WIND™

Open, Secure Industrial Automation Systems

Lower Expenses and Increase Flexibility

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Many of today's industrial automation solutions are overly expensive and inflexible, partly due to proprietary solutions that do not interoperate well with other products in the market. This has the effect of locking in industrial companies, which prevents end users from selecting their preferred components along the entire stack, including digital controllers, programmable logic controllers or distributed control systems (PLCs/DCSs), supervisory control and data acquisition (SCADA) software, human-machine interfaces (HMIs), process historians, application servers, and so on.

In another market, telecommunications service providers also faced a predominance of proprietary equipment, and over a dozen of the world's largest providers took action. They collaborated to propose a transition to interoperable solutions based on industry-standard servers—an approach called Network Functions Virtualization (NFV). After a few short years, telecom equipment vendors now offer software-based network functions that can run on commercial off-the-shelf (COTS) servers, enabling economies of scale, wide vendor choice, and interoperability.

This white paper describes how a comparable transformation is emerging within industrial companies. But while industrial and telecom equipment customers may have similar goals (e.g., lower cost and agility), the usage models and solution architectures can be vastly different.

TABLE OF CONTENTS

HISTORICAL PERSPECTIVE

In the 1980s and 1990s, industrial automation systems were built with proprietary software and hardware, providing no interoperability between different vendor solutions. As a result, industrial companies were locked into the platform they chose, and if they wanted a feature available elsewhere, they faced an uphill battle to incorporate it. Once an industrial automation solution was in place, it was prohibitively expensive to switch or upgrade to the latest technologies.

In the late 1990s, industrial companies were dissatisfied with the status quo and demanded interoperable solutions. This led to the development of the Open Platform Communications (OPC) standard that enabled communications between proprietary systems. Some industrial companies began writing their own code, while others hired developers to implement features.

But in the late 2000s, companies began moving in the other direction again, maintaining a single platform internally and only purchasing COTS products that worked with it.

PROPRIETARY SOLUTION PAIN POINTS

Working with a single industrial automation supplier has benefits, such as managing just one vendor that provides pre-validated, end-to-end solutions. However, there are some drawbacks, including those shown in Figure 1 and discussed in the following paragraphs.

High CapEx/OpEx

Due to smaller volumes, proprietary solutions do not benefit from the same economies of scale as COTS-based solutions. Moreover, proprietary automation solutions can be expensive to buy and maintain, since they typically have a number of specialized boxes at each International Society of Automation (ISA) level. In contrast, the COTS market is highly competitive, which increases the cost pressure on suppliers.

Inflexibility

Despite the OPC standard, industrial companies still do not have the flexibility to choose among vendors, because interoperability remains an issue in automation. Flexibility can also be an issue within a vendor's product line, such as when users try to move the code they wrote for one box to another box. This is likely due to insufficient abstraction of the box's implementation details—the purpose of an application programming interface (API). When a box becomes obsolete, users may need to overhaul their code for the next-generation box. This paradigm is changing as virtualization technology and NFV open up new avenues for where software is run and how it can be abstracted from the underlying hardware.

Security Deficiencies

Device and data security cannot be an afterthought; they need to be designed in from the ground up. Too often, automation solution vendors do not have the experience to implement a layered security defense that creates a root of trust spanning hardware, BIOS, operating systems, anti-malware, data encryption, VPN, security information and event management (SIEM) products, and other technologies. On the other hand, COTS product vendors are working together to "build in" security—as opposed to "bolting on" security—and to keep security measures up to date in their products.

