Study S1:
IIoT

IIoT Risk Assessment

Assessment Location
Meetings conducted virtually with LOGIIC members

aeSolutions

Final Revision: 04/19/2021

Table of Contents

I. Executive Summary

I.1 Background

The Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) consortium was established to study common cyber security issues as they pertain to the Oil & Gas sector. To date, LOGIIC has completed eleven (11) projects in areas relevant to Oil & Gas operations.

Study 1, Industrial Internet of Things (IIoT) Risk Assessment, was defined by the LOGIIC Executive Committee, the technical team, and the Department of Homeland Security (DHS) sponsor. It is comprised of assessments of four (4) IIoT architectures and associated use-cases. Results from this technical report may be compiled and extracted into overall lessons learned and be made available to public at study completion. This report documents the technical details of the Study 1: IIoT Risk Assessment.

The advent of the Industrial Internet of Things (IIOT/Edge) within the Oil and Gas domain has the potential to expose control and safety systems to significant Cyber Security threats. These include:

- Exposure of the industrial control system (ICS) to untrusted external connectivity
- Poor controls on generic IIOT Gateways or Edge Devices
- Weak Cloud Security
- Control conflicts and process upset derived from the advent multiple control schemes

The purpose of this study was to deliver practical guidance with regards the implementation of these technologies in a manner that does not result in a compromise of existing ICS security controls. The study evaluated four commonly deployed IIoT architecture types, evaluated the risks, and defined associated security controls appropriate to each.

I.2 Scope of the Project

aeSolutions was selected as the subject matter expert (SME) to facilitate this study. They executed the following scope as a part of this study:

- Reviewed commonly deployed IIoT architectures provided by LOGIIC members
- Selected 4 shortlisted architectures of varying complexity and design for detailed study
- Collected and researched information on the selected architectures
- Developed Zone and Conduit Drawings for each of the selected architectures
- Analyzed collected information and prepared all materials necessary for a CyberPHA
- Facilitated CyberPHA Workshops on each of the 4 selected architectures

I.3 Summary of Findings

The project identified several risks in the IIoT architectures studied. A summary of these findings includes:

Risks to Interconnected ICS Systems

The highest risks identified over the course of this study were related to IIoT architectures that potentially exposed ICS devices/systems to untrusted connections.

These connections could potentially lead to a compromise of the control system or allow for reconnaissance, data exfiltration, and a persistent presence in the system. Deployment of these architectures is typically driven by requirements to integrate data from existing ICS equipment into cloud-based analytics/optimization tools or corporate objectives to utilize existing infrastructure. However, the potential to compromise ICS or other connected systems or the consequence of compromise might not have been adequately considered. For example, an IIoT architecture that is acceptable for connecting to and monitoring a standalone cooling tower programmable logic controller (PLC) may not be sufficiently secure to connect to an electrical supervisory control and data acquisition (SCADA) system.

Risks to Corporate or Third-party Clouds

Cloud risks assessed by the team largely fell into two categories, denial of service and loss of confidential information. The level of risk associated with each varied depending on the criticality of the IIoT service to the organization as well as the importance of the data residing in the cloud.

Risks to IIoT Field Devices (e.g. gateways and sensors)

Through the course of the study the assessment team identified and reviewed scenarios that were not widely known or previously considered by the team including: file transfer from IIoT devices, management of IIoT devices with transient process control network (PCN) equipment, and poorly defined overall ownership of IIoT systems. These risks ranged from medium to high and can be mitigated in most cases by applying or adapting ICS best practices and programs that are already in place.

II. Introduction and Background

Study 1, Industrial Internet of Things (IIoT) Risk Assessment, was chartered to provide the foundations for the LOGIIC members to be able to:

- Define IIoT (and Edge computing) as it pertains to Oil and Gas Industrial Control Systems
- Architecture
    - State and propose recommendations for selecting and implementing IIoT/EDGE and Gateway Architecture
    - Indicate, from the proposed architecture(s), the exposure to ICS
- Hardware
    - Recommend basic security requirements for a secure IIoT Gateway
    - Recommend basic security requirements for a secure, dedicated Wired and Wireless IIoT Sensor
    - Recommend basic security requirements for use of an ICS Wired and Wireless Sensor
- Cloud (where applicable)
    - Propose recommendations for secure cloud connectivity
- Define the requirements to safely and reliably deliver IIoT derived data back into the ICS environment without compromising existing controls

For this project, four (4) distinct architectures with corresponding use cases were selected for evaluation based on the collective inputs from various LOGIIC members. These architectures, designated as Architecture 1, 2, 3 and 4, are presented in Appendix A of this report.

III. Description of IIoT Architectures and Use Cases

III.1 Architecture 1

III.1.1 Description of Architecture 1:

Architecture 1 is a fairly common IIoT implementation where traditional ICS sensors are connected to one or more IIoT Gateway that aggregate and report data to a third-party cloud service. The IIoT data is sent to the corporate IIoT cloud for additional analysis and integration with process data from the process historian.

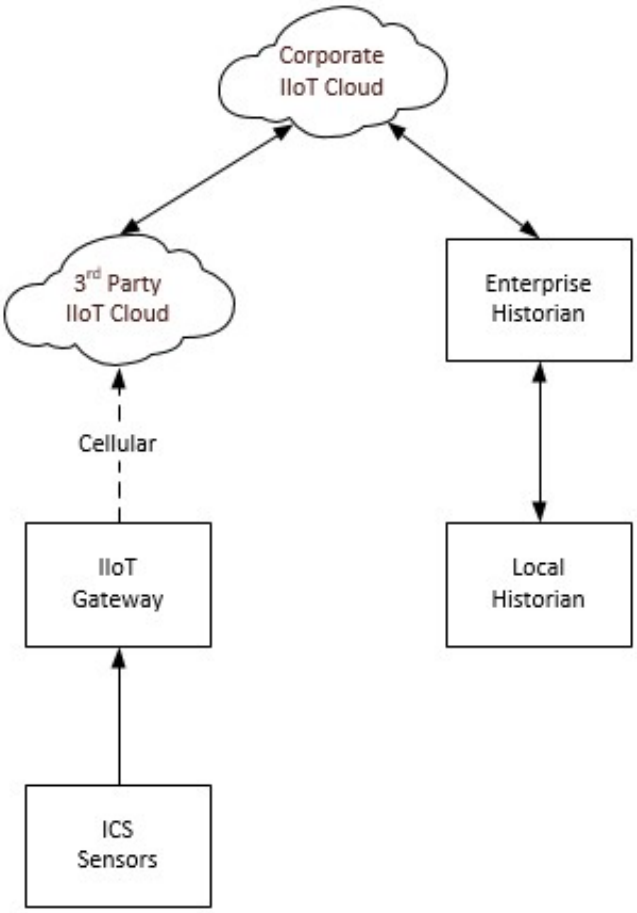


Figure 1: IIoT Architecture 1

III.1.2 Architecture 1 Use Case - Wellhead Monitoring

Remote monitoring of wellheads in areas where cellular reception is available (onshore or shallow water). Wellhead monitoring sensors (Pressure, Temperature, etc.) are wired directly (4-20 mA) to a Digi Connect Sensor. This sensor is powered via an onboard battery and communicates directly with the cloud via Cellular connection

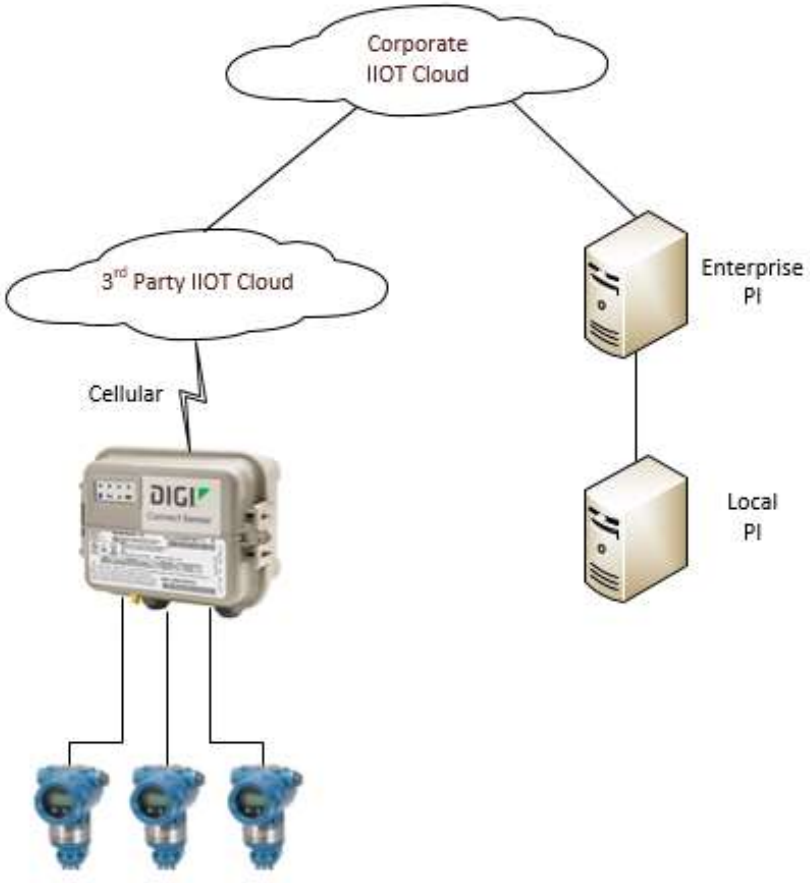


Figure 2: Wellhead Monitoring Use Case

III.2 Architecture 2

III.2.1 Description of Architecture 2:

Architecture 2 makes use of both an IIoT Wireless Gateway and Edge Gateway to further leverage the advantages of IIoT sensors. The IIoT Edge Gateway also collects data from the existing ICS devices. This direct connection to an ICS device greatly increases the risk of this architecture and has resulted in it being disallowed by many owner operators.

