je potřeba konfigurace komunikačního serveru DASPernet, který umožní komunikaci s PLC. Po nainstalování softwaru DASPernet na servery se softwarem ThinManager je možné přistoupit k dané konfiguraci. Konfigurace probíhá v programu System Management Console ve stromové struktuře Operations Integration Supervisory Servers, která je součástí instalace InTouch.



Obr. 42 – Stromová struktura DASPernet

Na začátku konfigurace je potřeba přidat do DASPernetu objekt „Device“. Tento objekt reprezentuje zařízení, respektive ethernetový port s IP adresou, která je určená ke komunikaci s řídícími stanicemi. Objekt se vytvoří vybráním volby „Configuration“, kde dojde pomocí stisku pravého tlačítka myši k vyvolání možnosti „Add Device Object“. Následně se objekt přidá do stromové struktury, kde je viditelný pod defaultním názvem, který je možný přejmenovat. V tomto objektu se poté nastaví IP adresa.

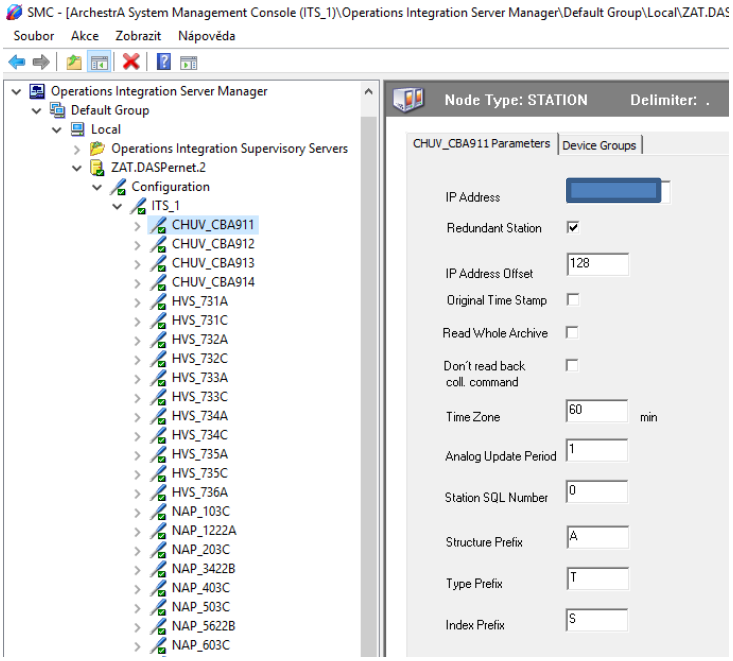


Obr. 43 – Objekt zařízení

Je možné zde zaškrtnout možnost „Redundancy“, která určuje, že komunikace bude redundantní, a je potřeba přidat IP adresu redundatního ethernetového portu. V okně je dále řádek „Reply Timeout“, kde tato hodnota udává dobu v milisekundách, do které musí řídící stanice odpovědět na požadavky serveru DASPernet. Tato hodnota je nastavena na 200 milisekund. Řádek „Repetition Count“ udává počet možných pokusů o žádost odpovědi na řídící stanice, než ji server prohlásí za nezodpovězenou. Hodnota, která udává délku impulzu pro impulzní výstupy v sekundách, je „Impulse Lenght“ defaultně nastavená na 3 sekundy.

Další částí konfigurace je přidání do objektu zařízení stanice, se kterými bude tento objekt komunikovat. Přidání stanice se provede vybráním objektu zařízení a následným vyvoláním možnosti „Add Statiton Object“ pomocí stisknutí pravého tlačítka myši.

Do stromové struktury se následně přidá objekt stanice opět s defaultním jménem, které je možné přejmenovat dle vlastního uvážení. V konfiguraci se poté nastaví IP adresa dané řídící stanice.

