

UPGRADING SECURITY

Engineer Edition

Secure-by-design SCADA for water and wastewater — with specification language

For consulting engineers preparing bid documents and project manuals, and for utility engineering staff who write or review specifications.

Parts 4 and 5 contain complete specification sections in CSI three-part format, ready to edit into a project manual. Parts 1 to 3 are the engineering rationale behind them — for the conversation where a client or a bidder asks why.

THE SPECIFICATIONS ARE CAPABILITY-BASED

With one deliberate exception, noted where it occurs, these sections describe what the system must do rather than who must supply it. Any product meeting the requirements can compete. Our interest is in the floor being higher, not in the bid being narrower.

Prepared by:



1-844-365-8647

info@d6labs.com

Free to use and adapt in project specifications, with or without attribution.

Supersedes: D6 Labs Recommended Bid Specs (May 2026).

Contents

How to Use This Document.....	1
What is here	1
Use one tier or the other. Never both.	1
Editing the specification sections	1
A note on how restrictive a specification should be.....	2
Part 1 · The Engineering Case	3
What the documented attacks actually exploited.....	3
Why hardening has a ceiling	3
The obsolescence problem, stated as a design constraint.....	4
What a cloud architecture changes	4
Part 2 · Architecture and Design Principles	5
Outbound-only connectivity	5
Why a firewalled listener is not equivalent	5
Transport security	5
Device identity and certificate management	5
Why this replaces password rotation rather than supplementing it.....	6
Signed configuration and program artifacts.....	6
Zones and conduits — mapping to ISA/IEC 62443	6
Local autonomy and failover.....	7
Control continuity	7
Dependent-site failover	7
Field replacement and provisioning	7
Part 3 · Ten Requirements and Why They Matter.....	8
1. Nothing at the utility accepts inbound connections.....	8
2. Encryption enabled by default and not defeatable by configuration.....	8
3. Per-device certificates, revocable by the owner, effective immediately	8
4. No unnecessary local attack surface.....	8
5. Replacement devices self-provision; replacement by owner personnel.....	8
6. Owner can modify screens, alarms, notification and reports without vendor services.....	8

7. Owner owns the data; documented export available at any time at no charge	9
8. Update responsibilities, frequency and cost stated in writing.....	9
9. CAT M1 cellular, multi-carrier, coverage confirmed by the supplier.....	9
10. Local control continues through an outage, including dependent-site failover	9
Part 4 · Base Specification	10
SECTION 40 90 00 — Instrumentation and Control for Process Systems — Basic Requirements.....	10
SECTION 40 96 00 — Cloud SCADA Software.....	12
SECTION 40 94 43 — Automation Controller and Telemetry Gateway	14
SECTION 40 94 53 — Field Input/Output Modules.....	15
SECTION 40 91 23 — Level and Pressure Instrumentation	16
Part 5 · Upgraded Specification	18
SECTION 40 90 00 — Instrumentation and Control for Process Systems — Basic Requirements.....	18
SECTION 40 96 00 — SCADA Software — Cloud and Control Room	20
SECTION 40 94 43 — Automation Controllers.....	22
SECTION 40 96 13 — Development Environment	24
SECTION 40 94 53 — Field Input/Output and Control Network.....	25
SECTION 40 91 23 — Level and Pressure Instrumentation	26
Part 6 · Evaluating Responses	28
Reviewing the security submittal.....	28
Judging a substitution request.....	28
Common non-compliant answers	28
Before recommending award.....	29
Appendix A · Compliance Matrix.....	30
Bidder declaration	30
Appendix B · Suppliers Known to Meet These Requirements.....	31
Appendix C · Mapping to Recognised Standards.....	32
ISA/IEC 62443	32
NIST Cybersecurity Framework 2.0	32
AWIA Section 2013.....	32
Appendix D · Acceptance Test Record	33
Appendix E · Glossary.....	34
About This Document.....	35
Disclaimer	35

How to Use This Document

What is here

Part	Content	Who reads it
1	The engineering case — why hardening a conventional architecture has a ceiling	You, and the client who asks why
2	Architecture and design principles in technical depth	You, and the bidder who objects
3	Ten requirements and the failure mode if each is omitted	You, when editing the specs
4	BASE SPECIFICATION — pump stations, towers, leak detection, master meters, simple lift stations	Copied into the project manual
5	UPGRADED SPECIFICATION — water plants and multi-controller sites	Copied into the project manual
6	Evaluating responses and substitution requests	You, at bid review
A–F	Compliance matrix, suppliers, standards mapping, acceptance tests, glossary, change record	Reference

Use one tier or the other. Never both.

COPY THE WHOLE TIER

Part 4 and Part 5 are complete and independent. They repeat material on purpose. Choose the tier that fits the project and copy all of its sections — do not assemble a project manual by taking some sections from one and some from the other. The tiers make different assumptions about controller capability, network topology and I/O density, and mixing them produces a specification no supplier can cleanly meet.

Use Part 4 — Base	Use Part 5 — Upgraded
Pump stations, lift stations, wells	Water and wastewater treatment plants
Elevated and ground storage tanks	Sites with multiple automation controllers
Leak detection and pressure monitoring	Sites needing a control-room SCADA computer
Master meters	More than 192 I/O at a single controller
Single controller per site	Controller-to-controller communication required

Editing the specification sections

- **Section numbers are suggestions.** They follow MasterFormat Division 40 (Process Interconnections). Renumber to match your office standard — the content matters, the numbering does not.

- **SPECIFIER NOTES are not specification text.** The shaded boxes explain the intent behind a requirement so you can defend it. Delete them before issuing for bid.
- **Bracketed text requires a project decision.** Anything in [square brackets] is a choice you must make or a value you must fill in.
- **Every requirement is written to be verifiable,** either at submittal or at commissioning. Part 3 of each section says how.

A note on how restrictive a specification should be

It is worth being explicit about where this language sits, because water sector SCADA specs vary enormously in how much competition they actually permit.

At one end are specifications that name two products and add “no exceptions” — where one of the named products costs two or three times the other. That is a sole-source specification wearing competitive clothing: the outcome is decided before bids open, and everyone involved knows it.

At the other end are specifications so generic that a compliant bid can be assembled from equipment that does none of the things the owner actually needed. Those are worse, because the owner finds out after commissioning.

These sections aim between the two. Requirements are stated as capabilities and are testable. Where a requirement is unusual — and a few are — it is severable: deleting it leaves a specification that still functions. Nothing here is written so that only one supplier can respond, and nothing here says “no exceptions.”

If you strike a clause, strike it deliberately. The Part 3 requirements in particular are the ones most often deleted for brevity, and they are the ones that determine whether the security requirements are real or decorative.

Part 1 · The Engineering Case

Compressed. You already understand control systems; this is the part of the argument that bears on specification decisions.

What the documented attacks actually exploited

Across the publicly reported incidents — Oldsmar in 2021, Aliquippa in 2023, the coordinated attacks on more than thirty Minnesota systems in July 2026 — no attacker defeated a sophisticated protection. The exploited conditions were:

- Controllers reachable from public address space, discovered by scanning and then accessed using the manufacturer's own engineering software over the vendor's own protocol
- Factory-default credentials, or credentials shared across a crew, or credentials belonging to departed staff
- Consumer remote-access software with a single shared login and no second factor
- No segmentation between business and control networks
- Cellular-connected controllers with no gateway or firewall in front of them

Every item on that list is a property of the architecture rather than a lapse by the operator. Specifying a stronger password policy does not remove any of them.

