Safety Monitoring of the Automated City Water Supply Management System Based on PSIM and SIEM Systems

Dmitrii Orel [1] and Tatyana Guseva [1]

[1] *North Caucasus Federal University, Pushkina st., 1, Stavropol, 355017, Russian Federation*

Abstract

The article is about the integration of monitoring functions of industrial facility security systems based on the PSIM system. The water supply company of a large city acts as an industrial facility. The analysis of the company structure and its security systems, as well as the means of physical security is done. The functionality of SIEM and PSIM systems is considered. At the end of the article, the algorithm for the operation of the Darvis platform, interacting with the video surveillance system and the existing pressure monitoring sensors in the city's water supply, was developed. The integration of the video surveillance system and the Darvis software will allow it use it as a single platform for providing a comprehensive security system and rapid response to incidents at the city's water supply company. Rapid response to accidents in the water supply line or at pumping stations will reduce water losses, which will reduce financial damage to the company.

Keywords

Security systems integration, industrial facility, SIEM system, PSIM system, Darvis softwar, automated process control system

1. Introduction

According to the report by the Russian company Positive technologies, working in the field of information security, the number of attacks on industrial and energy companies has increased since 2020 (Figure 1). The number of such attacks in 2020 increased by 91% compared to 2019. Basically, this industry has been attacked by ransomware operators, in particular RansomExx, Netwalker, Clop, Maze, Ragnar Locker, LockBit, DoppelPaymer, Snake. The last of them removes shadow copies before starting encryption, and has functions that allow to forcibly stopping processes in the automated control system. Due to the attacks, some companies, such as Huber+Suhner and Honda, were forced to suspend production.

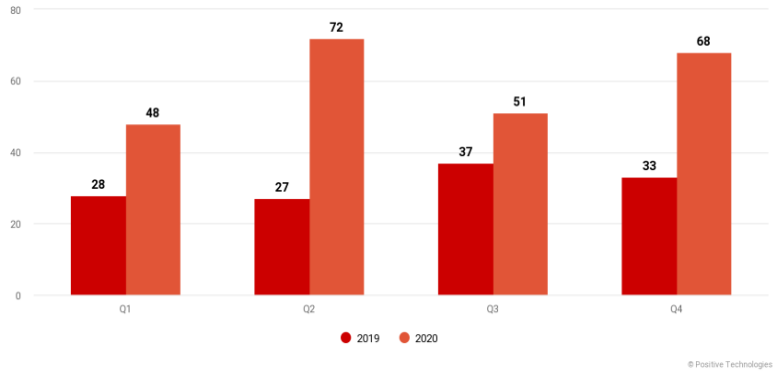

Figure 1: Number of attacks on industrial and energy companies

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: kde.def@gmail.com (Dmitrii Orel); tatyana.petrova.96@bk.ru (T. M. Guseva)
ORCID: 0000-0002-3433-2164 (Dmitrii Orel); 0000-0002-0291-635X (T. M. Guseva)

There is a lot of production infrastructure in Russia, including automated process control systems, and it is of interest to intruders.

Modern automated process control systems have ceased to be autonomous and are increasingly integrated with information systems, forming unified automated information management systems.

For example, in this paper we consider an industrial facility - a water supply company of a large city, which is an automated water supply management system integrated with the enterprise information system.

In such a convergent system, various channels of information transmission are used. All this creates a wide range of threats to the information security of an industrial facility.

The purpose of the work is to increase the efficiency of industrial facility security systems by creating a security monitoring system. The hypothesis is that combining information from sensors of various security systems will a) reduce the time for making decisions to prevent an incident b) increase the accuracy of management decisions in the field of security c) reduce the number of false notifications about information security incidents.