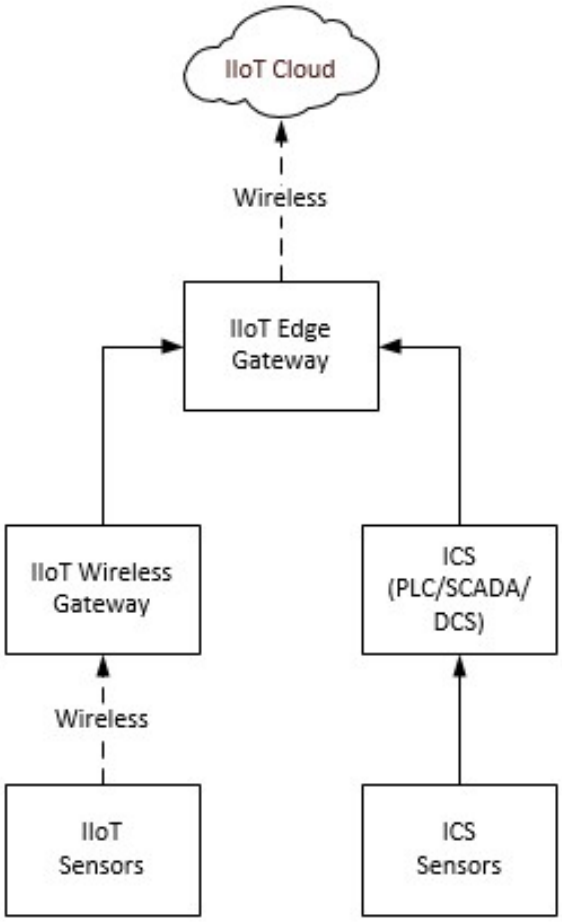


Figure 3: IIoT Architecture 2

III.2.2 Architecture 2 Use Case - Switchgear Monitoring

Wireless ZigBee sensors (temperature, humidity) connected to a ZigBee gateway are used for monitoring of switchgear and other electrical assets. The IIoT Gateway collects data from both the ZigBee gateway and electrical SCADA. This data is transferred to the cloud via Cellular connection.

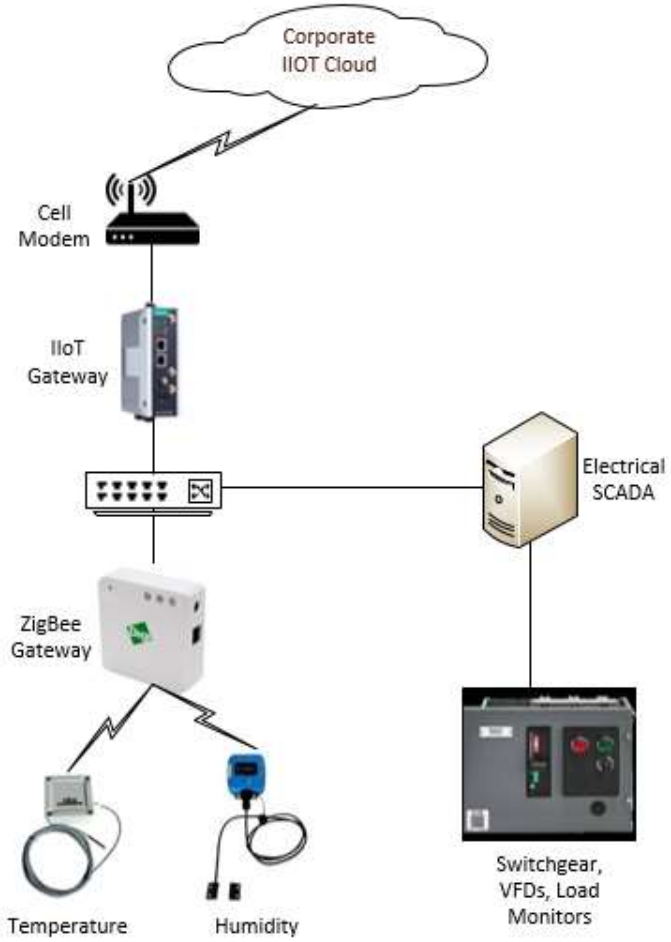


Figure 4: Switchgear and Electrical Monitoring Use Case

III.3 Architecture 3

III.3.1 Description of Architecture 3:

The Architecture 3 IIoT equipment deployment is very similar to Architecture 2 and also includes collection of data from existing ICS systems. However, Architecture 3 utilizes the existing ICS network, rather than cell or wireless, to transfer IIoT data to the cloud.

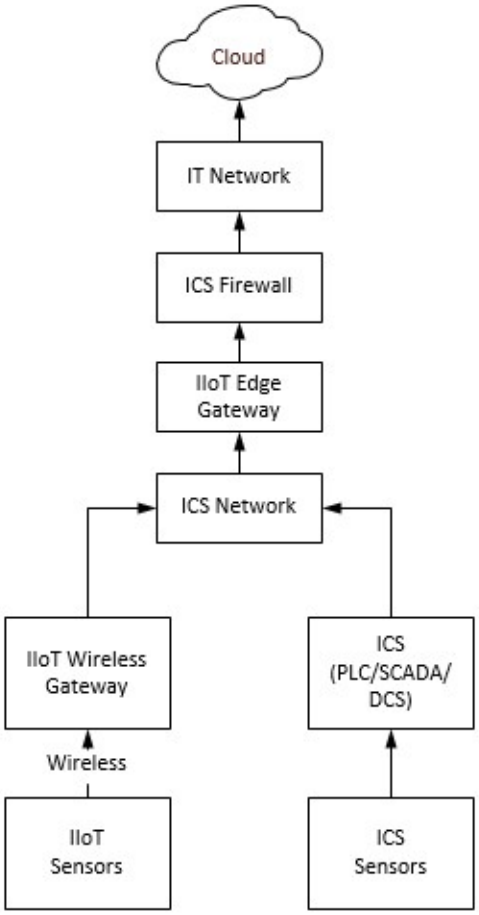


Figure 5: IIoT Architecture 3

III.3.2 Architecture 3 Use Case - Tank Monitoring

Wireless WiHART sensors (level, roof tilt, volatile organic compounds, etc.) connected to a WiHART gateway are used for tank monitoring and management. The IIoT Gateway collects data from both the WiHART gateway and process control equipment. This data is transferred to the cloud utilizing the existing network infrastructure.

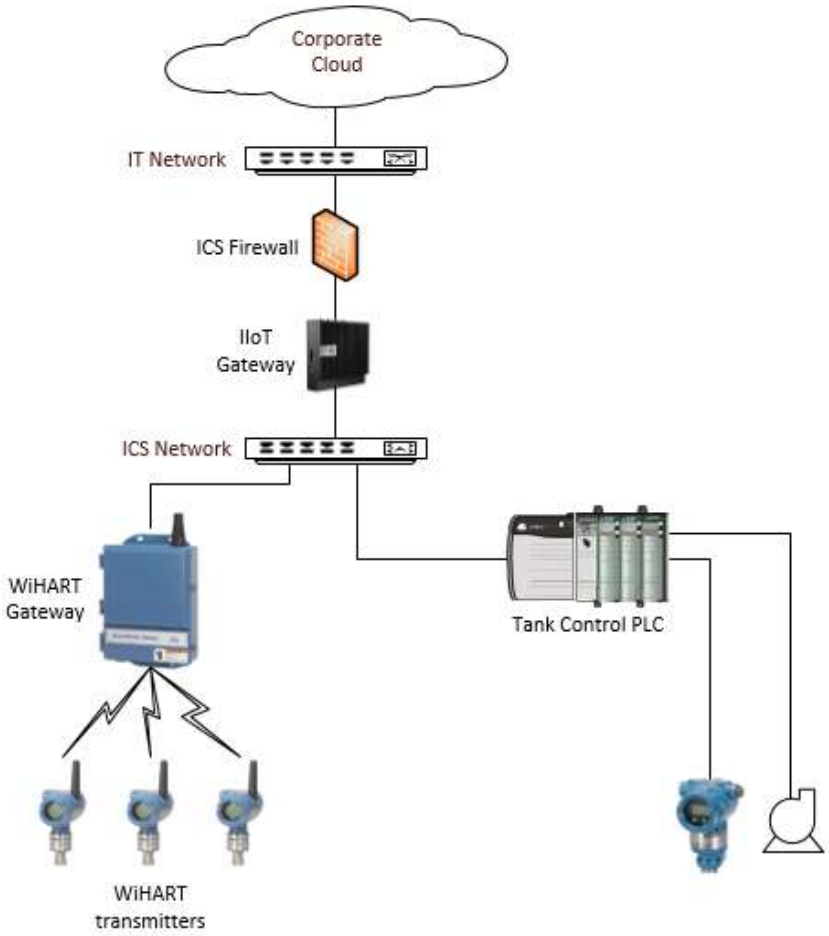


Figure 6: Tank Monitoring Use Case

III.4 Architecture 4

III.4.1 Description of Architecture 4:

Architecture 4 is the most complex of those studied by the team. This architecture utilizes a local IIoT server to collect sensor data, transfer it to the cloud, and interface with the distributed control system (DCS). Data passes through perimeter firewalls effectively creating an IIoT DMZ.