Why hardening has a ceiling

A conventional architecture can be hardened a long way. What hardening cannot change:

Property	Consequence
Something must listen for inbound connections, or remote access is impossible	The listener is discoverable and attackable. A firewall in front of it is a rule that can be misconfigured, and something is still answering behind it.
Credentials are shared secrets	They can be read aloud, written in a panel, reused across sites, and inherited. Rotation is a process that depends on people, indefinitely.
Supervisory function depends on a general-purpose operating system	Lifecycle is set by the OS vendor, not by the utility. Windows 10 support ended in October 2025; ESU escalates and ends in October 2028; current SCADA versions increasingly require hardware that existing machines do not have.
Site-to-site telemetry is a broadcast	Unless every link is encrypted and stays encrypted, traffic can be received and injected from outside the fence, with no alarm and no log entry.
Equipment is no longer supported by its manufacturer	No further firmware. A documented vulnerability in that firmware is permanent, and no compensating control changes the device's own risk profile.

The obsolescence problem, stated as a design constraint

This is the one that most often forces the project, and it is worth stating in engineering terms rather than commercial ones.

A device that cannot accept a signed firmware update cannot be remediated. Network segmentation, access control and monitoring reduce the probability that the vulnerability is reached; they do not reduce its severity if it is. For a device whose manufacturer has exited the product line, the residual risk is fixed for the remaining life of the asset, and the only variables left are how long that life is and what depends on it.

Where a client is running discontinued controllers, spares sourced from used inventory, and engineering software that will not install on a supported operating system, the honest engineering position is that no specification for hardening will resolve it. The asset needs replacing, and the question is what to replace it with.

What a cloud architecture changes

Not the control. Control logic executes in the controller, at the site, continuously, and does not depend on the wide-area link. What changes is the supervisory layer and, more importantly, four properties of the system:

- **Connection initiation reverses.** Site equipment connects outward and nothing at the utility listens. There is no discoverable attack surface at the site, and no firewall rule protecting a listener.
- **Credentials become certificates.** Per-device, non-transferable, individually revocable. Rotation stops being a recurring human process.
- **The supervisory OS lifecycle stops being the owner's problem.** There is no on-premises SCADA computer whose end of support forces a project.
- **Firmware and program delivery becomes routine.** Signed artifacts delivered over an authenticated channel, which is what makes remote update safe rather than reckless.

Part 2 · Architecture and Design Principles

The technical basis for the requirements in Parts 4 and 5. This is the material you need when a bidder objects or a client asks you to justify a clause.

Outbound-only connectivity

The site device establishes and maintains an outbound session to the platform. Telemetry, commands, configuration and firmware all travel inside that session. No inbound connection is accepted at the site, for any purpose, including support.

Why a firewalled listener is not equivalent

The common objection is that a listening service behind a firewall achieves the same result. It does not, for three reasons an engineer will recognise:

- The service is still reachable from any source the rule permits, and rules accumulate exceptions over a system's life. The failure mode is a misconfiguration, and misconfigurations are the most common root cause in this sector.
- The listener is discoverable. Internet-wide scanning identifies responding services in hours, and the scanning is continuous and automated.
- It concentrates security in a device the utility must configure and maintain correctly, which is precisely the resource small utilities do not have.

With no listener there is no rule to get wrong. This is the single largest structural difference between the two architectures and it is why requirement 1 in Part 3 is written as an absolute.

Transport security

Data in transit is protected with TLS. Where the design adds payload-level encryption beneath the transport, an intercepted session yields nothing usable even if the transport layer is later found deficient — which matters for equipment expected to remain in service for fifteen years, over which time transport-layer assumptions will change at least once.

The specification requires encryption enabled by default and not defeatable by configuration. That wording is deliberate: a great many radios in service today support encryption and shipped with it disabled, and a requirement that encryption be “supported” is met by such a product.

Device identity and certificate management

Each device holds a unique certificate issued at deployment. Mutual authentication means the device proves its identity to the platform and the platform proves its identity to the device, which is what prevents a substituted endpoint from collecting data or issuing commands.

Why this replaces password rotation rather than supplementing it

Shared secret	Per-device certificate
Can be communicated verbally or in writing	Cannot usefully be transcribed
Commonly reused across a fleet	Unique per device by construction
Departing personnel retain knowledge of it	Knowledge is not the credential
Changing it requires touching everything that used it	Revocation is a platform action, effective immediately
Scope of a compromise is usually unknown	Scope is exactly one device, and is known

The specification requires that revocation be available to the owner, not only to the supplier. A certificate scheme in which revocation requires a vendor ticket during business hours provides materially less protection than the mechanism implies, and it is worth checking at submittal.

Signed configuration and program artifacts

Authenticating the connection answers who is talking. It does not answer what is being run. The requirement that configuration and program artifacts be signed by the controller's own credential, and validated before execution, is what prevents an authenticated but unauthorised change from taking effect.

This is the requirement most often absent from competing specifications, and it is the one that would have prevented the logic modification seen in several documented incidents. Password protection on the programming port does not achieve it — which is why the clause states that explicitly rather than leaving it to interpretation.

Zones and conduits — mapping to ISA/IEC 62443

Where a client references ISA/IEC 62443, the architecture maps cleanly and it is worth being able to say so:

62443 concept	How it is satisfied
Zone	Each site is a zone. A plant control network is a zone. The supervisory platform is a separate zone.
Conduit	The authenticated outbound session between site and platform. Within a plant, the certificate-authenticated controller network.
Security level	Requirements here correspond broadly to SL 2 for the site zone, with the certificate and signed-artifact requirements reaching toward SL 3 for the conduit.
Least privilege	Role-based permissions with per-action authorisation, specified in the SCADA sections.
Audit	Change logging with user, object, previous and new value, and timestamp, exportable.

SPECIFIER NOTE — delete before issuing for bid

If your client has not referenced 62443, do not introduce it. It invites a scope discussion that this specification does not need. The mapping is here so you can answer the question if it is asked.

Local autonomy and failover

Two distinct requirements that are frequently conflated.

Control continuity

The controller executes its logic independently of the wide-area link. On loss of communication it continues to operate, buffers historical data locally, and forwards the buffer on reconnection so the historical record has no gap. What is lost during the outage is supervisory visibility and remote command — and the specification requires the supplier to state that plainly rather than imply there is no consequence.

Dependent-site failover

The requirement most often missing, and the one with the clearest public-health consequence. Where a site's normal control strategy consumes data from another site — a pump station starting and stopping on tower level being the common case — the loss of that data must produce a defined behaviour rather than an undefined one.

The specification requires a configured failover control mode for every such dependency. In the pump station example, the accepted approach is reversion to discharge pressure control: the station starts and stops to maintain system pressure rather than tank level. Tank level may then drift outside its normal band, and if the pressure setpoints are wrong the tank can overflow — but distribution stays pressurised, which is the outcome that matters.

SPECIFIER NOTE — delete before issuing for bid

Identify each inter-site data dependency during design and specify the failover strategy for each one. A blanket requirement will be answered with a blanket assurance. Listing the dependencies in the schedule forces a specific response per site.

Field replacement and provisioning

Self-provisioning replacement is normally presented as a convenience. It is also a security property, and worth understanding as one.

Where a replacement device retrieves its configuration and program from the platform after authenticating, the utility is no longer dependent on a locally held copy of each site's program — copies that in practice are frequently out of date, stored on an individual's laptop, or absent. It also removes the need for a technician to carry programming access to site, which is itself an exposure.

The security precondition is the same one that makes remote update safe: the device must authenticate before it receives anything, and what it receives must be signed. A self-provisioning device without those two properties is a liability rather than a feature, which is why the specification requires them together.

Part 3 · Ten Requirements and Why They Matter

Each requirement, the failure mode if it is omitted, and the objection you should expect from a bidder who cannot meet it.

1. Nothing at the utility accepts inbound connections

If omitted: Site equipment is discoverable by internet-wide scanning and reachable by anyone who finds it. This is the first step in the majority of documented water sector intrusions.

