

ANALÝZA VÝKONNOSTI PROCESNÝCH STANÍC VODNÝCH ELEKTRÁRNÍ PRI KOMUNIKÁCII PROTOKOLOM IEC 60870-5-104

Ing. Ondrej Štefánik

Slovenské elektrárne, a.s., závod Vodné elektrárne Trenčín

Ing. Rastislav Opatovský

Slovenské elektrárne, a.s., závod Vodné elektrárne Trenčín

ANNOTATION

This article deals with the analysis and optimization of communication in distributed control systems of hydropower plants, where communication is based on the IEC 60870-5-104 protocol. In Slovakia, hydropower plants are an important source of electricity, while Slovenské elektrárne, a.s., is the largest producer of electricity in the region, with a significant share of electricity production from water sources. The main goal of the work was the creation of a communication model and test software for process stations and operator stations based on the analysis of current communication problems between process stations of different manufacturers and SCADA/HMI systems.

As part of the work, the existing communication infrastructure was analyzed, the main problems such as communication breakdowns, loss of signals and congestion of the communication network were identified. Process stations from ABB and Siemens together with the operator station OS1 were the main focuses of the analysis. The IEC 60870-5 standard has been studied in detail, especially its fifth part concerning transmission protocols for remote control, which are crucial for effective communication in power distribution systems.

To eliminate the identified problems, a test platform was designed and implemented, created in the programming environment ABB's Automation Builder and CoDeSys, specialized in PLC programming. The testing approach included hardware and software configuration, communication setup according to the IEC 60870-5-104 standard, and communication packet definition and testing. The article describes in detail the process of creating test software, from the configuration of the environment to the implementation of test scenarios on simulation hardware in laboratory conditions.

The result was a successful testing of communication between process stations and the detection of weak points in the existing configuration. Based on these tests, measures were proposed and recommended to improve communication efficiency and reliability, including optimization of communication protocol settings.

This work thus represents a significant contribution to improving the management and operation of hydropower plants in Slovakia, provides a basis for further research and development in the field of communication technologies for energy systems and offers specific solutions for improving the performance and reliability of communication in distributed control systems.

KĽÚČOVÉ SLOVÁ

IEC 60870-5-104, ABB AC500, Siemens SICAM AK3, vodné elektrárne, riadiaci systém, testovací softvér, komunikačné protokoly.

1. ÚVOD

V súčasnom svete, kde technológia a inovácie neustále posúvajú hranice možného, sa stáva komunikácia medzi zariadeniami a systémami kľúčovým prvkom v mnohých odvetviach, vrátane energetiky. Význam efektívnej a spoľahlivej komunikácie v energetických systémoch, najmä v kontexte vodných elektrární, sa stáva čoraz viac zrejmým vzhľadom na rastúcu potrebu integrácie obnoviteľných zdrojov energie a zvyšovanie efektivity výroby elektrickej energie. Tento článok sa zameriava na hĺbkovú analýzu výkonnosti procesných staníc vodných elektrární pri komunikácii protokolom IEC 60870-5-104, s cieľom identifikovať a odstrániť existujúce komunikačné problémy a navrhnúť riešenia na zlepšenie celkovej efektivity a spoľahlivosti týchto systémov.

Vodné elektrárne hrajú nezastupiteľnú úlohu v energetickom mixe mnohých krajín vrátane Slovenska, kde predstavujú významný podiel na celkovej výrobe elektrickej energie. Efektívne riadenie a prevádzka týchto zariadení vyžaduje vysoko spoľahlivé a efektívne komunikačné systémy, ktoré umožňujú prenos dát medzi jednotlivými komponentmi riadiaceho systému a centrálnym dispečingom. Protokol IEC 60870-5-104, ako medzinárodný štandard pre diaľkovú kontrolu a dohľad nad elektrickými distribučnými sieťami, predstavuje základ pre komunikáciu v týchto systémoch. Napriek jeho rozšírenému využitiu však prax ukazuje, že existujú významné výzvy a problémy spojené s jeho implementáciou a výkonnosťou v konkrétnych aplikáciách. Komunikačné systémy, musia byť dostatočne flexibilné a adaptabilné, aby zabezpečili efektívnu prevádzku a riadenie. V tejto súvislosti sa článok zameriava na analýzu súčasných komunikačných problémov, ktoré sa vyskytujú medzi procesnými stanicami rôznych výrobcov, ako sú ABB a Siemens, a operátorskou stanicou SCADA/HMI. Hlavným cieľom je identifikovať kľúčové faktory ovplyvňujúce výkonnosť a spoľahlivosť týchto komunikačných systémov a na základe získaných poznatkov navrhnúť efektívne riešenia pre odstránenie identifikovaných problémov.

