Systém SCADA pro pokročilé monitorování průmyslových procesů

Veronika Gáčová

Fakulta strojního inženýrství, Vysoké učení technické v Brně
Ústav automatizace a informatiky
Technická 2896/2, Brno 616 69, Czech Republic
200534@vutbr.cz

Abstrakt: *Semimnární práce se zabývá popisem průmyslového systému SCADA, který zajišťuje pokročilé monitorování a centralizovanou kontrolu průmyslových procesů. Práce je koncipována jako literární rešerše a jejím cílem je seznámit čtenáře s průmyslovým systémem SCADA a jeho postavením z hlediska moderní průmyslové automatizace. V práci je dále uveden koncept automatizační pyramidy, rozebrána třívrstvá struktura systému SCADA a vzájemná komunikace jednotek dané struktury. Závěrem jsou shrnuty získané poznatky a vyvozen význam systému SCADA v rámci moderní průmyslové automatizace.*

Klíčová slova: *SCADA systém, automatizační pyramida, řízení procesů, PLC, RTU, monitorování, real-time systémy*

1 Úvod

Velká průmyslová zařízení a infrastruktury, jako jsou například chemické továrny, ropné rafinerie, ocelárny nebo elektrárny, jsou velmi závislé na automatických řídících systémech. Tyto systémy poskytují spolehlivý dohled a kontrolu nad každým procesem zapojeným do výroby. Nejrozšířenějším z nich je systém **SCADA** (Supervisory Control and Data Acquisition). [1, 2]
Jak název napovídá, jde o systém, který provádí supervizní kontrolu a sběr dat daného průmyslového procesu. Souhrnně představuje software, hardware a další postupy používáné k řízení a monitorování průmyslových procesů. Informace o průmyslovém procesu jsou poskytovány v reálném čase, kdy je možné prakticky okamžitě identifikovat problémy, které nastanou a přijmout nápravná opatření. Správné sledování procesu pomáhá udržovat průmyslové operace na optimální úrovni právě tím, že identifikuje a opravuje problémy dřív, než se promění ve významné selhání systému. [2]
V současné době nastává problém se zabezpečením těchto systémů, neboť se s postupným vývojem v oblasti výpočetní techniky tyto systémy staly pokročilejšími a složitějšími. Data v reálném čase v řídicích a monitorovacích systémech jsou přenášena přes intranet nebo dokonce internet, čím se systém stal zranitelnějším a méně bezpečným vůči potenciálním útokům. [1]

