

CITY OF MINNETRISTA



CITY COUNCIL AGENDA ITEM

Subject: Itron Temetra Meter Reading Software Upgrade

Prepared By: Jasper Kruggel, City Administrator
Gary Peters, Public Works Director

Meeting Date: October 5, 2026

Issue: The Itron Field Collection System (FCS) software the City uses to read water meters is reaching end-of-life and must be replaced in 2027. Staff are requesting City Council approval of a proposal from United Systems & Software, Inc. (USS) to upgrade to Itron Temetra, in the amount of \$37,510 plus shipping, with implementation beginning in January 2027.

Background: Staff previously presented this item to the City Council to outline the software transition and to solicit questions before bringing forward a formal agreement. As noted at that time, the City's Itron meters are required to use Itron Temetra, so there are no alternate software solutions. The City currently uses Itron FCS for Automatic Meter Reading (AMR), in which meters are read by drive-by collection. Temetra supports both AMR and Advanced Metering Infrastructure (AMI) meter reading, allowing the City to continue reading its existing meters by drive-by while adding cellular AMI meters over time.

Proposal Overview: USS, the City's Itron distributor, submitted the attached proposal on September 18, 2026. The proposal includes the following:

Item	Provider	Cost
Temetra Advanced annual subscription (up to 2,500 endpoints, 5-year data storage, customer portal)	Itron	\$5,250.00
AMI Essentials gateway update	Itron	\$9,260.00
Training, technical services, integration with the City's utility billing (CIS) system, and testing (40–48 hours, remote)	USS	\$10,000.00
126 cellular AMI ERTs for new construction and high-usage irrigation meters (2027/2028 inventory)	USS	\$13,000.00
Total (excluding shipping and sales tax)		\$37,510.00

The Temetra subscription covers up to 2,500 endpoints, which accommodates the City's approximately 2,350 water meters with room for growth.

Ongoing Costs: In 2026, the City paid \$6,621.34 for the annual Itron FCS software fee. The previous estimate placed ongoing annual costs for Temetra, including software and

Mission Statement:

The City of Minnetrista will deliver quality services in a cost effective and innovative manner and provide opportunities for a high quality of life while protecting natural resources and maintaining a rural character.

cellular data fees, at approximately \$9,073.61, an increase of roughly \$2,450 per year. Cellular data fees are approximately \$6.96 per AMI ERT per year, so ongoing costs will increase gradually as AMI ERTs are installed.

AMI Features: The Itron Cellular 500W AMI ERT connects directly to the Verizon and AT&T cellular networks, so no City-owned collection towers or network equipment are needed. Key features from the attached Technical Reference Guide include:

- 15-minute interval usage data, transmitted to the City four times per day (every six hours)
- Alerts for high flow, continuous flow (potential leaks), reverse flow (backflow), tampering, and low battery
- A 20-year expected battery life under the recommended configuration
- A backup local radio signal, allowing staff to read the meter in the field if the cellular connection is temporarily unavailable

These features address the high-usage cases the City has encountered, where issues were not detected until a substantial amount of water had passed through the meter. With the transition to monthly billing, AMR meters will still only identify high usage once per month, while AMI meters would identify it within hours.

Security: Staff asked USS to address the security of the cellular AMI ERTs. According to Itron and USS:

- The ERTs communicate over the existing Verizon and AT&T cellular networks, which use their own encryption and authentication protocols to protect data.
- Meter data is encrypted, and any command sent to an ERT must be digitally authenticated before the device will act on it.
- Itron's enhanced security is always on when the ERTs operate on the cellular network; it cannot be turned off. USS describes the encryption as bank-level, 256-bit encryption, which is used because these ERTs are capable of operating remote water shut-off valves.

Implementation: If approved, implementation would begin in January 2027, including software setup, integration with the City's utility billing system, and staff training. The initial 126 AMI ERTs would be installed on new home builds and any other irrigation meter that would benefit from more frequent readings. Existing AMR meters would continue to be read by drive-by through Temetra.

The proposal is valid for 60 days from September 18, 2026, and USS has indicated that price increases are expected for 2027. Invoices are due on a net 10-day basis.

Future Consideration: This proposal does not include converting the City's remaining approximately 2,224 AMR meters to AMI. Staff previously estimated a full conversion at approximately \$400,000 in one-time ERT hardware and installation costs, plus

Mission Statement:

The City of Minnetrista will deliver quality services in a cost effective and innovative manner and provide opportunities for a high quality of life while protecting natural resources and maintaining a rural character.

approximately \$15,500 per year in cellular data fees. Staff will continue to evaluate the pace of any future conversion as part of future budgets.

Brad Bersch, Senior Account Manager with USS, will be present to answer questions.

Next Steps: Staff are seeking City Council approval of the United Systems & Software, Inc. proposal to upgrade to Itron Temetra in the amount of \$37,510, plus shipping, with implementation beginning in January 2027.

Attachments:

- United Systems & Software, Inc. Itron Temetra Upgrade Proposal (September 18, 2026)
- Itron Cellular 500W Module Technical Reference Guide

Mission Statement:

The City of Minnetrista will deliver quality services in a cost effective and innovative manner and provide opportunities for a high quality of life while protecting natural resources and maintaining a rural character.



P.O. Box 547, 91 Southwest One Blvd, Benton, Kentucky 42025
Phone: (270) 527-3293 • Toll-Free: 1-800-455-3293
FAX: (270) 527-3132 • www.united-systems.com

United Systems & Software, Inc. (USS) is an information technology firm that specializes in serving the automation needs of utilities and local government. Founded in 1977, USS now serves over 1500 customers within a 30 State region. Since 1999, United Systems has been recognized as a distributor of Itron's Automatic Meter Reading/AMI technology, and we appreciate this opportunity to propose an Itron solution.

Proposal For: Jasper Kruggel
City Administrator

Sept. 18, 2026

City of Minnetrista
7701 Co Rd 110W
Minnetrista, MN 55364

P: 952-446-1660
E: jkruggel@cityofminnetrista.gov

Quotation: Itron Temetra Upgrade with Cellular Smart Start Promo

Quantity	Description	Cost	Invoice From	Note
1	Temetra Advanced, UP to 2500 Endpoints, 5-Year Data Storage, Customer Portal, Annual Subscription	\$5,250.00	Itron	Update Project
1	AMI Essentials G/W Update	\$9,260.00	Itron	Update Project
1	40-48 Hours of Training, USS Remote Technical Services, Integration into CIS, Testing and Training	\$10,000.00	USS	Training for Update Project
126	ERTs for new construction and high usage irrigation meters	\$13,000.00	USS	2027/2028 Inventory of ERTs

General- Prices do not include shipping and/or sales tax (if applicable).

Thanks for the opportunity.

Brad Bersch

Senior Account Manager
UNITED SYSTEMS & SOFTWARE, INC.
O: 800.455.3293 ~ M: 262.328.7241
E: bradb@united-systems.com

General— Unless specifically stated to the contrary, prices do not include shipping and/or sales tax, if applicable. Likewise, this quotation does not include technical services related to setup, installation & configuration of proposed items unless specifically stated above. All related invoices shall be paid on a Net 10 Day basis. This quotation shall remain firm for sixty (60) days from the quotation date or prior to calendar year-end, unless modified in writing by USS prior to USS acceptance. Price increases are expected for the ensuing calendar year.



Itron Cellular 500W Module Technical Reference Guide

For OpenWay Riva Network and UtilityIQ Gen6 Network

Copyright © 2025 Itron Inc. All rights reserved.

Confidentiality notice

Confidential information of Itron Inc., provided under nondisclosure obligations. The information contained herein is proprietary and confidential and is being provided subject to the condition that (i) it be held in confidence except to the extent required otherwise by law and (ii) it will be used only for the purposes described herein. Any third party that is given access to this information shall be similarly bound in writing.

Trademark notice

Itron® and the Itron logo, Gen, OpenWay, Riva, and UtilityIQ are registered trademarks of Itron Inc. in the United States and/or other countries and regions.

All other product names and logos in this documentation are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

For more information about Itron trademarks, go to [Itron's Trademarks and Brands](#).

Limitations

While Itron strives to make the content of its materials as timely and accurate as possible, Itron makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of, and expressly disclaims liability for errors and omissions in, such materials. No warranty of any kind, implied, expressed, or statutory, including but not limited to the warranties of non-infringement of third-party rights, title, merchantability, and fitness for a particular purpose, is given with respect to the content of product documentation.

Contact us

For more information about Itron or Itron products, go to:

Email: support@itron.com

Itron Customer Center: customer.itron.com

Products and documentation: products.itron.com

Itron Technical Support North America: 1-877-487-6602

For regional technical support, go to www.itron.com and select your country and language.

For suggestions, questions, or other feedback concerning Itron product documentation, contact us at: ItronDocumentation@itron.com.

Contents

New in this document	5
1 Introduction	6
About this document	7
Related documents	7
2 Operating, transmitting, and receiving	9
Transmit and receive cycle	9
Network mode	10
Data collection and transmission	11
Mobile mode	13
On the OpenWay Riva network	13
On the Gen6 network	13
Data collection and transmission	14
Local receive operations	16
Retry algorithm and registration	16
Operating modes	17
3 Time management	19
4 Security	20
On the Gen6 network	20
On the OpenWay Riva network	20
Mobile and network mode security fundamentals	21
Key and certificate types	21
Manufacturing and installation	23
Secured operations	24
5 Operational life	26
Operational and network impacts to battery life	26
Operational impacts	26
Network impacts	27
6 Standard device configuration and usage	28
7 Registration	30
8 Programming and reading	31
Default values	31
Programming parameters	31
Manufacturer system parameters	32

- Utility system parameters 32
- Meter-specific parameters 34
- Programming modules 34
 - Best practices and considerations 35
 - Itron programs and software variables 36
- 9 Meter display and encoding consumption data 37**
 - Status, events, and alarms 37
 - Tamper counters 38
 - Battery low warning 38
- A Events and alarms 40**

New in this document

Table 1 Revision history

Revision	Date	Description
REV 006	November 3, 2026	■ Updated to include modules compatible on a Gen6 network ■ Title changed from <i>OpenWay Riva Itron Cellular 500W Module Technical Reference Guide</i> to <i>Itron Cellular 500W Module Technical Reference Guide</i>. Information about modules compatible on a Gen6 network were previously tracked under document part number LDI-0765, title <i>Itron Cellular 500W Module Technical Reference Guide</i>. ■ Updates to Time management on page 19
REV 005	May 19, 2025	■ Updates to Operating modes on page 17 ■ Updated Standard device configuration and usage on page 28 ■ Updates to Waking up and programming from factory ship mode on page 35 ■ Updates to Events and alarms on page 40 ■ Reorganized content to improve flow of information. ■ This document was previously titled <i>Cellular 500W Module Technical Reference Guide</i>. It is now titled <i>OpenWay Riva Itron Cellular 500W Module Technical Reference Guide</i>.
REV 004	May 26, 2023	Updates to Data collection and transmission on page 11 .
REV 003	December 14, 2022	Updates to Data collection and transmission on page 14 .
REV 002	November 22, 2022	Added Events and alarms on page 40 .
REV 001	November 21, 2022	Minor updates to improve quality of content. No technical changes.
REV 000	September 15, 2022	First date of publication.

