Schlumberger

Agora

# Security Challenges for the Energy Industry on the Industrial Internet of Things

**By Anh Dang, IIoT Security Architect**

# Contents

**Introduction** 3

**Security Challenges Posed by IIoT** 4

**The Agora Platform** 4

**Agora Security Strategy** 6

**Secure By Design** 7

Edge Security 7

Identity and Access Management 8

Data Security 9

Cloud Security 10

Secure Development Lifecycle 11

Security Qualification Processes 11

**Secure Deployment** 12

Device Hardening 12

Network Segmentation 12

Edge Application Security Screening 13

**Secure Operation** 14

Secure Updates and Device Management 14

Security Compliance Dashboard 14

Security Monitoring and Incident Response 14

**Alignment with Industry Standards and Best Practices** 16

**SOC 2 Compliance** 17

**Third-Party Security Penetration Test** 17

**Conclusion** 18

# Introduction

The Industrial Internet of Things (IIoT) is a relatively new computing paradigm that combines machine learning (ML), artificial intelligence (AI), remote sensors, and device-control applications (or "apps") to help businesses and industry achieve more efficient and reliable operations. In the oil and gas field, IIoT is used for a variety of purposes—from fully autonomous pump and valve control to remote sensing of security breaches at isolated wellsites.

Agora, a division of Schlumberger Technology Corporation and the sponsor of this white paper, works with key vendors of IIoT applications, sensors, and control devices to provide secure implementations tailored specifically to the needs of oil and gas customers. Because many remote wellsites suffer from connectivity issues, Agora® edge AI and IoT solutions use a technology called edge computing that enables some AI-based control and decision-making functions to be concentrated at the wellsite (or "at the edge"), rather than exclusively at remote data centers located elsewhere on the Internet (or "in the cloud"). The use of edge computing is making wellsite operations increasingly autonomous, with AI providing the brains to keep remote sites operating completely on their own, at peak efficiency, even during episodes of poor connectivity.

When connectivity is available, the data collection and computing activities conducted at the wellsite ("the edge"), can be reported back to users and services operating at data centers and other locations "in the cloud." Even so, IIoT is not by its nature an intrinsically secure technology. In fact, when deploying it, great care must be taken to protect data and company operations from the significant potential for online cyberattacks, theft, or security breaches. This paper discusses the security challenges posed by the IIoT and how they can be uniquely addressed using Agora technologies.

# Security Challenges Posed by IIoT

The primary challenge posed by IIoT is the increased potential for cybersecurity attacks caused by the plethora of network-enabled devices used to move data between "the edge" and "the cloud." If these devices and their communication mechanisms are not carefully designed, developed, deployed, operated, and monitored, they can present a significant risk to safety, operations, asset health, privacy, reputation, and cost. Adding to this challenge is the desire to keep both edge devices and communications low-cost, which creates an economy-of-scale problem, where few devices manage to remain both secure and low-cost.

Poorly designed systems can be an easy target for hackers to exploit, and since IIoT devices (known as "endpoints") could stay in the field for a long time, a secure system can be breached overnight, potentially requiring a quickly executed action plan to address the vulnerability. In addition, because there may be little or no physical security in the field where an IIoT endpoint is deployed, tampering with the endpoint also becomes a significant security concern that must be considered in any deployment. Even in cases where high physical security is present, trusted personnel might carry compromised devices into secure areas, thereby introducing cybersecurity risks.

# The Agora Platform

.

Agora is a feature-rich platform devoted to the Industrial Internet of Things (IIoT). The platform is secure, open, and extensible; designed to meet stringent operational and environmental demands, extending intelligence and autonomy to the wellsite ("the edge"), and providing visibility and operability from the cloud. The platform implements the latest IIoT paradigms, including

- edge computing
- cloud computing
- advanced networking
- analytics
- artificial intelligence
- sensing.

Agora's architecture is intended to enable a marketplace of applications that can be executed at the edge or in the cloud, leveraging IIoT data captured at the wellsite.

Enabling these apps to be seamlessly deployed and operated at the edge via operational portals manned in public or private cloud infrastructure is a fundamental requirement and an important differentiator as it enables a variety of apps, developed by different companies, to be merged into a consistent, secure system.

The Agora Platform adopts a hybrid edge-cloud approach that enables best-of-breed edge and cloud vendor technologies to be adapted, built, deployed, and operated in a secure and scalable manner that provides tangible value across three functional tiers:

- **Edge**. Secures site assets, providing local intelligence, optimization, and automation, along with quality, health, safety and environmental (QHSE) adherence.
- **Cloud.** Provides higher-level contextual intelligence, transparency, analytics, control, and data persistence.
- **Enterprise.** Integrates IIoT with enterprise business systems and processes to accomplish business objectives, such as improving equipment health and performance, conducting resource and operations planning, and achieving environmental goals.

Figure 1 provides a diagram illustrating the Agora Platform's high-level architecture.

