International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-15 Issue-6, May 2026

Open Automation in Process Industries: Transition from Proprietary DCS to Software-Defined Control Systems

Mohammed Hazique Shaikh

Abstract: ***Industrial process control has relied on proprietary DCS for over five decades. The model worked. But working and working well are different things, and in 2026, the gap between what proprietary DCS delivers and what operators in manufacturing, oil and gas, chemical processing, and water treatment need has grown wide enough to drive real change. Vendor lock-in, hardware obsolescence that stretches across decades, and maintenance contracts that give a single supplier complete leverage over upgrade decisions are no longer tolerable when the alternative, open and software-defined control, has been proven at an industrial scale. The Open Process Automation Standard (O-PAS), the IEC 61499 function block model, and OPC UA connectivity together provide the technical foundation for software-defined control systems (SDCS) that break these dependencies. Documented lifecycle cost savings reach approximately 52% over twenty-five years when compared to equivalent proprietary DCS platforms [4]. This paper reviews the standards, examines real deployments, and confronts the barriers that still slow adoption, particularly the near-complete absence of IT-domain competencies in OT workforces. An original Software-Defined Automation Risk Mapping Model (SD-ARMM) is proposed, providing practitioners with a five-dimensional, risk-driven tool to determine which migration strategy fits their specific organisational and operational reality.***

Index Terms: ***Open Automation, Software-Defined Control, DCS Migration, IEC 61499, O-PAS, OPAF, Process Industries, Distributed Control Node, IT/OT Convergence, Risk Mapping, SD-ARMM, Industrial Digitalisation, Vendor Lock-in.***

Nomenclature:
SDCS: Software-Defined Control Systems
O-PAS: Open Process Automation Standard
SD-ARMM: Software-Defined Automation Risk Mapping Model
OPAF: Open Process Automation Forum
UAO: Universal Automation Organisation

I. INTRODUCTION

There's a moment that sticks with most plant engineers: when a controller card fails, and they're left scrambling. Maintenance looks up the part number, only to find out the vendor stopped making it three years ago.

Manuscript received on 30 April 2026 | First Revised Manuscript received on 06 May 2026 | Second Revised Manuscript received on 10 May 2026 | Manuscript Accepted on 15 May 2026 | Manuscript published on 30 May 2026.
*Correspondence Author(s)
Mohammed Hazique Shaikh*, Department of Industrial Automation & Engineering, 161 Mechanic Street, Bellingham (MA), United States of America (USA). Email ID: haziqueshaikh@gmail.com, ORCID ID: 0009-0009-7991-6073

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open-access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

The secondary market is willing to sell a refurbished unit, but at a whopping four times the original price. The other option is to migrate to a whole new platform, which would take a whopping eighteen months and cost even more than the original system. It's moments like these, happening in thousands of facilities all over the world, that spark the conversation about open automation- and it's not just about being dissatisfied with the current state of things; it's about the real, operational headaches that come with it.

Honeywell introduced the first DCS, known as the TDC 2000, in 1975, a breakthrough that brought centralised digital control to the forefront, replacing the traditional analogue panel boards commonly used. The industry quickly adopted this new technology and then continued to build upon it, but the problem was that it was all based on proprietary systems. As a result, over the next fifty years, the industry has been left with a large amount of closed, vendor-dependent automation infrastructure that is now ageing and very hard to modify or update.

The open automation movement has been gaining steam for about ten years now. A major milestone was reached in 2019 when the Open Process Automation Forum (OPAF) published its first standard, known as O-PAS. And even before that, there were already systems that worked with the IEC 61499 standard. But something feels different about the years 2025 and 2026- for one thing, the ExxonMobil Lighthouse Project is now up and running on a large scale. Also, all the major companies that make automation equipment have announced that they're going to make their platforms work with open systems. Plus, there are some pretty convincing numbers showing how much money can be saved by using open automation. Over twenty-five years, the cost of owning and maintaining these systems is 52% lower than that of traditional proprietary systems, as shown in a study [4]. This is a big deal, and it's changing the way people think about automation.