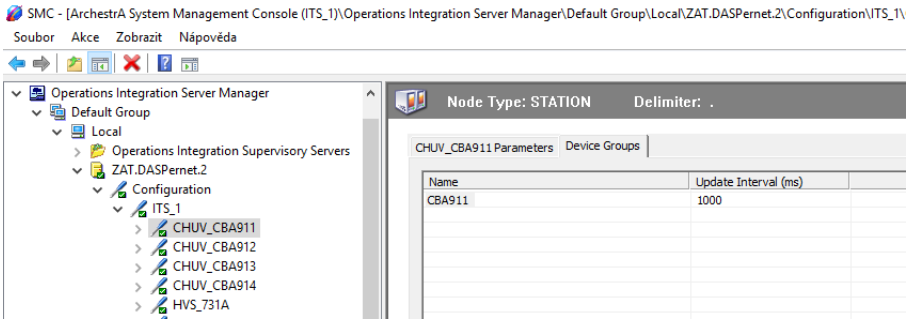


Obr. 44 – Objekt stanice

Jestliže je stanice redundantní, zaškrtne se možnost „Redundant Station“ a zadá se offset (posun mezi IP adresou stanice a IP adresou redundantní stanice) IP adresy redundantní stanice. Jestliže je ke komunikovaným proměnným nutnost přiřadit časovou značku, zaškrtne se možnost „Original Time Stamp“. Touto možností dojde k přiřazení časové značky pomocí protokolu Pernet. Hodnota „Time Zone“ je defaultně nastavena na

středoevropský čas (to je hodnota 60). Pomocí parametru „Analog Update Period“ lze nastavit periodu poskytování analogových a binárních proměnných připojeným klientům. Parametr je nastaven na 1, což znamená, že perioda je pro všechny klienty stejná. Poslední tři parametry „Structure Prefix“, „Type Prefix“, „Index Prefix“ určují formát adresy, ze které je proměnná čtena. V podniku se používá adresa, která začíná písmenem A, za kterým následuje číslo struktury. Po čísle struktury adresa pokračuje písmenem T, které určuje číslo typu proměnné (analogový typ nebo binární typ). Prefixový index je označen písmenem S, za kterým se nachází číslo indexu ve struktuře. Toto značení je libovolné a záleží na konkrétní firmě, jaké značení adres bude použito. Konfigurace všech ostatních stanic probíhá stejným způsobem.

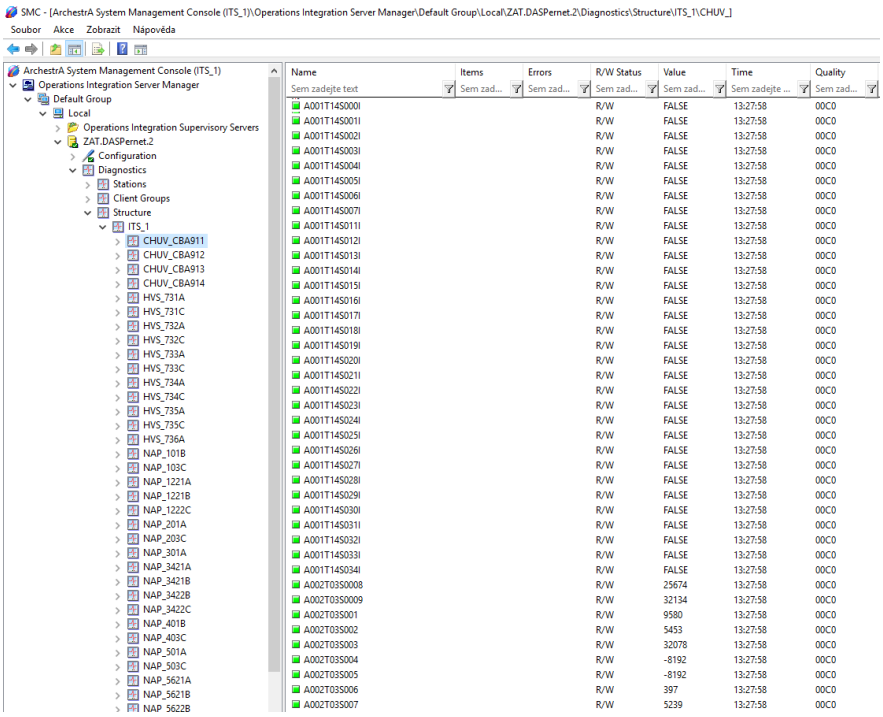
Poslední část konfigurace je nastavení názvu skupiny proměnných a doby aktualizace hodnot. Tato konfigurace je přístupná v sekci „Device Groups“ v okně konfigurace stanice (viz Obr. 44).