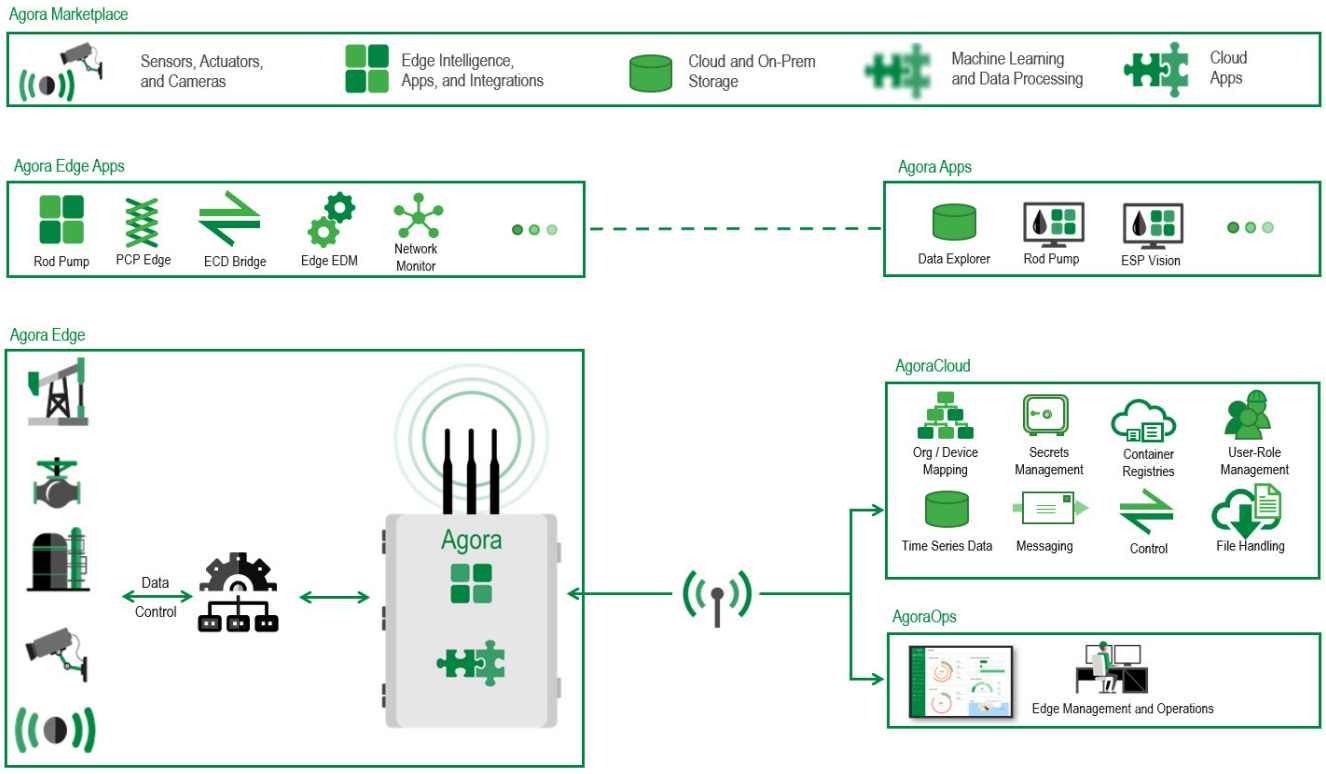



Figure 1: Agora Platform high-level architecture

# Agora Security Strategy

As an IIoT platform, Agora addresses security challenges by building a holistic security strategy that encompasses design, deployment, and operation, while aligning with industry security standards and best practices such as those promulgated by the US National Institute of Standards and Technology Cybersecurity Framework (NIST), the Industry IoT Consortium®, the Cloud Security Alliance® (CSA), and ISA/IEC 62443.

Agora works with multiple vendors to ensure their applications operate securely, following prescribed security standards in design, deployment, and operation. As such, security in Agora is a unique differentiator that is built into the entire product lifecycle including people, processes, and technology measures to build comprehensive protection for the platform.

Security within the Agora Platform is guided by the following paradigms, as illustrated by Figure 2:

- Security-by-design with defense-in-depth security controls built-in at many layers of the platform, from edge to cloud.
- Secure deployment with defined processes and controls to ensure that the security of the AgoraGateway® ruggedized edge computing device and the entire Agora Platform are not compromised during deployment.
- Secure operations focused on preventing, detecting, assessing, monitoring, and responding to cybersecurity threats and incidents.