This study takes a closer look at the shift happening in the industry. It discusses the issues with traditional proprietary systems, the new standards that are making this change possible, and the real-world examples that prove these standards work. But it also highlights the challenges that remain, such as the shortage of skilled workers. One of the key contributions of this study is the Software-Defined Automation Risk Mapping Model (SD-ARMM). This tool helps professionals determine the best way to make the transition by considering five factors that can affect the process. It's designed to give them a clear, structured approach to deciding which migration strategy is right for their situation.

II. PROPRIETARY DCS: ARCHITECTURE AND LIMITATIONS

A. How Traditional DCS Systems are Structured

The organization of conventional DCS systems. One company in the traditional distributed control systems (DCS) runs everything. That means they control the hardware, the firmware, the operating system and even the communication protocols. Engineers who work with these systems know them intimately enough to know they will be limited by the fact that every part of the system is vendor-specific. It's that company that owns the programs, the tools, the cables. As widely used now as ever model of organizations these systems may still be, the Purdue Enterprise Reference Architecture shows how they are hierarchical; it shows levels communication, control and so forth. This model is widely referred to as the OT network model, which is the template for configuring and segmenting OT networks, namely industrial control systems. IEC 61131-3 standardised some aspects of the programming language; however, the actual runtime, hardware abstraction, and data management were proprietary [16]. This was originally designed to operate in a single stable, closed, tightly controlled environment. This design paradigm made sense from the ground up, but those assumptions are outdated.

B. Vendor Lock-in: what it Actually Costs

Vendor lock-in is not some vague worry. It is precisely a set of concrete, expensive limitations that determines every major maintenance and upgrade decision a plant makes. Hardware failures with no alternative sourcing. Software bugs that can only be fixed by the vendor on the vendor's schedule. Process expansions that require new I/O in formats only the original vendor supplies. If the plant operator describes his DCS situation, his frustration is not only philosophical. It is about money and the operation's process. And the costs of switching to the new system are prohibitively high, and that is not an accident. When a vendor controls everything that makes up a system – from the hardware and software to the tools and staff – it can have significant power over the final customer decision. That system is a plus for vendors, since they can rake in quite a lot of money from it, they say. But it's a very inefficient process for the people who use the systems. It's becoming more difficult to ignore the differences as people compare IT systems. You can set up and scale a cloud service in relatively few hours, for instance, while you will be required to work with the vendor for months to upgrade a DCS system to change one component. It demonstrates just how much more flexible and efficient cloud services can be than legacy systems. It's just too slow and rigid a way of doing things, outdated, and it's time for a change.

C. Obsolescence and Maintenance Realities

In process industries, DCS platforms can last for twenty to thirty years, which is a big part of those fields where massive capital investments are required, and shutdowns rarely occur. However, throughout that long stretch of time, the vendor landscape changes drastically as well: companies merge (or become redundant), and hardware matures, while support contracts expire. What it was, as such, can become a gradually degrading, never-ending set of worries. This kind of evolution could be extremely disruptive to the industry that depends on them- when reliability and performance begin to degrade, companies face higher downtime rates, expenses, and reduced productivity. The challenge is to steer through these changes, adapt, and maintain platforms amid an increasingly fragmented vendor landscape. When spare parts are unavailable, and the vendor no longer encourages you to seek replacements, maintenance is a reactive measure, not a preventive one. Not least, because the data that could help anticipate and prevent issues is trapped in proprietary systems and isn't readily available to modern analytics tools without spending large sums on additional software. The study of 2024, presented at the ARC Industry Leadership Forum, showed that using open process automation can save approximately 52% in costs over 25 years compared to proprietary systems [4]. Large automation vendors have verified this result independently [19]. The reason is that it saves costs associated with integrating, maintaining, and upgrading the systems it supports. This discovery has brought major changes in how companies think about maintenance and automation, and is shifting the dialogue in boardrooms. Companies that operate on open systems can ensure that maintenance is done much more proactively and more affordably, which has a major effect on their bottom line.

