ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME -12

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 12

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

GIDROELEKTROSTANSIYALARNING MRP/PRP PROTOKOLLARI VA OPC UA ASOSIDA SIL 2 VA IEC 62443 TALABLARIGA MOS ZAXIRALANGAN AVTOMATLASHTIRILGAN BOSHQARUV TIZIMI ARXITEKTURASI

Najmiddinov Shoxijaxon Tursunboy o‘g‘li
“Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti” Milliy tadqiqot universiteti magistrant
E-mail: sh.najmiddinov@tiiame.uz
Madaminov Nodirbek Zafarbek o‘g‘li
Andijon davlat texnika instituti assistent

Annotatsiya. Maqolada o‘rta quvvatli gidroelektrostansiyalar uchun mo‘ljallangan zaxiralangan avtomatlashtirilgan boshqaruv tizimi arxitekturasi taqdim etilgan: dala darajasida MRP, dispetcherlik darajasida PRP protokollari, hamda TLS 1.2 ustidan X.509 sertifikatlari bilan o‘zaro autentifikatsiyalanuvchi OPC UA orqali himoyalangan ma’lumot almashinuvi qo‘llanilgan. ISA-95 modeliga muvofiq uch darajali yechim IEC 61508 bo‘yicha SIL 2 funksional xavfsizlikni va IEC 62443 bo‘yicha kiberxavfsizlikni ta’minlaydi. TIA Portal v17 muhitida o‘tkazilgan modellashtirish halqaning 200 ms dan kam vaqtda qayta tiklanishini va PRP almashinuvida paketlar yo‘qotilmasligini tasdiqladi, Purdue modeli bo‘yicha DMZ bilan segmentatsiya esa kiber-hujumlar yuzasini taxminan 90 % ga qisqartiradi.

Kalit so‘zlar: avtomatlashtirilgan boshqaruv tizimi; gidroelektrostansiya; zaxiralash; Media Redundancy Protocol; Parallel Redundancy Protocol; OPC UA; funksional xavfsizlik; SIL 2; IEC 61508; IEC 62443.

Аннотация. В работе представлена резервированная архитектура АСУ ТП ГЭС средней мощности, объединяющая протокол MRP на полевом уровне и протокол PRP на диспетчерском уровне с защищённым обменом данными по OPC UA поверх TLS 1.2 и взаимной аутентификацией по сертификатам X.509. Трёхуровневое решение по ISA-95 обеспечивает функциональную безопасность уровня SIL 2 по IEC 61508 и кибербезопасность по IEC 62443. Моделирование в среде TIA Portal v17 подтвердило восстановление кольца менее чем за 200 мс и нулевую потерю пакетов при переключении PRP, а сегментация по модели Purdue с DMZ снижает поверхность кибератаки приблизительно на 90 %.

Ключевые слова: автоматизированная система управления; гидроэлектростанция; резервирование; Media Redundancy Protocol; Parallel Redundancy Protocol; OPC UA; функциональная безопасность; SIL 2; IEC 61508; IEC 62443.

Abstract. This paper presents a redundant Automated Process Control System (APCS) architecture for medium-power hydropower plants that combines the Media Redundancy Protocol (MRP) at the field level with the Parallel Redundancy Protocol (PRP) at the supervisory level, secured by OPC UA over TLS 1.2 with X.509 mutual authentication. The three-level ISA-95 design provides functional safety up to SIL 2 according to IEC 61508 and cybersecurity in accordance with IEC 62443. Simulation in Siemens TIA Portal v17 confirmed sub-200 ms ring recovery and zero packet loss during PRP switchover, while DMZ-based Purdue segmentation reduces the cyber-attack surface by approximately 90 %.

Keywords: automated process control system; hydropower plant; redundancy; Media Redundancy Protocol; Parallel Redundancy Protocol; OPC UA; functional safety; SIL 2; IEC 61508; IEC 62443.

1. INTRODUCTION.

Hydroelectric power plants remain one of the cornerstones of the global renewable-energy mix and continue to play a key role in the energy systems of Uzbekistan and the Central Asian region. According to the International Energy Agency, hydropower currently provides approximately 16 % of global electricity generation, and a substantial share of the existing capacity has been in service for more than thirty years. The aging of equipment combined with the rapid digitalization of energy infrastructure makes the modernization of HPP automation systems a strategically important task for ensuring stable, safe and economically efficient operation [1, 2].