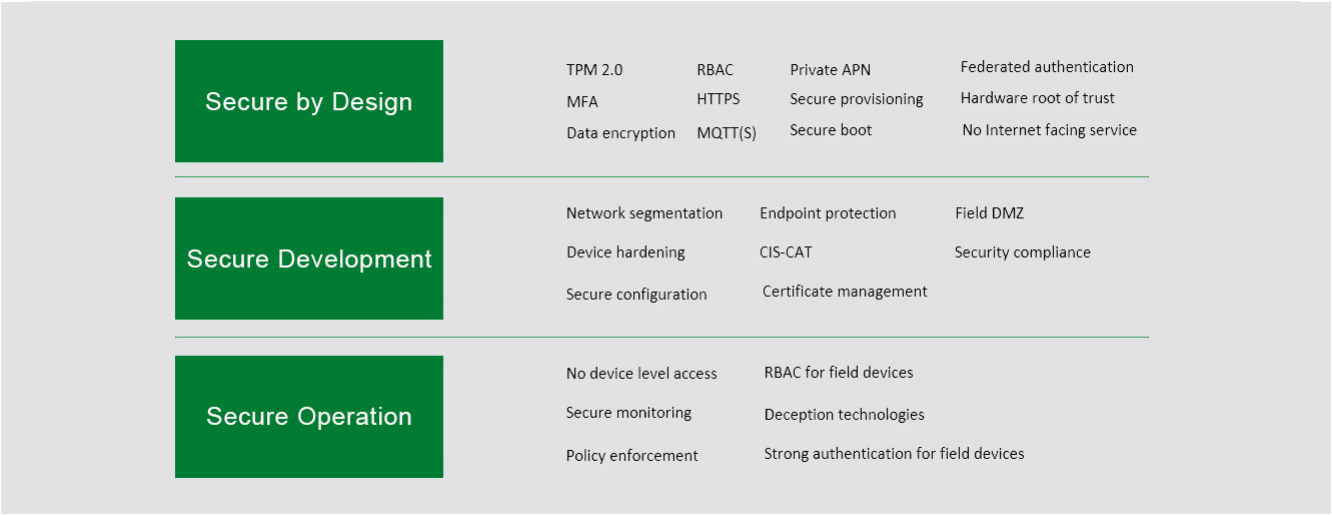



Figure 2: Agora security strategies.

# Secure By Design

Security is an architectural principle for the Agora Platform, meaning that security is considered in all architectural decisions including design, deployment, and operations, as well as in updates to features. Security is implemented across the entire spectrum of design, from integration of edge devices to presenting user data through Agora apps found in the Agora Marketplace.

### Edge Security

At the wellsite, the AgoraGateway device begins the process of connecting and interacting with edge devices. Agora provides protection for the gateway by embedding strong security controls in the design, including a hardware-based root of trust implemented using a Trusted Platform Module (TPM 2.0) in the hardware. The TPM provides the gateway with an unforgeable identity and secure storage for cryptographic secrets.

The gateway enforces a secure measured boot by leveraging the TPM to provide protection against software tampering and malware infection. The measured boot process assesses the integrity of critical components in the gateway's boot chain—from BIOS, to boot loader, to operating system kernel—against a known set of trusted reference values stored on the TPM. The boot process will stop if it detects any sign of system tampering. Figure 3 provides a conceptual illustration of the entire boot process.

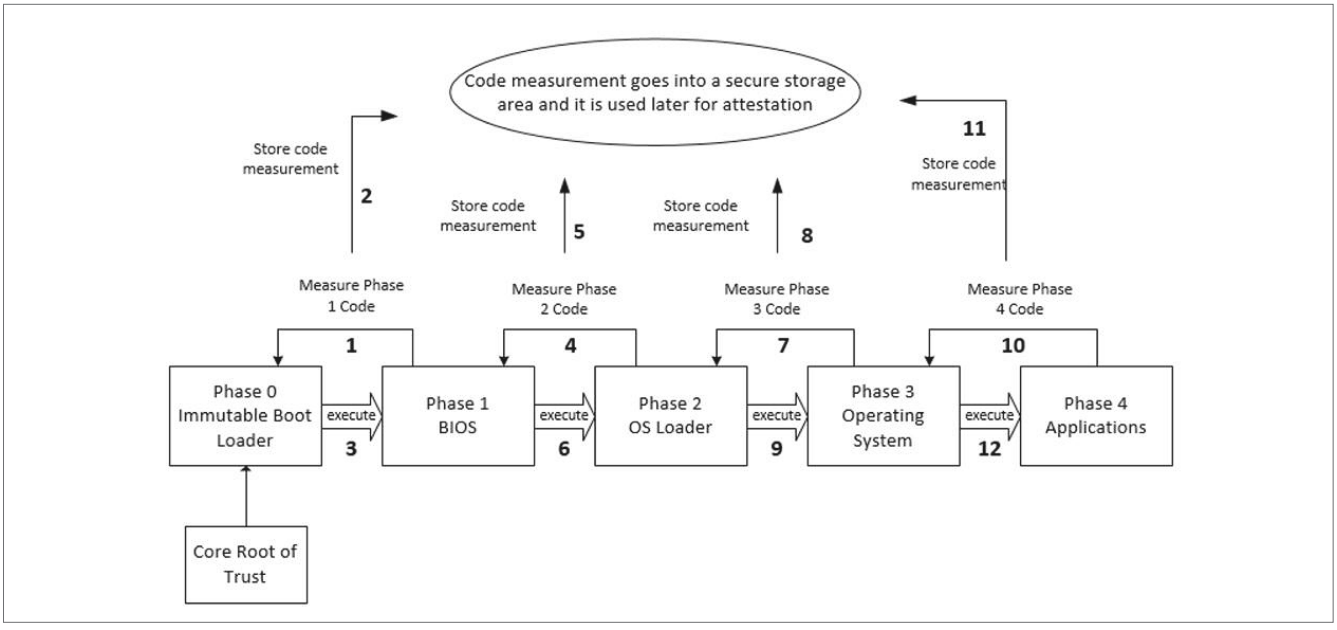



Figure 3: Measured boot implementation with hardware root of trust (HRoT).

