

Ensuring Safety in the Automation of Equipment Monitoring

Trutnev Vyacheslav¹, Mingaleev Gaziz² and Babushkin Vitaliy²

¹ Abak-Service LLC, 159, Adelya Kutuya street, Kazan, 420073, Russian Federation
vtrutnev@abak-service.ru

² Federal State Budgetary Educational Institution of Higher Education “Kazan National Research Technical University named after A.N. Tupolev-KAI”, 10, Karl Marx Street, Kazan, 420111, Russian Federation
kafedra@eupkai.ru

Abstract. The article deals with safety issues that need to be addressed when working with monitoring systems when working on equipment at an industrial enterprise. The organizational and technical tasks that the monitoring system solves at industrial enterprises are outlined. The requirements for monitoring systems of equipment operating at an industrial enterprise in the conditions of industrial workshops are investigated. An approach to the boundaries of the monitoring system, including the project documentation used in the implementation of the system, is formed, and attention is paid to the graphic part. The issues of the technical part and the software component of the monitoring system are taken into account. The ways of user interaction with the monitoring system are shown, including user authorization and authorization on the server. Special attention is paid to the information flows formed in the system, which allows you to form restrictions on access to the system by unauthorized persons. The indicators used in the monitoring system are given.

Keywords: Enterprise automation, Production planning, Production monitoring.

1 Introduction

1.1 A Subsection Sample

The main task of the equipment operation monitoring system is to independently fix the equipment useful operation time and the ability to control the equipment operation efficiency in an automated mode without human intervention. The second task of the monitoring system is to collect statistical data on the causes of equipment downtime and makes it possible to analyze the causes of productivity losses, develop and im-

* Copyright © 2021 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

plement corrective measures to eliminate them [1-3]. The third task is analytical support in making operational decisions on the management of production processes [4-7].

Functioning in the infocommunication network of an enterprise, the security requirements for the monitoring system used become more important [4; 7-10].

2 Materials and methods

Among the main requirements for software and hardware systems for planning and monitoring production processes, the following can be distinguished:

- The monitoring system software must be located on the enterprise server;
- The server part of the monitoring system must be located on the servers of the enterprise;
- The monitoring system should be able to distribute access rights among employees;
- The total number of users connected to the system should not be limited;
- Data should be accumulated on the server without overwriting the previously recorded ones. The data must be stored indefinitely;
- The system should return the requested data upon request from the client application or from the web client.

Also among the requirements are real-time monitoring and possible integration with other enterprise systems.

3 Results

Computer equipment and critical network equipment should be placed in lockable cabinets that restrict access to unauthorized persons; when the doors of the industrial and technological complex cabinets are opened, an alarm should be displayed at the operator's workplace. System blocks of Automated Work Places (AWPs) of operators should be placed in lockable cabinets.

Firewalls must be provided at the border of machines with a Data Exchange Server (DES). As a firewall, a specialized software and hardware FireWall (FW) should be used that controls all information exchange with the DES. Only the ports and services required to access these machines should be open on the firewall. All other ports and services must be blocked.

A demilitarized zone must be applied between the machines and the Local Area Network (LAN).

Direct access from the corporate network to the LAN of the machines should be excluded - access should be carried out only through the DES (the machines must transmit data by referring to the DES). The rules for adjusting the FW must be agreed and documented.

On the LAN of machines, the following should be prohibited:

- remote access to machine tools for technical support of system and applied software (SW);
- access to machine tools from public information networks, for example, the Internet;
- Internet access services and e-mail;
- direct access to the corporate network.

During implementation, specialists need to provide all the necessary equipment (including cabinets, cables) and software for transferring parameters from machines to the monitoring center. The list of parameters that need to be transferred are developed at the stage of collection of initial data and are agreed with the specialists of the enterprise.

The section of the project documentation on information security should contain:

- description of the object of protection;
- information security threat model;
- model of a potential illegal intruder;
- description of the technical means complex;
- solutions for ensuring information security, including solutions for access control, security audit, protection of machine storage media, ensuring integrity, ensuring availability, anti-virus protection, protecting the automated system and its components, etc.;
- specifications of equipment and software for the information security subsystem.

All decisions must be sufficient and justified in accordance with the results obtained in the process of analyzing current threats to information security and potential illegal intruder.