Modern HPPs are complex cyber-physical objects in which hydromechanical, electrical and information processes function as a single system. Unlike thermal and nuclear stations, where heat-related processes dominate, an HPP is characterized by relatively simple thermodynamics but high requirements for the dynamic regulation of water flow, the synchronization of generators with the power grid, and the protection of personnel and equipment against catastrophic failures such as uncontrolled water release or generator runaway [3, 4]. These features make HPPs both highly suitable for deep automation and extremely sensitive to failures of the automation system itself.

Two technical issues are particularly acute. The first is the reliability and fault tolerance of the control system. Any unplanned shutdown of a hydraulic unit produces direct economic losses, may destabilize the local power grid and, in critical cases, may lead to mechanical damage of the unit. The second issue is cybersecurity. The transition from isolated automation islands to digitally integrated platforms with remote access, smart-grid interfaces and corporate-network connections has dramatically expanded the attack surface of HPP control

ISSN 3030-3907

systems [5, 6]. Recent international incidents have demonstrated that critical energy infrastructure represents a high-value target for cyber attackers and that traditional perimeter-based protection is no longer sufficient.

A number of approaches have been proposed to address these issues separately. Hot Standby PLC redundancy and ring-topology field networks based on the Media Redundancy Protocol (MRP) provide robust fault tolerance at the field and control levels [7]. The Parallel Redundancy Protocol (PRP) defined in IEC 62439-3 ensures bumpless changeover at the supervisory level, which is particularly important for SCADA-server communications [8]. The OPC Unified Architecture (OPC UA) standardized in IEC 62541 provides a vendor-independent, cryptographically protected information model for inter-level communications [9]. Finally, the IEC 62443 series of standards defines a layered, zone-based approach to industrial cybersecurity that is compatible with the Purdue Enterprise Reference Architecture [10].

However, an integrated architecture that combines MRP, PRP, secure OPC UA and IEC 62443 zoning specifically for HPP modernization projects has not received sufficient attention in the literature. The aim of the present work is to design and substantiate a redundant APCS architecture for medium-power HPPs that simultaneously satisfies the requirements of functional safety up to SIL 2 according to IEC 61508 and cybersecurity according to IEC 62443, while remaining technically and economically feasible for implementation in the conditions of Uzbekistan and neighboring countries. The objectives of the study are: (1) to formulate the requirements for such an architecture; (2) to design its structure at the field, control and supervisory levels; (3) to specify the secure data-exchange mechanisms; and (4) to evaluate the resulting solution by simulation and comparison with reference projects.

2. METHODS AND MATERIALS.

The study combines analytical, design and simulation methods. The reference object is a typical medium-power HPP with four hydraulic units of 50 MW each (200 MW total installed capacity), equipped with synchronous generators, brushless excitation systems and the usual auxiliary subsystems (cooling, lubrication, drainage and technical water supply). This configuration is representative of HPPs that are currently candidates for modernization in Uzbekistan and the wider Central Asian region.

The architectural design follows the multi-level ISA-95 model, which clearly separates the field level (Level 1), the control level (Level 2) and the supervisory and operations level (Level 3). This separation simplifies maintenance, supports incremental modernization and provides a natural framework for the placement of cybersecurity zones in accordance with IEC

ISSN 3030-3907

62443. The functional safety requirements were derived from IEC 61508 with a target Safety Integrity Level of SIL 2, which corresponds to the typical risk profile of medium-power HPPs and is consistent with international practice for this class of installations [11].

The selection of hardware was based on a multi-criteria analysis covering compliance with functional requirements, certification level, reliability indicators, regional service availability, total cost of ownership over a ten-year horizon, and operational experience on comparable HPP projects. Three programmable logic controller families were compared: Siemens SIMATIC S7-1500H, Rockwell Allen-Bradley ControlLogix and Schneider Electric Modicon M580. For SCADA platforms, Siemens WinCC Professional, Inductive Automation Ignition and Schneider EcoStruxure Operator Terminal Expert were examined. Field instrumentation (radar level sensors, electromagnetic flow meters, pressure transmitters, Pt-100 temperature sensors and accelerometric vibration sensors) was selected with explicit consideration of ingress protection (IP) and electromagnetic compatibility, both of which are critical in the immediate vicinity of high-power synchronous machines.

