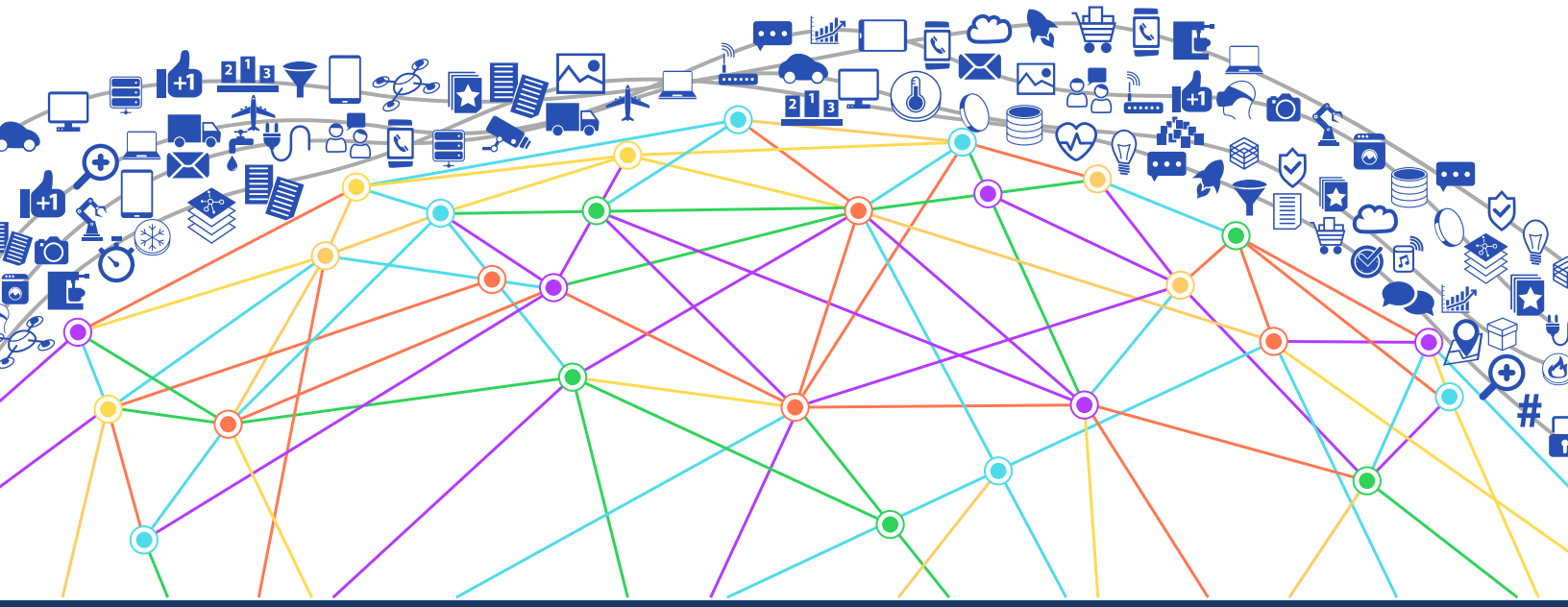
WesternStates CONTROLS



INDUSTRIAL INTERNET OF THINGS

Abstract

The cloud computing market is growing at a rate that is significantly outpacing the traditional, or legacy, IT market. In terms of compounded annual growth rate, or CAGR, there's just no comparison. That trend is expected to continue as cloud adoption continues to grow exponentially.

According to the experts at Statista, the global cloud market will end up at around $495 billion by the end of 2022. Growth is expected to exceed $1.5 trillion by 2030. The cloud services market is growing at around 18-20% per year, CAGR, in comparison to the overall IT market which is growing at around 5%.

Plant automation and process control engineers, technicians, and executives are seeing the tremendous promise of the cloud. They are also facing challenges with the design and adoption of cloud, and hybrid cloud, technology infrastructures.

But what exactly is driving the growth of cloud services? What challenges can industrial sector businesses of all sizes and scopes expect to face with cloud technology design, legacy system migrations, hybrid integrations, and long-term implementations?

What can plant automation, process, and control engineers expect to learn from this white paper?

In this document, we'll examine the issues and benefits associated with industrial-scale cloud adoption in the context of information integrity and security as it exists with today's industrial process and automation technologies. We'll discuss cloud data acquisition, user access, analytics, security, and information technology asset protection challenges. Finally, we'll discuss solutions and security best practices that members of the industrial technology and computing community need to be aware of.

What is the cloud?