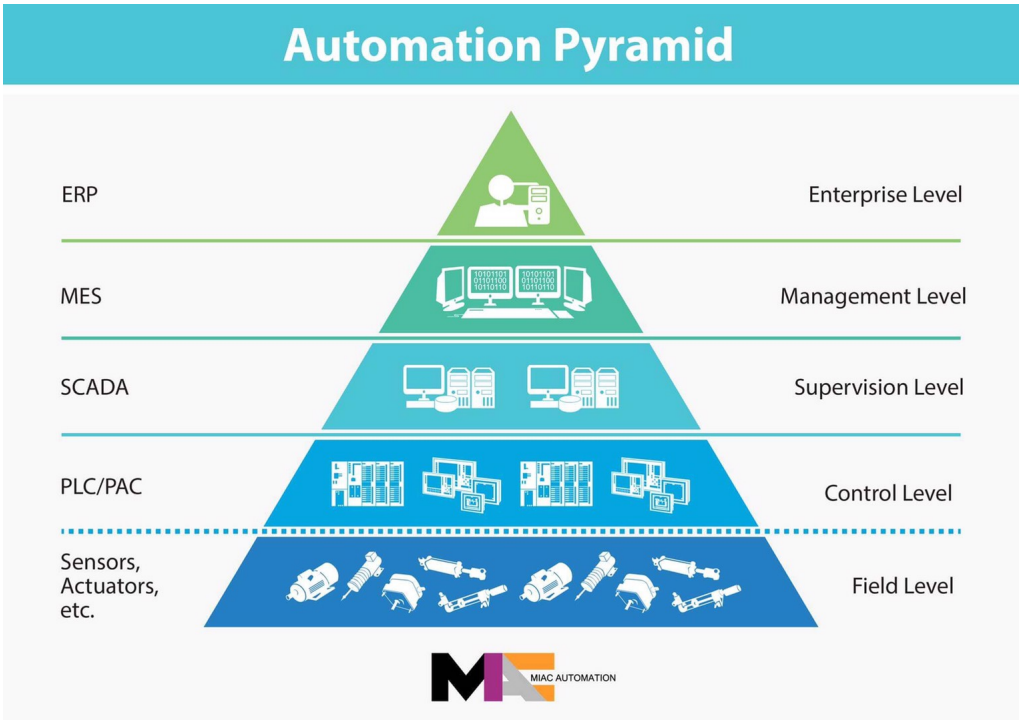
2 Formulace problému

Automatizační pyramida představuje architekturu řídícího systému v rámci automatizace procesní výroby. Skládá se celkem z pěti vrstev, jejichž vlastnosti a funkce jsou v práci vysvětleny. Struktura systému SCADA je složena primárně ze tří vrstev odpovídajících spodním vrstvám autamatizační pyramidy. Každá z vrstev má v rámci automatizačního procesu svoji funkci a obsahuje zařízení typická pro danou úroveň. Rozdělení funkcí jednotlivých vrstev je dáno postupným vývojem celého systému. Komunikace mezi jednotlivými vrstvami pracuje dnes již z velké části na open-source protokolech, což dělá systém více kompatibilním z hlediska vzájemného propojení zařízení od různých výrobců a usnadňuje tak integritu a řízení celého průmyslové procesu. Spolu s rychlým rozvojem vzrostl problém se zabezpečením systému. To je zapříčiněno především změnou struktury systému a jeho napojením do internetové sítě. [2, 3, 1]
Cílem této seminární práce je představit monitorovací a řídící systém SCADA, jeho strukturu a postavení v rámci automatizační pyramidy. Popsat komunikaci mezi jednotlivými zařízeními napříč vrstvami a nastínit aktuální problém se zabezpečení tohoto systému.

3 Řešení problému

3.1 Automatizační pyramida

Systém SCADA patří do třetí úrovně automatizační pyramidy, viz obr. 1. Tato vrstva představuje tzv. kontrolní stupeň, který provádí kontrolu a dohled nad jednotlivými procesy. Získává a kontroluje data z nižších dvou vrstev, které obsahují pro ně příslušná zařízení a nachází se obvykle na vzdálených místech v provozu. A dále přijímá informace z vyšších úrovní v souladu s produktivitou a požadovanými výkonnostními parametry. Pod ní se v pyramidě nachází úroveň provozní a řídící. Provozní vrstva zahrnuje základní fyzické vybavení nezbytné pro daný proces. Jsou jím například senzory, akční členy, měřidla apod. Řídící úroveň představuje první inteligentní úroveň automatizační pyramidy, neboť přijímá a zpracovává informace z provozní vrstvy. Využívá k tomu např. programovatelný logický automat (PLC) nebo vzdálenou terminálovou jednotku RTU (Remote Control Unit). [4]
Nadřazená čtvrtá a pátá úroveň, jsou úrovně plánovací a správní. Plánovací úroveň monitoruje kompletní proces v průmyslu od počátku (dodávky surovin) až po konečný krok (produkt). Využívá informace z předchozích z tří vrstev a zahrnuje je do procesu plánování. Nejvyšší, správní úroveň, potom propojuje veškeré monitorování a řízení všech činností oboru, jako jsou výrobní procesy, prodej, nákup nebo personální záležitosti. [4]



Obr. 1: Automatizační pyramida [5]