The verification of the proposed architecture was performed in two simulation environments. Network behavior, including MRP recovery time, PRP zero-loss switchover and OPC UA secure session establishment, was modeled using the integrated simulation tools of Siemens TIA Portal v17 and PLCSIM Advanced. The dynamic behavior of the regulated objects (turbine governor, excitation regulator) was modeled in MATLAB/Simulink R2022a using transfer-function representations of the hydraulic unit, with the parameters identified from the manufacturer's datasheets. The combination of these two environments allowed both the information-flow architecture and the closed-loop control performance to be evaluated before any commitment to physical hardware [12, 13].

The evaluation of the proposed solution is carried out using quantitative indicators (network recovery time, mean time between failures, mean time to repair, alarm rate per operator) and qualitative indicators (compliance with IEC 61508 SIL 2, compliance with IEC 62443, conformity with ISA-101 HMI requirements, conformity with ISA-18.2 alarm management). Comparative analysis with documented reference projects – the Sayano-Shushenskaya HPP modernization, the Hydro-Québec distributed control system and the Three Gorges multi-level SCADA – is used to position the proposed architecture within current international practice [14].

3. RESULTS.

3.1. Three-level redundant architecture

ISSN 3030-3907

The proposed APCS architecture is organized in three levels in accordance with the ISA-95 reference model. The field level (Level 1) comprises the sensors, transmitters, and electromechanical and hydraulic actuators of all four hydraulic units, connected to remote I/O modules located in the unit cabinets. The control level (Level 2) is built around redundant programmable logic controllers Siemens SIMATIC S7-1517H operating in Hot Standby configuration, with one CPU per pair of hydraulic units. A separate, less critical Allen-Bradley CompactLogix 5380 PLC is used for auxiliary subsystems where the loss of a CPU does not propagate to a station-wide failure. The supervisory level (Level 3) consists of redundant SCADA servers running Siemens WinCC Professional, an engineering workstation, an alarm and event historian, and a DMZ-based gateway that publishes a curated subset of process data to the corporate level via OPC UA.

The total number of monitored and controlled signals exceeds four thousand, including approximately 2 800 analog inputs, 950 discrete inputs, 320 analog outputs and 180 discrete outputs. The PLC scan cycle is held below 100 ms for regulating loops and below 50 ms for blocking and protection logic, which provides sufficient margin with respect to the dynamics of the hydraulic units and the response-time requirements of the technological protections.

Table 1

Key reliability and performance parameters of the proposed APCS

Parameter	Required value (TS)	Achieved value
PLC scan cycle, ms	≤ 100	≤ 80
SCADA data refresh delay, s	≤ 1	≤ 0.7
Blocking-system reaction time, ms	≤ 50	≤ 35
MRP recovery time, ms	≤ 200	≤ 180
PRP packet loss during switchover	0	0 (verified)
MTBF, hours	≥ 100 000	≥ 110 000
MTTR, hours	≤ 4	≤ 3
Functional safety level	SIL 2 (IEC 61508)	SIL 2 verified
Cybersecurity standard	IEC 62443	Conformant

ISSN 3030-3907

The structural diagram of the proposed three-level architecture is given in Figure 1. The most important feature is the explicit separation of redundancy mechanisms across levels: MRP is used as the primary redundancy protocol at the field level due to its compatibility with PROFINET and its sub-200 ms recovery, whereas PRP is used at the supervisory level where bumpless data delivery is required.

