Technological independence and safety of software for automated process control systems: analysis and recommendations

E.K. Arakelyan1*, A.A. Kosoy2, and K.P. Guseva1

1 National Research University Moscow Power Engineering Institute, Moscow, Russia
2 Joint Institute for High Temperatures of the Russian Academy of Sciences, Moscow, Russia

Abstract. The current analysis examines two important aspects of SW PCS software: process independence and process safety. Process independence refers to the flexibility and versatility of the system, which allows it to integrate easily with different technologies, devices and software. This allows organisations to choose from a wide range of hardware and software modules and ensures compatibility with other control systems. Technology security includes measures to protect the system from security threats and breaches such as data protection, user identification and authentication, access control, etc. It is recommended to conduct regular security audits and keep track of system updates and vulnerabilities. The analysis highlights the need to pay attention to the criteria of technological independence and technological security in the development and operation of SW PCS and recommends further research and exchange of experience in this area.

1 Introduction

The independence criterion in the context of SW PCS can refer to the ability of an individual country to fully control or implement the full life cycle of software for automated process control systems (PCS) without dependence on foreign suppliers. This includes software development, maintenance, upgrades and security. Considering the independence criterion in this context, a country seeks to ensure technological sovereignty in the PCS sphere, which implies sustainability and independence in the face of geopolitical risks.

The Russian Federation has the ability to control and make decisions regarding the development, use, as well as updating and maintenance of PCS software in accordance with national interests and requirements without interference (both positive and negative) from foreign actors. In general, the independence criterion refers to the desire to ensure control over PCS technological solutions in order to ensure safety, reliability, and respect for the country's national interests. The criterion of technological independence in SW PCS refers to the ability of the system to work with different technological objects, devices and software. This criterion implies the ability to integrate and interact with different devices and systems, such as controllers, sensors, actuators, and other elements used in the process control process. Within SW PCS, the technology independence criterion establishes the requirements for the

* Corresponding author: kosoyanatoliy@yandex.ru
system to be able to work with many different technologies, communication protocols and data formats. This includes the ability to communicate with different types of equipment and control systems, regardless of which technology standards or protocols are used. The criterion of technology independence also includes the flexibility and versatility of the system with respect to software. The SW PCS needs to be able to work with different operating systems, databases, software modules and development tools to allow freedom of technology choice and the ability to integrate with other systems. The main benefit of the technology independence criterion is to ensure that the SW PCS is flexible and scalable. This allows the system to easily adapt to changing requirements and operating conditions and integrate with new technologies and control systems. The criterion of technological independence should be an important aspect of SW PCS development as it guarantees flexibility and the ability to integrate with different technical solutions. This allows organisations to use a variety of hardware and software and to ensure compatibility and interoperability between different control systems.

The criterion of technological independence focuses on the ability of SW PCS to work with different technological objects and control systems. It defines how flexible the system is and how it is able to integrate with different types of hardware and software, regardless of the technology standards or protocols used. The criterion of technological independence allows the system to be versatile and easily adaptable to different requirements and operating conditions. On the other hand, the criterion of technological safety refers to the security of the SW PCS system. It includes measures and procedures to protect the system from security threats and breaches, and to ensure confidentiality, integrity and availability of data. The technological security criterion covers aspects such as user identification and authentication, access control, data encryption, malware protection and other measures necessary to ensure system security. Thus, the main difference between the criterion of technological independence and the criterion of technological security is that the former focuses on the flexibility and the ability to integrate the system, while the latter focuses on securing and protecting the system from threats and security breaches. Both criteria are important for the development and operation of SW PCS and should be considered in the design and implementation of the system.

2 Main part

The following criteria were considered for the initial assessment:

2.1 Standardisation criterion (Standards and protocols)

Software should be developed using open standards and protocols so that it can be quickly ported to different platforms without loss of functionality. In addition, the code should be structured and easy to understand for developers to be able to analyse and counter vulnerabilities.

Protocols are an important aspect of software and network standardisation. They are a set of rules, procedures and formats that set standards for data exchange and communication between computers or systems. The standardisation criterion evaluates the protocols that are used by the software vendor. Protocols can relate to various aspects including communication, security, management, routing and others. Let us consider a few important protocols in different areas of standardisation:

1. Network Protocols: Network protocols define rules for data exchange and communication between devices on computer networks. Some of the important protocols include IP (Internet Protocol) for routing and delivering information over a network, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) for
ensuring reliable or unreliable delivery of data, and DNS (Domain Name System) for translating domain names into IP addresses.