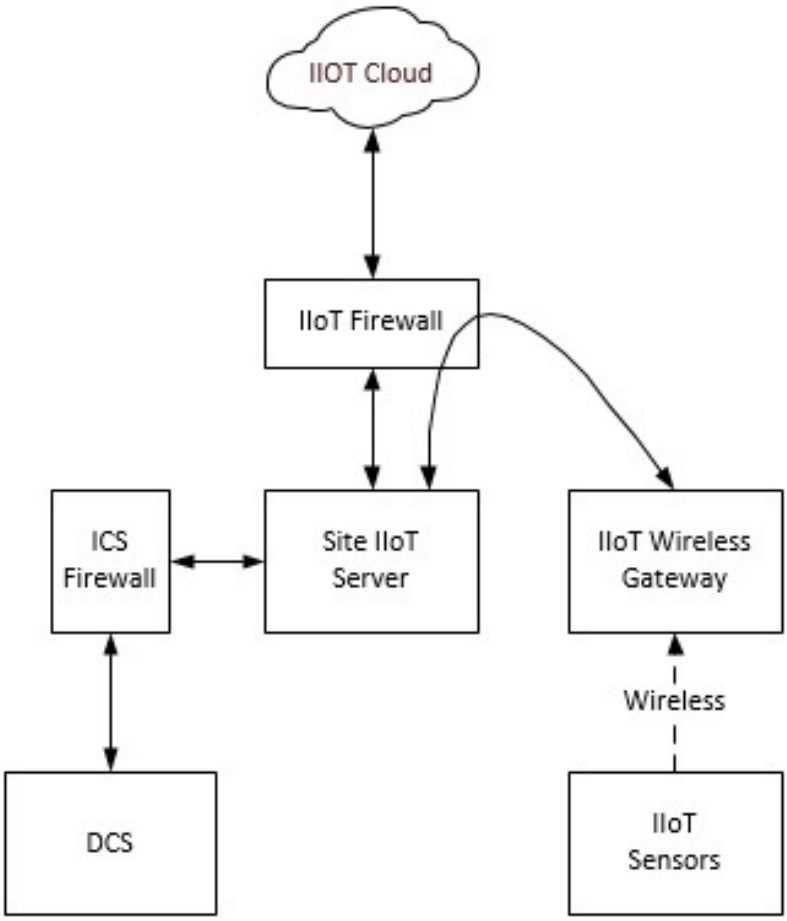


Figure 7: IIoT Architecture 4

III.4.2 Architecture 4 Use Case - Pump Monitoring

Wireless LoRaWan sensors (Vibration, On/Off status, pressure, etc.) connected to a LoRaWan gateway are used for pump monitoring. The local IIoT server collects data from the LoRaWan devices as well as the DCS for processing in the cloud. Processed data as well as raw IIoT sensor data is communicated to the DCS for display purposes.

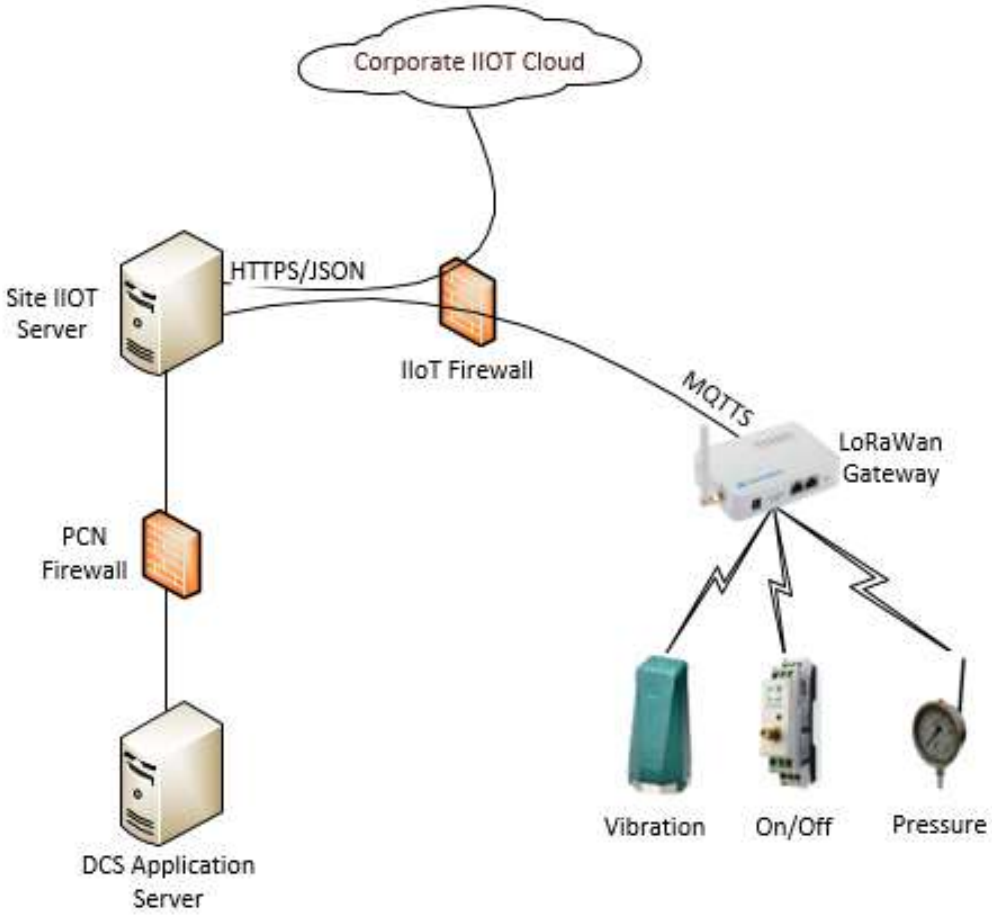


Figure 8: Pump Monitoring Use Case

IV. Risk Assessment Methodology

Risk assessments workshops were conducted on each of the architectures utilizing the Cyber PHA methodology which is a proven methodology for conducting ICS cybersecurity risk assessments based upon the requirements in ISA/IEC 62443-3-2 "Security Risk Assessment for Design". Figure 9 illustrates the workflow for the Cyber PHA methodology.

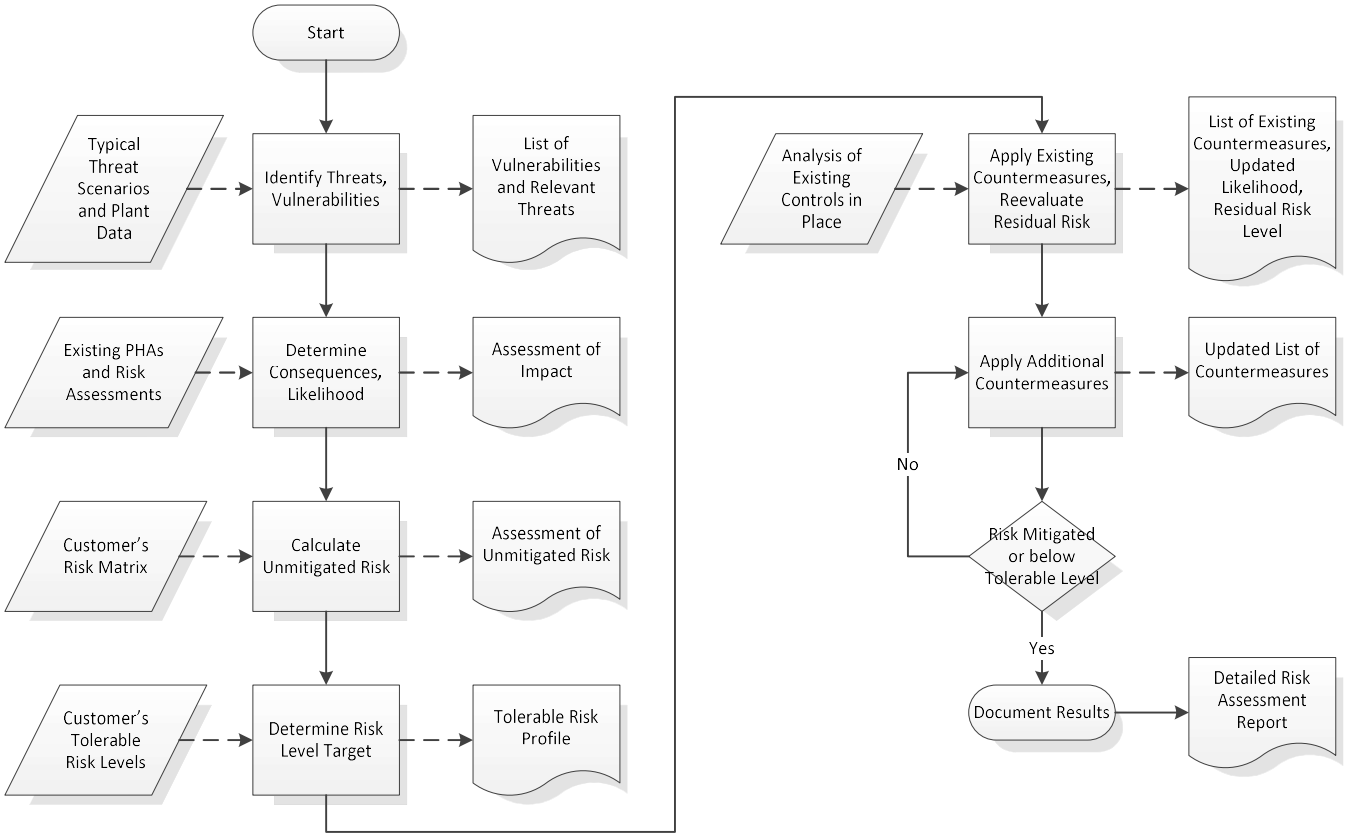


Figure 9: Cyber PHA Workflow (Adapted from ISA 62443-3-2)

Prior to the workshop, each of the architectures were partitioned into security zones. The workflow was repeated for each security zone in each architecture.

Also prior to the workshops, aeSolutions researched representative vulnerabilities for each of the selected architectures and use cases to provide the workshop team with realistic examples of the vulnerabilities that could be exploited by a threat actor.

aeSolutions provided subject matter experts (SMEs) experienced in facilitating risk assessments for industrial control systems (ICS) and IIoT architectures. LOGIIC members participated in the risk assessment to provide their knowledge of IIoT, the IIoT architectures and use-cases, and associated risks.