Expect to hear: "It is behind a firewall." Answer: a firewall is a rule that can be misconfigured, and a listener remains behind it. The requirement is that nothing listens, not that access is filtered.

2. Encryption enabled by default and not defeatable by configuration

If omitted: Telemetry can be received and injected from outside the site boundary, with no alarm and no log entry. Optional encryption is eventually disabled somewhere.

Expect to hear: "Encryption is supported and can be enabled at commissioning." Answer: supported is not the requirement. A product that can be configured into clear text does not comply.

3. Per-device certificates, revocable by the owner, effective immediately

If omitted: Credentials are shared secrets — reused, transcribed, and retained by departed personnel. The scope of any compromise is unknown.

Expect to hear: "Each device has a unique strong password rotated on a schedule." Answer: rotation is a recurring human process and the scope of a leak remains unknown. Certificates make revocation an action rather than a project.

4. No unnecessary local attack surface

If omitted: Physical access to a remote site yields control of the device. A fence and padlock is the only control, and it is adequate against casual trespass only.

Expect to hear: "The panel is locked." Answer: the requirement addresses what an attacker can do once inside the panel, which is the case the lock has already failed to prevent.

5. Replacement devices self-provision; replacement by owner personnel

If omitted: Every failure requires a technician with programming access and a current copy of the site's program. In practice that copy is frequently missing or stale.

Expect to hear: "We stock a configured spare for each site and respond next business day." Answer: that is a service level, not a system property, and it does not address the stale-program problem.

6. Owner can modify screens, alarms, notification and reports without vendor services

If omitted: Changes cost money and require scheduling, so they are not made. Alarms that cannot be tuned are disabled; displays drift out of correspondence with the plant.

Expect to hear: "Changes are handled promptly under our support agreement." Answer: the requirement is that the owner can make them, not that the supplier will.

7. Owner owns the data; documented export available at any time at no charge

If omitted: The owner cannot leave, cannot audit independently, and cannot recover their own history if the relationship ends.

Expect to hear: "Of course you own your data," with no corresponding contract language. Answer: request the clause. This is a commercial requirement, and it belongs in the agreement.

8. Update responsibilities, frequency and cost stated in writing

If omitted: Ambiguity here is how systems end years behind. The owner discovers the position when a vulnerability is published or a component fails.

Expect to hear: "Updates are included in ongoing support." Answer: state who updates what, how often, with what notice, and at what cost.

9. CAT M1 cellular, multi-carrier, coverage confirmed by the supplier

If omitted: Single-carrier equipment fails where that carrier is weak. Consumer-grade cellular technology has materially worse link budget. Coverage assumptions based on handsets are unreliable and the owner has no means to verify them.

Expect to hear: "Check whether a phone has signal at the site." Answer: a handset uses different radio technology on one carrier. Coverage verification against published band data is the supplier's obligation.

10. Local control continues through an outage, including dependent-site failover

If omitted: A communications failure becomes a process failure. Where a site depends on data from another site, undefined behaviour on loss of that data is the case with the clearest public-health consequence.

Expect to hear: "Our uptime is excellent." Answer: availability is not the question. The question is the defined behaviour when the link is down, per site, including dependencies.

Part 4 • Base Specification

SCOPE OF THIS TIER

Pump stations, lift stations, wells, elevated and ground storage tanks, leak detection, pressure monitoring and master meters — sites served by a single automation controller with fewer than 192 field I/O points and no requirement for a control-room computer. For treatment plants and multi-controller sites, use Part 5 instead. Do not combine the two.

SPECIFIER NOTE — delete before issuing for bid

Section numbers follow MasterFormat Division 40. Renumber to suit your office standard. Delete all SPECIFIER NOTE boxes before issuing for bid.

SECTION 40 90 00 — Instrumentation and Control for Process Systems — Basic Requirements

PART 1 — GENERAL

1.01 SUMMARY

- A. This Section specifies basic requirements applicable to all instrumentation and control work under this Contract, including the supervisory platform, telemetry, automation controllers, field input/output and field instrumentation.
- B. Related Sections:
 - 1. Section 40 94 43 — Automation Controller and Telemetry Gateway
 - 2. Section 40 94 53 — Field Input/Output Modules
 - 3. Section 40 91 23 — Level and Pressure Instrumentation
 - 4. Section 40 96 00 — Cloud SCADA Software

1.02 SYSTEM DESCRIPTION

- A. The control system shall consist of automation controllers located at each site, communicating over secure cellular telemetry to a cloud-hosted supervisory platform. Radio telemetry shall not be used.
- B. Control logic shall execute in the automation controller at each site and shall continue to execute during loss of communication with the supervisory platform.
- C. No equipment provided under this Contract shall accept inbound network connections from outside the site, for any purpose, including vendor support.

SPECIFIER NOTE — delete before issuing for bid

Clause C is the single most important requirement in this Section. A bidder proposing a firewalled listening service does not comply. See Part 2 of this guide for the reasoning if challenged.

1.03 SUBMITTALS

- A. Product data for each component, including published specifications for cellular technology, supported carriers, ingress protection rating and operating temperature range.
- B. A written statement of the security architecture, addressing:
 - 1. Direction of connection initiation for every communication path.
 - 2. Encryption in transit, including protocol and whether it can be disabled.
 - 3. Credential type, issuance, and the revocation mechanism and who may invoke it.
 - 4. Whether configuration and program artifacts are signed and validated before execution.
 - 5. All locally accessible interfaces and the authentication required for each.
- C. Cellular coverage assessment for each site, prepared by the Supplier from published carrier band and coverage data, identifying the carriers available and the expected signal condition at each location. The Owner shall not be required to perform this assessment.
- D. A completed Compliance Matrix in the form appended to these Specifications.
- E. Failover schedule identifying, for each site whose normal control strategy depends on data originating at another site, the control mode that will be adopted on loss of that data.

SPECIFIER NOTE — delete before issuing for bid

Submittal E is the one most likely to be returned incomplete. Listing each dependency in the project schedule, rather than asking for a general statement, forces a per-site answer.

1.04 QUALITY ASSURANCE

- A. The supervisory platform shall be hosted in a data centre operated by a tier-one cloud provider holding current SOC 2 Type II or ISO/IEC 27001 certification. Microsoft Azure satisfies this requirement.

SPECIFIER NOTE — delete before issuing for bid

Broadened from naming a single provider so the clause survives a procurement challenge, while still excluding a platform hosted on a server in an office. Certification evidence is a reasonable submittal request if the Owner is security-conscious.

- B. Certification evidence shall be provided on request.

PART 2 — PRODUCTS

2.01 GENERAL

- A. All equipment shall be of current manufacture and supported by the manufacturer with security and functional firmware updates for a minimum of [seven] years from Substantial Completion.
- B. Equipment that the manufacturer has designated end-of-life, end-of-sale or end-of-support shall not be provided.

SPECIFIER NOTE — delete before issuing for bid

Clause A is worth keeping. Much of the equipment being replaced on projects like this is discontinued hardware that can no longer receive firmware fixes; a support-horizon requirement prevents repeating that.

PART 3 — EXECUTION

3.01 PROVISIONING

- A. The Supplier shall provision all devices to the Owner's account. Device credentials shall be issued to the Owner's account and shall remain under the Owner's control.

3.02 DEMONSTRATION AND ACCEPTANCE TESTING

- A. The following shall be demonstrated to the Owner and Engineer before Substantial Completion. Each demonstration shall be witnessed and recorded.
 - 1. Loss of communications: interrupt the wide-area link at one site and demonstrate that control continues, that data is buffered locally, and that the buffer is forwarded with no gap in the historical record on restoration.
 - 2. Dependent-site failover: at one site whose control depends on data from another, interrupt that data and demonstrate adoption of the specified failover control mode.
 - 3. Field replacement: an Owner staff member, not a Supplier representative, shall replace one automation controller with a spare unit that has not been pre-configured for that site, and place it in service. Record elapsed time.
 - 4. Credential revocation: revoke one device credential from the Owner's account and demonstrate that the device is denied access. Reinstate afterwards.
 - 5. Owner self-service: an Owner staff member shall create one operator display element, one alarm with notification, and one report, without Supplier assistance.
 - 6. Notification: demonstrate alarm delivery to each configured notification path.