To monitor information systems for managing security incidents at the enterprise SIEM systems can be used. They monitor information systems, analyze real-time security events emanating from network devices, information security tools, IT services, system and application infrastructure, and help detect information security incidents. SIEM systems provide limited opportunities for cybersecurity of industrial facilities, they do not allow taking into account data on the infrastructure of industrial facilities, taking into account physical security issues. As a result, an industrial facility is exposed to a greater number of threats that cannot be controlled. Integration of SIEM systems and SCADA dispatch control and data collection systems allows to solve this problem. Integration will allow SIEM systems to receive data generated by systems that allow monitoring of industrial facilities [1].

Information protection in an automated process control system is achieved by taking a set of organizational and technical information protection measures aimed at blocking (neutralizing) threats to information security, the implementation of which may lead to a violation of the normal functioning of the automated control system and the controlled object and (or) process, localization and minimizing the consequences of the possible implementation of threats to information security, restoration of the normal mode of functioning of the automated control system in case of information security threats [2].

Thus, the integrated security system of industrial facilities, in addition to monitoring the safety of production processes, should also monitor threats related to information security.

It should be pointed that the integration of SIEM and SCADA requires the creation of a complex model that allows describing incidents and incident response algorithms based on data obtained from heterogeneous information systems. In this paper, it is proposed to develop an algorithm for integrating the video surveillance system of an industrial facility of a water supply enterprise with the Darvis software product.

2. Analysis of the structure and security systems of an industrial facility

The water supply company operates in the field of housing and communal services of a large city. The main types of services provided by the company are cold water supply and sanitation.

2.1. Analysis of the organizational structure of the company

The functions of the company are presented on Figure 2.

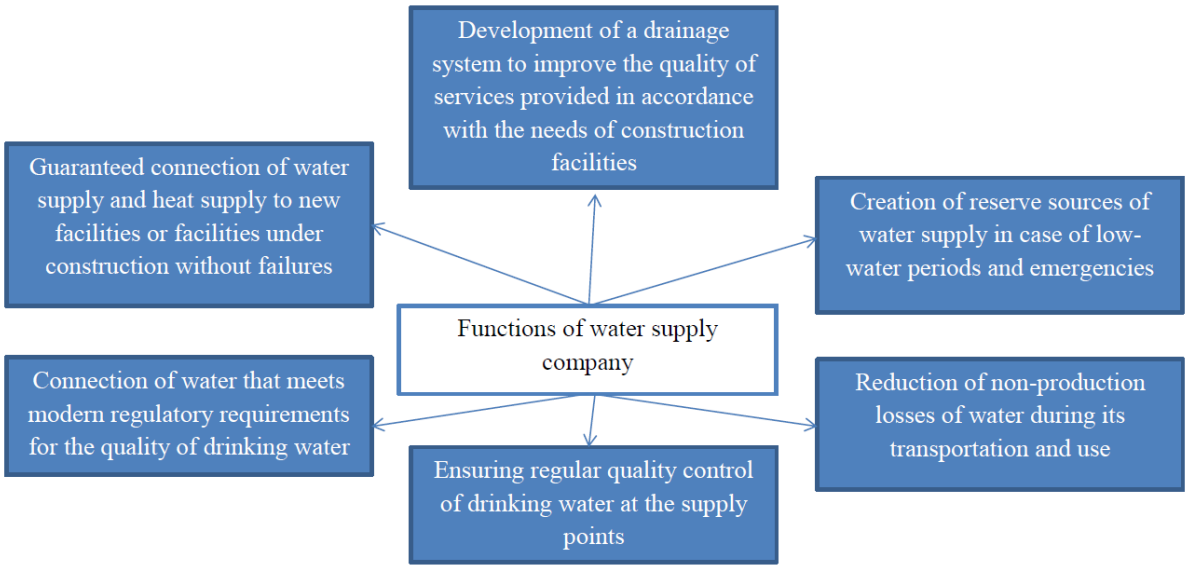

Figure 2: Functions of water supply company

Modern water supply and sewerage systems are a set of structures, mechanisms and equipment, all parts of which must work together accurately and without failures. These include water intake structures, water treatment plants, water supply and sewerage networks with their servicing devices, pumping stations, as well as internal water supply and sewerage systems of buildings.

