CLOUD COMPUTING IMPLICATIONS for Manufacturing Execution Systems

By Paul Irving, Gregory M. Ruklic, and Jonathan Hurle

Cloud computing can be described as networked access and utilization of configurable computing resources such as data and information storage, processing capabilities, applications, and other services on computerized systems provided and/or maintained by a remote organization. As life sciences companies consider the advantages and costs of utilizing cloud services, they first need to invest resources to understand the cloud-based model and implications for applying it in design or migration of the manufacturing execution systems (MES) domain.

The MES domain is defined as all systems with some functionality related to, or otherwise supporting, manufacturing operations [1]. This includes systems such as, but not limited to, enterprise resource planning (ERP), automation, document control (standard operating procedures management), MES software (e.g., recipe and batch management), and laboratory information systems (LIMS).

The impetus for moving to a cloud-based model is to keep various life sciences manufacturing organizations focused on their core businesses while outsourcing computer resources and related activities as necessary to expert providers. For further information on cloud computing standards, refer to the National Institute of Standards Technology's "The NIST Definition of Cloud Computing" [2], and "NIST Cloud Computing Standards Roadmap" [3], which are recommended resources for definitions and other information about cloud computing. For a visual representation of characteristics, service models, and deployment models of cloud computing identified by NIST [2], see Figure 1.

INTRODUCTION TO TECHNOLOGY TYPES

Cloud-based services are typically provided to the end user (your organization) by an external cloud service provider (CSP). Cloud architectures provide a virtualization methodology whereby end users experience computer system–related actions and interfaces running normally in their view regardless of the global CSP location. Dedicated groups within the end user organization may also provide cloud-based services to regional or global facilities without being physically located in those facilities.

This article focuses on three cloud computing service delivery models as defined by NIST [2], each with various advantages and risks for life sciences companies.

- Software as a service (SaaS). The end user accesses applications hosted and managed by the CSP. Data created or utilized by the application reside on the infrastructure belonging to the CSP. Applications are often provided by a CSP; however, applications may be developed by the end user and subsequently hosted and managed by the CSP. The end user does not manage the underlying cloud infrastructure. The end user may define specific configuration parameters of remote applications.
- Platform as a service (PaaS). A CSP hosts a computing platform (hardware, operating system, etc.) accessible to the end user, and the end user installs and manages either their own purchased applications or apps created using tools provided by the CSP. The platform may include network and other connectivity as well as servers and storage devices/systems. The end user does not manage the underlying cloud infrastructure.
- Infrastructure as a service (IaaS). The end user organization typically provides and controls the applications and operating

Figure 1: Visual model of cloud computing.

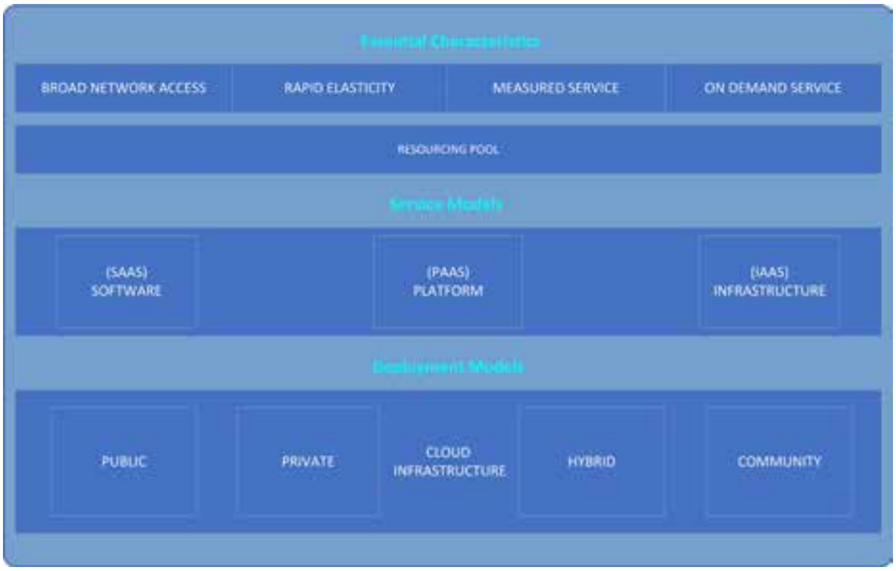
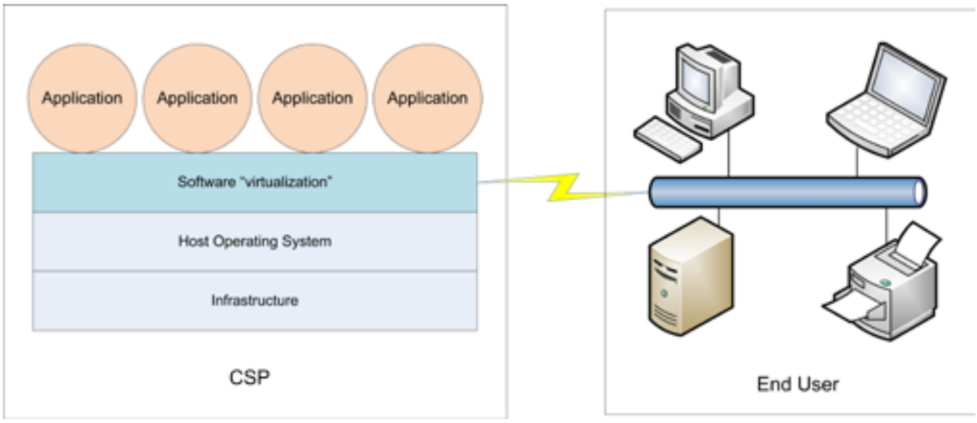


