IEC 60870-5-104 Driver for Tridium Niagara

User Guide

baudrate.io

niagara4

October 30, 2026

Contents

1 Introduction **2**

2 Requirements **2**

3 IEC 60870-5-104 Server Configuration **3**

4 Quick Start **3**

5 IEC 60870 Networks **4**

6 IEC 60870 Devices **6**

7 IEC 60870 Points **7**

7.1 Information Object Types 8
7.2 Quality Descriptors 9
7.3 Point Representation in Niagara 10
7.4 Niagara Point Types 10
7.5 Point Discovery Process 12
7.6 Point Update Logic 12
7.6.1 Spontaneous Reporting 12
7.6.2 Interrogations 12
7.6.3 Update Configuration 13

8 Troubleshooting **13**

8.1 Systematic Troubleshooting Methodology 13
8.2 Connection Problems 14
8.3 Discovery Problems 15

9 FAQ **15**

9.1 Can the driver control IEC 60870-5-104 devices? 15
9.2 What is the maximum number of points supported? 15
9.3 Can multiple Niagara stations connect to the same IEC 60870-5-104 server? 15
9.4 Does the driver support time synchronization or file transfer? 16
9.5 How often should periodic general interrogation be used? 16
9.6 What happens if the server connection is lost? 16
9.7 Can I use custom port numbers? 16
9.8 How do I know if my server is compatible? 16

1 Introduction

IEC 60870-5-104[1] is a widely used international standard for telecontrol in electrical power systems. The protocol is designed for communication between control centers (SCADA systems) and remote terminal units (RTUs) over TCP/IP networks. IEC 60870-5-104 is extensively deployed in:

- **Power System Automation** - Substations, distribution automation, smart grid applications
- **Industrial SCADA** - Manufacturing plants, process control, utilities
- **Energy Management Systems** - Load dispatch centers, generation control, grid operations
- **Renewable Energy** - Wind farms, solar plants, energy storage systems

The protocol provides reliable real-time data exchange, supporting both spontaneous reporting for immediate event notification and general interrogation for complete system status updates. Key features include:

- **TCP/IP Communication** - Standard port 2404 for reliable network transport
- **Real-time Data Exchange** - Spontaneous reporting of changes and events
- **Multiple Data Types** - Single/double points, measured values, integrated totals, commands
- **Time Synchronization** - Precise timestamping with various time formats
- **Flow Control** - Sequence numbering and acknowledgment mechanisms
- **Connection Management** - Proper handshaking and keepalive procedures

IEC 60870-5-104 Driver for Tridium Niagara acts as a **client** and connects to IEC 60870-5-104 **servers** such as RTUs, PLCs, and other automation devices. The driver automatically discovers available data points through general and counter interrogation and provides seamless integration with Niagara's point management system.

Note: This driver implements **read-only** functionality as per typical SCADA client requirements. It does not support control commands or setpoint operations to ensure safe operation in critical infrastructure environments.

2 Requirements

- Niagara-powered device with software v4.8 or later, such as JACE, Supervisor, or any OEM version
- IEC 60870-5-104 driver module and license
- IP address and common address of the target IEC 60870-5-104 server/RTU
- Network connectivity on TCP port 2404 (standard IEC 60870-5-104 port)

[1] All trademarks or registered trademarks are the property of their respective owners

3 IEC 60870-5-104 Server Configuration

Before configuring the Niagara driver, ensure your IEC 60870-5-104 server (RTU/PLC) is properly configured:

Server Requirements:

- TCP/IP interface enabled on port 2404 (or custom port if required)
- **Common Address** configured (typically 1-65534)
- **Information Object Addresses (IOA)** assigned to data points
- **Spontaneous reporting** enabled for real-time updates
- **General Interrogation** and **Counter Interrogation** support enabled

4 Quick Start

1. Copy iec60870-rt.jar module to Niagara /modules folder and restart the software.
    a. If the driver is hosted on PC: restart Supervisor / Workbench station.
    b. If the driver is hosted on JACE: import the module with all dependencies and restart it.
2. Ensure network connectivity to IEC 60870-5-104 server on TCP port 2404.
3. Add **Iec60870 Network** to the station.
4. Enter license code in **License** property under **Iec60870 Network**.
5. Add **Iec60870 Device** under the network.
6. Configure device **Address** with the server's **Ip Address**, **Port** (normally 2404) and **Common Address**.
7. **Discover** points in the device's **Points** extension.
8. Add discovered points to the station for monitoring.
9. See device's **Config** property to better understand how point values are updated.

