CODESYS

cisco
The bridge to possible

Improve Efficiency and Cut Costs with Industrial Automation and Control Systems Virtualization

Introduction

Digitization of manufacturing environments enables the use of software control in production processes to better realize the promises of Industry 4.0: driving optimization, improving security, and increasing sustainability. In addition to using software that analyzes real-time data to derive insights and improve production processes, manufacturers are now beginning to convert traditional appliance-based Industrial Automation and Control Systems (IACS) to their virtualized software-based equivalents. Software IACS gives manufacturers even more control over their production and helps enhance flexibility, drive efficiencies, and reduce costs.

However, transitioning from dedicated hardware on the factory floor to a virtualized environment places stringent performance and uptime requirements on the factory network to maintain tight synchronization and coordination needed for accurate machine control.

In this document, we will explain the gains virtualization can deliver, the requirements of an industrial network to make virtualization possible, and the architecture Cisco has built in partnership with CODESYS® to realize these gains.

What can virtualization do for your operations?

Virtualization technology has dramatically changed the way IT resources are used, and services are delivered, enhancing efficiency, flexibility, and scalability. However, virtualization has yet to impact industrial operations in any significant way. IACS hardware resources in these environments continue to exist as discrete resources. With digitization, the number of such hardware resources has risen rapidly and so has the time and expense of monitoring, updating, and troubleshooting them, which could require extended downtimes and result in productivity losses. Additionally, because these devices are notoriously hard to update, they have become a significant target of cybersecurity threats and risks.