The TPM also uses a hardware-based secure identity to authenticate the gateway-to-cloud services and is the first step in securing a communications session from the gateway to the cloud. Cryptographic secrets like encryption keys and private keys are stored in the TPM, further securing the gateway and its operation.

Microservices architecture—a way of breaking an application into smaller, more manageable pieces—is used with edge applications deployed at the gateway as nonprivileged Docker containers. Authentication is required for all module access requests. Isolation between Docker containers prevents one container from accessing the data in another container. If the system is compromised, this will prevent an attacker from moving laterally between containers.

The security posture of an edge device is maintained and monitored throughout the device lifecycle from manufacturing and deployment until the device's end-of-life phase.

### Identity and Access Management

The Agora Platform follows a zero-trust security principle. Every cross-component operation in the cloud requires authentication and access control validation. This applies to all platform entities including users, applications, and systems.

Most IIoT systems generally implement weak authentication. Oftentimes, the passwords are stored on the device itself. This weakness makes the IIoT system vulnerable to attackers, especially when incoming Internet connections are not blocked. Agora avoids these issues by ensuring that there are no credentials stored on the device, while still enabling strong authentication. This is achieved by leveraging identities used for authentication with corporate authentication systems such as Active Directory Federation Services (AD FS) and Azure Active Directory (AAD).

The credentials are stored and verified on external servers where sophisticated IT controls are protecting the servers. This also enhances usability, as users in the field or in the cloud can authenticate using a single identity. For offline environments, a secure FIDO2-compliant hardware token can be used to authenticate users. This technology leverages a public-private key pair that is used to identify the user to the gateway-based services. Example of such hardware are YubiKey®, Identiv, and FEITIAN.

For machine-to-machine authentication, the Agora Platform leverages the TPM's endorsement key to provide an unforgeable and unique hardware identity for each AgoraGateway device. This hardware-based identity is checked during gateway-to-cloud provisioning and each time a gateway communicates with the cloud backend.

Agora implements role-based access control (RBAC) in the cloud and at the edge. In cloud environments, application roles are configured with specific authorizations and then the roles are assigned to users appropriately. Access privileges for data and control actions are then mapped to these roles based on need-to-know and least-privilege principle. RBAC enforcement ensures that each customer will only have access to its own data and can perform control actions only on its deployments. Similarly, RBAC is enforced on the gateway device to limit access to data and gateway management functions.

### Data Security

All data on the Agora Platform are protected, including telemetry data, computed data, gateway configuration information, device management data, and system management data. Security controls are in place to protect all data at rest and data in transit, as discussed below.

#### Securing data at rest

Data at rest refers to data that are persistent in a storage medium. Within services like AgoraCloud® data contextualization system, and AgoraOps® edge device management services, data are encrypted using the advanced encryption standard (AES-256) with encryption keys managed securely by the hosting platform. And, because the AgoraCloud system and AgoraOps services are multitenant systems, access control is strongly enforced on every API call.

On the edge, the AgoraGateway device may store the data it acquires prior to transmitting it offsite. These data are encrypted using AES-256 with encryption keys stored in secure hardware storage (TPM).

#### Securing data in transit

Data in transit includes all data being communicated between the cloud and the gateway. As shown in Figure 4, all data in transit use two communication channels for moving data: The data channel is used for moving acquired data and data computed at the edge for domain-specific problems. The management channel is used for configuring and managing the device. On both channels, data are moved using the advanced message queuing protocol (AMQP) or the message queuing telemetry transport protocol (MQTTS) over the transport layer security (TLS) cryptographic protocol.

Data in transit is protected using TLS 1.2 for the AgoraCloud sytem, Agora On-Prem, AgoraOps services, and for data being transmitted from web services to consuming clients. All APIs require authorization via the OAuth 2.0 standard to access any data.

One purpose of an edge gateway is to make less-secure data communication protocols more secure by converting the data to a secure protocol for offsite transit. In other words, between the gateway and edge devices, data in transit may or may not be encrypted, depending on the protocol used or the way the protocol is configured to communicate. However, once in the gateway, any offsite data access s secure. Figure 4 illustrates the secure data lifecycle.