III. OPEN AUTOMATION STANDARDS

A. O-PAS: the Architectural Blueprint

OPAF, created in 2017 by ANSI and The Open Group [15], developed the Open Process Automation Standard, providing a supplier-neutral, interoperable control architecture for process industries. O-PAS describes three essential aspects of the overall system: the DCN, a compute apparatus that executes the control application; the ACP, a central platform for hosting historian, HMI and advanced control functionality; and the CF, based on OPC UA, that aligns the three elements [1] [20]. The underlying concept of this architectural alteration is quite straightforward: a DCN has an O-PAS interface that indicates its structure, rather than the hardware. That is, replacing one vendor's DCN with another's can be done relatively easily, and the control application, written in IEC 61499, will continue to run automatically and unchanged. As stated in its widely cited automation doc, an O-PAS is a full-stack DCS that gives you all the benefits of, but no lock-in to any one vendor's hardware or software [7]. And that's pretty cool, because process industries haven't used this before. This kind of flexibility and independence is transformative, and to many organisations in this space, it's absolutely going to unlock a ton of new opportunities.

B. IEC 61499: Hardware-Software Decoupling in Practice

The IEC 61499 standard is a game-changer for application portability. What makes it so special is that it separates the control application logic from the execution hardware, using an event-data interface model and a device model abstraction layer. This is a big improvement. over the older IEC 61131-3 standard. Schneider Electric has documented specific ways in which IEC 61499 helps process industries accelerate operational digitalization

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

[10]. Recent studies have shown that IEC 61499 really delivers on its promise of portability in real-world industrial settings [8]. For example, function block applications can be easily moved across different runtimes without having to redo the application logic. This is a breakthrough, and it's been confirmed by research- applications can be migrated across compliant runtimes without needing to be re-engineered, which is a huge time-saver [2] [9].

Write the control application once. Deploy it on any compliant runtime. When the hardware underneath needs replacing, replace it. The application is unaffected. This is the operational promise, and it has now been demonstrated at scale in real deployments. The Universal Automation Organization advances this further through a royalty-free runtime engine available to its 89-member ecosystem, and the Eclipse Foundation's 4DIAC provides an open-source implementation [6] [13].

C. OPC UA: Connectivity Without Proprietary Middleware

OPC Unified Architecture, standardised as IEC 62541, provides the secure, semantically rich data connectivity layer that O-PAS uses as its Connectivity Framework. Built-in security, authentication, authorisation, and encryption are part of the standard, not add-ons. Both client-server and publish-subscribe communication models are supported, covering real-time control and historian use cases equally. For the IT/OT integration problem, OPC UA removes the proprietary middleware layer that makes DCS data difficult and expensive to reach. Enterprise analytics, cloud historians, and AI inference engines connect directly to OPC UA data streams [3].

Table I: Proprietary DCS vs Software-Defined Control Systems

Attribute	Proprietary DCS	SDCS / O-PAS
Hardware	Vendor-specific	Multi-vendor
Software	Proprietary, closed	IEC 61499, portable
Connectivity	Proprietary fieldbus	OPC UA (IEC 62541)
Upgrade Cycle	20–30 years	Incremental refresh
Lifecycle Cost	Baseline	~52% lower [4]
Component Replace.	Vendor-only	Any compliant vendor
IT Integration	Difficult, costly	Native via OPC UA

Source: Author Synthesis from [1], [4], [7]

IV. SOFTWARE-DEFINED CONTROL SYSTEMS: ARCHITECTURE

A. Decoupling: the principle that Changes Everything

So, the thing is, what is really important is that software-defined control systems keep the control application and the hardware it's on separate. Simple to claim, yet it really gets at this great. As for the O-PAS model, the DCN is the brain of the operation, processing the whole process. It's actually the IEC 61499 application running on it that is smart. The connection between the two works via a runtime layer, not a particular hardware part specific to a vendor. That is to say, you can have the hardware swap, and then everything goes smoothly for the application. And the hardware will not be affected if you want to change the application, as if they were two independent pieces of software that can be updated without impacting each other. For users, this means that, at the very least, if a DCN fails, one can replace it with any unit that meets O-PAS standards, irrespective of how or by whom it was made, without needing to head to the original supplier or rerun the application. They can load the application and return to their jobs. For plant engineers who have had to confront the alternative, clarity on this aspect is the primary reason for their decision to switch. It's not a question of saving dollars or adhering to set standards; it's about being able to repair a damaged aspect of the system on their terms. This advantage gives you the freedom to easily replace faulty parts, which is why O-PAS compliance is very appealing. With open standards, customers in any project are not locked into any particular vendor or system. They can choose a method that satisfies their needs—and with that freedom they all the less need to be restricted in how to cope.

B. Edge Computing and Control Logic Distribution

Modern SDCS architectures distribute control execution across industrial edge nodes running hardened, real-time Linux-based operating systems—deterministic performance for closed-loop control. Local compute for analytics, protocol translation, and diagnostics [17]. Higher-level functions, historians, AI inference, and advanced control sit on ACPs that may be on-premises or in hybrid cloud deployments. The architecture adds capacity horizontally by adding nodes, not vertically by replacing platforms. This is a genuinely different scaling model from anything proprietary DCS supports.

C. Cybersecurity in Open Environments

Opening the architecture changes the cybersecurity problem. Proprietary DCS relied on obscurity and physical isolation. Neither assumption holds anymore, regardless of architecture. O-PAS aligns with IEC 62443 [11] for industrial control systems security, is consistent with NIST SP 800-82 guidance on OT cybersecurity architecture [14], and modern DCN platforms incorporate hardware security features, including TPM 2.0, for device identity and secure boot. Tamper-resistant Syslog-based audit trails support compliance with IEC 62443 SL2 and SL3. The open architecture requires explicit security engineering, whereas proprietary systems rely on implicit isolation. That is a trade-off worth making when isolation has already been compromised by remote access and IT/OT integration requirements.

V. THE SD-ARMM FRAMEWORK

A manufacturing plant that has been running a ten-year-old DCS with a reasonably skilled maintenance team faces a different migration situation than an oil and gas facility running a thirty-year-old system staffed primarily by OT engineers who have never touched a Linux terminal. Both may have read the same 52% cost-reduction headline. Their actual migration decisions should look completely different. The technology and economics are the same. The risk profiles are not.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The Software-Defined Automation Risk Mapping Model, or SD-ARMM for short, is a new framework we've developed to help people make informed decisions when moving to a new system. It's like a map that shows you where the potential problems are so that you can plan your journey accordingly. This model doesn't tell you exactly how to get from point A to point B, but rather helps you understand the risks involved, so you can figure out the best way to proceed. By using SD-ARMM, you can create a plan tailored to your specific situation, rather than just following what vendors or industry experts say you should do. It's all about identifying and prioritizing the risks that matter most to you, and then using that information to guide your decision-making process.

SD-ARMM identifies five key risk areas, each rated Low, Medium, or High. When you look at how these ratings work together across all five areas, it points to one of three possible approaches to migration: either doing it a little at a time, running the old and new systems side by side, or switching over to the new system in phases. You can see how this works in Table II, which lays out the structure of the model.

Table II: SD-ARMM — Five Risk Dimensions

Risk Dimension	What It Measures	High Indicator	Low Indicator
D1: Technology Lock-in Risk	Depth of vendor dependency: hardware, software, support contracts	Single vendor, EOL hardware, no alternate sourcing	Multi-vendor capable, active support available
D2: Operational Continuity Risk	Risk to production and safety if control is interrupted during migration	Continuous process, no safe shutdown window, safety-critical loops	Batch process, planned turnarounds available
D3: Workforce Capability Risk	The gap between existing OT skills and IT-domain competencies required by SDCS	No IT skills in the OT team, no training budget	Hybrid IT/OT team, training underway
D4: Legacy Integration Risk	Complexity of running legacy DCS and new SDCS infrastructure side by side	Deep fieldbus dependency, no OPC UA gateway	Ethernet-based I/O, existing OPC UA in place
D5: Cybersecurity Exposure Risk	Increased OT attack surface from IT-style connectivity	No IEC 62443 alignment, no network segmentation	Mature OT SOC, IEC 62443 SL2+, monitoring established

SD-ARMM: Author's Original Framework. Risk Scoring: Low / Medium / High Per Dimension

A. Strategy Selection: From Risk Profile to Migration Approach

An organisation with High D2 (Operational Continuity) and High D3 (Workforce Capability) ratings is not ready for aggressive cutover, regardless of how compelling the economics look. SD-ARMM makes this explicit, not as a judgment, but as a risk-management statement.