2. Metodika a spôsob analýzy

Pri analýze súčasných komunikačných systémov a identifikácii problémov sme sa opierali o dostupnú literatúru, ktorá zahŕňa vedecké články, technické správy a štandardy súvisiace s protokolom IEC 60870-5-104. Relevantné zdroje boli vyhľadávané v databázach ako IEEE Xplore, ScienceDirect a Google Scholar. Taktiež boli použité interné dokumenty firmy a technické špecifikácie poskytované výrobcami zariadení ako ABB a Siemens. Na analýzu komunikačných problémov sme využili sw nástroje na zachytávanie a analýzu sieťovej komunikácie, ako je Wireshark a Sicam Toolbox DataFlowTest. Simulácie a testovanie rôznych konfigurácií a nastavení boli realizované pomocou vývojového prostredia Automation Builder a programovacieho jazyka CoDeSys v prípade zariadení ABB a Sicam Toolbox v prípade Siemens zariadení. Testovacie scenáre zahŕňali komunikáciu medzi procesnými stanicami a operátorskou stanicou, pričom sme sledovali zaťaženie CPU, rýchlosť prenosu dát a výpadky v komunikácii. Okrem toho sme vyvinuli vlastný testovací softvér na automatizované testovanie komunikácie medzi procesnými stanicami a operátorskou stanicou. Tento softvér umožňuje simulovať rôzne scenáre a testovať výkonnosť komunikačných systémov v kontrolovanom prostredí pred ich implementáciou v reálnych podmienkach.

3. Výsledky

Prehľad aktuálnych problémov:

Pri komunikácii procesných staníc a operátorskej stanice (OS1/SCADA) sme identifikovali niekoľko komunikačných problémov:

- Výpadky kom. medzi proc. stanicami ABB AC500 a oper. stanicou (OS1/SCADA)
- Strata posielaných signálov
- Zahľtenie komunikácie

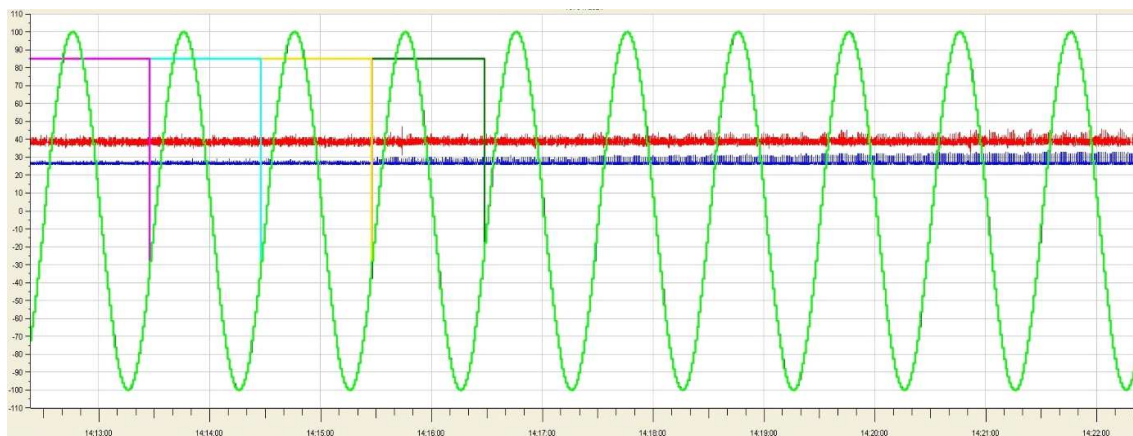
Analýza komunikačných systémov:

Prostredníctvom nástroja Wireshark sme analyzovali sieťovú komunikáciu a identifikovali, že stanica ABB odosiela jednotlivé signály jednotlivo, zatiaľ čo stanica Siemens Sicam AK3 ich agreguje do skupín a odosiela v balíkoch. Ďalšia analýza softvéru v stanici ABB AC500 ukázala, že komunikácia prebieha prostredníctvom systémových funkčných blokov, ktoré je potrebné naplniť požadovaným signálom. Po dôkladnej analýze dostupných algoritmov a funkčných blokov sme identifikovali bloky, ktoré umožňujú skupinové odosielanie signálov po 16, namiesto jednotlivého odosielania. Na základe uvedenej analýzy sme navrhli a implementovali testovací softvér, ktorého cieľom bolo overiť funkčnosť týchto 16-vstupových blokov a porovnať efektívnosť komunikácie oproti softvéru založenom na 1-vstupových blokoch.

Testovanie komunikačných nastavení:

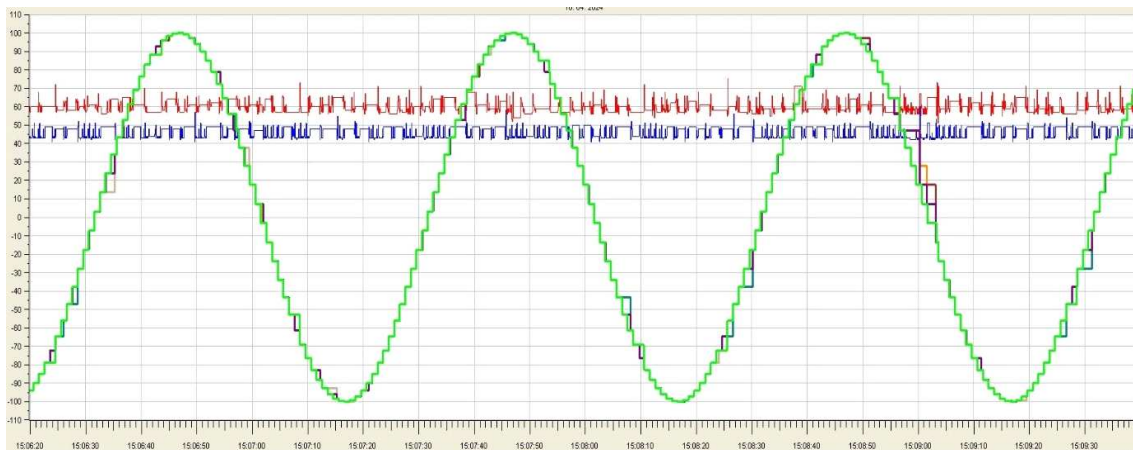
Testovanie sme realizovali pomocou vytvoreného testovacieho softvéru, ktorý umožňuje automatizované testovanie komunikácie medzi procesnými stanicami a operátorskou stanicou. Na základe výsledkov testovania sme zistili, že použitie 1-vstupových blokov na odosielanie signálov v staniaciach ABB nie je efektívne a vedie k oneskoreniam signálov. Navrhli sme nahradenie 1-vstupových blokov 16-vstupovými blokmi, čo výrazne zlepšilo komunikačné procesy, znížilo zaťaženie CPU a minimalizovalo oneskorenia.

Testovanie sme začali odosielaním jedného signálu za sekundu medzi dvoma stanicami ABB. Odosielajúca stanica súčasne prenášala signály aj na operátorskú stanicu, a podobne aj prijímacia stanica odoslala prijaté signály na operátorskú stanicu. Na operátorskej stanici sme pomocou SCADA systému monitorovali zaťaženie a oneskorenie komunikácie, ktoré sme vizualizovali prostredníctvom grafov. Postupným zvyšovaním počtu signálov sme analyzovali, pri akej počte posielaných signálov začne dochádzať k výpadkom odosielania resp. prijímania signálov.



