ENGINEER

international scientific journal

ISSUE 3, 2025 Vol. 3
E-ISSN
3030-3893
ISSN
3060-5172

SLIB.UZ
Scientific library of Uzbekistan

A bridge between science and innovation

TOSHKENT DAVLAT TRANSPORT UNIVERSITETI
Tashkent state transport university

ENGINEER

A bridge between science and innovation

E-ISSN: 3030-3893

ISSN: 3060-5172

VOLUME 3, ISSUE 3

SEPTEMBER, 2025

engineer.tstu.uz

TASHKENT STATE TRANSPORT UNIVERSITY

ENGINEER

INTERNATIONAL SCIENTIFIC JOURNAL
VOLUME 3, ISSUE 3 SEPTEMBER, 2025

Founder of the international scientific journal "Engineer" – Tashkent State Transport University, 100167, Republic of Uzbekistan, Tashkent, Temiryo'lchilar str., 1, office: 465, e-mail: publication@tstu.uz.

The "Engineer" publishes the most significant results of scientific and applied research carried out in universities of transport profile, as well as other higher educational institutions, research institutes, and centers of the Republic of Uzbekistan and foreign countries.

The journal is published 4 times a year and contains publications in the following main areas:

- Engineering;
- General Engineering;
- Aerospace Engineering;
- Automotive Engineering;
- Civil and Structural Engineering;
- Computational Mechanics;
- Control and Systems Engineering;
- Electrical and Electronic Engineering;
- Industrial and Manufacturing Engineering;
- Mechanical Engineering;
- Mechanics of Materials;
- Safety, Risk, Reliability and Quality;
- Media Technology;
- Building and Construction;
- Architecture.

Tashkent State Transport University had the opportunity to publish the international scientific journal "Engineer" based on the **Certificate No. 1183** of the Information and Mass Communications Agency under the Administration of the President of the Republic of Uzbekistan. **E-ISSN: 3030-3893, ISSN: 3060-5172.** Articles in the journal are published in English language.

Innovative method for managing the power supply of automation and telemechanics devices in railway infrastructure

A.A. Ablaeva[1][a]
[1]Tashkent state transport university, Tashkent, Uzbekistan

Abstract: The article discusses a system for managing the power supply of automation and telemechanics devices in railway transport. It provides an algorithm for the system's operation, ensuring secure data exchange between the control center and line control points. Additionally, improvements to the system are proposed, including the use of artificial intelligence technologies for predicting emergency situations, the use of secure communication channels, and the introduction of a decentralized event log.

Keywords: railway transport, uninterruptible power supply, signaling and communication, intelligent system, parameter control

1. Introduction

The reliability of the power supply to automation and The reliability of the power supply to automation and telemechanics systems is a basic prerequisite for the safe and uninterrupted operation of railway transport. The stability of the transport process, the prevention of emergencies and the minimisation of risks during train movement depend on the correct operation of signalling, centralisation and interlocking (SCI) facilities. Disruptions in the power supply to these systems can lead to serious failures, including forced stoppages, loss of control and significant economic costs.

Modern automated control and management systems, such as SCADA and automated monitoring and telemechanics (AMT) systems, provide a wide range of functions: from the collection and storage of technological information to remote control of switching equipment and energy consumption accounting. Their implementation has significantly increased the level of process automation and reduced the workload on operational personnel. However, despite their high level of functionality, these systems have a number of limitations. In particular, factors such as high electromagnetic interference immunity, the presence of long communication lines, a complex power supply structure, and the need for continuous real-time operation of control systems are of particular importance in the railway infrastructure.

Cybersecurity is a separate issue. Traditional SCADA systems, originally designed for energy and industrial production facilities, have limited mechanisms to protect against targeted cyberattacks. In recent years, there has been an increase in the number of incidents involving unauthorised interference with transport infrastructure facilities, making the protection of communication channels and control devices a priority. Vulnerabilities can manifest themselves at the level of network protocols as well as at the level of controller software and server applications. This increases the risk of unauthorised changes to equipment operating modes, the failure of critical nodes and, as a result, the occurrence of emergency situations[1-3].

In this regard, the development of new power supply control systems for automation and telemechanics devices with the integration of modern data protection methods is a relevant scientific and practical task. The use of cryptographic protection technologies, multi-level authentication, and intelligent data analysis algorithms will not only increase the reliability of the infrastructure, but also bring its resistance to external and internal threats to a qualitatively new level.

Thus, the research presented in this paper is aimed at solving a set of problems related to ensuring the stable power supply of signalling systems, their monitoring and protection from cyber threats, which together form the basis for improving the overall safety of railway transport.

2. Research methodology

The proposed system includes hardware and software complexes integrated into a single control network. The central element is the automated workstation (AWS) of the energy dispatcher, which generates control commands and visualises the status of the equipment. To protect data exchange channels, a cryptographic protection module is used at the dispatch centre, which performs digital signing and verification of messages. The IP data transmission network is based on a local computer network and managed switches that provide packet routing. Linear control points are equipped with their own protection modules and perform command authentication, cryptographic processing, and interaction with power supply devices (switching equipment, distribution boards, uninterruptible power supplies). Each control point has a unique network address, which ensures accurate command routing [4,5]. A block diagram of the control architecture of the integrated power supply control system for automation and telemechanics devices for railway transport is shown in Figure 1.

The automated workstation (AWS) of the power dispatcher is the central control element. It generates control commands, provides visualization of the control circuit mnemonic diagram, and displays the status of the equipment in real time.

The control center protection module is a specialized microprocessor responsible for digitally signing outgoing packets, checking incoming messages, and coordinating the protection of line points.

The IP data transmission network includes a local computer network and network switches. The network provides packet routing and connection to line control points[6].

[a] https://orcid.org/0000-0002-7713-1602

Line control points (CP) are hardware and software complexes that have unique network addresses and interact with specific power supply devices. Each CP is equippedwith a protection module. Line control point protection modules verify the authenticity of commands and return messages. They perform cryptographic processing using digital signatures, which eliminates the possibility of interference [7-10].

Power supply devices for automation and telemechanics devices are switching equipment, distribution boards, uninterruptible power supplies, and other equipmentresponsible for powering signaling and interlocking facilities.

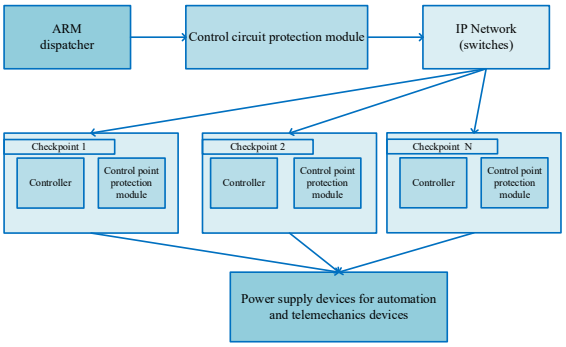

Fig. 1. Block diagram of the control architecture of an integrated power supply monitoring system for automation and telemechanics devices for railway transport

In addition, artificial intelligence algorithms are being incorporated into the architecture, enabling the analysis of telemetry data and the identification of hidden patterns that precede failures.

Developed method

The algorithm for the functioning of the control system for the power supply of automation and telemechanics facilities, shown in Figure 2, can be divided into four levels of processes: command formation, command processing and transmission, command execution, and feedback.

Command formation and preparation. The dispatcher, working at the ARM, selects the control object (e.g., feeder, sectional disconnector, or backup power source) on the mnemonic diagram. The workstation software generates a primary data packet that includes the unique network address of the line control point (CP), the identifier of a specific power supply device, the command type (enable, disable, switch, request diagnostics, etc.), and a timestamp to prevent "repeated attacks." The packet is transmitted to the control center protection module for protection [11].

Cryptographic processing and data protection includes packet signing, key pair generation, channel encryption, and routing. The control center protection module applies an electronic key to the packet using a private key. The system generates a public/private key pair for a specific exchange session. This prevents data substitution during long-term operation. The packet can additionally pass through a secure VPN tunnel, which prevents interception at the network level. The signed packet is sent to the IP network and transmitted to the required control point via network switches.

The packet is then received and verified at the line control point. The control point receives the message through the control point protection module. The electronic key is then verified, and the control point protection module uses the public key to verify the authenticity of the packet. If the key is correct, the packet is forwarded. If the key does not match, the packet is blocked and a report of an unauthorized access attempt is sent. The control point analyzes the device ID and command. If the command does not match the control point configuration or equipment operating mode (for example, re-enabling an already enabled device), it is ignored and recorded in the log[12-14].

The control command is then executed. The control point converts the command into a physical signal, the power supply device closes or opens the circuit, switches the power source, turns on the backup power supply, and performs a self-diagnostic test cycle.

The power supply device performs a self-diagnostic test: checking the status of the control sensors. The control point collects monitoring data and forms a return packet containing the current status of the device (on/off/error), diagnostic parameters (voltage, current, temperature), and a timestamp. The return packet is signed with an electronic key in the control point's protection module and sent to the IP network.

The control room circuit protection module at the control room checks the electronic key of the incoming packet. The ARM updates the status of the object on the control room circuit mimic diagram. The dispatcher receives visual and audible indications of the successful execution of the command or the presence of errors or alarm signals. All events are automatically recorded in the log for subsequent analysis [15].

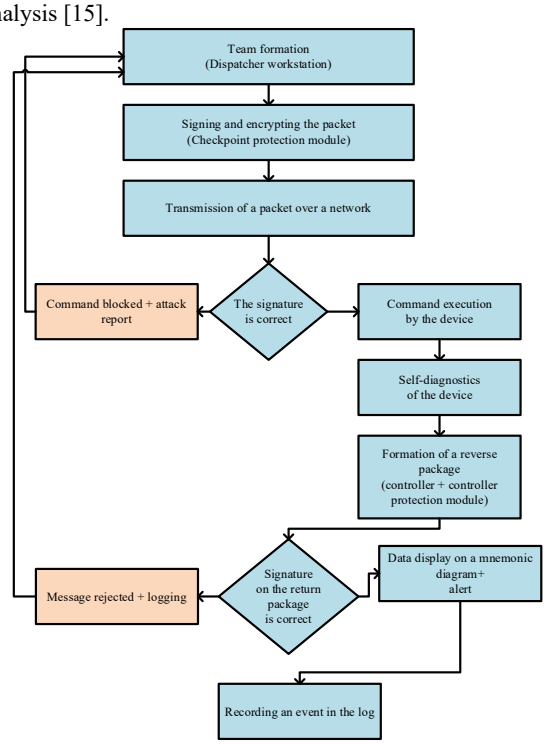

Fig. 2. System operation algorithm

If an invalid key is detected, the command is blocked. In the event of a repeated attack, the system can automatically terminate the connection with a suspicious controller. In the event of a communication channel failure, a backup channel is activated. If one of the control point protection modules is faulty, control of the facility can be transferred via a neighboring control point if a bypass route is available.

3. Results

The presented architecture and algorithm have shown that the implementation of cryptographic mechanisms in the power supply control system of telemechanics facilities allows the following results to be achieved. The electronic key eliminates the possibility of substitution or modification of control commands, which makes the system secure against man-in-the-middle attacks and replay attacks. Data from linear control points is protected by an electronic key, which prevents falsification of diagnostic indicators. Reduced likelihood of emergencies. Filtering of invalid commands at the control point eliminates the possibility of erroneous or malicious actions. The system displays the status of equipment in real time, records all events, and automatically warns of malfunctions.

Unlike SCADA, the new system has built-in cryptographic protection mechanisms, protects not only the transmission protocol but also each control command, operates on a zero trust principle (a command is considered valid only when its authenticity is confirmed), and provides for the redundancy of communication channels and control nodes, which increases fault tolerance.

The introduction of artificial intelligence algorithms significantly expands the capabilities of the proposed system, taking it beyond traditional control and diagnostics. Based on the analysis of telemetry data (currents, voltages, temperature, frequency of operations), neural network models can identify hidden patterns that precede a failure. This allows for advance planning of equipment replacement or repair, reducing the risk of accidents. Machine learning algorithms can automatically detect deviations from normal operating conditions (voltage surges, sudden load changes). The system generates alerts to the dispatcher and recommends corrective actions. Using intelligent load management techniques, the system can balance consumption and connect reserves only when necessary. This is especially relevant when integrating renewable sources (solar panels, wind turbines) into the railway infrastructure. AI can analyze network traffic and identify suspicious commands, even if they pass cryptographic verification but differ from the typical control profile. This implements the concept of a "second line of defense" against cyberattacks.

The introduction of artificial intelligence can reduce accidents and the number of unscheduled repairs, increase the efficiency of equipment use, automate some of the dispatcher's functions (smart prompts, recommendation systems), and increase the cyber resilience of the system.

4. Conclusion

The control algorithm for the integrated power supply control system for automation and telemechanics devices for railway transport is an innovative solution that ensures secure data exchange and reliable equipment control.

The implementation of cryptographic mechanisms prevents command substitution and ensures the reliability of data exchange between the dispatcher and line control points. The system implements a closed control loop: from command formation to feedback and visualization of the result, including error handling and cyberattacks. The system has been shown to respond effectively to both emergency situations (power outages on the line) and cyber threats, ensuring recovery of operability and documentation of events. The use of artificial intelligence methods (failure prediction, digital twins, intelligent command filtering) allows a transition from reactive to predictive control. This reduces accidents and increases economic efficiency. In the future, the system may be supplemented with blockchain logging, quantum-resistant cryptography, and Smart Grid technologies, which will create the basis for building a digital railway infrastructure. Promising areas for further development include the introduction of quantum-resistant cryptography, blockchain event logging, and integration with the Smart Grid concept.

