A Publication for AGA Members

Prepared by the AGA Operations Section
Natural Gas Security Committee –
Cybersecurity Subcommittee
400 North Capitol St., N.W., Suite 450
Washington, DC 20001
U.S.A.
Phone: (202) 824-7000
Fax: (202) 824-7082
Web site: www.aga.org

October 2020

Cloud Service Considerations for Migrating Industrial Control Systems

ACKNOWLEDGEMENTS

AGA would like to extend a special thank you to the members of the AGA Natural Gas Security Committee Cybersecurity Subcommittee for contributing their shared knowledge, insight, and time to the development of this technical note.

DISCLAIMER

The American Gas Association's (AGA) Operations and Engineering Section provides a forum for industry experts to bring their collective knowledge together to improve the state of the art in the areas of operating, engineering and technological aspects of producing, gathering, transporting, storing, distributing, measuring and utilizing natural gas.

Through its publications, of which this is one, AGA provides for the exchange of information within the natural gas industry and scientific, trade and governmental organizations. Many AGA publications are prepared or sponsored by an AGA Operations and Engineering Section technical committee. While AGA may administer the process, neither AGA nor the technical committee independently tests, evaluates or verifies the accuracy of any information or the soundness of any judgments contained therein.

AGA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of or reliance on AGA publications. AGA makes no guaranty or warranty as to the accuracy and completeness of any information published therein. The information contained therein is provided on an "as is" basis and AGA makes no representations or warranties including any expressed or implied warranty of merchantability or fitness for a particular purpose.

In issuing and making this document available, AGA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is AGA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

AGA has no power, nor does it undertake, to police or enforce compliance with the contents of this document. Nor does AGA list, certify, test or inspect products, designs or installations for compliance with this document. Any certification or other statement of compliance is solely the responsibility of the certifier or maker of the statement.

AGA does not take any position with respect to the validity of any patent rights asserted in connection with any items that are mentioned in or are the subject of AGA publications, and AGA disclaims liability for the infringement of any patent resulting from the use of or reliance on its publications. Users of these publications are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Users of this publication should consult applicable federal, state and local laws and regulations. AGA does not, through its publications intend to urge action that is not in compliance with applicable laws, and its publications may not be construed as doing so.

Changes to this document may become necessary from time to time. If changes are believed appropriate by any person or entity, such suggested changes should be communicated to AGA in writing and sent to: ***Operations & Engineering Section, American Gas Association, 400 North Capitol Street, NW, Suite 450, Washington, DC 20001, U.S.A. Suggested changes must include: contact information, including name, address and any corporate affiliation; full name of the document; suggested revisions to the text of the document; the rationale for the suggested revisions; and permission to use the suggested revisions in an amended publication of the document.***

Objective

The objective of this technical note is to help the operator better understand the risks and benefits of moving critical services, such as industrial control systems (ICS) environments, to the cloud. The information provided in this paper should also help increase the operator's awareness of the benefits and risks that should be evaluated when considering employing cloud technology.

Problem Statement

Cloud computing offerings have created opportunities for businesses to migrate services typically hosted in an internal corporate computer network to an external public or private virtual environment known as "clouds". There are risks and benefits associated with moving critical services such as control system environments to the cloud. The decision to migrate and what to migrate depends on the risk tolerance of the operator. As such, understanding the right questions to ask helps the operator design a more predictable cloud experience.

Migrating Beyond Our Comfort Zone

With the growth of cloud services and the relief they provide on day to day maintenance tasks, traditional data center designs are called into question as hybrid models become more prevalent. As this trend continues, it is to our benefit to evaluate how we can leverage cloud infrastructure to provide value to our business securely…bearing in mind users are secondary in an ICS – the process is what is critical. As we grow cloud environments and can confirm security is at an adequate level, we should consider what other services could get migrated.

Defining "Cloud"

A "cloud computing environment" is a shared pool of configurable resources (e.g. servers, networks, applications, storage, services) that are centrally managed, available over a network, and can be provisioned and deprovisioned on-demand. Migrating any portion of operations to the cloud means the operator relinquishes complete control over those particular operations. In the case of migrating one's ICS, it should be presumed the ICS is no longer completely under the operator's direct control.

To leverage the benefits of the cloud, an operator should consider working WITH the cloud vendor to understand risks to operations introduced by the cloud environment and to address potential increases in cyber exposure.

> For example, if data acquisition is migrated to a cloud-based application, the operator will need to work with the vendor to ensure network connectivity, response times, and data integrity are sufficient to support control systems and incident response processes that may be reliant upon that data.

The migration can be applied to portions of a system rather than a system in its entirety.

