Cloud: Experience It Before Making Your Decision!

Authors

Chris Crowley, Big River Steel – A U. S. Steel Co., Osceola, Ark., USA
ccrowley@bigriversteel.com

Aurobinda Laha, Manager – IT (Cloud & AI), Big River Steel – A U. S. Steel Co., Osceola, Ark., USA
alaha@bigriversteel.com

Pedro Ruiz, Tamdrea, Cypress, Texas, USA
pedro.ruiz@tamdrea.cloud

In today's rapidly evolving technological landscape, cloud computing has emerged as a pivotal solution for businesses across various industries. However, the decision to adopt cloud technologies in the industrial sector should not be taken lightly. This article emphasizes the importance of first-hand experience with cloud solutions before committing to their implementation. By engaging in pilot projects or proof-of-concept (PoC), trials, and hands-on evaluations, organizations can better understand the practical benefits and potential challenges associated with cloud adoption. This approach allows businesses to assess the suitability of different cloud architectures and service providers, evaluate security measures, and ensure compatibility with existing data models and infrastructure. Additionally, gaining experience helps in identifying the necessary skills and expertise required for a successful transition to the cloud. Ultimately, experiencing cloud technologies firsthand enables informed decision-making, reduces risks and maximizes the potential for achieving strategic business objectives. This article explores the steps involved in developing and executing a successful cloud pilot project, specifically from the perspective of smart manufacturing implementation.

Introduction

The manufacturing industry is undergoing a significant transformation, driven by the adoption of cloud technologies. Cloud computing offers unparalleled scalability, flexibility and cost-efficiency, making it an essential component of modern manufacturing operations. However, the journey to the cloud is full of potential pitfalls that can undermine these benefits if not navigated carefully. According to a study by Nordcloud, effective decision-making is crucial throughout the cloud adoption process to avoid misalignment and delays.[1] Similarly, Comarch highlights the importance of a structured cloud adoption strategy that aligns with business goals and enhances operational efficiency.[2] Additionally, Science Times emphasizes the need for thorough migration planning and selecting the right cloud provider to ensure a smooth transition.[3]

One of the primary reasons for experiencing cloud technologies firsthand is to gain a comprehensive understanding of the practical implications of cloud adoption in the manufacturing sector. Pilot projects and trials provide valuable insights into how cloud solutions perform in real-world scenarios, allowing organizations to identify potential challenges and address them proactively. This experiential approach helps businesses evaluate the suitability of different cloud service providers, ensuring that they choose a provider that aligns with their specific needs and objectives.

Security is another critical factor that must be considered when adopting cloud technologies. By engaging in hands-on evaluations, organizations can assess the security measures implemented by various cloud providers and determine whether they meet their standards. This is particularly important given the increasing prevalence of cyber threats and the need to protect sensitive data.

Furthermore, experiencing cloud technologies firsthand allows manufacturing organizations to evaluate

the compatibility of cloud solutions with their existing data models and infrastructure. This ensures a seamless integration process and minimizes disruptions to business operations. It also helps in identifying any necessary adjustments or upgrades that may be required to optimize the performance of cloud solutions.

In addition to technical considerations, the transition to cloud technologies requires a skilled and experienced workforce. By engaging in pilot projects and trials, organizations can identify the specific skills and expertise needed for successful cloud adoption. This enables them to invest in the necessary training and development programs to build a capable team that can effectively manage and operate cloud solutions.

Ultimately, experiencing cloud technologies firsthand enables informed decision-making, reduces risks and maximizes the potential for achieving strategic business objectives. By taking a proactive approach and thoroughly evaluating cloud solutions before making a commitment, manufacturing organizations can ensure a smooth transition to the cloud and fully leverage its benefits to drive sustainable growth and innovation.

Smart manufacturing is a transformative approach that leverages advanced technologies, such as cloud computing, artificial intelligence (AI), Internet of Things (IoT) and data analytics, to optimize production processes, improve product quality and reduce costs. A cloud pilot project is an essential step in implementing smart manufacturing, allowing organizations to test and refine their strategies before scaling up.