Figure 2: Functional interface overview.



system environments. The CSP is responsible for all underlying computer system architecture, such as networks, servers, processors, and utility or system support software. Depending on company requirements, the end user may control security software such as firewalls, or they may cede control of that software to the CSP.

The three cloud models can be referenced collectively as XaaS. Figure 2 illustrates how XaaS service delivery types can operate in the production environment.

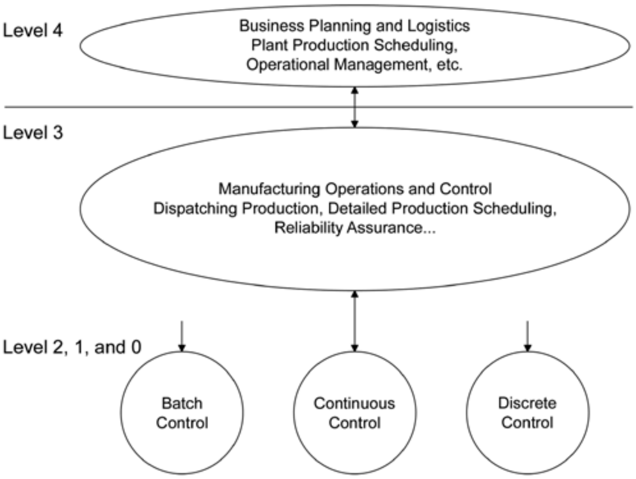
BUSINESS DRIVERS

As part of the ISPE Pharma 4.0™ initiative, companies have opportunities for an increasingly globalized supply chain, improved compatibility of systems and data, and cost optimization. The use of XaaS technologies helps businesses cost effectively and efficiently provide products and services of the highest quality. XaaS can offer the following benefits:

- Reduced internal departmental requirements for designing, installing, and maintaining sophisticated technologies allow internal personnel to be more focused on the actual output of products and services.
- Global deployments can be managed from a single source or a reduced number of sources.
- Instead of managing internal technical environments daily, quality departments can use audits and other periodic oversight to monitor the CSP's quality management system.

To achieve the desired return on investment, companies with diverse suites of products may utilize multiple XaaS delivery

Figure 3: ANSI/ISA-95 functional hierarchy. (Reprinted from *GAMP® Good Practice Guide: Manufacturing Execution Systems* [1].)


Level 4
Business Planning and Logistics
Plant Production Scheduling,
Operational Management, etc.
Level 3
Manufacturing Operations and Control
Dispatching Production, Detailed Production Scheduling,
Reliability Assurance...
Level 2, 1, and 0
Batch Control
Continuous Control
Discrete Control

models to minimize costs and maximize benefits for each location or process.

The choice of whether to implement IaaS, PaaS, or SaaS should be based on a strategic assessment—a documented examination of the existing company technology processes and performance, as well as the desired future state. This process will be described later in this article.