1

Introduction

The Itron Cellular 500W Module (from here forward referred to as "500W Module") is a cellular radio frequency (RF) transmitting module that attaches to water registers or meters to collect consumption usage, event, and alarm data. It is an IPv4- or IPv6-compliant endpoint and supports either Itron's Gen6 or OpenWay Riva solution, transmitting in network mode or mobile mode. This document describes 500W Modules on both networks. In many respects, the modules' behavior and features are the same; when a module's behavior is dependent on the network to which it is deployed, it is specified.

500W Modules are designed with the following characteristics:

- **Cellular device.** In network mode, the module is a cellular radio device that attaches to a water meter to collect usage (consumption) data and alarm or event (tamper) alerts. The module encodes and transmits the data and alerts to the Itron Mobile Radio (IMR) or head end. The module records consumption by either retrieving a consumption register value directly from an electronic encoded meter, or by counting the number of times the index rotates. The number of rotations indicates the amount of water consumed. The 500W Module uses two radios: a 900 MHz radio for communicating to the IMR when using Itron Field Tools and a cellular radio when communicating to the head end over the cellular network.
- **Data logging.** The module stores and logs the hourly consumption data. In mobile mode, the 500W Module stores the preceding 40 days of hourly data. In network mode, the 500W Module stores a network-specific number of configurable buckets:

Table 2 Configurable buckets by network

Network	Number of configurable buckets	Equates to
OpenWay Riva	3,840	160 days of hourly data or 40 days of 15-minute interval data
Gen6	5,952	248 days (8 months) of hourly interval data or 62 days of 15-minute interval data

- **Security.** The Itron Security Manager (ISM) offers enhanced network security with authentication and encryption when the module is accessed in the field using Itron Field Tools or FDM Tools (FDM Tools is only supported on modules deployed in an OpenWay Riva network). For network operations on the Gen6 network, link layer security protects a network by denying access to it if a device cannot be authenticated.

The 500W Module communicates with its head end system by:

- **Encoding.** 500W Modules record consumption and alarm/event information and encode that information.
- **Receiving.** 500W Modules receive radio signals for module programming, reads, and commands.
- **Transmitting.** 500W Modules transmit encoded information to an Itron Mobile Radio (IMR) or head end system.

About this document

This document provides information about 500W Modules for field dispatchers, utility personnel, Itron personnel, and customers. This guide includes descriptions of the features and functionality of the 500W Modules and focuses on the high-level network architecture, system operations, theory supporting IoT technology, and supporting software.

Related documents

The following documents may be of use to you. All documents can be viewed and accessed at <https://customers.itron.com/products>.

- *Battery Life in Itron Cellular 500G, 550G, and 500W Modules*
- *Field Tools Help*
- *Itron Cellular 500W Module Spec Sheet*
- *Itron Mobile Radio (IMR) Quick Reference Guide*
- *Itron Mobile Radio (IMR) User Guide*
- *Itron Security Manager (ISM) User Guide*
- *Itron Cellular 500G/550G Module Ordering Guide*
- *Water Meter and Telemetry Module Compatibility Matrix*
- For modules running on an OpenWay Riva network:
 - *FDM Tools Mobile Application Online Help*
 - *OpenWay Collection Manager Device Interface Guide*
 - *OpenWay Collection Manager User Guide*
- For modules running on a Gen6 network:
 - *Advanced Metering Manager (AMM) Events*
 - *Advanced Metering Manager (AMM) User Guide*
 - *Gen6 Cellular Troubleshooting Guide*

- *UtilityIQ Installation Guide*
- *UtilityIQ Security Overview*

2

Operating, transmitting, and receiving

500W Modules are IPv4 and IPv6 open-standards based and are designed to be read over the cellular network (the use of IPv4 or IPv6 over the cellular network is dependent on the cellular access point name [APN] used). The module converts consumption or status data to a cellular transmission, providing an efficient solution for collecting utility meter reading data without requiring a field technician physically inspect each individual installation location. The 500W Module transmits in either network mode or mobile mode. When in network mode, the module can be read over a cellular network. When in mobile mode, it can be read locally by an IMR or Mobile Collector. This section describes the reading cycles used to collect monthly data or status reads while in these modes.

Note: The communication features described in this chapter may be dependent on the firmware version. For more information about firmware, see the *Itron Cellular 500W Module Ordering Guide*.

Note that the 500W Module's transmit and receive behavior is determined by its operating mode: factory ship mode, audit mode, meter quiet mode, or run mode. These modes are described in detail in [Operating modes on page 17](#). However, run mode is the 500W Module's most commonly used operating mode and is the mode that supports the focus of this chapter.



Caution: Switching between operating modes (network to mobile or mobile to network) results in a loss of interval data. The consumption register reads are not affected.

Transmit and receive cycle

The module's cycle of encoding, transmitting, and receiving support a two-way messaging structure to transmit data in response to requests from data collection devices.

The Itron Cellular 500W Module reading cycle is outlined in the following steps.

1. The Itron Cellular 500W Module collects consumption data from a water meter.

When connected to an encoded meter, the module interrogates the water meter once, at the top of each interval period, to collect consumption and alarm data.

When connected to a pulse meter, the module counts the number of pulses the water meter outputs.

2. The 500W Module transmits meter reading and status data to an IMR, Mobile Collector, or the head end. When in network mode, the meter reading is transmitted using point-to-point cellular connection, so data collection reads are obtained from all meters in a neighborhood in a very short time.

3. The data is uploaded and stored in the module's head end system. Customer bills are calculated and generated from the gathered data. Status information is also available in the data upload.

Instead of a meter reader visually reading the meter and recording data, the 500W Module can operate in two different fundamental operating modes to deliver that data to application software – mobile mode and network mode. The module transmits its meter reading data using point-to-point cellular connection, so data collection reads are obtained from all meters in a neighborhood in a very short time.

Network mode

The 500W Module communicates to the head end over cellular LTE-M CAT-M1 networks using the following 3GPP regulated and licensed industrial, scientific, and medical (ISM) radio spectrum bands:

- **Verizon Wireless®**. Band 13 and 4
- **AT&T®**. Bands 2, 4, and 12

The 500W Module also sends a local RF access (network contingency) beacon every 60 seconds that allows users to gather local readings locally when needed. For local RF access transmissions (local reads), the 500W Module utilizes the unlicensed 902 to 928 MHz ISM frequency band and does not require a Federal Communications Commission (FCC) license.

The cellular module's head end system (OWCM for OpenWay Riva networks or UtilityIQ for Gen6 networks) allows users to choose between two cellular connection methods:

- **Power Save Mode (PSM)**. High battery life, longer communication latency
- **Extended Discontinuous Reception Mode (eDRX)**. Modest battery life, shorter communication latency

The difference between these two cellular connection methods is in the timing of interactive communication that can be initiated between the head end and the 500W Module. When PSM is disabled (that is, eDRX is enabled), the head end can communicate more frequently with the device, but the increased availability of the device comes at the expense of battery life. For more information about PSM on 500W Modules, see [Cellular modes on page 12](#).

Regardless of the cellular connection method, devices can be configured to automatically push data to the head end on a recurring schedule (called a "push schedule"), which eliminates the need for scheduled Interrogation Jobs. The configuration group defines the push schedule. The scheduled push is the primary mechanism used to deliver regularly collected data (interrogation data) from the device to the head end.

Data collection and transmission

In network mode, the module wakes up and transmits its data over the cellular network to the head end at specified times (typically four times per day). The head end can also transmit either a scheduled interrogation read request or an individual on-demand read request to the module over a point-to-point cellular connection. The module receives and confirms the request and transmits the requested (collected) data to the head end for storage or presentation by the head end.

The 500W Module transmits and receives data based on the configuration set up in the head end and module settings programmed at manufacturing. Configuration of read requests depends on the 500W Module's firmware version and head end of read configuration. For more information about firmware, see the *Itron Cellular 500W Module Ordering Guide*.

Interval data

The 500W Module supports a different number of native intervals depending on your module's network:

- 3,840 native intervals for modules on an OpenWay Riva network. When configured for hourly data collection, this translates to 160 days of hourly data.
- 5,952 native intervals for modules on a Gen6 network. When configured for hourly data collection, this translates to 8 months of hourly interval data.

The module's default configuration specifies 15-minute interval configuration, as this is the most common use case. Optionally, the 500W Module features customer-configurable interval data options of 5-, 15-, 30- and 60-minute data intervals. This increased granularity supports load studies and enables utilities to conduct detailed investigations.

Head end data collection

Typical data collection occurs through the cellular network, with the module waking up at specified times to transmit data to the head end system. Modules are designed to transmit several times a day, based on a schedule determined by the utility, while retaining their 20-year battery life. Itron recommends four schedule-determined reads per day; higher rates are supported with dependencies on battery life. The scheduled collection of data is referred to as the "push schedule." Push messages can include data such as meter register value or events and alarms such as communication errors, reverse flow, high flow, and low battery.

Local data collection

Local data collection, which is most commonly used for troubleshooting or to collect data if the module temporarily has trouble connecting to the network, is also supported using Itron Field Tools or FDM Tools using an IMR. The 500W Module sends a local RF access (network contingency) beacon every 60 seconds that allows users to gather readings

locally when needed. For local RF access transmissions (local reads), the 500W Module utilizes the unlicensed 902 to 928 MHz ISM frequency band and does not require an FCC license.

For more information about reading devices for your system or hardware and software requirements, reference the appropriate product specification sheet.

Cellular modes

Itron cellular modules typically operate in either eDRX mode or PSM.

When operating in eDRX mode, cellular modules replace the traditional transmit/receive cycle with eDRX cycles. These cycles enable uplink and downlink communications on a defined and configurable schedule, typically every 10.92 minutes by default when in eDRX mode. Each eDRX cycle corresponds to a wake cycle in the head end system. During these cycles, the module "wakes" to transmit and receive data. The reachability of the module, that is, its ability to associate with and be recognized by the network for head end transmissions, is coordinated between the head end and the carrier's back office, based on the defined eDRX schedule.

PSM is a low-power operational mode used by cellular IoT modules, including those based on CAT-M1 and NB-IoT technologies. In PSM, the module remains in a sleep state for extended periods to conserve battery, waking infrequently to send data or perform scheduled tasks. Modules default to PSM for battery conservation purposes. Factory and field configurations determine wake-up frequency, balancing data freshness with battery longevity. Unlike eDRX mode, the network cannot communicate with the module at will during PSM; it must wait until the module wakes and initiates contact.

In both PSM and eDRX modes, cellular modules are configured to push data at scheduled intervals, several times per day. The module autonomously wakes itself to initiate mobile-originated communication with the head-end system. After transmitting a message, the modem remains awake for a short, configurable period (typically 16 seconds) to allow for any downlink communication from the network.

During normal operation, modules default to PSM to maximize battery efficiency. However, for operations requiring rapid response, such as registration, firmware downloads, or reconfiguration, the module automatically switches to eDRX, then reverts to PSM once the task is complete.

Operational considerations

- **Communication timing.** The head end system can only communicate with a module in PSM during its active period immediately following a push message.
- **Event handling.** If the module is reconfigured from push to pull mode but the head end system is not configured to periodically pull data from the device, the device may issue a "No Comms" event after a defined period (approximately 16 hours).

- **Randomization.** Wake-up and push times are randomized within a defined window to reduce network congestion.

Transmission rates, power, and battery life

Transmission output power and associated module battery life for network mode is summarized in [Table 3](#).

Table 3 Network mode transmission details

Transmission mode	Transmission rate	Approximate conducted output power	Battery life
Network mode (local port)	N/A	+10 dBm (10 mW) beacon +16 dBm (40 mW) responses	Dependent on configuration
Network mode (Cellular modem)	N/A	+23 dBm (200 mW)	Dependent on configuration

Mobile mode

Modules behave differently in mobile mode depending on the network to which they are deployed.

On the OpenWay Riva network

In mobile mode, the module transmits (bubbles up) a message every 15 seconds. This message contains the current register read, or standard consumption messages (SCM+) and is transmitted over multiple RF channels to report on:

- Meter register value
- Cut cable or communication error event
- Reverse flow (encoder version selected)
- Consumer leak status
- Low-battery indicator

On the Gen6 network

In mobile mode, the Itron Cellular 500W Module transmits (bubbles up) a message on an average of every 15, 30, or 60 seconds depending on the mobile mode submode (described later in this section). This message contains the current register read, or SCM+. An IMR receives the data in the SCM+, which contains the following data:

- Module ID
- Module type

- Meter reading (register) value
- Event and alarm values

Note: This is a limited list of the functionality of the 500W Module. Additional functionality, events, alarms, and thresholds are supported. See [Events and alarms on page 40](#) for more information.

If pre-programmed to wake into mobile mode, the 500W Module starts bubbling up SCM+ messages when it is taken out of factory ship mode. The SCM+ message enables larger data fields with event and alarm status information in the expanded beacon that allows modules to communicate data such as a battery status indicator.

Mobile mode has several submodes it can be configured to:

- **Mobile high power mode.** The 500W Module transmits a high-powered RF message every 60 seconds.
- **Mobile and handheld mode.** The 500W Module transmits a medium-powered RF message every 15 seconds.
- **Hard to read mode.** The 500W Module transmits a high-powered RF message every 30 seconds. This mode should only be used for exceptionally difficult to read installations, for example, meters installed in sub-basements.

When an IMR receives an SCM+ message, it can optionally request more historical information from the 500W Module, including the following read requests:

- **Read one day of hourly interval data.** This request prompts the 500W Module to return one day of hourly interval data ending at the specified hour offset. The hour offset is the number of hours back from the current hour.
- **Read 40 days of daily interval data.** This request prompts the 500W Module to return 40 days of daily interval data measured at the specified hour offset. The hour offset is the number of hours back from the current hour.
- **Read 40 days of hourly interval data (960 intervals).** This request prompts the module to return 40 days of hourly interval data for the hours specified. Due to the amount of data requested, the 500W Module sends this data in multiple packets. This request method requires a multi-packet message (more than one response).



Caution: Modules running on an OpenWay Riva network may experience loss of interval data if you perform a mode switch (network mode to mobile mode or mobile mode to network mode).

Completion of a switch from mobile mode to network mode clears the interval data and reading history.

Data collection and transmission

When 500W Modules are programmed to mobile mode, regular data collection is performed using Itron mobile reading systems to leverage existing reader investments and

allow utilities to mix AMR 500W and 100W+ endpoints while the utility moves to an IoT networking solution.

Data collection is supported using Field Tools or FDM Tools using an IMR. The 500W Module transmits on 1 of 50 channels it picks pseudo-randomly. If there are several 500W Modules in close proximity, it's likely that two 500W Modules could transmit at the same time. Even though two 500W Modules could transmit at the same time, it's most likely that they do not transmit on the same channel. To eliminate the likelihood of transmissions ending up on top of each other repeatedly, the transmit time is varied randomly by ± 2 seconds. For example, in mobile and handheld mode, the 500W Module bubbles up every 13 to 17 seconds.

The frequency (channel) hopping and time dithering combined with the bubble-up rate and the likelihood of being in range to receive multiple messages provide for highly reliable communication between the 500W Module and the data collection method.

For more information about reading devices for your system or hardware and software requirements, reference the appropriate product specification sheet.

Interval data

The 500W Module continually stores and updates the last 40 days (960 buckets) of hourly interval data. As the module collects new data, it overwrites the oldest interval data such that the most recent intervals are preserved.

To transmit daily or hourly interval data, the 500W Module receives a specific request from the IMR. When it sends interval data, the 500W Module sends the index reads at the end of the interval set.

The total consumption sent in an interval packet is the same as the SCM+ (adjusted for pressure compensation, rate multiplier, and initial consumption), but the reading is not adjusted for rollover. Intervals are sent as a raw count value. The multiplier, pressure compensation, and rollover values are included in the message.

To calculate the value at a prior interval, the reader can sum the subsequent interval values and then apply the rate multiplier and compensation to get a consumption offset.

The consumption offset can be subtracted from the total sent consumption with the remainders adjusted for rollover. This approach eliminates complex or time-consuming math in the 500W Module and transfers it to the reader, where more powerful resources can process the data.

Transmission rates, power, and battery life

Transmission output power and associated module battery life for mobile mode is summarized in [Table 4](#).

Table 4 Transmission in mobile mode

Transmission submode	Transmission rate	Approximate conducted output power	Battery life
High power mobile mode	60 seconds	+16 dBm (40 mW)	20 years
Mobile/handheld mode	15 seconds	+10 dBm (10 mW) beacon +16 dBm (40 mW) responses	20 years
(Optional) Hard to read Mobile/Handheld mode	60 seconds	+16 dBm (40 mW)	20 years

Note: Optimum battery life is dependent on the device operating in a standard configuration. For standard configuration settings, see [Standard device configuration and usage on page 28](#).

Local receive operations

The 500W Module receives commands in the Industrial-Scientific-Medical (ISM) 900 MHz band. When 500W Modules are manufactured, they are left in factory ship mode with the transmitter off. While modules are in factory ship mode, the receiver turns on every four seconds to listen for a command from FDM Tools (**Program Endpoint** or **Check Endpoint**) or Field Tools (**Check**).

Note: FDM Tools is supported only on modules deployed in an OpenWay Riva network.

In a run mode, the 500W Module responds to a specific command from the IMR. The IMR transmits a command during the time the module has its receiver on. The module must conserve power, so its receive time is set to a minimum. The module leaves its receiver on just long enough to detect a command. When a command is heard from an IMR, the cellular modem is turned off and a 12.5-minute timer is set. The timer is refreshed (reset to 12.5 minutes) whenever a local command is received. If the timer expires (reaches zero), the cellular mode is turned back on and the device will attempt to join the cellular network again.

Retry algorithm and registration

In network mode, the 500W Module network is provided by Tier 1 cellular mobile network providers, such as Verizon Wireless and AT&T. The cellular modules are designed to operate on these licensed and 3GPP regulated networks.

The 500W Module can be ordered to wake from factory ship mode in either network mode or mobile mode. The default setting for the 500W Modules is to wake in network mode. If ordered in mobile mode, the devices can be locally configured to network mode via FDM or Field Tools at the time of installation or at a later time.

In network mode, the 500W Module can be configured to automatically wake when it detects consumption from the attached meter. The 500W Modules are shipped pre-

activated to the carrier's cellular network, and automatically register to the cellular network when installed in the field (based on the "wake on use" configuration).

In typical cellular conditions, the 500W Module registers with the cellular network within approximately 30 minutes and then attempts to register with the head end. In challenging cellular connectivity environments, the 500W Module could either fail to initially find the cellular network or exceed daily battery usage limitations in trying to register with the network. This can extend the head end registration time.

These modules continue to attempt to register with the cellular network. However, to limit battery utilization and reduce congestion in the network with these repeated attempts, the module implements a back-off window and randomizes the registration attempts. The back-off window algorithm gradually increases the time in between registration attempts. These durations are determined by the failure type and amount of battery used, and can range between a few minutes to two hours. Between these longer back-off times, the cellular modem may be put into a low-power mode to conserve battery and wait for better network conditions.

The 500W Module attempts network connections until ultimately successful, but if a module continually struggles to register with the cellular network, the module remains available for reads locally using Itron Field Tools or FDM Tools. This method can be used to either troubleshoot the installation or obtain reading data from the device.

Modules that remain unable to connect to the network should be investigated for additional mitigations, such as replacement or return material authorization (RMA), secondary carrier variant installation, or carrier network support and troubleshooting.