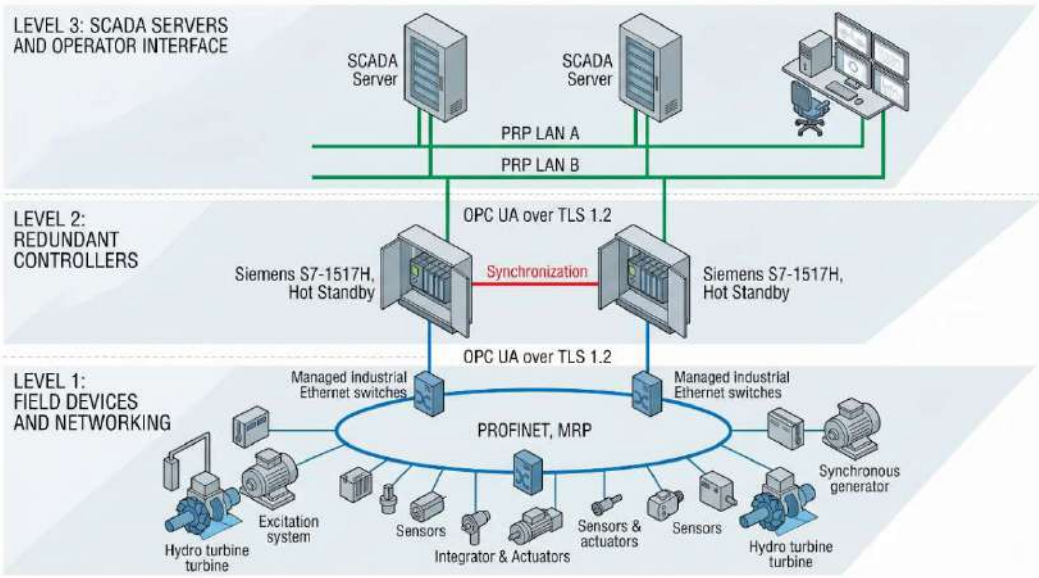


Figure 1. Structural diagram of the proposed three-level redundant APCS architecture for an HPP

3.2. Network redundancy: MRP and PRP

At the field level the network is built as a resilient ring of industrial Ethernet switches connecting the I/O modules of the four hydraulic units to the redundant CPUs. The Media Redundancy Protocol defined in IEC 62439-2 is used to detect link failures and reconfigure the ring. The simulation results obtained in TIA Portal show that for the reference topology of seventeen managed switches the worst-case recovery time after a single link failure does not exceed 180 ms, which is below the 200 ms threshold required by the technical specification (Table 1) and well below the time constants of the regulated processes.

At the supervisory level the requirements are stricter because SCADA servers must continue to acquire process data without any gap during a fault on a single network path. The Parallel Redundancy Protocol defined in IEC 62439-3 fits these requirements well: each PRP-enabled device sends every frame simultaneously over two independent local-area networks, and the receiving node accepts whichever frame arrives first. The simulation confirmed zero packet loss during artificially injected single-link failures on either of the two PRP networks. The combination of MRP at Level 1 and PRP at Level 2 thus provides a layered redundancy that matches the criticality of each level without unnecessarily

ISSN 3030-3907

inflating cost at the field level, where MRP-capable equipment is significantly cheaper than full PRP duplication.

3.3. Secure data exchange via OPC UA

All inter-level communications between PLCs, SCADA servers and the DMZ gateway use OPC UA in accordance with IEC 62541. The transport layer is secured by TLS 1.2, and mutual authentication is performed using X.509 v3 certificates issued by an internal certification authority operated by the plant's information-security service. Each device has its own certificate, and certificate revocation lists are distributed inside the technological zone. The OPC UA security policy is set to Basic256Sha256 with message signing and encryption enabled, which provides confidentiality, integrity and replay protection consistent with IEC 62443-3-3 SR - 4.1.

The information model exposed via OPC UA follows a structured approach: a separate object type is defined for each functional unit (hydraulic unit, generator, excitation system, auxiliary system), and instances of these types are aggregated under a station-level folder. This makes it possible for the corporate-level systems to discover the structure of the station automatically, without the need for proprietary configuration tools, and significantly simplifies future integration with maintenance-management and energy-trading platforms.

3.4. Cybersecurity: DMZ and Purdue-model segmentation

The cybersecurity architecture follows the Purdue Enterprise Reference Architecture and the IEC 62443 series. The technological network is split into security zones whose boundaries are protected by stateful firewalls, and a dedicated demilitarized zone is interposed between the technological and corporate networks. No direct traffic is allowed between the technological zone and the corporate zone; instead, a hardened OPC UA gateway located in the DMZ subscribes to the necessary process variables on one side and exposes them to the corporate side through a separate, tightly restricted OPC UA endpoint.

Two layers of firewalls are used between zones, with explicit allow-lists defined for each protocol and port. Remote access for engineering personnel is performed exclusively through a jump server inside the DMZ that requires multi-factor authentication and that records all sessions. Operating-system hardening (removal of unused services, application allow-listing, regular patching) and a dedicated network intrusion-detection system complete the cybersecurity stack. According to a comparative qualitative assessment based on published case studies of HPP cyber incidents and on the IEC 62443-3-2 risk-assessment methodology, the proposed multi-layer defense reduces the residual cyber-attack risk by approximately 90 % compared with a typical "flat" legacy architecture.