Obr.1 Graf odosielania signálov od 1 po 10 za sekundu

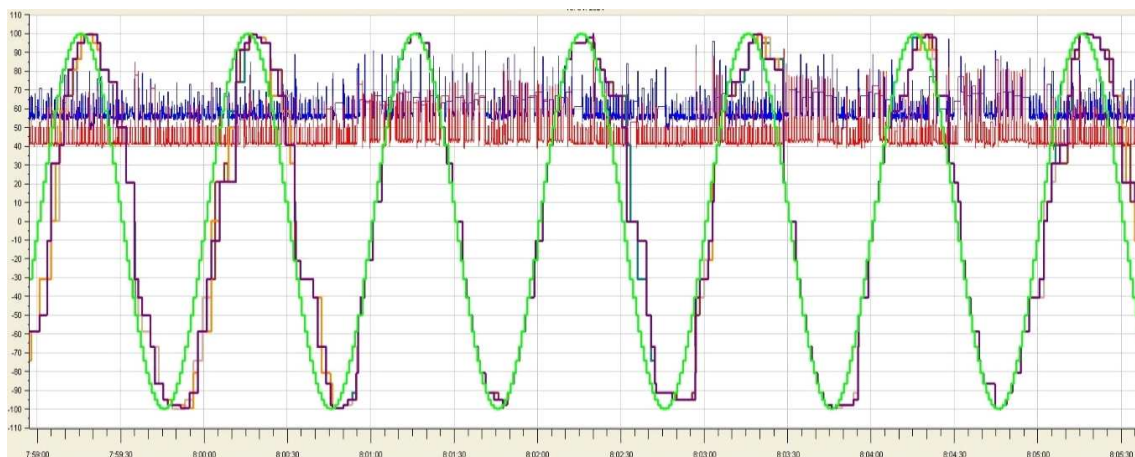
Prvé výrazné oneskorenia v komunikácii sa objavili, keď sme dosiahli úroveň 12 signálov za sekundu. Na grafe si môžeme všimnúť, že už pri zaťažení procesora odosielaajúcej stanice od 59% do 69% a prijímajúcej stanice od 42% do 50%, dochádza k oneskoreniam resp. výpadkom odosielaania signálov. Pri dôslednom skúmaní sme prišli na to, že „nahromadené“, signály ktoré sa nestihnú v rámci stanice spracovať resp. odoslať sa zahodia a odošlú sa len novšie signály (farebné skoky v grafoch na sínusoide).



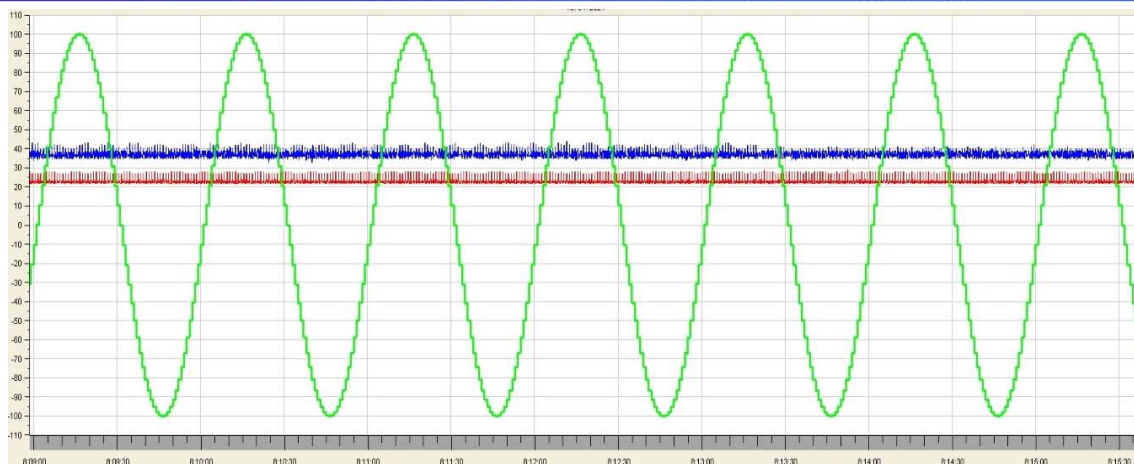
Obr.2 Graf odosielaania 12 signálov za sekundu