MES AND THE CLOUD

As noted previously, the overall production environment, or MES domain, is composed of multiple functions provided by various technologies; examples of MES technologies are material management for materials master and inventory data, automation/equipment for processes, recipe management and production records, and quality material testing and status control. From the end user's perspective, a properly vetted single-source XaaS integration of MES functionality may be more cost effective to implement and maintain over time than traditional onsite client-managed systems and infrastructure. The business would typically perform a cost/benefit analysis as part of the strategic assessment to determine the value of using external sources for software and hardware provision or management.

In the design of the MES domain, as noted in *GAMP® Good Practice Guide: Manufacturing Execution Systems* [1], the layers defined by the Purdue Enterprise Reference Architecture incorporated in the ANSI/ISA-95 [4] (IEC 62264 [5]) Enterprise-Control System Integration Standard (see Figure 3) are not tied to any specific hardware or system. Instead, the architecture describes the functionality to be provided by any appropriate computerized system.

In the ISA-95 model, levels 0, 1, and 2 control the execution of defined operations for manufacturing. Level 3 system functions execute the production plan determined at level 4 by the business. The life sciences industry has, for better or worse, assigned whole systems such as ERP or LIMS to only one of the model layers, which has led some professionals within the industry to conclude that the ISA-95 model is not applicable to cloud computing or Pharma 4.0™. However, given the complexity and broad range of functionality in some computerized systems, the ISA-95 model describes an approach whereby functionality residing within any given system is assigned to the appropriate ISA-95 model layer.

For example, some ERP systems contain weigh/dispense functions tied to hardware scales or other automation devices. The business functions of the ERP system reside at the top layer of the ISA model, whereas recipe and dispensing operations are found in lower layers of the model. When considering cloud paradigms, the thought process in modeling and designing the manufacturing environment still basically fits the ISA-95 hierarchical approach.

The life sciences industry is discussing how to apply big data and analytics to level 4 planning systems as well as interactively at level 3, where MES functions such as recipe/batch control, resource management, and production results receive planning information from level 4. These concepts are related to Pharma 4.0™, whereby future big data and analytics will interact with systems at several levels. The details of this industry discussion are beyond the scope of this article; readers are encouraged to use expert resources in planning migrations for MES functionality to the cloud as the evolution of Pharma 4.0™ takes place. One recommended resource with advanced information is "Formalizing ISA-95 Level 3 Control with Smart Manufacturing System Models" published by NIST [6].

In this article, we focus on migrating typical systems functionality and technology in the MES domain to the cloud, although the methods of analysis and planning apply to future paradigms as well. The strategic assessment discussed in this article includes consideration of smart manufacturing, the Internet of Things (IoT), and Pharma 4.0™ to help the end user organization determine the need and methodology to move to those paradigms.

The MES domain of functions can be more complex to analyze for cloud implementations than for business functions alone. GxP production in continuous and live processes often requires data, recipes, quality unit disposition status, and other timely information from electronic production records at any hour from anywhere in global operations. To determine which cloud services models could be best applied to specific facilities and manufacturing processes, the business analyzes production requirements from all manufacturing operations, assessing both current and planned future methodologies. The organization conducts a similar assessment when migrating the existing MES domain to a cloud-based model, with the added constraints that the end user must maintain existing functionality and execute validation activities to demonstrate equivalency of functionality between the existing MES domain and the proposed cloud-based version. A critical decision for the end users is whether to move functionality related to real-time automation and sensor monitoring (including the IoT) to the cloud.

INITIAL STRATEGIC CHALLENGES

Typically, an organization embarking on use of cloud computing methodologies faces the following challenges:

- The organization may lack sufficient cloud experience to develop a cohesive strategy; thus, the goals to be achieved by means of cloud computing are neither clear nor verifiable.
- Critical elements in the introduction process are overlooked due to poor planning or lack of resources. For example, an organization may not fully understand that CSPs themselves often obtain services (e.g., administration or backup of data) from subcontractors; therefore, the organization does not consider how cloud service subcontracting may affect its operations. Subcontractors could increase the risk that personal or proprietary data are leaked in an unauthorized or unintended manner (with possible legal consequences), or a security certificate might be jeopardized because an auditor cannot audit CSP subcontractors. Additionally, business continuity planning and contingencies from the CSP, as well as overall planned integration of cloud services with the client's subcontractors might be inappropriate for the criticality of certain manufacturing operations.