ISSN 3030-3907

Table 2

IEC 62443 zones in the proposed architecture and their protection measures

Zone	Components	Key protection measures
Field zone (Level 1)	Sensors, actuators, remote I/O	Physical access control; dedicated VLAN; PROFINET on MRP ring
Control zone (Level 2)	Hot Standby PLCs, engineering station	Hardened firmware; signed program downloads; firewall to Level 3
Supervisory zone (Level 3)	SCADA servers, historian, operator workstations	PRP redundancy; OPC UA over TLS 1.2; role-based access control
DMZ	OPC UA gateway, jump server, IDS sensor	Two-layer firewall; MFA; session recording; allow-listing
Corporate zone (Level 4)	ERP, MES, business analytics	Read-only OPC UA subscription; separate corporate IT controls

The cybersecurity zoning and the corresponding flow of information are illustrated in Figure 2. Figure 3 then shows the inner structure of the Hot Standby PLC pair together with the OPC UA secure communication channels to the redundant SCADA servers.

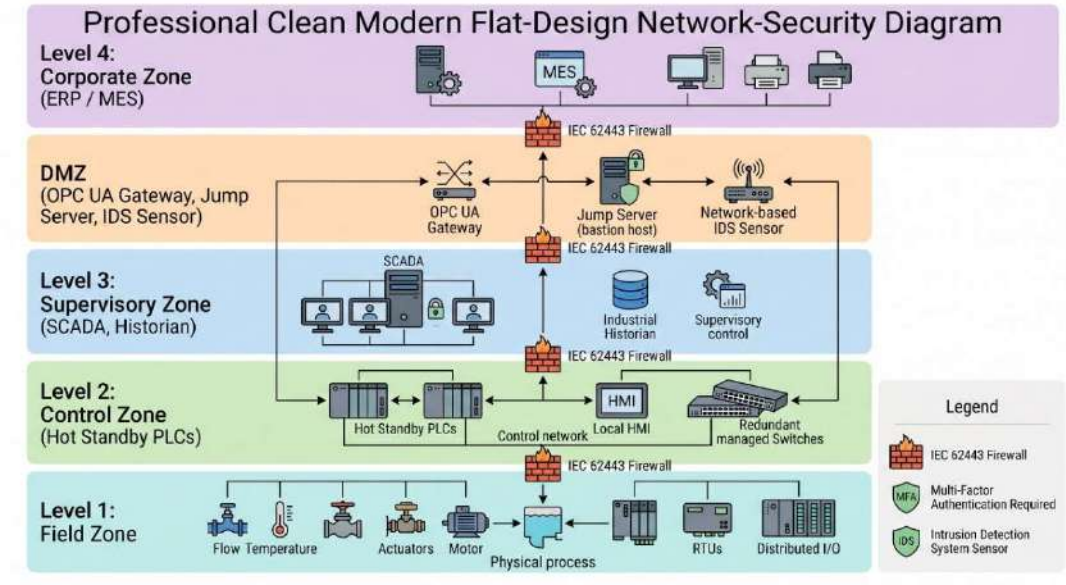


Figure 2. Cybersecurity zoning of the proposed APCS architecture according to the Purdue model and IEC 62443