3.2 Třívrstvá struktura systému SCADA

SCADA systémy jsou v principu velmi rozdílné. Často se jedná o kombinaci specializovaných zařízení, jako jsou PLC (Programmable Logic Controllers) a tradičních systémů, jako jsou počítače se systémem Windows nebo Linux, které plní roli HMI (Human Machine Interface) pro účely vizualizace a interakce s operátorem. Obecně se SCADA systém skládá z operátorů (pracovníci), hlavní stanice MTU (Master Terminal Units), jednotek vzdáleného terminálu RTU a inteligentních elektronických zařízení IEDs (Intelligent Electronic Devices), kterými jsou například senzory, relé a řídící bloky. [6, 7, 8]

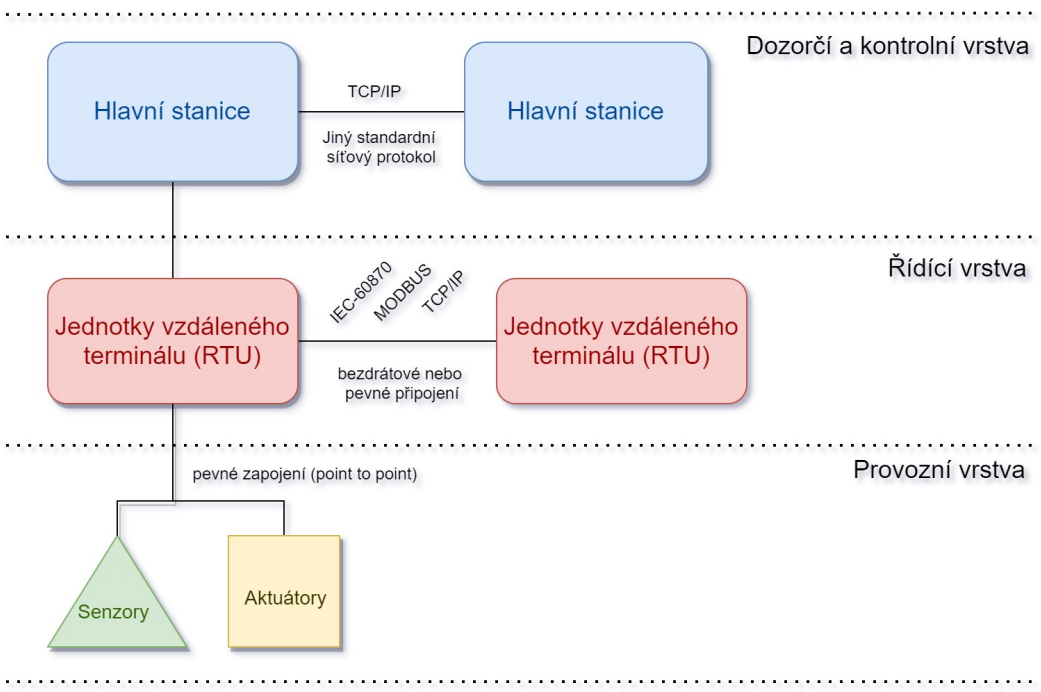
Na obr. 2 můžeme vidět obecnou **třívrstvou strukturu SCADA** systému, která odpovídá spodní části automatizační pyramidy. Vrchní úroveň kontroly a dozoru obsahuje dvě hlavní stanice, které mají funkci pravidělně získávat data v reálném čase a ovládat vzdálená zařízení z centralizované stanice. Hlavní stanice je složena z jednoho nebo více počítačů nakonfigurovaných pro její správnou funkci. Plnění povinností hlavní stanice představuje sledování trendu, alarm handling, protokolování a archivace, generování zpráv a celkové usnadnění automatizace. Tyto povinnosti mohou být distribuovány na více PC, a to buď samostatně, nebo v

síti. [2, 9]

Řídící vrstva se obvykle skládá z několika zařízení. Typickým zařízením je **programovatelný logický automat** (PLC), který představuje tzv. moderní RTU, využívající *ladder-logic programming*. PLC se rychle stávají standardem v řídicích systémech. Pokroky v CPU a programovací schopnosti RTU umožnily sofistikovanější monitorování a řízení. Aplikace, které byly dříve naprogramovány na centrální hlavní stanici, lze nyní programovat na takovémto RTU. [2, 9, 10]