Operating modes

The module's operating mode determines its transmit and receive behavior. The 500W Module has the following operating modes:

■ Factory ship mode

- Modules are shipped from the factory in factory ship mode.
- The module's transmitter is turned off.
- The module's receiver listens for a programming command.
- Modules attempt to read the register every hour.
- Register Error Detected and Register Error alarm or event flags may be set when a register is not connected.
- If the 500W Module reads a connected register, the module automatically moves to run mode.
- The module can be configured via an FDM snapshot file to wake from factory ship mode to run in either network mode or mobile mode.

■ Audit mode

- Audit mode reduces the normal read latency time associated with standard modes of operation and is often used after initial installation.
- This mode is useful in network installations where the normal bubble rate is very slow.

■ Run mode

- The 500W Module can be configured in the factory through an FDM snapshot file to transition to run mode only after seeing positive consumption from a meter.
- The 500W Module's typical operation mode.
- In network mode, the module's transmission operation is dependent on the loaded configuration.
- In mobile mode, the SCM+ bubble-up rate and power are dependent on its programming at install.
- In mobile mode, the 500W Module's default bubble-up rate is 15 seconds.

■ Meter quiet mode

- Meter manufacturers can configure the 500W Module for quiet mode after programming and direct mounting the 500W Module in a factory.
- The remote 500W Module is awakened from meter quiet mode and enters run mode in one of two ways:
 - The 500W Module is connected to a meter and there has been positive consumption of the least significant dial greater than two.
 - Receiving a two-way command, such as a **Check Endpoint** command (using FDM Tools) or **Check** command (using Field Tools).

If a 500W Module installed in meter quiet mode is not bubbling up SCM+ messages, it may be due to zero consumption on the module, such as in the case of a vacant or vacation home. Initiate a two-way command (for example, perform a **Check Endpoint** command (using FDM Tools) or **Check** command (using Field Tools) to test for normal functionality before removing the unit.

3

Time management

The 500W Module maintains a Coordinated Universal Time (UTC) 24-hour clock. At the application layer, this clock is used for timestamping all data collected within the device.

The module obtains its network clock time (network time) from the cellular tower during registration with the cellular network. This synchronization occurs every time the device registers with the tower. If the device has not registered within the last 30 days, it initiates a forced registration to ensure the time is set at least once every 30 days, provided it is connected to the cellular network. This update frequency is designed to balance battery preservation with minimal clock drift.

The maximum expected drift is ± 26 seconds over a 30-day period. In mobile mode, when the device is read monthly, the maximum time drift is less than ± 5 minutes per month.

Application time is slewed to match network time at a rate of 15 seconds per minute, with a maximum adjustment of ± 6 hours per day.

Events and flags are generated on intervals when slewing between network time and application time exceeds a user-configurable threshold. Depending on your network type, this threshold is configured using Itron Device Configuration Manager (IDCM) for Gen6 networks, or OpenWay Collection Manager (OWCM) for OpenWay Riva networks. The default setting is ± 5 minutes.

If Field Tools is used to configure the 500W Module during installation, the module sets its time according to the programming application. If the module is configured with zero touch deployment (ZTD), then the 500W Module uses the last factory setting. When the module registers with and joins the network, it resets its clock to match network time. Accordingly, data collected before the cellular network registration may not be time-aligned with network time. The initial time is set in the 500W Module at that time of installation using Field Tools.



Caution: If the 500W Module device was installed using ZTD, the time drift between manufacture and deployment may be significant until the device self-adjusts based on the time received from the cellular network.

4 Security

Security is managed differently depending on your module's head end system and network.

On the Gen6 network

500W Modules support three security models:

- **Network access.** Security is based on public key infrastructure (PKI). All battery-powered devices (BPDs) use the same certificate hierarchy, which provides a common root of trust for all certificates used by devices in a GenX network (mesh or cellular) and the HES to establish trust and authenticate identity. Two critical certificates for BPDs are the Birth Certificate (BC) and Driver's License (DL), which include the device's MAC address and are used for device trusted identity.
- **Local access in network mode.** This is a signed authorization process based on asymmetric keys.
- **Local access in mobile mode.** This model is based on a proprietary security model using symmetric keys.

For details on the Itron security model for BPDs, refer to the *UtilityIQ Security Overview*.

On the OpenWay Riva network

The Itron Cellular 500W Module follows the OpenWay Riva network security managed by Itron Security Manager (ISM) that includes a complete system knowledge of the content and purpose of each message. Security-related decisions (such as which key type—reading or command—to use when securing a message) are based on the function of the command. The enhancement of secure communications provides greater protection for bubble-up and two-way messaging to prevent unauthorized users from gaining access to the system. Enhancing encrypted communications helps prevent others from monitoring user information and increases user privacy. After the Itron Cellular 500W Module is installed and the appropriate keys are injected, the module begins secure operations.

This section provides an overview of the 500W Module Itron Security Manager (ISM) enhanced security. For information about anti-tampering and anti-theft events and alarms, see [Status, events, and alarms on page 37](#).

Mobile and network mode security fundamentals

500W Module enhanced security applies to the cellular and RF communications between the Itron data collection devices and the 500W Module. ISM, the endpoints in the system, and the head end use two fundamental security processes to ensure confidentiality and validity of the communications across the cellular/RF link.

- **Authentication.** Authentication is the process of confirming that an artifact is genuine or valid. ISM authentication is the process of verifying that the request is from a valid source and that the request is in its original form.
- **Encryption.** Encryption is the process of transforming information to make it unreadable to anyone who does not possess the required security key. There are two types of encryption: symmetric and asymmetric. Symmetric uses a shared key to decrypt/encrypt information. Asymmetric uses a private key to encrypt and a public key to decrypt. ISM uses both symmetric and asymmetric encryption in our enhanced security solution.

500W Modules provide both authentication and encryption. Privacy is maintained on data collection messages from 500W Modules with enhanced security through encryption. Two-way commands from the data collection systems are authenticated by the 500W Modules to ensure that the source of the data is valid.

ISM security is always enabled in network mode, but is optional and configurable while in mobile mode.

Key and certificate types

500W Modules can be set to operate in mobile mode or network mode (see [Operating, transmitting, and receiving on page 9](#) for more information).

When the modules are operating in mobile mode, nine security keys are maintained for each 500W Module. Module ISM security keys include the following key types:

- **Two reading keys.** Reading keys are used to secure and remove decipher reading data. For the 500W Modules, this includes bubble-up messages and two-way data logging commands.

Reading keys are optional in mobile mode. While in mobile mode, the 500W Module can operate in three security modes:

- Ready to Secure (no reading keys, no command keys, not sure which of the other keys might be present). No enhanced security is enabled, although it is available. Remote disconnect/connect are not available when the security level is ready to secure. This security level only uses the utility factory key for the device. Ready to secure is the default factory ship mode for all gas and water modules.
- Command Secure (all keys EXCEPT reading keys). All commands between the endpoint and collection system are authenticated and encrypted with unique command keys. Command security is the minimum level of operation for devices

offering service disconnect. Command security is the minimum level of security to utilize remote disconnect valves.

- Fully Secure (all keys including reading keys). In addition to the endpoint and collection command system settings, all readings from the endpoint are encrypted with a shared reading key. ISM can use all keys that are available for the device. This is the most secure ISM mode.
- **Two command/programming keys.** Command/programming keys are used to secure commands that modify both the metrology and non-metrology state of a 500W Module.
- **Two revocation keys.** Revocation keys are used to perform key exchanges. 500W Module key exchanges support adding new keys, exchanging one key for another, or removing reading keys.
- **One recovery key.** The recovery key is a special revocation key. The recovery key is a customer-generated and managed key that does not participate in the active/standby rollover operations as the other two revocation keys do. The intent of this key is to allow the customer to set a key aside in a secure location for use if the revocation keys are lost. When security is removed from a module, configuration tools include a delete all non-factory keys method that must be secured using the recovery key.
- **One utility factory key.** The utility factory key is injected during the manufacturing process into non-volatile memory and is used to manage security keys in the 500W Module while the device is operating in an unsecured mode. When the 500W Modules are operating in the enhanced security mode, this key is non-functional.
- **One Itron factory key.** The factory key is a permanent key that is injected in non-volatile memory during the manufacturing process. The sole purpose of this key is to allow Itron to change the utility factory key using an RF-based command. Changing the utility factory key is typically completed as a step in the returned sales order process (RSO). Like the utility factory key, this key is non-functional when 500W Modules are operating in enhanced security mode.

When the 500W Module operates in network mode, security is applied at the network and application layers.

Note: The 500W Module's injected security credentials are dependent on whether the devices are built to stock or built to order.

- **Birth Certificate Chain.** Used to authenticate the device to the utility's network domain when joining a network.
- **AAA CA Certificate.** Used as a trust anchor when authenticating the utility's network domain during the join process.

The network layer includes a set of certificates injected during the manufacturing process. The **IoT FND CA Certificates** are used to authenticate messages sent from IoT FND to the device.

At the application layer, the following sets of credentials are managed:

- **OpenWay Enhanced Security Key set.** Used to secure application messages between OWCM and the device. Also, used in part during communication sessions between FDM and the device.

Manufacturing and installation

500W Module security features are determined by the device's operation mode (for more information about operating modes, see [Operating modes on page 17](#)).

In mobile mode, the security features of the 500W Modules are determined by the presence or absence of one or more key types. Enhanced security operation begins in manufacturing where two unique factory keys (utility factory key and Itron factory key) are injected into each module. The utility factory key and Itron factory key are created and managed by the ISM key generator server. The key generator server/network maintains the association between the module ID and its unique factory keys. With just the factory keys in place, the module operates in the basic security mode.

As part of a 500W Module shipment or upon subsequent customer requests, an enhanced security key transfer file (SKTF) is provided to the utility. This file contains the 500W Module ID/utility factory key pairings. After the utility receives the file, the utility customer imports the file into their ISM server and then the 500W Modules with enhanced security are activated and installed.

Field Deployment Manager (FDM) Endpoint Tools Enhanced can be used to install and set the module security state. When in mobile mode, FCS can also be used to set the security state. A module is moved from a basic security state to an enhanced security state by injecting keys. The state change is requested from the ISM server by the appropriate utility personnel or assigned during key import based on the ISM configuration. After the request is made, the ISM server generates the appropriate keys based on the wanted security level and creates key exchange commands secured by the utility factory key of the module.