At a fundamental level, the public cloud offers technology services along with compute, storage, application, and network resources over the internet. The Microsoft Azure cloud is one of the leading providers of cloud services globally. Azure defines the cloud as:

> ***Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.***

Azure is one of the "big three" public cloud providers, along with Amazon Web Services (AWS), and Google Cloud Platform (GCP). These three global cloud service providers collectively represent over 56% of the cloud services market on a global basis, and they all have their niche.

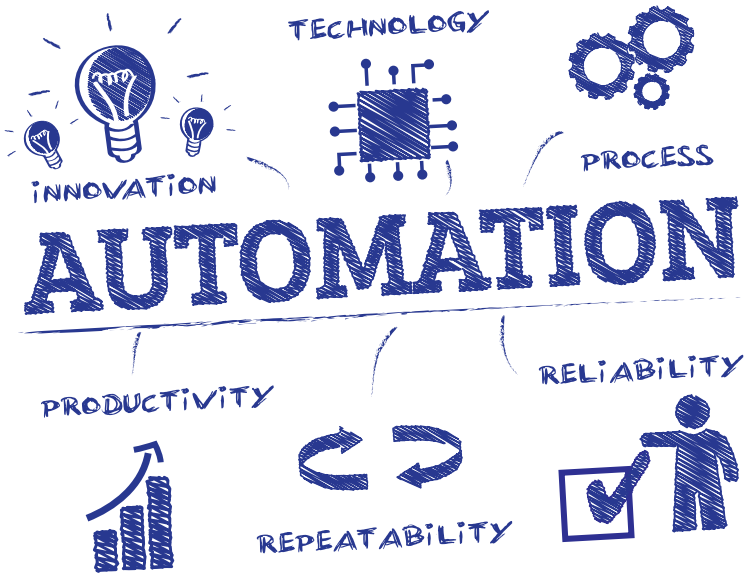
There is no doubt that the cloud offers tremendous promise for the industrial technology sector, which will be discussed in context. But first, let's review the differences between the cloud and legacy IT.

What does a typical process/plant automation IT environment look like?

All plant and process automation environments are different, but there are some commonalities.

Mechanical and electrical machinery, power, devices, processes, people, technologies, and systems comprise workflows that are at the core of every industrial manufacturing process.

All of these devices, machines, technologies, and systems must be assertively monitored and accessible by operators, plant managers, safety professionals, data acquisition tools, and management on a 24X7 basis. Information gathered from these industrial plant assets is utilized to maintain safety, monitor equipment usage and power consumption, manage equipment maintenance contracts, and provide insights that can be analyzed for purposes of plant process optimization.



Some of the more familiar industrial automation and process control systems and functions include:

- SCADA Systems-Supervisory control and data acquisition systems
- DCS and PLC Configuration-Programming and testing of distributed control systems and programmable logic controllers
- HMI-Human machine interface configuration
- Process control and industrial system integrations
- Control Panel Design

At the core of industrial information technology is the data that is collected, processed, and analyzed from the devices, machines, and information systems in the manufacturing or process workflow. These systems are known collectively as the Industrial Internet of Things, or IIoT.

There is typically a data transfer protocol, like Bluetooth, WiFi, etc. that is used to transmit information from devices, for example, industrial devices and machines like valves, pumps, conveyors, etc., to data collection endpoints. These endpoints are most often computers that process the collected information to create an output, such as a safety alert or alarm, or an operator message, etc. This data is also used by business operations professionals and management teams to analyze, improve, and optimize plant processes and workflows.

Industrial data processing endpoints can consist of internet gateways to cloud IIoT infrastructures, computer systems located on-premise, computers in hosted data centers, or a combination of all three.

How does the cloud differ from traditional on-premise industrial process and control IT?

The decision for industrial automation professionals to move IT assets and infrastructure to the cloud is as much about finance and operations as it is about technology.

One of the most basic differences between traditional industrial IT and cloud services comes down to the question of ownership. Who owns, or leases, the real estate where the compute, network, application, and storage assets live? Who owns or leases the physical assets, i.e. computers, storage, network devices, and software applications themselves? From an industrial process user experience perspective, there should theoretically be no difference as to where the IT infrastructure is located, as long as the information is secure and accessible.

In a traditional IT environment, the end-user owns or leases the data center facility, as well as the compute, storage, network, and application assets. IT engineers, administrators, and operations personnel have full, unfettered access to their data center, hardware, and software assets at any time. In traditional industrial IT, the information assets and infrastructure are located in the plant facility itself, or in a hosted data center. These resources are also on the business's balance sheet as depreciating assets.