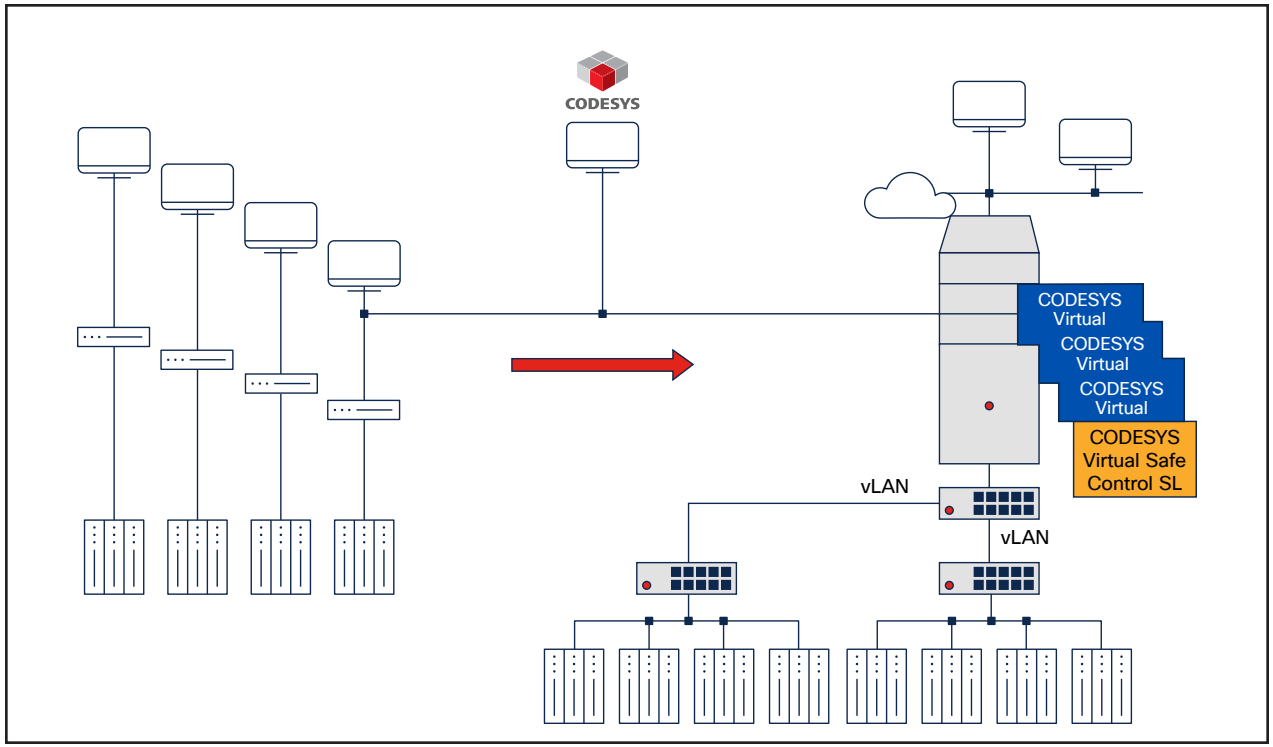

Figure 1. From direct wired to virtualized control systems

Manufacturing facilities stand to gain a lot through virtualization. They can consolidate Programmable Logic Controllers (PLCs), Industrial PCs (IPCs), Human-Machine Interfaces (HMIs), gateways, and other physical compute resources currently on their factory floors onto virtual machines that run on a Hyperconverged Compute and Storage Infrastructure (HCI).

- **Scalable and agile operations:** Virtualization enables manufacturers to easily scale their operations by adding or removing virtual machines on demand instead of repeatedly deploying and retiring hardware. Virtualization also makes it easier to deploy new applications, make updates, accommodate product redesigns, etc.
- **Increased security:** Removing hard-to-update, discrete hardware from the factory floor minimizes potential avenues that an attacker or malware can exploit to gain unauthorized access to manufacturing assets and processes. Virtualization can improve the security of operations by making faster updates that close known vulnerabilities. Additionally, segmenting networks and implementing security measures at the virtualization layer can minimize the risk of malware propagation. And in the event of a successful breach, the compromised virtual control system can easily be shut down and replaced by a newly deployed virtual machine.
- **Improved disaster recovery:** Virtualization allows for efficient backup, replication, and restoration of virtual machines for better disaster recovery planning. It enables manufacturers to recover from system failures or disasters, reducing downtime and minimizing any impact on production.
- **Faster development:** Virtualization provides an ideal environment for testing and development activities. Manufacturers can create virtual replicas of their production systems for testing new software, configurations, or system updates, enabling them to reduce the time to market for new products.
- **Reduced costs:** Virtualization can help reduce both operating and capital expenses. Upfront hardware purchase costs can be reduced by running multiple virtual machines on a single server. Fewer physical servers also mean fewer machines to maintain and repair. Virtualization often comes with management tools that simplify and automate the maintenance of virtual machines. This can reduce the need for manual administration, increase productivity, and reduce OpEx.
- **Better sustainability:** Consolidation of computing and storage resources into a set of central services helps reduce the total energy requirements. In addition, easier access to more processing data can help increase efficiencies, reduce waste, and further lower energy consumption.
- **Lifecycle extension:** Being able to add new features and functions as software updates on the virtualization platform, with access to existing plant applications, extends the viable life of existing (brownfield) IACS devices.

CODESYS

CISCO
The bridge to possible

The path to virtualized IACS

Even with its benefits, virtualization of control systems is not yet mainstream in the manufacturing sector. Manufacturers are hesitant to change their tried-and-true processes and systems without assurance of a solution that addresses challenges in the transformation.

While discrete compute resources such as PLCs, HMIs, and IPCs are all candidates for virtualization, there are some key differences between the three.

HMIs are the user interface, the visual representation of the factory floor that allows operators to monitor and interact with machines. Virtualization focuses on making this interface accessible from anywhere on the network, using Virtual Desktop Infrastructure (VDI) solutions or specialized HMI software.

IPCs are industrial computers that run control software or act as gateways between different systems. Virtualization allows running multiple operating systems or applications on a single physical IPC or on virtual machines hosted on a server.

PLCs are the brains of the operation, the industrial computers that receive sensor data, execute control logic, and send instructions to machines. Virtualization focuses on running multiple PLC programs on a virtual machine hosted on a server.