The risk assessment results were captured in a software tool provided by aeSolutions which is based upon a commercial software program, PHA-Pro by Sphere, that has been customized by aeSolutions for industrial cybersecurity risk assessments.

Identifying Threats

Specific threat scenarios were identified for each security zone based upon the following general classification of threat types:

Tampering – Deliberate

Deliberate and malicious tampering to control system assets (computers, controllers, network equipment) by either personnel authorized to be in the area or unauthorized personnel. May take place either locally or remotely.

Malware – Targeted

Specific and malicious malware targeted at the system assets with the intention of causing a dangerous event, denial of service, or to access proprietary data.

Malware – General

Any malicious software introduced into the control system which may compromise the functionality of the system or cause a complete denial of service.

Denial of Service

Any event that causes a control system asset to be unavailable for its intended purpose either temporarily or permanently.

Identifying Vulnerabilities

Research into known vulnerabilities was conducted prior to the risk assessment workshops. This information, coupled with the expertise of the workshop facilitators and attendees, was used by the assessment team to develop realistic scenarios.

Identifying Consequences

Consequences were identified by the workshop team based on general industry experience and knowledge of the applications. The consequences were assigned severity scores using Table 1 of the risk matrix found in Appendix A.

Determining Likelihood

Unlike process safety PHAs that often make use of Layer of Protection Analysis, Fault Trees, and complex modelling to better estimate likelihood, there is currently no industry standard for assessing the likelihood of cybersecurity events. This can lead to inconsistent results both between and within studies. To address this the Cyber PHA methodology uses well established principals to separate cybersecurity likelihood into its constituent parts (refer to Figure 10. These can then be analyzed in greater depth based on the specific scenario being considered. The factors are then weighted and normalized to the Risk Matrix likelihood scale. The likelihood scales used for this study is Table 2 of the risk matrix found in Appendix A

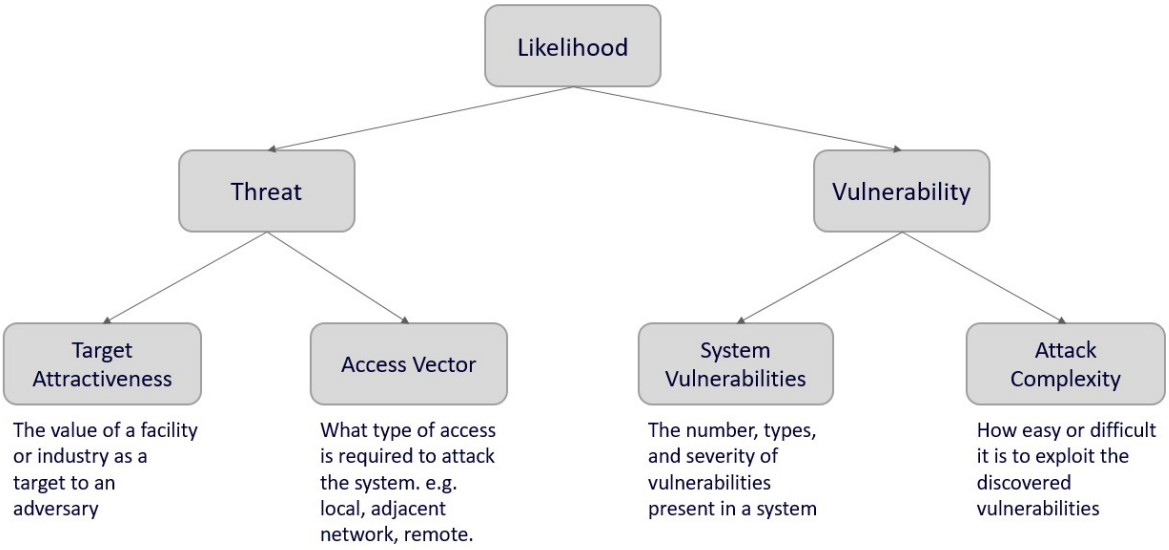


Figure 10: The Components of Likelihood

Other methodologies using a similar process include the Common Vulnerability Scoring System (CVSS) used by NIST for the National Vulnerability Database as well as many Chemical Facility Anti-Terrorism Standards (CFATS) studies.

V. Risk Assessment Findings

The results of the risk assessments performed for the four reference architectures are broken out into risks and suggested control measures that were common to all architectures as well as risks and control measures specific to individual architectures.

V.1 Common Findings

The following is a summary of risk assessment findings that were common to all four (4) architectures assessed.

V.1.1 IIoT System Ownership

The assessment team noted that after the deployment of IIoT equipment there were frequently questions about who (or what organization) had overall responsibility for ownership, maintenance, and monitoring of the system. For systems isolated from the ICS this resulted in relatively low risk, however, for systems connected to the ICS this could result in a greatly increased attack surface if these systems are poorly managed. Responsibilities for IIoT systems must be clearly defined prior to, as well as after, deployment.

V.1.2 Utilization of IIoT Data for Process Optimization

Utilizing IIoT data for process optimization or as an additional data point for operators is quickly becoming a key aspect of IIoT deployments. These have the potential to impact systems regardless of the architecture. The risk associated with these scenarios is highly dependent on the process as well as how the data is being used and should be mitigated accordingly. Two different use cases were evaluated in this study.

The first case is providing IIoT data to operators as a reference for manual process adjustment could result in upsets or activation of other safety measures if the operator is presented with unreliable, outdated, or inaccurate information. The team's recommendation focused on ensuring that the operator understands the source of the data as well as limitations that it may have. Unlike the process data that operators typically use, IIoT data is updated much less frequently. If possible, the time that the data point was last updated should be presented to the operator to prevent the use of stale data.

Similar to utilizing data to operators for manual adjustment, some applications of IIoT are utilizing analysis data for process optimization via setpoint adjustment. In a worst-case scenario, the data feeding these setpoints could be corrupted or manipulated leading to process disruption or spurious activation of other safety measures. This use case is similar to the decades-old application of Advanced Process Control (APC) systems that may be configured to automatically adjust setpoints. However, using IIoT and cloud analytics can present even greater risk to operations. The team made several recommendations, including: inputs into the control system be restricted via "guardrails" on the setpoints to keep them within an acceptable range, operators should have the ability to override external setpoints, and IIoT data use should be limited to setpoint adjustment only, not alarming or safety functions.

V.1.3 File Transfer

IIoT devices are increasing in complexity as well as the number of functions that they can perform. In particular, the assessment team was concerned that data transfer, especially file transfer, from IIoT devices could potentially bypass countermeasures currently in place to protect the ICS or the enterprise. Principles of least functionality should be employed for data transfer to/from IIoT to limit data transferred to only data types that are required. Further hardening of all ICS devices should be completed based on the risk.

V.1.4 IIoT Edge Gateway

The elevated risks associated with IIoT gateways are, predictably, related to their function as a gateway between different zones. The level of risk is greatly increased when one of those zones is an industrial control system. A large percent of the gateways on the market today ship with full commercial operating systems (Windows or Linux) and the remainder use a custom OS. As a result, these edge gateways are vulnerable to the same types of attacks as many other workstations and servers.

These vulnerabilities should be mitigated using hardening best practices already in place for most ICS systems. If the edge gateways are internally managed (not by a 3rd party) familiarity with operating system hardening should be considered as a part of OS selection. If a 3rd party is managing the security of the devices, then minimum hardening requirements should be provided to them. Example hardening best practices will vary by operating system, but include malware prevention (AV, USB control, patching, and application whitelisting), enabling host-based firewall features, and least privilege user access. This is particularly important for higher risk systems that utilize IIoT in the process rather than just for preventative maintenance and monitoring. In these applications users should consider implementation of secure boot and enhanced/advanced edge gateway security measures.

When connecting to a process control device, IIoT edge gateways should utilize protocols that have lower potential to impact the process control system (or have a reduced severity) if the IIoT edge gateway or server is compromised. For example, utilize serial communications or Ethernet protocols that support only data transfer rather than using protocols that support both data and configuration changes. When connecting externally (e.g. via cellular) secured communications (e.g. private APN) should always be used.

V.1.5 Cloud

Cloud risks assessed by the team can be group into two categories, denial of service due to intention or accidental tampering and loss of confidential information. The risk associated with each varied depending on the criticality of the IIoT service to the organization as well as the criticality of the data residing in the cloud. In both cases, a top remediation was proper user management best practices including separation of duties, least privilege access, 2-factor authentication for administrative and configuration access, and periodically running a cloud security tool to validate security settings. To help mitigate intentional or accidental loss of cloud data and configurations regular backups should be implemented as a part of the cloud solution (it was noted that backups are typically an optional cloud service that must be enabled). The team

also reviewed several scenarios where a mass denial of service could occur due to accidental changes to the system including accidental deprovisioning of the cloud service and pushing invalid or corrupted firmware to IIoT devices. In both cases, standard best practices of separation of duties, affirmative prompts, and firmware/patch validation should be utilized.

In addition to measures to prevent the loss of confidential data from cloud services, the team reviewed mitigations that could reduce the severity of a release if it did occur. This primarily focused on ensuring non-attribution of the data in the cloud by minimizing or eliminating identifiable information (e.g. company name, place name/locations). When utilizing a third-party cloud service, the team recommended that these requirements be incorporated as requirements in the service contract.

V.1.6 Risk Elimination

To reduce the overall risk of IIoT deployments the team recommended that whenever possible organizations should consider using existing data paths (e.g. process historian) and connecting at higher Purdue levels (preferrable outside the ICS) rather than creating new connections to lower levels.