Discussion

Key Considerations for Developing a Proof of Concept

Implementing a pilot project effectively involves a series of well-planned steps to ensure that the project runs smoothly and provides valuable insights. The following points were considered for the PoC:

Define Clear Objectives

- Identify goals: Clearly define what you aim to achieve with the pilot project. This could include testing feasibility, assessing performance or identifying potential issues. For example, if you're in the manufacturing industry, you might want to test a new cloud-based inventory management system.
- Set metrics: Establish specific metrics to measure the success of the pilot project. These could be related to performance, cost, user satisfaction or other relevant factors. Metrics might include system uptime, user adoption rates or cost savings.

Plan

- Develop a detailed plan: Outline the scope, timeline, resources and responsibilities for the pilot project. Ensure that all stakeholders are aware of their roles and the project's objectives. For instance, create a project timeline that includes key milestones and deadlines.
- Risk management: Identify potential risks and develop strategies to mitigate them. This includes technical, operational and financial risks. For example, consider potential cybersecurity threats and plan how to address them.

Select the Right Participants

- Choose a representative sample: Select participants who represent the broader user base or target audience. This ensures that the pilot project results are relevant and applicable to the larger implementation. In a manufacturing context, this might include selecting a few production lines or departments to participate.
- Engage stakeholders: Involve key stakeholders early in the process to gain their support and ensure their needs are considered. This could include managers, information technology (IT) staff and end users.

Execute the Pilot

- Implement the plan, follow the detailed plan and ensure that all activities are carried out as scheduled. Monitor progress closely and make adjustments as needed. For example, regularly check in with participants to ensure they are following the new processes.
- Collect data: Gather data on the performance of the pilot project. This includes quantitative metrics as well as qualitative feedback from participants. Use surveys, interviews and system logs to collect comprehensive data.

Evaluate Results

- Analyze data and costs: Review the data collected during the pilot project to assess its success. Compare the results against the predefined metrics and objectives. For instance, analyze whether the new system improved inventory accuracy and reduced costs.
- Identify learnings: Document any lessons learned, including what worked well and what could be improved. This information is crucial for refining the larger implementation. Create a report summarizing the findings and recommendations.

Make Informed Decisions

Decide on the next steps: Based on the evaluation, decide whether to proceed with a full-scale implementation, adjust or abandon the project. For example, if the pilot

was successful, plan the rollout to additional production lines or departments.

Communicate findings: Share the results and recommendations with all stakeholders to ensure transparency and buy-in for the next steps. Hold a meeting or send a detailed report to all parties involved.

What Is Cloud Computing?

Cloud computing is the on-demand delivery of computing resources, such as servers, storage, databases, networking, software and more, over the internet. Instead of owning and maintaining physical data centers and servers, businesses can access these resources as needed from a cloud service provider, typically on a pay-as-you-go basis.[4]

Advantages of Cloud Computing

- Cost Savings: Reduces the need for physical hardware and maintenance, lowering capital and operational expenses.[4,5]
- Scalability: Easily scale resources up or down based on demand, ensuring optimal performance without overinvesting in infrastructure.
- Accessibility and mobility: Access data and applications from anywhere with an internet connection, supporting remote work and collaboration.
- Reliability: Cloud providers offer robust disaster recovery and backup solutions, ensuring business continuity.
- Automatic updates: Software and security updates are managed by the cloud provider, reducing the burden on IT staff.[5]

Disadvantages of Cloud Computing

- Security and privacy: Storing data off-premises can raise concerns about data security and compliance.
- Downtime: Dependence on internet connectivity means that outages can disrupt access to cloud services.[4]
- Limited control: Users have less control over the infrastructure and may face restrictions imposed by the cloud provider.
- Potential costs: While cost-effective, unexpected usage spikes can lead to higher-than-anticipated expenses.[4,5]

Types of Cloud Architecture

Public Cloud

- Description: Services are delivered over the internet by third-party providers like AWS, Google Cloud, Oracle and Azure.
- Advantages: Cost-effective, scalable and easy to deploy.
- Challenges: Potential security and compliance concerns.

Private Cloud

- Description: Dedicated to a single organization, hosted either on-premises or by a third-party provider.
- Advantages: Greater control over security and compliance, customizable to specific business needs.
- Challenges: More expensive to maintain and manage.

Hybrid Cloud

- Description: Combines public and private clouds, allowing data and applications to be shared between them.
- Advantages: Flexibility to move workloads between environments, optimized cost and performance.
- Challenges: Complex to manage and integrate.