Obr. 45 – Skupina proměnných

Název této skupiny je v rámci celé konfigurace jedinečný a nemůže se opakovat. Pomocí tohoto názvu je poté navázáno čtení proměnných ve vizualizačním softwaru InTouch. Doba aktualizace je důležitým parametrem a nelze přesně stanovit její doporučenou hodnotu. Záleží zde na mnoha okolnostech, například na rozsáhlosti sítě, typu komunikujících stanic a zatížení sítě. V případě nastavení nízké hodnoty může docházet k výpadkům komunikace. Z tohoto hlediska je na všech nakonfigurovaných stanicích parametr nastaven na 1000 milisekund. V případě problému z komunikací je možné tento parametr zvyšovat.

Po konfiguraci daných stanic, které jsou potřeba, je nutné server DASPernet spustit, a to tím, že ve stromové struktuře vybereme „ZAT.DASPernet.2“ a pravým tlačítkem myši vyvoláme možnost „Activate“. Po aktivaci je možné sledovat hodnoty proměnných daných řídících stanic. Ve stromové struktuře vybereme volbu „Diagnostics“ a poté objekt zařízení, ve kterém se následně zobrazí strom všech nakonfigurovaných stanic. Po vybrání stanice se zobrazí všechny proměnné dané řídící stanice. [20]



Obr. 46 – Sledování proměnných

5.5 Zabezpečení serverů

Zabezpečení se oproti desktop řešení do jisté míry změní. Nebude již třeba věnovat se zabezpečení koncových stanic (tenkých klientů). Nastavení tenkých klientů je uzpůsobeno tak, aby uživatel koncových stanic obdržel jen to nejnutnější k obsluze technologie (vizualizační software). Operátor nemá možnost dostat se do operačního systému a nemá možnost zavádět jakákoliv přenosná média, která by mohla obsahovat škodlivý kód (CD, USB a podobně).

V novém řešení již také není potřeba instalovat na každou stanici antivirový software. Zároveň také není třeba instalovat bezpečnostní aktualizace na koncové stanice. Toto všechno je zajištěno na serverové straně. Administrátorovi se tedy ulehčí práce

s instalování bezpečnostních aktualizací a také v záplatě možných bezpečnostních děr. Aktualizace antivirových komponent a instalace bezpečnostních aktualizací zůstane stejná, jako tomu bylo i v desktop řešení, tedy přes server ESET Mirror a server WSUS.
Pravidelné zálohování bude probíhat velmi podobně jako v desktop řešení. Prováděno bude před každou bezpečnostní aktualizací prostřednictvím aplikace Acronis, která umožňuje vytvoření obrazu disku. V případě neočekávané chyby po aktualizaci zde bude možnost vrátit se zpět do fungujícího stavu a problém s aktualizací před jejím nasazením vyřešit. Dále pak bude zálohován adresář s vizualizační aplikací a adresáře, které jsou nutné nebo důležité pro bezproblémový chod vizualizační aplikace a serverů.
Zároveň se administrátor nemusí obávat výpadku jednoho serveru. Jestliže dojde k výpadku jednoho serveru, pak se vizualizační aplikace díky jejich konfiguraci automaticky přepnou na sekundární server a obsluha technologie tak není ztracena. Administrátor má poté dostatek času na to, aby vyřešil problémy se serverem, který zkolaboval.

5.6 Náklady

Implementace nového řešení bude probíhat v rámci investiční akce. Náklady nejsou zanedbatelné, ale očekává se, že postupem času se tato investice vrátí. Nebude se muset investovat do velkého množství desktopů, jako tomu bylo doposud, ale investice bude probíhat pouze do terminálových serverů.