2.2. The need to integrate industrial facility security systems

The company manages complex and geographically distributed processes for water supply and sanitation in the city. Radio channel communication is used to transmit information from sensors to dispatch control and data collection systems. The exchange between the SCADA system and the operator's ARM takes place over an Ethernet network.

Automated process control systems have two actual threats that allow to disrupt and intercept the management of the enterprise:

1. The threat of disruption of the technological / production process due to time delays introduced by the means of protection.
2. The threat of interception of control by an automated process control system.

Information protection in an automated process control system is achieved by adopting, within the framework of the automated control system protection system, a set of organizational and technical information protection measures aimed at blocking information security threats, the implementation of which may lead to a violation of the normal functioning of the automated control system and the controlled process, to localize and minimize the consequences of the possible implementation of information security threats, restoration of the normal mode of functioning of the automated control system in case of information security threats.

To ensure the full operation of the enterprise, as well as the ability to eliminate the implementation of security threats, the integration of physical security means of the enterprise's automated control system with a SIEM system that allows analyzing security events in real time coming from network devices, information security tools will help.

Using the Methodology for assessing information security threats, three negative consequences that may occur from the implementation (occurrence) of information security threats were identified. The objects of influence: operator's workstation, database, controller for process control, controller for water treatment process control, programmable logic controller (PLC) for pumping station control. The main categories of violator (internal, external), the type of violator and possible goals of information security threats are considered.

The following categories of people can be identified as actual violators (Table 1):

Table 1
Current threats and violators of information security

#	Type of violator	Cat. of the violator	Object of influence	Available interfaces	Methods of implementation
1.	Persons providing the functioning of systems and networks or providing the operator's systems (administration, security, cleaners, etc.)	internal	Information system database	Web user interface for accessing the information system database	Exploiting Database Management System configuration vulnerabilities
2.	System Administrators and Security Administrators	internal	Operator's computer	Access via the organization's local area network	Introduction of malicious software
3.	Former employees (users)	external	Information system database	Web user interface for accessing the information system database	Exploiting Database Management System configuration vulnerabilities
4.	Terrorist, extremist groupings	external	Controller for controlling technological processes of water purification	Remote controller control channel	Data modification in communication channel Introduction of malware
			Programmable logic controller (PLC) for control of pumping stations	Remote controller control channel	Data modification in communication channel Introduction of malware

2.3. Analysis of the automated process control system of the water supply company

Significant difficulties of technological management at the enterprise arise as a consequence of the geographical remoteness of the objects of control and management from each other: technological objects are arbitrarily located throughout the city and beyond. Therefore, management tasks, first of all, require the creation of an effective system for collecting and transmitting information about the parameters and operating modes of technological equipment at various remote facilities. An automated control system (automated process control system) is used to control and conveniently manage the technological processes of the enterprise. The automated process control system allows:

- Create dispatching control of the technological process of water supply and sanitation;
- Provide centralized control of parameters;
- Predict and prevent emergency situations related to the operation of technological equipment;
- Control technological processes, optimize and improve the efficiency of work at the pumping station;
- Minimize the impact of the human factor on the technological process;

- To carry out automatic transmission of the agreed information to the control room of the water supply company;
- Keep commercial records of pumped water, energy carriers and electricity;
- Extend the service life of the units;
- Reduce personnel labor costs by automating control and management functions;
- Increase the safety of the technological process for personnel and the environment.

The automated process control system combines several levels of hardware:

1. Sensors and actuators.
2. SCADA controllers.
3. Computer connecting the operator's workstation and SCADA controllers.

2.4. Analysis of the means of physical security of the water supply company

As means of physical security at the enterprise are provided:

- Access control and management system for the territory and individual premises of the enterprise;
- Security and fire alarm system;
- Video surveillance system.

All security features have events recorded in special logs. Appropriate security personnel are assigned to each means of protection. Actually, they can view service information in the event logs. Figure 3 shows the general structure of the location of the physical security facilities of the water supply company.

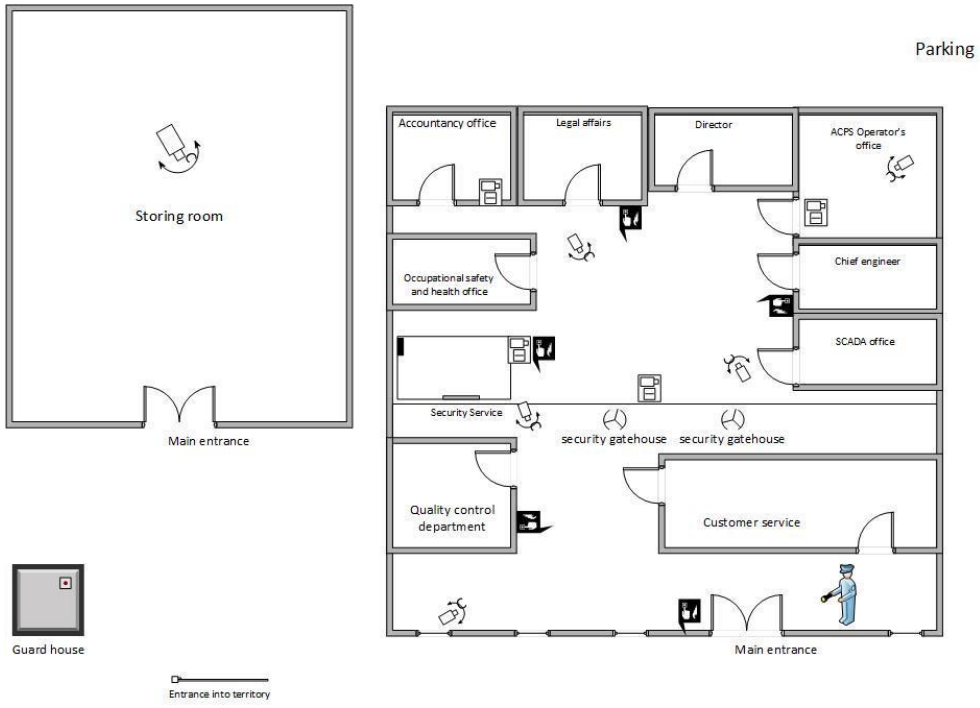

Figure 3: The general structure of the location of physical security facilities of the water company

Figure 3 shows that in order to fully assess the security status of an industrial facility, a security officer must first visit all the points in order to present a picture of what is happening in the building. The lack of interconnection between the means of physical security will complicate the work of the employee and complicates the possibility of early prevention or rapid response in the event of information security attacks affecting the performance of technological processes of the enterprise.

By enabling a security service specialist to see the interconnected state of physical and information security of an enterprise, it is possible to significantly simplify its work and improve its quality. The specialist will not have to spend time collecting information from various journals, and conduct a long

analysis. He will be able to react in a timely manner or even in advance to the incident, preventing an emergency or a malfunction of the enterprise.

This problem will be solved by the introduction of a SIEM system at the enterprise, which will monitor the information system, analyze security events in real time coming from network devices, information security tools. It will be necessary to integrate the existing means of physical security of the enterprise with the installed SIEM system.

3. Analysis of ways to integrate security systems

To date, the number of enterprises that use SIEM systems in their information security management centers to ensure cybersecurity is increasing. Information security management centers use a variety of means to protect important information, which in most cases keep a log of all incidents.

3.1. Functional analysis of the SIEM system

Every year the number of means of protection increases, and it becomes more difficult for information security specialists to process accumulated records in incident logs. At the same time, if you do not analyze emerging threats in a timely manner and do not try to prevent them, then any protection system will be useless. Under these conditions, you should think about using Security Information and Event Management (SIEM) class systems. As a rule, in serious companies with a mature information security function, there are monitoring and response centers where SIEM systems are used [3]. There are often situations when attackers use complex and distributed methods of accessing information, while security tools may not react to such incidents, considering them frivolous. However, if you analyze all the minor incidents, you can form a more visual picture that will indicate a serious attack. It is precisely these properties that characterize modern SIEM systems, they are able to detect attacks by post-analysis of events, by minor incidents, as well as anomalous phenomena in the system.

Consider the generally accepted definition of a SIEM system [3].

SIEM (Security Information and Event Management) - solutions that monitor information systems, analyze real-time security events originating from network devices, information security tools, IT services, system and application infrastructure, and help detect information security incidents. SIEM are provided by providers as hardware devices, software or services and are used to collect and process events, alerts, generate reports and visualize information security violations. It should be noted right away that SIEM systems are designed to monitor and respond to incidents, but do not allow you to protect yourself from threats or prevent negative events [4]. As a rule, these systems appeared much earlier than their application was in demand.

SIEM systems are used to solve the following tasks [3]:

- Data consolidation, collection of information security events from various sources (network devices and IT services, security systems, operating systems, databases, business applications);
- Storing security events from various sources in historical order for retrospective analysis and identification of chains of actions that caused security incidents;
- Correlation and processing of security events, the use of various techniques to compare audit data from various sources and identify significant information;
- Providing tools for expert analysis of events and analysis of security incidents with the ability to search through a variety of parameters and build models of the relationship of events with each other;
- Contextual enrichment of incidents with information about the belonging of the data affected in the IB events to certain business applications, employees of the organization and processes, their criticality for business or vulnerability to threats based on information from security systems and vulnerability scanners;
- Automatic notification of the security administrator via the SIEM interface through integration with the application accounting system, as well as by e-mail, SMS, etc.

Examples of Russian SIEM systems:

- COMRADE;
- Garda Analytics;
- MaxPatrol.

3.2. Analysis of the PSIM system functionality

It should be noted that SIEM systems, like others, evolve over time. As a result of this development, SIEM systems have subclasses with various functional extensions: SOAR, COM, PSIM. In particular, PSIM systems allow not only to collect incident data from network devices, like classic SIEM systems, but also to work with physical security systems and automated process management systems, while PSIM systems not only collect data and generate warnings, but also have the ability to monitor the operation of equipment.

Since it is important for an industrial facility to control the situation using a video surveillance system, PSIM systems are considered in the work.

For the most part, SIEM systems work as network hosts (information system). PSIM systems are used to work with physical security systems and automated control systems.

One of the main additions of PSIM systems is working with video information, which is very important for monitoring the situation at industrial facilities, since the video surveillance system at such facilities is an integral part of physical security. They have connectors to hundreds of models of physical security devices, the rules system allows you to send only important information to the SIEM system, and video data can be transmitted to the SIEM system as a link to the PSIM interface.

Examples of PSIM systems:

- Darvis;
- ESM – PSIM;
- CoordCom.

One of the representatives of the PSIM system is the Darvis software product developed by Infocom-S LLC. The main task of Darvis is the qualitative integration of all existing systems of the facility to ensure full control and management without the use of additional technical units and with minimal participation of employees [5]. Therefore, we will choose it as an integrated system for a water supply company. Below we will consider the algorithm for handling security incidents of the Darvis platform.

3.3. The algorithm of integration of the video surveillance system of the water supply company and the software product "Darvis"

As part of the work, the algorithm for the operation of the Darvis platform will be developed, interacting with the video surveillance system and the existing pressure monitoring sensors in the city's water supply.

Figure 4 shows an interface for creating an event management algorithm for the Darvis platform.

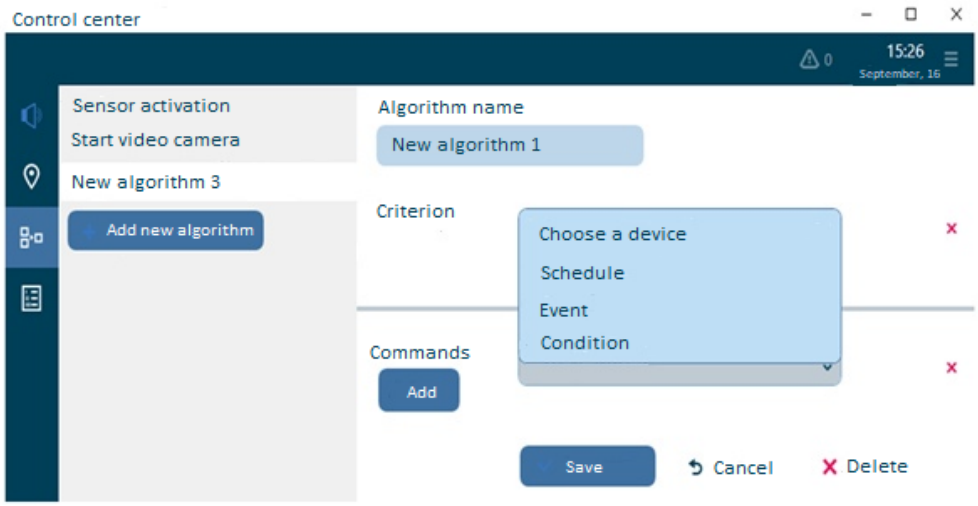

Figure 4: Interface for creating an algorithm for managing events of the Darvis platform

The algorithm for processing an emergency situation will be developed in such a way that it will allow to form a division of alerts into:

- The presence of a high level of danger of an incident that has occurred, which requires immediate notification of the responsible person, and requires an ultra-fast response to eliminate. In this case, the notification to the employee can come in the form of SMS messages, e-mail messages and information output to the computer monitor through integration with the SIEM system, as well as information output to the dashboard;
- The presence of a situation that is not so dangerous, and does not need urgent elimination and response. The alert does not require immediate attention, so it will be implemented only on the workplace monitor.

The response algorithm should be developed taking into account the following aspects of the company's work:

1. Sensors measuring water pressure in water pipes are placed at water supply and discharge sites, pumping stations;
2. There are automatically controlled valves for the supply or emergency shutdown of water in the city;
3. In the chambers and pumping stations within the radius of the placement of sensors, video surveillance of what is happening is conducted;
4. Any changes in the water pressure level are recorded and transmitted to the operator's workstation, after which the operator analyzes the surveillance cameras in the relevant areas and takes measures to eliminate the situation.

The developed algorithm assumes automating point 4, presented above. Until the operator finds the necessary sensor in the video surveillance system, examines the picture of the accident on the line, and then contacts the head of the emergency repair team, and until the employees arrive at the accident site, a long period of time will pass.

The Darvis system will allow you to automatically monitor these emergency situations and promptly respond to the resolution of the situation, depending on the actions laid down in the algorithm. For example, with a significant decrease in pressure, the system itself will display an image from the surveillance cameras of the area where the deviation from the norm occurred on the operator's monitor. In the case when the pressure in the pipeline has significantly decreased or has become zero at all, the system will determine this situation as a burst of the pipeline and immediately automatically take action to close the valves on this section of the line. Thus preventing damage caused to the city (blurring of roads, etc.), to individuals (flooding of the yard territory of private houses, causing harm to the health of passers-by, due to the release of a huge amount of water under high pressure, etc.), as well as the loss of a large amount of water for the organization itself. The above algorithm can be represented as follows (Figure 5).

