SA Water

Engineering

Technical Standard

TS 0351 – IoT/IIoT Systems

Version: 1.0
Date: 16 May 2024
Status: Final
Document ID: SAW-ENG-0351
Confidentiality: OFFICIAL

Government of South Australia

Issue and version number

This version of this Technical Standard was created on 16 May 2024.

Only the current version of the Technical Standard should be used. Earlier versions of this Technical Standard are superseded and must not be used.

This Technical Standard document is not controlled when printed or downloaded. Only on-line versions from the SA Water website may be used.

Copyright and intellectual property

This Technical Standard has been produced by the South Australian Water Corporation (SA Water). SA Water owns the copyright to all material produced by SA Water.

No part of this Technical Standard may be reproduced, copied or transmitted in any form or by any means, except with the express written consent of SA Water.

Where any material is extracted from this Technical Standard, which may occur only with express written consent of SA Water, that material must be attributed to SA Water as: © SA Water

Intellectual property

Where any material is extracted from this Technical Standard, which may occur only with express written consent of SA Water, that material must be attributed to SA Water as: © SA Water

Unless indicated expressly to the contrary, SA Water (and/or any third-party licensors of SA Water) own the copyright and other intellectual property rights, which is contained in the text, graphics, information, designs, data and other content in this Technical Standard.

This Technical Standard may not, without consent in writing from SA Water, or otherwise except to the extent permitted under the Copyright Act 1968 (Cth), be reproduced for any purpose, including particularly: purposes associated with government operational activities, commercial activity, or education.

SA Water are committed to upholding the rights of owners of copyright and intellectual property, and SA Water will make every effort to contact copyright owners and request permission to reproduce and make available copyright material. If you believe that any content in this Technical Standard may infringe your copyright or other intellectual property rights, please contact us at legal@sawater.com.au and we will investigate the position, and if appropriate, endeavour to correct the situation.

If you have access to this Technical Standard and the Technical Standard is used by you or any other entity, for purposes other than to progress SA Water's statutory functions, you could be infringing SA Water's copyright, and or SA Water's intellectual property, and you may face penalties under the Copyright Act 1968 (Cth), otherwise under law, or under any other policy of SA Water or the South Australian Government that may apply.

Technical Standards are applicable or only intended use.

This Technical Standard may be used by only: SA Water staff, SA Water contractors and persons expressly authorised in writing by SA Water to do so.

This Technical Standard may be used only for application to progress activities associated with SA Water's statutory functions described particularly within the Water Industry Act 2012 (SA) and the Water Industry Regulations 2012 (SA) and the South Australian Water Corporation Act 1994 (SA), and this Technical Standard may not be used for any other activity outside of the scope of the functions described in that legislation.

If you have access to this Technical Standard, and the Technical Standard is used by you or any other entity, for purposes or activity other than to progress SA Water's statutory functions, the Technical Standard may not be applicable to that other purpose or activity, in which you or that other entity intend to engage, and you could be misinterpreting the contents and you may not correctly apply the Technical Standard. This may result in loss or damage to you, the entity or to other parties, and must be avoided.

This Technical Standard has been prepared to address general and not particular circumstances. This Technical Standard is intended to be used in conjunction with designs and project instructions that are prepared in response to particular circumstances and toward particular objectives. Any user of this Technical Standard must ensure, by independent verification, that the application of the Technical Standard is suitable to any design for any particular project, and to ensure that the Technical Standard is in accordance with the latest relevant Australian standards, legislation, regulations and codes and also with any relevant and applicable policy.

SA Water does its best to provide accurate and up-to-date information in the Technical Standards we prepare, but you should use your own skill and judgement before you rely on it. SA Water does not guarantee or warrant the accuracy, completeness, or currency of the information provided. SA Water recommends that you ask for professional advice from your own advisors on any aspect of your own circumstances.

Liability disclaimer

This Technical Standard may be used by only: SA Water staff, SA Water contractors and persons expressly authorised in writing by SA Water to do so.

To the extent that the use of the Technical Standard constitutes you acquiring goods or services from SA Water, as a consumer within the meaning of the Australian Consumer Law set out in Schedule 2 to the Competition and Consumer Act 2010 (Cth), as amended or replaced from time to time, you may have certain rights and remedies (including:, consumer guarantee rights) that cannot be excluded, restricted or modified by agreement.

Nothing in this disclaimer operates to exclude, restrict or modify the application of any implied condition or warranty, provision, the exercise of any right or remedy, or the imposition of any liability under the Australian Consumer Law or any other statute, where to do so would contravene that statute or cause any term of this agreement to be void.

You acknowledge and agree that:

- Except for any non-excludable obligations, SA Water gives no warranty (express or implied) or guarantee that information, services and materials contained in this Technical Standard are accurate, complete, current, or fit for any use whatsoever.
- All such information, services and materials are provided "as is" and "as available" without warranty of any kind. This means, for instance, that you should not rely on the accuracy or completeness of any information displayed within this Technical Standard and its suitability for application to your particular circumstances, and furthermore it is your responsibility to contact an appropriate member of our staff if you have any questions about suitability of the Technical Standard to any particular circumstance, prior to your use of the Technical Standard.

To the maximum extent permitted by law and subject to any non-excludable obligations, SA Water excludes all liability for any loss or damage arising out of access to, use of, or reliance upon information, services and materials contained within this Technical Standard.

Documents superseded by this standard

Nil - This is the first issue of this Technical Standard.

Significant/major changes incorporated in this edition

Nil - This is the first issue of this Technical Standard.

Document controls

Version history

Version	Date	Author	Comments
1.0	16 May 2024	IoT Technical Working Group	First issue

Template: Technical Standard Version 8.0, 9 April 2024

Approvers

Approver Name	Approver Role	Signature
Justin Hamra	Principal Engineer - Electrical	17/05/2024 X Justin Hamra Principal Engineer - Electrical Signed by: HA003627
Matthew Davis	Manager Engineering Quality and Innovation	21/05/2024 X Matthew Davis Manager Engineering Quality and Innovation Signed by: DA003681
Sofia Chouli	Senior Manager Engineering	23/05/2024 X Sofia Chouli Senior Manager Engineering Signed by: CH005288

Reviewers

Name	Role	Version	Focus	Review Date
Vineeth Maruvada	Technology Manager	0.1	A	18/04/24
Laughlin O'Donnell	Manager Operations Control	0.1	A	06/05/24
William Brennan Ross Kemp Justin Hamra Hamish Reid Damien Stone Mark Kopunic	IoT Technical Working Group	0.1	R	Authors
Harvey Pantow	Manager Maintenance Tactical Reliability	0.1	C	N/C
Samuel Quirk	Technology Manager Operations	0.1	C	N/C
Blake Slatter	Technology Networks	0.1	C	N/C
Leslie Lawrence	Technology Infra & Cloud	0.1	C	18/04/2024
Michael Paradowski	Mgr. Tech Strategy and Enterprise Arch.	0.1	C	N/C
Phil Bath	Snr SCADA Environment Analyst	0.1	C	10/05/2024
Charl Du Plessis	SCADA Environment Analyst	0.1	C	N/C
Darren Duncan	Senior SCADA Environ Analyst	0.1	C	N/C
Paul Grey	SCADA Environment Analyst	0.1	C	N/C
Dmitriy Lukin	Lead SCADA Systems Analyst	0.1	C	N/C
Andy Millington	Team Leader Operations Control	0.1	C	N/C
Brett Whitworth	SCADA Environment Analyst	0.1	C	N/C
Brian McAvoy	Interim Lead Cyber Security	0.1	C	N/C
Damien Stone	Cyber	0.1	C	8/3/24
William Brennan	Team Leader - SCADA	0.1	C	8/3/24
Ross Kemp	Technology Strategy & Architecture	0.1	C	8/3/24
Hamish Reid	Network Architect	0.1	C	8/3/24
Justin Hamra	Principal Engineer	0.1	C	8/3/24
Mark Kopunic	Technology Strategy & Architecture	0.1	C	8/3/24
Aled Jones	Program Manager	1.0	C	8/3/24
Candice Coetzee	Project Manager	1.0	I	
Dan Falzon,	Asset Team	1.0	I	
Michael Nicholas	Asset Team	1.0	I	
Nicole Arbon,	Asset Team	1.0	I	

Contents

List of figures

List of tables

1 Introduction

An IoT (Internet of Things) or IIoT (Industrial Internet of Things) refers to a network of physical devices, vehicles, appliances, and other objects that are embedded with sensors, software, and connectivity capabilities, allowing them to collect and exchange data over wide area networks, be they public or private. The devices, commonly known as 'things', communicate with centralised platforms, enabling remote monitoring, control, and automation.

The defining difference between IoT and IIoT solutions lies in the grade of solution applied for applications that demand different levels of criticality, resilience and integrity.

SA Water utilise several IoT/IIoT systems and from time to time, will need to implement new IoT/IIoT systems, make changes to existing IoT/IIoT systems, or retire IoT/IIoT systems.

It is important to ensure a coherent strategy and methodology is maintained within SA Water to reduce risk, simplify the selection and purchasing process, and to maximise the value of any IoT/IIoT systems used.

1.1 Purpose

This document is designed to provide clear guidance for the planning, specification, selection, and implementation of IoT/IIoT systems and hardware.

By providing clear scope, guidance, boundaries and requirements, this Technical Standard will eliminate much of the guesswork, variance, incompatibility, and conflict that could occur through improper selection, implementation, and combination of IoT/IIoT systems.

This document should be referred to whenever:

- determining the nature of the systems as IoT or IIoT,
- planning a new IoT/IIoT system,
- selecting, evaluating, or purchasing IoT/IIoT hardware or systems,
- engineering the installation of new IoT/IIoT hardware,
- engineering the new IoT/IIoT platform, or
- making changes to existing IoT/IIoT systems.

1.2 Glossary

The following acronyms, technical definitions and abbreviations are used in this Technical Standard:

Term	Description
4G	The fourth-generation wireless stage of broadband mobile communications.
API	Application Programming Interface
APN	Access Point Name
Bluetooth	A (trademark) standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
CAT-M1	A low-power, wide-area (LPWA) communication technology that is specifically designed for IoT/IIoT devices.
Cloud	Servers that are accessed over a public or private network, and the software and databases that run on those servers.

Term	Description
Communication Protocol	A communication protocol is a set of rules governing the exchange of data between devices or systems.
Contractor	A person or firm that undertakes a contract to provide materials or labour to perform a service or do a job.
COTA	'Configuration Over the Air' The process of updating the configuration of wireless devices by an over-the-air code transfer.
Critical Infrastructure	Any SA Water asset that must continually operate, including those prescribed under adverse events (i.e. natural disasters)
DC	Direct Current
DNP3	Distributed Network Protocol (DNP or DNP3 or DNP 3.0) is a communications protocol used in Supervisory Control and Data Acquisition (SCADA) and remote monitoring systems.
DPC	Department of the Premier and Cabinet
DPC-OCIO	Department of the Premier and Cabinet - Office of the Chief Information Officer
Edge Computing	Edge computing processes data near where it's generated, rather than in a centralized data centre.
EXT-IOT	Dedicated VRF for IoT network for SAW
FOTA	'Firmware Over the Air' The process of updating the firmware in wireless devices by an over-the-air code transfer.
Gateway/Concentrator	A gateway connects two or more networks thereby also providing routing and firewall functionality in addition to VPNs. A concentrator is a termination device which handles a large number of VPN connections.
GEO	Geo-Stationary Earth Orbit
GIS	Geographic Information System
GPS	Global Positioning System
HMI	Human Machine Interface
HTTP/TLS	TLS is a network protocol that establishes an encrypted connection to an authenticated peer over an untrusted network.
IAMP	IoT Asset Management Plan
iFIX®	SCADA software application developed by General Electric
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol

Term	Description
IPSEC	A group of protocols for securing connections between devices.
IPxx	Ingress Protection. Degrees of protection provided by enclosures (IP Code)
IT	Information Technology
LAN	Local Area Network
LEO	Low Earth Orbit
LoRa	from Long Range, an unlicensed wireless radio communication technology utilising spread spectrum modulation techniques derived from chirp spread spectrum technology offering long range, low power and secure data transmission
LPWAN	Low Power Wide Area Network
LTE-M	Long-Term Evolution Machine Type Communication
MAO	Maximum Allowable Outage
MD5	Message Digest (method 5)
MQTT	Message Queuing Telemetry Transport
NBIoT	Narrow Band-Internet of Things
Non-operational Assets	Refer to systems or processes that are not directly involved in the day-to-day production, treatment, distribution, or maintenance of water/wastewater but are still essential for the overall functioning of the organisation. These systems typically support administrative, regulatory, or strategic functions.
OCC	SA Water's Operations Control Centre
Operational Assets	Operational assets are the physical assets and infrastructure used in the daily operations and distribution of water.
OSI	Open Systems Interconnection
OSN	Operational SCADA Network
OT	Operational Technology
PCN	The Plant Control Network (PCN) is typically a network at a plant control site (treatment plant, pump station, etc.) which hosts one or a number of automation controllers (PLCs).
PLC	Programmable Logic Controller
PLCR	SA Water Regional PLC VRF
PoE	Power over Ethernet

Term	Description
RTU	Remote Terminal Unit - A special computer device that sends sensor information from assets via a communications network to a SCADA server.
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
StateNet	South Australian Government's federated data network
TCP/IP	Transmission Control Protocol/Internet Protocol
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

1.3 References

1.3.1 Australian and international

Any Standard referred to in this Specification shall be of the latest edition (including amendments) of that Standard at the date of calling of tenders.

The following table identifies Australian and International standards and other similar documents referenced in this Technical Standard:

Number	Title
IEC 60529:1989+	Degrees of protection provided by enclosures (IP Code)

1.3.2 SA Water documents

The following table identifies the SA Water standards and other similar documents referenced in this Technical Standard:

Number	Title
TS0300	Supply and Installation of Low Voltage Equipment
TS0350	SCADA Systems
TS0360	PLC and HMI Systems
	Technology Strategy - IoT Communication Capability
IAMP	IoT Asset Management Plan Template
	IoT Technical Working Group – Terms of Reference
	SA Water Data Governance Framework
	SA Water Corporate Records Management Policy

Number	Title
SAWC-IS-0032	Data Management Procedure.docx (sharepoint.com)
	SA Water API security standard V1.0

1.3.3 Other Documents

The following table identifies other documents referenced in this Technical Standard:

Title	Application
Azure IoT Platform	IoT Management Systems
Code of Practice	Australian Government Code of Practice – Securing the Internet of Things for Consumers (2020)
Engaging Suppliers and Cloud Security	https://security.sa.gov.au/documents/documents/SACSF-G3.0-Engaging-Suppliers-and-Cloud-Security.pdf
Information Security Manual	https://www.cyber.gov.au/sites/default/files/2023-09/22.%20ISM%20-%20Guidelines%20for%20Cryptography%20%28September%202023%29.pdf
Internet of Things (IoT) Policy Guidance	NSW Government publication Rev 1.2 - 8/3/2021
IoTAA IoT Standards	https://iot.org.au/page/resources (Guidelines & Codes of Practice)
IoT Secure-by-Design Guidance for Manufacturers	https://www.cyber.gov.au/sites/default/files/2023-09/PROTECT%20-%20IoT%20Secure-by-Design%20Guidance%20for%20Manufacturers%20%28September%202023%29.pdf
NIST special Publications 800-53 Revision 5	Roles and Access Levels
SACSF IoT Security Guideline	https://www.security.sa.gov.au/__data/assets/pdf_file/0010/947845/SACSF-G17.0-Internet-of-Things-Security-Guideline.pdf
StateNet Conditions of Connection. Version 5.0 - Policy	Department of Premier and Cabinet's Conditions of Connection
	Patching Applications and Operating Systems (online resource) First published: 01/22/2011 (content link 27/11/2023) Australian Signals Directorate - Australian Cyber Security Centre
SACSF Ruling 2	https://www.security.sa.gov.au/documents/documents/SACSF-Ruling-2-Storage-processing-information.pdf

1.4 Definitions

The following general definitions are applicable to this document:

Term	Description
Accepted	Determined to be satisfactory by SA Water's Representative
Constructor	The organisation responsible for constructing and installing infrastructure for SA Water whether it be a third party under contract to SA Water or an in-house entity.
Contract Documents	A set of documents supplied to Constructor as the basis for construction; these documents contain contract forms, contract conditions, specifications, drawings, addenda, and contract changes
Designer	The organisation responsible for designing infrastructure for SA Water whether it be a third party under contract to SA Water or a Constructor, or an in-house entity. A Designer is a person who effects design, produces designs or undertakes design activities as defined in the *Work Health and Safety Act 2012 (SA)*.
Manufacturer	A person, group, or company that owns and operates a manufacturing facility that provides materials for use in SA Water infrastructure
SA Water Representative	The SA Water representative with delegated authority under a Contract or engagement, including (as applicable): • Superintendent's Representative (e.g. AS 4300 and AS 2124, etc.) • SA Water Project Manager SA Water nominated contact person
Shall and should	In this Standard the word "shall" indicates a requirement that is to be adopted in order to comply with the Standard. The word 'should' indicate practices which are advised or recommended.
Supplier, Service Provider or Vendor	A person, group or company that provides goods for use in SA Water infrastructure
TDRF	Technical Dispensation Request Form. This form is part of SA Water's Technical Dispensation Request Procedure which details the process by which those required to comply, or ensure compliance, with SA Water's technical requirements may seek dispensation from those requirements.
Terminology	• Where an obligation is given and it is not stated who is to undertake these obligations, they are to be undertaken by the Constructor. • Directions, instructions and the like, whether or not they include the expression "the Constructor shall" or equivalent, shall be directions to the Constructor, unless otherwise specifically stated. • Where a submission, request, proposal is required and it is not stated who the recipient should be, it is to be provided to SA Water's Representative for review. • Each word imparting the plural shall be construed as if the said word were preceded by the word "all".

Term	Description
	• Each word implying persons shall, where appropriate, also be construed as including corporations. • "Authorised", "approval", "approved", "selected", "directed" and similar words shall be construed as referring to the authorisation, approval, selection or direction of SA Water's Representative in writing. • "Allow" shall mean that the cost of the item referred to is the responsibility of the Constructor. • "Provide" shall mean "supply and install". • "Submit" shall mean "submit to the SA Water Representative or their nominated delegate". • Submissions, requests, proposals are to be provided at least 10 business days prior to work commencing or material ordering (unless noted otherwise). 'Informative' shall mean 'provided for information and guidance'
Work	• Elements of a project which require design and/or construction

2 Scope

The scope of this Technical Standard pertains to any IoT and IIoT systems that are to be utilised within SA Water, whether owned by SA Water or third parties. Just as TS0350 specifies standards for SCADA systems, and TS0360 specifies standards for PLCs and related hardware, this document specifies when and how IoT and IIoT may be adopted.

This Technical Standard outlines the following functions in terms of IoT/IIoT:

- Alignment of the high-level functions of both Operational Technology and Smart Infrastructure,
- The definition of a reusable model with common terminology for the harvesting and interpretation of telemetry,
- The defining of the core functionality of each 'layer' within the model, and
- The definition of a strategic intention for each function. i.e., where to standardise, consolidate and commoditise, and where to facilitate specialisation and bespoke solutions.

The scope of the document aims to standardise how device telemetry is ingested, stored, analysed and visualised, with a common data management mechanism to facilitate the sharing of data and simplifying its access for advanced analytics and visualisation.

2.1 Technical dispensation

Departure from any requirement of this Technical Standard shall require the submission of Technical Dispensation Request Form (TDRF) for the review and approval (or otherwise) of SA Water Principal Engineer listed in Page 3, on a case-by-case basis.

The Designer shall not proceed to document/incorporate the non-conforming work before the Principal Engineer has approved of the proposed action in writing via the Technical Dispensation Request Form (TDRF).

SA Water requires sufficient information to assess dispensation requests and their potential impact. The onus is therefore on the proponent to justify dispensation request submissions and provide suitable evidence to support them.

Design works that are carried out without being appropriately sanctioned by SA Water shall be liable to rejection by SA Water and retrospective rectification by the Designer/Constructor.

2.2 Design criteria

The design criteria must be ascertained and agreed with SA Water or its representative during all stages of investigation, concept design and detailed design in order to achieve a value-for-money installation that is fit for purpose and with minimum or negligible risks to SA Water. The design criteria should consider the following aspects:

1. Life Cycle Costs

Designs should be innovative and incorporate the appropriate techniques and technology, in conjunction with the selection of appropriate equipment, to minimize the life cycle costs, while satisfying operation and maintenance requirements. Energy consumption must be given particular attention in this respect.

2. Security of Operation

Designs should take into account the failure of a single item of equipment or a fault in a particular area of an installation is confined to the associated part of the installation and does not affect the continuous operation of the remaining parts of the installation, where possible.

3. Reliability

The installations are to be designed to minimize the likelihood of a failure, taking into consideration the electricity supply characteristics, ambient conditions, load characteristics and operation and maintenance requirements.

4. Upgradability

The installations are to be designed to facilitate future upgrades where applicable.

5. Interchangeability

The installations are to be designed to maximize the interchangeability of components and assemblies as far as practical to improve flexibility and reduce the spare parts inventory.

6. Operation, Maintenance and Fault-Finding Facilities

The installations are to be provided with suitable and adequate facilities to allow ease of operation, maintenance and fault finding.

7. Environmental Considerations

The installations are to be designed and suitable equipment selected to avoid or minimize unacceptable impact on the environment as far as possible.

8. Safety Considerations

The installations are to be designed with the safety and welfare of construction, operation and maintenance personnel and the general public in mind, complying with statutory regulations. Wherever possible, electrical equipment and wiring should not be located in areas classified as hazardous.

3 Key definitions and criteria

The seamless communication between devices, sensors and software, through adaption of IoT/IIoT systems allow an environment where data can be shared and analysed easily. It is important to emphasise that **IoT/IIoT solutions have a range of strengths and weaknesses, and their adoption and use shall be determined in line with the criteria outlined within this Technical Standard.**

3.1 Operational and Non-Operational assets

SA Water **Assets** are defined as physical devices only, and not the monitoring/control devices associated with them. (i.e. pumps, tanks, pipes, valves, process equipment, etc.) and can be divided into two main classes, being Operational Assets (e.g. pumps) and Non-Operational (e.g. security system) Assets. Each class has attributes that are outlined in Table 3-1.

Table 3-1 - Attributes of Operational Assets vs Non-Operational Assets

	Operational Assets	Non-Operational Assets
1	require 24/7 operator monitoring on SA Water SCADA*.	may be displayed on SA Water SCADA, but not OCC*** monitored 24/7.
2	have a requirement where a change in status needs to be displayed on SA Water SCADA.	not essentially required to be displayed on SA Water SCADA and may use SA Water SCADA only as a 'dashboard' facility for display of data and sensor health.
3	have an immediate real-time impact on SA Water key services (including energy, water and wastewater)	used for non-time critical decision making and are tolerant of a 'store and forward' mode of data treatment.
4	need to be (are) directly connected to the SA Water Plant Control Network (PCN)** (e.g. typically through a PLC or RTU).	not to be (are not) directly connected to the SA Water Plant Control Network (PCN).
5	required to have continuous 24/7 monitoring and control availability with only planned outages for maintenance.	not required to have continuous availability.

* SA Water SCADA - The SA Water owned and operated iFIX SCADA system (OSN).

** PCN – Plant Control Network: Typically, a TCP/IP network at a process control site (treatment plant, pump station, etc.) that connect host devices that are non-deterministic/non-guaranteed communication devices that exhibit slow response times. (i.e. greater than 100msec). Refer to the detailed definition in TS0360 sec 4.3.3.1

*** OCC – SA Water Operational Control Centre.

3.2 Control and monitoring of SA Water assets

Within SA Water, monitoring and control of assets falls into four distinct application categories:

1) Monitoring and/or control of Operational Assets;
2) Monitoring only of Operational Assets;
3) Monitoring and/or control of Non-Operational Assets; and
4) Monitoring only of Non-Operational Assets.

where 'monitoring' refers to systems that observe and record data in a particular environment using sensors, e.g. recording the level of a tank. 'control' refers to systems that actively maintain or change the state of devices in a particular environment using actuators.

3.3 Operational SCADA Network (OSN)

SCADA infrastructure resides on a dedicated Operational SCADA Network (OSN) and is logically separated from SA Water's business and security networks. Communications between these networks is strictly controlled in accordance with SA Water Security Policies.

3.4 OT, Non-OT, IoT and IIoT definitions

Operational Technology (OT) refers to the technology used to manage data to and from physical assets through the SA Water Operational SCADA Network (OSN). The communication and systems that support this interaction is over a private network. Therefore, OT solutions shall only be used for monitoring and/or control of **Operational Assets**.

Internet-of-Things (IoT) refers to technology that obtains inputs or inputs and outputs from physical assets over public and private networks and services (cloud), often requiring minimal specialist or dedicated infrastructure.

Industrial Internet-of-Things (IIoT) is an extension of IoT which provides a reinforced level of resilience, security and trust regarding the interference or modification of the data it is handling.

A table showing the basic distinction between IoT and IIoT is offered in Table 3-2.

Table 3-2 – Comparison of IoT and IIoT Technologies

Parameter	IoT	IIoT
Design Life	2-10 years	Up to 20 years
Resilience	Recovery time ranges from 'minutes' to 'days' (A3 to A1)	Recovery time ranges from 'minutes' to 'hours' (A4 to A3)
Interoperability	Open transports and protocols	A combination of open and highly optimised proprietary transports and protocols
Measurement precision	low to medium	medium to high
Latency to user	minutes/hours	seconds/minutes
Roles	Lower cost, ease of commissioning, convenience, informing analytical insights.	Low to medium cost, ease of commissioning, convenience, informing analytical insights and informing operational decisions, programmable firmware and edge logic.
Maintenance requirements	Ad-hoc, based-on alerts	Scheduled and planned

3.5 Where to use OT, IoT or IIoT applications

Within SA Water, there are three classes of instrumented systems that may be applied to various measurement and control applications:

1. **Internet of Things (IoT)** systems (comply with TS0351)
2. **Industrial Internet of Things (IIoT)** systems (comply with TS0351 as well as either TS0350 or TS0360)
3. **Operational Technology (OT)** systems (comply with TS0350 and TS0360)

In choosing an acceptable technology, the following table (Table 3-3) should be consulted.

Table 3-3 - Technology Selection for Instrumentation and Control Applications in SA Water

Application	Acceptable Technology		
	IoT	**IIoT**	**OT**
Monitoring and/or control of Operational Assets	No	No	Yes
Monitoring only of Operational Assets	No	Where justified (Not Preferred)	Recommended
Monitoring and/or control of Non-Operational Assets	Yes	Yes	Where justified
Monitoring only of Non-Operational Assets	Yes	Yes	Where justified

Note:

1. IoT (non-operational) technology is considered as being suitable for lower criticality business functions. IoT technology <u>shall not</u> be utilised for control of Operational Assets. IoT may be used for monitoring and/or control of Non-Operational Assets, or where justified, for monitoring only of Operational Assets.
2. IIoT may be used for IoT use-cases as well as ‘informing’ operational decisions.
3. All OT deployments will need approval by the Operations P&T.
4. Only OT will be considered for control purposes.
5. Technology selection will depend on cost, technology fit and criticality of the data.

3.6 Architectural layers of IoT/IIoT landscape

The following diagram summarises the layers in SA Water's IoT/IIoT/OT reference architecture that forms the basis for the specifications within this Technical Standard.

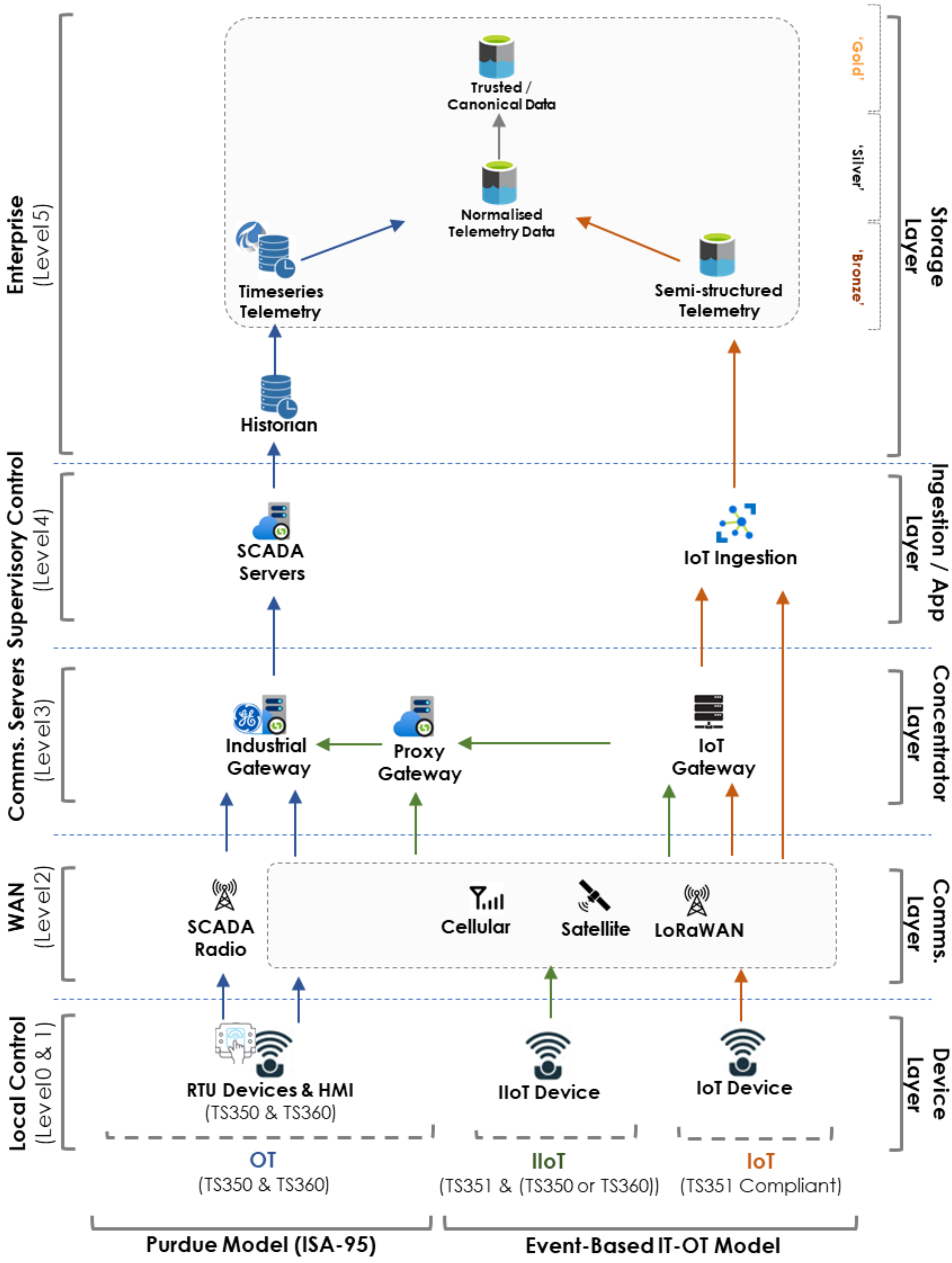

Figure 3-1 - SA Water OT/IoT/IIoT Architecture

3.6.1 Device/Edge layer

This is the lowest level in the hierarchy and refers to the devices or 'things' in the OT/IIoT/IoT system. These devices include sensors, actuators, and other connected hardware.

At this level, data is collected from the physical environment through sensors, and basic local processing and control may occur. Control in the context of IoT is limited to changing the functioning of the IoT device itself (e.g., preprocessing/filtering of data to reduce the amount of data which is transmitted to the gateway.) For IIoT devices, a very limited and specific level of control is permitted of the physical asset. Some definitions that will assist in the assignment of these scenarios are as such:

- **Local Manual Control -** Refers to the ability of users to adjust the output or setpoint of a device locally. This would usually be done using a mobile phone, laptop or tablet connected to the device. Alternatively, some devices have pushbuttons and LEDs or a display which enable limited manual control of the device.
- **Local Automatic Control -** Refers to the ability of a device to manage closed-loop control using local data and affecting setpoints of a local actuator. The setpoint may be provided by remote means, however, the control is managed by the device. (e.g. in the case of a flow or pressure regulating device.)

3.6.2 Communications layer

This level acts as an intermediary between the edge devices and the cloud or central server. Gateway or Edge Computing devices are responsible for aggregating, filtering, and preprocessing the data collected from edge devices. They may also perform local analytics and decision-making. Gateways help reduce latency, optimise network bandwidth, and provide localised intelligence. This is beneficial if a loss of connectivity to the Cloud/server is an issue (e.g. in regional or remote areas), data is needed in real-time, or bandwidth is not adequate to transmit the data to the Cloud/server.

The communications layer sends and receives messages to the Concentrator/Gateway layer, or, in specific cases, directly to the application layer.

The communications layer might include repeaters, gateways, private satellite connections, communications towers and more. Typically, there may be hundreds or thousands of devices transmitting messages.

3.6.3 Gateway/concentrator layer

Data can be ported to the internet through a variety of mechanisms, which will collectively be referred to as the 'Gateway'. Note that for different systems this may be hardware or software and may consist of multiple components. For example, for low earth orbit satellite systems the Gateway might be a network of satellites, communications towers, and modems.

3.6.4 Application / ingestion layer

The application is the software system that ingests the data and potentially also draws value from the data. The primary function being to retrieve the telemetry, decode and/or decrypt the data, log any exceptional cases, and persist the data. The application may also present data to the user to extract meaningful insights, trigger alarms and notifications, or route the data to third-party applications or services.

The application layer also enables remote configuration, administration, centralised management, and monitoring of the IoT/IIoT ecosystem.

3.6.5 Storage layer

The storage layer provides linkages to the relevant location, asset, customer construct to be able to associate value and context to the data returned from the device.

Storage includes the delineation between raw data, semi-processed/structured data, and curated data.

4 Assessment of data needs

The selection of a given IoT/IIoT device is based on several factors. From a data perspective the following need to be determined:

a) **What data** is required to be obtained.
   - i.e., timestamp, physical quantity reading, device battery level, etc.

b) The **level of accuracy/precision** of the data required.
   - i.e., metres, centimetres, millimetres, etc.

c) The **frequency** that data is to be read and how often it is to be communicated.
   - i.e., how many times per second/minute/hour/etc data should be read and if the data is communicated immediately or if it is to be sent in batch form every hour/day/etc.

d) The degree of **edge processing** required/allowed.
   - i.e., whether data should only be communicated where it breaches a given threshold.

e) **What stakeholders** will use the data.
   - i.e., field crews, maintenance teams, data analysts, planners, operators, etc.

f) **What business functions** the data will be used for.
   - i.e., long term forecasting, plant operation, predictive maintenance, etc and therefore what level of performance, continuity, and integrity is required.

g) The **criticality** required.
   - i.e., what level of business impact there will be from an outage. This will determine the level of resilience, recoverability and quality of service that needs to be factored into the device selection and solution.

The type of users and business functions that the data will be used for will be a key factor relating to whether an IoT device, IIoT device or an OT device is required.

The type and frequency of the data will be key factors that determine the type of communication that will be required.

4.1 Identify stakeholders

SA Water's data strategy highlights the need for data to be open, accessible, and shared (and only restricted by exception). Therefore, data requirements and criteria shall consider the needs and opportunities of the organisation, not merely for the project.

Thus, for each undertaking, stakeholders from across the organisation are to be identified and consulted, to recognise any wider opportunities for the data (and therefore the devices).

4.2 Define data model

Data from IoT and IIoT[1] devices is persisted into storage once it has been ingested via either the IoT Platform or the Operational Technology proxy.

The raw data shall be stored in the format it is received, which must be in:

- non-proprietary format; and
- as standard / open file structures (csv, json, xml, parquet, ODF, text, etc).

Devices shall transmit:

- the timestamp of the read.
- the values of the read; and
- the device identity.

[1] Note that IIoT data is also routed into the Operational SCADA Network (OSN) where it is stored and managed separately.

Additionally, devices shall transmit metadata, including:

- battery level (refer conditions of section 8.2.3).
- quality of data (i.e., metrics related to the sensor reading, etc).
- communication signal strength.
- retry or failed transmission statistics.
- geospatial information; and
- the unit of measure for the reading.

IoT and IIoT devices configured within the SA Water Asset Management Platform require the following metadata recorded, at a minimum:

- device manufacturer.
- device serial number.
- device reading frequency.
- device communication frequency.
- device type (i.e., pressure, flow, level, etc.).
- reading parameters (i.e., where there are multiple data feeds available); and
- device calibration.

4.3 Data quality

Data quality in the context of this Technical Standard includes:

- accuracy of the sensor reading.
- reliability of the device.
- stability and accuracy of any Edge processing on the device, including device firmware logic such as buffering and retry.

The data quality criteria for an IoT/IIoT device are determined by the project sponsor for the device being considered and all stakeholders identified in section 4.1 who will utilise the data.

The quality assurance of the ingestion and storage of device data is required to comply with the standard SA Water quality assurance and testing requirements. i.e., in line with the SA Water Technology delivery process for IoT data or the Operational Technology change process for IIoT data.

4.4 Availability

The availability (Service Level Agreement) for IoT devices is set by the project sponsor for the device being considered and all stakeholders identified in section 4.1 who will utilise the data, but not be less than 95%.

The minimum availability of IIoT devices shall be 99%.

The minimum availability of communication services shall be 99.95% as these are required to be shared between IT and OT.

The minimum availability of IoT application services (i.e., the Enterprise IoT Platform) is 99.95%.

5 Service provider qualifications

This section outlines the requirements of a Service Provider who may either supply IoT products or services, or both. Refer to SA Water Procurement policies for further details. Note any plant data requirements should reference the SA Water IoT/IIoT catalogue first and leverage the already qualified instrumentation first.

5.1 Minimum requirements

Given the difference between the provision of IoT/IIoT services and PLC/SCADA services are primarily: that to deliver PLC/SCADA services to SA Water, a Service Provider needs to have met a stringent and detailed prequalification to earn a position on the SA Water 'Automation Panel', a suitable IoT/IIoT Service Provider will need to meet any of the following criteria:

1. Be sub-contracted under one of the approved Automation Panel members.
2. Be an existing approved Service Provider with SA Water for IoT/IIoT type services.
3. Apply for, and qualify as, an IoT/IIoT Service Provider through SA Water procurement processes.

An IoT/IIoT Panel arrangement should be investigated and implemented to ensure easier and cheaper deployment of equipment.

The procurement processes mentioned above would include all the usual commercial reference checks, but most importantly, a technical evaluation which would be conducted internally by SA Water personnel. As a part of the reference checks, it could be expected that the following details and evidence is provided:

- product/service offerings;
- potential usage;
- previous length and depth of experience;
- alignment with device manufacturers;
- relevant case studies;
- resource skills and capability;
- personnel resumes;
- service capability;
- warranty conditions;
- etc.

5.2 Robustness of supply chain

An IoT/IIoT Service Provider is expected to maintain the integrity and security of its supply chain. This includes contractual undertakings for the Service Provider to provide SA Water with information about its local and global supply chain as it relates to, or impacts on, the hardware and software.

5.3 Intellectual property

An IoT/IIoT system proposal must specify who owns the intellectual property. The SA Water default position is that SA Water owns the intellectual property unless otherwise negotiated with the vendor. In which case the vendor must grant a perpetual, transferable, royalty-free licence for SA Water to use it.

5.4 Transfer/right of use by other parties

Vendor lock-in, where an IoT/IIoT Service Provider restricts access to data or the way it can be used, is not acceptable and shall be excluded. This includes the use of proprietary data or protocols where proprietary software is required to access the data.

SA Water Procurement Policies contain guidance and advice in this aspect.

6 Data storage rules

Storage volumes for plant generated data will grow over time so storage models need to be carefully considered for longer term storage forecast requirements. All IoT data is to be stored within the SA Water IoT Platform. All operational required IIoT data is to be stored within the SA Water OT Platform.

6.1 Data governance and management

The SA Water policy for how/where data from IoT/IIoT systems will be stored in the data lake and possibly the OT environment dependant on the data usage. Such considerations include:

- how close to real-time the data is needed;
- the type of data and the bandwidth required (e.g. video);
- the level of connectivity (e.g. offline processing);
- how the data is to be used; and
- the level of security.

6.2 Data retention rules

SA Water data retention/destruction rules are defined within the SA Water Corporate Records Management Policy.

No specific data retention or records management policy exists for IoT/IIoT data and therefore, in the interim, all retention and destruction decisions need to be authorised and documented in the IoT Asset Management Plan (IAMP) to achieve transparency and accountability.

In terms of data retention and associated storage costs, it is preferred that sensor data is only transmitted when there is a change from the previous transmitted value. This may require some simple Edge processing.

If very large volumes of data are involved, approaches will be needed to routinely purge data that is not needed for ongoing purposes.