Řešení s klasickými desktopy	
10x Operátorská stanice	150 000,- Kč
Výměna desktopů 1x za 4 roky	
Náklady na 20 let	**750 000,- Kč**
Předpokládaná životnost ŘS, se kterým operátorské stanice komunikují je 15 – 20 let	
Řešení s tenkými klienty	
10x Tenký klient	100 000,- Kč
2x Terminálový server	300 000,- Kč
Výměna serverů 1x za 5 let	
Náklady na 20 let	**1 200 000,- Kč**
Tenký klient – bez pravidelné výměny, předpokládaná životnost je 20 let (neobsahuje žádné rotační součástky, průmyslové provedení)	

Tabulka 5 – Náklady obou řešení

Předpokládá se, že na 2ks terminálových serverů bude nasazeno 20 tenkých klientů, tím se cenový rozdíl oproti klasickým desktopům sníží.

Nákladové rozdíly	
Původní řešení	
20x Operátorská stanice (5 výměn za 20 let)	**1 500 000,- Kč**
Nové řešení	
20x Tenký klient	200 000,- Kč
2x Terminálový server (4 výměny za 20 let)	1 200 000,- Kč
Celkem za nové řešení	**1 400 000,- Kč**

Tabulka 6 – Nákladové rozdíly

K nákladům na řešení terminálových serverů je potřeba připočítat cenu licencí ThinManager. Na druhou stranu, dojde k významnému snížení pracnosti administrace operátorských stanic a tomu odpovídající vytížení správců zařízení, kteří se tak budou moci věnovat i jiným věcem a stoupne tak produktivita práce.

Pokud by se zůstalo u řešení s klasickými desktopovými stanicemi, muselo by se řešit jejich důkladnější zabezpečení a z toho vyplývající finanční náklady. Použití ThinManageru přináší velkou flexibilitu a jeho přínosy významně přispívají ke snižování celkových nákladů na vlastnictví provozovaného informačního systému.

6 Hodnocení implementace

Na terminálové servery byly nainstalovány všechny prostředky, které jsou nutné k fungování RDS serveru. Tyto terminálové servery byly umístěny na bezpečné místo, kam má přístup jen administrátor serverů. Po instalaci potřebných funkcí a programů následovala konfigurace obslužného softwaru pro tenké klienty (ThinManager, viz 5.3).

Při této konfiguraci bylo postupováno tak, aby splňovala nároky provozu technologického zařízení podniku. Tedy spolehlivě doručit aplikaci na koncovou stanici, zajistit komunikaci s PLC pro plnou ovladatelnost technologického celku, odepřít operátorovi vstup do operačního systému a povolit pouze ovládání aplikace. Konfigurace tenkých klientů byla provedena pro 10 operátorských stanovišť. Na těchto stanovištích byla provedena výměna desktopové koncové stanice za tenkého klienta. K tomu, aby byl klient nabootován, je vyžadováno připojení k počítačové síti, pomocí které klient komunikuje s terminálovými servery po protokolu RDP. RDP zajistí multimediální informace (obraz, zvuk, atd.) ze serveru a dále pak zajistí přenos interaktivních akcí (interakce myši, klávesnice, atd.) od klienta směrem k serveru.

Operátoři těchto stanovišť velmi pomohli při odhalování chyb vizualizační aplikace způsobené migrací ze starého softwaru InTouch 2014 R2 na novou verzi InTouch 2020 R2. Důvodem chyb při migraci jsou rozdíly mezi verzemi softwaru InTouch.

V řešení je také velmi pozitivně vnímána redundance terminálových serverů, kdy při výpadku nedojde ke ztrátě ovládání, ale tenký klient se automaticky přepne na sekundární server. Zároveň s tím pak nedochází k výpadku sběru dat z těchto vizualizačních aplikací. Při výpadku serveru, ze kterého se provádí sběr dat, je tento sběr také automaticky přepnut na fungující sekundární server.

Současně s nasazením byl otestován i výkon samotných terminálových serverů. Testování probíhalo při průběžném nasazování tenkých klientů do provozu. Výsledek testování výkonnosti serverů, na kterých běží 10 aplikací InTouch, byl velice překvapivý. Toto množství totiž servery nijak nezbrzdilo a mohli by klidně pohltit všechny aplikace InTouch, které má podnik k dispozici (30 aplikací). Nasazení zbylých tenkých klientů na místo desktopového řešení je naplánováno v průběhu roku 2021.