When certain areas, like D1 and D4, are really strong but D2 and D3 are more middle-of-the-road, a step-by-step approach to migration works well. You start with the less critical parts, get some experience with integration, and then gradually expand. But if D3 is the main issue, it's better to run the old and new systems side by side for a while, so the team can get up to speed with the new technology without slowing everything down. And if all these areas are scoring low or medium, it's best to do a phased rollout, timing it with scheduled maintenance, to get the benefits of open automation as quickly as possible. This way, you can balance the need for progress with the need to manage risk.

Here's the thing: SD-ARMM isn't something you do just once. As things change, like when you're moving to a new system or your team is learning and growing, the risks you face will also change. And let's not forget that the world of automation is always evolving, too. So, it's really important to keep using the SD-ARMM model at each step of the way, to make sure your strategy is still on track with what's actually happening, not just what you thought would happen. This way, you can stay focused on the real situation rather than just following an outdated plan.

VI. INDUSTRY DEPLOYMENTS

A. Exxon Mobil Lighthouse Project

The biggest argument for open automation isn't about cost or technical features — it's a practical example: the ExxonMobil Lighthouse Project. This is game-changing: the project launched in 2025 at the Resins Finishing Plant in Baton Rouge, Louisiana, and has already had its first major impact on the world. It has over 100 DCN controllers, 1,000 I/O points and components from multiple vendors, and everything runs like clockwork with O-PAS. What's also amazing is that it has been consistently shown to run well and without friction among the various components from different vendors. ExxonMobil's DeBari confirmed this at the 2025 ARC Industry Leadership Forum [5]. The effort spanned 16 years, all of which highlight how complicated it was and how well-thought-through it was. From a strategic viewpoint, this marks a key instance of Parallel Operation migration, a proven-effective approach, especially in high-D2 environments, as characterised by the SD-ARMM framework. However, taking this long to reach this point is indicative of the issues that have emerged, but it also shows you could implement open automation and make it happen with some forethought and a phased approach. But beyond scale, what matters is how it shows that replacing hardware works. If an O-PAS system component needs to be changed, the system continues to run on the O-PAS replacement hardware without interruption. That is the decoupling principle, proven at production scale — not in a lab or a pilot.

B. Vendor Ecosystem Development

Now big companies, such as Emerson, Honeywell, Rockwell Automation, Schneider Electric, Siemens, Yokogawa etc are utilizing virtualized industrial controller programs based on open automation philosophy. This is a big change. In earlier years, these companies made money with proprietary technology- no sales, and you just used their products. Now they're moving toward open architectures, which means that customers will be freer to choose what products they use. Because People want to work this way; the fastest-moving companies to switch to wide-open

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

automation will be in a position to work with a diversity of vendors and a degree of capability they cannot offer competitors still using proprietary platforms. This will give them a huge market advantage. Companies that are open to doing this can build relationships with many vendors and develop a flexible, adaptable structure. That is a major change in the industry, driven by customer demand. This shift in the world of data is happening today and will greatly affect the companies they work with. The 2024 ARC Industry Leadership Forum demonstrates this, as it will significantly affect how companies do business [12].

C. Universal Automation Organization Ecosystem

As late as September 2024, the Universal Automation Organisation (UAO) made a royalty-free runtime for IEC 61499 available on GitHub to 89 member organisations, easing the barrier to installing IEC 61499 across multiple vendors [6]. But this time, still, the UAO has let itself be known as not yet having the ability- the full portability of its applications across all vendor runtimes, let alone this runtime. The overall direction is obvious, yet the deployment is ongoing, and there are still some interoperability gaps. When using this runtime, organisations need to ensure they can interoperate correctly with the platforms on which they will deploy it, rather than relying on it to follow the rules. The reason is that standards compliance does not guarantee seamless interoperability, and organisations must ensure interoperability among systems. Doing so minimises their chances of encountering any problems and guarantees a successful migration.