The key exchange commands can be retrieved by the FDM Application Server when the installation work order for the module is created. The FDM Mobile Application performs the installation workflow and sends the key exchange commands to the module. After the module successfully receives and processes the key exchange commands, the module is in enhanced security mode. FDM returns the completed work orders and notifies the ISM server of the completed key exchange commands. The ISM server updates the state of the newly generated keys from pending to active and operation with enhanced security begins.

In network mode, 500W Modules can be built to order. Device security configuration parameters are determined by the manufacturing type.

Build-to-order

Modules that are build-to-order have their public keys and customer-supplied NMS, AAA Server CA, and device birth certificates injected during the manufacturing process eliminating the need to inject a large portion of the required key set during device installation or a mobile mode to IoT system mode/network mode switch.

Secured operations

After a 500W Module is installed and the appropriate keys are injected, the module begins secure operations. The listed reading and programming operations are secured for all 500W Modules.

Note: In network mode, security is required. In mobile mode, enhanced security operation is optional.

- **Bubble-up data collection.** The 500W Module's enhanced security in bubble-up messages utilizes the reading key. A field in the message is used to identify the particular reading key. The point where the message security is removed by the collection system differs between modules operating in either network mode or mobile mode systems.

- In modules operating in mobile mode, the reading keys for the modules are downloaded to the module reading application.

While the intent is for the utility to use a common reading key through the key update processes, it is likely that some modules within the utility may have a different reading key than others. For this reason, the module reading application obtains up to 16 of the most recent reading keys issued to modules and downloads that list to the data collection application. The radio uses the key identifier in the bubble-up message to determine which reading key to use to decipher the secure message. This allows the module reading applications to process the secure message following Itron existing reading methods.

- **Two-way operations.** Programming commands issued to a module are secured by the ISM security application utilizing a command key that resides in the target module. The use of the active command key is recommended.

When a two-way command is requested at the application server—either through a user request or through an internal job—the application server creates a command, formats the command packet, inserts a unique tracking ID, and sends the command to ISM to be secured using the module's command key.

The application server forwards the secure command message to the appropriate data collection application which sends it to the 500W Module. The module validates the command message, executes the command, and logs the command instance, identifying it by the command tracking ID. If reading keys are present, then the response is encrypted

and is transmitted to the collection application. The application receives the response. Security is deciphered based on the application type.

Modules operating in mobile mode can generate commands at the application level and secure commands using the reading key. The collection method inspects the bubble-up message from the target 500W Module to identify the module's reading key. The reading key allows the collection method to secure a pending read command using the identified key. The collection method can also inject the current time into the reading command prior to securing the message to force the module to update its time, thus ensuring the ad-hoc reading operation of the collection device is maintained even in a secure environment.

5

Operational life

The 500W Module uses a single D cell lithium (LiSOCl₂) battery and a Hybrid Layer Capacitor (HCL). The expected 20-year battery life is a function of the current and voltage requested from the battery due to the operation of the module. Itron applies a twofold approach to determine battery life: theoretical/lab experimental data and field data.

The theoretical approach is based on models to simulate the failure mechanism. In a typical battery, the various failure mechanisms are as follows:

- Exhaustion of battery capacity, relative self-discharge and voltage drop due to the operating conditions.
- Integrity of the mechanical can (that is, battery packaging).

Itron has developed battery life models based on battery chemistry to simulate the preceding failure mechanisms. Itron also conducts accelerated lab tests to simulate the preceding failure modes. These experiments include discharge under various conditions as well as micro-calorimetry to determine the pertinent model parameters. For more information about battery life, see [Battery low warning on page 38](#).

Operational and network impacts to battery life

Two main factors in combination affect an endpoint's battery life:

- **Operational impacts.** This includes the metering application itself, how often meter data is collected, the number of on-demand requests, and the number of firmware updates.
- **Network impacts.** This includes the network connectivity and the quality of the communication link.

Operational impacts

Utility users look beyond meter reading and require more advanced use cases from AMI solutions to increase their overall operational efficiency and provide new services. This has led to more features and flexibility in the use of those features in the endpoints, demonstrated by examples such as configurable tampers, alarms, low-latency commands, and variable intervals.

As a result, battery consumption, and therefore battery lifetime, can vary dramatically depending on the endpoint configuration, types of features enabled, and duty cycle of these features. Utilities are also looking to connect and interact with a variety of devices to support their distribution operations. These telemetry devices may have significantly different usage profiles and battery capacity than the traditional AMR endpoint.

The typical operational impacts and/or use cases for water metering applications include:

- Up to four interrogation cycles per day; each collects intervals and events data over cellular LTE-M (Cat-M1) networks.
- On average one two-way command per week to the module. For example, a move-in/out and on-demand read after alarm notification.
- Firmware download five times over the expected 20-year life of the module.
- Network discovery once per week (52x annually).

Network impacts

The network connectivity or the quality of the link also impacts battery life. The cellular solution provided from Tier 1 mobile network features intelligent battery management and link control applications that have been redesigned to provide a reliable connection link within the inherently dynamic cellular environment.

The cellular network provides the data link at a device level to achieve long range, low latency, high throughput, and high capacity. This allows the overall network to be optimized at an endpoint level, thus providing optimal cellular link quality. For example, devices that have a high link quality to the network do not need to retry the transmissions as often, and therefore do not consume as much battery life. The result of variation in network impact is that two devices connected to the network may have different battery lifetimes, even if they are within the same device family and have the same application usage profile. An endpoint's signal quality and signal strength are the primary two network determinants of the variations in battery life. For more information, see [Operational and network impacts to battery life on page 26](#).

The 500W Modules configured for either 15- or 60-minute intervals are designed to achieve a 20-year battery life with data collected four times per day.

Itron recommends that meters and devices be deployed on a first-in, first-out (FIFO) basis and within a period of three–four years from the date of manufacture. Itron shall not be liable for any performance degradation, failure, or damages resulting from the failure to store, install, test, handle, or operate Itron equipment in accordance with its documentation or outside the recommended deployment timeline.

6

Standard device configuration and usage

Itron offers a standard device configuration (opted into during the ordering process) that provides a 20-year battery life:

- 15-minute interval data
- Four scheduled push times
- Five firmware downloads over the life of the 500W Module
- Operating mode set to network mode
- Meter configuration set to auto detect

This list assumes one alarm per month.



The battery life description in this document is dependent on the 500W Module being deployed in a standard configuration.

The following configurations are supported in the 500W Module:

- **Manufacturing configuration.** Manufacturing configurations are parameters programmed during the manufacturing process. During the build-to-order process, manufacturing supports:
 - FDM or Field Tools parameters programmed through a FDM snapshot.
 - Remote application configuration is programmed in manufacturing. For modules on an OpenWay Riva network, remote application configuration is completed using a file produced by OpenWay Collection Manager (OWCM). For modules on a Gen6 network, it's completed using a file produced by Itron Device Configuration Manager (IDCM). These configuration files are created at the head end system.
 - Security keys or files are created from the security appliance and are programmed in during manufacturing. For more information about security, see [Security on page 20](#).
- **Local in-field configuration.** Local in-field configuration is completed using FDM Tools, Field Tools, or a third-party work order system.

Note: For module installations to a new meter, programming the 500W Module is not required. When retrofitting the 500W Module to meters already installed in the field, the 500W Module can auto-detect when attached to an encoded register. If retrofitting to a meter with a pulse output, local in-field configuration is required.

- **Remote configuration from the head end.** 500W Modules deployed on an OpenWay Riva network can be remotely programmed or configurations updated over-the-air via the head end system. 500W Modules deployed on a Gen6 network is completed using

IDCM and MPC.

- *(Applicable only to modules on an OpenWay Riva network)* **Third-party work order installation.** The third-party work order installation requires the following configuration during the manufacturing process:

- Programmed with a Network ID/SSID
- Injected with the utility's wanted security (from the utility's ISM)
- Shipment from the factory in mobile mode in a Ready to secure level.

500W Modules may be shipped from the factory in a Ready to secure mobile mode or a Fully secured network mode.

7

Registration

FDM Tools or Field tools can be used to query or display registration, view the module's network status, and capture the module's first data information for modules running on the OpenWay Riva network.

For 500W Modules that run on a Gen6 network, AMM displays the module's current operational state which may be:

- New
- Installed
- Discovered
- Initializing
- Initialized
- Active
- Disconnected

The Network Center application, which is part of the UtilityIQ suite, displays the last time a read or registration was received from the 500W Module. Discovery and registration typically take from 30 minutes to four hours. Itron recommends allowing up to two days before investigating a possible issue.

8

Programming and reading

When a 500W Module ships from the factory using Itron's standard configuration, all programmable parameters are set to their manufacturing default values. A configuration file defines the module's programming parameters. Units can be shipped pre-programmed using this configuration file. If a user chooses not to use a configuration file, the device is programmed to Itron's standard configuration, as outlined in [Default values on page 31](#).

Default values

This section shows the default values for a 500W Module that uses Itron's standard configuration. If a **Check Endpoint** command (using FDM Tools) or **Check** command (using Field Tools) was performed prior to programming, these values would be read and returned. The following table describes a partial list of the default values set in the 500W Module when it's manufactured.

Table 5 Parameter and value

Specification or parameter	Value
Operating mode	Network mode
Leak Period	48 hours
Truncation	0
Network Interval	15 minutes
Meter Configuration	Auto detect
Wake on	Connection to an encoded water meter Note: 500W Modules auto detect Neptune Meter's eight-dial output by default. This addresses potential underbilling situations. Customers who require a six-dial output when connected to their Neptune encoded meters are required to program their 500W Modules at time of installation.
Scheduled reads	Four per day

Programming parameters

The 500W Module has the following general programming parameters:

- **Manufacturer system parameters.** Manufacturer parameters are set by Itron and cannot be changed by the utility. See [Manufacturer system parameters on page 32](#).
- **Utility-specific parameters.** All 500W Modules are build-to-order devices; they can be built with IDCM/OWCM (depending on your head end system) and FDM snapshot files provided by the customer during the ordering process. Utility system parameters are common to a family of modules for a specific utility. See [Utility system parameters on page 32](#).
- **Meter-specific parameters.** Meter-specific parameters vary by the meter type connected to the module. These parameters are programmed at time of installation using Itron Field Tools and an IMR. See [Meter-specific parameters on page 34](#).