Zpětná vazba od operátorů daných technologických pracovišť byla také velice překvapivá. Nejsou zde žádné hlášené chyby jako například „zamrzání“ aplikace, samovolné vypnutí aplikace, samovolné vypnutí počítače, dlouhé načítání historických

dat a mnoho jiných podobných hlášení. Zpětná vazba z hlediska nasazení nové technologie je velice důležitá. Od operátorů se mi dostalo spíše mnoho pozitiv, která převládala nad negativy.

7 Závěr

V této práci bylo popsáno stávající řešení pomocí desktopových koncových stanic. V důsledku velkých nevýhod s přechodem na novější operační systém desktopů (Windows 10), je následně součástí této práce návrh nového řešení pomocí terminálových serverů a tenkých klientů. Zároveň je v této práci popsáno možné praktické nasazení tenkých klientů do průmyslové společnosti, která získala prvotní zkušenosti s tímto novým systémem. Na základě těchto zkušeností byl nový systém otestován a nasazen do provozu na deseti operátorských stanovištích.

Několikatýdenní provoz odhalil, že servery jsou minimálně zatížené, a proto dojde v průběhu roku 2021 k nahrazení všech desktopových stanic tenkým klientem. Následně se ověřovala spokojenost s implementovaným novým systémem, kde pozitiva převládala nad negativy. Zpětná vazba od operátorů při implementaci nového systému je velice důležitá a je potřeba reagovat na podněty, které od nich přicházejí. Proto bylo provedeno vše, aby uživatelé tenkého klienta (koncové stanice) byli s implementací maximálně spokojeni.

Výhody, které s sebou přináší přechod na tenké klienty, jsou - nízká pořizovací cena klienta a také větší doba používání oproti desktopové stanici. Desktopová stanice musí odpovídat výkonovým požadavkům instalovaného software a tato stanice v sobě obsahuje součástky, které jsou často poruchové (ventilátory, rotační HDD). Oproti tomu se tenký klient jen připojí k serveru a veškeré operace, které jsou potřeba, zajistí server. Nutné je pouze vyhovět používanému komunikačnímu protokolu.

Implementace terminálových serverů a tenkých klientů a návrh nového řešení se ukázaly nejen jako vhodné do průmyslových aplikací, které patří do kritické infrastruktury, ale ukázaly se být také ekonomicky srovnatelné s řešením pomocí klasických desktopových stanic.

8 Seznam použité literatury

[1] BODUNGEN, Clint E., Bryan L. SINGER, Aaron SHBEEB, Stephen HILT a Kyle WILHOIT. *Hacking exposed industrial control systems: ICS and SCADA security secrets & solutions*. New York: McGraw-Hill Education, [2017]. ISBN 9781259589713.

[2] Daneels, Axel, and Wayne Salter. "What is SCADA?." (1999).

[3] GAUSHELL, Dennis J.; DARLINGTON, Henry T. Supervisory control and data acquisition. *Proceedings of the IEEE*, 1987, 75.12: 1645-1658.

[4] InTouch SCADA HMI. Pantek. [online]. © 2020 [cit. 2020-10-12]. Dostupné z: http://www.pantek.cz/produkty/intouch/

[5] SHANKAR, K. Gowri. Control of boiler operation using PLC–SCADA. In: *Proceedings of the International MultiConference of Engineers and Computer Scientists*. 2008. p. 19-21.

[6] HAWKINSON, Ellen; FORTIN, Timothy; VIDYASHANKAR, Anuradha. *OPC server redirection manager*. U.S. Patent Application No 11/786,510, 2007.

[7] Williams, Ian. "An Investigation into Current Thin Client/Server Computing Technology and its Impact Upon PC based Industrial Control and Supervisory Systems." (2002).

[8] GALEA, Nicholas. *Thin client server*. U.S. Patent Application No 11/179,131, 2007.

[9] THINMANAGER. Pantek (CS) s.r.o. Pantek (CS) s.r.o. – *Software pro digitální průmyslový svět* [online]. Dostupné z: https://www.pantek.cz/produkty/thinmanager/

[10] DOYLE, Paul, et al. Case studies in Thin Client acceptance. *ICIT Journal*, 2009, 3.1: 48-54.