VII. BARRIERS TO ADOPTION

A. The IT-Skills Gap: the Constraint that Determines Everything

The IT skills gap: the limiting constraint on everything. And here is what gets overlooked in discussions about open automation: the technology is ready, the economics are proven, and the deployments are validated. It will also be their ability to operate and maintain a software-defined control system that ultimately determines whether a company can cope with this transition. And for most process industry players, the honest answer in 2026 is no, and not without some heavy investment. In the process domain, OT technicians are primarily trained on vendor-specific DCS tools. They become specialists in configuring and troubleshooting the platforms they have operated with over the years. However, the skills that they acquire are often reserved for the OT domain. IT-domain skills such as Linux system administration, IEC 61499 function block programming, OPC UA server configuration, network security principles, and security mechanisms are vital for integrating OT systems with IT infrastructure. The challenge is that OT and IT are usually organised as separate functions in most process industry firms, with their own management, risk appetite, and language. This division can impede integration between the two domains. Consequently, OT's engineers may lack the IT skills to integrate OT and IT systems fully, and IT professionals may not understand the OT environment's unique requirements and challenges. Dimension 3 — Workforce Capability Risk — would seem to focus on the SD-ARMM model. This is the aspect most often ignored in migration planning, and it is also the main cause of projects getting stuck or crashing. Companies that succeed with open automation transitions focus on training the workforce across all components before even considering the technology. Those who treat migration as simply a tech purchase, on the other hand, typically get into trouble later and end up paying much more. Achieving this will mean organisations avoid the costly errors made by previous organisations during transitions by investing in their staff upfront. Having the right people with the right skills is just as important as having the right technology.

B. Legacy Integration Complexity

But to transition from proprietary DCS to open automation isn't straightforward. You can't just get rid of years' worth of installed systems overnight. It's going to require tools from protocol translation gateways to OPC UA wrappers for older fieldbus protocols, to software adapters for proprietary HMI and historian systems. These tools serve as a bridge connecting old and new infrastructure. This integration work is currently much more costly and complex than similar projects in IT. However, as tools improve and the ecosystem grows, those costs are coming down. That's not to say the switchover is easy, but it is becoming easier and cheaper over time. The idea is to move from a closed system to a larger, open environment that enables many open production methods. Doing so helps businesses adopt new technologies and innovations to get beyond proprietary systems that can be more confining. That's a big change, but an important one for firms that want to stay ahead of the curve.

C. Safety System Scope Limitations

The Open Process Automation Standard (O-PAS) has been deliberate in omitting safety instrumented systems from the initial version. It is an engineering decision, as the certification process for these systems is specified in IEC 61511 and ISA 84, and the O-PAS architecture currently does not meet these standards [18]. For hazardous-material industries, this means that, for now, open automation is complementary to existing safety systems rather than a replacement. Although we would predict future revisions of O-PAS to include safety instrumented systems, professionals planning projects today should accommodate this as part of their system design. Such an approach enables open automation to be used as a supplement to, but not an alternative to, existing safety infrastructure. In so doing, businesses retain the benefits of open automation while maintaining the safety and reliability of their operations.

D. Front-Loaded Costs Versus Long-Cycle Savings

The fact that you can save 52% on costs over the long term is well-documented [4]. However, the issue is that these savings happen over 25 years, whereas the costs of integrating and transitioning to a new system come right away. This can be a problem for companies that review their budgets only every three to five years. It's hard to make a strong case for spending money now, when the benefits won't be seen for a long time. To get around this, you need leaders who are willing to think about the big picture and consider all the costs over the system's whole lifespan, not just the

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

initial cost. As more companies adopt new systems and collect data on how they work, it's getting easier to have these conversations. However, it's still a challenge for companies accustomed to making decisions based on short-term budgets.