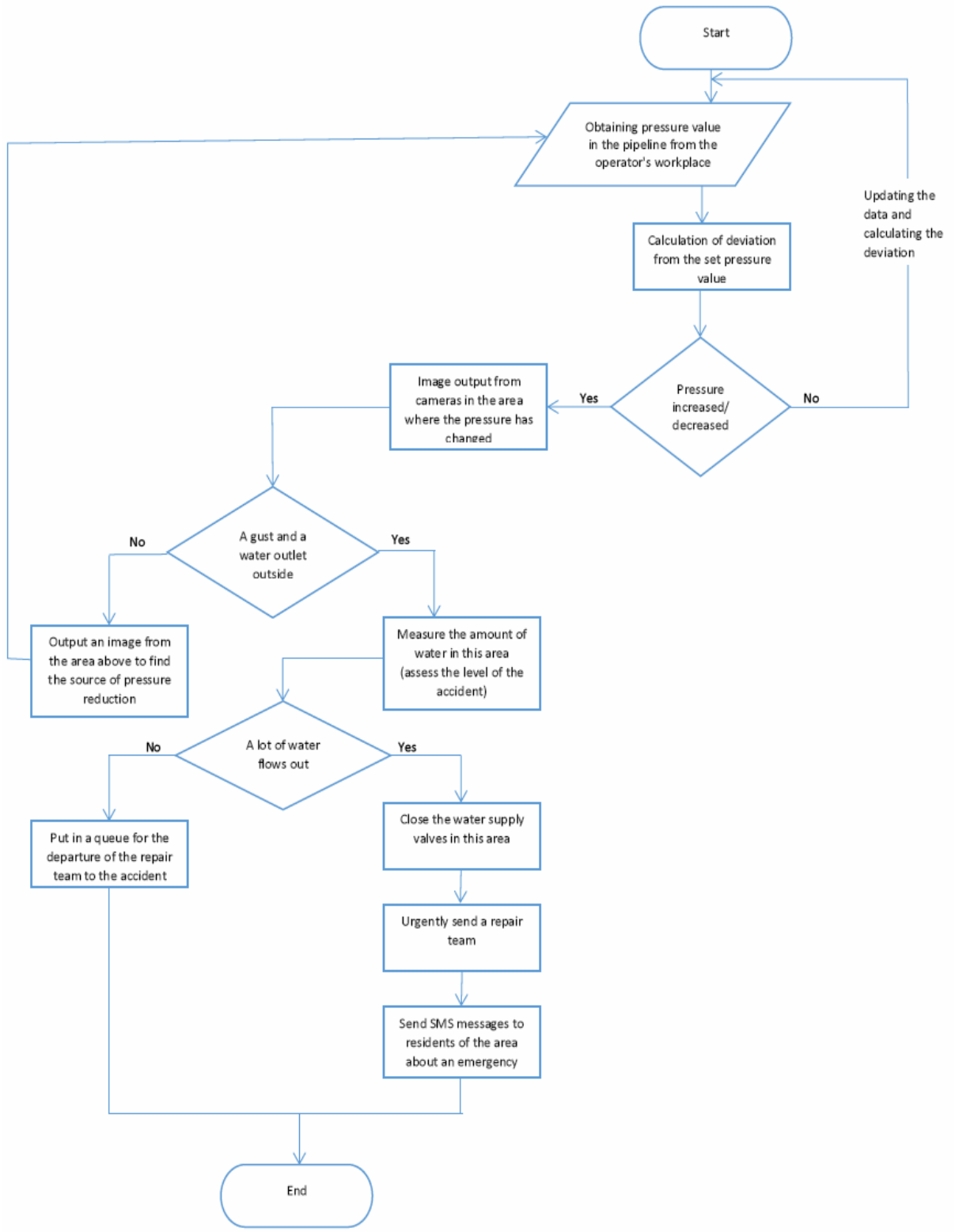

Figure 5: The general structure of the location of the physical security facilities of the water supply company

The work on the integration of the video surveillance system and the Darvis software will allow it to be used as a single platform for providing a comprehensive security system and rapid response to incidents. Rapid response to accidents in the water supply line or at pumping stations will reduce water losses, which will reduce material damage to the enterprise.