[11] *Provozní předpis MaR č. 01/2014*.Neveřejný interní podnikový dokument, 2014. Mar – SKŘ všeobecná část.

[12] *Procesní stanice SandRA Z200.* [online]. Copyright © 2021 ZAT a. s. [cit. 2021-01-07]. Dostupné z: https://www.zat.cz/cz/procesni-stanice-rady-sandra-z200.htm

[13] *Co je OPC? OPC server? OPC klient?. FOXON / Opravy, prodej a IIoT v průmyslové automatizaci* [online]. Copyright © [cit. 2021-01-07]. Dostupné z: https://www.foxon.cz/blog/prakticka-teorie/159-co-je-opc-opc-server-opc-klient

[14] *Rozhraní OPC v systémech ZAT.* [online]. Copyright © Automa – časopis pro automatizační techniku, s. r. o. [cit. 2021-01-07]. Dostupné z:

https://automa.cz/cz/casopis-clanky/rozhrani-opc-v-systemech-zat-2006_07_31264_3236/

[15] *DDE And SUITELINK Explanation.* IPCS. [online]. 27. září 2019 [cit. 2021-01-07]. Dostupné z: https://ipcsautomation.com/blog-post/dde-and-suitelink-explanation/

[16] *System Platform 2017 Update 3 Readme.* Industrial Software Solutions. [online]. Copyright © 2018 AVEVA Group plc and its subsidiaries. All rights reserved. [cit. 2021-01-08]. Dostupné z: https://industrial-software.com/wp-content/uploads/System-Platform-2017-Update-3-Readme.html

[17] *NISE 105-E3845 – Fanless Computer.* NEXCOME. [online]. Copyright © 2011 [cit. 2021-03-29]. Dostupné z: https://www.nexcom.com/Products/industrial-computing-solutions/industrial-fanless-computer/atom-compact/fanless-computer-nise-105-e3845

[18] *Remote Desktop Services roles.* Microsoft Docs. [online]. Copyright © Microsoft 2021 [cit. 2021-03-29]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-roles

[19] *Thin Client Software and Thin Client Management.* Automation Software | ThinManager ® [online]. Copyright © [cit. 2021-03-29]. Dostupné z: https://thinmanager.com/support/manuals/files/ThinManual.pdf

[20] *DAServer Manager User´s Guide.* Invensys Systems. [online]. Copyright © [cit. 2021-03-29]. Dostupné z: https://cdn.logic-control.com/media/DAServerManager.pdf

Přílohy

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

Studijní program: Systémové inženýrství a informatika
Forma studia: Kombinovaná
Obor/kombinace: Informační management (im3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Petr Hruška**
Osobní číslo:	**I1800662**
Adresa:	Jozífova 363, Opatovice nad Labem – Pohřebačka, 53345 Opatovice nad Labem, Česká republika
Téma práce:	Řešení pro centrální správu řídicích systémů Scada
Téma práce anglicky:	Central administration of Scada control systems
Vedoucí práce:	Mgr. Josef Horálek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je zmapovat, navrhnout a realizovat vhodné řešení využití tenkých klientů pro systémy řízení založených na Scada řešeních. V teroetické části práce autor zmapuje a popíše požadavky řídicí Scada systémů na komunikační a systémové zdroje. Na základě této analýzy představí možnosti řešení přechodu z desktop řešení na serverově řízenou správu a vybere technologicky, bezpečnostně a ekonomicky nejlepší řešení. V praktické části autor podrobně popíše a otestuje jeho implementaci a efektivitu.

Seznam doporučené literatury:

BODUNGEN, Clint E., Bryan L. SINGER, Aaron SHBEEB, Stephen HILT a Kyle WILHOIT. *Hacking exposed industrial control systems: ICS and SCADA security secrets & solutions*. New York: McGraw-Hill Education, [2017]. ISBN 9781259589713.
THOMAS, Orin. *Windows server 2016 inside out (includes current book service)*. Redmond, WA: Microsoft Press, 2016. ISBN 9781509302482.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: