Universal Library of Engineering Technology
Research Article

ISSN: 3064-996X | Volume 2, Issue 3

Open Access | PP: 89-93

DOI: https://doi.org/10.70315/uloap.ulete.2025.0203016

Methodology for the Implementation and Operation of Multivendor Automation Systems at Large-Scale Industrial Facilities

Chata Marat Muratuly

New York, USA.

Abstract

In the context of the Fourth Industrial Revolution (Industry 4.0), ensuring the interaction of equipment and software products from different vendors at large-scale industrial facilities becomes an important element for increasing operational efficiency and sustaining competitive advantages. This study is aimed at forming and methodologically substantiating a comprehensive approach to the implementation and operation of multivendor automation systems. The main objective is to propose a unified mechanism for integrating heterogeneous components that reduces risks associated with incompatibility, cyberthreats, and unwarranted operational costs. The methodological basis of the work relies on a systematic analysis of recent scientific literature, the comparison and application of international standards, in particular IEC 62264, as well as an empirical investigation of a practical case involving the creation of an integrated infrastructure at a strategically significant facility—the company Қазақстан Ғарыш Сапары. As a result, a phased methodology has been developed that covers pre-project surveying, the selection of an architecture based on a service-oriented approach (SOA), the unification of data-exchange protocols (OPC UA, MQTT), and the development of a strategy for managing the system life cycle. The scientific novelty lies in the proposal of an adaptive model for managing integration projects that takes into account both the specific features of industrial sites and the accelerated dynamics of technological transformations. The materials presented in the article possess practical value for system architects, automation specialists, managers of manufacturing enterprises, and experts in industrial cybersecurity.

Keywords: *Multivendor System, Industrial Automation, Industry 4.0, System Integration, IEC 62264, OPC UA, MQTT, Industrial Control System Cybersecurity, System Life Cycle, Interoperability.*

INTRODUCTION

In the context of the rapid digital transformation of the industrial sector, enterprises are faced with the task of deep re-engineering and modernization of existing automated process control systems (АСУ ТП). The expansion of global markets and the shortening of technology life cycles make the use of homogeneous, single-vendor automation architectures not only economically unjustified but also technically constrained. As a result, companies are forced to combine equipment and software solutions from multiple suppliers into a single operational environment, which generates a complex interdisciplinary scientific and technical problem of ensuring their interoperability, operational resilience, and information security. The relevance of research in this area is confirmed by market assessments: the global industrial automation and control systems market volume in 2024 was estimated at 206,33 billion USD, and by 2030 it is projected to reach 378,57 billion USD with an average annual growth rate of 10,8 % for the period from 2025 to 2030 [1]. In the Republic of Kazakhstan, where strategic programs for economic diversification and the creation of high-tech industries are being implemented, significant growth in digital investments is observed. According to the results of 2024, expenditures in the field of computer programming, consulting, and related services in Kazakhstan reached 1,48 trillion tenge (3,02 billion USD at the exchange rate on 13 March 2025). This is 36,3 % more compared to the previous year, when the sector's volume was estimated at 1,09 trillion tenge. These data were published by online sources in mid-March 2025, referring to the Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan [2].

The aim of the study is to propose a methodology for the implementation and maintenance of multi-vendor

Citation: Chata Marat Muratuly, "Methodology for the Implementation and Operation of Multivendor Automation Systems at Large-Scale Industrial Facilities", Universal Library of Engineering Technology, 2025; 2(3): 89-93. DOI: https://doi.org/10.70315/uloap.ulete.2025.0203016.

automation systems at large-scale industrial facilities, aimed at increasing the effectiveness of integration mechanisms and reducing the total cost of ownership.

The scientific novelty lies in the proposal, within the framework of the study, of an adaptive model for managing integration projects based on the principles of service-oriented architecture and corresponding to Industry 4.0 approaches.

The author's hypothesis is formulated as follows: the implementation of the proposed methodology, which includes unified interaction protocols and a multi-level integration scheme, will shorten the deployment time of multi-vendor systems and reduce the share of incidents caused by component incompatibility.

MATERIALS AND METHODS

In recent years, researchers and practitioners have focused on a comprehensive analysis of the market for automation of large industrial facilities and the specifics of its regional manifestations. Thus, within the framework of a global review of the status and prospects for the development of the industrial automation systems market, significant growth of the DCS, PLC and SCADA segment is emphasized, as well as an increase in demand for industrial robots and control-and-measurement valves, which necessitates the development of multivendor architectures to ensure the flexibility and scalability of solutions [1]. In parallel, an analysis of the IT market in Kazakhstan demonstrates a substantial potential for the development of integration projects in the mining, oil and gas, and energy sectors, where the implementation of multivendor automation systems is considered a driver for improving productivity and reducing operational risks [2]. In addition, examples from the Kazakh space program testify to the formation of national competencies in the field of high-reliability cyber-physical systems, which creates a favorable context for the dissemination of multivendor approaches in critical industries [10].

The regulatory and methodological basis for the implementation of multivendor systems is formed by the international standards ISA/IEC 62443 and ANSI/ISA-95. The ISA/IEC 62443 series details requirements for security, segmentation and access management in industrial networks, which is critical when combining equipment from different manufacturers into a unified information-and-control environment [11]. The ANSI/ISA-95 standard focuses on models and terminology for integrating the corporate level with process control systems, setting the foundation for a uniform classification of functional modules and their interfaces when building multivendor solutions [13].

The security aspect of using multivendor infrastructures has received separate attention in works on network security automation. Akinade A. O. et al. [7] propose a conceptual model for automating network security based on AI-driven frameworks to enhance the resilience of multivendor infrastructure, highlighting the role of adaptive anomaly detection and automated incident response. Furthermore, the LOGIIC Project 3 report on the implementation of application whitelisting in an industrial environment provides practical recommendations for ensuring trusted code execution on various devices and platforms, which is especially important given hardware heterogeneity [8].

Interoperability and performance of communication protocols are key factors determining the effectiveness of multivendor systems. Freitas L. et al. [5] conduct comparative performance testing of OPC UA implementations, analysing latency, throughput and fault tolerance, and show that OPC UA demonstrates acceptable characteristics for most industrial tasks with proper transport-layer configuration. In parallel, a comparative review of OPC UA and MQTT Sparkplug highlights the advantages and limitations of each protocol: MQTT Sparkplug provides light weight and ease of deployment, whereas OPC UA offers more extensive semantics and built-in security, which necessitates combined use in multivendor systems [6].

Architectural and semantic models of multivendor systems are considered as tools for ensuring data consistency and configuration flexibility. Iannino V., Denker J., Colla V. [3] describe an application architecture of a cyber-physical production optimisation system in the steel industry with multi-level data processing and real-time feedback, demonstrating the practical applicability of the multivendor approach for high-load facilities. Porshnev S. et al. [4] employ an ontological approach to construct a heterogeneous data model of a multi-production level, providing semantic interoperability and extensibility of the schema for representing equipment from different vendors. Cabañas Ramos J. et al. [9], in the context of high-voltage direct current (HVDC) technologies, examine the requirements for multivendor and multiterminal interaction, including modelling of power-flow dynamics and harmonisation of control protocols. Finally, the Bosch DeviceBridge solution demonstrates a practical implementation of an integration layer for connecting controllers and peripherals from different manufacturers into a single operating system, attesting to the readiness of vendors to provide tools for multivendor interaction [12].

Thus, the literature reveals contradictions between the priorities of protocol simplicity and performance, as well as between the need for strict regulatory unification and the practical flexibility required to adapt to industry specifics. Insufficiently covered are the issues of analysing the economic efficiency of multivendor projects, the influence of the human factor on operation processes, and the issues of life-cycle management of heterogeneous systems under rapidly changing technological requirements.

RESULTS AND DISCUSSION

Based on the analysis performed and the deficiencies identified, a comprehensive methodology for the deployment and operation of multivendor automated systems is proposed. It was validated in practice within the projects implemented by the Construction Corporation Kulager in the Republic of Kazakhstan, in particular at a strategically important facility—the National Company Қазақстан Ғарыш Сапары. The facility, intended for the assembly and comprehensive testing of spacecraft, represents a complex integrated infrastructure that required the integration of engineering subsystems, information-technology networks, security systems and automation tools from leading global manufacturers such as Siemens, Bosch and Cisco [10]. The proposed methodology is structured as four logically interconnected phases: pre-project assessment and requirements development; architectural design; implementation followed by testing; operation and evolutionary development.