But no matter which IACS device we choose, an effective virtualization strategy would require:

- **A robust virtualization platform:** IACS applications can be demanding in terms of processing power, graphics capabilities, and network bandwidth. The virtualization platform needs to be high performing to handle these requirements efficiently. It must be able to handle the demands of real-time operations, be scalable to accommodate additional IACS VMs (Virtual Machines) or increased processing demands, and secure to safeguard the VMs from unauthorized access, malware, and data breaches.
- **Improved bandwidth and latency:** Industrial control systems require real-time performance with deterministic responses. These systems control physical equipment in which minor delays can lead to serious problems, including outages and disruption. Just a few years ago, the bandwidth and resiliency of standard networks would have made it challenging and expensive to virtualize key assets. Networks capable of supporting virtualization must have required bandwidth, low latency, high reliability, and software-defined operations.
- **Industrial protocols:** Traditionally, industrial control systems and machinery have been designed to communicate via Layer 2 networks, given the emphasis on precision timing requirements. Layer 2 connectivity has the advantage of having fewer network hops with no routing, which results in lower latency. Replacing individual controllers with a central computing environment would require a Layer 3 network, as packets would need to be routed between the machines and controlling applications. Not only would a Layer 3 network need to tunnel Layer 2 traffic, but it would also need to satisfy strict timing and packet loss requirements.

- **Resiliency and reliability:** Replacing a Layer 2 network with a routed Layer 3 network adds new links and network functions between the machines and controlling applications, exposing manufacturing processes to the risk of delays and interruptions. A high-performing resilient network able to withstand link and device failures can ensure continuity of operations.
- **Security:** With more connected industrial assets and a greater dependence on the network, coupled with extended Layer 2 networks that expose more of the data, security risks increase. Therefore, securing operations in a virtualized environment becomes even more important and requires the network and applications to have more awareness. The solution must provide detailed visibility, be able to spot vulnerabilities, segment the network granularly, and monitor connected devices continually for any breaches.
- **Automation and assurance:** Network operations must be automated to allow the addition of new networking equipment and the reconfiguration of existing equipment and must grow and change as needed to serve the demands of virtualized systems. To minimize disruptions, networks must also be able to proactively monitor their own performance, identify bottlenecks, and perform root cause analysis and either take corrective action or suggest fixes for faster resolution.

The network is the key to IACS virtualization

The network is the key to migrating individual PLCs, HMIs, IPCs, and other discrete hardware resources to central hyperconverged environments.

A traditional industrial network may have switches and routers that need to be configured individually to handle traffic flows. Any desired flow change requires consistent reconfiguring of these switches and routers. In a large network, this manual process can be time consuming and error prone.

A modern Software-Defined Network (SDN), on the other hand, has an intelligent central SDN controller that can configure and reconfigure switches and routers to realize the desired traffic flows. Instead of configuring devices one by one, you can make changes to the entire network at once from the SDN controller. The ability to make quicker changes helps in rerouting traffic faster and in isolating misbehaving assets to keep operations safe. This level of control increases flexibility, simplifies management, and improves security. It also allows for greater programmability and agility in network configuration and management.

These benefits of SDN are key to virtualizing control systems and help to get the maximum benefit of virtualization by further increasing operations flexibility, allowing customization to support diverse requirements, and being able to scale networks easily.

Virtualizing PLCs requires overcoming challenges related to real-time determinism, specialized hardware, legacy code, and safety considerations, that makes them more complex to virtualize than either HMIs or IPCs. The rest of this document focuses on virtualization of PLCs.

CODESYS

cisco
The bridge to possible

Cisco and CODESYS solution for IACS virtualization

As shown in Figure 2, Cisco has built and tested a software-defined industrial network architecture to support virtualized controllers. The following are the key building blocks of the Cisco® industrial solution.