> For example, an operator may choose to internally retain the 'Supervisory Control" of the operator's Supervisory Control And Data Acquisition (SCADA) system but move historian and data analysis to the cloud.

Understanding the cloud service offerings – associated limitations and expectations – is critical for choosing the cloud service that best suits the operator's needs and risk tolerance.

Ownership & Accountability

Control systems are high-value assets. Maintaining clear lines of ownership, responsibility, and accountability of one's ICS is prudent practice. Many systems and infrastructures makeup the ICS environment, including but not limited to:

- Field assets (e.g., Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), instrumentation, remote control valves and other machinery),
- Communications infrastructures (e.g., microwave, satellite, narrow and wideband radios, cellular, fiber optic and leased lines) required to communicate with field assets, and
- Operations center(s) (i.e., the physical location of the operators), and
- Software/Firmware.

Internal control and accountability for ICS system components is generally divided among several parties. How an operator chooses to address the management of ICS environment components does not relieve the operator of accountability. Though responsibilities of operations, management, and troubleshooting may be fractured and spread across multiple internal and external parties, the operator is still ultimately responsible for the integrity of the operation. When ICS operations are not owned and managed end-to-end by the same operator, shared security controls and processes may be applied to address vulnerabilities to viably mitigate risk.

Cloud offerings for ICS environments may introduce risks that are unique to the globally dispersed and shared tenancy environment often characteristic of clouds. For example, legislative or regulatory requirements may dictate that one's data be confined within specified geographical areas[1]. As a result, the operator should verify where data and cloud services will be located. While the vendor can potentially be audited against information technology (IT) best practices, the operator's specific use-case may not have a generally available set of applicable ICS practices against which the vendor may also be audited. Migrating computing infrastructure or applications to cloud can introduce ICS operational risks at multiple levels – risks an operator should be aware of and evaluate. Transferring technical responsibility to the vendor is not the same as transferring legal risk. There are some ICS functions that may be easily moved to the cloud; others may have the potential to critically impact life or safety. All function should be thoroughly considered before migration.

> For example, digital forensics can have its challenges and complexities that should be well understood before implementation. Further, alternatives, in the way of an 'exit strategy' should be considered in the event the cloud service tuns out not to be the appropriate solution.

Approaching the Cloud

The Purdue Model, developed by the International Society of Automation ISA99 Committee for Manufacturing and Control Systems Security, is a commonly used architectural reference model for managing ICS Control Hierarchy[2]. Leveraging the Purdue Model can help the operator better understand the risks associated with introducing cloud service at various points within the ICS environment. The model uses the concept of zones to subdivide an Enterprise and ICS network into logical segments (commonly referred to as "levels") comprised of systems that perform similar functions or have similar

[1] FedRAMP, standardized approach to security for the cloud, https://www.fedramp.gov/

[2] Purdue Model - Theodore J. Williams, *The Purdue Enterprise Reference Architecture and Methodology (PERA),* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.194.6112&rep=rep1&type=pdf

requirements[3]. The zones are Enterprise Zone, Demilitarized Zone, Manufacturing Zone, Cell/Area Zone, and Safety Zone[4]. For the purposes of this discussion, the ICS architecture associated with the various zones is further distinguished by the following five levels:

- Level 4 – business logistics (e.g., analytics and optimization)
- Level 3 – site operations (e.g., scheduling and nominations)
- Level 2 – area supervisory control (e.g., SCADA)
- Level 1 – basic control (i.e., intelligent devices that receive information from sensors and used for supervising, monitoring, and/or controlling processes; e.g., SCADA control, HMI)
- Level Zero – process (e.g., sensor, actuator, and valve operations)

See Appendix A for Control Levels Diagram.

By considering *function* as opposed to *device*, the thought an operator puts into the applicability/inapplicability of cloud service may be the same regardless of the level, i.e., Level Zero or Level Four, in which the system is classified.

ICS environments generally carry the highest level of risk to the operator in the form of safety. Failures in an ICS have the potential to result in loss of life, loss of property, and/or damage to the environment. Assessing a function's impact if disrupted helps an operator weigh the benefits and risks associated with ICS hosted by cloud service. Non-ICS hosted in the cloud do not generally have a direct impact on operational safety. When operators consider whether IC should be moved to the cloud, operational safety is a leading risk factor that should not be marginalized. Operators should take into consideration stringent real-time performance, data availability and integrity, and latency requirements when assessing whether a move to the cloud is appropriate. There is no one-size-fits-all cloud service given the variation of risk tolerances across different companies and within a company. As such, the decision to employ ICS-hosted cloud service is ideally left to the operating company to determine.