The cloud transfers ownership from the capital side of the balance sheet to the operational side.

In a cloud computing environment, all compute, storage, application, and network assets are 100% rented, usually on a month-to-month, or hour-to-hour basis. The resource consumer, or user, has no ownership of any real estate or technology assets, and no physical access to them whatsoever. This model can provide a higher level of information security, operational efficiency, and data protection than the legacy paradigm.

Absence of direct ownership is also one of the reasons cloud technology has seen such wide adoption. IT infrastructure and services have been moved from the capital expense side of the equation to the operating expense side. That one simple distinction, along with relinquishing actual asset ownership, can have a massive impact on an industrial business's IT and financial operations.

Since cloud computing assets can be rented on a monthly, weekly, daily, or hourly basis, industrial process and control engineers can use them to precisely match plant production requirements. There is no longer a need to buy excess technology equipment and infrastructure that is designed to meet peak demands. Users often refer to the ability to use cloud resources and services on-demand as "resource liquidity". Information technology can now be used on a just-in-time, just-in-the-right-amount basis with automatic scaling capabilities offered by cloud providers.

What are the primary drivers of a business decision to move IT assets to the cloud?

We discussed the primary financial and operational drivers in the previous section.
In today's world of industrial information technology where requirements move at lightning speed, the cloud can literally be the difference between industrial businesses just staying competitive and dominating their competition. Up-to-the-minute business insights are almost a necessity in today's competitive world of plant operations and manufacturing.

There are, however, additional advantages to using the cloud for process control and automation engineers. These include enhanced security and data protection capabilities provided by the public cloud providers.

Industrial applications from Desktop as a Service (DaaS), to advanced data analytics, can potentially leverage the cloud for the benefit of the business. Serverless technology is also exploding as a game-changing business information management service. As pointed out by tech research giant Forrester "Cloud-native tech consumption will spike, with serverless rising to 25% adoption (by the end of 2021)."

As an example, DaaS platforms can enhance HMI applications by replicating the industrial user's laptop or device-to-machine interface to the cloud for disaster recovery purposes. Likewise, serverless technology allows for unprecedented repeatable, auto-scale capabilities for computing resources based on real-time compute requirements in the plant or facility. The ability for digital resources in the cloud to automatically scale with demand alleviates the need to overprovision on-prem information technologies to meet incidental peak demands. In other words, the past no longer equals the future.

The end goal is to streamline industrial information workflows and workloads, and for industrial IT users to leverage IT assets for the exclusive benefit of business operations. The cloud offers tremendous promise in providing these benefits. But what are the risks?

Section 3.0 Microsoft Azure Cloud security and reliability for plant operations, automation, and industrial control applications

There are three primary functional layers of cloud infrastructure. These layers of abstracted infrastructure include:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

In all cases, the industrial user has pay-as-you-go access to compute, storage, network, and application assets in the cloud. The level of abstraction between the user and the infrastructure defines the level of access.

The Instrumentation, Systems, and Automation Society defines IaaS as:

> ***Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.***

IaaS is essentially virtualized hardware. The hardware in IaaS is operating system, storage, and application agnostic. As the user moves further out into the realm of virtualized software, or virtualized OS, they enter the realm of PaaS. PaaS can also present virtualized development tools and environments to software developers and custom IIoT applications.

The most visible version of cloud infrastructure is Software as a Service, or SaaS. With SaaS, users access software tools through the web, often through a browser, and are completely abstracted from the hardware and software environment that runs the software app in the cloud.

Is the Microsoft Azure Cloud a safe information technology infrastructure for industrial automation?

The answer is a definite yes. But the term "security" can be somewhat subjective.

The Microsoft Azure Cloud provides at-scale security capabilities that are not feasible for even the largest industrial clients. As an example, consider the sheer scale of Azure's network security implementation.

According to ZDNet, Microsoft employs over 8500 cybersecurity professionals and spends over a billion dollars a year on general network security. There is a significant level of advanced network expertise, security, and protection for resources deployed in the Azure Cloud. This level of security is virtually impossible to replicate for most plant operations and industrial control end-users.

End-users can benefit tremendously from the security provided at scale by the Microsoft cloud. However, they are ultimately responsible for designing, building, and maintaining their internal and external network infrastructure for private usage.