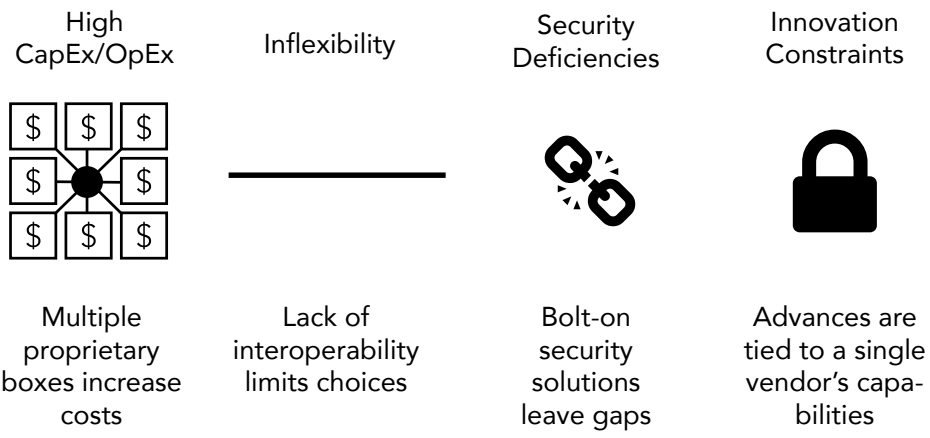

Figure 1. Proprietary solution drawbacks

Innovation Constraints

Industrial companies do not want their pace of innovation to depend on their vendor's capabilities or motivations. Whether it is predictive maintenance, big data, or virtual reality, users want to adopt best-of-breed technologies on their own timeline.

SOFTWARE-DEFINED ARCHITECTURE

Like the industrial automation market, information technology (IT) faced issues with proprietary communications interfaces that produced walled gardens of enterprise computing systems. The resolution was to widely adopt Ethernet and TCP/UDP/IP, with a focus on open standards and open platforms. The modern data center is full of low-cost, virtualized COTS servers running cloud management software and supporting the Internet protocol (IP) for communications and industry-standard backplane fabrics, like Ethernet.

These IT concepts are now being applied to industrial automation, a trend called software-defined architecture. The premise is that most of the functions found in layers L1 to L3 of the ISA-95 model, shown in Figure 2, can be run on COTS servers capable of satisfying the real-time performance requirements of industrial environments. As a result, the individual L1–L3 products found in today's proprietary automation solutions can be consolidated onto servers that deliver benefits equivalent to the IT data center. Like IT, software-defined architecture utilizes open standards and open platforms, extending them to meet industrial requirements, thereby reducing operating and capital expenses (OpEx and CapEx) and reaping the benefits of the IT cloud.

> Software-defined architecture consolidates operations and control functions onto standard, high-volume servers, creating an alternative to proprietary industrial solutions while enabling up to 99.9999% system uptime.

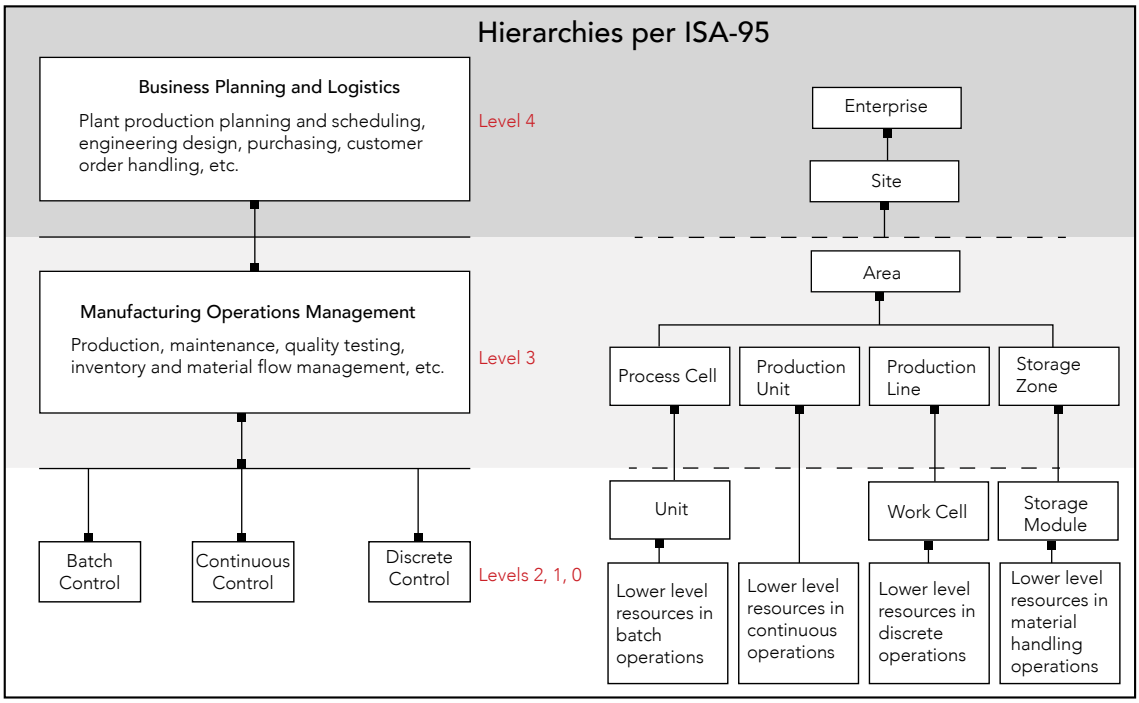

Figure 2. ISA-95 model for developing an automated interface between enterprise and control systems[1]