Manufacturer system parameters

The manufacturer system parameters contain the information required for basic device operation. These parameters are configured as default values or during manufacturing process via FDM snapshot or configuration files or meter spec form inputs, and include but are not limited to the following:

- Access Point Name
- Audit Mode Duration
- Battery Utilization Threshold
- Carrier Configuration Operator ID
- Carrier Configuration PDP Type
- Cellular Band Configuration / Radio Access Technology
- Cellular Data Context
- Cellular Minimum Technology
- Network Scan Configuration
- Reverse Period
- Signal Quality Threshold

These properties are determined by fields specified in the product specification form (for more information, see your product's ordering guide), the FDM snapshot file, and the configuration file. Depending on the network your module is deployed to, you will have either an OWCM configuration file (in OpenWay Riva network deployments) or an IDCM configuration file (in Gen6 network deployments).

Utility system parameters

The 500W Module's utility system parameters contain information required for the utility's system operation. Generally, all 500W Modules within a defined group are programmed

with the same utility system's parameters. The utility system parameters for the 500W Module include:

- Meter configuration
- Utility ID
- SSID (applicable only to modules on an OpenWay Riva network)
- Network ID (applicable only to modules on a Gen6 network)
- Security lock level (No lock, hard lock)
- SKG ID

These properties are determined by a combination of configuration files, including the spec form, the FDM snapshot file, and the configuration file. Depending on your network, you will have either an OWCM configuration file (in OpenWay Riva network deployments) or an IDCM configuration file (in Gen6 network deployments).

Itron sets the utility system parameters for use by a specific utility. They are designed to provide proper communication and 500W Module security for all the utility's 500W Modules.

When a 500W Module is programmed, the new parameters take effect immediately.

Note: When a 500W Module is programmed in mobile mode, the utility ID and security lock level are set, which defines how subsequent reprogramming is performed. When the 500W Module is programmed and set for hard lock security level, the 500W Module cannot be unlocked.

Utility ID

Note: The utility ID is used during mobile mode operation only.

The utility ID parameter specifies the unique, utility-specific security code that prevents an unauthorized individual from communicating with the module.

Itron assigns the utility ID, which ranges from 0 through 255. The utility ID is contained in the Meter Configuration File loaded into FDM or Field Tools.

Without the correct utility ID, a data collection method can read the beacon (network mode) or SCM+ (mobile mode), but it cannot alter the parameters or display the module's encoded data. With the correct utility ID, an operator can perform the following functions.

- Program the module
- Read the module's programmed parameters
- Read the tamper value. For more information, reference the product specification sheet for your module.

Security lock level (mobile mode only)

The security lock level parameter controls module reprogramming. The 500W Module uses the following security lock levels:

- **No lock.** A module programmed with this lock level can be reprogrammed with a compatible programming method and the correct utility ID.

Note: Itron recommends No lock whenever possible for greater flexibility.

- **Soft lock.** The soft lock security level provides the same functions as no lock: however, the **Unlock Endpoint** functions must be successful before the module can be reprogrammed.
- **Hard lock.** If a module is programmed with this lock level, billing parameters such as consumption or number of dials cannot be reprogrammed. System parameters, such as operation mode (mobile mode or network mode) can be reprogrammed.

Run mode operating settings

This parameter specifies the 500W Module's run transmission environment and specifies how the module is read:

- Network mode
- Mobile mode
 - Mobile/handheld mode
 - Mobile high power mode
 - Hard-to-read mobile/handheld mode

Note: For more information, reference [Operating modes on page 17](#).

Meter-specific parameters

A 500W Module's meter-specific parameters contain information required for modules to operate properly with a certain meter type or model. Meter-specific parameters are different for all meters. There are two types of meter outputs that the 500W Module is compatible with:

- **Encoded Output:** The 500W Module auto-detects a water meter's encoded protocol to read the meter's consumption and/or event data.
- **Pulse Output:** The 500W Module must be programmed with the meter type and its initial reading (Refer to the *Field Deployment Manager (FDM) Tools User Guide* or [Field Tools Help](#) for more information).

Programming modules



Important! The 500W Module can come pre-configured from the factory via customer specific FDM snapshot and configuration files, or must be programmed at the time of installation, prior to use.

Field Tools or FDM utilizes an IMR for programming devices.

Programming Itron Itron Cellular 500W Modules requires an understanding of:

- Your meter's configuration and the number of dials
 - The configuration and number of dials is important for programming the module to count correctly and roll over to zero at the correct time.
- How your system interprets the meter reading
 - Some systems modify the consumption reading with the collection software. Other times, the billing system is used to make modifications. If modifications are made in both systems, issues may cause consumption reading errors.

It is important to understand your system before the 500W Modules are programmed.

Program the 500W Module in network mode or mobile mode using an IMR and FDM Tools or Field Tools.

To enable enhanced security and for more complete programming information, see the [FDM Tools Mobile Application Online Help](#) or [Field Tools Help](#) as applicable (for documentation information, see [Related documents on page 7](#)).

Best practices and considerations

For initial module programming, reprogramming, or performing a **Check Endpoint** command (using FDM Tools) or **Check** command (using Field Tools), Itron recommends holding the IMR upright and facing the module to facilitate successful communications.

Time to program

The time required to program the 500W Module (in mobile mode only) is dependent on the operating mode.

Time to program in normal operation

In mobile mode normal operation, the module bubbles up an SCM+ message every 15 or 60 seconds (30 seconds for mobile mode hard-to-read mobile/handheld mode). The IMR does not have an opportunity to send a command (program) to the module until it receives the SCM+ message. It could take 60 seconds before the IMR receives the message and has an opportunity to transmit back. On average, the IMR receives the module's message within half the bubble-up rate time (for example, 7.5 seconds for mobile mode).

The programming process completes a few seconds after the handheld programmer successfully receives the module's message.

Waking up and programming from factory ship mode

The 500W Module must first be woken from factory ship mode. This can be accomplished by either enabling **Check Endpoint Type** in FDM Tools or issuing either the **Auto-Detect**, **Program**, or **Check** commands via Field Tools.

When **Check Endpoint Type** is enabled, FDM Tools performs a Check Mode on any endpoint before displaying a task menu based on the module's mode. This setting can be used to wake an endpoint from factory ship mode.

The **Auto-Detect** command determines the 500W Module's factory-programmed mode (mobile or network) and then presents the user with the associated task menu. After it is awake, the 500W Module can take anywhere from 15 to 65 seconds to program.

Note: If the mode is already known (for example, the user knows the 500W Module was shipped from Itron in network mode), the user can directly select the network mode menu in Field Tools and go directly to the program operation. The program operation could take slightly longer because that task first determines if the 500W Module is awake and wakes it up if necessary prior to programming.

Itron programs and software variables

This section defines and clarifies possible system variables you may encounter in programming 500W Modules.

Programming example

See the [FDM Tools Mobile Application Online Help](#) or [Field Tools Help](#) for examples on programming endpoints.

OpenWay Operation Center (OWCM)

Note: This section is applicable only to modules running on the OpenWay Riva network.

The OpenWay Collection Manager (OWCM) collects the raw reading and passes it on without making any formatting changes.

Itron Enterprise Edition (IEE) Meter Data Management

Note: This section is applicable only to modules running on the OpenWay Riva network.

The standard unit of measure (UOM) in IEE is cubic feet for water endpoints. The reading passed on by the water endpoint is not in cubic feet if endpoints with six- and seven-dial meter configurations are programmed, so adjustments are required to set the correct unit of measure. If you are having issues with your readings in IEE but your endpoint and meter index match, check your unit of measure within IEE.

9

Meter display and encoding consumption data

The primary operation a 500W Module performs is recording the amount of water flowing through a pipe to a place of use that is reported by a water meter.

Using a typical ultrasonic water meter as an example: ultrasonic signals are sent with and against the flow of water to determine the velocity of water flow, which is used to calculate consumption.

In the case of an encoder meter, the 500W Module is connected to the water meter with an ILC cable (Inline Connector). The 500W Module reads the water meter's encoded protocol at the top of every hour to gather consumption data.

In the case of a pulser meter, a reed switch, close to the shaft containing the magnet, is used to count revolutions generated by the meter's drive dog. As the magnet rotates near the reed switch contained in the sensing device, the reed switch closes. When the reed switch closes, a pulse is sent to the 500W Module.

In mobile mode, the hourly interval count data is stored in a data array in flash memory within the module. The data is overwritten every 960 intervals (40 days) in a round-robin fashion. By definition, the first interval is the latest written interval and the last interval is the one written 40 days ago.

In network mode, the interval period is configurable dependent on the 500W Module's firmware version. For more information about the module's firmware functionality, see the *Itron Cellular 500W Module Ordering Guide*.

Status, events, and alarms

500W Modules report their status in the system and detect when someone tampers with the meter or module. Statistics that the 500W Module tracks include:

- Cellular signal quality
- Network attachment
- Tower/sector
- Missed or aborted transmissions
- Modem current consumption
- Battery reserve aggregate
- Battery counter

Tamper and event values, interpretations, status information, and reporting may differ among various 500W Module types.



Important! Tamperers are available when the 500W Module is operating in mobile mode. Events and alarms are available when the 500W Module is operating in network mode. The available events and alarms are dependent on the module's firmware and head end versions.

Sensors in the device detect when certain tamper conditions occur. The module then increments the tamper counters and logs appropriate events.

The head end system standardizes native device event identifiers by translating them into system event codes, a process commonly referred to as "normalization." This enables the head end system to apply a consistent system event code to represent similar event types across different device-specific event codes.

- For modules on the OpenWay Riva network: The mapping between device event IDs and system event codes is detailed in the *OpenWay Collection Manager Device Interface Guide*.
- For modules on the Gen6 network: Refer to [Events and alarms on page 40](#) and the *Advanced Metering Manager (AMM) Events* documentation. *Advanced Metering Manager (AMM) Events* not only outlines the mapping from device event IDs to system event codes but also provides in-depth descriptions of event messages and their associated arguments.

500W Module events are configurable in the listed ways:

- An event can be enabled or disabled.
 - If the event is disabled, it is not detected or reported.
 - If the event is enabled, the event is logged in an event log and retrieved from the event log during a read. If an event is enabled and configured as an alarm, the event is immediately sent to the back-office system as a trap.
- Event configuration is set up in the 500W Module's configuration file and can be programmed during manufacturing, locally, or remotely.
- All supported events are enabled by default.
- Some events include additional detailed information in the event log.