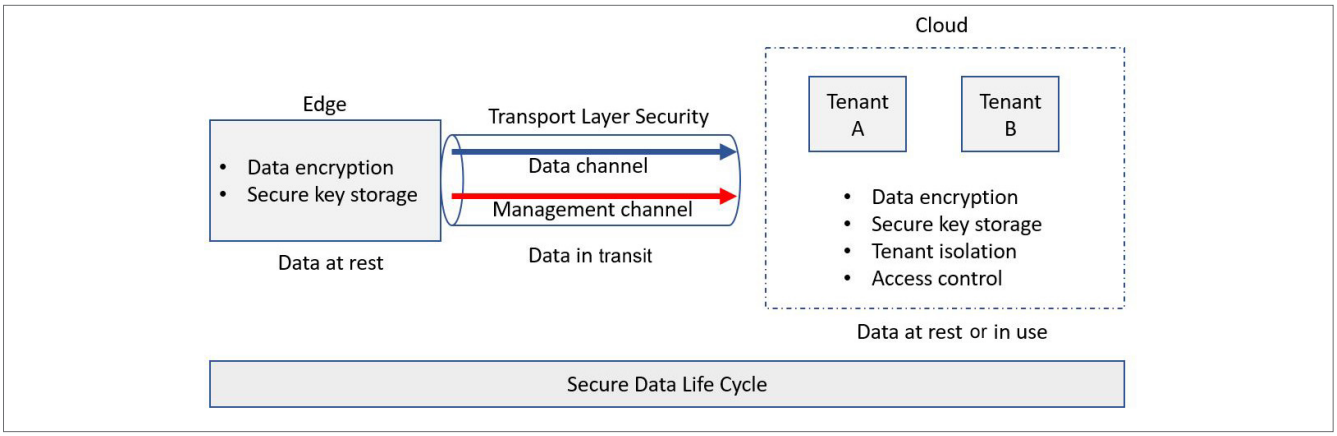



Figure 4: The secure data lifecycle.

### Cloud Security

Agora follows a multiple-cloud strategy that currently incorporates Microsoft Azure and the Google Cloud Platform (GCP). Device commissioning and management is performed through Microsoft Azure services. This includes the device provisioning service (DPS) and the Azure IoT Hub. Telemetry data can be sent to the Google cloud, the Azure cloud, or a customer's private cloud, depending on the deployment.

AgoraCloud services are developed based on a comprehensive body of Schlumberger cloud security standards and guidelines. These include—among others—the cloud security framework, encryption standards, penetration testing, secure deployment, authentication and access control, and compliance. Cloud security guidelines are published to provide guidance on secrets management, network security, secure deployment practices, and threat modeling. Agora leverages these standards and best practices to build a secure cloud service.

As mentioned earlier in the Data Security section, the AgoraCloud system utilizes AES-256 encryption with secure key management. Multifactor authentication is enforced, and identity federation is supported to enable customers to authenticate using their native credentials. A strong tenant-isolation model is used to keep data and applications segregated for each customer, and security-related events are logged and monitored 24/7 to ensure that security incidents are detected and responded to in a timely manner.

### Secure Development Lifecycle

Software development for the Agora Platform follows secure software development practices to ensure that security has been included in every stage of the software lifecycle. All software developers are required to complete mandatory application security training, which covers common application security vulnerabilities and security best practices in application development. Security requirements, threat modeling, and design reviews are included in the early stages of development. Static and dynamic code analyses are performed during the implementation and testing phases. Static, dynamic, and software composition analysis tools are integrated into the automated software deployment platform to ensure it is consistently performed during each development cycle. Finally, periodic vulnerability review and penetration testing are performed by both an internal security team and a third-party security vendor to ensure the security of the Agora Platform. Figure 5 illustrates the secure software development lifecycle.

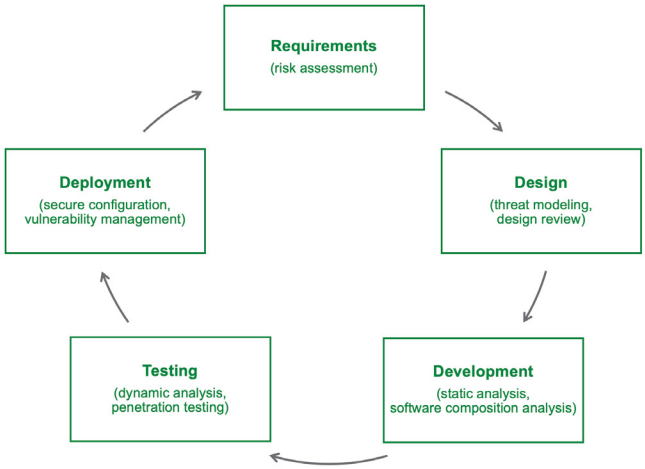



Figure 5: The secure software development lifecycle.

### Security Qualification Processes

Security qualification is a standard process for security validation that checks the readiness of an application for deployment against the security standard. Compliance is maintained throughout development and audited at certain development stages. For Agora, two security qualification processes were undertaken: the security application qualification process (SAQP) and the cloud security qualification process (CSQP).