SPECIFIER NOTE — delete before issuing for bid

Article 3.02 is what converts the Part 2 requirements from claims into acceptance criteria, and it is the article most often deleted for brevity. Deleting it means the security requirements are never verified. Item 3 in particular tends to reveal whether self-provisioning is real.

3.03 TRAINING

- A. Provide [8] hours of training for Owner personnel covering operator display editing, alarm and notification configuration, report and trend creation, device replacement, and user and permission administration.

3.04 CLOSEOUT SUBMITTALS

- A. As-built configuration documentation, network diagram, device inventory with identifiers, and the failover schedule as implemented.
- B. Written confirmation of the export procedure by which the Owner may retrieve all historical and configuration data.

SECTION 40 96 00 — Cloud SCADA Software

PART 1 — GENERAL

1.01 SUMMARY

- A. This Section specifies the cloud-hosted supervisory control and data acquisition platform.

PART 2 – PRODUCTS

2.01 PLATFORM

- A. The SCADA software shall be cloud based and shall be hosted as specified in Section 40 90 00, Article 1.04.
- B. The SCADA software shall communicate with field devices using the MQTT protocol with TLS encryption.
- C. The SCADA software shall provide an HTML5 browser-based application and native Android and iOS applications. Access shall be available from any laptop, tablet or smartphone, from any location with internet access, at any time.

2.02 SECURITY AND ACCESS CONTROL

- A. The SCADA software shall provide granular role-based permissions, with each action requiring a specified role. Users may be assigned multiple roles.
- B. The SCADA software shall log each change made by a user, including username, the object changed, previous and new values, and date and time. A user interface shall be provided for viewing, filtering and exporting these logs.
- C. The SCADA software shall support two-factor authentication, configurable per user or enforced for all users on an account.
- D. Device credentials shall be unique per device and revocable individually by the Owner, with revocation effective immediately.

2.03 OPERATOR CONFIGURABILITY

- A. The SCADA software shall allow the Owner to create new operator displays and modify existing displays. The display designer shall be WYSIWYG with a drag-and-drop interface.
- B. The SCADA software shall support unlimited user-defined alerts and shall notify designated recipients by SMS text message and email.
- C. The SCADA software shall provide voice callout as an option for alerts and alarms.
- D. The SCADA software shall support user-defined dashboards for historical trend analysis.
- E. All features of the SCADA software shall be editable and maintainable by the Owner without requiring vendor or engineering services.

SPECIFIER NOTE — delete before issuing for bid

Clause E is the operator self-service requirement, stated so that it is testable. It is verified by Article 3.02 item 5 of Section 40 90 00.

PART 3 – EXECUTION

3.01 CONFIGURATION

- A. Configure user accounts, roles and permissions as directed by the Owner. Configure operator displays, alarms and notification routing for all facilities in this Contract.

3.02 DEMONSTRATION

A. Demonstrations relating to this Section are specified in Section 40 90 00, Article 3.02.

SECTION 40 94 43 — Automation Controller and Telemetry Gateway

PART 1 — GENERAL

1.01 SUMMARY

- A. This Section specifies secure cellular telemetry gateways and automation controllers. Automation controllers shall be provided in lieu of programmable logic controllers. Automation controllers shall include all gateway functionality specified in Article 2.01.

PART 2 — PRODUCTS

2.01 SECURE CELLULAR TELEMETRY GATEWAY

- A. Secure CAT M1 4G cellular gateways shall be provided in lieu of radio telemetry.

SPECIFIER NOTE — delete before issuing for bid

CAT M1 is a 4G technology intended for equipment rather than handsets. It offers materially better link budget than consumer cellular, lower hardware and data cost, and avoids the stranded-asset exposure created by the retirement of 3G networks.

- B. The gateway shall use AES-256 encryption for all data, with unique, revocable encryption credentials per device.
- C. The gateway shall automatically switch between AT&T, T-Mobile and Verizon networks using a single SIM.

SPECIFIER NOTE — delete before issuing for bid

Multi-carrier switching is what makes a site connected if any one carrier reaches it. Single-carrier equipment fails wherever that carrier is weak.

- D. The gateway shall support expansion using IP67-rated field input/output over Modbus RTU (RS-485) via a standard M8-4 or M12-5 connector.
- E. Solar-powered gateways shall provide a minimum of seven days autonomy. Line-powered gateways shall provide a minimum of 24 hours of battery-backed operation on loss of supply.
- F. The gateway shall be housed in an IP67-rated enclosure.

SPECIFIER NOTE — delete before issuing for bid

IP67 housing removes the need for a separate field enclosure, which is a meaningful cost and installation saving at remote sites.

- G. The gateway shall automatically retrieve its configuration and program from the supervisory platform on startup.
- H. Replacement of a gateway shall be performable by Owner personnel, using a spare unit that has not been pre-configured for the site, without attendance by the Supplier or an engineer.

SPECIFIER NOTE — delete before issuing for bid

Clause H promotes the field-replacement outcome into a testable requirement rather than leaving it as a benefit of clause G. Verified by Article 3.02 item 3 of Section 40 90 00.

- I. The gateway shall be programmable in Python.

SPECIFIER NOTE — delete before issuing for bid

Python programmability provides for protocol conversion, local automation and future requirements not identified at design.

2.02 AUTOMATION CONTROLLER

- A. Automation controllers shall meet all requirements of Article 2.01 and the additional requirements of this Article.
- B. The automation controller shall include a sunlight-readable LCD of not less than 2.7 inches with push buttons, or a waterproof capacitive touch screen, for local user interaction.
- C. The automation controller shall be programmable in Python.
- D. The automation controller shall automatically retrieve its configuration and program from the supervisory platform on startup, and shall be replaceable by Owner personnel in accordance with Article 2.01, clause H.
- E. The automation controller shall have a dual-core processor of not less than 150 MHz and not less than 520 KB SRAM.
- F. The automation controller shall include internal SD card storage of not less than 8 GB.
- G. The automation controller shall be housed in an IP67-rated enclosure.
- H. The automation controller shall operate from an 8–30 VDC supply.

PART 3 — EXECUTION

3.01 INSTALLATION

- A. Install in accordance with the manufacturer's instructions. Mount antennas to achieve the signal condition identified in the coverage assessment submitted under Section 40 90 00.

SPECIFIER NOTE — delete before issuing for bid

Cellular antennas are normally compact and mounted at or near grade, since the link does not require line of sight to another site. This avoids the elevated strike target and the long feedline associated with radio telemetry — a meaningful reduction in lightning exposure in this region.

3.02 DEMONSTRATION

- A. Demonstrations relating to this Section are specified in Section 40 90 00, Article 3.02.

SECTION 40 94 53 — Field Input/Output Modules

PART 1 — GENERAL

1.01 SUMMARY

- A. This Section specifies modular field input/output for systems with fewer than 192 digital and analog points per automation controller.

PART 2 – PRODUCTS

2.01 FIELD INPUT/OUTPUT SYSTEM

- A. The field I/O system shall be modular and expandable. Each module shall provide not less than two 4–20 mA analog inputs, six digital inputs, one digital output and one analog output.

SPECIFIER NOTE — delete before issuing for bid

The intent is that a single I/O module provides sufficient points to monitor and control one pump or motor. Size the system on that basis.

- B. The field I/O system shall support up to 16 modules, for a total of up to 192 analog and digital points.
- C. Field I/O modules shall provide pluggable headers for field connections and shall be hot-swappable, replaceable without removing system power.
- D. Field I/O modules shall communicate via Modbus RTU (RS-485).
- E. Field I/O modules shall operate from an 8–30 VDC supply.
- F. Field I/O modules shall provide LED indication for digital and analog points. For digital points the indicator shall be lit when the point is active. For analog inputs the indicator shall be lit when the input is within range. For analog outputs the indicator shall be lit when the output is non-zero and within range.
- G. Field I/O modules shall connect via a five-pin TBUS connector mounted on the DIN rail. The connector shall provide a five-pin 3.8 mm pluggable female header on the left side and a five-pin 3.8 mm pluggable male header on the right to permit stacking. Power and RS-485 signals shall pass through the connector to each attached module.

PART 3 – EXECUTION

3.01 DEMONSTRATION

- A. Demonstrate hot-swap replacement of one field I/O module without removing system power, and confirm that the replaced module returns to service without reconfiguration.

SECTION 40 91 23 — Level and Pressure Instrumentation

PART 1 – GENERAL

1.01 SUMMARY

- A. This Section specifies radar level transmitters and leak detection sensor assemblies.

PART 2 – PRODUCTS

2.01 RADAR LEVEL TRANSMITTERS

- A. Level transmitters shall be 60 GHz pulsed coherent radar with Modbus RTU or two-wire 4–20 mA output.
- B. Level transmitters shall operate from an 8–30 VDC supply.
- C. Level transmitters shall consume not more than 300 mW at maximum measurement range.
- D. Level transmitters shall be capable of measuring fluid level through the wall of a plastic storage tank without an opening in the tank, and shall have a maximum measurement range of not less than 30 feet.

2.02 LEAK DETECTION SENSOR ASSEMBLIES

- A. Each leak detection sensor assembly shall comprise:
 - 1. A telemetry gateway complying with Section 40 94 43, Article 2.01, capable of reading pressure and reporting to the supervisory platform at intervals of one minute over a secure cellular connection.
 - 2. A 12 VDC solar power supply providing not less than seven days of autonomous operation without insolation.
 - 3. A 200 psi pressure transducer with an M12 A-coded connector to permit replacement without rewiring.

PART 3 – EXECUTION

3.01 CALIBRATION AND VERIFICATION

- A. Verify each level transmitter against a physical measurement at two points across the operating range and record the results.

Part 5 · Upgraded Specification

SCOPE OF THIS TIER

Water and wastewater treatment plants, and any site requiring multiple automation controllers, controller-to-controller communication, more than 192 field I/O at a single controller, or a control-room computer with access to all tags in all controllers. For simple remote sites, use Part 4 instead. Do not combine the two.

SPECIFIER NOTE — delete before issuing for bid

This tier repeats material from Part 4 on purpose, so that it can be copied whole. Do not cross-reference back to Part 4 in a project manual — use one tier or the other in its entirety.

SECTION 40 90 00 — Instrumentation and Control for Process Systems — Basic Requirements

PART 1 — GENERAL

1.01 SUMMARY

- A. This Section specifies basic requirements applicable to all instrumentation and control work under this Contract, including the supervisory platform, telemetry, automation controllers, control network, field input/output and field instrumentation.
- B. Related Sections:
 - 1. Section 40 94 43 — Automation Controllers
 - 2. Section 40 94 53 — Field Input/Output and Control Network
 - 3. Section 40 91 23 — Level and Pressure Instrumentation
 - 4. Section 40 96 00 — SCADA Software
 - 5. Section 40 96 13 — Development Environment

1.02 SYSTEM DESCRIPTION

- A. The control system shall consist of automation controllers, field input/output and operator interfaces on a plant control network, communicating over secure cellular telemetry to a cloud-hosted supervisory platform, with a control-room application providing local access to all tags in all controllers.
- B. Control logic shall execute in the automation controllers and shall continue to execute during loss of communication with the supervisory platform.
- C. No equipment provided under this Contract shall accept inbound network connections originating outside the plant control network, for any purpose, including vendor support.

- D. Communication between automation controllers, and between automation controllers and operator workstations, shall be mutually authenticated and encrypted.

1.03 SUBMITTALS

- A. Product data for each component, including published specifications for processor, memory, storage, display, network interfaces, cellular technology, supported carriers and ingress protection rating.
- B. A written statement of the security architecture, addressing:
 - 1. Direction of connection initiation for every communication path, including controller-to-controller and controller-to-workstation.
 - 2. Encryption in transit for each path, including protocol and whether it can be disabled.
 - 3. Credential type, issuance, and the revocation mechanism and who may invoke it.
 - 4. Whether configuration and program artifacts are signed, and how signatures are validated before execution.
 - 5. All locally accessible interfaces and the authentication required for each.
- C. Cellular coverage assessment for each remotely communicating site, prepared by the Supplier from published carrier band and coverage data. The Owner shall not be required to perform this assessment.
- D. Control network topology drawing showing redundancy and the recovery behaviour on single link failure.
- E. A completed Compliance Matrix in the form appended to these Specifications.
- F. Failover schedule identifying, for each site or process area whose normal control strategy depends on data originating elsewhere, the control mode adopted on loss of that data.

1.04 QUALITY ASSURANCE

- A. The cloud supervisory platform shall be hosted in a data centre operated by a tier-one cloud provider holding current SOC 2 Type II or ISO/IEC 27001 certification. Microsoft Azure satisfies this requirement.
- B. Certification evidence shall be provided on request.

PART 2 – PRODUCTS

2.01 GENERAL

- A. All equipment shall be of current manufacture and supported by the manufacturer with security and functional firmware updates for a minimum of [seven] years from Substantial Completion.
- B. Equipment that the manufacturer has designated end-of-life, end-of-sale or end-of-support shall not be provided.

PART 3 – EXECUTION

3.01 PROVISIONING

- A. The Supplier shall provision all devices to the Owner's account. Device credentials shall be issued to the Owner's account and shall remain under the Owner's control.

3.02 DEMONSTRATION AND ACCEPTANCE TESTING

- A. The following shall be demonstrated to the Owner and Engineer before Substantial Completion. Each demonstration shall be witnessed and recorded.
1. Loss of wide-area communications: interrupt the cellular link and demonstrate that plant control continues, that data is buffered locally, and that the buffer is forwarded with no gap in the historical record on restoration.
 2. Control network single link failure: interrupt one link in the control network ring and demonstrate that all controllers, workstations and field I/O remain in communication. Record recovery time.
 3. Dependent-site failover: interrupt data from a remote site on which a local control strategy depends, and demonstrate adoption of the specified failover control mode.
 4. Field replacement: an Owner staff member, not a Supplier representative, shall replace one automation controller with a spare unit that has not been pre-configured for that position, and place it in service. Record elapsed time.
 5. Credential revocation: revoke one device credential from the Owner's account and demonstrate that the device is denied access to the control network and the platform. Reinstate afterwards.
 6. Unauthorised program rejection: attempt to load an unsigned or improperly signed program to one automation controller and demonstrate that it is rejected before execution.
 7. Owner self-service: an Owner staff member shall create one operator display element, one alarm with notification, and one report, without Supplier assistance.
 8. Notification: demonstrate alarm delivery to each configured notification path.

SPECIFIER NOTE — delete before issuing for bid

Item 6 has no equivalent in the base tier and is the highest-value test in this Section. It is the only demonstration that verifies the signed-artifact requirement, and a supplier who cannot perform it does not meet Article 2.02 of Section 40 94 43 regardless of what the submittal claimed.

3.03 TRAINING

- A. Provide [24] hours of training for Owner personnel covering operator display editing, alarm and notification configuration, report and trend creation, device replacement, user and permission administration, and use of the development environment.