Tamper counters

In mobile mode, tamper counters track each tamper event and are reported in the SCM/SCM+. The 500W Module uses the tamper counters to know if there is an active tamper being reported.

Battery low warning

The 500W Module includes a battery life estimator. The estimator is based on the number of data packets sent at the various power levels and the age (self-discharge) of the module. The battery low warning event allows the utility to easily identify which modules

are nearing the end of life. This advanced warning gives the utility the opportunity to schedule module replacement. The battery low warning is set when the battery has less than 10% remaining capacity, typically two years life remaining. Battery life is evaluated daily at midnight.

The battery counter is retrievable using Field Tools. The battery counter is displayed in Field Tools as either a "Good" or "Low" indicator, and displays years of remaining battery life. The estimated remaining years of battery life is calculated based on the current Battery Counter value which takes into account battery usage from past module operations. Because the number of future operations is dependent on how the utility interacts with the module, the Projected Remaining Years is not a guarantee of remaining battery life.

A

Events and alarms

Events captured within the 500W Module during normal daily monitoring must be configured for them to be logged. Configured events support event notification and troubleshooting. Events logs are available for data collection using the standard interrogation process.

By default, all events described in *OpenWay Collection Manager Device Interface Guide* or *Itron Device Configuration Manager (IDCM) User Guide* should be configured for delivery. Additionally, events can be configured as priority alarms, enabling asynchronous delivery on detection to the head end system. The logs in the 500W Module use a profile-generic class structure allowing for selective access.

Alarms are events that have been configured to be sent to the head end system as they occur. Alarms are collected as events during normal data collection, but because they are deemed time sensitive, they are also sent immediately as they occur.

Alarm delivery to the head end system is separate from typical data delivery.



Important! To ensure critical events are communicated effectively without overwhelming the network or head end system, Itron has predefined specific events to be transmitted as alarms. These default settings strike a balance between timely notifications and system performance. Unless a clearly defined use case necessitates a change, customers are advised to retain Itron's default alarm configurations.

The 500W Module's supported events and alarms are described in [Table 6](#). The Event code column applies to modules running on OpenWay Riva and Gen6 networks. The AMM event code column applies only to modules running on a Gen6 network.

