INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Research Article | DOI: 10.2478/ijssis-2026-0078 Issue 1 | Vol. 19 (2026)

Developing a Traffic Monitoring and Control Model for Communication Channels of TCCNs

J.I. Zeynalov[1], F.H. Pashayev[2], M.E. Aliyev[1] and H.T. Najafov[1,*]

[1]Nakhchivan State University, Nakhchivan AZ 7012, Republic of Azerbaijan

[2]Ministry of Science and Education of the Republic of Azerbaijan, Institute of Control Systems, Baku AZ 1142, Republic of Azerbaijan

*E-mail: hasan.nacafov@ndu.edu.az

Received for publication October 24, 2025.

Abstract

This study investigates the technical characteristics of controllers operating at the lower layers of cyber-physical systems, known as industrial networks, which are designed for reliable long-term operation in harsh environments and are widely deployed in such systems. Monitoring and controlling communication traffic in technological corporate computer networks (TCCNs) has become a critical challenge. To address this issue, traffic behavior is analyzed at both the lower level, where industrial networks connect primary transducers and object controllers, and the upper level, which interfaces with corporate networks. Experimental results show that traffic volume in industrial networks remains nearly constant over time, whereas segments closer to corporate networks exhibit periodic patterns associated with daily human activities. Based on these observations, appropriate traffic control algorithms and methods are proposed for both scenarios. Furthermore, a traffic control model is developed for the periodic case, and its analytical solution is presented to support efficient network management.

Keywords

MicroPC controller, industrial network, corporate network, traffic monitoring, traffic control, time dependence of traffic volume

I. Introduction

There are various known variants and designs of technological corporate computer networks (TCCNs) [1–6].

TCCNs retain many features of modern monitoring, diagnostics, control systems, Supervisory Control and Data Acquisition (SCADA) systems, and Corporate networks and computer networks, and are created on their basis. SCADA systems provide direct links from a digital world into physical processes [7].

In cyber-physical TCCN/SCADA environments, traffic throttling and buffering also affect security and resilience. Controlled throttling can reduce the impact of denial-of-service-type traffic bursts by preventing channel saturation, while buffering introduces bounded latency that must remain within process-control tolerance. Therefore, the proposed model is designed to keep the overload probability low while maintaining predictable delay, which is important for both availability and safety in industrial control systems.

This includes monitoring, diagnostics, and control systems created for technical objects; these systems are mainly created as three-level systems. In a corporate environment, networks and systems should be organically linked to the architecture of the enterprise, and are mainly created in interconnection with the architecture of the enterprise. The lower level of TCCNs contains primary transducers that convert various physical parameters into analog signals. The analog signals generated at the outputs of these transducers are converted into binary codes by means of analog-digital converters (ADCs) of the system's object controllers [8–11]. These object controllers group the primary transducers and ensure

Open Access. Professor Subhas Chandra Mukhopadhyay. CC BY-NC-ND
© 2026 Zeynalov et al., This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License https://creativecommons.org/licenses/by-nc-nd/4.0/

that the signals received from these transducers are assigned unique numbers corresponding to the signal sources [12,13]. Studies show that the construction of lower-level cyber-physical systems, called industrial networks, and the software and hardware tools used to protect these systems and the data generated here, call for special attention [10,11]. The creation of a package of software and hardware tools for each system is one of the main parts of the system design process. Listed in the following paragraphs are some technical characteristics of the MicroPC-type controller by Fastwell, which is used in many projects and is designed to work in harsh environments [13].

These controllers are sometimes referred to as object controllers. Developed by the Canadian company Fastwell, these controllers are designed to operate continuously for long periods of time in harsh environments without human involvement. These controllers have a simple and easy-to-understand architecture and high performance characteristics.

The controller runs under the control of the MS DOS operating system; the interrupt system, memory structure, and programmability are similar to those of the IBM PC. The main technical characteristics of the controller are given in Table 1.

To temporarily store and preprocess analog or digital signals received from the primary transducers, a Memory Base is created in the Non-Volatile Random-Access Memory (NVRAM) and RAM of the controller. The Base containing parameters such as mode parameters and limit values that ensure the operation of the system is created in the NVRAM, and the Base containing collections of signals is created in the RAM.

Another powerful STM32F4XX controller is widely used for connecting various control systems to technological processes and technical objects [13].

This controller has 100 input and output signals. If there is a need to use several signals during communication with any external device or if several inputs and outputs are used simultaneously to provide communication with a device, these inputs and outputs are grouped under one logical name. Some inputs and outputs of this controller are grouped to establish communication with any external device that can provide the serial peripheral interface (SPI) protocol [14].

The controller's corresponding inputs and outputs use the Inter-Integrated Circuit (I2C) protocol to provide communication with external devices. Any device that supports this protocol can be connected to the controller [15,16].

The controller has been used in various projects for data exchange between devices whose inputs and outputs can communicate via the Universal Asynchronous Receiver-Transmitter (UART) (RS485) protocol. During the experiments, these inputs and outputs are used to exchange data with a computer [17,18].

Apart from these, during the experiments, separate single-use inputs and outputs are used. These inputs and outputs can be used for indicators, flags, keys, and so on.

Table 1: Technical characteristics of the MicroPC-type controller by Fastwell

Processor		Am 188 ES, 40 MHz
Timer		Super call and watchdog timer
Memory	RAM	1,024 Kb
	NVRAM1024 Kb	1,024 Kb
Analog inputs	Number of channels	8 (12 bit)
	Conversion speed	12.5 μs
	Conversion range:	±10 V; ±5 V; 0÷5 V, ±20 mA, 0÷20 mA.
Analog outputs:	Number of channels	2 (12 bits)
	Conversion speed:	12.5 μs.
	Conversion range:	±5 V; 0÷5 V, 0 ÷10 V;
Serial port speeds	RS-232	200 kbps
	RS-422/485	2,500 kbps
Environmental conditions:	Operating temperature range:	–40 ÷+85°C;
	Storage temperature range:	–55÷+60°C.

Inputs/Outputs (I/Os) that work with the I2C protocol, I/Os that work with the UART protocol, and I/Os built in indicator lights are described as general-purpose input/outputs (GPIO) when creating a software project.

Recently, there has been a growing focus on the distribution of network resources and traffic monitoring in multipurpose networks. Various methods have been used to solve the problem of traffic monitoring and distribution in critical infrastructure information and communication networks [19,20].

a. Contribution and novelty of the proposed model

Unlike conventional queue-based buffering or traditional SCADA/Industrial Control Systems (ICS) load-balancing mechanisms, which typically rely on fixed-rate transmission, First In, First Out (FIFO) scheduling, or static bandwidth allocation, the proposed traffic control model introduces an adaptive and analytically derived control strategy specifically designed for multilayer TCCNs.

The main contributions and distinctions of this study are summarized as follows:

- Adaptive δ-based traffic throttling: Instead of static rate limiting, the transmission rate is dynamically regulated using an analytically derived parameter ($\delta < 1$) that guarantees that the channel load remains below capacity.
- Time-dependent traffic modeling: Traffic is modeled as a deterministic time-varying function (periodic or non-periodic), rather than assuming stationary stochastic arrivals as in classical queuing theory.
- Predictive overload prevention: The model estimates future overload intervals (T_1–T_2) and proactively buffers selected files before congestion occurs, whereas conventional queues react only after buffer overflow.
- Analytical delay and loss bounds: Closed-form expressions are derived for maximum delay and late-transmission probability, which are not provided in standard SCADA/ICS load-balancing schemes.
- Cyber-physical compatibility: The approach is specifically tailored for controller-based industrial networks with constrained memory and deterministic timing requirements, unlike general-purpose Information Technology (IT) traffic engineering solutions.
- Lightweight implementation: The proposed algorithm requires only local measurements and simple arithmetic operations, enabling deployment on embedded controllers without additional hardware or complex optimization engines.

These characteristics demonstrate that the proposed approach is not a conventional queuing or load-balancing mechanism but a predictive and analytically controlled traffic regulation framework tailored for industrial cyber-physical networks.

This section highlights the importance of information flows and communication protocols in network creation, and shows the distinctive features of networks. Examples of literature describing software tools and models of computers that are network users are given.

The "Methodology and Materials" section provides the necessary parameters for solving the problem regarding the structure of the network. In the "Results and Discussion" section, traffic management models are established by monitoring the communication channels of the TCCN.

II. Literature Review and Problem Statement

Studies show that the correct integration of control system modules in cyber-physical systems and accurate consideration of computing power requires knowing the information flows of control systems [19–22].

Some studies suggest that the future of technologies such as 5G and Wi-Fi 6, and networking in general, will be built on open platform controllers and software. Programmability is considered to be the foundation of every network [23].

Analysis of the created TCCN examples shows that the lower levels of these networks can be called industrial networks. The importance of communication protocols in industrial networks is self-evident [24,25].

The main distinguishing features of TCCNs are as follows:

a) The network controllers and the software running on the computers are the main network users;
b) The computer resources of the network include the computing resources of the controller and computers, their memory, and so on;
c) When network resources are shared between users, computing resources and software are also shared in addition to controllers and computers;

d) Since the communication channels in the network are considered as one of the main software and hardware tools of the network, it is very important to correctly solve the issue of their correct distribution among users.

Distribution functions are mainly implemented in second- and third-level computers [1].

There are M users at the second level, corresponding to the number of computers, and L users at the third level.

Computer resources are basically understood as K controllers at the first level and the software tools in these controllers. We can assume that each controller has one software tool, and the number of these is K.

The software tools in the controllers and the software tools in the second-level computers are also a source of information for each of the second- and third-level users. The software tools in the third-level computers also act as a source of information for the users of this level [26].

As can be seen from the above, many studies have been devoted to solving the problem of distributing computer resources among users under certain conditions. The problem posed in this article is solved in a more general form in accordance with the created conceptual model.

As is known, models created for mechanical and discrete systems are classified according to various characteristics:

- In terms of functionality, there are deterministic and stochastic models;
- In terms of the development of processes over time, there are continuous or discrete models;
- In terms of the system's operating modes, there are stationary and non-stationary models.

This also includes mathematical, abstract, program models, and other models.

Conceptual models describe the system under study in words and provide the main structural and functional characteristics of the system [27,28].

Traffic management models in computer networks are mainly based on the principles of storing data to be transmitted in buffers and then ensuring that it is transmitted at a constant speed so as not to disrupt the operation of the network. In general, traffic management issues have various problems [29]. In the present work, it is proposed to establish a time-dependent function of traffic based on the previous results of the network operation and to delay it by a certain amount if the file to be transmitted at the current time violates the channel's throughput. As a result, the probability of this event occurring is calculated and the maximum delay time is shown. This algorithm can prevent the channel overflow event without loss.

Thus, the article analyzes variants of the time dependence of traffic volume in TCCN communication channels, and builds and solves a traffic control model.

III. Methodology and Materials

For instance, there can be $K = M + L$ users at the second and third levels of the system shown. To solve the problem, let us assume the following:

- Number of controllers is K;
- Total number of transmission channels between the first and second levels is N;
- Transmission rate in the channels between the first and second levels can be denoted as β_{km}. Here k is the number of the controller at the first level, and m is the number of the computer at the second level: $k \in [1, K]$, $m \in [1, M]$;
- Transmission rate in the channels between the second and third levels can be denoted as β_{ml}, where m is the number of the computer at the second level and l is the number of the computer at the third level: $l \in [1, L]$, $m \in [1, M]$.
- Memory capacity of the k-th controller is V_k, $k \in [1, K]$;
- Volume of data generated per unit time in the k-th controller is $v_k, k \in [1, K]$;
- Transmission period of the information generated in the k-th controller is $T_k, k \in [1, K]$;
- Number of channels for transmitting information generated in the k-th controller to the second-level computers is $n_k, k \in [1, K]$;
- Memory capacity of computer number m located at the second level is $V_m, m \in [1, M]$;
- Volume of information generated per unit time on the m-th computer of the second level is $v_m, m \in [1, M]$;
- Transmission period of the information generated on the m-th computer of the second level is $T_m, m \in [1, M]$;
- Memory capacity of computer number l at the third level is $V_l, l \in [1, L]$;
- Volume of information generated per unit time on the l-th computer of the third level is $v_l, l \in [1, L]$.

Some intelligent primary transducers have built-in ADCs that convert analog signals into digital ones, and transmit a signal consisting of a sequence of digits (codes) to mid-level elements via exchange channels. The codes of both types are grouped in such a way that upper-level users can process them using the same algorithms.