V rámci PLC/RTU se v řídící vrstvě využívá různých **vstupních a výstupních modulů**. Jejich množství a typ je určen konfigurací senzorů, akčních členů, apod. V závislosti na výrobci a modelu mohou být moduly navrženy výhradně pro vstup nebo výstup. Dále rozdělujeme moduly digitální a analogové zpracovávající buď spojitý nebo diskrétní signál. **Analogový** vstupní modul má řadu rozhraní. Typické analogové vstupní/výstupní moduly mají 4, 8, 16 nebo 32 vstupů/výstupů. **Digitální** vstupní moduly se obvykle používají k indikaci stavu a výstražných signálů. Specializovaný digitální vstupní modul se používá k počítání pulzů napětí, spíše než k přímé indikaci "on" nebo "off". Tuto funkcionalitu však lze implementovat také pomocí standardních vstupních modulů a funkcí, které se nacházejí v programovacím jazyce ladder-logic PLC. [2, 9]

Provozní vrstva je složena především ze **senzorů a akčních členů**. Senzory provádějí měření a získávají tak potřebná data pro příslušný zásah akčních členů. Zpracování a určení toho, co je třeba udělat, provádí právě hlavní řídicí systém SCADA. [2]



Obr. 2: Třívrstvá SCADA struktura

3.3 Komunikace v rámci třívrstvé struktury

Systémy SCADA se vyvíjely souběžně s růstem a propracovaností moderní výpočetní technologie. Dříve měl každý výrobce jednotlivých technologií (PLC, průmyslových sítí, SCADA systémů, HMI) svůj vlastní standard průmyslové sběrnice, což byl problém z hlediska vzájemné komunikace přístrojů různých dodavatelů. Během 80. let byly vytvořeny standardy průmyslových sběrnic a dnes již celá třívrstvá architektura SCADA závisí spíše na open-source technologii než na proprietárním prostředí řízeném prodejcem. Tato architektura je vhodná, neboť na trhu existuje stále více výrobců průmyslových zařízení, kteřá mezi sebou potřebují vzájemně komunikovat. [2, 9, 3, 10] Obr. 2 zobrazuje typické způsoby komunikace v rámci SCADA systému.

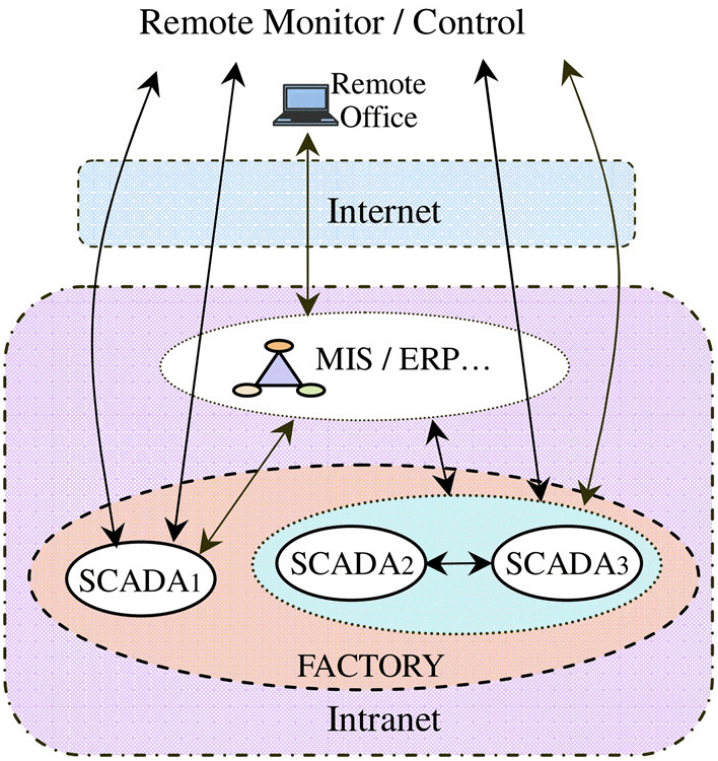
A) Komunikace mezi hlavními stanicemi
Existují možnosti využití proprietárních protokolů mezi hlavními stanicemi stejného výrobce nebo specifických SCADA open-source protokolů mezi stanicemi odlišných výrobců. V dozorčí a kontrolní vrstvě probíhá komunikace obvykle prostřednictvím standardního síťového protokolu, jako je TCP/IP nebo IPX přes Ethernet nebo Token Ring. SCADA aplikace se obvykle instalují na standardní PC systémy, které jsou schopné používat standardní protokoly poskytované operačním systémem. [2, 9]