Multicloud

- Description: Uses multiple cloud services from different providers.
- Advantages: Avoids vendor lock-in, optimizes performance and cost, enhances redundancy.
- Challenges: Requires careful management and integration.

Community Cloud

- Description: Shared by several organizations with common goals or regulatory requirements.
- Advantages: Collaborative approach, balances cost and security.
- Challenges: Limited control compared to private cloud, potential for conflicts in shared resources.[4,5]

Each type of cloud architecture has its own set of benefits and challenges, making it essential to choose the one that best aligns with your business goals and requirements.

The Proof of Concept

The objective of the PoC was to demonstrate the potential of implementing smart manufacturing technology as well as generate a data repository to access it through the cloud-native applications or AI-based technologies in a cloud environment within the existing infrastructure, while respecting strict security protocols, as well as identifying specific needs such as data processing speed and integration with current systems. This initiative sought to establish a noninvasive smart manufacturing solution that would seamlessly integrate with existing production processes without causing disruption, ultimately leading to optimal use of existing resources.

Figure 1

ANSI/ISA 95 Standard.

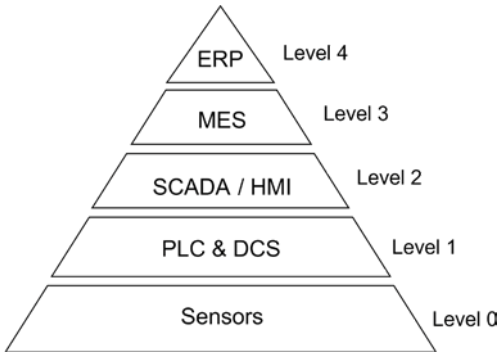
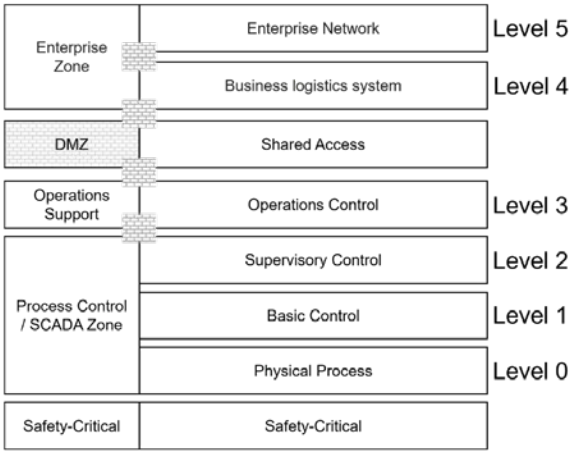


Figure 2

Purdue Model.



Data Transport Chain Based on the ANSI/ISA 95: The PoC was designed to interface with an existing configuration based on the automation pyramid, defined by the ANSI/ISA 95 standard[6] as shown in Fig. 1, which is a model for the integration of business and control systems at hierarchical levels and provides a standard for the integration, focusing on information exchange and interoperability. This model is crucial to ensure efficient data flow and communication within industrial and manufacturing operations.

Security Based on the Purdue Model: The main purpose of the Purdue Model (Fig. 2), also known as the Purdue Enterprise Reference Architecture (PERA), is to provide a structured framework for integrating and securing industrial control systems (ICS) and enterprise systems. The Purdue Model is indispensable for ICS security due to its multifaceted benefits:

- Defense-in-Depth: The model's layered architecture creates multiple security checkpoints, making it more challenging for cyber threats to infiltrate critical systems.
- Risk mitigation: The isolation of critical components minimizes the potential for unauthorized access and accidental damage, safeguarding operational integrity.
- Enhanced visibility: The clear segmentation provided by the model facilitates comprehensive monitoring and threat detection, enabling proactive incident response.
- Regulatory compliance: The alignment with industry standards like IEC 62443 ensures adherence to best practices and regulatory requirements.[7]

How Do Purdue Model and ANSI/ISA 95 Complement Each Other? The Purdue Model and the ANSI/ISA 95 standard are two frameworks used in industrial automation and manufacturing environments. They serve different but complementary purposes, and their integration can create a robust framework for industrial control systems. Both models provide a hierarchical structure, enhancing their compatibility. However, in terms of security and interoperability, the Purdue Model emphasizes network segmentation and security, while ISA-95 focuses on standardized information exchange and interoperability. The Purdue Model's role in security is particularly clear and well defined. Additionally, the hierarchical structure of the Purdue Model supports scalable integration, while the detailed models of ISA-95 help manage and optimize production processes. By combining the strengths of both models, organizations can create a comprehensive framework that enhances security, efficiency and scalability in industrial automation environments.