As mentioned above, TCCN users are mainly the computers in the network and the software running on these computers. Communication channels are considered to be the main elements of the network and their protection from overloads is a key management issue.

a. Selection of δ and practical guidance

To ensure overload-free operation, the controlled traffic must satisfy $\delta v(t) \le \beta$ for most operating intervals, where $v(t)$ is the measured traffic rate and β is the channel capacity (Figure 3). Therefore, a practical choice of δ can be obtained directly from measurements as:

$$\delta = \min\left(1, \frac{\beta}{v_{max}}\right),$$

where v_{max} denotes the peak observed traffic rate for the considered period (e.g., a day or a work shift). This choice guarantees $\delta < 1$ whenever peaks exceed the channel capacity and provides implementable guidance rather than a conceptual parameter.

Numerical example: From Figure 3, if the channel capacity is $\beta \approx 10$ Mbit / s and the peak traffic is $v_{max} \approx 14$ Mbit/s, then $\delta \approx 10/14 \approx 0.71$. In practice, a conservative margin can be used (e.g., $\delta \approx 0.7$) to account for day-to-day variability and measurement noise.

IV. Results and Discussion

Studies show that the time dependence of traffic volume in communication channels can be different in different cases and in different parts of the network. In the lower parts of the network, associated with primary transducers and controllers operating without human intervention, the time dependence of traffic volume can be approximately evenly distributed. At the upper levels of the network, associated with human activity, there is certain observed periodicity of the time dependence of traffic volume.

Figures 1 and 2 illustrate certain metrics obtained through traffic monitoring on communication channels.

It should be noted that the time-dependent traffic pattern shown in Figure 1 was obtained at the lower levels of the corporate technology computer network; these levels are connected to technical equipment and operate around the clock without human intervention. Long-term experiments and practical applications indicate that traffic patterns at the lower levels of the network—despite certain variations—can resemble the pattern shown in this graph.

The pattern depicted in Figure 2, which is essentially cyclical in nature, represents actual data obtained from a week of activity on the AzScience.net network of the Azerbaijan National Academy of Sciences. Since the traffic volume here is linked to the operations of the Academy's institutes, a cyclical pattern was observed corresponding to the standard workday, spanning approximately 08:00 to 17:00 local time.

The article presents a control model for all three cases; this model compares channel throughput and ensures that traffic volume does not exceed channel throughput.

In both graphs, the abscissa (*x*-axis) axis shows time in minutes, and the ordinate (*y*-axis) axis shows the volume of information passing through the channel per minute.

For clarity, the full model assumptions and derivations for the periodic-traffic case are provided in Section 3 (Methodology). Here, we focus on the interpretation of the measured traffic patterns (Figures 1–3) and the practical implications of applying the control model.

As can be seen from Figures 1 and 2, in some cases the distribution of traffic volume as a function of time is approximately uniform, close to a constant function, and in some cases, it is strictly periodic [30–32]. If we use the average values of several days in cases where the time dependence of traffic volume has daily periodicity, we can determine this dependence for the average day. Figure 3 in the article presents a graph illustrating network traffic, server load, or request processing speed. Existing caption for the graph: “Dependence of average daily request volume on time (in minutes).”

A traffic control algorithm must be created for each non-periodic and periodic case. The throughput of a suitable communication channel β is baud. Let us use the notation adopted above to solve the problem. In Figure 3, the channel throughput is indicated by the green line. Experiments show that a situation similar to that in Figure 1 can occur in parts and channels of the network that operate without human intervention. In this case, traffic can exceed the channel throughput in random cases and for a short time. In

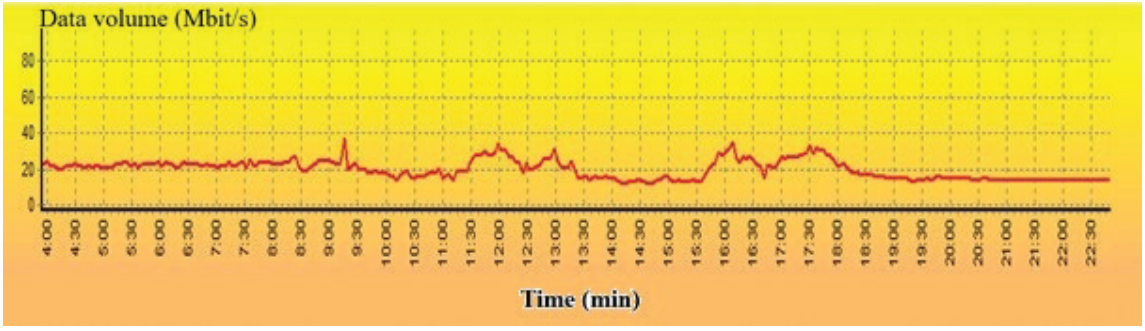


Figure 1: Time dependence of traffic volume in technological channels.