More specifically, software-based digital controllers, PLCs/DCS, SCADA software, HMIs, process historians, and applications in L1–L3 can run in an industrial software-defined architecture, as shown in Figure 3. Servers interface to sensors, actuators, and other physical industrial devices via distributed control nodes. Software-defined architecture makes the data center "industrial grade," delivering the CapEx and OpEx benefits of an IT-based approach while satisfying industrial requirements—such as high availability, real-time determinism, lifecycle management, and hitless upgrades—that typical IT data center solutions cannot.

BENEFITS OF SOFTWARE-DEFINED ARCHITECTURE

Based on open standards and open platforms, software-defined architecture allows industrial companies to avoid vendor lock-in and the associated drawbacks of proprietary solutions.

Lower CapEx/OpEx

Compared to purpose-built solutions, software-defined architecture lowers hardware CapEx by substituting low-volume, custom computing platforms with a small set of high-volume COTS servers. These servers can be easier to manage than a large number of unique proprietary devices, thereby decreasing OpEx. Additionally, software-defined architecture lowers CapEx and OpEx for logistics by significantly reducing the number of unique boxes that must be kept on hand for maintenance and the related costs to train and support staff on a number of unique articles.

Software-defined architecture scales and expands with less effort because there are fewer wires, cables, and systems to deal with, minimizing connectivity-related costs. Software-defined architecture solutions also take up less physical space near the industrial equipment they control.

Systems based on software-defined architecture require less field service support than traditional systems, since they can be remotely monitored, diagnosed, and updated in real time without deploying field service engineers, thus further reducing OpEx costs. If a failure occurs in the field, high-availability system failover mechanisms help reduce the need for a 911 truck roll, which is more expensive than a standard truck roll.

The long service lifetimes of industrial systems introduce obsolescence issues, and the decoupling of functions implemented in software from the underlying hardware/software platforms allows software-defined architecture to mitigate CapEx and OpEx costs associated with platform updates that address obsolescence.

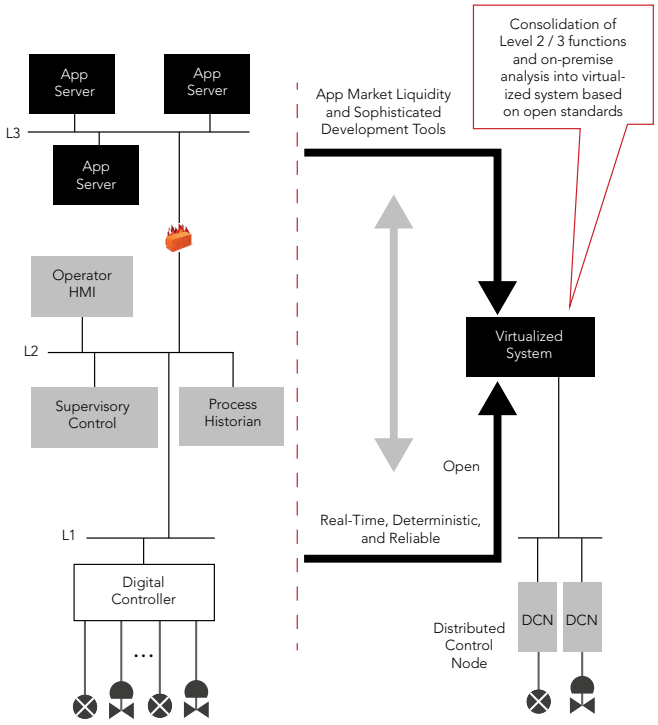

Figure 3. Software-defined architecture consolidates software-based ISA-95 L1–L3 functions onto highly available, real-time COTS servers[2]

BEYOND INDUSTRIAL AUTOMATION

The principles of software-defined architecture can be applied to non-industrial application areas that have an operational hierarchy similar to ISA-95 and could benefit from system centralization and consolidation.