6.3 Cloud providers and hosting

Vendor hosted solutions are required to adhere to SA Water's Cyber, Resilience and Data Sovereignty policies. Contact the owner of this Technical Standard for further details.

Any components within an IIoT solution that are required to conform to SA Water's Operational Technology 'chain of custody' criteria will mean that the SA Water Operations team will retain exclusive administrative access to the solution components.

Additionally, any components of solutions hosted outside of SA Water's infrastructure shall comply with the Department of Premier and Cabinet's Conditions of Connection.

7 Cyber security requirements

Every IoT/IIoT device is a potential security vulnerability, so an IoT/IIoT implementation must include careful consideration of IoT/IIoT configuration and integration into existing security tools and platforms, such as intrusion detection and prevention systems and anti-malware tools. Similarly, the data produced by IoT/IIoT devices will be subject to data protection, compliance and retention requirements that must be considered.

Care needs to be observed with the selection of IoT/IIoT devices as they typically have limited processing capacity, memory, and power, which in turn means they often lack the ability to enable advanced security controls. Manufacturers can be inclined to leave security features out to drive down production costs.

Solutions must meet the below requirements, as specified.

(Refer to the Commonwealth Code of Practice on Securing the IoT for consumers)

7.1 Minimum requirements

An IoT/IIoT system is required to establish robust security protocols to safeguard data, especially during transmission. This includes encryption and secure authentication methods. They must remain compliant with regional and international standards and regulations concerning frequency usage, data transmission, and deployment.

The following cyber security requirements shall apply to IoT/IIoT devices and platforms:

1. It must be possible to restrict logical access to the configuration portal, management platform, and connected network devices.
2. Default secrets (including passwords) and default account names for devices and management platforms must be changeable.
3. Any device, platform, software/firmware or supporting application that uses a hard-coded secret (password, certificate, etc) shall not be permitted.
4. Patching and/or upgrades of devices must be supported.
5. The device must support the ability to patch/upgrade remotely to allow critical vulnerabilities to be addressed within required timeframes.
6. Interfaces to devices, gateways, and / or applications must only be accessible from the local network, unless the device is specifically required to be remotely managed from the internet.
7. Devices and gateways must be able to be physically secured to prevent unauthorised access. Installing the device in a locked cabinet, or in an area that is not physically accessible to the public is acceptable.
8. IoT and IIoT systems must be segregated from corporate and OT networks with SA Water cyber security approved methods of connecting to each network.
9. Prior to and after being put into production, IoT/IIoT systems shall be assessed by penetration testing. External penetration testers (having suitable qualifications and experience) will be required to penetration test any system that has an interface which is accessible on the internet. Internal penetration testing may only be performed on non-critical, non-SCADA solutions. A penetration test also needs to be performed in line with any major feature enhancements or configuration changes to a system if it is public-facing.

A Cyber Security representative must be assigned as a stakeholder to the solution.

Any component of an IoT/IIoT solution that provides or is suspected of providing a ‘backdoor’ will not be permitted (e.g., a covert method of bypassing normal authentication or encryption).

IoT/IIoT solutions must comply with the following cyber/architecture principles:

1. Minimisation of attack surface: minimise and restrict access to certain areas / functions by reducing entry points for unauthorised users.
2. Secure by default: security is built into the solution and not added later.
3. Least privilege: only the minimum privileges necessary to achieve the desired outcome should be granted to a user, system, or process.
4. Defence in depth: no single security component failure should result in the compromise of an entire environment.
5. Fail securely and gracefully: failure of a component must not lead to a lower state of security.
6. Enforce minimal trust: validate everything received or entered.
7. Separation of duties: no one person should have complete control over critical functions, and security should be enhanced through the division of privileges amongst multiple parties.
8. Keep security simple: security designs must be as simple as possible to achieve the required outcomes and minimise the number of errors and vulnerabilities.
9. Protect sensitive data in transit and at rest: protect data that is travelling between networks and data that is being stored.
10. Secure the weakest link: Prevent attackers gaining access through the weakest link, whether this is a person, vulnerable application or unsecured method of entry.

7.2 Data privacy and security

No personal data shall be used by Service Providers for a purpose other than what is specified in the project specification. Service Providers must limit their data collection to only the approved purposes specified.

Unless deemed absolutely necessary by SA Water, personal information shall not be collected, as it is subject to stricter storage and access requirements.

Examples of personal data within IoT/IIoT sensors include:

- Data that can identify a person/individual.
- If Data can 'reasonably' be linked to an identified person. Information is 'reasonably identifiable' if there is a reasonable likelihood that re-identification can occur.
- Data held by an organisation with the capability to identify the information, even if the organisation has not yet done so.

Default settings which route data back to the device manufacturer if a device loses connectivity are not permitted without approval. This can be a security and privacy risk and could result in data loss. Full disclosure of any such default settings is required.

7.3 APIs

An Application Programming Interface (API) developed by a third-party or provided as part of a commercial product must support the release of open data and maintain the safeguards for sensitive information.

Any APIs provided by solution components must meet the requirements of SA Water's API standard.

8 Technical requirements

Irrespective of what system architecture is in place or is adopted, an IoT/IIoT system shall have the following features:

1. Support of multiple sensor types;
2. Be extensible to easily support extensions, upgrades, and inclusion of new modules as they are integrated; and
3. Support at least one of the stated protocols (see section 8.3.1).

8.1 Performance requirements

Performance requirements, business continuity and back-up requirements will determine the design of an end-to-end IoT/IIoT solution. The solution requirements will also help determine the level of automation required at the Hub and Edge.

The following technical performance aspects shall be assessed for suitability for any proposed IoT/IIoT system:

a. Data integrity
b. Data rate
c. Mobility (if relevant)
d. Latency
e. System reliability
f. Device accuracy
g. Load handling capability and response to gradual or sudden overload conditions
h. System stability in environmental conditions
i. Device and user capacity/connection density
j. Energy efficiency

8.2 Hardware requirements

8.2.1 Design life

Devices require a minimum design life of 5 years with a preference for greater than 10 years.

The design life of a device shall be defined by SA Water stakeholders and stipulated in the market scan for a suitable product.

The design life shall be based on both the criticality of the system and the financial viability of the total cost of the solution, after maintenance and replacements are factored in.

8.2.2 Materials of construction

Material selection for any device shall consider aspects of strength, thermal/electrical resistance, flammability, opacity, UV resistance, machinability, and conditions of the environment in which the device will be installed/used.

Protecting the sensors and circuitry in any device from ingress of both solids and liquids shall follow the principles outlined in SA Water Technical Standard TS0300.

8.2.3 Device power

Where an IoT/IIoT device is not powered by mains power, battery life is a part of the primary selection criteria. Primary battery cells (non-rechargeable) shall have a minimum ‘shelf life’ of 10 years, and secondary battery cells (rechargeable) shall have a minimum shelf life of 5 years.

An IoT/IIoT device must have a minimum operational (powered) life of 2 years.

Where electrical load permits, long-life primary battery cells shall be preferred over secondary battery cells, that require solar or energy harvesting ancillary components.

Batteries shall have a stainless steel or plastic enclosure.

If there is no fuse on the device, batteries shall have an integral fuse or other over-current protection.

Batteries and devices shall have reverse polarity protection, which could include but is not limited to:

- keyed connectors;
- electronic/mechanical protection in the battery; or
- electronic/mechanical protection in the IoT device.

Lithium batteries shall be hermetically sealed.

The IoT/IIoT device shall provide an accurate means for remote determination of remaining battery capacity unless it can be proven through past performance or controlled testing, that its consumption is consistent enough to predict battery life with an accuracy of ±10%.

The IoT Asset Management Plan must define a battery replacement plan.

8.2.4 Gateways and aggregators

Gateway hardware (typically LoRaWAN gateways) require:

1. Endorsement from SA Water Operational Technology, Networks and Cyber Security stakeholders;
2. Support, installation and administration by SA Water SCADA Applications Support as per the reference architecture and the ‘OT chain of custody’;
3. 4G or satellite connectivity with Ethernet (RJ45);
4. A carrier grade (IP67) casing for industrial use;
5. Multiple channels to accommodate traffic splitting or segregation;
6. Mounting kits allowing simple and quick installation without opening the casing; and
7. Built-in high-rejection filters for co-localization with other radio devices, enabling strong interference resistance.