VIII. FUTURE DIRECTIONS

We're already seeing some clear paths forward in open automation. For instance, using AI to optimise processes, predict when maintenance is needed, and detect anomalies all rely on being able to access data and use edge computing, which software-defined architectures are particularly well suited to provide. The thing is, these capabilities can't be used with traditional, closed DCS platforms because the data is locked away in proprietary systems, and there isn't enough computing power available. Open automation solves both problems at once. The Open Process Automation Forum, or OPAF, has confirmed that integrating AI is an area they're actively working on for future updates to the O-PAS specification. That translates into more creative solutions in the future. The first is open automation, and by doing that, we can take down some of the barriers that have held us back for so long. It helps us achieve significant increases in efficiency and productivity. So, let's take it apart and humanise it a bit. So, here the second area is integrating digital twins. Here is where OPC UA and IEC 61499 become valuable: they allow simulation models of control systems to be maintained at all levels, from their cradle of development through end-of-life. But one advantage of this is that, instead of deploying new systems in some form, you test changes in a simulated environment, which makes it a whole new world, not to mention when compared with traditional proprietary DCS systems. All in all, this approach totally flips the paradigm around how we view risk when it comes to updating software down the line. More precisely, in manufacturing and production-based environments, a flexible, reconfigurable production architecture is enabled by integrating open automation, edge computing, and 5G private networks. As fast as the production setting it serves. That has never been possible with fixed proprietary DCS infrastructure, and it is exactly what software-defined automation, at full maturity, will deliver.

IX. CONCLUSION

The issues with proprietary DCS are not going away. Vendor lock-in, obsolescence, and maintenance dependencies are structural aspects of the model, not fixable defects. End-users in manufacturing, production, and process industries face these issues every operating day, and the push toward open alternatives is real and growing. The case for software-defined control is just as distinct. The ExxonMobil Lighthouse Project verifies O-PAS at the production scale [5]. IEC 61499 runtimes are open-source and royalty-free. OPC UA is a connection layer. Economic analysis corroborates the transition, with documented lifecycle cost savings of 52% over twenty-five years [4]. SD-ARMM is a decision-making tool that supports practitioners' well-informed migration decisions. This tool is designed with the five most relevant considerations of the migration outcome: the degree to which a company is connected to a specific technology, the likelihood of disruptions to regular business operations caused by that technology, workforce skills and capabilities, the difficulty of merging new systems with legacy ones, and the exposure of the company to cyber threats. Based on these considerations, the model recommends either migrating gradually by running old and new systems side by side or switching to the new system in phases. It is an organisation-based approach and should be considered in the context rather than as a 'one size fits all' approach. For these five dimensions, it is often the Workforce Capability Risk that makes or breaks a project's success. Technology and economics are no longer the No. 1 challenges. The real difficulty is creating a team capable of working across domains, deploying software-defined control, and maintaining it in process-centric environments. This is the real work that has to be conducted, and businesses that begin investing in this now will get much ahead of the curve, leading the transition instead of responding to it. They will be well-prepared to capitalise on new opportunities and remain competitive in the long term by getting a head start.

DECLARATION STATEMENT

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and without external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed solely.

REFERENCES

1. Open Process Automation Forum (OPAF), "Open Process Automation Standard (O-PAS), Version 3.1," The Open Group, 2023. [Online]. Available: https://www.opengroup.org/open-process-automation/opas
2. A. Zoitl and T. Strasser, "Interoperability in Software-Defined Process Automation Using O-PAS and IEC 61499," IEEE Industrial Electronics Technology News, vol. 11, no. 1, Jan. 2025. [Online]. Available: https://www.ieee-ies.org/pubs/industrial-electronics-technology-news
3. International Electrotechnical Commission, "IEC 62541: OPC Unified Architecture," IEC, Geneva, 2020. [Online]. Available: https://www.iec.ch/iec62541
4. M. T. Hoske, "New cost analysis: Open process automation saves 52% versus DCS," Control Engineering, Apr. 2024. [Online]. Available: https://www.controleng.com/articles/new-cost-analysis-open-process-automation-saves-52-versus-dcs
5. M. T. Hoske, "New insights: 100-controller ExxonMobil Open Process Automation," Control Engineering, Jan. 2026. [Online]. Available: https://www.controleng.com/articles/new-insights-100-controller-exxonmobil-open-process-automation
6. Universal Automation Organization, "Open Automation Systems: Update on the State of the Art," Automation.com, Sept. 2024. [Online]. Available: https://www.automation.com/en-us/articles/september-2024/universal-automation-organization-open-automation