For example, oil and gas companies might use software-defined architecture to link sensors and actuators in oil wells to systems for control, production monitoring, logistics, business planning, and so on.

Similarly, the medical industry may well see operational improvements by consolidating the chain of systems from the hospital floor device to finance and accounting.

> "Software-defined architecture offers tremendous potential to improve business performance. Companies will be able to use data that has long been stranded inside machines and processes due to proprietary solutions to help identify production inefficiencies; compare product quality against manufacturing benchmarks; and pinpoint potential safety, production, or environmental issues."
>
> —Craig Resnick, Vice President, ARC Advisory Group

Flexibility

Software-defined architecture is designed with open platforms that allow users, independent software vendors (ISVs), systems integrators, best-in-class off-the-shelf applications, and so on to more easily develop interoperable components than is possible with proprietary solutions. Since software and server hardware are decoupled, software can be easily migrated and reused. In addition, orchestration and management frameworks, such as OpenStack, are available to help ensure that the overall industrial automation solution is flexible and works efficiently.

Built-in Security Efficiencies

With software-defined architecture, the primary hardware platform is a server, which takes less effort to make secure than the large number of custom platforms found in a proprietary automation solution. The IT industry has developed various hardware and software technologies for safeguarding servers that can be carried over to software-defined architecture to create robust and layered security.

The virtualized function aspects of software-defined architecture also allow best-in-class network security functions (and industrial automation security functions) to be incorporated into the system easily and cost-effectively, as with NFV in telecommunications. These functions can include firewalls, VPN concentrators, intrusion detection systems (IDS)/intrusion prevention systems (IPS), SIEM, and even security functions that are yet to be developed.

Accelerated Innovation

Since software-defined architecture is based on open platforms, industrial companies are free to work with any supplier they choose to adopt the latest technologies and process innovations. Because these solutions run on COTS servers, it is relatively easy to propagate these advancements throughout the corporation, and even to enterprise systems, thus providing a higher return on investment.

VIRTUALIZATION AND SOFTWARE-DEFINED CONTROLS FOR SAFETY-CRITICAL SYSTEMS

Software-defined architecture (with extensions for real-time performance) is a good fit to satisfy recent trends in avionics systems such as Integrated Modular Avionics (IMA). IMA represents a transition away from federated architectures, where each individual subsystem performs a dedicated function, toward generic computing platforms that can be used in multiple types of applications and, in some cases, run multiple applications concurrently. Similar to the way software-defined architecture solutions can be used in industrial applications, original equipment manufacturers (OEMs) are consolidating applications on COTS-based systems, resulting in fewer subsystems, reduced weight, lower power consumption, and less platform redundancy.

The Future Airborne Capability Environment (FACE™) for U.S. military avionics programs and IMA standards place new demands on the software architecture, especially the real-time operating system (RTOS) implementation provided by the COTS supplier. Wind River® has specifically addressed these needs by developing Wind River VxWorks® 653 Platform to support Aeronautical Radio, Incorporated (ARINC) 653 and the FACE Safety Base Profile.

REQUIREMENTS FOR SOFTWARE-DEFINED ARCHITECTURE INFRASTRUCTURE

Software-defined architecture solutions must run reliably and safely, gathering real-world industrial data and actuating responses in real time. In order to achieve this, software-defined architecture infrastructure must consolidate operations and control functions and satisfy the following criteria:

- **Low-latency virtualization:** Software-defined architecture servers must support virtualization in order to run the diverse functions and applications found in industrial applications. The virtualization technology must have minimal overhead in order to provide real-time, deterministic performance for critical applications while optimizing resources for non-critical applications.
- **Deterministic networking:** Fully deterministic, real-time communication over Ethernet is needed for control functions in industrial environments. Time-sensitive networking (TSN) achieves this by creating a global sense of time and a schedule among industrial components.
- **High availability:** In the event of software failure, software-defined architecture servers and applications must be able to perform automatic failover quickly enough to support control system integrity. Failover speed requirements are often orders of magnitude faster than standard IT solutions, whereas carrier grade telecommunications NFV solutions are approaching the automatic failover speeds needed for software-defined architecture. Virtualization technology facilitates failover in a number of ways, such as restarting a clean backup software image without a reboot or turning control over to a full redundant server to overcome catastrophic hardware or software issues.