Gateway hardware shall also support:

1. An ability to add external antennae for GPS, 4G, or LoRa;
2. An ability to add a back-up power source with solar panel charging; and
3. PoE injector or DC power.

8.3 Communication

8.3.1 Communication types

SA Water’s ‘IoT Communication Strategy’ outlines the types of communication the organisation supports and the scenarios best suited to each type. The selection guide is summarised as follows:

- **Cellular** capability
  - **NBIoT is the preferred cellular LPWAN service.** CAT-M1 and LTE-M may be used where NBIoT is not available.
  - Cellular communications are required for IoT/IIoT scenarios where devices are dispersed, where there are heightened message delivery or security requirements, larger message payloads or for sub-surface or mobile devices.
  - Cellular services can be provisioned as a private WAN link or a public internet link. It is preferred that IIoT cellular communications are via a private WAN link.
- **High-frequency radio** capability
  - **LoRaWAN is SA Water’s high frequency LPWAN radio service for IoT/IIoT.**

  - The selection of LoRaWAN must account for any existing OT radio services within the region, to ensure compliance and quality of signal.
  - Solutions shall comply with ACMA requirements.
- **Low-frequency radio** capability
  - The use of proprietary radio technologies is actively discouraged.
- **GEO and LEO Satellite** capability
  - GEO (Geo-stationary Earth Orbit at ~35,000km above ground level) satellite can be provisioned as both internet and private WAN but SA Water has only provisioned it as the latter.
  - LEO (Low Earth Orbit at ~550km above ground level) satellite is high bandwidth, low latency.
  - SA Water has endorsed GEO and LEO vendors, details of which can be obtained from SA Water procurement.

8.3.2 Visualisation and communication of data

Data visualisation refers to the visual representation of data as a means of extracting insights from the data in a meaningful way to support decision making.

Visualisation is provided by SA Water's endorsed reporting, dashboard and visualisation platforms which include GE Proficy Historian®, OSi PI®, PowerBI®, Grafana®, Shiny® or the SA Water advanced analytics platform (Azure®).

8.4 Data sharing rules

Shared data is data that is shared within SA Water, or with external organisations or people, for a specific purpose.

The SA Water IoT Platform is an open platform for use by all IoT devices within the organisation and for facilitating the sharing of IoT device data across all business units. Access to the data is provided through SA Water's data access and sharing controls.

The sharing of IIoT data is required to follow the TS350 specifications.

Like SA Water corporate data sets, IoT/IIoT device data can be shared with external parties in accordance with SA Water's External Data Sharing Policy and associated approvals. Data can then be shared via the IoT platform.

The External Data Sharing requirements include stipulations such as:

1. Legal constraints and conditions and required permissions.
2. Restrictions around the appropriate use of the data.
3. Security and privacy issues to be managed.
4. The classification of the type and sensitivity of the data
5. A description of the controls required to mitigate the risks associated with the data being shared.

8.5 Network segregation

8.5.1 Background

Network segregation separates business IT traffic from SCADA OT traffic on SA Water's internal networks. Internal networks (SA Water Business and SCADA networks) run 'inside' SA Water's Edge firewall. Internal networks can be in SA Water data centres or at SA Water remote sites like depots, water treatment plants and telemetry sites. External networks, like the other SA Government departments' networks and the internet, run 'outside' SA Water's firewall.

SA Water's internal network types and their VRF designation (Cisco Virtual Routing and Forwarding instance which defines the network segregation) is shown below.

Table 8-1 - SA Water Internal Network VRF Designations

Internal Network Types	Location and Description	VRF
Business	Depot or Hub Office with Cisco Routers	SAW
SCADA	WTP, WWTP or Pump Station, etc (should be a control site only) with Cisco Routers or Sierra Routers	SCADA
Radio Telemetry	Radio Repeater Site (with dual uplinks to IP WAN networks) with Cisco Routers	RADIO
External Telemetry	Telemetry or control site with 4G Sierra routers	EXT-TELEM

It is critical SA Water only use the approved StateNet CDN internet gateway for all internet access for devices located on the internal networks. Un-authorised rogue internet routers connected to internal networks are not permitted (as defined by DPC's Conditions of Connection Policy).

IoT and IIoT field devices can have the below **uplink** connectivity types:

- Private SA Water managed WAN uplinks (e.g. 4G cellular, Fixed Line, LEO, etc).
- Private Third Party managed WAN uplinks (LPWAN / NBIoT networks); or
- Public WAN or Internet uplinks (e.g. 4G cellular, LEO, etc).

IoT and IIoT field devices can have the below **downlink** connectivity types:

- LoRaWAN (LoRaWAN does not use the Internet Protocol (IP), so TCP/IP network segregation is not directly applicable; or
- TCP/IP LAN networks.

IoT and IIoT field device uplink network and downlink networks need to comply with network segregation requirements.

8.5.2 Network segregation detail

IoT and IIoT projects **must** consult with:

- SA Water Technology Networks Team; and
- SA Water Solution Architecture Team (IoT, SCADA or Networks).

One of the above SA Water IT teams must explain the proposed IoT and IIoT network architecture to DPC-OCIO Governance if the architecture has not already been endorsed by DPC. **Early consultation is highly recommended to avoid project delays.**

This is conducted in two phases:

- Initial concept presentation; and
- Formal approval presentation.

For internally hosted IoT and IIoT field devices:

- IoT and IIoT LAN networks **must not** be connected directly to the SAW vrf, SCADA vrf and PLCR vrf LAN networks.
- IoT and IIoT LAN networks **must** be connected to the EXT-IOT vrf.
- IoT and IIoT cellular devices **must** be connected to the 4G Cellular networks TELSTRA vrf or OPTUS vrf. Note the TELSTRA vrf supports CAT M1 connectivity but OPTUS vrf does not.
- IoT and IIoT devices **must not** use any other SA Water WAN vrf.
- For IoT/IIoT devices that use 4G Cellular networks, these require a new unique APN sub-domain which **must** be used to logically separate the new IoT and IIoT WAN networks from other existing WAN networks.
- IoT and IIoT **should** use IPSEC or TLS encryption when connecting to the internal WAN networks.

Externally internet hosted IoT and IIoT field devices on the internet:

- **must** comply with DPC-OCIO conditions of connection to transfer data into SA Water internal networks. DPC-OCIO conditions of connections policies can be checked via the SA Water Technology Networks Team or an SA Water Solution Architect.
- IoT and IIoT devices **must** use IPSEC or HTTPS/TLS encryption when connecting to other internet services.

LoRaWAN gateway devices **must** use LoRaWAN channel separation to segregate IIoT and IoT data traffic.

Please consult SA Water Technology Networks Team to clarify any of the above requirements.

8.6 IoT Device position integrity

Positioning applications include mobile and stationary devices that communicate regarding their position, time, and status.

To communicate effectively, IoT/IIoT devices must be clear on the:

- datum in which they express their position.
- date and time that the dataset is measured; and
- quality of the data measured.

Location data must be compatible with SA Water's Geographic Information System (GIS) which is ESRI's ArcGIS®.

Refer to SA Water's Infrastructure Management team for further details.

8.7 Edge processing

Edge processing allows the devices to perform calculations before communicating results back to the application layer and therefore either push intelligence out to the Edge or reduce the amount of data to be communicated.

For devices with high frequency data reads (i.e. sub-second) or with large message payloads (i.e., audio or video data), Edge computing should be considered to reduce communication and storage costs.

Latency issues caused by large amounts of sensors trying to send data to the Cloud requires an architecture that allows for computing to occur at the Edge and not in the Cloud. Effective Edge computing reduces traffic, storage and costs whilst maximising the value of the data that is transmitted.

9 IoT systems management

The IoT/IIoT project is responsible for developing the IoT/IIoT Asset Management Plan (IAMP) to detail the ongoing maintenance and management of every component within a solution. The management plan for the specific project/solution is required to be stored in SA Water's Engineering Document Management System (Meridian).

The IAMP shall identify how each asset component will be managed over its lifecycle and what the trigger criteria should be for replacement (e.g. obsolescence, failure rate) repair and upgrade of assets. The Service Provider must inform the project of the product lifecycle of any specified components of an IoT/IIoT system.

A template for the IoT Asset Management Plan (IAMP) is available from the SA Water external website or the Principal Electrical Engineer, on request.