The graphic part of the section should include:

- structural diagram of a technical means complex for information protection, superimposed on the corresponding diagrams of the information and technological infrastructure of the object, communication systems, etc. The diagram should clearly highlight the computer equipment and information security equipment installed or modified within the framework of the project;
- diagram of information interaction of machine tools with external systems;
- diagram of the functional structure of the information security subsystem.

As a result, the main requirements for the safety of the industrial equipment monitoring system were formulated.

4 Discussion

Ensuring safety when working in the equipment planning and monitoring system is carried out in the following three areas.

- 1) User (client) authorization:

- Only a user (client) with an MS Windows account and access to the enterprise information network can start the Dispatcher's AWP;
- The user works only with the interface of the Dispatcher's AWP, which does not have any functionality to influence the operation of both equipment and the monitoring system;
- In the basic configuration, user authentication is disabled. If an unauthorized person has access to the user's computer, the Dispatcher's AWP can be launched;
- If user authentication is enabled (with an MS Windows account), when starting the Dispatcher's AWP, the client's rights to work with the monitoring system are checked, and in the absence of such rights, access to the Dispatcher's AWP is not possible;
- To work with the monitoring unit, the operator must be authorized, while he has no opportunity to influence the operation of the equipment through the monitoring system.

2) Server authorization:

- Only the system administrator has access to the server;
- When working with the Dispatcher's AWP, the user (client) has no opportunity to influence the operation of both the equipment and the server;
- Only monitoring services operate on the server, which are not able to influence the operation of the equipment.

3) Information flows in the monitoring system:

- The information flow from the server to the machine is a request for the state of the equipment using the library of the equipment control system without the possibility of controlling the equipment;
- The information flow from the machine to the server is the response to the system's request for the equipment status;
- The information flow from the monitoring unit to the server is the result of the operator's actions on the monitoring unit (authorization, entering the reason for downtime, etc.) without the possibility of controlling the equipment;
- The information flow from the server to the monitoring unit is confirmation or non-confirmation of operator authorization;
- The information flow from the Dispatcher's AWP to the server is one request (at the first start of the Dispatcher's AWP) about the state of the equipment in real time without the possibility of controlling the equipment and a request for generating a report;
- The information flow from the server to the Dispatcher's AWP is the result of a change in the state of the equipment in real time and a response to a user's request for generating a report. Set-up takes quite a long time, which is 30 % of the total time, or more than half of the processing time. Consequently, reducing the time of production losses when setting up equipment can significantly increase the proportion of processing.

The general diagram of data transmission in the system is shown in Figure 1.

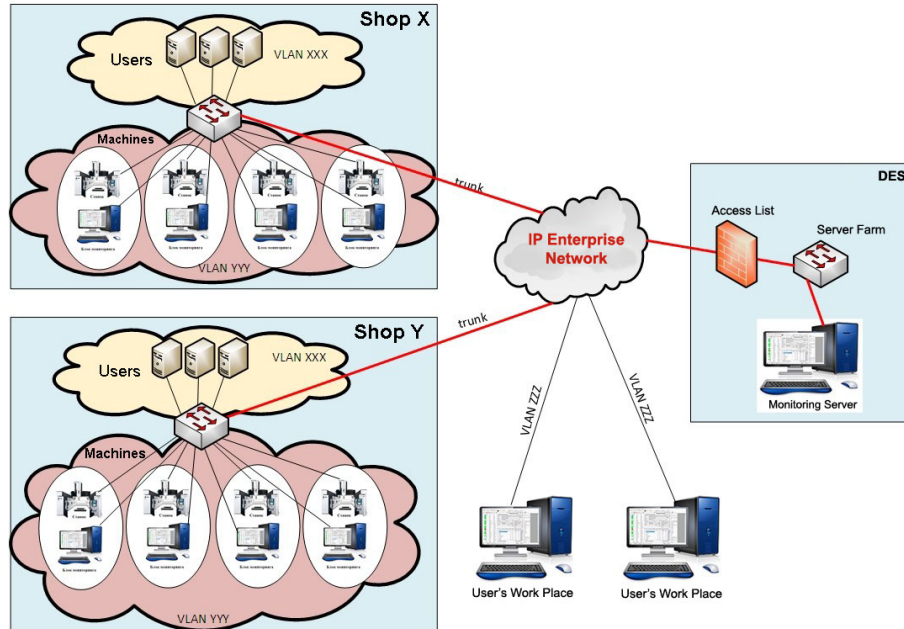


Fig. 1. Data transfer diagram in the equipment monitoring system.

Noting the data transfer structure shown in Figure 1, the parameters of the generated indicators, summarized in Table 1, should be highlighted.