3.04 CLOSEOUT SUBMITTALS

- A. As-built configuration and program documentation, control network topology drawing, device inventory with identifiers, and the failover schedule as implemented.
- B. Written confirmation of the export procedure by which the Owner may retrieve all historical and configuration data.
- C. All source programs, HMI designs and configuration in editable form, together with the licences required for the Owner to modify them.

SECTION 40 96 00 — SCADA Software — Cloud and Control Room

PART 1 – GENERAL

1.01 SUMMARY

- A. This Section specifies the cloud-hosted supervisory platform and the control-room SCADA application.

PART 2 – PRODUCTS

2.01 CLOUD PLATFORM

- A. The primary SCADA software shall be cloud based and shall be hosted as specified in Section 40 90 00, Article 1.04.
- B. The SCADA software shall communicate with field devices using the MQTT protocol with TLS encryption.
- C. The SCADA software shall provide an HTML5 browser-based application and native Android and iOS applications. Access shall be available from any laptop, tablet or smartphone, from any location with internet access, at any time.

2.02 SECURITY AND ACCESS CONTROL

- A. The SCADA software shall provide granular role-based permissions, with each action requiring a specified role. Users may be assigned multiple roles.
- B. The SCADA software shall log each change made by a user, including username, the object changed, previous and new values, and date and time. A user interface shall be provided for viewing, filtering and exporting these logs.
- C. The SCADA software shall support two-factor authentication, configurable per user or enforced for all users on an account.
- D. Device credentials shall be unique per device and revocable individually by the Owner, with revocation effective immediately.

2.03 OPERATOR CONFIGURABILITY

- A. The SCADA software shall allow the Owner to create new operator displays and modify existing displays. The display designer shall be WYSIWYG with a drag-and-drop interface.
- B. The SCADA software shall support unlimited user-defined alerts and shall notify designated recipients by SMS text message and email.
- C. The SCADA software shall provide voice callout as an option for alerts and alarms.
- D. The SCADA software shall support user-defined dashboards for historical trend analysis.
- E. All features of the SCADA software shall be editable and maintainable by the Owner without requiring vendor or engineering services.

2.04 CONTROL-ROOM SCADA APPLICATION

- A. A Windows or Linux application shall be provided for a control-room computer, giving the operator access to all tags in all automation controllers.
- B. The control-room application shall meet all security requirements specified in Article 2.02.
- C. The control-room application shall support multiple monitors and shall allow the Owner to assign a default display page to each monitor.

- D. The control-room application shall include a local historian using a time-series database. It shall provide a trend graphing tool permitting the Owner to create custom on-demand trend graphs of up to six tags, and a data export tool producing CSV output for Owner-selected tags and time ranges.
- E. The control-room application shall be provided with a licence permitting the Owner to edit and customise every aspect of the application.
- F. The control-room application shall include drivers for NexusSec, EtherNet/IP and Modbus TCP for reading and writing tag data to automation controllers and field input/output.
- G. The control-room application shall include an alarm and alert history page presenting all alarms in tabular form, with selective acknowledgement and deletion.

PART 3 – EXECUTION

3.01 CONFIGURATION

- A. Configure user accounts, roles and permissions as directed by the Owner. Configure operator displays, alarms and notification routing for all process areas in this Contract, on both the cloud platform and the control-room application.

3.02 DEMONSTRATION

- A. Demonstrations relating to this Section are specified in Section 40 90 00, Article 3.02.

SECTION 40 94 43 — Automation Controllers

PART 1 – GENERAL

1.01 SUMMARY

- A. This Section specifies automation controllers. Automation controllers shall be provided in lieu of programmable logic controllers.
- B. Requirements are stated separately for controllers serving fewer than 128 input/output points and for controllers serving 128 or more points.

PART 2 – PRODUCTS

2.01 TELEMETRY GATEWAY FUNCTIONALITY – ALL CONTROLLERS

- A. All automation controllers shall provide secure CAT M1 4G cellular telemetry.
- B. Telemetry shall use AES-256 encryption for all data, with unique, revocable encryption credentials per device.
- C. Telemetry shall automatically switch between AT&T, T-Mobile and Verizon networks using a single SIM.
- D. Solar-powered units shall provide a minimum of seven days autonomy. Line-powered units shall provide a minimum of 24 hours of battery-backed operation on loss of supply.
- E. Units installed in unconditioned or outdoor locations shall be housed in an IP67-rated enclosure.
- F. Automation controllers shall automatically retrieve their configuration and program from the supervisory platform on startup.

- G. Replacement of an automation controller shall be performable by Owner personnel, using a spare unit that has not been pre-configured for the position, without attendance by the Supplier or an engineer.

2.02 AUTOMATION CONTROLLERS SERVING FEWER THAN 128 POINTS

- A. The automation controller shall include a sunlight-readable LCD of not less than 2.7 inches with push buttons, or a waterproof capacitive touch screen.
- B. The automation controller shall be programmable in Python.
- C. The automation controller shall have a dual-core processor of not less than 150 MHz and not less than 520 KB SRAM.
- D. The automation controller shall include internal SD card storage of not less than 8 GB.
- E. The automation controller shall be housed in an IP67-rated enclosure.
- F. The automation controller shall operate from an 8–30 VDC supply.

2.03 AUTOMATION CONTROLLERS SERVING 128 POINTS OR MORE

- A. The automation controller shall include an integrated sunlight-readable colour LCD of not less than 10 inches with a waterproof front bezel and capacitive touch screen. Where the controller carries more than 250 defined tags, the display shall be not less than 15 inches.
- B. The automation controller shall provide user-programmable operator displays using vector graphics and a dark theme.
- C. The automation controller shall be programmable in Python and ladder logic. Ladder programs shall be able to invoke Python functions and retrieve results through a common tag.

SPECIFIER NOTE — delete before issuing for bid

Ladder for sequential and interlock logic, Python for computation, communications and anything algorithmic. Requiring both, with the ability to call across, avoids forcing the programmer to express one kind of problem in the wrong language.

- D. The automation controller shall have a quad-core 32-bit processor of not less than 1.8 GHz, not less than 2 GB SDRAM, and not less than 32 GB solid-state storage.
- E. The automation controller shall communicate with field input/output using NexusSec, Modbus TCP or EtherNet/IP.
- F. The automation controller shall communicate controller-to-controller and controller-to-workstation using NexusSec: TLS with a unique security certificate per controller. Certificates shall be managed by the cloud supervisory platform and shall be revocable on demand or on schedule.

SPECIFIER NOTE — delete before issuing for bid

NexusSec is named here deliberately, as the practical way to state this requirement without asking the specifier to evaluate a security protocol. An approved equal shall provide mutually authenticated TLS with per-device certificates that are issued and revocable by the supervisory platform, for controller-to-controller and controller-to-workstation communication. That sentence is the test to apply to a substitution request.

- G. The automation controller shall verify that operating configuration and program artifacts are authorised and authenticated before execution. All configuration and program artifacts shall be

signed using the controller's security certificate. Password protection alone shall not be accepted as meeting this requirement.

- H. The automation controller shall store not less than 60 days of history for each defined tag. Operator displays shall provide a user-configurable trend graph capable of displaying up to 60 days of history for up to six user-selected tags.
- I. The automation controller shall provide not less than two 10BASE-T or 10BASE-T1L ports and shall support Rapid Spanning Tree Protocol (RSTP) for recovery from a single link failure.
- J. The automation controller shall operate from a 9–30 VDC supply.

PART 3 – EXECUTION

3.01 INSTALLATION

- A. Install in accordance with the manufacturer's instructions. Mount antennas to achieve the signal condition identified in the coverage assessment submitted under Section 40 90 00.

3.02 DEMONSTRATION

- A. Demonstrations relating to this Section are specified in Section 40 90 00, Article 3.02, including unauthorised program rejection under item 6.