9.1 Device management

Device Management of IoT/IIoT devices refers to changing the operational status or configuration of the device. Where this is performed remotely it is known as Firmware-over-the-air (FOTA) for firmware updates or Configuration-over-the-air (COTA) for changes to the device's configuration settings.

SA Water require devices to be monitored and managed remotely.

Where IoT devices have actuating capabilities (i.e., the ability to interact with the underlying asset), this will be termed IoT Device Control. IoT Device Control should be available at the Application Level and should not be exposed via API and requires endorsement by relevant stakeholders (i.e., Operations Group).

If a device can be controlled locally (at the device level) there must be a means for preventing IoT device control by the public. This could be password protection, physical barriers, or HMI disconnects/interlocks. Refer to section 7 for Cyber Security requirements.

For IoT device controls that are only required at the time of commissioning, or otherwise very rarely (less than once/year), it is generally acceptable to limit the control to local mechanisms like a user interface on the IoT device itself, or from a mobile device over a Bluetooth® (or similar) connection.

For all IIoT device commissioning and configuration, a SCADA Change Request and Outage Notification is required.

IoT/IIoT device commissioning is required to adhere to SA Water's asset commissioning process using iAuditor® to record deployment details and test records.

9.1.1 Device configuration

All SA Water IoT and IIoT devices are required to be registered in the Asset Management platform (Maximo®) in line with the specified convention. This configuration allows the device to be connected to the IoT landscape and for the data to be ingested.

For all IIoT device configuration changes, a SCADA Change Request and Outage Notification is required.

9.1.2 Device maintenance

IoT/IIoT device maintenance shall be considered when specifying a system, such as how (and how often) devices need to be updated and whether they can be maintained easily.

Many aspects of the data collected relating to IoT/IIoT sensors can be used for maintenance purposes. This includes information such as who installed the device, who has access to repair it, when the battery life began, what keys are needed to access the device and the location of the device. This information is required to be captured in Maximo® on the 'IoT Asset' entity and is a mandatory requirement for all IoT/IIoT devices.

IoT/IIoT devices shall be able to be managed, monitored, and maintained at a component level. This capability shall be built-in to SA Water asset management systems (Maximo®) with the relevant metadata fields by the IoT Service Provider.

The SA Water Enterprise IoT platform shall provide device status information for all IoT/IIoT devices. This information is provided to through SA Water's IoT device health dashboard to allow technicians to be informed and to perform troubleshooting.

9.1.3 Software and firmware upgrades

IoT/IIoT solutions include software that will require bug fixes and software updates. Although these are generally conducted on an as-needed basis when updates are available, they may be required more urgently when security vulnerabilities are identified.

If numerous IoT/IIoT Service Providers have contributed to the manufacture of IoT/IIoT devices, these complex supply chains may make it difficult to receive software updates. Some components might be discontinued, meaning there is no owner responsible for providing updates. Care should be applied in the selection of devices and interfaces.

IoT/IIoT devices are required to support remote firmware updates or Firmware Over the Air (FOTA). Over-the-air updates allow an IoT/IIoT platform to track and monitor a device, maintain its software, manage firmware, fix bugs, add features, and customise devices even once the device has been installed in a network.

Key Patching Considerations:

- Patching must be applied taking into consideration the criticality of the device (sensor or actuator) and the criticality of the function the device performs. Patching requirements are based on SA Water's Cyber Security policy.
- Ensure the source of patching software is valid with MD5 download check.
- Devices and Gateways shall support the ability to report their firmware version to the application layer.

9.1.4 Disposal

Disposal of assets is required when assets reach their end-of-life.

The IoT Asset Management Plan shall detail the end-of-life planning for deregistration and disposal of devices and associated assets (e.g., batteries, solar panels, device certificates, etc.).

Device de-registration works in a similar manner to registration, including the requirements of revocation of security certificates and removal of devices from the platform.

10 Implementation of an IoT/IIoT solution

The IoT/IIoT solution is required to integrate with either SA Water's IoT platform, or the IIoT Proxy Service. Both provide the ingestion, storage, routing, and device management.

The implementation is therefore required to follow SA Water's IoT/IIoT process of:

1. Engaging the IoT Technical Working Group and relevant stakeholders.
2. Determining whether an IoT, IIoT, or OT solution is required.
3. Selecting candidate device and communications method (Including the recommendation report).
4. Drafting the IoT Asset Management Plan.
5. Obtaining endorsement for the devices and solution from:
    a. IoT/IIoT Technical Working Group.
    b. Architecture Governance Committee.
    c. Operations Group.
6. Procurement of the device(s).
7. Commissioning the device (including the metadata configuration).
8. Integrating the device with the IoT or IIoT platforms.
9. Finalising the IoT Asset Management Plan (including acceptance of the plan); and
10. Transitioning to production (including operational cost model).

10.1 Research and proof of concept requirements

The selection of any new IoT/IIoT devices is required to follow SA Water's device procurement process. This process requires the key information relating to the problem/opportunity to be specified. Where a device is required and a market scan is conducted, an evaluation is required in a non-production, isolated environment to ensure the device:

- meets the functional and non-functional requirements of the project and complies with this specification (TS0351);
- is compared with the existing endorsed list of devices to avoid duplication; and
- identifies any deviations from the requirements.

key information required before considering selection of a device includes:

- The location of the devices (now and with potential future deployments);
- The type, volume, and frequency of data to be communicated;
- The proximity of devices to each other (i.e., will multiple devices be deployed within 10km of other devices);
- The business criticality of the data from the devices; and
- The reputation of the provider, their ability to support the device and the stability of the supply chain.

10.2 Identification of suitable devices and services

The selection of IoT/IIoT devices and services needs to evaluate the following:

1. Speed/latency (poor to good)
2. Volume handling of data (small to large)
3. Frequency of data reading
4. Frequency of data communication
5. Security of device, communication, and software (poor to good)
6. Cost (low to high)
7. Complexity of implementation (simple to complex)
8. Complexity of maintenance (simple to complex)
9. Availability of devices (limited to plentiful)

10.3 Definition of support requirements

All IoT/IIoT systems shall have a Service Level Agreement (SLA) in place for the device and a resilience classification for the network, communications and the application.

The SLA shall define the required performance and reliability targets and agreed fault restoration targets. This shall be recorded in the IoT Asset Management Plan.

The resilience requirements are defined within the SA Water Technology Resilience framework. The **resilience ratings** required are expressed in terms of availability ratings in Table 10-1.

Table 10-1 - Resilience Rating Table

Availability (Tier) Uptime (SLA)	Description	Technology	Maximum outage time per event (approx.)	Typical Response
A4 99.95%	ABSOLUTE requirement, meaning that the business would be crippled by the loss and recovery must be virtually instantaneous (no longer than a few minutes).	OT	20 minutes	Within minutes
A3 99.5%	HIGH requirement, meaning that loss would cause major disruption to the business and full service restoration must be achieved within a period measured in hours.	IIoT	4 hours	Within hours
A2 98%	MODERATE requirement, implying the loss would have a significant impact and full service restoration must be achieved within a period measured in days.	IoT	3 days	Within 1 day

The support model shall:

- outline how the device vendor will meet the required device SLAs;
- align with SA Water's existing IoT and OT support processes;
- summarise the additional support costs that need to be contributed to each support team; and
- summarise the required interactions between each support team (i.e., support ticket flow).

Once again, this information should be documented in the IoT Asset Management Plan.

10.4 Training and skill development

Any new IoT/IIoT solution or major update is required to provide appropriate training for deployment, administration, and support teams. This is required to be delivered by the implementation project.

10.5 Device deployment rules and configuration

The commissioning of IoT/IIoT requires SA Water's process to be followed which includes the capturing of the installed device within the iAuditor application and its metadata configured within Maximo®.

Deployment or installation of an IoT/IIoT solution or device shall comply with relevant regulatory requirements. Common regulatory requirements are listed in Table 10-2 (this is not an exhaustive list).

Table 10-2 - Device Deployment Regulations Guide

Regulatory requirements	Information
Business	Australian Communications and Media Authority (ACMA) - radiocommunications standards
SCADA	Australian Communications and Media Authority (ACMA) – radiocommunications licensing
Radio Telemetry	Australian Communications and Media Authority (ACMA) – telecommunications standards
External Telemetry	Australian Communications and Media Authority (ACMA) – Telecommunications (Mobile Equipment Air Interface)
Electrical safety	Technical Standard TS0300, which quotes a number of Australian Standards and regulatory requirements.