Table 6 Events and alarms

Event code	AMM event code	Event name	Event description
1	901057	Inter Digit	There is a corrupt digit in the encoded register reading.
2	901001	Register Error	No communication with the register.
3	901058	Invalid Read	The register is not sending a valid read.
6	901004	Low Battery	The module has a low battery warning. Just 10% of the battery's life remains.
7	901059	Consumer Leak Detected	The module has detected continuous flow over a set period of time.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
8	901060	Consumer Leak End	The module has detected the end of continuous flow after having reported a leak.
9	901061	Reverse Flow Detected	The module has detected reverse flow. Note: This is sometimes referred to as <i>backflow</i> .
10	901062	Reverse Flow End	The module has detected the end of reverse flow after having reported reverse flow.
11	901063	Leak Sensor OK	The module detects a leak sensor attached and it is working properly. The event is triggered when the state was previously unknown or was previously not working properly.
12	901064	Leak Sensor No Comm	The module detects a leak sensor is attached, but it is not working properly.
13	901065	Leak Sensor Detached	The module does not detect that a leak sensor is attached after previously having one attached.
14	901066	Valve OK	The module detects that a remote disconnect valve is attached and is working properly. The event is triggered when the state was previously unknown or previously not working properly.
15	901067	Valve No Comms	The module detects a remote disconnect valve is attached but it is not working properly.
17	901068	Pulse Mismatch	The module has detected an internal pulse mismatch.
18	901006	Cut Cable (Pulser) Detected	A physical cut cable has been detected by the module.
19	901007	Cut Cable (Pulser) End	A physical cut cable is no longer detected by the module.
20	901008	High Flow Detected	The module detects consumption has exceeded the high-flow threshold.
21	901009	High Flow End	The module detects consumption has dropped below the high-flow threshold after having been in a high flow state.
41	901200	External Antenna Attached	An external antenna has been attached to the module. Applicable only to modules on a Gen6 network.
42	901201	External Antenna Detached	An external antenna has been detached from the module. Applicable only to modules on a Gen6 network.
500	901010	Critical Error (Internal)	A critical internal error has occurred that is not described by other events.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
504	901014	Flash Error	A flash error has been detected.
505	901015	Meter Quiet Mode Exit	Occurs when the module first gets pulses, or detects consumption and wakes from meter quiet mode. If the device wakes from just factory ship mode (not meter quiet mode), then this event is not logged.
506	901016	Entering Network Mode	The device has been changed to network mode.
507	901017	Battery Parameters Set	A battery parameter has been changed.
509	901019	Key Update Succeeded	A security key has been updated in the device. Event text that states 'key at index 99', indicates the device was accessed locally, using a signed authorization.
511	901021	Load Profile Cleared	The load profile data has been cleared.
512	901022	Manual Time Sync	The time has been changed manually. This event is also be logged the first time the device joins a network and gets network time after being manufactured.
515	901024	Time Outside Automatic Sync Threshold	A time change greater than the warning level threshold has been detected.
516	901025	Time Outside Automatic Sync Threshold Ended	A time change greater than the warning level threshold has ended and is back below the threshold.
517	901026	Entering 100S Mode	The device has been changed from network mode to mobile mode.
541	901174	Corrupt Alarm Data Received From Meter	The module received a corrupt data character from the meter. This event is logged a maximum of one time per day. This event is not logged if the corrupt data character is received as part of the volume or consumption field.
1000	901089	Register Removal	Badger extended alarm: bit 0 = register removal.
1001	901090	Meter Temperature Alarm	Badger extended alarm: bit 1 = temperature alarm.
1002	901091	End of Meter Life	Badger extended alarm: bit 2 = end of life alarm.
1003	901092	Zero Consumption Detected	Badger extended alarm: bit 3 = no usage alarm.
1004	901093	Reverse Flow Meter	Badger extended alarm: bit 4 = reverse flow alarm.
1005	901094	Leak Meter Alarm	Badger extended alarm: bit 5 = leak alarm.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
1006	901095	Encoder Programming	Badger extended alarm: bit 6 = program alarm.
1007	901096	Meter Tamper	Badger extended alarm: bit 7 = tamper.
1500	901097	Active Reverse Flow	Kamstrup extended alarm byte 1: bit 0 = active reverse flow. This event is logged a maximum of once per 24 hours.
1501	901098	Historic reverse Flow Meter	Kamstrup extended alarm byte 1: bit 1 = historic reverse. The active info-code within the last 30 days, no matter how long the info-code was active. This event is logged a maximum of once per 30 days.
1502	901099	Active Empty Pipe	Kamstrup extended alarm byte 1: bit 2 = active dry. The meter is in a current empty pipe state. This event is logged a maximum of once per 24 hours.
1503	901100	Historic Empty Pipe	Kamstrup extended alarm: Kamstrup extended alarm byte 1: bit 3 = historic dry. The active info-code within the last 30 days, no matter how long the info-code was active. This event is logged a maximum of once per 30 days.
1504	901101	Active Burst	Kamstrup extended alarm byte 1: bit 4 = active burst. The meter is currently in a high flow state outside of the meter parameters. This event is logged a maximum of once per 24 hours.
1505	901102	Historic Burst	Kamstrup extended alarm byte 1: bit 5 = historic burst. The active info-code within the last 30 days, no matter how long the info-code was active. This event is logged a maximum of once per 30 days.
1506	901103	Encoder Programming	Kamstrup extended alarm: byte 1: bit 6 = the encoder setup has been changed one or more times since production.
1507	901104	Active Leak Meter Alarm	Kamstrup extended alarm byte 2: bit 0 = the meter is in an active leak state. This event is logged a maximum of once per 24 hours.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
1508	901105	Historic Leak Meter Alarm	Kamstrup extended alarm byte 2: bit 1 = historic leak. The active info-code within the last 30 days, no matter how long the info-code was active. This event is logged a maximum of once per 30 days.
1509	901106	Low Temperature Alarm	Kamstrup extended alarm: The minimum meter temperature detected. This alarm is sent when the temperature on the Kamstrup meter is lower than 36° F.
1510	901107	High Temperature Alarm	Kamstrup extended alarm: The maximum meter temperature has been detected. This alarm is sent when the temperature on the Kamstrup meter is higher than 125° F.
1513	901108	Zero Consumption Detected	Kamstrup extended alarm: The meter has detected no usage. This event is logged a maximum of once per 24 hours.
1600	901109	Backflow Detected	Intelis Water Meter extended alarm: The meter's backflow consumption register indicates a total backflow that is outside of the threshold values for expected backflow.
1601	901110	Empty Pipe Alarm Detected	Intelis Water Meter extended alarm: The device detects that the pipe is empty, possibly due to the meter being removed from the installation.
1602	901111	Meter Reversed	Intelis Water Meter extended alarm: The meter has detected that it has been installed in a reverse orientation.
1603	901112	Battery Low	Intelis Water Meter extended alarm: The meter's battery life has less than six months (for the NAM meter) or 12 months (for the international meter) remaining.
1604	901113	Leakage	Intelis Water Meter extended alarm: The meter has detected a leak. The average flow rate during each of the hours over the past day (for NAM meter) or over a configured number of days (for international meter) was above the leakage flow rate threshold. This event clears when the average flow rate for one hour returns to within the configured threshold.
1605	901114	Burst Flow Alarm Detected	Intelis Water Meter extended alarm: The meter has detected a burst flow alarm which can indicate a broken pipe.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
1607	901115	Tamper Alarm	Intelis Water Meter extended alarm: The meter has detected that the cover was opened. This can indicate that the meter has been tampered with.
1608	901116	Temperature Alarm Detected	Intelis Water Meter extended alarm: The meter has detected a temperature alarm. The meter has reached a temperature that is outside of the temperature range. This event clears after the alarm duration time passes (one day minimum).
1800	901155	Air In Tube Error	Diehl Hydrus Meter extended alarm: The meter has detected air in the supply system and water flow rate measurement is not possible.
1801	901156	Leak Alarm	Diehl Hydrus Meter extended alarm: The meter has detected leakage above threshold for 24 consecutive hours. The alarm is reset 15 minutes after consumption is below the leakage threshold.
1802	901157	Checksum Error	Diehl Hydrus Meter extended alarm: The meter has detected that flash or RAM is corrupted or manipulated. This is a fatal error, the meter must be replaced. This error is cleared three days after it is raised.
1803	901158	Temperature Measurement Error	Diehl Hydrus Meter extended alarm: The meter has encountered a temperature measurement error. The median temperature is too low or too high (22° F / 212° F, -30° C / 100° C), or the cable temperature sensor is cut or disconnected.
1804	901159	Ultrasonic Hardware Error	Diehl Hydrus Meter extended alarm: The meter's ultrasonic hardware has encountered an error. The ultrasonic transducer is defective or short-circuited, or the ultrasonic transducer cable is cut or disconnected.
1805	901160	Power Consumption Out of Limit Error	Diehl Hydrus Meter extended alarm: The meter is experiencing too much communication on its DMEI or optical interface over a short period of time. When communication capacity reaches zero (0) bytes, communication is temporarily paused. When communication capacity reaches below the minimum threshold (500 bytes is the default), then communications resume again.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
1806	901161	Overflow Error	Diehl Hydrus Meter extended alarm: The meter detects that flow is over the undersized meter threshold for one minute. The error is cleared after the meter detects flow that is under the undersized meter threshold for one minute.
1807	901162	Temperature Hardware Error	Diehl Hydrus Meter extended alarm: A hardware temperature error is detected for one minute. The temperature cable is damaged or cut. After three days of no hardware temperature error detected, the meter clears the alarm.
1808	901163	Reverse Flow Alarm	Diehl Hydrus Meter extended alarm: The meter detects that consumption is below its configured limit. The 1.3 meter and the 2.0 meter versions reset this alarm after different consumption conditions are met.
1809	901164	No Usage Alarm	Diehl Hydrus Meter extended alarm: The meter detects consumption below the no usage threshold for 30 days. The alarm is active one time ever 30 days. The alarm is cleared after consumption above the no usage threshold is measured for 15 minutes.
1810	901165	Measurement Alarm	Diehl Hydrus Meter extended alarm: The meter has detected seven consecutive days of measurements disturbed by influences of cavitation, air water mixture, heavy electromagnetic, or heavy mechanic interferences (vibration). These interferences can be caused by pumps or other heavy equipment operating near the meter. After three days of no disturbed measurements, the meter clears the alarm.
1811	901166	Low Temperature Alarm	Diehl Hydrus Meter extended alarm: The meter detected the temperature is lower than 3° C after four consecutive temperature measurements and the meter detects an Err4 at the same time. The meter resets the alarm after 30 days if the issue is resolved.
1812	901167	Empty Pipe Alarm	Diehl Hydrus Meter extended alarm: The meter detected an active Err7. The meter resets the alarm after 30 days without air detected in the pipe.
1813	901168	Overflow Alarm	Diehl Hydrus Meter (version 2.0 only) extended alarm: The meter detects flow that is above the Undersized Meter Threshold for 30 consecutive minutes. When the meter detects flow below the threshold for one minute, it resets the alarm.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
1814	901169	End of Life Alarm	Diehl Hydrus Meter extended alarm: The meter detects the calculated battery life is fewer than 400 days. The meter resets the alarm when the calculated battery life is more than 400 days.
1815	901170	High Temperature Alarm	Diehl Hydrus Meter extended alarm: The meter detects the medium temperature is hotter than 90° C for 60 consecutive minutes. The meter resets the alarm after medium temperature is 90° C or cooler for 60 consecutive minutes.
1816	901171	Fallback Mode	Diehl Hydrus Meter extended alarm: The meter detects a significant deviation between measurements of the two measuring paths. The meter resets the alarm three days after the deviation of measurements between the two paths goes away.
1817	901172	Metrological Log Access	Diehl Hydrus Meter extended alarm: The meter detects an entry into the metrological log. The module logs this event only one time and logs it again only if the meter alarm goes away and then reappears.
3000	901027	Device Reconfigured	The HES configuration in the device has changed.
3001	901028	Event Log Cleared	The Itron event log has been reset.
3003	901029	Configuration Downloaded	A new configuration has been downloaded.
3004	901030	System Reboot	A watchdog error. Reboot.
3005	901031	System Restart	A planned restart of the module (for example, after a firmware download completes).
3006	901032	Improper Installation Detected	The module was unable to adopt configuration information.
3007	901118	Disconnect Completed	The disconnect command was received and has completed.
3008	901119	Disconnect Failed	The disconnect command was received but failed to execute. The event detail will contain the verbose_result attribute of the DisconnectControl object.
3011	901122	Connect Completed	The reconnect command was received and has completed. The event detail will contain the verbose_result attribute of the DisconnectControl object.
3012	901123	Connect Failed	The reconnect command was received but failed to execute. Event detail will contain the verbose_result attribute of the DisconnectControl object.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
3013	901124	Flow Restriction Setting Changed	A restrict/service limit event was received and has been completed. The event detail will contain the verbose-result attribute of the DisconnectControl object..
3014	901125	Flow Restriction Setting Failed	A restrict/service limit was received but failed to execute. The event detail will contain the verbose-result attribute of the DisconnectControl object.
3015	901033	Authentication Failed	An application level security failure - authentication. This event occurs with an application level security failure for authentication.
3016	901034	Access Control Failed	An application level security failure - access control. This event occurs with an application level security failure for access control.
3017	901035	Key Rollover	A key rollover command was received.
3018	901036	Key Signing	An application-level security failure for certificates.
3019	901037	Takeover Package Accepted	A takeover package was presented and accepted by the module. Applicable only to modules on an OpenWay Riva network.
3020	901038	Takeover Package Rejected	A Takeover Package was presented but rejected by the 500W Module. Applicable only to modules on an OpenWay Riva network.
3021	901039	Replay Attack Detected	An application-level security failure for replays. Applicable only to modules on a Gen6 network.
3022	901040	RMA Signed Authorization Received	A signed authorization issued to "Itron-RMA" has been received.
3040	901173	High-flow Threshold Configuration Changed	A change was made to the High Flow Event Configuration threshold.
3048	901198	EDHOC Initiated	The EDHOC process has been initiated. Applicable only to modules on a Gen6 network.
3049	901199	EDHOC Error	An error occurred during the EDHOC process. Applicable only to modules on a Gen6 network.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
3052	901243	Driver's License Import Validation Error	A validation error occurred when importing a driver's license. The module logs this event as soon as the error occurs, but does not log the event again for the current 24-hour period (the 24-hour period restarts at midnight, UTC). This results in a maximum of one of this event being logged per day at the time that the error occurred. Applicable only to modules on a Gen6 network.
6000	901203	Cellular Communications Stopped	Communications reliability is inadequate and communications have been aborted. This can occur due to poor signaling conditions (such as a bad coverage area) or to exceeding the battery threshold for transmission. Reason codes are as follows: 0. Battery utilization 1. Signal quality 2. Registration battery utilization 3. Daily battery use exceeded 4. Daily battery use exceeded override
6001	901204	Modem Reset	The module's modem has been reset. The reason code for the reset condition and the anticipated modem off time, in minutes, is listed in the details.
6002	901205	No Comms	The modem has not passed a paging request in >15 hours and 45 minutes when in eDRX or in PSM Cellular Operating Mode. The event is logged upon every expiration of the timer. The timer is reset and starts counting down again after each logging. This event should always be configured as an alarm to assure assistance with modem communications reestablishment and to help avoiding the PDN timer behavior on cellular networks.
6004	901207	Cell ID Change Count	The Cell ID (tower/sector) has changed throughout the day. This event provides a count of incidents (if non-zero) along with the latest Cell ID value.
6005	901208	Low Temperature Shutoff Started	The module has detected that ambient temperature has dropped below -20° C/-4° F.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
6006	901209	Low Temperature Shutoff Ended	The device detected that ambient temperature has returned to operating range and the debounce parameter thresholds have been met, allowing normal operations to resume.
6007	901210	Low Voltage Shutoff Started	The module has detected voltage that has dropped below the low-voltage threshold. Only one event shall be logged when voltage is recognized to be below threshold, it is not logged continuously. The power off threshold voltage default is 2.95 volts.
6008	901210	Low Voltage Shutoff Ended	The module has detected that voltage in the device has recovered to the recovery voltage threshold, allowing normal operations to resume. The power-on recovery voltage default is 3.4 volts.
6011	901244	Cellular Network Assessment Start	The module has started a cellular network assessment.
6012	901245	Cellular Network Assessment End	The device has concluded a cellular network assessment.
10000	901041	PCOMP Changed	The metrology parameter for pressure compensation (PCOMP) changed.
10001	901042	Count Rate Changed	The metrology parameter for count rate changed.
10002	901043	Rollover Count Changed	The metrology parameter for rollover count changed.
10003	901137	Count Sample Debounce Changed	The metrology parameter for count sample configuration debounce changed.
10004	901138	Encoder Driver Type Changed	The metrology parameter for encoder driver type changed.
10005	901139	Prescaler Changed	The metrology parameter for prescaler changed.
10006	901044	Initial Index	The metrology parameter for initial index changed.
10007	901045	Image Transfer Initiated (Enabled)	An image transfer was successfully initiated.
10008	901046	Image Transfer Canceled (Disabled)	An image transfer was successfully canceled.
10009	901047	Image Transfer Cancel Failed	An attempt to cancel an in-progress image transfer failed.
10010	901048	Image Verification Initiated	The process to verify an image has started.
10011	901049	Image Verification Successful	The image verification process was successful.

Table 6 Events and alarms (continued)

Event code	AMM event code	Event name	Event description
10012	901050	Image Verification Failed	The image verification process was initiated, but was not successful.
10013	901051	Image Activation Initiated	The image activation process was initiated.
10014	901052	Image Activation Successful	The image activation process was successful.
10015	901053	Image Activation Failed	The image activation process was initiated, but was not successful.
10019	901054	Load Profile Interval Changed	A change was made to the load profile interval period.
10020	901140	Count Sample Width Changed	The metrology parameter for count sample configuration sample width parameters changed.
10021	901141	Count Sample Rate Changed	The metrology parameter for count sample configuration sample rate parameters changed.
10033	901229	Image Transfer Failed	An image transfer operation has failed.
10034	901230	Image Transfer Resumed.	An image transfer operation has been resumed.