B) Komunikace kontrolní a řídící vrstvy + komunikace v rámci řídící vrstvy
Dané prostředky komunikace se velmi liší a obvykle závisí na výrobci hardwaru. Pokud jsou RTU, senzory a akční členy od jednoho dodavatele, může být protokol proprietární. Nedávné trendy naznačují přechod na možnost použití open-source protokolů (Modbus, profibus, UCA) za účelem začlenění zařízení od různých výrobců. [2, 9]

C) Komunikace řídící vrstvou a provozní vsrtvou
Komunikace mezi řídící vrstvou a provozní vsrtvou je obvykle pevné "point to point" zapojení, které přenáší napěťové impulsy. Tyto impulsy pak RTU interpretuje na základě toho, jak je naprogramováno. Nedávné trendy v inteligentních senzorech a akčních členech umožňují jejich vzájemnou bezdrátovou komunikaci. Používané protokoly v rámci senzorů a akčních členů jsou Foundation Fieldbus a profibus-AS. [2, 9]

3.4 Zabezpečení systému SCADA

Systémy SCADA prošly za posledních několik let poměrně rychlým vývojem. První generace systémů nebyly propojeny s jinými systémy a počítačovými sítěmi. Řízený systém i jeho řídící jednotka byly umístěny na jednom místě a ovládány pracovníkem prostředníctvím HMI. Přístup k nim byl tak fyzicky zabezpečen v prostorách majitele. Druhá generace již fungovala v rámci celého podniku nebo společnosti. Sítě řídicího systému byly připojeny k podnikovým sítím Management Information System (MIS) a staly se součástí jejich intranetu. Dnešní, třetí generace systému SCADA je již integrována do systému Enterprise Resource Planning (ERP) Systémy jsou již plně integrovány do podnikových IT sítí, které jsou propojeny s internetem. [1] Architekturu takového systému můžeme vidět na obr. 3



Obr. 3: Architektura internetového a intranetového SCADA systému [1]

4 Závěr

Řídící systém zajišťuje v rámci moderní průmyslové automatizace centralizované real-timové řízení, což hraje důležitou roli především u složitých systémů, které musí být řízeny velice přesně a včas. Takovým příkladem je proces řízení jaderné elektrárny, kde jakékoliv pochybení nebo časové prodlení může způsobit nenávratné a nedozírné škody.

Systém SCADA představuje jednu z úrovní automatizační pyramidy. Systém přijímá požadavky z vyšších, plánovacích a správních, vrstev a zároveň snímá a zpracovává příslušné signály z vrstev nižších. Na základě požadavků nadřazených vrstev pak provádí rozhodnutí a řídí správný chod vrstev spodních a spolu s tím i celého průmyslového procesu. Třívrstvá struktura SCADA systému reprezentuje spodní část automatizační pyramidy. Hlavními složkami této struktury jsou hlavní stanice (MTU), jednotky vzdáleného terminálu (RTU) a komponenty patřící provozní vrstvy automatizační pyramidy, jako jsou senzory, měřidla a akční členy. Provozní vrstva je nejnižší úrovní pyramidy. Nad ní se nachází úroveň řídící, která obsahuje zařízení potřebná pro ovládání provozní vrstvy, kterým je například programovatelný logický automat PLC. Základem monitorovací a kontrolní vrstvy moderního SCADA systému jsou hlavní stanice. Jejich primární úlohou je pravidelné získávání potřebných dat v reálném čase a následné ovládání příslušných zařízení z jedné vzdálené centralizované řídící stanice.