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

7. Yokogawa Electric Corporation, "Open Process Automation is Gaining Sustainable Momentum," Yokogawa America, 2024. [Online]. Available: https://www.yokogawa.com/us/library/resources/yokogawa-technical-reports/open-process-automation
8. I. Prado, "Open Process Distributed Automation using IEC 61499," Proc. 2022 ASEE Annual Conference & Exposition, Minneapolis, MN, 2022. [Online]. Available: https://peer.asee.org/open-process-distributed-automation-using-iec-61499
9. A. Zoitl and T. Strasser, "Towards Industrial Cyber-Physical Systems Using Open-Source Platforms," IEEE Trans. Ind. Inform., vol. 17, no. 1, pp. 390–398, Jan. 2021. DOI: https://doi.org/10.1109/TII.2019.2945739
10. Schneider Electric, "Three Ways IEC 61499 Helps Process Industries to Accelerate Operational Digitalization," Schneider Electric Blog, Jun. 2023. [Online]. Available: https://www.se.com/ww/en/work/campaign/innovation/open-automation.jsp
11. ISA/IEC, "ANSI/ISA 62443: Security for Industrial Automation and Control Systems," International Society of Automation, 2018. [Online]. Available: https://www.isa.org/standards-and-publications/isa-iec-62443-series-of-standards
12. ARC Advisory Group, "Industrial Controller Software Standards: Discussions at ARC Industry Leadership Forum 2024," Automation.com, Mar. 2024. [Online]. Available: https://www.automation.com/en-us/articles/march-2024/arc-forum-2024-industrial-controller-software
13. Eclipse Foundation, "4DIAC: Open-Source IEC 61499 Runtime," Eclipse Foundation, 2023. [Online]. Available: https://www.eclipse.org/4diac/
14. National Institute of Standards and Technology, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82, Revision 3, 2023. DOI: https://doi.org/10.6028/NIST.SP.800-82r3
15. Open Group, "OPAF: Open Process Automation Forum Charter and Architecture Overview," The Open Group, 2021. [Online]. Available: https://www.opengroup.org/open-process-automation
16. Control Engineering, "Standardising Control System Programming with IEC 61131-3," Control Engineering, Apr. 2025. [Online]. Available: https://www.controleng.com/articles/standardizing-control-system-programming-with-iec-61131-3/
17. DMTF, "Redfish API Specification," Distributed Management Task Force, Version 1.20, 2024. [Online]. Available: https://www.dmtf.org/standards/redfish
18. International Society of Automation, "ISA-84 / IEC 61511: Safety Instrumented Systems for the Process Industry Sector," ISA, 2017. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards/isa84
19. Honeywell International, "The Quantified Value of Open Process Automation," Honeywell International, 2024. [Online]. Available: https://www.honeywell.com/us/en/press/2024/open-process-automation
20. IEC TC65, "IEC 62714: AutomationML — Engineering Data Exchange Format," IEC, Geneva, 2021. [Online]. Available: https://www.iec.ch/iec62714

AUTHOR'S PROFILE



Mohammed Hazique Shaikh is a Senior Future Offer Manager in the Industrial Automation division at Schneider Electric, where he leads new product introduction strategy and execution for next-generation software-defined industrial controllers. His professional work focuses on developing open automation platforms, edge computing architectures, and product value proposition frameworks for mission-critical process automation environments across the energy, chemical, water treatment, and manufacturing sectors. He holds a Master of Science in Engineering Management from Northeastern University, Boston, MA, and a Bachelor of Technology in Mechanical Engineering from the Vellore Institute of Technology, India. Before his current role, he held engineering and product management positions at Tata Consultancy Services, where he led cross-functional teams delivering technology products for Ford Motor Company and Mitsubishi Motors across automotive electronics, battery management systems, and ADAS domains. His research interests include software-defined industrial automation, open process automation standards, edge computing for process control, cybersecurity in IT/OT converged environments, and product strategy in engineering-intensive B2B technology markets.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© Copyright: All rights reserved.