Volume 1, Issue 7, October 2023 **ISSN(E):** 2938-3773

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3

INFORMATION INTEGRATIONS AND INFORMATION SECURITY ISSUES IN INDUSTRIAL AUTOMATION SYSTEMS IN INDUSTRY 4.0

B. O. Djalilov,
M.A. Tursunaliyev
Fergana Branch of Tashkent University of Information Technologies, Fergana, Uzbekistan

Abstract
This article analyses the issues of information security of technological process automation systems widely used in industrial enterprises, the vulnerabilities of such systems, and the risks and threats to them.

Keywords: TJABT, information security, cybersecurity, rootkit.

Introduction

The issue of information security has a special place, especially for automated process control systems (TJABT), i.e. industrial automation. This is because, unlike other industries, such as banking and finance, education or e-services, industrial automation systems are cyber-physical systems. And any potential security breaches in these systems are not just the disclosure of confidential information or the loss of this information to third parties, but the cessation of production, equipment failure, and damage to human health and the environment. as important as real physical risks. Therefore, when it comes to information security in industrial computer networks, especially in TJABT, it is appropriate to use the term “cybersecurity” rather than just the term “information security”.

In the era of Industry 3.0, based on the widespread use of computer technology in the industry, as well as automation tools, the issue of cybersecurity for industrial automation has reached a critical point. This is because the introduction of computer and network technologies in such systems has opened the door to great opportunities for malware developers (hackers) and malicious people who use their services. Threats such as making wax money with the threat of disrupting a particular technological process through external computer attacks, or stealing important technological information about the process (for example, trade secrets) have played a key role. Therefore, especially after the 2000s, when the era of large-scale computerization of the industry began, the issue of information security in TJABT became one of the main issues on the agenda for professionals in this field.

However, during Industry 3.0, there was a very simple, yet 100% guaranteed solution to ensure information security in systems directly used in production: at that time, almost all enterprises operated TJABTs in complete isolation, and the computer network and processors of TJABT in a particular production shop had no contact with the world. For TJABT specialists in enterprises, not only the connection of the system to the global Internet but also the connection to the internal IT perimeter, organized for the accounting, personnel department and administrative services of the enterprise, was absolutely unacceptable and strictly prohibited.

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3

Therefore, even the TJABTs of technologically interconnected shops within an enterprise operated individually, without integration with each other. To ensure more reliable information security in TJABT, radical measures were taken in some categories of hazardous production facilities, such as physically disabling or completely removing all external communication interfaces of computers - USB ports, network cards and so on iron curtain ”method) [1].

The Main Part

However, the era is changing, and now, in the new era of Industry 4.0, which began around 2010, logic-based programmable controllers (PLCs), FTE-type computer networks, touch panels providing HMI interfaces, and industrial computers based on traditional TJABT architecture in addition, it requires the use of industrial product Internet (IIOT), artificial intelligence, large-scale data (BigData) and tools for integrated integration with the outside world in general. This need is due not only to the production process itself but also to the introduction of modern automation systems (such as MES / ERP) in business management.

In such systems, first of all, by integrating TJABTs in all production shops within one enterprise, they are combined into a single network, and a centralized dispatching system (MES) is established between them. Based on it, enterprise resource management is automated (ERP). This includes the integration of production resources (staff, fixed assets, raw materials and energy resources), as well as financial reporting, production, logistics, capital turnover cost planning and other issues. The final stage of business management automation will cover the highest level of strategic management and management of the enterprise (BPM). Later, a wider scale of such integration will continue, for example, with the mutual cyberintegration of related enterprises that are part of a single holding, and the integration architecture will now form a unique pyramid (Figure 1).

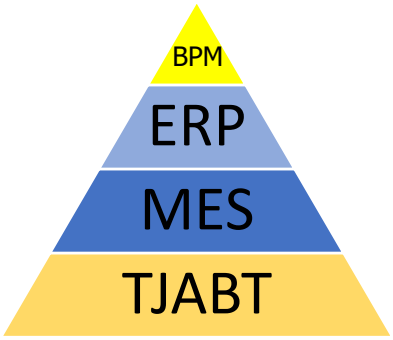

Figure 1. Automated business management pyramid

Thus, large-scale integration processes now, whether we like it or not, necessitate the "shadowing" of cyber-physical systems, i.e. TJABTs, which are the basis of this hierarchy and have worked so far in isolation. Integration requires that TJABTs leave no choice but to connect the enterprise first to the IT perimeter and then to the global Internet. Because the basic production data for the formation of financial statements is obtained from TJABT and MES systems, the system of internal financial reporting and financial operations will be integrated with the information networks of banking, finance and tax authorities, the global logistics system will operate through the global Internet. This, if cybersecurity is not properly organized,

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3

will technically allow criminals to infiltrate the cyber-physical system TJABT via the Internet and launch malicious activities, the most important and serious step in this hierarchy.

Because the basic production data for the formation of financial statements is obtained from TJABT and MES systems, the system of internal financial reporting and financial operations will be integrated with the information networks of banking, finance and tax authorities, the global logistics system will operate through the global Internet. This, if cybersecurity is not properly organized, will technically allow criminals to infiltrate the cyber-physical system TJABT via the Internet and launch malicious activities, the most important and serious step in this hierarchy. Given that, for example, each of the IIOT sensors is an independent device with its IP address, this aspect, example, will become a target for those involved in mining. Because, firstly, the industry uses a very large number of sensors (that is, their number is large, which means that there are many independent network devices with their unique IP address), and secondly, because most industrial enterprises operate in continuous mode, such devices will be in a continuous network over time (months or even years) and this is exactly the aspect that seems extremely attractive to miners. As a result, the miner, who managed to infiltrate the TJABT network, will be able to use the resources of all IIOT sensors in it to work for their own benefit. And the possibility of using TJABT resources for this type of mine is just one of the threats to industrial automation.