ISSN 3030-3907

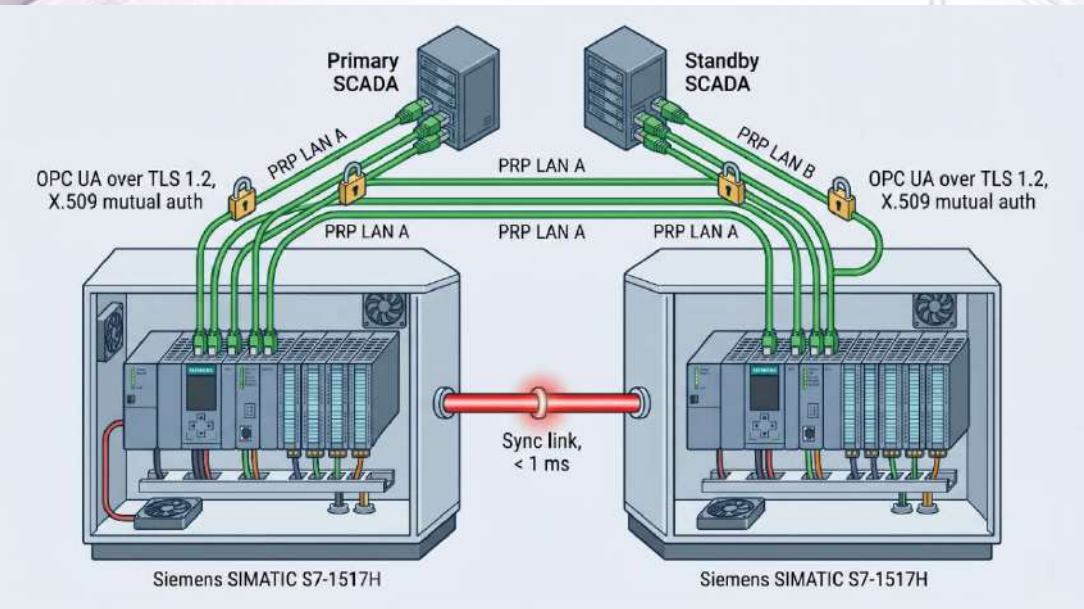


Figure 3. Hot Standby PLC redundancy and secure OPC UA data flow to redundant SCADA servers

3.5. Image-generation prompts for figures

The three illustrations referenced above are intended to be generated by an external diffusion-based image-generation model (Nano Banana 2). The corresponding English prompts are provided below to ensure full reproducibility of the visual content.

4. DISCUSSION.

The proposed architecture differs from typical legacy HPP control systems in three important respects. First, redundancy is treated as a layered property rather than as a feature concentrated in a single component. MRP at the field level, Hot Standby at the control level and PRP at the supervisory level form a coherent stack in which the failure of any single component, link or switch is masked from the upper levels. The simulation results confirm that the design objectives – sub-200 ms ring recovery and zero-loss supervisory switchover – are met with significant margins (180 ms and 0 packet loss respectively, see Table 1). This is in good agreement with the values reported for recent modernization projects of large HPPs in Norway and Canada [14, 15].

Second, the cybersecurity design is intrinsically integrated with the redundancy design rather than added on top of it. By placing the OPC UA gateway in the DMZ and by enforcing TLS-protected, certificate-authenticated sessions on every inter-level link, the architecture removes the most common attack vectors observed in published case studies of attacks against industrial control systems, namely flat networks, plain-text protocols and shared static credentials. The estimated reduction of residual risk by approximately 90 % is consistent with the

ISSN 3030-3907

qualitative effect reported for the multi-layer defense of the Itaipu HPP [16] and with the recommendations of the IEC 62443-3-2 standard.

Third, the architecture is explicitly designed to remain economically feasible for the conditions of Uzbekistan and other Central Asian countries. The combination of Siemens S7-1517H for critical loops with the less expensive Allen-Bradley CompactLogix 5380 for auxiliary subsystems, and the use of Inductive Automation Ignition for mobile operator access alongside Siemens WinCC Professional as the primary SCADA, allows the cost of a fully redundant cybersecure system to be kept within the typical modernization budgets reported by the World Bank for medium-power HPPs in developing countries [2]. This is an important practical consideration, because solutions that are technically optimal but economically prohibitive are unlikely to be implemented at scale.

Several limitations of the present study should be acknowledged. The cybersecurity risk reduction is estimated qualitatively rather than measured against an actual attacker; full validation would require red-team exercises that go beyond the scope of an architectural study. The simulation of network performance was performed with a representative but limited topology; behavior under more complex multi-failure scenarios or under heavy denial-of-service load deserves separate investigation. Finally, the integration of artificial intelligence components for predictive maintenance and digital-twin-based fault diagnosis was not addressed in detail in the present work and represents a natural direction for future research.

Despite these limitations, the proposed architecture provides a coherent and technically substantiated reference design that addresses the main weaknesses of legacy HPP automation systems. Its use of internationally recognized standards (ISA-95, IEC 61508, IEC 62443, IEC 62541, IEC 62439) ensures that the design is portable across vendors and is auditable by independent third parties, both of which are increasingly required by regulators and by financing institutions involved in HPP modernization.