SECTION 40 96 13 — Development Environment

PART 1 – GENERAL

1.01 SUMMARY

- A. This Section specifies the development environment used to configure, provision and program automation controllers, operator interfaces and field input/output.

PART 2 – PRODUCTS

2.01 REQUIREMENTS

- A. A single development environment shall be used for all automation controllers, operator interfaces and field input/output provided under this Contract.
- B. The development environment shall require no licence fees.

SPECIFIER NOTE — delete before issuing for bid

This matters more than it appears. Licensing of programming software is one of the principal reasons owners cannot modify their own systems, and one of the reasons discontinued platforms become unmaintainable.

- C. The development environment shall support application-level development with multiple controller and operator interface projects in a single workspace.
- D. The development environment shall connect to the cloud supervisory platform for authentication, configuration and device provisioning.
- E. The development environment shall provide role-based permissions controlling who may view and edit programs and operator displays.

- F. The development environment shall be capable of importing .L5X files and converting them to programs compatible with the automation controller.
- G. The development environment shall include an AI-assisted designer capable of generating a multi-controller and operator interface application from a written specification, and of amending Python programs, ladder programs and operator display designs from text prompts.

PART 3 – EXECUTION

3.01 DELIVERY AND TRAINING

- A. Deliver the development environment to the Owner with all licences required for the Owner to modify every program and display provided under this Contract.
- B. Training on the development environment is included in Section 40 90 00, Article 3.03.

SECTION 40 94 53 — Field Input/Output and Control Network

PART 1 – GENERAL

1.01 SUMMARY

- A. This Section specifies field input/output and the plant control network. Requirements are stated separately for fewer than 192 points per automation controller and for 192 or more points.

PART 2 – PRODUCTS

2.01 FIELD INPUT/OUTPUT – FEWER THAN 192 POINTS PER CONTROLLER

- A. The field I/O system shall be modular and expandable. Each module shall provide not less than two 4–20 mA analog inputs, six digital inputs, one digital output and one analog output.
- B. The field I/O system shall support up to 16 modules, for a total of up to 192 analog and digital points.
- C. Field I/O modules shall provide pluggable headers for field connections and shall be hot-swappable, replaceable without removing system power.
- D. Field I/O modules shall communicate via Modbus RTU (RS-485).
- E. Field I/O modules shall operate from an 8–30 VDC supply.
- F. Field I/O modules shall provide LED indication for digital and analog points, as described in Article 2.03.
- G. Field I/O modules shall connect via a five-pin TBUS connector mounted on the DIN rail. The connector shall provide a five-pin 3.8 mm pluggable female header on the left side and a five-pin 3.8 mm pluggable male header on the right to permit stacking. Power and RS-485 signals shall pass through the connector to each attached module.

2.02 FIELD INPUT/OUTPUT – 192 POINTS OR MORE PER CONTROLLER

- A. The field I/O system shall be modular and expandable, with each module providing not less than 32 digital points or 16 analog points.
- B. The field I/O system shall comprise a block controller and up to 512 total points per block.

- C. The block controller shall provide not less than one 10BASE-T or 10BASE-T1L port and shall support Modbus TCP and EtherNet/IP. Where used with automation controllers specified in Section 40 94 43, Article 2.03, it shall also support NexusSec.
- D. Field I/O modules shall provide pluggable headers for field connections and shall be hot-swappable, replaceable without removing system power.
- E. Field I/O modules shall operate from an 8–30 VDC supply.
- F. Field I/O modules shall provide LED indication for digital and analog points, as described in Article 2.03.
- G. Field I/O modules shall connect to the block controller and to one another via a bus connector mounted on the DIN rail, passing power and communications between the controller and all attached modules.

2.03 INDICATION — ALL FIELD INPUT/OUTPUT

- A. For digital points, the indicator shall be lit when the point is active. For analog inputs, the indicator shall be lit when the input is within range. For analog outputs, the indicator shall be lit when the output is non-zero and within range.

2.04 CONTROL NETWORK

- A. The control network connecting automation controllers, operator workstations and field input/output shall support Rapid Spanning Tree Protocol (RSTP) so that the network remains operational on failure of any single link.

SPECIFIER NOTE — delete before issuing for bid

The source document referred to this as RTSP. RSTP — Rapid Spanning Tree Protocol, IEEE 802.1w — is the correct term. RTSP is Real Time Streaming Protocol and is unrelated.

PART 3 — EXECUTION

3.01 DEMONSTRATION

- A. Demonstrate hot-swap replacement of one field I/O module without removing system power, and confirm that the replaced module returns to service without reconfiguration.
- B. Control network single link failure is demonstrated under Section 40 90 00, Article 3.02, item 2.

SECTION 40 91 23 — Level and Pressure Instrumentation

PART 1 — GENERAL

1.01 SUMMARY

- A. This Section specifies radar level transmitters and leak detection sensor assemblies.

PART 2 — PRODUCTS

2.01 RADAR LEVEL TRANSMITTERS

- A. Level transmitters shall be 60 GHz pulsed coherent radar with Modbus RTU or two-wire 4–20 mA output.

- B. Level transmitters shall operate from an 8–30 VDC supply.
- C. Level transmitters shall consume not more than 300 mW at maximum measurement range.
- D. Level transmitters shall be capable of measuring fluid level through the wall of a plastic storage tank without an opening in the tank, and shall have a maximum measurement range of not less than 30 feet.

2.02 LEAK DETECTION SENSOR ASSEMBLIES

- A. Each leak detection sensor assembly shall comprise:
 - 1. A telemetry gateway complying with Section 40 94 43, Article 2.01, capable of reading pressure and reporting to the supervisory platform at intervals of one minute over a secure cellular connection.
 - 2. A 12 VDC solar power supply providing not less than seven days of autonomous operation without insolation.
 - 3. A 200 psi pressure transducer with an M12 A-coded connector to permit replacement without rewiring.

PART 3 – EXECUTION

3.01 CALIBRATION AND VERIFICATION

- A. Verify each level transmitter against a physical measurement at two points across the operating range and record the results.

Part 6 · Evaluating Responses

Reviewing the security submittal

The written security architecture statement required by Article 1.03 is where a non-compliant proposal becomes visible. Read it against these five questions:

Question	What a compliant answer looks like
Which direction does each connection initiate?	Every path from the site initiates outward. No path requires an inbound connection, including support access.
Can encryption be disabled?	No. Not by configuration, not at commissioning, not for troubleshooting.
What is the credential, and who can revoke it?	A per-device certificate. The Owner can revoke it from the platform, and revocation takes effect immediately.
Are programs and configuration signed?	Yes, with the device's own credential, validated before execution. Password protection is identified as insufficient rather than offered as equivalent.
What is locally accessible on the device?	An enumerated list, with the authentication required for each. Absence of USB, Bluetooth and wireless configuration interfaces is stated rather than implied.

Judging a substitution request

Where a bidder proposes an alternative to a named item, the test is capability, not equivalence of brand. For the one named requirement in these Specifications:

THE TEST FOR AN APPROVED EQUAL TO NEXUSSEC

Mutually authenticated TLS with per-device certificates, issued and revocable by the supervisory platform, applied to controller-to-controller and controller-to-workstation communication, with configuration and program artifacts signed and validated before execution. A proposal offering password authentication, a shared pre-shared key, or unauthenticated encryption does not meet the requirement.

Require the substitution request to state, in the bidder's own words, how each element above is satisfied. A bidder who can meet it will answer in a paragraph. A bidder who cannot will answer with a product brochure.