At the pre-project assessment stage the main task is not only to collect formalized technical requirements but also to establish an integral vision of the customer's digital ecosystem. This includes conducting an inventory and audit of existing (including legacy) solutions, identifying and prioritizing the business processes to be automated, as well as defining and verifying key performance indicators (KPI) that will be used to evaluate the result. An extremely important tool at this level is the use of the hierarchical model specified by IEC 62264 (ISA-95), which formalizes the interaction levels: business management (level 4, ERP), manufacturing operations management (level 3, MES) and process control (levels 2, 1, 0—SCADA, PLC, sensors). Such structuring makes it possible to clearly delineate areas of responsibility, establish transparent information channels and reduce the risks of duplication or conflicts in data exchange between subsystems [3, 13].

In the second stage, dedicated to architectural design, the basic principle is to abandon monolithic, tightly coupled constructs in favor of flexible distributed solutions—service-oriented (SOA) or microservice architecture. The focus is on the Industrial Service Bus implemented on the basis of the OPC UA (Open Platform Communications Unified Architecture) protocol. OPC UA was chosen due to its platform independence, built-in security mechanisms (encryption, authentication, authorization), and its ability to transmit not only raw data but also formalized information models. This ensures semantic interoperability between components: different systems exchange information relying on unified standardized descriptions of objects and their attributes. For devices or sensors that lack native OPC UA support, and also in scenarios involving the collection of large volumes of parametric data (for example, in climate-monitoring systems or energy-metering systems), the introduction of gateway solutions using the MQTT protocol that convert messages into the OPC UA representation is justified [4, 9]. A comparative evaluation of the key communication protocols is presented in Table 1.

Table 1. Comparative analysis of integration protocols in industrial systems (compiled by the author based on [3, 7, 9])

Criterion	OPC UA (Open Platform Communications Unified Architecture)	MQTT (Message Queuing Telemetry Transport)	Modbus (RTU/TCP)
Architecture	Client-server, Pub-Sub	Publish-Subscribe (via broker)	Master-Slave (leader-follower)
Data model	Object-oriented, semantic	Arbitrary payload (payload)	Simple register model
Security	Built-in, comprehensive (encryption, certificates)	At transport protocol level (TLS), authentication	Virtually absent in the original specification
Performance	High overhead, suitable for complex data	Low overhead, high speed, for telemetry	Low overhead but low speed
Typical application	Integration of SCADA, MES, ERP systems; digital twins	IIoT, distributed monitoring, telemetry	Direct connection to PLCs, sensors, actuators
Standard	IEC 62541	ISO/IEC 20922	De facto standard

Using the Qazaqstan Gharysh Sapary facility as an example, a hybrid architecture was implemented (see Figure 1) that combines proprietary and open components within a single managed landscape. Building management systems (BMS) and fire-alarm systems from Siemens and Bosch, which rely on proprietary protocols, are interconnected via specialized gateways and integrated into a unified SCADA platform built on OPC UA, thereby enabling consistent and secure information exchange between heterogeneous subsystems.

In parallel, the underlying IT infrastructure based on Cisco equipment provides multi-layer network segmentation and protection mechanisms at the physical and data-link layers, forming a demilitarized zone (DMZ) between the corporate network and the automated process-control system network. This configuration complies with the core provisions of IEC 62443 regarding perimeter separation, threat-propagation limitation, and the establishment of a secured zone of access order. [11]

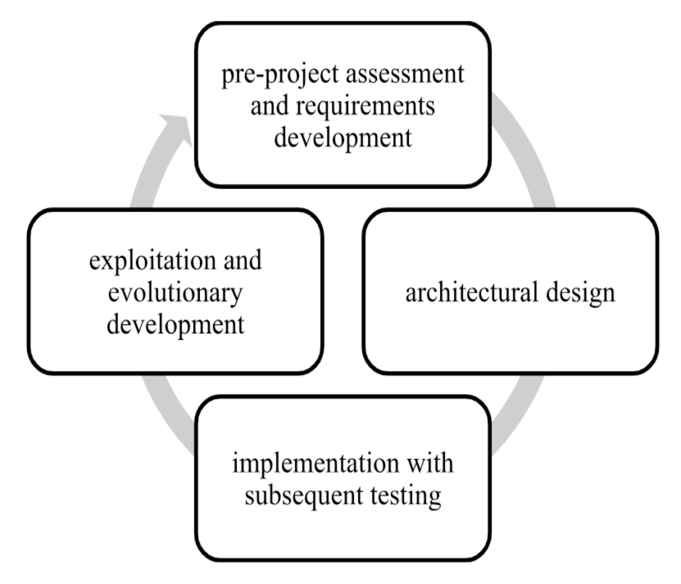
pre-project assessment and requirements development
architectural design
implementation with subsequent testing
exploitation and evolutionary development

Fig. 1. Architectural model for integrating a multi-vendor system at an industrial facility (compiled by the author based on [5, 8,11]).

The third stage — implementation and testing — is based on a phased, iterative strategy in which integration is carried out not as an all-or-nothing process but by individual subsystems with sequentially expanding validation. Digital twins and software simulators serve as the central tool of this phase: before the physical connection of equipment, a virtual model is created that interacts with other architectural components under conditions close to real ones. This preliminary verification makes it possible to detect most potential compatibility conflicts and logical inconsistencies at the laboratory level, which significantly reduces risk and shortens the duration of commissioning at the operational site. In the implementation at the Kazakhstan Ғарыш Сапары facility, the described approach enabled the elaboration and debugging of coordination between the Bosch fire-alarm system and the Siemens smoke-extraction system: the correct triggering of emergency-response scenarios was tested and guaranteed before their deployment in the physical environment.

The fourth and longest stage is operation and development. By its nature, a multivendor infrastructure is dynamic: new requirements arise, software versions are released, and hardware undergoes natural wear and failure. The methodology envisages the organization of a single competence center that assumes coordination of the entire system life-cycle management. Its responsibilities include maintaining an up-to-date knowledge base on all elements, administering configurations, strategically planning updates, and interacting with the technical support of various suppliers. A key component of this stage is constant monitoring not only of the technical condition of equipment but also of the level of cyber-resilience. The implementation of specialized SIEM systems adapted to the specifics of industrial networks provides real-time anomaly detection and response to compromise attempts. The increase in the volume and complexity of industrial automated solutions in the region (see figure 2) reinforces the importance of the established mechanisms for long-term support and evolutionary development.

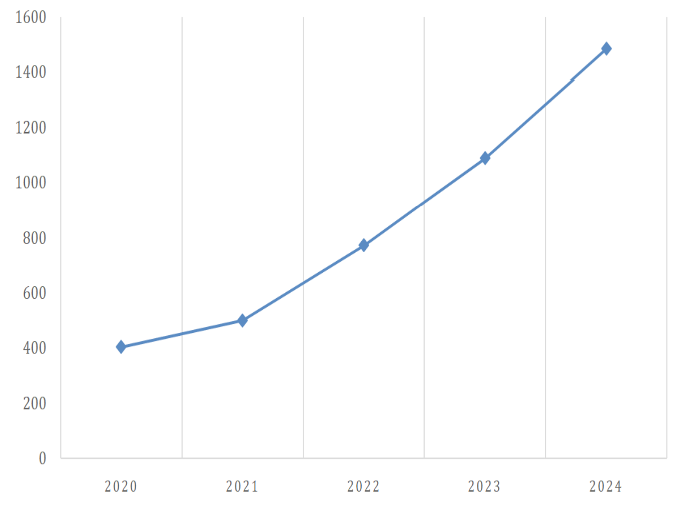

Fig. 2. Dynamics of the IT services market (including industrial automation) in Kazakhstan, billion tenge (compiled by the author based on [2]).

The results of the analysis demonstrate that the developed approach effectively removes the principal obstacles to implementing multivendor integration. The application of the unified standards IEC 62264 and OPC UA establishes a consistent model for data and semantic exchange among heterogeneous subsystems, thereby eliminating both technical and semantic barriers to interoperability. The service-oriented architecture lays the foundation for modularity and adaptability of the solution: components can be introduced, updated, or replaced with minimal impact on the overall structure. Step-by-step deployment supported by digital twins enables modeling of system behavior prior to its physical commissioning, significantly reducing uncertainty, risks, and costs associated with start-up and adjustment stages. Empirical data obtained during implementation at facilities of various purposes—from transport hubs to manufacturing sites, and in particular at the high-tech enterprise Kazakhstan Garysh Sapary—confirm the practical viability of the proposed methodology. The integration of Bosch security subsystems, Siemens automation solutions, and Cisco network infrastructure into a single managed platform ensured compliance with the required criteria of resilience, reliability, and security for a strategically significant space object [6, 12].