Driven by Risk Profile

The key to using cloud in an ICS environment is to be aware of how the risk landscape changes. It is important to be cognizant of the risk profile associated with moving some or all of ICS to the cloud. The cloud is a very broad service. Each type of offering has different costs and different risk profiles. The leading and worst-case risk factor an operator should be prepared to assess is loss of control over reliability. This is the foundation upon which the decision to move functions to cloud service should be constructed.

The Different Offerings & Points to Consider

The National Institute of Standards and Technology (NIST) defines cloud computing as a model that enables on-demand access to a shared resource pool consisting of servers, networks, applications, services and storage which can be rapidly deployed with minimal management efforts[5]. Cloud offerings

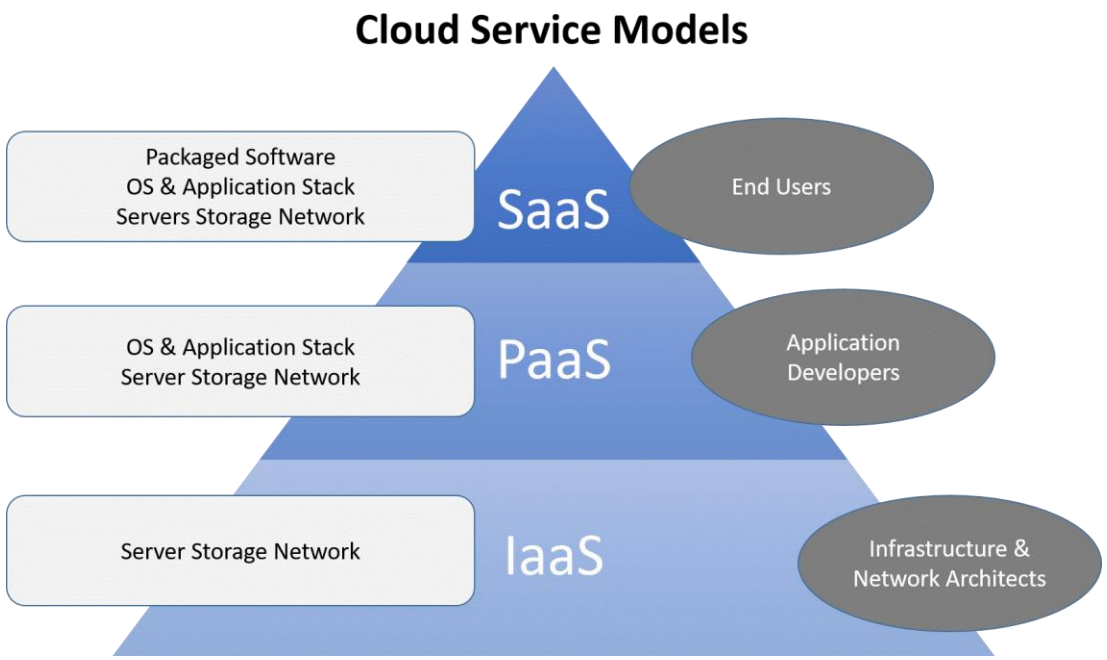
[3] SANS Secure Architecture for Industrial Control Systems (2019)

[4] Defining the different Zones - Luciana Obregon (2015), *Secure Architecture for Industrial Control Systems*, https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

[5] NIST definition of cloud computing - Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf (2011), Recommendations of the National Institute of Standards and Technology, *NIST Cloud Computing Reference Architecture (NIST SP 500-292)*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf.

vary among three lead models: *Platform as a Service* (PaaS), *Infrastructure as a Service* (IaaS), *Software as a Service* (SaaS). Figure 1 is a graphical depiction of the various cloud service models. Cloud computing, often described as a stack, has a broad range of services built on top of one another under and including the services in the model(s) beneath. See the Appendix B for further description of each.

Figure 1: Cloud Computing Stack Pyramid



Mahmoud A. Salam, Waleed M. Bahgat, Eman El-Daydamony, Ahmed Atwan, A Novel Framework For Web Service Composition, *International Journal of Simulation: Systems, Science & Technology 20(3):1 · July 2019*, https://www.researchgate.net/publication/334226116_A_NOVEL_FRAMEWORK_FOR_WEB_SERVICE_COMPOSITION accessed Aug 21, 2020

Another type of cloud offering not discussed here but worth noting is *Function as a Service* (FaaS), which is designed to potentially be a serverless architecture. Additionally, cloud integrators may play a dominant role as a product or a service that helps the operator navigate the complexities of cloud computing.