ACCESS CONSIDERATIONS

Systems in the MES domain often require uninterrupted 24/7 operations. Local business operations, especially globally spaced operations, need to access services continuously for time zones different from CSP locations. Access considerations become more complex when CSP applications and local site systems require strict coordination to achieve production with real-time automation systems. Some major considerations are:

- Time stamps for production records, activity logs, and audit trails must be presentable in human-readable format in the context of the local site time of creation/execution for business operations, internal investigations, and regulatory audits.
- Remote data download/upload requirements must be clearly defined and implemented.
- Application interfaces must operate smoothly and efficiently and provide immediate access to production systems, including timely presentation of operator instructions and recording of operator responses.
- Timely coordination of quality unit assessments of activities across systems must be achieved.
- Gating operations must be well defined for activities related to electromechanical systems sequencing and recipe execution, with timely approval steps for production and quality unit personnel.
- Master data for continuous processes must always be available by verified means for reference by real-time downstream systems.
- Updates to master data must be carefully coordinated between end users and CSPs to prevent disruption of operations or unintentional changes to recipes or other processes.
- Inventory usage, creation, and disposition updates across facilities, production lines, and processes must be coordinated.
- Alert/alarm management for production records with timely access to manufacturing and quality unit review/approval must be achievable.
- Timely access must be provided to historical data in formats conforming to regulatory requirements and business analysis.

IT risks related to access of cloud-based systems include:

- Internet/international network disruptions
- Local network disruptions (for the CSP or the end user)
- Inadequate pause and resynchronization methods and algorithms
- Poor data transmission verification
- Data comingling among clients on common servers/systems
- Inadequate disaster recovery elements or lack of coordination between business and provider network facilities and human communications
- Unacceptable provider response times for errors and outages during real-time operations
- Lack of procedures and methods for remote (provider) data correction due to process control upsets coordinated with the business

XAAS MODEL-SPECIFIC CONSIDERATIONS

Each of the XaaS service delivery models may provide a range of risks and benefits for end users [3, 7].

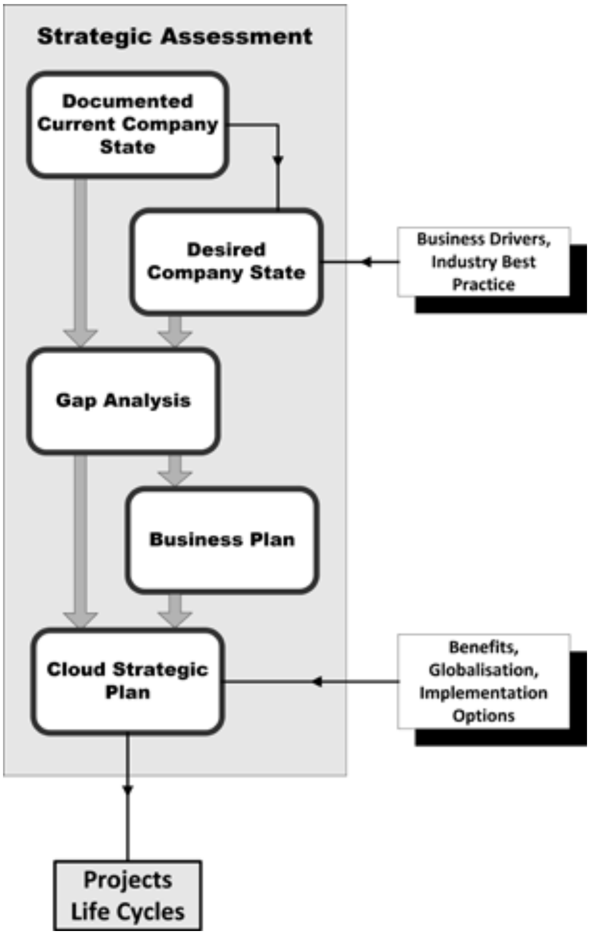
- SaaS. The end user is highly reliant on hosted operational functionality because master, production master, and original data are typically stored in the cloud. SaaS can provide substantial cost savings to end users, but it may require considerable effort to interface with local automation systems.
- PaaS. Standardized applications may not fit end user needs and desires across global sites, languages, and cultures. However, PaaS can reduce verification efforts and software maintenance costs.
- IaaS. Because infrastructure setup/maintenance by end user subcontractor(s) is already a common practice, IaaS is typically the least risky type of XaaS, with relatively modest savings of internal business resources. Thus, it is closer to standard practice and a smaller evolution for many organizations preparing for a cloud model.