Challenge to Fit Into the Purdue Model: One of the challenges in using the Purdue Model is that there is a new player: the cloud. This new player represents significant challenges to the Purdue Model by in many cases bypassing some traditional hierarchical levels and allowing direct communication from physical devices to cloud services or through edge devices to the cloud. In smart manufacturing deployments, data is not constrained by traditional Purdue hierarchies and no longer resides entirely within the enterprise. Consequently, the Purdue Model can be considered obsolete in these new environments.

In traditional operation technology (OT) environments, efforts are underway to understand how smart manufacturing impacts the Purdue Model. Some organizations have modified the traditional Purdue Model to incorporate smart manufacturing components. For example, the European Union Agency for Cybersecurity[8] has proposed a revised version of the Purdue Model that recognizes a level 3–based industrial smart manufacturing

platform, which communicates directly with level 1 devices. However, it should be noted that this model focuses on leveraging new technologies to deliver secure products and services, rather than retrofitting its solutions to preexisting architectures. However, the goal of this PoC is to demonstrate that it is possible to integrate the cloud environment with existing production processes without causing disruption or compromising security.

Making the Connection: Data processing speed and integration with current systems are essential for the success of the PoC. However, it is important not to compromise security and the existing ecosystem to achieve these goals. Following the Purdue Model, the communication line to the data source is situated in the demilitarized zone (Fig. 3). The DMZ serves as a buffer between the operational technology (OT) and information technology (IT) environments, enhancing security by preventing direct access between these two domains. This configuration establishes a logical connection to the existing on-premises cloud, where services collect data from two sources located at levels 2 and 3.

For this PoC, data acquisition includes a server with a message queuing telemetry transport (MQTT) broker, which supports up to 1,000 tags. MQTT is a lightweight messaging protocol. Production data is also gathered from an SQL server, which stores structured data in a relational database format. The information collected from both sources pertains to a galvanizing line.

In this setup, data from both the MQTT process and the SQL database is sent to a MongoDB (NoSQL) database located in the Azure Cloud, and all the information collected is displayed on a webpage that users can access within the organization's network. As shown in Fig. 4, all connections are established using transport layer security (TLS).

TLS is a cryptographic protocol designed to ensure privacy, data integrity and authentication for secure communications over networks. TLS components include encryption to protect data from unauthorized access, authentication to verify the identities of communicating parties, and integrity to ensure data is not altered during transmission. The TLS handshake is a process where the client and server agree on encryption methods and establish a secure connection. TLS certificates, issued by certificate authorities, authenticate servers to clients.9

TLS ensures data integrity using hash functions and message authentication codes (MACs). When data is transmitted, TLS uses cryptographic hash functions to create a unique fingerprint (hash) of the data. This hash is sent along with the data. Additionally, a MAC is generated using a secret key and the data itself, and this MAC is also sent with the data. Upon receiving the data, the recipient uses the same hash function and secret key to generate a hash and MAC, then compares these with the received hash and MAC. If they match, it confirms that the data has not been altered during transmission. This process protects against data tampering and ensures that the data received is exactly what was sent.[9]

Finally, all the software involved in the PoC was developed and deployed using container[10] technology within a Linux environment. This approach ensures a high level of robustness and isolation, which are critical for maintaining the integrity and security of the system. Container technology allows for the creation of isolated virtual environments (Fig. 5), where each process can run independently without interfering with others. This isolation is not limited to processes within the same virtual

Figure 3

Purdue Model, customized.