V.2 Architecture 1 Findings

Zone & Conduit Diagram:

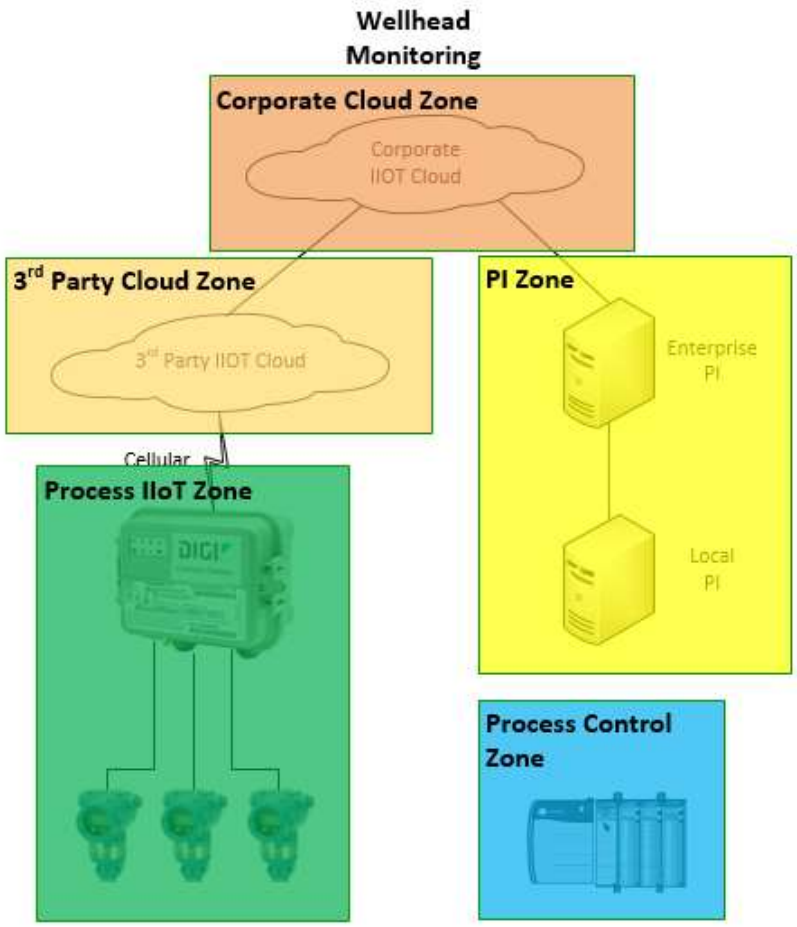


Figure 11: Architecture 1 Zone & Conduit Diagram

Zone Descriptions:

Architecture	Zone/Conduit	Z/C Description
Architecture 1	Process IIoT	Wellhead monitoring sensors (Pressure, Temperature, etc.) are wired directly (4-20 mA) to a Digi Connect Sensor. This sensor is powered via an onboard battery and communicates with the cloud via Cellular connection.
	Process Control	Well control PLC that is not connected to the IIoT devices, but is physically adjacent
	3rd Party Cloud	A 3rd part cloud is used to relay data and manage devices. Device management options include: editing

Architecture	Zone/Conduit	Z/C Description
		configurations, updating firmware, device monitoring, and automating tasks.
	Process historian zone	Data is also transferred to/from the Process historian (both corporate and local) for operational use.
Common	Corporate Cloud	The corporate cloud is utilized for data analysis, processing, and reporting of current and predicted system health.

Risk Profile:

Architecture	Zone	Max Unmitigated Risk
Architecture 1	Process IIoT	M
	Process Control Zone	H
	3rd Party Cloud	E
	Process historian zone	L

Risk Summary:

Architecture 1 was determined to be low risk because of the lack of a direct connection to the ICS network or other ICS devices. The parallel data architecture utilizes existing secure communication via the historian.

There is potential for low risks associated with physical compromise of the devices (e.g. tampering with or stealing the IIoT Gateway) that can be mitigated with additional physical hardening and geolocation alerts (via GPS or cellular tracking) if the device is taken from its original location.

In addition to common cloud risks this architecture includes a 3rd party cloud. These cloud risks must be managed via contractual language, and often through the purchase of optional security services.

Refer to Appendix C for details of the threat scenarios for Architecture 1.

V.3 Architecture 2 Findings

Zone & Conduit Diagram:

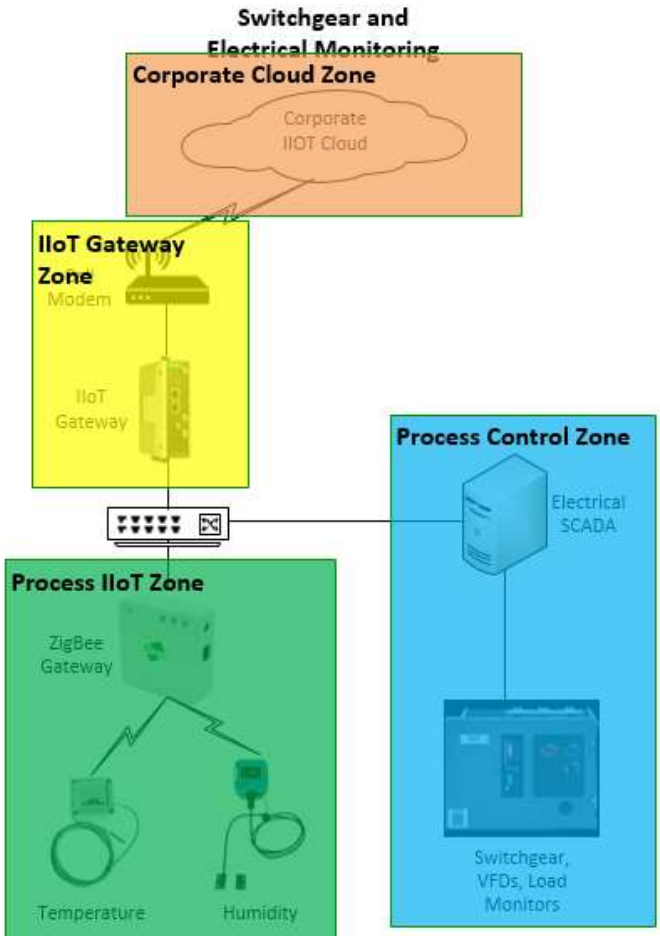


Figure 12: Architecture 2 Zone & Conduit Diagram

Zone Descriptions:

Architecture	Zone/Conduit	Z/C Description
Architecture 2	Process IIoT	Wireless ZigBee sensors (temperature, humidity) connected to a ZigBee gateway are used for monitoring of switchgear and other electrical assets.
	Process Control	Existing electrical equipment process data (load, current, events, etc.) is collected via a SCADA system. This SCADA system has control but is limited to opening circuits and stopping VFDs.
	IIoT Gateway	The IIoT Gateway collects data from both the ZigBee gateway and electrical SCADA. This data is transferred to the cloud via Cell Modem.

Architecture	Zone/Conduit	Z/C Description
Common	Corporate Cloud	The corporate cloud is utilized for data analysis, processing, and reporting of current and predicted system health.

Risk Profile:

Architecture	Zone	Max Unmitigated Risk
Architecture 2	Process IIoT	L
	Process Control	E
	IIoT Gateway	E

Risk Summary Architecture 2:

Architecture 2 was the highest risk and most problematic of the architectures reviewed by the assessment team. The lack of separation between the internet facing gateway and the ICS represented a very high risk of ICS compromise and direct violation of many team members ICS policies. This architecture is not recommended for use; however, it could potentially be approved by exception for very low risk processes.

Additional modifications to requiring more robust separation should be employed to separate the external connection from the ICS. Depending on the requirements of the deployment this could be accomplished through the use of a DMZ, separation using a process firewall, or other means (e.g. data diode).

Refer to Appendix C for details of the threat scenarios for Architecture 2.

V.4 Architecture 3 Findings

Zone & Conduit Diagram:

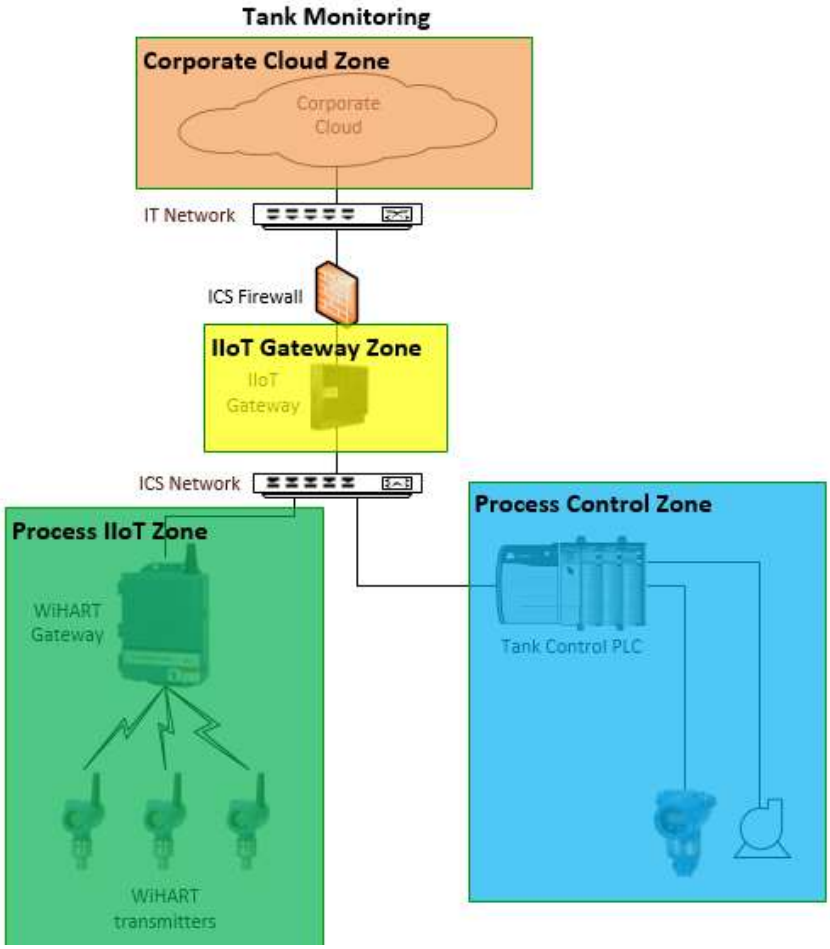


Figure 13: Architecture 3 Zone & Conduit Diagram

Zone Descriptions:

Architecture	Zone/Conduit	Z/C Description
Architecture 3	Process IIoT	Wireless WiHART sensors (level, roof tilt, VOC, etc) connected to a WiHART gateway are used for tank monitoring and management.
	Process Control	Existing process control equipment (Pump controls) has the ability to start/stop pumps and make valve lineup changes.
	IIoT Gateway	The IIoT Gateway collects data from both the WiHART gateway and tank PLC. This data is transferred to the cloud utilizing the existing network infrastructure.