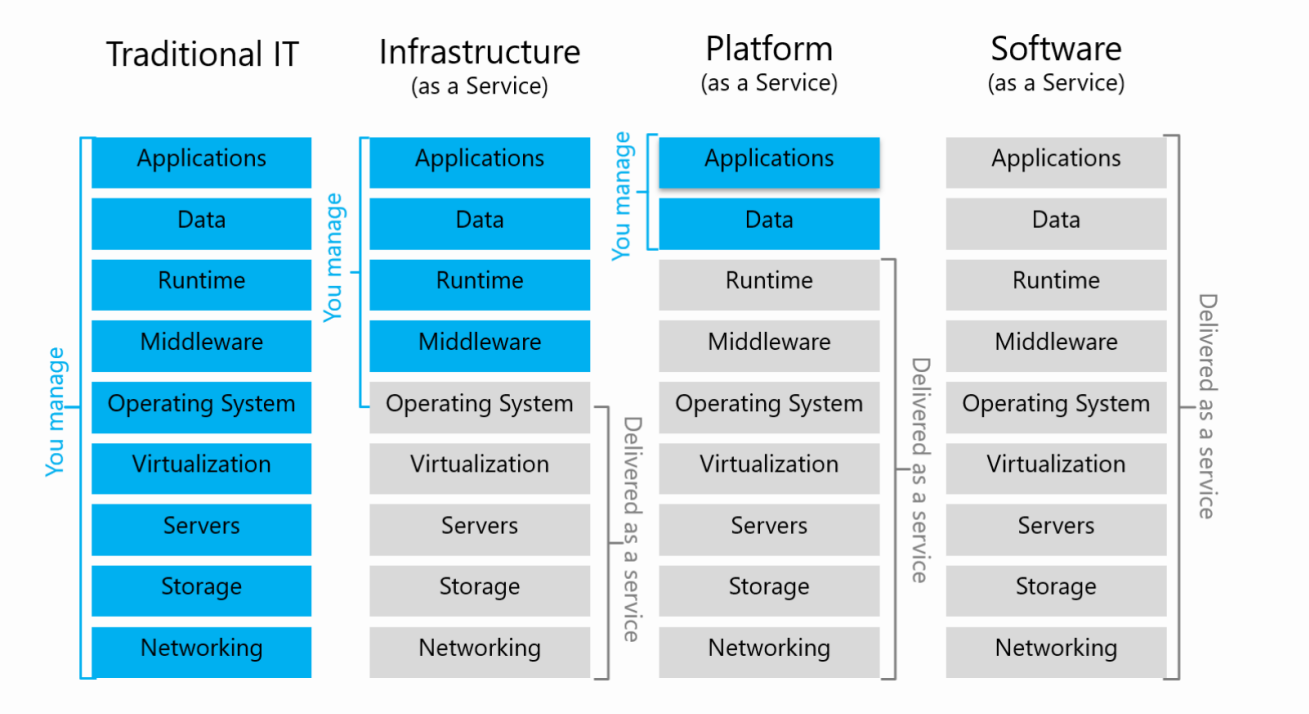
Connectivity is the most critical component of cloud service. In ICS, careful consideration should be given to the communications avenues for the SCADA environment since there are potential risks associated with loss of connectivity. The operator should not assume connectivity is a given.

> For example, an end user with a slow or broken network connection to field equipment may not be able to reach the SaaS apps. Regardless of whether SCADA loses connection to field or the operator loses connection to the SCADA in the SaaS app, there is increased risk for the compromise of reliability and accountability that should be recognized and planned for.

Such scenarios should be factored in when determining the applicability/inapplicability of deploying SCADA apps to in the cloud.

Figure 2 provides a visual representation highlighting the differences of the cloud service models as they compare to traditional IT security. The diagram further conveys that which is generally the vendor responsibility and that which is the operator responsibility.

Figure 2: Comparison of traditional IT infrastructure to cloud service models.



D.Chou, Rise of the Cloud Ecosystems, https://dachou.github.io/2011/03/16/cloud-ecosystems.html, 2011, accessed on May 18, 2020.

ICS environments are time-sensitive and require deterministic behavior – meaning actions and results within the environment are repeatable and predictable. Dedicated owner-operated computing environments can be designed, implemented, and maintained throughout their lifecycle to perform at a defined specification of performance, latency, and throughput as determined by the operator.

SaaS

SaaS providers generally offer data centers and internet service providers designed and operated to serve to the largest pool of customers as practically possible and still meet advertised levels of performance, latency, and throughput. The operator should take such factors into consideration and discuss with the cloud service provider any potential impact on the SCADA performance requirements.