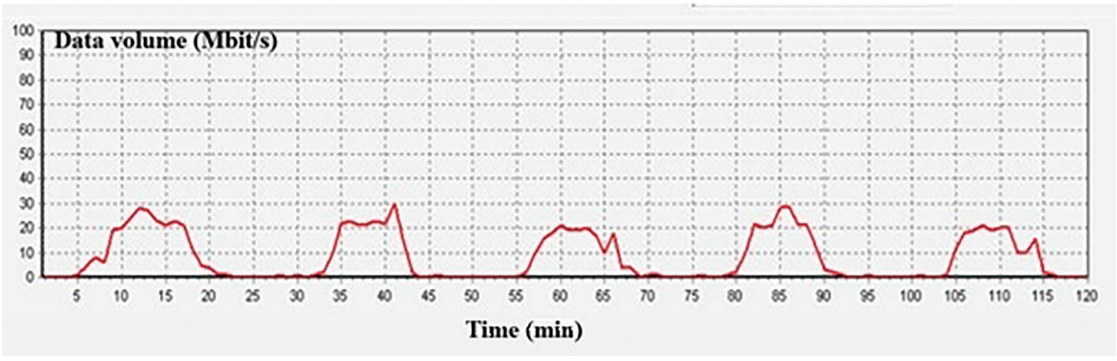


Figure 2: Time dependence of the volume of network requests during the working days of selected week.

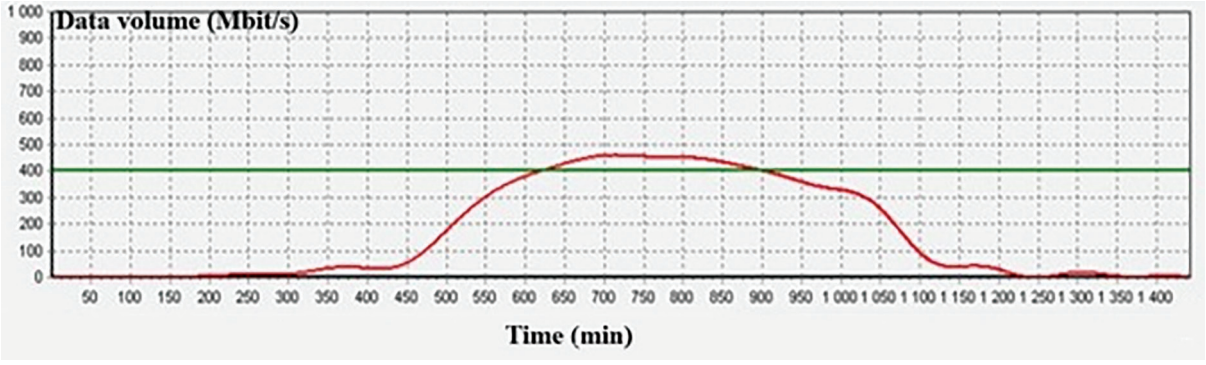


Figure 3: Time dependence of the average daily volume of requests, in minutes.

such cases, disruptions in the channel quickly recover on their own. To eliminate the possibility of that happening altogether, the frequency of reading and digitization of the primary transducers can be lowered.

To solve the traffic load problem, it is necessary to estimate the volume of information coming from sensors, which are primary data transmitters in various network nodes, especially at the technical equipment control level and at the technological process control level. It is known that sensors whose outputs are analog signals and smart sensors whose outputs are binary codes are used in practice. ADCs and controllers are selected depending on the frequency characteristics and sensitivity of the sensors used. Reading information transmitted by sensors with frequencies exceeding their frequency range can lead to repeated

reading of the same information. Therefore, the maximum reading frequency can be determined as

$$w = \min\left\{\begin{matrix}\text{upper limit of the sensor frequency range,}\\ \text{maximum conversion frequency of ADC}\end{matrix}\right\}.$$

However, the actual sensor reading frequencies are selected in accordance with the strategy of process monitoring and control, taking into account the information needs of corporate network users, adjusted for network capacity.