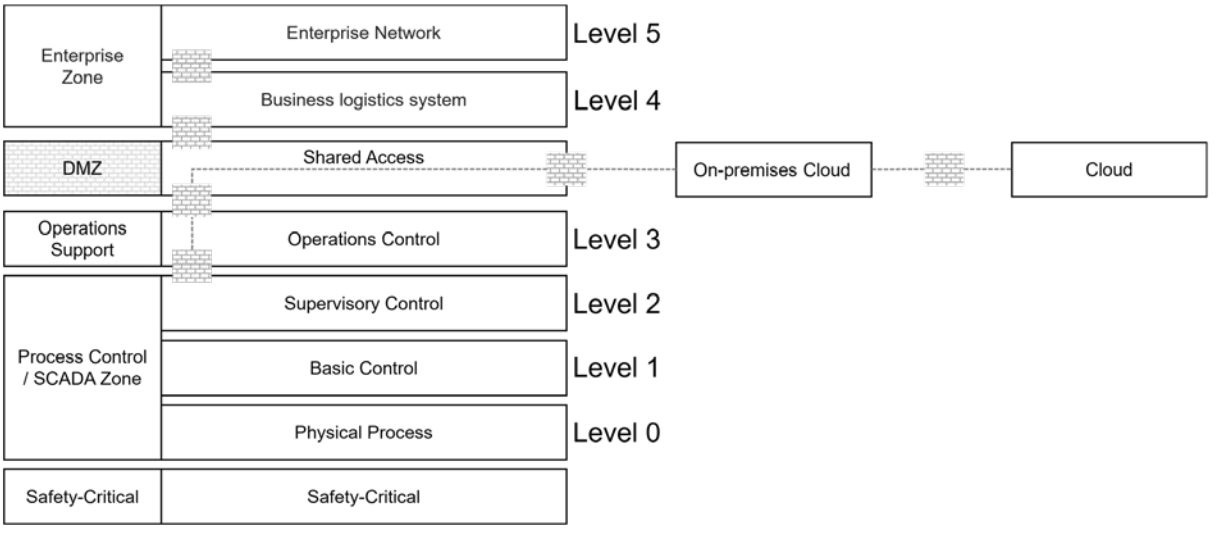
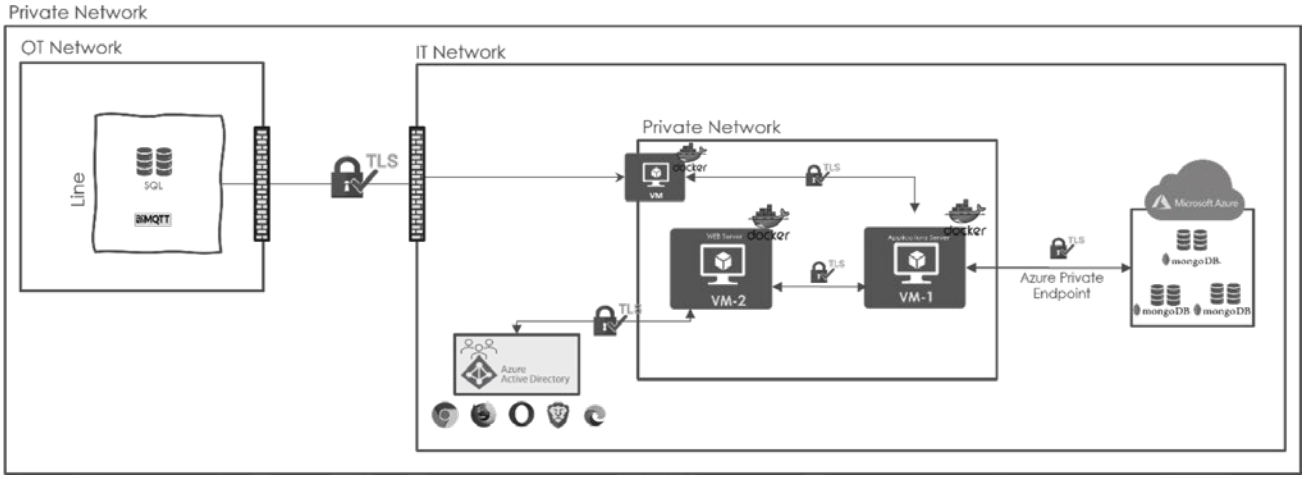


Figure 4

Diagram of interconnection.