When leveraging SaaS, the operator generally does not have control or visibility of the underlying infrastructure (e.g., firewalls, routers, switches, servers, storage, etc.) used by the provider. The operator should evaluate the service terms with the cloud provider to assure adequate protection and maintenance are provided that satisfy the operator's risk tolerance. Recognizing, the SaaS provider's value proposition typically includes improved security and the provider's economies of scale likely dictate that all customers are running the same software versions, the SaaS provider cannot be assumed

to fully understand the operator's use of the SCADA system. The operator should also consider how its Management of Change processes and those of the vendor can be integrated.

> For example, if a gas utility's practice requires permission from the control center before proceeding with upgrades, a SaaS provider with multiple customers may not be able to accommodate this Management of Change requirement.
>
> On the other hand, patching ICS environments can be difficult due to the security controls put around accessing the environment and the variety of hardware in different environments. SaaS providers may take these maintenance tasks out of company's hands and can better test patches due to the knowledge of the infrastructure that the application is running on.

PaaS

PaaS leverages a cloud provider's hardware and operating system software allowing the operator to install and administer their own applications and control their own data. PaaS is not as easy to setup as a SaaS; however, PaaS provides a unique ability to control the application and manage the associated data without the confines of the provider's one-size-fits-all approach.

It should be noted that PaaS is not an easy service to transition from and usually results in downtime if moving to a different provider. Also, upgrades may occur to the underlying infrastructure that do not align with the operation of the application, which may result in undesired results.

> For example, the PaaS provider could stop supporting a certain programming language, application critical libraries, or performs upgrades that is not compatible with the operator's application leaving the operator offline and scrambling to resolve with the Application Vendor. This is different than SaaS in that SaaS has control of the complete computing stack and can validate prior to changes.

IaaS

IaaS provides operators the ability to move part or the entire on-premise infrastructure to a cloud-based virtual environment, including the complete stack from servers, storage, networking, operating system, and applications. IaaS generally provides greater reliability than most on-premise data centers, offers improved security functions, and allows for the technology teams to focus more on the business needs rather than the underlying infrastructure reliability.

When it comes to IaaS, it is key that the same security principles apply in the cloud as they do on premise. Even though the service provider has security features, the responsibility of security implementation still falls on the operator. The same types of technologies that protect the operator's environment should be implemented to include, but not limited to, firewalls, end point protection, backups, monitoring solutions, multifactor authentication, etc. as these are not generally inherent with IaaS.

> For example, IaaS providers are like an apartment complex. They provide the 24x7 guards, lights, security cameras, and all other essential services for securing the complex. The Operators rents an apartment at the complex and finds that their place was broken into and stuff missing. This is the responsibility of the Operator and not the Provider.

Additional Considerations

With all cloud service provider (provider) types, the following points at a minimum should be considered:

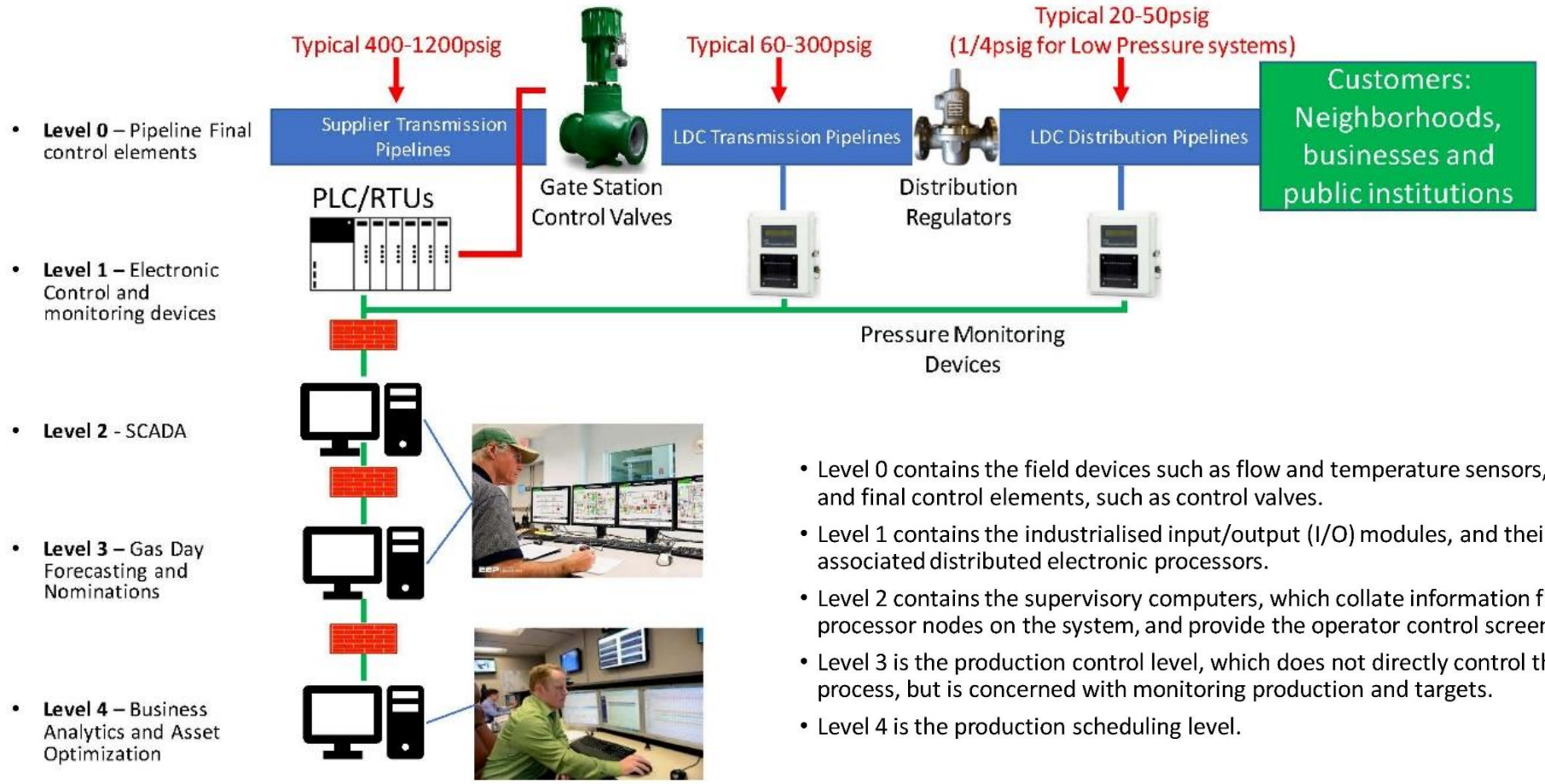
- Security Service Level Agreement (SLA) – The SLA between a cloud service provider and the customer helps set expectations for both the provider and operator. The SLA is key when it comes to issue reporting within the operator's environment and availability of the service provide for timely response. Financial damages should be considered as part of the agreement to incentivize adherence to the SLAs.
- Fallback Contingency – The operator should maintain a fallback contingency for on-premise control in the event the cloud service is interrupted or has extended downtime.
- Security Policy – The security policies of the cloud service provider should be evaluated to ensure the provider is following, at a minimum, the same security policies enforced at the operator's company. This may include password policies, background checks, patching cycles, etc. Such an evaluation may be assisted by reviewing the provider's SOC2 type 2 reports. The operator should also consider proper certifications and independent audits of the service provider when evaluating the use of the cloud.
- Incident Response Plan (IRP) – The operator should consider establishing an IRP that accounts for the event the cloud service provider is a victim of cyber compromise. This should include roles and responsibilities of the operator and the provider as well as align with the SLA regarding reporting. Contractual language is key for any type of liability as a result of a compromise.
- Change Management – The operator should properly align Change Management between the cloud service provider and the operator with respect to updates and testing protocols. Worth noting is that even though the application may function appropriately, the testing should be end-to-end, including equipment used in the field.
- Training – Cloud training is critical for proper understanding of application, benefits, and limitations of retained cloud services. Training should target technology teams and operators to understand the impacts of the transition before committing.
- Managed Service Providers – There is a difference between a Managed Service Provider (MSP) and a cloud service provider. IT departments often outsource specific services (e.g., security monitoring) to MSPs. MSPs may have their own cloud offerings or resell cloud services from other vendors, possibly with some sort of value-add. There is no one-size-fits-all solution, and interdependencies among the ICS components create a complex ecosystem. The operator should be aware of how the MSPs manages the services and the responsibilities associated within the contract.
- Capital vs. O&M - Traditional utility spending models focus on spending capital dollars. Cloud service business models typically require the purchase of subscription services, which may be difficult to capitalize. This distinction should be understood, especially regarding applicability in cost recovery mechanisms.
- Appendix C provides Uses Cases that highlight the security considerations that would ideally be scrutinized when moving ICS to the cloud

Conclusion

There are both risks and benefits of moving critical services such as control system environments to the cloud. The decision to migrate, and what to migrate, depends on an operator's unique operational requirements and the risk acceptance of the operator. Understanding the cloud service offerings – associated limitations and expectations – is critical for choosing the cloud service that best suits the operator's needs and risk tolerance.