Vzájemná komunikace v rámci SCADA systému je rozdílná v rámci jednotlivých vrstev. To je zapříčiněno především postupným a poměrně rychlým vývojem průmyslových SCADA systémů, které se při jejich postupném rozšiřování staly složitějšími a komplexními strukturami. SCADA systémy byly nejprve omezeny pouze lokálně, kdy ovládací a monitorovací systém byl umístěn přímo u systému řízeného. V rámci efektivní a integrované správy celého průmyslového procesu vzrostla potřeba ovládat z jednoho místa více zařízení zároveň. Z tohoto důvodu se systémy SCADA rozšířily nejprve v rámci firemních intranetů a později se staly součástí internetové sítě a internetu. Komunikace dnes již z velké části využívá open-source protokoly, aby bylo možné bez problémů propojit několik zařízení od různých výrobců.

Systém SCADA tedy výrazně zintegroval a zefektivnil řízení průmyslových procesů. Všechny systémy mohou být spravovány z jediného místa v reálném čase, což přináší nespornou výhodu v rychlém a účinném monitorování a řízení průmyslových procesů. Většina komunikací mezi jednotlivými zařízeními probíhá na open-source protokolech, což ještě více zjednodušuje ovládání celého systému. Používání open-source protokolů a důsledky rychlého vývoje SCADA systémů s sebou však nesou riziko internetových hrozeb, se kterými se sytémy již v současné době potýkají.

Použitá literatura

[1] Ning Cai, Jidong Wang, and Xinghuo Yu. *IEEE Xplore: SCADA system security: Complexity, history and new developments.* [online] URL: https://ieeexplore.ieee.org/document/4618165/, [cit. 25.3.2021].

[2] Mohamed Endi, Y. Z. Elhalwagy, and Attalla hashad. *IEEE Xplore: Three-layer PLC/SCADA system Architecture in process automation and data monitoring.* [online] URL: https://ieeexplore.ieee.org/abstract/document/5451799, [cit. 24.3.2021].

[3] Kenneth C. Wiberg. *NAVAL POSTGRADUATE SCHOOL MONTEREY CA: Identifying Supervisory Control and Data Acquisition (SCADA) Systems on a Network via Remote Reconnaissance.* [online] URL: https://apps.dtic.mil/sti/citations/ADA457371, [cit. 24.3.2021].

[4] J. A. López-Leyva, A. Talamantes-Álvarez, M. A. Ponce-Camacho, O. Meza-Arballo, B. Valadez-Rivera, and L. Casemiro-Oliveira. *The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0.* Springer International Publishing, 2019.

[5] *M.I.A.C. Automation Co., Ltd.* [online] URL: http://www.miac-automation.com/mes-oee-track-and-trace/, [cit. 24.3.2021].

[6] Naoum Sayegh, Imad H. Elhajj, Ayman Kayssi, and Ali Chehab. *IEEE Xplore: SCADA Intrusion Detection System based on temporal behavior of frequent patterns.* [online] URL: https://ieeexplore.ieee.org/abstract/document/6820573, [cit. 24.3.2021].

[7] G. P. H. Sandaruwan, P. S. Ranaweera, and Vladimir A. Oleshchuk. *IEEE Xplore: PLC security and critical infrastructure protection.* [online] URL: https://ieeexplore.ieee.org/abstract/document/6731959, [cit. 24.3.2021].

[8] Robert E. Johnson. *IEEE Xplore: Survey of SCADA security challenges and potential attack vectors.* [online] URL: https://ieeexplore.ieee.org/abstract/document/5678102, [cit. 24.3.2021].

[9] Michael P. Ward. *NAVAL POSTGRADUATE SCHOOL MONTEREY CA: An Architectural Framework for Describing Supervisory Control and Data Acquisition (SCADA) Systems.* [online] URL: https://apps.dtic.mil/sti/citations/ADA427541, [cit. 24.3.2021].

[10] Sebastian Dransfeld. *IEEE Xplore: Measurement and Supervision in Automated Production.* [online] URL: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/240600/123503$_F ULLTEXT01.pdf?sequence = 1, [cit.$24.3.2021].