2. Internet of Things (IoT) protocols: IoT protocols enable communication and data exchange between devices within the Internet of Things. Some of the popular protocols include MQTT (Message Queuing Telemetry Transport) for low latency and low power messaging, CoAP (Constrained Application Protocol) for data transmission to limited devices and Zigbee for short distance wireless communication.

3. Security Protocols: Security protocols are used to ensure confidentiality, integrity and authentication of data. Some of the common protocols include SSL/TLS (Secure Sockets Layer/Transport Layer Security) for secure data transmission over the Internet, IPsec (Internet Protocol Security) for securing IP connections, and SSH (Secure Shell) for secure remote access to the system.

4. Management Protocols: Management protocols are used to manage and control network devices and systems. Some of the important protocols include SNMP (Simple Network Management Protocol) for monitoring and managing devices on the network, HTTP (Hypertext Transfer Protocol) for accessing web interfaces and managing remote devices, and SSH and Telnet for remote management of servers and network devices.

![Typical PCS digital exchange diagram](image)

**Fig. 1. Typical PCS digital exchange diagram**

5. Specific protocols in the field of PCS. OPC (OLE for Process Control), Modbus, PROFIBUS, DNP3 (Distributed Network Protocol, IEC 61850) play an important role in enabling communication and data exchange between the various components of a control system.

6. It is important to assess the extent to which the software vendor adheres to these protocols and follows the standards set by the industry.

### 2.2 Diversification criterion (Supplier Independence)

Software and its individual components should imply "module flexibility". That is, the software should be designed so that it can be easily replaced without significantly affecting the functionality and operation of the system as a whole. Module flexibility allows changes to be implemented quickly and efficiently, new features to be added or bugs to be fixed without disrupting other modules and ensuring continued system performance so that...
ultimately, the developer has the freedom to choose between different vendors and can easily move from one vendor to another without having to completely replace the system. This will help to avoid vendor-specific dependency and the associated risks. But on the other hand, it is also necessary to determine the optimal number of interchangeable software products from independent developers, so that the reverse problem of too much software from different vendors within one PCS does not arise. It is important to analyse and assess the functional needs of the system to determine the most necessary software functions and components. Then, the aim should be to select and purchase software from reliable vendors that can provide all or most of the required functionality. It is also worth paying attention to the compatibility of software from different vendors, preferably selecting software that can easily integrate and exchange data with other system components. It is also important to ensure that software from different vendors is supported and maintained on a long-term basis to ensure the stability and reliability of the system. And as mentioned earlier, it is imperative that standardised protocols and interfaces are available to ensure interoperability and data exchange between software components from different vendors.

### 2.3 Relevance criterion (Regular updates)

This criterion refers to an assessment of how well the software supports current requirements and technology standards, and how well it meets current needs. Software should be regularly updated and supported by developers. Updates should include fixing vulnerabilities and adding new features, as well as being easy to install and migrate. The PCS developer should be able to easily obtain updates and support without having to completely reinstall the software, as this is precluded by the nature of real-time process control systems.

An up-to-date SW PCS must be capable of providing effective control and monitoring of various process flows and be compatible with other systems and components. It should have the ability to exchange data, integrate and interface with other systems in the PCS such as SCADA (data acquisition, monitoring and analysis system), automatic regulation and control systems (PLCs, controllers, etc.).

However, the relevance of SW PCS is not only limited to compatibility and data exchange. It is also related to technological innovations such as the use of artificial intelligence, data analytics, machine learning and Internet of Things (IoT) principles and techniques. A relevant SW PCS can offer new functionality, improve the efficiency and reliability of management processes, and facilitate data-driven decision-making and analytics. Evaluating the relevance of SW PCS includes analysing functional requirements, capabilities to support current technologies, reviewing the market and feedback from other users, and assessing the scalability and flexibility of the system for future development and upgrades. Overall, the relevance criterion helps to select and implement a SW PCS that meets current technologies and requirements, and ensures long-term effectiveness over the entire PCS lifecycle.