APPENDIX A: Control Levels

DNG Purdue diagram



- Level 0 contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.
- Level 1 contains the industrialised input/output (I/O) modules, and their associated distributed electronic processors.
- Level 2 contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.
- Level 3 is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.
- Level 4 is the production scheduling level.

Illustrated by David Tappen, 2019

APPENDIX B: Definitions[6]

Cloud Service Models

- IaaS (Infrastructure as a Service)
    - Cloud computing environment for resources such as virtual systems, servers, storage, and networking hardware.
    - The consumer uses their own software such as operating systems, middleware, and applications.
    - The consumer is responsible for:
        - Data security, including data at rest, data in use, and data in motion.
        - Key Management
        - Patch Management
        - Management Plane restriction
        - API Automation (Application Programming Interface) protection

    - The underlying cloud infrastructure is managed by the Cloud Service Provider (CSP).
- PaaS (Platform as a Service)
    - Cloud computing environment for development and management of a consumer's applications.
    - Designed to support the complete application lifecycle while leaving the management of the underlying infrastructure to the CSP.
    - CSP is generally responsible for the following infrastructure hardware: virtual servers, storage, and networking while tying in the middleware and development tools to allow the consumer to deploy their applications.
    - The consumer is responsible for vulnerability management, application security, and logging.
    - In general, the CSP is responsible for the security starting at the networking components up to the middleware/runtime environment, while the consumer is responsible for configuration, application, database, and vulnerabilities.

- SaaS (Software as a Service)
    - Cloud computing software solution that provides the consumer with access to a complete software product.
    - The software application resides on a cloud environment and is accessed by the consumer through the web or an application program interface (API).
    - The consumer can utilize the application to store and analyze data without the responsibility of managing the infrastructure, service, or software, as that falls to the CSP.
    - Contractual language should could key points such as data encryption, data breach notification, audit rights, service level agreements (SLA), authentication, limitation on 'vendor lock-in', and cyber insurance.

[6] CIS Controls Cloud Companion Guide Version 7

- FaaS (Function as a Service) is a cloud computing service that allows the consumer to develop, manage, and run their application functionalities without having to manage and maintain any of the infrastructure that is required. The consumer can execute code in response to events that happen within the CSP or the application without having to build out or maintain a complex underlying infrastructure.

Cloud Deployment Models

- Private cloud (on-premises)
    - Consists of all the computing resources being hosted and used exclusively by one consumer (organization) within its own offices and data centers.
    - The consumer is responsible for the operational costs, hardware, software, and the resources required to build and maintain the infrastructure.
    - Used for critical business operations and applications that require complete control and configurability.
- Private cloud (third-party hosted)
    - Private cloud hosted by an external third-party provider.
    - The third party provides an exclusive cloud environment for the consumer and manages the hardware.
    - Consumer is responsible for all costs associated with the maintenance.
- Community cloud (shared)
    - Computing resources and infrastructure shared across several organizations.
    - The resources can be managed internally or by a third-party.
    - Can be hosted on-premises or externally.
    - The participating organizations share the cost and often have similar cloud security requirements and business objectives.
- Public cloud
    - Computing resources and infrastructure hosted by a third-party company defined as a CSP.
    - Available over the internet, and services are delivered through a self-service portal.
    - The CSP is responsible for the management and maintenance of the system, while the consumer pays only for resources they use.
    - The consumer is provided on-demand accessibility and scalability without the overhead cost of maintaining the physical hardware and software.
- Hybrid cloud
    - An environment that uses a combination of private cloud (on-premises), private cloud (third- party hosted), and public cloud with an orchestration service between the three deployment models.

APPENDIX C: USE CASES

ICS environments generally support two overarching functions – operational-based decisions and financial-based decisions. From an operational perspective, ICS environments serve the reliability of product quality and delivery, which may be perceived to carry the highest level of risk to the operator in the form of life safety when the information received feeds real-time decisions. On the other hand, ICS environments may serve as the source of operational data for trending and tracking but without the urgency of real-time portrayal of the system. From a financial perspective, ICS may serve as the source of accounting information. The latter two functions – data archiving and accounting – are generally lower risk since they do not impact safety.

A clear understanding of the responsibilities of the cloud provider and the responsibilities of the operator cannot be overemphasized. Coordination and communication between the two helps promote reliability.

The following "use cases" are intended to highlight the security considerations that would ideally be scrutinized when moving ICS to the cloud. The first use case assumes the functions being migrated to a cloud service do not have a life safety impact. The second and third use cases list considerations in the event of migrating a function that has a life safety impact. As stated early on in this discussion, considering *function* as opposed to *device*, helps the operator more effectively focus on the applicability/inapplicability of cloud service regardless of architecture level.