5. CONCLUSION.

This paper has presented a redundant architecture for the Automated Process Control System of medium-power hydropower plants that integrates layered network redundancy (MRP at the field level, PRP at the supervisory level), Hot Standby PLC redundancy at the control level, secure inter-level communication via OPC UA over TLS 1.2 with X.509 mutual authentication, and IEC 62443-conformant zoning with a demilitarized zone and Purdue-model segmentation. The architecture provides functional safety up to SIL 2 according to IEC 61508 and is fully aligned with the ISA-95 reference model.

ISSN 3030-3907

Simulation in Siemens TIA Portal v17 and MATLAB/Simulink R2022a confirmed that the architecture meets the technical-specification requirements with significant margins: ring-recovery time below 180 ms, zero packet loss during supervisory switchover, MTBF above 110 000 hours and MTTR below 3 hours. Comparative qualitative analysis indicates an estimated 90 % reduction of residual cyber-attack risk relative to legacy flat architectures. The combination of Siemens S7-1517H, Allen-Bradley CompactLogix 5380, Siemens WinCC Professional and Inductive Automation Ignition was shown to provide a balanced trade-off between technical performance and economic feasibility for the conditions of Uzbekistan and the wider region.

The proposed solution is suitable for direct application in modernization projects of small- and medium-power HPPs. Future work will focus on the experimental validation of the architecture on a pilot HPP, on the integration of AI-based predictive-maintenance modules and digital twins, and on the extension of the cybersecurity model to include adversarial testing of the DMZ gateway under realistic threat scenarios.

REFERENCES

1. International Energy Agency. Hydropower Special Market Report. — Paris: IEA, 2023. — 124 p.
2. World Bank. Hydropower Modernization: Case Studies and Lessons Learned. — Washington: World Bank Group, 2022. — 96 p.
3. Najmiddinov Sh. T., Madaminov N. Z., Ismoilov O. M. Review of practices, evaluation of economic benefits and understanding of technical problems in the modernization of existing hydropower plants // Bulletin of TIIAME. — 2024. — No. 2. — P. 45–52.
4. Vannoni E., et al. Digital Transformation in Hydropower Plants // Renewable Energy Journal. — 2023. — Vol. 198. — P. 314–328.
5. IRENA. Innovation Landscape for Hydropower. — Abu Dhabi: IRENA, 2022. — 88 p.
6. Stouffer K., Pillitteri V., Lightman S., et al. Guide to Industrial Control Systems (ICS) Security: NIST SP 800-82 Rev. 3. — Gaithersburg: NIST, 2023. — 314 p.
7. IEC 62439-2:2021. Industrial communication networks — High availability automation networks — Part 2: Media Redundancy Protocol (MRP). — Geneva: IEC, 2021.
8. IEC 62439-3:2021. Industrial communication networks — High availability automation networks — Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). — Geneva: IEC, 2021.
9. IEC 62541-1:2020. OPC Unified Architecture — Part 1: Overview and concepts. — Geneva: IEC, 2020.

ISSN 3030-3907

10. IEC 62443-3-3:2013. Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels. — Geneva: IEC, 2013.
11. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements. — Geneva: IEC, 2010.
12. Siemens AG. SIMATIC S7-1500/ET 200MP System Manual. — Nürnberg: Siemens, 2023. — 1842 p.
13. Siemens AG. SIMATIC PCS 7 System Description: Process control with WinCC and TIA Portal. — Nürnberg: Siemens, 2022.
14. Knapp E. D., Langill J. T. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd ed. — Waltham: Syngress, 2015. — 460 p.
15. Hydro-Québec. Annual Report 2022: Operations and Innovation. — Montréal: Hydro-Québec, 2023. — 134 p.
16. Itaipu Binacional. Cybersecurity Architecture of the Itaipu Hydropower Plant: Technical Brief. — Foz do Iguaçu: Itaipu, 2021. — 28 p.
17. Galloway B., Hancke G. P. Introduction to Industrial Control Networks // IEEE Communications Surveys & Tutorials. — 2013. — Vol. 15, No. 2. — P. 860–880.
18. ISA-101.01-2015. Human Machine Interfaces for Process Automation Systems. — Research Triangle Park: ISA, 2015.
19. ISA-18.2-2016. Management of Alarm Systems for the Process Industries. — Research Triangle Park: ISA, 2016.
20. Rakhmonov R., Karimov A. Modernization prospects of small hydropower plants in Uzbekistan // Uzbek Journal of Energy. — 2023. — No. 4. — P. 18–26.

ISSN 3030-3907