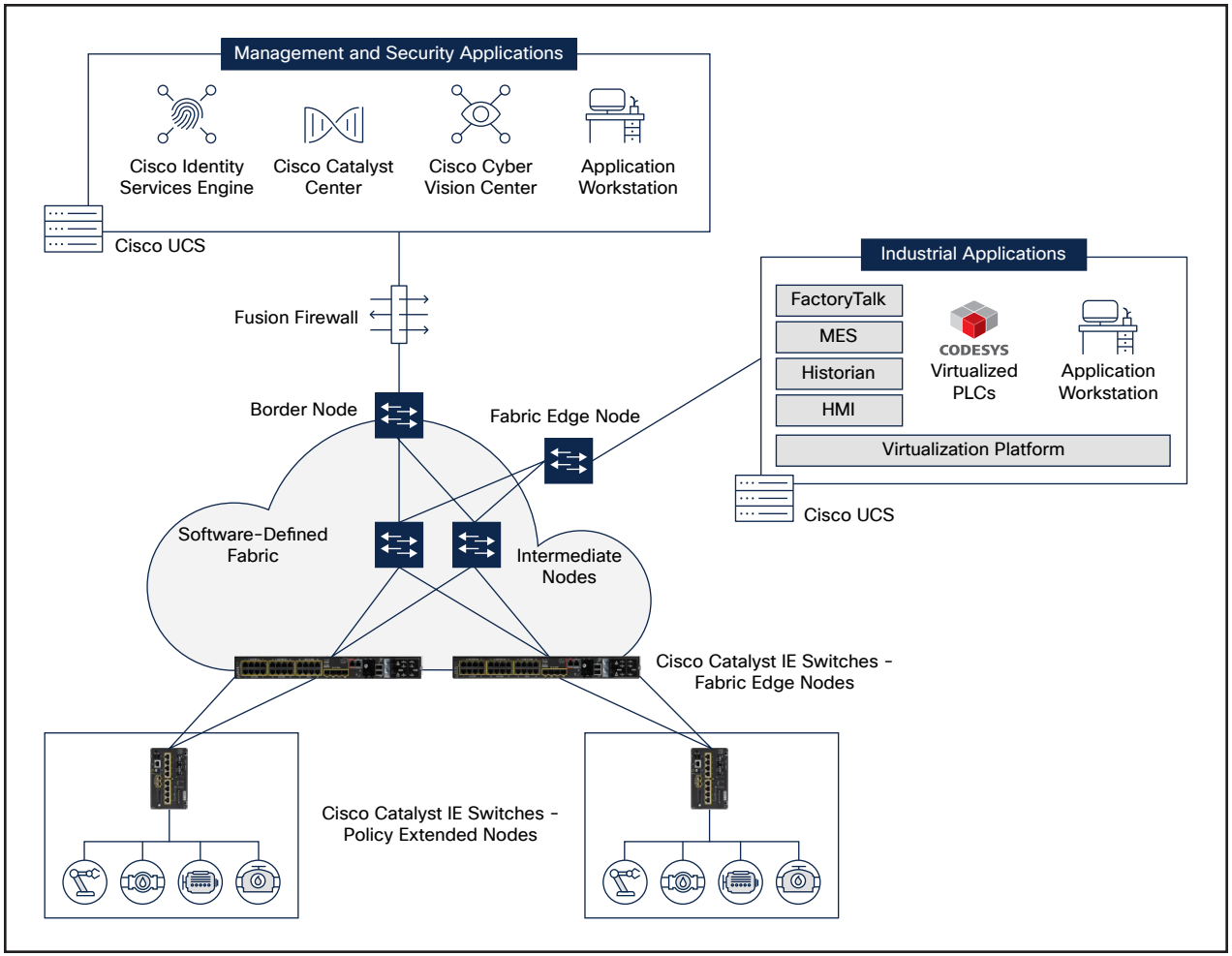

Figure 2. Cisco software-defined industrial network architecture facilitates IACS virtualization

Cisco industrial switches: Cisco Catalyst® Industrial Ethernet switches provide the high-capacity packet switching and lossless resiliency required for uninterrupted connectivity of IACS applications with the controlled machines.

Cisco Catalyst Center: Cisco Catalyst Center (formerly Cisco DNA Center) directs all functions of the network, from onboarding devices to performing initial and ongoing configurations, handling performance monitoring and proactive troubleshooting, defining networking and security policies, and everything else needed for maintaining network performance and security. It enables the software-defined fabric and helps ensure that the network is always ready.

Cisco Software-Defined Network (SDN): An SDN architecture can help automate, scale, and optimize networking. The key benefits of Cisco SDN include increased flexibility, simplified management, automation, scalability, programmability, and improved security. Key components of this architecture include Cisco Catalyst Center as the SDN controller and Cisco Catalyst Industrial Ethernet switches.

By increasing operations flexibility and allowing customization to support diverse requirements SDN offers benefits that are key to virtualizing control systems.