> "The trend towards convergence brings together IT and OT systems that have long remained separate, and as a result, systems that previously leveraged standards to communicate within their own domain now must also communicate using mutually open technologies. Software-defined architecture lowers these barriers between the enterprise and manufacturing domains, opening up islands of automation to enable plant-wide, information-centric systems that enable the secure flow of information throughout the manufacturing enterprise and beyond."
>
> —Craig Resnick, Vice President, ARC Advisory Group

- **Robust security:** Software-defined architecture allows security technologies to be built in from the ground up and across hardware platforms, middleware, applications, communications, and cloud infrastructure. The flexibility of software-defined architecture allows security solutions to adapt over time to respond to system and threat changes. Required technologies include Secure Boot; robust roots of trust (e.g., Trusted Platform Module [TPM]); digital random number generators; secure identities; local and remote attestation; anti-malware; data encryption; firewalls; authentication; authorization; and accounting (AAA), IDS/IPS, SIEM, and VPN tunneling.
- **Lifecycle management:** An integrated orchestration and management framework should support a process automation environment designed to remain in continuous operation for years. Users must be able to perform lifecycle operations, such as software upgrades, live patching, capacity expansion, hardware updates and replacement, and physical and logical networking changes, without any loss of service. Easy installation and provisioning (e.g., deployable remotely, or with a single USB stick and via orchestration and management) facilitates lifecycle management in a wide spectrum of operational scenarios, including ones where outages require physical access to remediate issues. In addition, alarms, logging, and extensive monitoring of platforms, hardware, applications, and services are essential to maintaining an efficient, highly available automation system.
- **Enhanced platform awareness and monitoring:** Software-defined architecture solutions need to support awareness of hardware capabilities, hardware and software status, and the ability to match these with application requirements in order to guarantee required levels of service. These platform awareness and monitoring capabilities enable automated resource allocation as well as reallocation necessary to adapt to change while preserving critical performance, safety, and resiliency properties.
- **Best-in-class applications:** Based on open x86 virtualization architecture using COTS hardware, software-defined architecture solutions must support the easy integration of IT technologies (Hadoop, Apache Storm, Java Analytics engines, Linux, and Linux containers). At the same time, these solutions must implement OT technologies capable of satisfying real-time requirements that are more stringent than what is needed for IT through the use of operating systems such as Linux or VxWorks for hard, real-time performance. This allows for the migration of these technologies across the industrial environment and lowers the barriers to entry for solution providers desiring to add value to the system. System integrators and operators can then take advantage of the open solution to incorporate and enable ISVs and best-in-class applications.

> "All manufacturers and processors must demonstrate measurable business value to obtain CapEx or OpEx funding for any IT and OT functionalities needed to run their factories and plants, each with clear key performance indicators (KPIs), such as return on investment (ROI), return on assets (ROA), and overall equipment effectiveness (OEE). Software-defined architecture helps to substantially lower both CapEx and OpEx funding requirements, which will lower the ROI and ROA time periods to the point that automation projects that were previously not justifiable can now be approved, allowing manufacturers and processors to derive all the business value that higher KPIs, such as OEE, bring to the table."
>
> —Craig Resnick, Vice President, ARC Advisory Group

HOW TO GET STARTED

Many of the requirements for software-defined architecture have already been addressed by telecommunications networks that implement NFV. The Wind River Titanium Cloud™ portfolio of products represents the industry's first fully integrated and feature-complete network virtualization software platform, providing ultrareliability and exceptional performance efficiencies while simultaneously supporting the extremely low latencies needed for real-time workloads. Wind River Titanium Control is a product within this portfolio and is built specifically for the industrial market. Software-defined architecture solution providers can jump-start their development with this platform designed for COTS server hardware. For more information about Titanium Control, visit www.windriver.com/products/titanium-control.

NOTES

1. The figure is based on one by Nicholas Sheble, *InTech Magazine*. https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2007/march/channel-chat-iec-62264-and-isa-95-enterprise-control-system-integration/
2. The figure is based on a Lockheed Martin/ExxonMobil next-generation open automation system Industry Day presentation, January 26, 2016.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.