To prevent the selected channel from overloading, we can write

$$w = \delta * \min\left\{\begin{matrix}\text{upper limit of the sensor frequency range,}\\ \text{maximum conversion frequency of ADC}\end{matrix}\right\}.$$

Here we can take $\delta < 1$. Thus, the average volume of data received from the initial data sources will be reduced and the volume of data transmitted will not exceed the channel throughput. Therefore, in this case, the traffic control problem is reduced to a simple matter of selecting the parameter $\delta < 1$. It should be noted here that this parameter can be determined experimentally.

In cases where the time dependence of traffic volume is periodic, a case close to the one given in Figure 3 can be analyzed. In this figure, the time dependence of traffic volume is shown for one average day. The channel throughput is indicated by the green line and, as mentioned, its value is β. Let us denote the beginning of time by T_0 and the end of time by T. Let us denote the intersection points with the green line by T_1 and T_2. Here we can note the following.

1. The indicated periodicity cannot be exact periodicity. If we record the values of T_1 and T_2 for several days or weeks in practice, then we can obtain the set $\{[T_{1i}; T_{2i}]\}$, which consists of the sequence of time segments $[T_{1i};T_{2i}]$. The right and left sides of the segments in this set will differ slightly. If during the observation period there are Z time intervals in which the amount of information exchanged in the channel exceeds the channel throughput, the segment $[T_1;T_2]$ can be specified as follows:

$$[T_1; T_2] = \bigcup_{i\in[1Z]} [T_{1i}; T_{2i}]$$

2. The volume of information that has to go through the channel during the day can be

$$V_d = \int_{T_0}^{T} v(t)dt.$$

The volume of information going through the channel in the segment $t \in [T_1, T_2]$ when the volume of information exceeds the throughput can be

$$V_{1,2} = \int_{T_1}^{T_2} v(t)dt.$$

Therefore, the volume of information generated in the information sources of the system in the time interval $t\in[T_1, T_2]$ is also $\int_{T_1}^{T_2} v(t)dt$ and we can consider it equal to the price. At this time, information equal to $(T_2–T_1)^*\beta$ can be transmitted through the appropriate communication channels on average. Given this, we can calculate the value of the parameter δ that is independent of random choices and can be calculated as:

$$\delta \le \frac{(T_2 - T_1)^*\beta}{\int_{T_1}^{T_2} v(t)dt}$$

However, in this case, excess information equal to the quantity $\int_{T_1}^{T_2} (v(t) - \beta)dt$ will be transmitted through the channel. This can cause serious malfunctions in the operation of the channel and disrupt the operation of the network. The number of data transmissions through the channel can be determined as follows. If a transmission event occurs at every Δt, and we denote the number of transmission events in the interval as $t \in [T_1, T_2]$ by K_t, we can determine this parameter as

$$K_t = \frac{T_2 - T_1}{\Delta t} + 1.$$

3. In order not to disrupt the operation of the channel by transmitting information in excess of the channel's capacity, a portion $v_k - \beta$ of the total information volume v_k to be transmitted in each k-th transmission case can be stored and transmitted after time T_2. According to the logic of the organization of the exchange process in the channel, the stored portion may be one of the files to be transmitted. Thus, it is not efficient to transmit one part of the file and store another part. Therefore, the volume of the stored file must be $v_f \ge v_k - \beta$. This stored file can be transmitted together

with $v(t)$ in the time $t > T_2$ within the conditions $t > T_2$ and $v(t) + v_f \le \beta$. Organizing and managing traffic monitoring with the indicated algorithms can prevent channel disruptions and ensure the transmission of stored files without much delay.

Thus, we obtain the following traffic control model in cases where traffic volume has daily periodicity:

$$V_d = \int_{T_0}^{T} v(t)dt \to \max$$

The following conditions must be fulfilled here:

$$\int_{T_1}^{T_2} \left(v(t) - \beta\right)dt \to \min$$

A file must be found satisfying the condition $\exists\, v_f \ge v_k - \beta \ge 0$ such that the conditions $t \in [T_1, T_2], v(t) = v(t) - v_f \le \beta$ & $t \in [T_2, T], v(t) = v(t) + v_f \le \beta$ are satisfied.