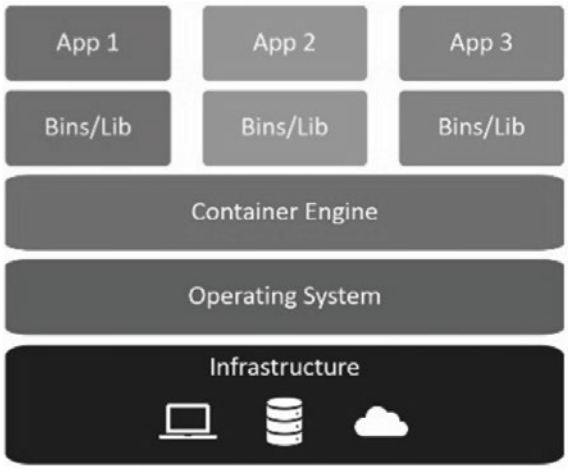
location but extends to remote locations as well, enabling seamless and secure communication across different environments. By leveraging container technology, the PoC benefits from enhanced scalability, as containers can be easily replicated and managed across various platforms. This flexibility ensures that the system can adapt to changing demands and workloads without compromising performance. Additionally, the use of containers simplifies the deployment process, as applications and their dependencies are packaged together, ensuring consistency across different stages of development and production. Furthermore, container technology enhances the overall security posture of the PoC by isolating applications and minimizing the attack surface. Each container operates in its own secure environment, reducing the risk of vulnerabilities spreading across the system. This robust isolation also facilitates easier management and monitoring of individual components, allowing for quicker identification and resolution of potential issues. In summary, the adoption of container technology in the PoC provides a comprehensive solution that combines robustness, isolation, scalability and security, ensuring the successful implementation and operation of the system.

Conclusions

The advent of cloud computing has revolutionized modern life, and its significance is poised to escalate in the coming years. However, this shift also introduces substantial cybersecurity risks that demand swift and effective mitigation strategies. Prioritizing security during the transition process is crucial to navigating these challenges.

Figure 5

Container methodology.



The steel industry is on the cusp of a transformative journey, driven by the adoption of cutting-edge technologies. To stay ahead of the curve, it's essential to leverage tools like AI and machine learning. A practical approach to harnessing these innovations involves conducting a proof of concept focused on real-world applications. By doing so, organizations can pinpoint strengths and weaknesses, identify best practices, and unlock the full potential of emerging technologies.

References

1. S. Maas, "Make Better Decisions in Your Cloud Journey," https://nordcloud.com/blog/decision-making-a-key-success-factor-in-your-cloud-journey.
2. "Cloud Computing in Manufacturing: Benefits and Use Cases," COMARCH, July 2024, https://www.comarch.com/trade-and-services/ict/news/cloud-computing-in-manufacturing-benefits-and-use-cases.
3. S. Guduru, "Cloud Adoption and Migration Best Practices Key Points to Include," November 2024, https://www.sciencetimes.com/articles/51584/20241112/cloud-adoption-and-migration-best-practices-key-points-to-include.htm.
4. S. Susnjara and I. Smalley, "What Is Cloud Computing?" IBM, https://www.ibm.com/think/topics/cloud-computing.
5. "What Is Cloud Architecture? Understanding the Building Blocks of the Cloud," Digital Ocean, https://www.digitalocean.com/resources/articles/cloud-architecture.
6. "Purdue Model for ICS Security," Fortinet, https://www.fortinet.com/resources/cyberglossary/purdue-model.
7. "Beyond the Pyramid: Using ISA 95 for Industry 4.0 and Smart Manufacturing," https://www.isa.org/intech-home/2021/october-2021/features/beyond-the-pyramid-using-isa95-for-industry-4-0-an#:~:text=The%20ISA95%20functional%20model%20(figure,the%20systems%20supporting%20the%20functionality.
8. "Good Practices for Security of Internet of Things in the Context of Smart Manufacturing," ENISA, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.
9. "What Is TLS (Transport Layer Security)?" Cloudflare, https://www.cloudflare.com/learning/ssl/transport-layer-security-tls.
10. "What Is Containerization?" AWS, https://aws.amazon.com/what-is/containerization.

AISTech This paper was presented at AISTech 2025 — The Iron & Steel Technology Conference and Exposition, Nashville, Tenn., USA, and published in the AISTech 2025 Conference Proceedings.