Common non-compliant answers

What you will read	What it means
"Secured behind an industrial firewall"	A listener exists. Does not meet Section 40 90 00, Article 1.02, clause C.
"Supports AES-256 encryption"	Supports is not enabled-by-default-and-not-defeatable. Ask

	whether it can be configured off.
"Unique password per device, rotated quarterly"	A shared secret with a process wrapped around it. Does not meet the certificate requirement.
"Configuration is password protected"	Explicitly insufficient under Article 2.03, clause G of Section 40 94 43.
"Field replacement supported with a pre-configured spare"	Not self-provisioning. Verify against the Article 3.02 demonstration before accepting.
"Cellular coverage to be verified by Owner"	Reassign. The coverage assessment is a Supplier submittal.
"Changes performed under our support agreement"	Does not meet the Owner-configurability requirement.

Before recommending award

- ☐ Compliance Matrix returned, complete, with no requirement marked as an exception without an accompanying substitution request
- ☐ Security architecture statement addresses all five submittal items, not four
- ☐ Coverage assessment provided for every site, from published band data
- ☐ Failover schedule lists every inter-site dependency with a named control mode
- ☐ Support horizon for all equipment meets Article 2.01, and no proposed item is end-of-sale
- ☐ Development environment licensing permits Owner modification, in writing
- ☐ Data export right stated in the proposed agreement, not only in the proposal

Appendix A • Compliance Matrix

Issue with the bid documents. The bidder completes and returns it. Any entry other than "Complies" requires an accompanying substitution request.

#	Requirement	Complies	Exception — attach substitution request
1	No equipment accepts inbound connections from outside the site		
2	Encryption enabled by default; cannot be disabled by configuration		
3	Per-device certificates, revocable by Owner, effective immediately		
4	No USB, Bluetooth or wireless configuration interface		
5	Replacement device self-provisions; replaceable by Owner personnel		
6	Owner may edit displays, alarms, notification and reports without vendor services		
7	Owner owns data; documented export at any time at no charge		
8	Update responsibilities, frequency and cost stated in writing		
9	CAT M1, multi-carrier, coverage assessed by Supplier		
10	Local control continues through outage, including dependent-site failover		
11	Configuration and program artifacts signed and validated before execution		
12	Equipment supported with firmware updates for the specified period		

Bidder declaration

Bidder: _____ Date: _____

Signed: _____ Title: _____

Appendix B · Suppliers Known to Meet These Requirements

SPECIFIER NOTE — delete before issuing for bid

This appendix is provided for the Engineer's information. It is not part of the specification and should be deleted before issuing for bid.

A specification that no supplier can meet is a defective specification. This list exists so that the Engineer can confirm at least one compliant source exists before issuing. It is not exhaustive and is expected to grow.

Requirement area	Known compliant offering
Cloud supervisory platform, per-device certificates, Owner-editable displays and alarms, browser and mobile access	D6 Labs — Whisker.io Cloud SCADA
Telemetry gateway and small automation controller, CAT M1 multi-carrier, IP67, self-provisioning	D6 Labs — SmartController Classic
High-performance automation controller, Python and ladder, signed artifacts, certificate-authenticated controller network	D6 Labs — Nexus.io AC with NexusSec
Field input/output, modular, hot-swappable, DIN rail bus	D6 Labs — m.Smart Field I/O and m.Smart Universal I/O
High-density field input/output with Ethernet block controller	D6 Labs — Nexus.io Field I/O
Radar level transmitter, 60 GHz, through-wall measurement	D6 Labs — PulsarQ
Control-room SCADA application	D6 Labs — WhiskerHMI

If you are aware of another product that meets these requirements, we would like to know about it. The purpose of publishing this specification is to raise the minimum standard in water sector procurement, not to narrow the field. A requirement that only one supplier can satisfy is a requirement that will eventually be struck.

Appendix C · Mapping to Recognised Standards

For clients who reference a framework, or ask what these requirements correspond to.

ISA/IEC 62443

Requirement	62443 concept
No inbound connections; authenticated outbound session	Zone and conduit definition; conduit protection
Per-device certificates, revocable	FR 1 — Identification and Authentication Control
Role-based permissions, per-action authorisation	FR 2 — Use Control
Signed configuration and program artifacts	FR 3 — System Integrity
Encryption in transit, not defeatable	FR 4 — Data Confidentiality
Control network segmentation and RSTP resilience	FR 5 — Restricted Data Flow
Change logging with user, object, values and timestamp	FR 6 — Timely Response to Events
Local control continuity and dependent-site failover	FR 7 — Resource Availability

NIST Cybersecurity Framework 2.0

Function	Addressed by
Identify	Device inventory and as-built documentation (closeout submittals)
Protect	Requirements 1–4, 11 — connection direction, encryption, credentials, local interfaces, signed artifacts
Detect	Change logging and alarm notification
Respond	Credential revocation by Owner; dependent-site failover
Recover	Self-provisioning replacement; platform-held configuration and programs

AWIA Section 2013

Community water systems serving 3,300 or more are required to assess “electronic, computer or other automated systems, including the security of such systems” as part of their Risk and Resilience Assessment. The security architecture submittal required by Article 1.03 produces documentation directly usable in that assessment, and it is worth telling the Owner so.

Appendix D • Acceptance Test Record

A form for recording the Article 3.02 demonstrations. Attach to the closeout submittals.

Project: _____ Date: _____

Witnessed by (Owner): _____ (Engineer): _____

#	Demonstration	Site / device	Result	Time
1	Loss of communications — control continues, data buffered and forwarded			
2	Control network single link failure — network remains operational			
3	Dependent-site failover — specified control mode adopted			
4	Field replacement by Owner personnel with unconfigured spare			
5	Credential revocation — device denied access			
6	Unsigned program rejected before execution			
7	Owner creates display element, alarm and report unassisted			
8	Alarm delivered to each configured notification path			

SPECIFIER NOTE — delete before issuing for bid

Item 2 applies to the upgraded tier only. Item 6 applies where signed artifacts are specified. Delete rows that do not apply to the project.

Appendix E • Glossary

Term	Meaning
CAT M1	A 4G cellular technology for machine communication. Lower data rate than consumer cellular, materially better link budget, lower device and data cost.
Certificate	A cryptographic credential binding an identity to a key pair. Not transferable by transcription; revocable individually.
EtherNet/IP	Industrial Ethernet protocol maintained by ODVA.
L5X	XML program export format produced by Rockwell Studio 5000.
Modbus RTU / TCP	Serial and Ethernet variants of the Modbus protocol.
MQTT / MQTTS	Publish-subscribe messaging protocol suited to constrained links. MQTTS denotes MQTT carried within TLS.
Multi-carrier	Device capable of registering on more than one mobile network and switching automatically.
Mutual authentication	Both endpoints prove identity to each other, rather than the client alone proving identity to the server.
NexusSec	Certificate-authenticated TLS transport for controller-to-controller and controller-to-workstation communication. See Part 6 for the equivalence test applicable to substitution requests.
Outbound-only	Device initiates all connections; accepts none.
RSTP	Rapid Spanning Tree Protocol, IEEE 802.1w. Provides recovery from a single link failure in a bridged network.
Revocation	Withdrawal of a credential such that it is no longer accepted.
Self-provisioning	A replacement device retrieves its identity, configuration and program after authenticating, without local programming.
Signed artifact	Configuration or program whose integrity and origin are verified cryptographically before execution.
TBUS	DIN-rail mounted bus connector passing power and communications between stacked modules.
TLS	Transport Layer Security.

About This Document

Published by D6 Labs. Free to use and adapt in project specifications, with or without attribution. If you use these sections and find a requirement that does not survive contact with a real bid, we would like to hear about it.

Companion document: the operator edition of this guide, written for utility staff making the decision rather than specifying it.



1-844-365-8647

info@d6labs.com

Disclaimer

This document is provided for professional information only, without warranty of any kind. It is not engineering advice and does not constitute a design. The Engineer of Record is responsible for the suitability, completeness and legality of any specification issued for construction, including compliance with applicable procurement law.

Version 1.0 — August 2026