From the results obtained in the article, the probability of a file being transmitted late, falling within the interval $[T_1; T_2]$, can be calculated as:

$$p = \frac{V_d}{V_{1,2}} = \frac{\int_{T_0}^{T} v(t)dt}{\int_{T_1}^{T_2} v(t)dt}$$

The maximum latency of the delayed file is approx. $T_{gmax} = T_2 - T_1$.

V. Conclusion

Research and analysis of existing literature samples show that TCCNs retain many features of modern monitoring, diagnostics, control systems, SCADA systems, and Corporate networks and computer networks, and are created on their basis. These networks can combine, on the one hand, industrial-type networks closely related to technical objects, and on the other hand, local and Internet-connected networks. Being a multilevel network, the lower levels of the Telecommunication and Computer Systems (TCCNs) are related to the controller, primary data converters. The upper levels of these networks are related to computer networks.

It is shown that the lower levels of networks require extensive use of controller techniques. Here, the characteristics of controllers that are widely used in some difficult conditions are given. The importance of communication channels and protocols in the construction of Telecommunication and Computer Systems (TKKS) networks is noted and it is shown that the organization of monitoring of information flows in communication channels is of great importance.

This article analyzes variants of the time dependence of traffic volume in TCCN communication channels observed in the industrial-type part of the network and in the parts close to corporate networks. It is shown that in both cases, the traffic volume can exceed the channel throughput and disrupt the channel's operation. This situation necessitates the solution of the traffic control problem. The article proposes solutions for both cases. A control model is built for cases where the time dependence of traffic volume is periodic and the solution of the model is given.

VI. Practical Outcomes, Limitations, and Future Work

Based on the measured daily traffic patterns (Figure 3), the proposed framework provides a practical procedure to select δ\deltaδ from observed peak traffic and channel capacity, enabling overload mitigation without hardware changes. The model also yields interpretable performance indicators such as the overload interval $[T_1, T_2][T_1, T_2][T_1, T_2]$, late-transmission probability, and a bounded maximum delay for buffered files. A limitation of the current study is that the validation is based on measured traffic profiles without a dedicated hardware-in-the-loop testbed. Future work will focus on extended validation across multiple industrial sites and on adaptive δ\deltaδ scheduling that jointly considers control-loop delay constraints and cyber-security-driven availability requirements.

In practice, various traffic patterns can be found in systems implemented and operated in various industrial sectors. In these cases, models similar to those given in the article have been applied to protect communication channels from overloads. In many cases, the solution to the problem is to increase the throughput of communication channels. In some applications, information blocks have been used. The issue of adaptive management of information blocks in the system is one of the issues to be faced in the future.

References

[1] F. H. Pashayev, J. I. Zeynalov, and H. T. Najafov, "Monitoring and security assessment of traffic in communication channels of technological corporate computer networks," *Electrica*, vol. 25, 0216, 2025. https://doi.org/10.5152/electrica.2025.24216

[2] A. A. Abdullaev, A. A. Dzhavadov, and A. A. Levin, *Telemechanical complexes for the oil industry*. Nedra, 1982.

[3] T. A. Aliyev et al., "Complex of measurement, monitoring, diagnostics and control for oil wells operated by sucker rod pumps," *Azerbaijan Oil Industry*, no. 1, pp. 54–59, 2012.

[4] T. A. Aliev et al., "Intelligent system for online managing oil production based on innovative technologies," *Transactions of ANAS: Informatics and Control Problems*, vol. 37, no. 3, 2017.

[5] V. V. Golenkov et al., "Intelligent computer systems of new generation," *Doklady BSUIR*, 2024. https://doi.org/10.35596/1729-7648-2024-22-2-70-79

[6] O. I. Sheluhin, A. V. Osin, and D. I. Rakovsky, "New algorithm for predicting network states," *Automatic Control and Computer Sciences*, vol. 57, pp. 48–60, 2023. https://doi.org/10.3103/S0146411623010091

[7] J. A. Kumar, G. P. Kulkarni, and J. R. Munavalli, "Recent trends and developments in computer networks," *IJAECS*, vol. 6, no. 9, pp. 107–113, 2019.