SAQP assesses the security risks in the system architecture and requires the development organization to perform security testing against the application. It examines various aspects of the endpoint or application communications channels and performs security testing on all those channels. The process also provides recommendations for retesting or acceptance of the application.

Similar testing is performed for any cloud-hosted application as part of the CSQP. In this case, special emphasis is placed on the security of publicly exposed services or endpoints to ensure that proper communications security and network security are in place. Additionally, the process ensures compliance with Schlumberger cloud security standards. Threat modeling is performed to ensure that the application architecture follows best practices and adequately addresses any threat that is discovered during the analysis process.

## Secure Deployment

Secure deployment of Agora IIoT technology involves several operations including device hardening, network segmentation, and screening.

### Device Hardening

The AgoraGateway device is based on Linux Debian long-term support (LTS). The system is hardened to ensure that the gateway and operating system attack surface is minimized. All unnecessary ports, services, and communication links are blocked. Industry-standard benchmarks like the Center for Internet Security's (CIS®) control assessment tool (CIS-CAT) for Debian Linux have been deployed to reduce the attack surface qualitatively and quantitatively. Endpoint security assessment tools are utilized to map the attack surface to produce recommendations which are then analyzed to further reduce the residual attack surface.

### Network Segmentation

Secure connectivity to external networks is provided using a defense-in-depth approach. The AgoraGateway device can only send data to selected trusted destinations as prescribed in the gateway configuration.

The AgoraGateway device can connect via cellular, Ethernet, or satellite infrastructure for northbound connectivity (i.e., outbound traffic that goes to the cloud) as shown in Figure 6. Applications and services on the gateway are not directly exposed to the Internet. The exposure to the customer's network over Ethernet or over satellite is lower than over a cellular LTE connection. To minimize the attack surface on cellular networks, the AgoraGateway device uses an access point name (APN) to directly send the traffic to a landing point in the Schlumberger demilitarized zone (DMZ), which is a physical and logical subnet that separates the Agora network from other untrusted networks. This enables superior protection since the data is traveling only over a private network.

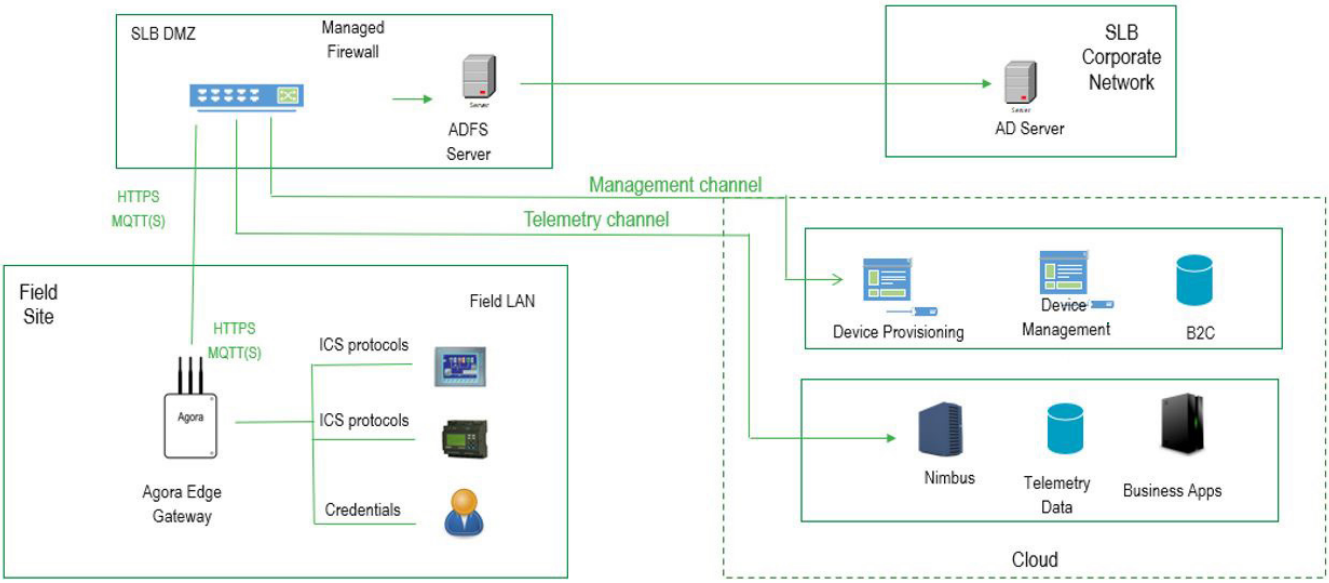
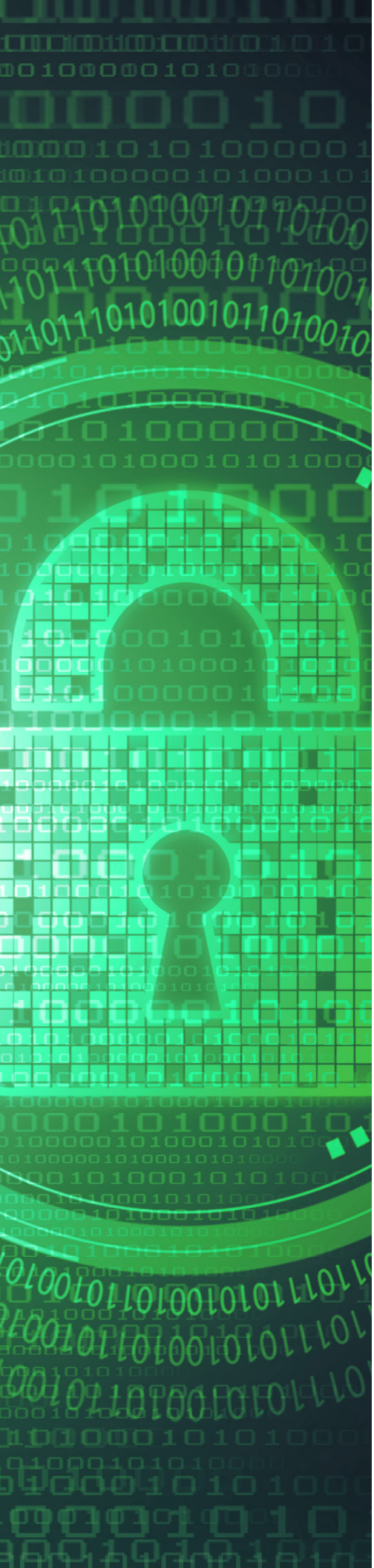