4. Acknowledgements

The work was carried out using the equipment of the Center for Collective Use of North-Caucasus Federal University with financial support from the Ministry of Science and Higher Education of Russian Federation, unique project identifier RF ---- 2296.61321X0029 (agreement no. 075-15-2021-687).

5. References

[1] Federal Law "On Industrial Safety of Hazardous Production Facilities" dated 21.07.1997 No. 116-FL.

[2] Elena Basan, Maria Lapina, Dmitry Orel. "Host-based Method and System for Detecting Anomalies in Network Traffic for a Robotic System". Proceedings of the Young Scientist's Third International Workshop on Trends in Information Processing (YSIP3 2019), Stavropol, September 17th to 20th, 2019; CEUR Workshop Proceedings Volume 2500, 2019.

[3] Guseva, T.M., Badun, A.A. Analysis of the problem of ensuring cybersecurity of industrial facilities based on SIEM systems. Innovation in the modern world: experience, problems and prospects for development. Collection of materials of the II International Conference, Ufa, 2020, pp. 61-67.

[4] Zolotukhin Alexey Vitalievich, Timokhovich Alexander Stepanovich. The principle of operation and the typical structure of information security event management tools. Academy. 2017. No. 10 (25). URL: https://cyberleninka.ru/article/n/printsip-raboty-i-tipovaya-struktura-sredstv-upravleniya-sobytiyami-bezopasnosti-informatsii.

[5] The Darvis platform. PSIM is a platform for managing and monitoring the security subsystems of an object. URL: https://darvis.pro.

[6] Calculation of water by pipe diameter and pressure: factors and methods. URL: https://strojdvor.ru/vodosnabzhenie/rascet-rashoda-vody/.

[7] Gonzalez-Granadillo, G., Menesidou, S.A., Papamartzivanos, D., Xenakis, C., Romeu R., Navaroo-LIobert D., Okoh C., Nifakos S., Xenakis C., Panaousis, E. "Automated cyber and privacy risk management toolkit". Sensors 21(16), 549, 2021. doi:10.3390/s21165493

[8] Orel, D. V., Zhuk, A. P., Zhuk, E. P., Luganskaia, L. A. A method of forming code sets for CDMA in communication, navigation and control systems. 2nd Young Scientist's International Workshop on Trends in Information Processing, YSIP2 2017; Dombai; Russian Federation; 16-20 May 2017; CEUR Workshop Proceedings Volume 1837, 2017, pp. 158-167.

[9] Rikhtechi, L., Rafe, V., Rezakhani, A. Secured Access Control in Security Information and Event Management Systems. Journal of Information Systems and Telecommunication 9(33), pp. 67-78, 2021.

[10] González-Granadillo, G., González-Zarzosa, S., Diaz, R. "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures". Sensors 21(14), 4759, 2021.

[11] Aleksandr Zhuk, Viktor Sazonov, Dmitrii Orel, Vladimir Pashintsev. Computer Modeling of Orthogonal in the Amplified Sense Signal. Atlantis Highlights in Computer Sciences, volume 3, 2019, pp. 215-217. doi: 10.2991/csit-19.2019.37.

[12] Aleksandr P. Zhuk, Dmitrii V. Orel, Igor A. Kalmykov, Andrey V. Studenikin. Improved Method of Formation of an Increased Number of Binary Quasi-Orthogonal Code Sequence Systems with the Required Statistical and Correlation Characteristics. Atlantis Highlights in Computer Sciences, volume 3, 2019, pp. 209-214. doi: 10.2991/csit-19.2019.36.

[13] Eswaran, S., Srinivasan, A., Honnavalli, P. A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise. Network Security 2021(4), 2021, pp. 7-16.

[14] Berdibayev, R., Gnatyuk, S., Yevchenko, Y., Kishchenko, V. A concept of the architecture and creation for siem system in critical infrastructure. Studies in Systems, Decision and Control 346, 2021, pp. 221-242.