The values of the indicators indicated in Table 3 allow to generate various tabular and graphical reports indicating the dynamics of key values. From the values of technological modes (feed, speed), economic indicators are identified, which are set individually for each type of equipment.

5 Conclusion

If the safety requirements of the equipment monitoring system are met, the managers and specialists of the enterprise receive objective data for making management decisions.

The management assesses the Overall Equipment Efficiency (OEE), monitors the dynamic indicators of the equipment efficiency, receives data on the onset of a condition or violation of technological modes (sms, e-mail).

The technological service receives data on the equipment operation for the selected period in the context of production-equipment-operator-detail-operation-modes of processing-machine time-reasons for stops-program frames-tool, which was used for processing. In addition, it is possible to track the change in the NC program, the duration of stops during NC execution, the NC execution time, pauses between NC starts, program blocks.

The equipment maintenance service is promptly informed about the number, type and frequency of equipment breakdowns.

Table 1. Indicators' parameters and their statuses.

| Indicators' parameters | Status |
|--|--|
| Parts processing time | Work on the program Manual operation |
| Planned downtime | Lunch Personal needs |
| Unplanned downtime | |
| 1) Downtime due to setup | Adjustment / Installation Correction of the control program Cleaning the machine Working with a technologist Quality control department check Control measurements by the operator |
| 2) Downtime | Machine downtime Waiting for the slinger Lack of control program Waiting for a decision on the defect Lack of detail Cycle (service state) Machine stopped The program is over Machine is on |
| 3) Downtime due to repair | Failure Waiting for repair Unplanned repair Planned repair |
| 4) Downtime due to assembly or lack of tools | Assembling the tool Lack of tool |
| 5) Lack of work shift | Lack of work shift The machine is switched off without giving any reason |
| Amending of defects | Amending of defects |

References

1. Valitov S.M., Mingaleev G.F., Khadeev N.R., Antonova N.V.: Methods to assess economic loss while implementing energy saving programs in oil-production enterprises. Mediter-ranean Journal of Social Sciences, 6(3), 766-769 (2019).

2. Shleymovich M.P., Medvedev M.V., Lyasheva S.A.: Contour segmentation based on image points energy estimation in object and processes control systems. 2017 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017 - Proceedings, 8076422 (2017).
3. Nadreeva L., Gaynutdinova J., Rakhimova G.: Productivity and motivation of employees in the services sector. Proceedings of the 27th International Business Information Management Association Conference - Innovation Management and Education Excellence Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA 1211-1219 (2016).
4. Snegurenko A.P., Sosnovsky S.A., Novikova S.V., Yakhina R.R., Valitova N.L., Kremleva E.Sh.: Using E-Learning Tools to Enhance Students-Mathematicians' Competences in the Context of International Academic Mobility Programmes. Integratsiya obrazovaniya = Integration of Education, 23(1), 8-22 (2019).
5. Bikhullin A.L., Pavlov B.P., Zufar K.K.: Analyzing accuracy and sensitivity in forecasting at the variant level. Espacios, 38, 49, 9 (2017).
6. Shleymovich M.P., Medvedev M.V., Lyasheva S.A.: Object detection in the images in industrial process control systems based on salient points of wavelet transform analysis. 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016 - Proceedings, 7911633 (2016).
7. Nadreeva L., Abramov V.: Problems and directions for improving labor rating. Proceedings of the 30th International Business Information Management Association Conference, IBIMA 2017 - Vision 2020: Sustainable Economic development, Innovation Management, and Global Growth, 1184-1190 (2017).
8. Bakeev M., Nikolaeva A., Safargaliev M., Garifullin R., Nefedova J.: Factors of corruption on the firm level Influence of level of development of innovative potential of region on results of innovative activity. Proceedings of the International conference "Economy in the modern world", 17-22 (2018).
9. Butov G., Nadreeva L., Abramov V.: Digitalization and digital transformation of human resource management in Russia. Proceedings of the 33rd International Business Information Management Association Conference, Education Excellence and Innovation Management through Vision, 1514-1520 (2019).
10. Lyasheva S., Shleymovich M., Shakirzyanov R.: The Image Analysis Using Fast Radial Symmetry Transform in Control Systems Base on the Computer Vision. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2019, 8934298 (2019).
11. Dmitriev O.N., Novikov S.V. Optimizing the economic information transparency level of high-tech enterprises in the post-industrial globalized economy. Moscow (2019).