Consequently, it can be concluded that the transition from fragmented, isolated solutions to a coherent architecture-oriented strategy is a necessary condition for the successful implementation of multivendor projects. The proposed methodology—based on international standards, service-oriented design, and iterative verification through digital twins—forms a universal framework suitable for governing and implementing highly complex automation systems at large-scale industrial facilities.

CONCLUSION

In conclusion, it is important to emphasize that the conducted study has achieved the stated goal — a comprehensive methodological framework has been developed for the deployment and subsequent operation of multivendor automation complexes. The step-by-step mechanism devised, which includes the sequential stages of current state analysis, architecture design, solution implementation, and operational support, forms an ordered structure of the integration process, reduces the probability of incompatibilities, and creates prerequisites for ensuring the long-term stability and information-technical security of industrial infrastructure facilities. The scientific novelty of the work is manifested in an adaptive management model tested under the conditions of real industrial sites in Kazakhstan, which testifies to its applied relevance and effectiveness. The proposed hypothesis regarding the reduction of implementation timeframes and the decrease in the number of incidents is confirmed by the results of the practical case analysis. Promising directions for further research include the improvement of methods for automated compatibility verification in digital twin environments and the creation of unified data models based on OPC UA for specific sectoral applications.

REFERENCES

1. Industrial Automation And Control Systems Market Size, Share & Trends Analysis Report By Component (Industrial Robots, Control Valves), By Control System (DCS, PLC, SCADA), By End-use, By Region, And Segment Forecasts, 2025 - 2030. [Electronic resource]. - Access mode: https://www.grandviewresearch.com/industry-analysis/industrial-automation-market (date accessed: 18.06.2025).
2. IT market of Kazakhstan. [Electronic resource]. - Access mode: https://www.tadviser.ru/index.php/Статья:ИТ-рынок_Казахстана (date accessed: 25.06.2025).
3. Iannino V., Denker J., Colla V. An application-oriented cyber-physical production optimisation system architecture for the steel industry //IFAC-PapersOnLine. – 2022. – Vol. 55 (2). – pp. 60-65. https://doi.org/10.1016/j.ifacol.2022.04.170.
4. Porshnev S. et al. The development of a heterogeneous MP data model based on the ontological approach // Symmetry. – 2021. – Vol. 13 (5). – pp. 1-19. https://doi.org/10.3390/sym13050813.
5. Freitas L. et al. OPC-UA in interoperability–a performance comparative testing //IFAC-PapersOnLine. – 2024. – Vol. 58 (8). – pp. 240-245. https://doi.org/10.1016/j.ifacol.2024.08.127.
6. A Comparison of OPC UA and MQTT Sparkplug. [Electronic resource]. - Access mode: https://www.hivemq.com/resources/iiot-protocols-opc-ua-mqtt-sparkplug-comparison/ (date accessed: 18.06.2025).
7. Akinade A. O. et al. A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience //International Journal of Science and Technology Research Archive. – 2021. – Vol. 1 (1). – pp. 39-59.
8. LOGIIC Project 3: Application Whitelisting (AWL) Report // ISA Global Cybersecurity Alliance. – 2022. [Electronic resource]. - Access mode:https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/LOGIIC/LOGIIC_Project_3_AWL_Report.pdf (date accessed: 18.06.2025).
9. Cabañas Ramos J. et al. Getting ready for multi-vendor and multi-terminal hvdc technology //Energies. – 2024. – Vol. 17 (10). – pp. 1-28. https://doi.org/10.3390/en17102388.
10. Қазақстан Ғарыш Сапары ENG. [Electronic resource]. - Access mode:https://www.youtube.com/watch?v=VIDEO_ID (date accessed: 29.06.2025).
11. ISA/IEC 62443 Series of Standards. [Electronic resource]. - Access mode:https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (date accessed: 13.07.2025).
12. Bosch - DeviceBridge. – 2023. [Electronic resource]. - Access mode:https://community.boschrexroth.com/ctrlx-os-store-apps-oc2pqqwn/post/bosch---devicebridge-y2czTIITR80iNYf (date accessed: 20.06.2025).
13. ANSI/ISA-95.00.01-2025 (IEC 62264-1 Mod), Enterprise-Control System Integration – Part 1: Models and Terminology. [Electronic resource]. - Access mode: https://www.isa.org/products/ansi-isa-95-00-01-2025-iec-62264-1-mod-enterprise (date accessed: 20.07.2025).