Cisco Cyber Vision: Cisco Cyber Vision is a visibility and threat detection solution dedicated to industrial control systems. It maintains a dynamic inventory of all industrial devices and detects threats and abnormal behaviors in real time so you can control OT (Operational Technology) endpoint compliance and leverage your IT security tools to build security policies that segment your operations and limit spread of potential threats.

Cisco Identity Services Engine (ISE): Cisco ISE facilitates creation of access policies and enforces them through Cisco industrial switches in the network infrastructure, creating segmented operations that keep assets in unrelated parts of the operation separate from one another. It uses asset groups created in Cyber Vision by automation engineers to limit communications between assets and implement zone segmentation as defined by ISA/IEC 62443.

Cisco Secure Equipment Access: Cisco Secure Equipment Access (SEA) is a Zero-Trust Network Access (ZTNA) solution enabling OT vendors and remote experts to easily maintain and troubleshoot remote assets while providing granular access controls to secure industrial operations. It is a hybrid-cloud service that works with a ZTNA gateway embedded in Cisco industrial networking equipment, eliminating the need for specific hardware or extensive VPN infrastructure or jump servers.

CODESYS virtualized controller software: Automation software from CODESYS consists of two basic parts. The CODESYS Development System is an Integrated Development System (IDE) in accordance with IEC 61131-3 for programming the control logic and contains various textual and graphical editors. The application code created is translated into binary code with its own compilers for the respective target hardware. All conditional functions can be configured in the CODESYS Development System, including user interfaces/HMI screens, fieldbus and I/O configuration, safety-relevant logic functions, and data exchange with various other participants in the network, as well as coordinated motion control systems or robot kinematics.

Implementing virtualized IACS

Besides the network, there are four main components required to implement and use virtual control systems:

- A **PLC runtime system** that receives the application code, executes it in real time, reads or writes I/O data from the machine, and provides debugging functions. For use as a virtual controller, the CODESYS runtime system is provided as a platform-independent image and therefore enables the controller to be set up quickly and easily.
- An **Integrated Development System (IDE) for programming PLC applications,** suitable for the PLC runtime system. In addition to Ladder Diagram and Structured Text, the CODESYS Development System also implements the other languages of the IEC 61131-3 international standard and is therefore very well suited for different application areas. It cooperates perfectly with the runtime system and therefore also runs industrial communication protocols such as EtherNet/IP and PROFINET on the virtual controller without the need for additional software. For this purpose, the application code and the protocol stacks used are translated into native machine code for the respective target system by integrated compilers. The IDE can be extended with additional products to create, for example, certifiable safety applications in a project in parallel with the logic applications.
- A **computer architecture with container technology** for virtualization. In principle, this can be any computer system with x86 or ARM processors running an operating system on which containers can be set up. Typically, these are the above-mentioned central hyperconverged infrastructures on Linux-based systems with, for example, Debian Linux and Docker, or Red Hat Enterprise Linux and Podman. The performance of the computer architecture, that is, whether the

virtual controllers run on IT servers, server farms, or discrete edge devices, influences the maximum number of controllers set up in parallel and their performance but makes no difference when it comes to implementation.

- A **platform for orchestrating or deploying** the virtual controller on the target system. In the simplest case, the virtual controller images can be started with Linux board resources, including the container. This gives Linux professionals full access and maximum control. IT administrators, however, prefer to use typical orchestration tools like Kubernetes or OpenShift. However, users of industrial control systems are overwhelmed by these options. Specific tools simplify the use for them. The CODESYS Automation Server, for example, is a web platform hosted on the target system that not only enables convenient orchestration of virtual controllers but also covers other typical tasks, such as the central rollout of applications on identical controllers, collection and analysis of controller data, and central storage of controller projects in the source code. In addition, even the CODESYS Development System offers a straightforward way to define, configure, and start and stop virtual controllers.

Using the CODESYS virtual controller with the integrated deploy tool is faster and easier than with discrete controllers. Users can simply copy the virtual controller image on the target system and, depending on the performance of the target platform, instantiate the image as often as required and configure each virtual controller with the necessary parameters, such as with physical or virtual Ethernet adapters. This enables customers to avoid the cost and hassle of deploying physical devices in the production environment.