[8] Empowered Automation, *What is a PLC and its main characteristics?*, online article. [Online]. Available: https://www.empoweredautomation.com/what-is-a-plc-and-what-are-its-main-characteristics

[9] Engineering Institute of Technology, *Introduction to PLC and SCADA systems*, lecture notes. [Online]. Available: https://cdn.eit.edu.au/cms/images/Webinar_Slides/03_SK_Chapter-01_r4.pdf

[10] F. H. Pashaev et al., "Data protection software and hardware tools," in *Proc. Int. Conf. Technical Means of Information Protection*, pp. 267–270, 2025.

[11] F. H. Pashaev et al., "Development of software and hardware to protect technological processes," *Automatic Control and Computer Sciences*, 2024. https://doi.org/10.3103/S0146411624701074

[12] Fastwel, *CPU188-5 v.3 Processor Module Datasheet*, technical documentation. [Online]. Available: http://syscom.md/products/Fastwel/rus/Fastwel.pdf

[13] STMicroelectronics, *RM0090 Reference Manual: STM32F405/415/407/417 ARM-based MCUs*, technical manual. [Online]. Available: https://www.st.com

[14] STMicroelectronics, *STM32 Serial Peripheral Interface (SPI) documentation*, technical documentation. [Online]. Available: https://www.st.com

[15] GeeksforGeeks, *I2C communication protocol overview*, online tutorial. [Online]. Available: https://www.geeksforgeeks.org/computer-organization-architecture/i2c-communication-protocol

[16] Y. Duan, "I2C data transfer program design," *Lecture Notes on Wireless Networks and Communications*, vol. 1, no. 1, pp. 1–16, 2018.

[17] STMicroelectronics, *STM32 USART peripheral documentation*, technical documentation. [Online]. Available: https://www.st.com

[18] J. Gong, W. Guo, and W. Sun, "UART communication protocol application," in *Proc. Int. Conf. Computing and Data Science*, 2023. https://doi.org/10.54254/2755-2721/14/20230757

[19] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82r2, 2015. [Online]. Available: https://nvlpubs.nist.gov

[20] V. Kosenko et al., "Traffic distribution methods in critical infrastructure networks," *Innovative Technologies and Scientific Solutions for Industries*, vol. 2, no. 2, pp. 48–55, 2017.

[21] L. A. Chizhikova, "Classification of data flows of control complexes," *IJ Open Information Technologies*, vol. 10, no. 5, pp. 69–80, 2022.

[22] M. Mujevic et al., "Trends and new technologies in computer networks," *Int. Scientific Journal Monte*, vol. 9, no. 1, 2024. https://doi.org/10.33807/monte.20243119

[23] Istanbul Technical University, *Programming Logic Controllers course notes*, lecture notes. [Online]. Available: https://web.itu.edu.tr/yalcinme/files/courses/MMG/ch19_1%20PLC.pdf

[24] M. J. Hamill, *Industrial communications and control protocols*, 2020.

[25] M. Popovic, *Communication protocol engineering*. CRC Press, 2018.

[26] A. O. Salau and M. M. Beyene, "Software defined networking based traffic classification," *Scientific Reports*, vol. 14, 20060, 2024. https://doi.org/10.1038/s41598-024-70983-6

[27] T. I. Aliyev et al., *Modeling: Problems, tasks, tests*. ITMO University, 2011.

[28] T. I. Aliyev, *Fundamentals of modeling of discrete systems*. SPbGU ITMO, 2009.

[29] L. Titarenco et al., "Traffic engineering queue optimization models with QoS support," *Electronics*, vol. 14, no. 20, 4078, 2025. https://doi.org/10.3390/electronics14204078

[30] R. K. Alekperov and A. A. Huseynova, "Adaptive load distribution in corporate networks," *Telekommunikatsii*, no. 9, pp. 17–21, 2012.

[31] J. Kolbusz and S. Paszczynski, "Network traffic model for industrial environment," *IEEE Trans. Industrial Informatics*, vol. 2, no. 4, pp. 276–284, 2006.

[32] M. Khvostivskyy et al., "Mathematical modelling of daily computer network traffic," [Online]. Available: https://ceur-ws.org/Vol-3039/short24.pdf