Architecture	Zone/Conduit	Z/C Description
Common	Corporate Cloud	The corporate cloud is utilized for data analysis, processing, and reporting of current and predicted system health.

Risk Profile:

Architecture	Zone	Max Unmitigated Risk
Architecture 3	Process IIoT	L
	Process Control	H
	IIoT Gateway	H

Risk Summary Architecture 3:
The High risk of this architecture is primarily due to the potential to pivot from the IIoT Edge gateway to other devices on the process control network. In this case the intention to utilize existing architecture has opened another potential path for compromise of the ICS network. The degree of increased risk is partially determined by how these devices are managed; risk increases as more management of the IIoT edge gateway, wireless gateway, and sensors, is completed externally from the cloud. This architecture can also increase device complexity if IIoT devices are managed by a 3rd party or different organization than ICS devices. Finally, this architecture as drawn does not meet the requirement of many end-users that all connections terminate in the DMZ, mitigation of which could require a local server and increased complexity.

The assessment team recommended that all IIoT devices located on the ICS network (below the ICS firewall) be managed and hardened to the same degree as other ICS devices. Required connects from the Edge gateway to the cloud should be minimized. Other best practices should be implemented to segregate the IIoT traffic onto a separate VLAN or network segment and configure firewalls rules and ACLs where required to enforce this.

Refer to Appendix C for details of the threat scenarios for Architecture 3.

V.5 Architecture 4 Findings

Zone & Conduit Diagram:

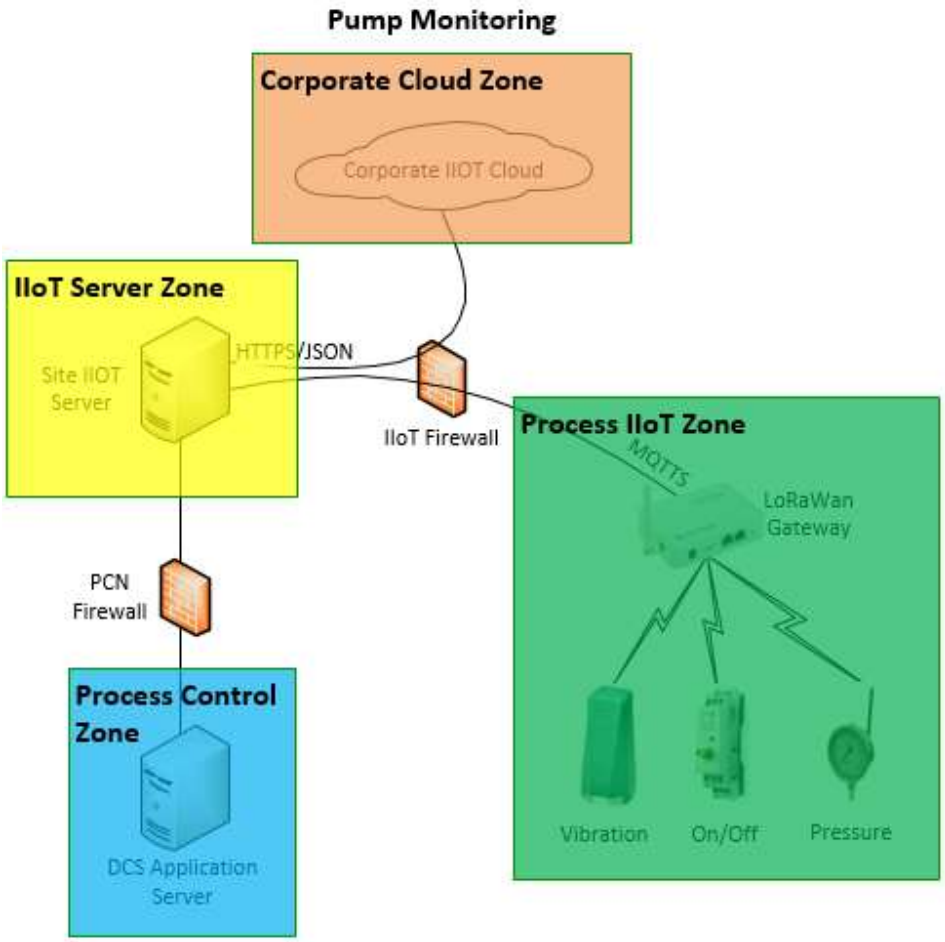


Figure 14: Architecture 4 Zone & Conduit Diagram

Zone Descriptions:

Architecture	Zone/Conduit	Z/C Description
Architecture 4	Process IIoT	Wireless LoRaWan sensors (Vibration, On/Off status, pressure, etc.) connected to a LoRaWan gateway are used for pump monitoring.
	Process Control	The existing process control (DCS application server) has full control over the process. Indication from IIoT devices is used for monitoring only, not alarming or real-time control.
	IIoT Server	The local IIoT server collects data from the LoRaWAN devices as well as the DCS for processing in the cloud.

Architecture	Zone/Conduit	Z/C Description
		Processed data as well as raw IIoT sensor data is communicated to the DCS for display purposes.
Common	Corporate Cloud	The corporate cloud is utilized for data analysis, processing, and reporting of current and predicted system health.

Risk Profile:

Architecture	Zone	Max Unmitigated Risk
Architecture 4	Process IIoT	M
	Process Control	H
	IIoT Server	H

Risk Summary Architecture 4:
Architecture 4 utilizes an IIoT DMZ and was found to be a similar or lower risk compared to other architectures. Architecture 4 is more complicated and expensive to deploy but, assuming firewall rules are configured correctly, it is similar to other established and accepted DMZ architectures used to transfer data to process control. Risk can be further reduced by implementing several common recommendations including limiting the DCS connection protocol to one that minimizes what tampering could occur and ensure that operators are properly trained in the use and limitations of IIoT data.

The gateways are not directly internet facing so good physical controls and hardening can largely reduce the risk of tampering.

Refer to Appendix C for details of the threat scenarios for Architecture 4.

VI. Recommendations

This section presents recommendations from LOGIIC for both end-users of IIoT solutions as well as IIoT solution vendors.

VI.1 Overall Recommendations

VI.1.1 General

1. Ensure that all IIoT devices are properly inventoried.
2. Formalize IIoT device ownership and responsibility. (e.g. who is responsible for maintenance of the device, who is responsible for security of the device, is ICS involved and/or consulted about ICS connections).
3. If utilizing IIoT for external setpoint control or adjustment, implement best practices for utilizing external setpoint inputs into the process control including:
    - Restrict inputs into the control system via "guardrails" on the setpoints to keep them within an acceptable range
    - Ensure operators have the ability to override external setpoints
    - Limit external data to control adjustment only, do not use this data for alarming or safety functions.
4. Implement principles of least functionality for data transfer to/from IIoT (e.g. limit data transfer to only data types that are required).
5. Implement file inspection practices for any file transfer that is required from an IIoT device.
6. Change default username/passwords on IIoT devices as a part of deployment.
7. Use a private carrier (APN) when utilizing a cellular connection to limit exposure to internet facing devices.
8. Wherever available and feasible consider using an existing or established pathway for transferring data (e.g. via a process historian) in lieu of connecting/communicating directly with the process control system.
9. Consider the following options to ensure that operators who have access to IIoT data/tags understand the source of the data:
    - Train operators and develop operating procedures for use of IIoT data
    - Employ of a different tag naming convention/structure or other visual indication near the data to indicate its source
    - Display information on the last time each tag was updated so the operator is aware of stale data
    - Consider also relaying connectivity and/or health status on the IIoT devices when the tag is displayed on the control system (similar to a BadPV)
    - Utilize a dedicated IIoT Display
10. Utilize intrusion detection and prevention monitoring/alerting where possible (e.g. on IIoT edge firewalls)

VI.1.2 IIoT Edge Gateways

1. When connecting to a process control device, utilize protocols that have the potential to limit the impact and scope on the process control system if the IIoT edge gateway or server is compromised (e.g. Modbus TCP vs Ethernet/IP).
2. Implement hardening best practices on the edge gateway including use of host-based firewall features.
3. Consider implementation of secure boot and/or enhanced/advanced edge gateway security measure for high risk systems (e.g. systems that rely on IIoT or use IIoT in the process)
4. Encrypt communications to/from all IIoT devices. Ensure that all applicable security settings are used.
5. Implement best practices for malware prevention including: AV, USB control, patching, and application whitelisting.

VI.1.3 Maintenance Devices (Laptop, tablet, etc.)

1. Consider use of separate maintenance devices and removable media for management for IIoT and PCN devices when the IIoT system is being managed as untrusted to ensure that all PCN device remain secure.
2. If using shared maintenance devices limit physical connections port and protocols to only those that are required to administer the device.