When the user starts a virtual controller, a new container is created based on the selected image and started up – just like a real controller. The virtual PLC is therefore immediately available. If the runtime system and the associated IDE are designed from the outset to be manufacturer- and platform-independent, as in the case of CODESYS, their use is no different from that of discrete controllers, with one exception: By encapsulating the virtual controller in the container, the communication gateway between the IDE and the virtual controller must also run in a container. This feature secures the virtual controllers against unauthorized access, in addition to the security aspects mentioned above.

Where do virtualized IACS excel?

So far, two application scenarios have emerged in which virtual controllers have a clear advantage over discrete controllers:

- Production systems and lines that are controlled with many discrete PLCs. In such systems, new functions have traditionally often been implemented using additional discrete hardware, which makes the procurement, installation, and especially the maintenance of these controllers, labor intensive and costly. With virtual controllers, this effort can be massively reduced so that OT teams can accomplish more in less time and focus on more value-added tasks.
- Machines and systems whose IT security is to be hardened using a new application design approach. For this purpose, the entire control application is broken down into individual, independent components. These are executed on separate virtual controllers – just like micro-services in IT. Each controller and the application running on it can therefore be maintained and updated separately or deleted and reinstalled in the event of a compromise. In the event of a successful attack, a virtual controller can be replaced by a new system within seconds, unlike a discrete controller – without the need to replace any hardware.

In addition to these scenarios that have already been tested in practice, there are many other use cases in which virtual control systems have advantages over discrete control systems. In general, virtualization makes it possible to use available performance resources from existing computer architectures without interference.

Get started

Virtualization of IACS is an exciting new development in industrial IoT (Internet of Things), decoupling hardware from the software that runs on it to allow greater flexibility, higher productivity, and lower costs.

However, virtualizing a complex system like IACS requires careful planning and execution. Manufacturers must carefully prepare and plan their transition, starting with a thorough assessment of the existing infrastructure and definition of end goals. They must then select a suitable virtualization platform that meets the specific needs of IACS, upgrade the network if necessary, and implement security best practices like network visibility, segmentation, and continuous monitoring. We recommend a phased approach that starts with virtualizing a non-critical segment of the IACS to test the functionality and identify any challenges before large scale deployment, followed by rigorous testing to ensure real-time response times, and verification of security measures.

To facilitate your journey to virtualization, Cisco offers a comprehensive industrial switching, routing, wireless, and security portfolio, as well as validated design guides for manufacturing that can help remove risk from your deployments.

Watch Dr. Henning Löser, head of the Audi Production Lab, explain how they intend to transform their factories. “To increase security, decrease support requirements, and improve flexibility, Audi is developing its Edge Cloud for Production (EC4P) platform. EC4P virtualizes production assets and relies on software-defined networking by Cisco IoT and enterprise solutions that provide a scalable, resilient, secure, and deterministic network.”

It is not too early to start laying the networking foundation for the future of manufacturing. For specific questions, please schedule a free, no obligation, consultation with a Cisco manufacturing expert.

Learn more

Learn more about Cisco smart manufacturing solutions: Smart manufacturing for the modern age.

About CODESYS

CODESYS is the world’s leading automation software that is independent of device manufacturers. International automation groups, as well as smaller suppliers of controllers for special applications, have implemented CODESYS in their hardware. Currently, CODESYS is used in about 1000 different industrial controllers. Several hundred thousand users from different industries worldwide use the platform to engineer their automation tasks. CODESYS is deployed in paper, printing, and packaging machines, in mobile machines for the construction industry or agriculture, for the automation of power generation and transport systems, and for the intelligent control of large buildings of all kinds.

About Cisco

Cisco Industrial IoT (IIoT) transforms critical industries and improves lives by bringing IT to the physical world to increase business resiliency and employee safety. For over 20 years, Cisco has offered a comprehensive portfolio of industrial switches, routers, wireless, and cybersecurity, which are purpose-built to serve every industrial sector. Cisco’s industrial automation and control networking solutions integrate industrial-strength networking equipment with enterprise-grade network management and security tools and provide validated and field-proven guides designed to accelerate your adoption of and benefit from IIoT.

C22-4309618-00 05/24