Okrem zvyšovania frekvencie odosielaaných signálov sme experimentovali aj so spôsobmi ich zoskupovania. V jednom prípade sme odosielaali každý signál individuálne, zatiaľ čo v druhom prípade sme odosielaali signály v skupinách po šiestnástich. Tento test mal za cieľ zistiť, ako rozdielne metódy odosielaania ovplyvňujú výkon komunikácie.

Začali sme odosielaaním signálov prostredníctvom jednovstupových blokov a následne sme ich porovnávali s použitím šestnást'vstupových blokov. Už z grafov je na prvý pohľad vidieť, ako sa komunikácia zlepšila po použití šestnást'vstupových blokov. Prekvapujúce je, že aj keď sme odosielaali až 50 signálov za sekundu, komunikácia prebiehala bez výrazných oneskorení a systém nebol preťažený. Navyše, táto metóda odosielaania značne znižovala zaťaženie CPU na odosielaajúcej aj prijímajúcej stanici. Podľa grafu bol rozsah zaťaženia CPU pri použití jednovstupových blokov medzi 43% až 90%, zatiaľ čo pri použití šestnást'vstupových blokov bol rozsah zaťaženia CPU znížený na 23% až 45%. Z toho vyplýva, že použitie šestnást'vstupových blokov má výrazný vplyv na zlepšenie komunikácie a zefektívnenie komunikačných procesov.



Obr.3 Graf odosielaania signálov 1-stupovými blokmi – rýchlosť 50 signálov/s.



Obr.4 Graf odosielania signálov 16-stupovými blokmi – rýchlosť 50 signálov/s.

4. ZÁVER

Testovaním sme dospeli k výsledku, že použitie 1-vstupových blokov na odosielanie (nepovelových) signálov v staniciach ABB nie je efektívne a v dôsledku ich použitia dochádza k výpadkom odosielania signálov už pri relatívne malom počte. V reálnej praxi bol tento problém identifikovaný napr. v súvislosti so zaznamenávaním meraných el. veličín do archívu čo môže následne skomplikovať ďalšie procesy napr. predcertifikácia podporných služieb a pod. kde bude chýbať potrebná spojitosť zaznamenávaných údajov.

Na základe týchto zistení sme navrhli vyriešiť komunikačné problémy nahradením 1-vstupových blokov 16-vstupovými blokmi. Toto riešenie výrazne odľahčí zaťaženie procesora procesnej stanice ako i umožní odosielanie veľkého množstva signálov bez výpadkov odosielaných dát.

Na druhú stranu, nevýhodou použitia 16-vstupových blokov je to, že príznaky signálov (napr. not topical, invalid, overflow a pod.) je možné nastaviť resp. odoslať iba pre všetkých 16 signálov spolu. V 1-vstupových blokoch má každý signál svoj príznak. Riešením by mohlo byť zgrupovanie signálov do 16-vstupových blokov na základe spoločných parametrov, ako napríklad to, keď sú na spoločnej hw línii. Výpadok línie znamená zneplatnenie všetkých signálov, ktoré sú do nej pripojené. Dôležité signály ako napríklad výkon turbogenerátora zostanú posielané 1-vstupovými blokmi, aby sa zabezpečilo správne sledovanie ich príznakov.

Uvedené zistenie nám pomôžu pri optimalizácii a návrhu nových riadiacich systémov ako a zároveň otvárajú cestu pre ďalšie výskumné aktivity v oblasti riadiacich systémov a komunikačných technológií. Tieto poznatky a odporúčania môžu slúžiť ako cenný príspevok pre technické a sw tímy v rámci energetických spoločností.