Common across all use cases are risks that can be categorized into one of four areas –

- Safety Risks,
- Security Risks
- Reliability Risks, and
- Performance Risks

Some level of safety risks is inherent in security, reliability, and performance risks. For the purposes of the Use Cases, safety is listed as its own area for the purposes of specifically distinguishing the life-safety impact. The risks listed below are categorized accordingly and provided to the reader for consideration. Company-specific operations and risk appetite will vary. The use cases are provided as examples to help the reader better understand the thought process encouraged for determining whether functions under their responsibility are viable candidates for cloud service and what risks should be considered. The risks listed are not all-inclusive.

Use Case 1:

Process Control Data to the Cloud for use by the business to perform some function (no life-safety impact)

A. Scenario: Measurement equipment needs to upload information for trending and tracking purposes. Historical data. Data NOT used for making real-time operational decisions.

B. Risks to Consider if move service to cloud:

1. Safety Risks – not necessarily applicable for short-term impact
2. Security Risks
    - Device visibility into network
    - Tampering
    - Privacy information
3. Reliability Risks
    - Connectivity
    - Data availability
4. Performance Risks
    - Data integrity

C. Additional Considerations - data in transit, data at rest

Use Case 2:

New industrial internet of things (IIOT) type devices not on SCADA network with data to cloud for the purposes of monitoring operations (quasi life safety impact)

A. Scenario: Measurement data used for planning, forecasting, daily operations, pipeline balance, and nominations is moved to the cloud. The data is not real-time but affects operations.

B. Risks to Consider if move service to cloud:

1. Safety Risks
    - Increased difficulty in managing pressures
2. Security Risks
    - Provider hacked information not available as needed
    - systematic tampering with the measurement data and that causes an imbalance
3. Reliability Risks
    - Data integrity
4. Performance Risks
    - consequence would be seen on long-term

C. Additional Considerations - none

Use Case 3:

SCADA service in the cloud, communicating to IIOT and non-IIOT devices (life-safety impact)

A. Scenario 1: A utility is looking to leverage a cloud SaaS offering to connect directly to its site supervisory controllers and rely completely on a cloud offering for direct and/or indirect control of all aspects for transmission/distribution systems. The level 1 devices will be reporting directly to the SaaS platform, and all interaction from the control room happens through the SaaS offering. The utility's Network Operations Center (NOC) manages and monitors the telecommunications service providers that provide the service between the SCADA system and the level 1 devices on site.

   Scenario 2: A utility feeds a series of small communities. The system is base-loaded and managed at city gate stations; there is no gas control center. The utility operator control does not control the data received back. However, the same data have an impact on another system that does have a control feature. That is, output of what being monitored is input to a life safety impact procedure.

B. Risks to Consider if move service to cloud:

   1. Safety Risks
      - No longer under direct control of operator.
      - Timeliness of alarming to remote-control for each monitored site and of real-time pipeline conditions, equipment failures, etc., may be called into question if SCADA connectivity is unreliable. This has potential to result in dispatch and/or response delays.
   2. Security Risks
      - Relying on third party network that operates in a shared environment may be susceptible to eavesdropping and cyber-attacks.
      - It is unknown how the vendor is managing platform and operator data.
      - The SaaS provider is not immune to the same challenges as the operator with respect to testing security patches – the effort required is considerable, and the testing is never fully conclusive given the complexity and timing-sensitive nature of the environment.
   3. Reliability Risks
      - Network connection cannot be guaranteed.
      - SCADA field networks are often quite complex – due to redundancy and performance requirements – and may require working with multiple service providers, multiple generations of various technologies, etc. To achieve target levels of reliability, a comprehensive overall design is required, including key components inside the data center, such as firewalls. These would typically be designed and operated by the SaaS provider or an IaaS provider contracted by the SaaS provider.
      - Cloud service providers typically deal with systems and applications that are largely unaffected after a brief pause; this may be fundamental to their design for security patching, migrating systems to balance resources, etc.

4. Performance Risks
    - Latency/monitoring; need to keep data in real-time or near real-time (life/safety); near real time monitoring data is necessary for control

C. Additional Considerations - Agreements with cloud provider – ability for provider to measure and for operator to hold provider accountable. We foresee that there could be a hybrid scenario for this use case. Ultimately the control and data will be used within the local SCADA environment however we do believe that there will be scenarios where local near-realtime that is required for control and safety purposes however the historical data as well as the overall system command and control will be leveraged by a SaaS solution. (A secondary check and balance have local logic based on preset parameters.)