VI.1.4 Cloud Security

1. Implement cloud security best practices including: separation of duties, least privilege access, 2-factor authentication for administrative and configuration access, and periodically running a cloud security tool to validate security settings.
2. Implement patching/updated best practices when utilizing cloud updates and management including: firmware/patch validation, testing on a subset of device prior to widespread deployment, separation of roles and responsibilities to ensure that firmware/patches validation.
3. Consider requiring that end devices support either firmware rollback or affirmative assurance.
4. Where applicable, implement procedures to minimize identifiable information for data stored in the cloud (e.g. company name, place name/locations).
5. Ensure that affirmative prompts are in place to ensure that users are aware of the impact of potential changes to the system.
6. Implement regular backups as a part of the cloud solution; backups are typically an option that must be enabled.
7. Implement anomaly detection as a part of the IIoT environment where possible.
8. Consider penetration testing of all vendor APIs that connect to the cloud.
9. Verify that vendor security policies are included in assessment and contracts.

VI.2 Architecture 1 Recommendations

1. Ensure that control system credentials are unique (different from) adjacent IIoT devices. Enforce this at the local device and/or at the cloud management level.
2. When utilizing a 3rd party cloud for device management (e.g. Digi RM) utilize optional security enhancements including: Separation of duties within device and data management, device configuration monitoring vs gold standard, cell carrier management.
3. Utilize SLA and contractual requirements to ensure the security of the 3rd party cloud environment and non-attribution of the IIoT data.
4. Enable geolocation monitoring of devices to alert if a device is stolen or relocated.

VI.3 Architecture 2 Recommendations

1. Consider use of this architecture only for very low risk processes.
2. Limit access to the process control system through the use of alternative architectures. For example: the use of a DMZ, separation using a process firewall or other means (e.g. data diode).
3. Where possible consider an alternative architecture or IIoT endpoints that would bring in data directly from read-only sensors (shared transmitters at L0) or use of separate sensors rather than directly interfacing with process controllers.

VI.4 Architecture 3 Recommendations

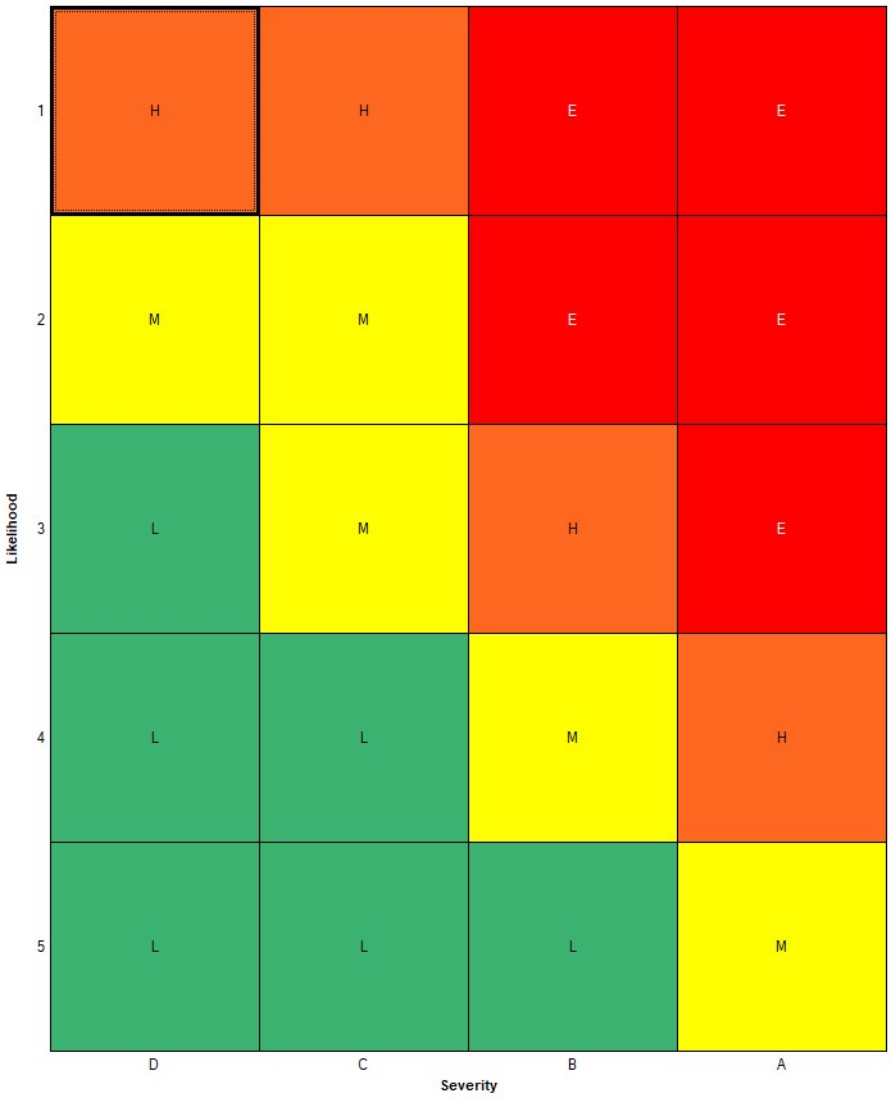
1. Segregate IIoT traffic onto a separate VLAN or network segment. Configure ACLs where required to enforce this.
2. Manage and harden the IIoT gateways and devices to the same standards as other devices below the ICS firewall.

VI.5 Architecture 4 Recommendations

1. Consider the following options to ensure that operators who have access to IIoT data/tags understand the source of the data:
    - Train operators and develop operating procedures for use of IIoT data
    - Employ of a different tag naming convention/structure or other visual indication near the data to indicate its source
    - Display information on the last time each tag was updated so the operator is aware of stale data
    - Consider also relaying connectivity and/or health status on the IIoT devices when the tag is displayed on the control system (similar to a BadPV)
    - Utilize a dedicated IIoT Display

Appendix A. Risk Matrix

This risk matrix was developed specifically for this project using input from LOGIIC members.



Risk Rank	Description
E	Extreme
H	High
M	Medium
L	Low

Table 1: Risk Matrix Severity Scale

Severity Code	Safety	Environmental	Reliability	Confidentiality of Information	End User Impact
A	1+ Fatality	Release with significant damage over a large area	Downtime >1 week	Loss of trade secrets (business critical)	200+ users impacted
B	Permanent disabling injury	Uncontained release with impact to local area	Downtime <1 Week	Loss of confidential information (e.g. Networking/Control information)	50 to 200 users impacted
C	Recordable or lost time injury	Contained Release above RQ	Downtime <1 day	Loss of sensitive information	10 to 50 users impacted
D	First-aid/Minor injury	Minor release below RQ	Downtime <12 hour	Loss of information with negligible impact	< 10 users impacted

Table 2: Risk Matrix Likelihood Scale

Code	Likelihood	Description
1	Frequent	Almost certain to occur
2	Likely	Likely to occur
3	Possible	Possible or not unusual to occur
4	Rare	Conceivable but unlikely to occur
5	Improbable	Reasonably not expected to occur

Appendix B. Risk Profile

Architecture	Zone	Max Unmitigated Risk
Architecture 1	Process IIoT	M
	Process Control Zone	H
	3rd Party Cloud	E
	Process historian zone	L
Architecture 2	Process IIoT	L
	Process Control	E
	IIoT Gateway	E
Architecture 3	Process IIoT	L
	Process Control	H
	IIoT Gateway	H
Architecture 4	Process IIoT	M
	Process Control	H
	IIoT Server	H
Common	Corporate Cloud	E
	IIoT Devices	E

Appendix C. Threat Scenario Summary

Architecture 1:

Zone: Process IIoT

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Equipment Damage	Potential for physical equipment damage to the IIoT equipment resulting in loss of the equipment and loss of the data.	-	-	D	D	Unauthorized Local User		Physical Tampering	3	L
	Theft	Potential for theft of physical equipment resulting in an unauthorized connection to the cloud.	-	-	D	C	Unauthorized Local User	Theft of equipment	Physical Tampering	3	M
	False information	Potential for unauthorized configuration changes including change scaling values resulting in an inaccurate reading.	-	-	D	D	Unauthorized Local User	Note via BT/NFC	Change the Configuration	4	L
							Unauthorized Remote User	Via Cloud configuration manager	Change the Configuration	4	L
	Loss of Col	Potential for redirection of wellhead data to another cloud or destination. Redirect the data from the Digi Device Man in the middle	-	-	-	B	Unauthorized Local User		Change the Configuration	4	M
							Unauthorized Remote User		Man in the middle attack	4	M
Denial of Service	Loss of Data	Potential for denial of service due to jammed signal resulting in loss of data. Potential for impact to a small number of users	-	-	D	D	Unauthorized Local User		Signal Jamming	4	L

Zone: Process Control Zone

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of containment	Potential for theft of the credential from the IIoT device that could be used on the control system if the same credentials/password are shared. Worst case would be manipulation of the control system resulting in loss of containment	D	B	-	B	Unauthorized Local User	Using stolen credentials from IIoT device	Change the Configuration	4	M
Authorized Changes	False information	Potential for use of historian data to feed the control system for optimization purposes. If this data is false/incorrect potential for poor optimization resulting in decreased process efficiency or loss of control.	D	B	C	B	Unauthorized Remote User	Incorrect data fed into Historian	Manipulate Variables	3	H

Zone: 3rd Party Cloud

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Accidental	False information	Potential for misconfiguration of field devices (e.g. firmware, settings, alarming/alerting) from the cloud management interface	-	-	C	C	Authorized Remote User	Accidental	Account misconfiguration	2	M
									Equipment updates	2	M
Tampering - Intentional	Loss of Col	Potential for release of information and data due to breach or misconfiguration of the 3rd party cloud	-	-	-	B	Unauthorized Remote User	Compromise of 3rd party services	Data exfiltration	2	E
	Loss of Col	Potential for redirection to data to an unauthorized 3rd party	-	-	-	B	Unauthorized Remote User	Compromise of 3rd party services	Data exfiltration	2	E