CYBERSECURITY AND VULNERABILITIES

Global organizations typically have cybersecurity measures in place, but occasional large data breaches still take place. While moving operations to the cloud has the potential to increase security risks, standard network security systems will mitigate most of them. To provide additional protection either procedurally or technically, consideration should be given to the following:

- Because the IoT seeks to interconnect all digitally connected devices, it improves efficiency but may introduce new security risks.

Figure 4: Strategic assessment for organizations considering CSP services.


Strategic Assessment
Documented Current Company State
Desired Company State
Business Drivers, Industry Best Practice
Gap Analysis
Business Plan
Cloud Strategic Plan
Benefits, Globalisation, Implementation Options
Projects Life Cycles

- Mobile devices such as smartphones and tablets used on or off site to perform operations must be secured.
- Data encryption is highly effective in preventing data corruption, but it increases network and data demands on systems.
- Employee error or negligence in the end user organization can heighten inherent risks from CSPs and their subcontractors; it is important for organizations to mitigate such risks by vetted hiring, oversight, and training standards and methods.

For further current guidance in this area, the authors recommend guidance from the Cloud Security Alliance, a not-for-profit organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment [7].

REGULATORY CONSIDERATIONS

The end user is required to validate the MES implementation, including all cloud-based elements (see reference 1 for further information on regulatory requirements). The use of recognized and standardized components as part of the cloud element may reduce the end user's validation burden as the CSP takes on some aspects of validation; however, it does not remove the end user's burden completely, as decided in compliance determination.

The life sciences organization must ensure guidance addressing cloud-based data encryption/decryption, secure data entry and storage, and related issues is appropriate. Data entry will ultimately involve externally supported tools, products, and infrastructure outside of the end user's direct control, and the process must be appropriately recorded, verified, and validated.

It remains the responsibility of the end user organization, based on the target environment, target market, and proposed solution, to identify relevant regulations. Then, the end user must determine how well the proposed XaaS application complies with those regulations, and where deviations exist.

STRATEGIC ASSESSMENT SUMMARY

As mentioned previously, a strategic assessment is essential to efficiently plan and design a cloud-based model implementation or migration. Strategic assessments are defined in detail in the *GAMP® Good Practice Guide: Manufacturing Execution Systems* [1]. Figure 4 outlines the process, and key considerations are outlined in this section.

A project management office with high-level management support is highly recommended to lead the strategic assessment because the MES domain includes cross-departmental functionality. The strategic assessment establishes the current state of the end user organization; target sites and production activities for cloud-based services, with attendant resources, requirements, and constraints; specific goals, benefits, and risks of cloud migration; barriers to implementation; and the basis for a project plan that meets the needs of the company. Such an evaluation should:

- Separate business- and manufacturing-related processes/functions to clearly define requirements.
- Provide information about the overall design. This design should be defined by functions and how they interact, independent of the potential applications; the business should be able to present this type of design to CSPs as high-level requirements.
- Ensure process understanding is accomplished in a documented fashion by the end user for accurate and appropriate systems design and configuration.

The importance of understanding the current and desired states of the end user organization cannot be overstated. There are many CSPs to choose from, and execution of a strategic assessment puts the organization in a position to intelligently evaluate each one and choose the most appropriate vendor. Established CSPs typically are highly skilled at their core services, including global security policies, and they often can provide controls that are more powerful than end user organizations can implement on their own.

A properly vetted cloud service provider provides technical expertise, systems reliability, and business support at high levels on a consistent basis.

The strategic assessment defines the initial and long-term goals by documenting a broad discussion and decisions about the following questions:

- Does the organization need to implement XaaS at one site, regionally, or globally?
- Will implementation be vertical (covering the entire MES domain for the complete site) or partial (addressing certain MES functionalities, processes, or products at one or more sites)?
- What are the organization's timelines and resource constraints?
- How will XaaS impact production schedules?
- What are the costs and benefits of adopting or altering XaaS for MES?
- What are the requirements and scope to implement smart manufacturing (Pharma 4.0™, IoT, etc.)?
- What upgrades or replacements of existing systems would be required if XaaS were adopted?

The strategic assessment answers these questions, and more, to prepare the organization to develop the project plan (or plans) for successful cloud implementations.