5. LITERATÚRA

- [1] Slovenské elektrárne - O nás [online]. www.seas.sk, [cit. 2023-12-07]
- [2] Slovenské elektrárne - Vodné elektrárne [online]. www.seas.sk, [cit. 2023-12-07]
- [3] V. Muthukrishnan, *Programmable Logic Controllers (PLCs): Basics, Types & Applications*. electrical4u (2021)
- [4] Q. Shengbo, L. Jiangchao, Z. Jing, B. Xuesong and F. Lili, "An upper monitor system design for security packet processing testing based on IEC 60870-5-104," 2023 IEEE

- 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), Shenyang, China, 2023, pp. 378-381*
- [5] P. Ilgner, R. Fujdiak, in *ACM International Conference Proceeding Series (Association for Computing Machinery, 2022)*, pp. 190–194
 - [6] ANSARI, Shoaib, et al. *Testing IEC 60870-5-104 and C37. 118 based control center applications using a real time simulation platform. In: Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MEDPOWER 2018). IET, 2018. p. 1-5.*
 - [7] RADOGLUO-GRAMMATIKIS, Panagiotis, et al. *Attacking iec-60870-5-104 scada systems. In: 2019 IEEE World Congress on Services (SERVICES). IEEE, 2019. p. 41-46.*
 - [8] M. Petr, *Description and analysis of IEC 104 Protocol. Faculty Inf. Technol., 38 (2017)*
 - [9] N. Liu, B. Duan, *Discussion on security message of IEC 60870-5-104 telecontrol protocol. Dianli Xitong Zidonghua/Automation of Electric Power Systems. 29, 93–96 (2005)*
 - [10] LIN, Chih-Yuan; NADJM-TEHRANI, Simin. *Understanding IEC-60870-5-104 traffic patterns in SCADA networks. In: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security. 2018. p. 51-60.*
 - [11] GRIGORIOU, Elisavet, et al. *Protecting IEC 60870-5-104 ICS/SCADA systems with honeypots. In: 2022 IEEE international conference on cyber security and resilience (CSR). IEEE, 2022. p. 345-350.*
 - [12] MATOUŠEK, Petr. *Description and analysis of IEC 104 Protocol. Faculty of Information Technology, Brno University o Technology, Tech. Rep, 2017.*
 - [13] ABB. (2024). *Getting started with AC500 V2 products. [online]. https://library.e.abb.com/public/fa58c86b1eb943c7bc11b67b0d1dbc49/Getting_Started_AC500_V2,%205,%20en_US.pdf, [cit. 2024-02-15]*
 - [14] ABB. (2024). *PLC Automation System Manual. [online]. <https://search.abb.com/library/Download.aspx?DocumentID=3ADR011074&LanguageCode=en&DocumentPartId=&Action=Launch>, [cit. 2024-02-15]*
 - [15] POPOVICI, Diana; POPOVICI, Ovidiu. *A Study Regarding the Configuration of Tasks at ABB PLCs Programming. Journal of Computer Science & Control Systems, 2010, 3.1.*
 - [16] Smart Software Solutions GmbH. (2007). *User Manual for PLC Programming with CoDeSys.[online]. <https://library.e.abb.com/public/08057e49639db3dfc1257c210040dd77/2CDC125019M0202.pdf>, [cit. 2024-02-15]*

- [17] POPOVICI, Diana; POPOVICI, Ovidiu. *A Study Regarding the Configuration of Tasks at ABB PLCs Programming. Journal of Computer Science & Control Systems*, 2010, 3.1.
- [18] SICAM RTUs, SICAM AK 3 User Manual
- [19] NDATINYA, Vivens, et al. *Network forensics analysis using Wireshark. International Journal of Security and Networks*, 2015, 10.2: 91-106
- [20] SUCHARDA, Michael. *Nástroje pro testování protokolu IEC-104 pro automatizaci distribučních sítí. Bakalárska práca. Liberec: Technická univerzita v Liberci, 2016*