Azure provides some valuable insight into its approach to infrastructure security:

> ***Strengthen the security of your cloud workloads with built-in services:***
>
> ***Protect data, apps and infrastructure quickly with built-in security services in Azure that include unparalleled security intelligence to help identify rapidly evolving threats early—so you can respond quickly. Implement a layered, defense in-depth strategy across identity, data, hosts and networks. Unify security management and enable advanced threat protection across hybrid cloud environments.***

Security Basics in the Azure Cloud

Since the cloud is essentially a pay-per-use pool of compute, storage, network, and application resources, when we talk about security benefits, we're really talking about protecting and securing these four tiers of information resources:

- Compute and Storage Asset Protection
- Application Protection
- Access Protection
- Threat Protection

Compute and Storage Asset Protection in the Azure Cloud

The Microsoft Cloud infrastructure protects compute and storage assets at their most fundamental levels of availability. For example, when users create Azure Virtual Machine instances with connected Azure Storage, those assets are automatically replicated in the background.

The Azure infrastructure is designed for its most basic compute and storage elements to be highly available and redundant. This built-in level of reliability and availability of compute and storage infrastructure can be extremely expensive, complex, and challenging to implement in an on-prem IT environment with limited IT resources and budgets. This again speaks to the advantages of provisioning digital resources and services at scale in massive, regionally dispersed data centers.

The strategic benefit of redundancy and automatic data protection to the end-user is hard to place a value on. The challenge for industrial information technology professionals is effectively managing the usage and access to these valuable IT resources in the cloud.

Application Protection

Industrial automation applications can be developed, used off the shelf, or customized in the Azure cloud. Azure provides customized IIoT environments and management infrastructures designed specifically for automation and control technicians and engineers to use. These apps and software products can be managed individually or as part of a larger bundle of software and services in the Azure cloud. Software updates, security patching, and maintenance policies and procedures can also be automated in the cloud.

The ability for technicians and engineers to automate software application maintenance, clustering, replication, and backups in the cloud empowers industrial IT professionals to leverage accessible, affordable digital resources. This can enable streamlined operations and optimized costs

The caveat is that users always need to be aware that they are responsible for their user data, proper backup procedures, and access to their business-critical applications and the information that resides in them. The cloud, however, makes the access and security tools that technicians need accessible, affordable, and available on a pay-per-usage basis.

Identity and Access Management and Control

User access is essentially divided logically into three categories:

- Active Directory Services—these services manage how information about users is stored in directories, how they are grouped, and who has access to different subsets of that information.
- Identity and Access Management—these services, known as IAM, store information about users. IAM systems are used by many other services, like Active Directory, to control access to infrastructure, systems, and applications.
- RBAC—Azure RBAC, or role-based access control, is used to assign permissions to users based on their defined role in the organization

Managing access to resources is a critical aspect of any security ecosystem, and the cloud is no different.

The Azure cloud provides industrial and plant operations users with all of the infrastructure necessary to implement secure access controls as a service. This reinforces the “as a service” model that the cloud provides. Security tools and services are abstracted from physical infrastructure and available to cloud technology end-users in the industrial sector in purpose-built IIoT ecosystems.

It’s important to note that although the infrastructure is in place, significant expertise is still required to implement and enforce access management and control in the Microsoft cloud.

Security Threat Protection

The Microsoft cloud offers threat protection at scale. Industry-tested security policies, best practices, and tools are in place to prevent denial of service (DDoS) attacks, volumetric attacks, HTTP and SQL protocol attacks, etc. on the Azure infrastructure at large.

Some inherent protection against user-level social attacks like Phishing and Ransomeware is built into applications like Exchange and Office 365. Microsoft Defender is also an excellent pay-for-use application for threat management. Although these back-office applications are typically out of the realm of process automation and control professionals, it is important to note that the cloud provides an enterprise-level infrastructure suitable for all aspects of the information technology ecosystem of an industrial organization of any size or scope.

Conclusion

The Azure cloud provides digital resources and services at a scale that were previously not available to industrial, plant, control, and process engineers and technicians. Digital resources are presented to users on a pay-for-usage, pay-by-the-hour basis in secure data centers strategically located globally for enhanced data protection capability and accessibility.

At-scale compute, storage, network, and application infrastructures combine with granular IIoT microservices and frameworks to provide end-to-end digital solutions for process control engineering designed for the next generation of plant operations.

There is no doubt that the cloud offers inherent infrastructure and resource security capabilities that are simply not available to traditional IT users. Microsoft continues to spend billions of dollars on infrastructure and human resources to provide an unrivaled technology environment for secure computing.

The Microsoft Azure cloud offers tremendous promise to be sure. Significant expertise is still required to make all of the moving parts work like a well-oiled machine for the process automation and industrial end-user. However, the cloud provides access to the secure infrastructure, services, tools, and financial model that it takes to build the next generation of plant, control, and automation solutions.