Implementation of Pharma 4.0™ models and technologies adds complexity to the strategic assessment. For example, the IoT can involve a vast network of devices feeding information into integrated monitoring and control systems, as well as future decision-making applications based in artificial intelligence. The design of such paradigms and technology must ensure continuing operations and fail-safe conditions because, despite the stellar record of CSPs, no technology can guarantee 100% operational uptime in all circumstances.

Service Provider Selection

A properly vetted CSP provides technical expertise, systems reliability, and business support at high levels on a consistent basis. The following CSP attributes and conditions should be considered and documented in the strategic assessment:

- The vendor's relevant history. CSPs with MES experience or existing clients in the pharma industry are preferable.
- Regulatory expertise. Does the CSP have knowledge and experience in areas relevant to the end user?
- Staffing levels, expertise, and training.
- Evidence of the CSP's financial stability.
- Physical and digital security of the CSP's operations, networks, and data.
- Locations of CSP facilities. Consider factors such as local, national, and regional stability; the locality's network infrastructure; and whether the locality has a qualified workforce.
- Equipment/software to be supplied to the end user.
- Adherence to applicable software and hardware development, implementation, maintenance, and verification best practices, such as those found in *GAMP® 5* guidance,, ASTM International standards, the Information Technology Infrastructure Library, and ISA standards.
- Proof that the CSP's internal auditing capabilities are established and verified.

End User Responsibilities and Capabilities

During the strategic assessment and CSP selection process, it is important to understand that the end user remains ultimately responsible for the following:

- Service level agreements, support models, quality agreements, and escrow concerns
- Performing software and hardware development and verification audits
- Performing regular infrastructure and audit reviews
- Determining the extent and rigor of customer versus service provider maintenance (requirements will vary depending on service type)
- Clear policies and procedures for requirements gathering and communication
- Testing to ensure rigorous data integrity controls

Though the use of CSPs may lessen the end user's risks for IT implementations and maintenance, there are many CSP- and XaaS-related risks to be evaluated. For example, the end user needs to assess the likelihood of widespread area or regional internet/network disruptions beyond its control, and evaluate contingency plans for scenarios such as denial of service attacks with the potential to take a global system offline.

During the strategic assessment, the end user should review and document:

- Pause and resynchronization algorithms for with real-time control systems that must be coordinated between the CSP vendor and the end user organization, and possibly across time zones
- Policies and procedures for external data updates and transmission verification, both from the end user organization to the CSP and from the CSP to the organization
- Typical disaster recovery elements to be applied to the loop between the end user organization's networks and the CSP's networks, and to human communications

- The CSP's response times for errors and outages during real-time operations
- Policies and procedures for remote (CSP) data correction due to process control upsets, including how data correction will be coordinated between the CSP and the end user organization

The end user organization must put in place procedural and, whenever possible, electronic controls to ensure that its cloud-based systems are reliable, with minimal risk for the MES. To maintain the validated state of its MES, the end user's transfer and updates of information to XaaS must be accurate and thoroughly documented. Validation concerns include, but are not limited to the following types of data:

- Critical quality attributes
- Critical process parameters
- Critical aspect information
- Work instructions/recipes
- Metadata
- Audit trails

A CSP is not responsible for misconfigured systems caused by inadequate controls at the end user organization. End user and CSP personnel must be clearly identified and dedicated to the validation process, which must be coordinated within the end user's oversight structure.

CONCLUSION

This introductory article introduces the concepts and considerations of applying cloud-based models to the strategic and implementation phases of an MES for a life sciences organization. The authors encourage readers to learn more by exploring the publications cited in the references.