Figure 6: Agora network segmentation for northbound communication.

At the DMZ, the landing point is a firewall that inspects the headers and ensures that only data destined for white-listed locations are enabled, while everything else is denied. From the DMZ, data destined for Microsoft Azure is sent over a Microsoft Azure ExpressRoute, which is a private direct connection between the Schlumberger DMZ and the Azure data center. At the protocol level, TLS 1.2 is used to protect all traffic. Southbound connections (to other systems at the wellsite) are secured using an adaptive approach. Communications with web servers uses HTTPS with TLS 1.2. Network and application configuration services are accessed over Secure Shell Protocol (SSH) using the common well-established method of certificate-based authentication.

### Edge Application Security Screening

Every edge application must pass a security-screening process before it is approved for deployment on the AgoraGateway device. This process includes edge app vulnerability scanning, malware scanning, and detection of malicious runtime behaviors. Edge applications are hosted on secure repositories (isolated by the customer). Periodic scans are performed on repositories to flag applications with high or critical vulnerabilities.



# Secure Operation

Secure operation of an Agora-based IIoT system relies on several important pillars, including regular software updates, a security dashboard, and robust monitoring and incident response.

### Secure Updates and Device Management

Software deployed on IIoT systems tends to be unpatched for long periods of time, which creates publicly known vulnerabilities. Patching IIoT systems can be challenging because cloud-based updates require secure connectivity to the cloud, whereas local updates require manual intervention, which opens avenues for malware infection.

The Agora Platform uses a comprehensive vulnerability management program that includes weekly scanning of the cloud infrastructure and the dedicated edge gateway to detect any new potential vulnerabilities. All findings are assessed by the Agora security and engineering team to create proper patching as part of a vulnerability mitigation plan.

The AgoraGateway device leverages its continuous and secure connection to the cloud to update software on the device from the cloud. It does not provide local update functionality, which—in combination with secure boot—protects against any potential malware infections. Cloud-based software updates ensure that edge software is running the correct versions. Hot patches for security can be deployed on-demand through the cloud in a fast and smooth manner.

### Security Compliance Dashboard

For a gateway deployed in the field, its health and security compliance status are reported and displayed on the AgoraOps services portal for tracking purposes. This enables an accurate security baseline and inventory of gateways and enables faster incident response and security updates.

### Security Monitoring and Incident Response

Agora's security posture meets or exceeds industry expectations. However, in the rare event a cybersecurity breach is encountered, the Agora Platform not only employs security controls to reduce the likelihood of a cybersecurity breach but also implements security monitoring and incident response procedures to ensure a breach will be quickly detected, so that its impact to the business is reduced and contained. An effective security monitoring and incident response program requires good system and operational visibility.

Typically, organizations have no visibility into the IIoT environment. If an attacker tries to attack an IIoT device, the organization will receive no alerts. To address this, Agora has partnered with major technology vendors to provide security monitoring. At the wellsite, a security agent is deployed on the AgoraGateway device to continuously monitor system activities and upload system security telemetry to the cloud. The cloud service correlates the received data with known attack patterns and threat intelligence. Once it is confirmed that the events are due to a security incident, a security alert incident report is sent to the automation platform at the Schlumberger Cybersecurity Operations Center (CSOC). After initial alerts are sent, a CSOC analyst is assigned to the incident. The CSOC will collaborate with the Agora Edge Operations Center (EOC) to resolve the incident and initiate incident response actions based on a predefined security playbook.