Zone: 3rd Party Cloud

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
	False information	Potential for misconfiguration of field devices (e.g. firmware, settings, alarming/alerting) from the cloud management interface	-	-	C	B	Unauthorized Remote User		Change the Configuration	3	H
Denial of Service	Loss of Data	Potential for downtime of 3rd party cloud services and loss of data	-	-	C	C	Equipment Malfunction		Network or equipment downtime	4	L
							Unauthorized Remote User		Denial Of Service attack	4	L

Zone: Process historian zone

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	False information	Potential for false/incorrect data fed to/from the process historian. Potential for poor optimization resulting in decreased process efficiency.	-	-	C	C	Unauthorized Remote User	Incorrect data fed into Historian	Manipulate Variables	4	L
Denial of Service	Loss of Data	Potential for loss of communication to/from the process historian with minimal impact	-	-	-	-					

Architecture 2:

Zone: Process IIoT

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	False information	Potential for compromise of the gateway or field devices leading to changes in data resulting in an inaccurate reading.	-	-	D	D	Unauthorized Local User	Note via BT/NFC	Change the Configuration	4	L
							Unauthorized Remote User	Via Cloud configuration manager	Change the Configuration	4	L
							Unauthorized Remote User	Known encryption weaknesses	Rogue Device connected	3	L
Denial of Service	Loss of Data	Potential for denial of service due to jammed signal resulting in loss of data.	-	-	D	D	Unauthorized Local User		Signal Jamming	4	L
	Loss of Data	Potential for denial service due to network or communications malfunction leading to loss of data from IIoT devices.	-	-	D	D	Equipment Malfunction		Hardware Failure	2	L

Zone: Process Control

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of containment	Potential for unauthorized remote connection the IIoT edge gateway. Potential to use the IIoT server gateway as a pivot point to other connected systems. Potential for manipulation of SCADA control points.	-	-	-	B	Unauthorized Remote User	Increased UEL due to external facing connection	Change the Configuration	2	E

Zone: IIoT Gateway

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of Col	Potential for data exfiltration or use of the IIoT edge gateway as a reconnaissance tool (e.g. network detection, device information).	-	-	-	B	Unauthorized Remote User	Increased UEL due to external facing connection	Data exfiltration	2	E
Denial of Service	Loss of Data	Potential for loss of the device due to download of invalid firmware.	-	-	C	C	Authorized Local User		Download invalid firmware	3	M
							Authorized Remote User		Download invalid firmware	3	M
	Loss of Data	Potential for loss of the device due to malware/ransomware	-	-	C	C	Generic Malware		Data encryption	1	H
							Targeted Malware		Data encryption	3	M

Architecture 3:

Zone: Process IIoT

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	False information	Potential for compromise of the gateway or field devices leading to changes in data or configuration resulting in an inaccurate reading.	-	-	D	D	Unauthorized Local User	Note via BT/NFC	Change the Configuration	4	L
							Unauthorized Remote User	Via Cloud configuration manager	Change the Configuration	4	L
Denial of Service	Loss of Data	Potential for denial of service due to jammed signal resulting in loss of data.	-	-	D	D	Unauthorized Local User		Signal Jamming	4	L
	Loss of Data	Potential for denial service due to network or firewall malfunction leading to loss of data from all IIoT devices.	-	-	D	D	Equipment Malfunction		Device Failure	2	L

Zone: Process Control

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of containment	Potential for unauthorized remote connection the IIoT edge gateway. Potential to use the IIoT edge gateway as a pivot point to other connected systems. Potential for manipulation of PLC control points leading to tank overfill and LOPC.	-	B	-	B	Unauthorized Remote User	From external connection (through firewall)	Change the Configuration	3	H
							Unauthorized Remote User	From Wireless/IIoT Zone	Change the Configuration	3	H
	Loss of Optimization	Potential for unauthorized remote connection the IIoT edge gateway. Potential to use the IIoT edge gateway as a pivot point to other connected systems. Potential for manipulation of control point used for process optimization	-	-	D	B	Unauthorized Remote User		Change the Configuration	3	H

Zone: IIoT Gateway

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of Col	Potential for data exfiltration or use of the IIoT Server as a reconnaissance tool (e.g. network detection, device information).	-	-	-	B	Unauthorized Remote User		Data exfiltration	3	H
Denial of Service	Loss of Data	Potential for loss of the device due to download of invalid firmware.	-	-	C	C	Authorized Local User		Download invalid firmware	3	M

Zone: IIoT Gateway

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
							Authorized Remote User		Download invalid firmware	3	M
	Loss of Data	Potential for loss of the device due to malware/ransomware	-	-	C	C	Generic Malware		Data encryption	1	H
							Targeted Malware		Data encryption	3	M

Architecture 4:

Zone: Process IIoT

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	False information	Potential for compromise of the gateway or field devices leading to changes in data or configuration resulting in an inaccurate reading.	-	-	D	D	Unauthorized Local User	Note via BT/NFC	Change the Configuration	4	L
							Unauthorized Remote User	Via Cloud configuration manager	Change the Configuration	4	L
							Unauthorized Remote User	Known encryption weaknesses	Rogue Device connected	3	L
	Equipment Damage	Potential for theft of physical equipment resulting in an unauthorized connection to the IIoT Server.	-	-	D	C	Unauthorized Local User	Theft of equipment	Physical Tampering	3	M
	Loss of CoI	Potential for a man in the middle attack leading to exfiltration of data.	-	-	-	C	Unauthorized Local User		Data exfiltration	3	M
Denial of Service	Loss of Data	Potential for denial of service due to jammed signal resulting in loss of data.	-	-	D	D	Unauthorized Local User		Signal Jamming	4	L
	Loss of Data	Potential for denial service due to network or firewall malfunction leading to loss of data from all IIoT devices.	-	-	D	D	Equipment Malfunction		Device Failure	2	L

Zone: Process Control

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of containment	Potential for unauthorized remote connection the IIoT server. Potential to use the IIoT server gateway as a pivot point to other connected systems. Potential for manipulation of DCS control points leading to release and LOPC.	-	B	-	B	Unauthorized Remote User	From external connection (through firewall)	Change the Configuration	3	H
							Unauthorized Remote User	From Wireless/IIoT Zone	Change the Configuration	3	H
	Loss of Optimization	Potential for unauthorized remote connection the IIoT edge gateway. Potential to use the IIoT edge gateway as a pivot point to other connected systems. Potential for manipulation of control point used for process optimization	-	-	D	C	Unauthorized Remote User		Change the Configuration	3	M
	False information	Potential for incorrect or manipulated data presented to the operator resulting in unnecessary or incorrect control actions. Potential for equipment damage and downtime if the operator incorrectly assesses the situation.	-	-	-	B	Unauthorized Local User	From IIoT Devices - Man in the Middle	Data tampering	3	H
							Unauthorized Remote User	From IIoT server	Data tampering	3	H
							Equipment Malfunction		Bad data	3	H

Zone: IIoT Server

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of Col	Potential for data exfiltration or use of the IIoT Server as a reconnaissance tool (e.g. network detection, device information).	-	-	-	B	Unauthorized Remote User		Data exfiltration	3	H
Denial of Service	Loss of Data	Potential for loss of the device due to malware/ransomware.	-	-	C	C	Generic Malware		Data encryption	1	H

Common:

Zone: Corporate Cloud

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Loss of Col	Potential for release of information and data due to breach or misconfiguration of the cloud servers	-	-	-	C	Unauthorized Remote User		Data exfiltration or exposure	3	M
	Loss of Data	Potential for misconfiguration of field devices (e.g. firmware, settings, alarming/alerting) from the cloud management interface	-	-	B	B	Authorized Remote User		Bad Firmware	2	E
							Unauthorized Remote User		Change the Configuration	3	H
	False information	Potential for manipulation of data leading loss of confidence in data and potential de-optimization of processes using IIoT data	-	-	C	C	Unauthorized Remote User		Manipulate Values	4	L
	Unauthorized Access	Potential for the use of a connection to a 3rd party cloud as a pivot point into the wider corporate network	-	-	-	B	Unauthorized Remote User	Typically exploiting an accidental access exposure	Unauthorized access	3	H
	Unauthorized Access	Potential for the use of and IIoT edge device via file transfer capabilities to deliver a malicious file to the corporate network	-	-	-	B	Unauthorized Local User		Send malicious file over network	3	H
	Unauthorized Access	Potential for transfer of malicious files or malware infection when using the same device to manage/support both trusted (PCN) and untrusted (IIoT) networks	-	-	-	B	Targeted Malware		Malicious file transfer	3	H
Denial of Service	Loss of Data	Potential for downtime of corporate cloud services and loss of data	-	-	B	B	Authorized Remote User	Accidental misconfiguration	Change the Configuration	3	H
									Deprovision the Service	3	H
									Download invalid firmware/Patch	3	H
	Regulatory Breach	Potential for regulator breach if IIoT data that is used for regulatory purposes is lost as a part of denial of service.	-	-	-	C	Equipment Malfunction		Device Failure	2	M
							Unauthorized Remote User		Denial Of Service attack	3	M

Zone: IIoT Devices

Threat Class	Consequence	Consequence Description	Severity				Threat Source	Notes	Threat Action	Unmitigated Risk	
			S	Env	EUI	Max				UEL	RRu
Tampering - Intentional	Unauthorized Access	Potential for IIoT devices to be compromised by botnet malware (e.g. mirai) resulting in use of those devices as a part of DDoS attacks or locked by ransomware. Potential for adverse media attention and downtime of the IIoT system until it can be remediated.	-	-	B	B	Generic Malware		Malicious device use	2	E