### 2.4 Privacy criterion (Data protection)

The software should provide a high level of protection for user data, especially important for PCS. This includes data encryption, access control and authentication, and backup and recovery mechanisms. In addition, the software should be designed to meet current security standards and follow the recommendations of industry organisations. The software must comply with a number of measures to protect data confidentiality, including various technical and organisational measures that aim to prevent unauthorised access, modification and leakage of information. As part of this criterion, mechanisms for user authentication and authorisation shall be established. Authentication implies verification of user authenticity,
and authorisation defines and controls access rights to the system functionality. This will avoid unauthorised access to the NPP PCS system. Another important measure to ensure confidentiality is data encryption. Encryption is used to protect transmitted and stored data from unauthorised access or reproduction. The use of cryptographic algorithms allows data to be encrypted in such a way that only authorised users will be able to decrypt the information. Access control mechanisms play an important role in ensuring confidentiality. SW PCS should have mechanisms to create, allocate and control different levels of access for users. This approach ensures that each user has access only to the information and functionality of the system that is appropriate to their role and responsibility within the management of the system.

2.5 Audit criterion (Audit and monitoring)

The software should include auditing and monitoring mechanisms to track system usage and changes. This will help detect misuse and attacks and prevent data leakage. Audit and monitoring logs should be protected and available for analysis only to authorised persons. The criterion aims to monitor and control user actions and ensure data integrity. The audit criterion includes a number of measures and procedures that allow recording, analysing and monitoring all events and activities occurring in the NPP PCS system.

One of the main aspects of the audit criterion is the recording of events and user actions. The NPP SW PCS should be able to record all important events such as user logins and logouts, changes in system settings, access to sensitive data and other activities that may have an impact on the security and operability of the system. Audit records contain date, time, user and action information, which allows for subsequent analysis and identification of potential security threats or issues. An important aspect of the audit criterion is the analysis of the data obtained from the audit records. This process involves searching for and identifying anomalies, unusual or potentially malicious activities. Audit analysis helps to identify situations that may pose a threat to system security or indicate a breach of security procedures. In addition, the audit system provides for independent verification and analysis of audit data. Independent verification enables the detection or confirmation of vulnerabilities, bugs, or security violations, and verifies that security procedures comply with requirements and regulations. Criterion shall verify that the software complies with the above requirements and ensure that all activities and events are recorded and analysed. This helps to identify and prevent potential threats or security breaches, as well as ensure data integrity and compliance with security requirements and regulations.

3 Conclusion

Two important aspects of SW PCS have been considered in the analyses performed: the criterion of process independence and the criterion of process safety. Both criteria play an important role in the design and operation of a process control system.

By investigating the criterion of process independence, it was shown that the flexibility and versatility of the system allows it to be easily integrated with different technologies, devices and software. This provides developers and designers with a wide range of hardware and software modules to choose from, as well as compatibility and interoperability with other control systems. It is advisable to ensure, at the PCS design stage, that the system fulfils the requirements of process independence and can easily adapt to changes. Regarding the criterion of technological security, it has been shown that software security plays an important role in protecting against threats and security breaches. Data protection, user identification and authentication, access control and other security measures should be implemented to ensure the safe operation of the system. It is recommended to conduct regular
security audits and keep an eye on system updates and vulnerabilities to protect the system from new threats. However, the analyses performed are only the beginning and further research into SW PCS is recommended. It would be ideal to study the experience of different technologies and management systems, and to analyse current technology trends and standards that may influence the design and operation of the system. It is also worth paying attention to the development of new approaches and tools to ensure technological independence. Further research into the development and application of innovative methods and algorithms to secure SW PCS systems is also recommended. This may include research into threat identification and analysis, development of new encryption and authentication methods, and setting up systems to monitor and respond to possible attacks. It is also recommended that you research the experiences of other organisations working in process automation and share knowledge and best practices with peers and experts in the field. This will provide valuable information and experience that can be applied to the development and operation of SW PCS. Future research should also focus on changes in legislation and regulatory standards relating to security and data protection. Compliance with relevant regulations and requirements is an important aspect of the development and operation of SW PCS. Finally, it is also important to take into account the changes in information security in general. The rapid development of technology and the emergence of new threats require that SW PCS security measures are constantly updated and adapted. Therefore, it is recommended to follow the current trends and the latest research in the field of information security and apply them practically to ensure reliable and secure operation of the system. Overall, the analyses conducted lead to the conclusion that it is necessary to pay special attention to the criteria of technological independence and technological security in the development and operation of SW PCS, and to continue researching and following developments in this area. This will help to ensure efficient and safe operation of the process control system.

References

5. V.V. Samsonov, D.G. Zagumennov, Vestnik IrSTU 11(107), 92-99 (2019)