References

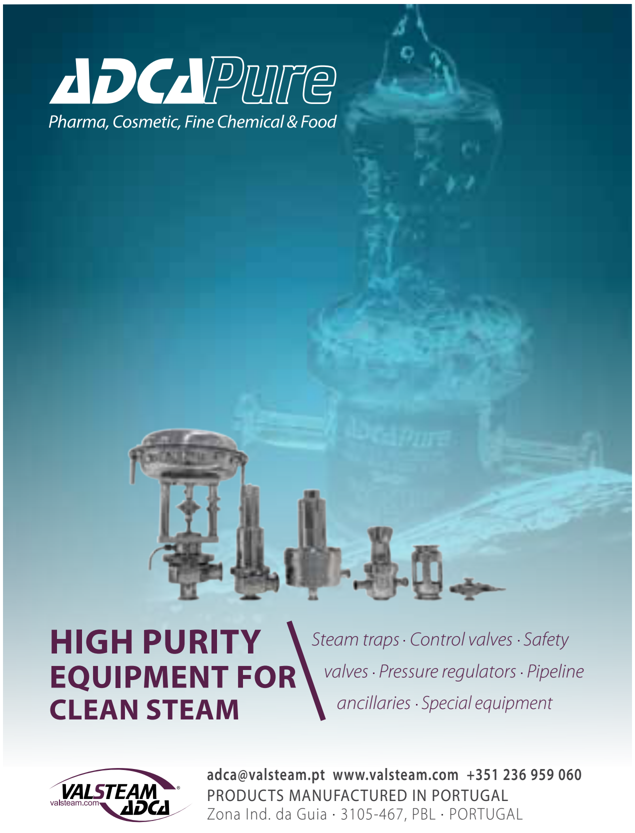
1. International Society for Pharmaceutical Engineering. *GAMP® Good Practice Guide: Manufacturing Execution Systems—A Strategic and Program Management Approach.* North Bethesda, MD: International Society for Pharmaceutical Engineering, 2010.
2. Hogan, M., F. Liu, A. W. Sokol, and T. Jin. "NIST Cloud Computing Standards Roadmap." National Institute of Standards and Technology. NIST-SP 500-291. 10 August 2011. https://www.nist.gov/publications/nist-sp-500-291-nist-cloud-computing-standards-roadmap
3. Mell, P., and T. Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology. NIST-SP 800-145. September 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final
4. International Society of Automation. *ANSI/ISA-95: Enterprise-Control System Integration Standard.* Research Triangle Park, NC: International Society of Automation. https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95
5. International Electrotechnical Commission. *IEC 62264: Enterprise-Control System Integration Standard.* Geneva, Switzerland: International Electrotechnical Commission.
6. McGinnis, L. F. "Formalizing ISA-95 Level 3 Control with Smart Manufacturing System Models." National Institute of Standards and Technology. NIST GCR 19-022. November 2019. doi:10.6028/NIST.GCR.19-022
7. Cloud Security Alliance. "Security Guidance v4.0: Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing v4.0." 26 July 2017. https://cloudsecurityalliance.org/research/guidance

About the authors

Paul Irving has extensive experience as a compliance and validation consultant in the life sciences industry. He specializes in information governance, data integrity program setup and implementation, and computerized systems validation. While working at Kimberly-Clark, Paul also gained experience in all aspects of quality control, including statistical process control and development of management information systems. In recent years, he has led large programs of quality and compliance transformations for leading biotechnology organizations.. Currently, Irving operates as a Strategic Consultant for Northern Life Sciences Ltd. within the UK, US, and CEE. He has been an ISPE member since 2001, serves on the GAMP® EU Steering Committee, was formerly Cochair of the GAMP Special Interest Group on Manufacturing Execution Systems, and has contributed to various GAMP guidance documents.

Gregory M. Ruklic, Senior Life Sciences Professional, is an expert in design and compliance activities for computer systems throughout the industry. He has designed, installed, validated, and managed multiple integrated automation and manufacturing execution systems/upgrades during his career. Greg has been an independent consultant for 10 years, following 23 years with Pfizer at manufacturing sites and global groups in systems engineering, project leader and quality systems roles. He has authored corporate policy and standards documentation and system/site validation plans, and is a contributing author to *GAMP® 5,* the *GAMP® Good Practice Guide: Manufacturing Execution Systems—A Strategic and Program Management Approach,* and articles for *Pharmaceutical Engineering.* Greg has been an ISPE member since 1992.

Jonathan Hurle has worked in the pharmaceutical industry for more than 20 years and has extensive experience as a compliance and validation consultant in the international life sciences industry. He is a versatile project manager/consultant with strong external client–facing experience and a demonstrable track record of delivering results with IT and business change projects. Jonathan has been an ISPE member since 2018.


ADCAPure
Pharma, Cosmetic, Fine Chemical & Food
HIGH PURITY EQUIPMENT FOR CLEAN STEAM
Steam traps · Control valves · Safety valves · Pressure regulators · Pipeline ancillaries · Special equipment
VALSTEAM ADCA
valsteam.com
adca@valsteam.pt www.valsteam.com +351 236 959 060
PRODUCTS MANUFACTURED IN PORTUGAL
Zona Ind. da Guia · 3105-467, PBL · PORTUGAL