The AgoraCloud system is also monitored by the CSOC around-the-clock. All operations and performed tasks are logged and malicious activities are quickly detected and resolved. Figure 7 illustrates the CSOC security monitoring and incident response workflow.

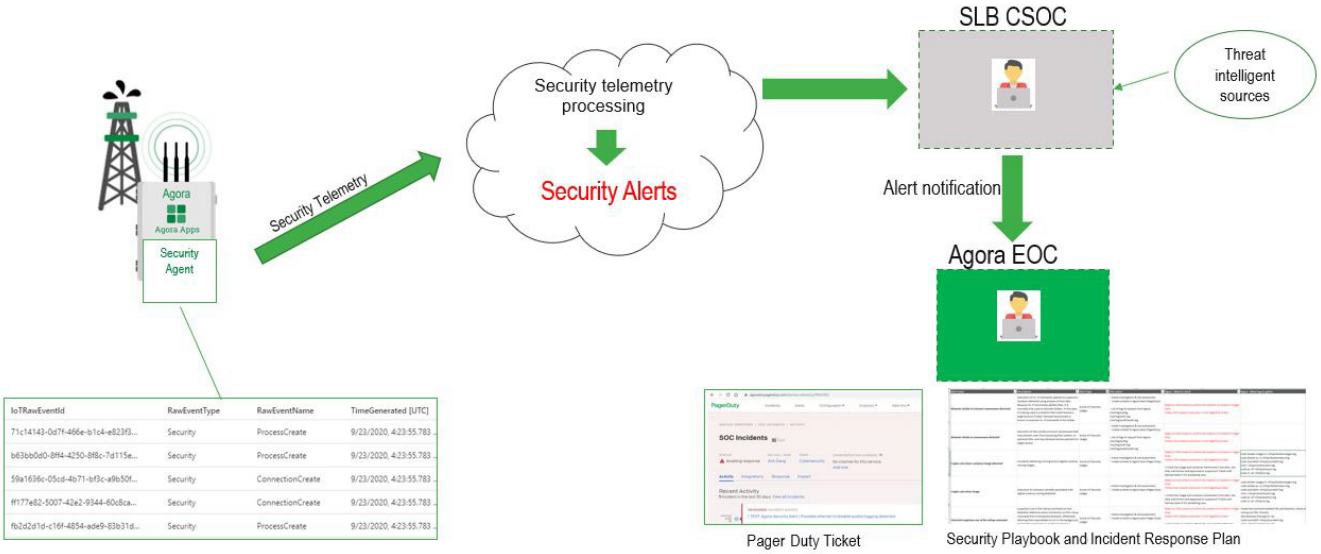



Figure 7: Security monitoring and incident response workflow.

# Alignment with Industry Standards and Best Practices

The Agora security strategy is fully aligned with well-known security standards and best practices. Prominent among them are the security standards and cybersecurity frameworks promoted by the US National Institute of Standards and Technology (NIST), the Industry IoT Consortium (IIC), and the Cloud Security Alliance® (CSA). NIST has several cybersecurity guidelines published to cover subareas such as the cybersecurity framework (CSF), cryptography (NIST SP 800-175B), security controls (NIST SP 800-53), cybersecurity baseline for IIoT (NISTIR 8259), and industrial cybersecurity (NIST SP 800-82), among others.

Agora edge security incorporates the relevant parts of these guidelines in developing the Agora Platform. For instance, all the cryptography mechanisms such as encryption, digital signing, hashing, and key management are compliant with the NIST cryptography guideline. Also, the Agora security team reviews changes and updates to these guidelines to ensure that the updated recommendations are implemented in the platform.

Similarly, the Agora Platform is aligned with the IIC security framework and security controls from the CSA. Suggested controls from the IIC security framework that are related to endpoint protection, secure connectivity, security monitoring, security configuration, and data protection are all implemented in the Agora Platform.

# SOC 2 Compliance

The Agora security team has completed an assessment for industry-standard Service Organization Controls 2 (SOC 2, Type 2) and achieved accreditation for security and availability. SOC 2 certification means that all best practices are followed for high-quality service delivery and management on the Agora Platform. The certification attests to the fact that Agora security controls ensure top-notch security and availability in the Agora environment to meet operational demands. Figure 8 shows the factors considered as part of the SOC 2 certification process.


Figure 8: Security monitoring and incident response workflow.

# Third-Party Security Penetration Test

A third-party security penetration test was conducted by a reputable cybersecurity company in 2022 on the AgoraCloud platform. The outcome of this test was quite positive because no major security issues were detected. The third-party company issued a detailed report to acknowledge the high level of security present in the AgoraCloud system.

# Conclusion

The Agora Platform is secure by design and its security posture is maintained throughout the entire platform and system life cycle from development, deployment, and operation to the system's end of life. The Agora security strategy is aligned with well-known security standards and industry best practices. It is widely recognized that cybersecurity is a journey, not a destination. And, because of this, the Agora Platform is continuously updated and regularly assessed to improve its capabilities and security controls so that it is best equipped to adapt to the evolving IIoT threat landscape.