Thus, the proposed system could become the basis for building a digital and cyber-resilient railway transport infrastructure capable of effectively countering modern challenges and threats.

References

[1] C.P. Aboelela, W. Edberg, V. Vokkarane, “Wireless sensor network based model for secure railway operations,” Proceedings of the 25th IEEE Performance, Computing, and Communications Conference, 2006, pp. 623-628.

[2] G.M. Shafiullah, S.A. Azad, “Energy-efficient wireless MAC protocols for railway monitoring applications,” IEEE Trans. Intell. Transp. Syst. 14 (2) (2013) pp. 649-659.

[3] J. F. Kurbanov, D. N. Roenkov and N. V. Yaronova, “Diagnostic and Control System for Increasing the Efficiency of Solar Panel Based on Microprocessor Elements,” 2023 Seminar on Electrical Engineering, Automation & Control Systems, Theory and Practical Applications (EEACS), Saint Petersburg, Russian Federation, 2023, pp. 186-189, doi: 10.1109/EEACS60421.2023.10397328.

[4] Sapozhnikov V. V., Kovalev N. P., Kononov V. A., Kostrominov A. M., Sergeev B. S. Power Supply for Railway Automation, Remote Control and Communication Devices. Moscow: Educational and Methodological Center of Railway Transport, 2005.

[5] Serdyuk T. M., Oleynik A. R. Use of batteries at electrical centralization posts, crossings and battery cabinets of incoming traffic lights. Electromagnetic compatibility and safety on railway transport, 2016, no. 11, pp. 24–34.

[6] Serrano-Jiménez D., Abrahamson L., Castaño-Solís S., Sanz-Feito J. Electrical railway power supply systems: Current situation and future trends. International Journal of Electrical Power & Energy Systems, vol. 92, pp. 181–192, 2017. doi:10.1016/j.ijepes.2017.05.008

[7] A.A. Ablayeva,. N.V. Yaronova, O.O. Ruzimov, “Ensuring a Reliable Power Supply for Railway Traffic Lights Using Renewable Energy Sources,” Proceedings - 2024 International Ural Conference on Electrical Power Engineering, UralCon 2024, 2024, pp. 600-604

[8] V. V. Sapozhnikov, N. P. Kovalev, V. A. Kononov, A. M. Kostrominov, and B. S. Kostrominov, “Power Supply for Railway Automation, Remote Control and Communication Devices,” Moscow: Educational and Methodological Centre of Railway Transport, p.543, 2005.

[9] D. Serrano-Jiménez, L. Abrahamson, S. Castaño-Solis, and J. Sanz-Feito, “Electrical railway power supply systems: Current situation and future trends,” International

Journal of Electrical Power & Energy Systems, vol. 92, pp. 181-192, 2017.

[10] J. Qian, W. Guo, H. Zhang, and X. Li, “Research on automatic test method of computer-based interlocking system,” International Conference on Communications, Information System and Computer Engineering (CISCE), 3-5 July 2020, Kuala Lumpur, Malaysia, pp. 298-302.

[11] A. Srivastava, A. Singh, G. Joshi, and A. Gupta, “Utilisation of wind energy from railways using vertical axis wind turbine,” International Conference on Energy Economics and Environment (ICEEE), 27-28 March 2015, Noida, India, pp. 1-5.

[12] Kuraish Bin Quader Chowdhury, Moshiur Rahman Khan, Md. Abdur Razzak, “automation of rail gate control with obstacle detection and real time tracking in the development of bangladesh railway,” IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), pp.1-6, 2020.

[13] A. Khalikov, A. Khurramov, O. Urokov, S. Rizakulov, “A mathematical model of the operation process of a radio communication network based on IP technologies in the conditions of information impact during the transmission of a non-repetitive data stream,” E3S Web of Conferences 420, art. no. 03022, 2023

[14] N. Zhao, C. Roberts, S. Hillmansen and G. Nicholson “A multiple train trajectory optimisation to minimize energy consumption and delay,” IEEE Transactions on Intelligent Transportation Systems, vol. 16, art. no. 5, pp. 2363-2372, 2015.

[15] J. Andruszkiewicz, J. Lorenc, A. Weychan, “determination of the optimal level of reactive power compensation that minimises the costs of losses in distribution networks." Energies 2024, pp.150.

Information about the author

Ablaeva Aliye Ayderovna
Tashkent State Transport University, Department “Radio-electronic Devices and Systems”
E-mail: aliewka4703@mail.ru
Tel.: +998 97 403 42 20
https://orcid.org/ 0000-0002-7713-1602

CONTEXT / MUNDARIJA