Since integrated integration and the transition to Industry 4.0 are inevitable and have already begun, this process means that TJABT professionals will now have to abandon previous methods, such as the “iron curtain method” of cybersecurity at TJABT, and be prepared for new challenges.

To do this, first of all, it is necessary to be well aware of the weaknesses of the TJABT itself and to understand how it attracts the wicked.

First of all, it should be noted that TJABT contains the most important technological information for the enterprise. Such data include, first of all, the consumption of raw materials and energy resources per unit of output and the cost formed on their basis, the norms of the technological regime, the level of safety (SIL) to prevent accidents at work, confidential documents and cases. Such information is primarily of interest to those involved in industrial cyber espionage and is primarily sought to be acquired by competitors, commercial firms, or large and small licensors. The second aspect was also mentioned above: TJABT usually works continuously and this seems to be attractive for those who want to use its resources mainly for mining purposes. In addition, there are cases of the realization of geopolitical goals by infiltrating the technological network of large strategic industrial enterprises and disrupting the production process. The first major industrial cyber espionage was caused by the Stuxnet virus in 2010 and the resulting accident was aimed at just such a goal. At that time, as a result of a well-prepared ART attack, uranium enrichment processes at Iran's Bushehr nuclear power plant were disrupted and the country's nuclear program was disrupted. Currently, this cyberattack has already become a "classic example" of the risks posed to the TJABT network of industrial enterprises [2].

In all of these potential threats to TJABT, pests will inevitably take advantage of one or a vulnerability in the system. It is worth noting that the Stuxnet virus, which led to the temporary suspension of Iran's nuclear program, even managed to penetrate a technological network that

is not connected to the Internet and has no connection to external networks at all. The illiteracy and negligence of the staff of this facility on information security played an important role in this, as Stuxnet Busher accessed the control computers of the NPP via a USB flash drive [3]. This fact indicates that in order to ensure cyber security in TJABT, it is first necessary to increase the awareness of employees about information security and to form a culture of cybersecurity in the community. It should also be noted that Stuxnet-type viruses are not actually viruses that spread freely on the Internet and infect computers en masse. They are distributed by technically well-trained and well-funded ART gangs, and this type of cyberattack is targeted. This is why such cyber weapons can skillfully mask themselves in the system and do not reveal malware activity for long periods. This is why experts call such pests rootkits, and Stuxnet is a typical example of this. When the Stuxnet rootkit entered the Busher AES technological network, it made changes to the engine speed control commands. As a result, the engines began to rotate at speeds exceeding their specified limits, although this was not noticed by the process control operators at all. This is because this rootkit is also designed to distort the indication of the number of revolutions of the engine, and the process is displayed on the operator's screen in the same mode as before. As a result, the motors were initially overheated due to very high speeds, resulting in higher amperage current consumption. When the cooling system broke down, the process failed and the reactors had to be shut down. In general, the share of TJABT damage through portable data sources (USB flash drive, external HDD disk) is 5.2% of the total number of incidents. Although the number may seem a bit small, as mentioned above, this method is usually used mainly by ART gangs, so the cases of large-scale damage are also in this direction.

Another potential threat to TJABT is of course the risk factors posed by the system’s internet connection. According to a study by Kaspersky Lab, in the first half of 2021, 39% of TJABT computers infected with this or that pest were infected with the pest from the Internet. Another 3.4% of TJABT computers were infected with e-mail applications. While most of these failures do not aim to disrupt the technological regime, as in the Stuxnet rootkit, they still present very unpleasant problems for system engineers. This is mainly aimed at those behind the malware, such as mine, data encryption and encryption (extortion), compensation for non-disclosure of confidential information (again extortion) and, in most cases, industrial cyber espionage.

Conclusions

In order for such criminals not to achieve their goals in the system, it is necessary to ensure that they do not enter the system in any way and to take all necessary organizational and technical measures. In order to solve these problems, of course, on the basis of a scientific approach, it is expedient to develop technical solutions that do not physically allow to penetrate into the TJABT.

References:

1. Kasimov M.M. (2020). Challenges of cyber threats in automation systems of industrial enterprises and measures to protect against them. Collection of scientific articles on the results of the international scientific conference "Priority directions of innovative activity in industry". Part 1. pp. 55-57. Kazan: Envelope LLC.

2. https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and-detection-methods/#id7. pp. 55-57. Kazan: OOO “Envelope”.
3. https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and-detection-methods/#id7.
4. Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, symantec corp., security response, 5(6), 29.
5. Grigoriev, A. D., & Djalilov, B. O. (2017, February). Electrically tuned antenna for 4G mobile communication. In 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 151-154). IEEE.
6. Djalilov, B. O. (2022). Use of pesoelectric effects in in measurement technology. International Journal of Advance Scientific Research, 2(12), 145-148.
7. Zikirov, M. C., Qosimova, S. F., & Qosimov, L. M. (2021). Direction of modern design activities. Asian Journal of Multidimensional Research (AJMR), 10(2), 11-18.

Web of Discoveries: Journal of Analysis and Inventions
webofjournals.com/index.php/3