5 IEC 60870 Networks

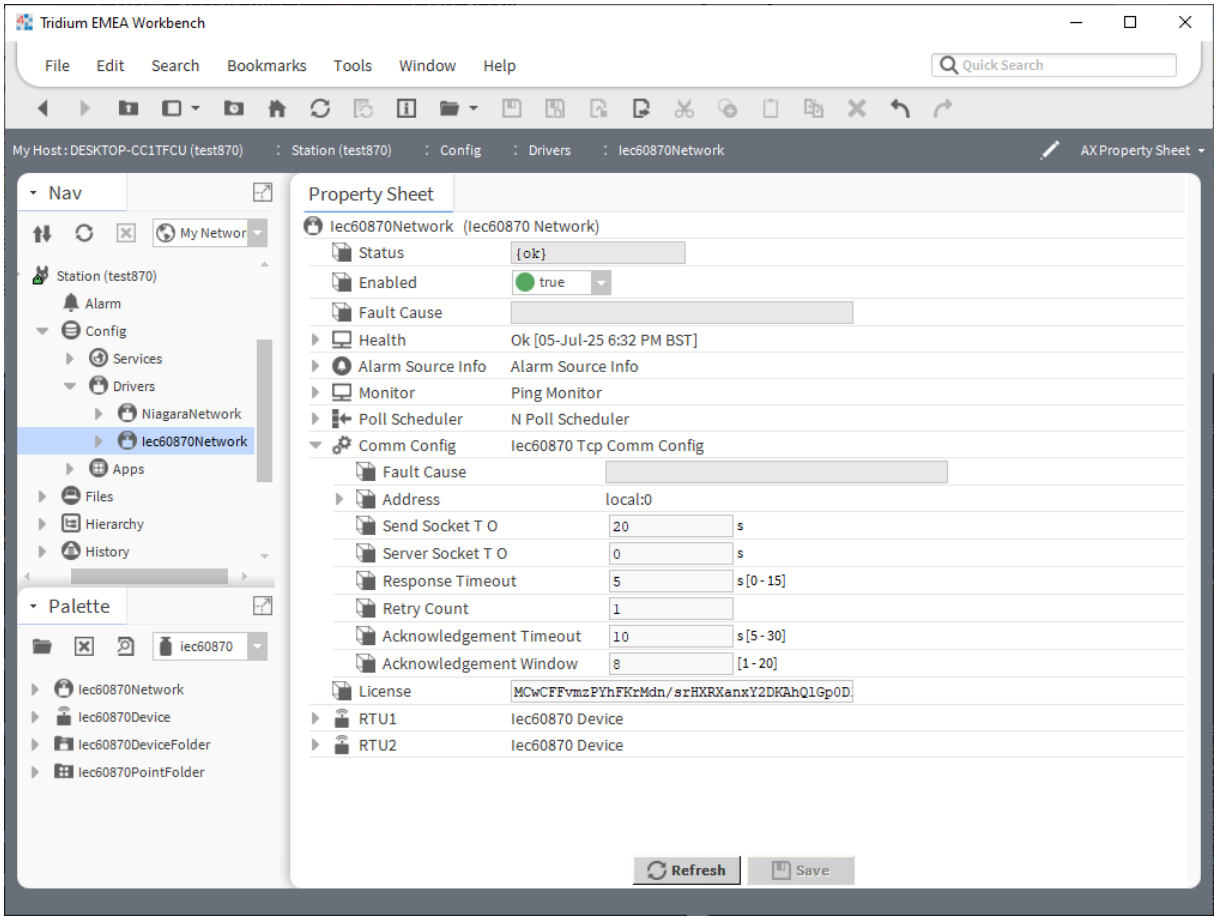

Figure 1: IEC 60870 network properties

Iec60870 Network contains standard Niagara network properties plus IEC 60870-specific configuration:

- **License** – the code that allows the driver to run on your host.
- **Comm Config** – communication parameters for the IEC 60870-5-104 protocol:
  - **Fault Cause** – cause of communication failure.
  - **Address** – local Niagara address for the IEC 60870-5-104 server. Should not be changed.
  - **Send Socket Timeout** – time to wait for sending data (default 20s).
  - **Server Socket Timeout** – time to wait for server response (default 0s).
  - **Response Timeout** – time to wait for server response (default 5s). Same as **t1 parameter** in IEC 60870-5-104.
  - **Retry Count** – number of retries for failed requests (default 1).

  - **Acknowledgement Timeout** – time before sending S-frame acknowledgment (default 10s). Same as **t2 parameter** in IEC 60870-5-104.
  - **Acknowledgement Window** – maximum unacknowledged I-frames before sending S-frame (default 8). Same as **w parameter** in IEC 60870-5-104.

- **Monitor / Ping Frequency** – time between TESTFR keepalive frames (default 20s, range 10-60s). Same as **t3 parameter** in IEC 60870-5-104.

In most cases only the **License** value needs to be configured at the network level. Users should not usually adjust the communication parameters, as the defaults are optimized for most applications. However, advanced users can tune them based on network characteristics and server requirements.

- **Poll Scheduler** – polling rates for periodic general and counter interrogation operations:
  - **Fast**: 1 minute (high-priority applications)
  - **Normal**: 5 minutes (standard operation)
  - **Slow**: 10 minutes (backup data collection)

In IEC 60870-5-104, most information is sent spontaneously, so periodic polling is not required for most applications. However, it can be useful for backup data collection or when spontaneous reporting is not available.

All these parameters implement the standard IEC 60870-5-104 timing requirements for flow control and connection management. For basic deployments, only the **License** value needs to be configured.

After network properties are configured, the **IEC60870 Device Manager** can be used to add devices and discover points.

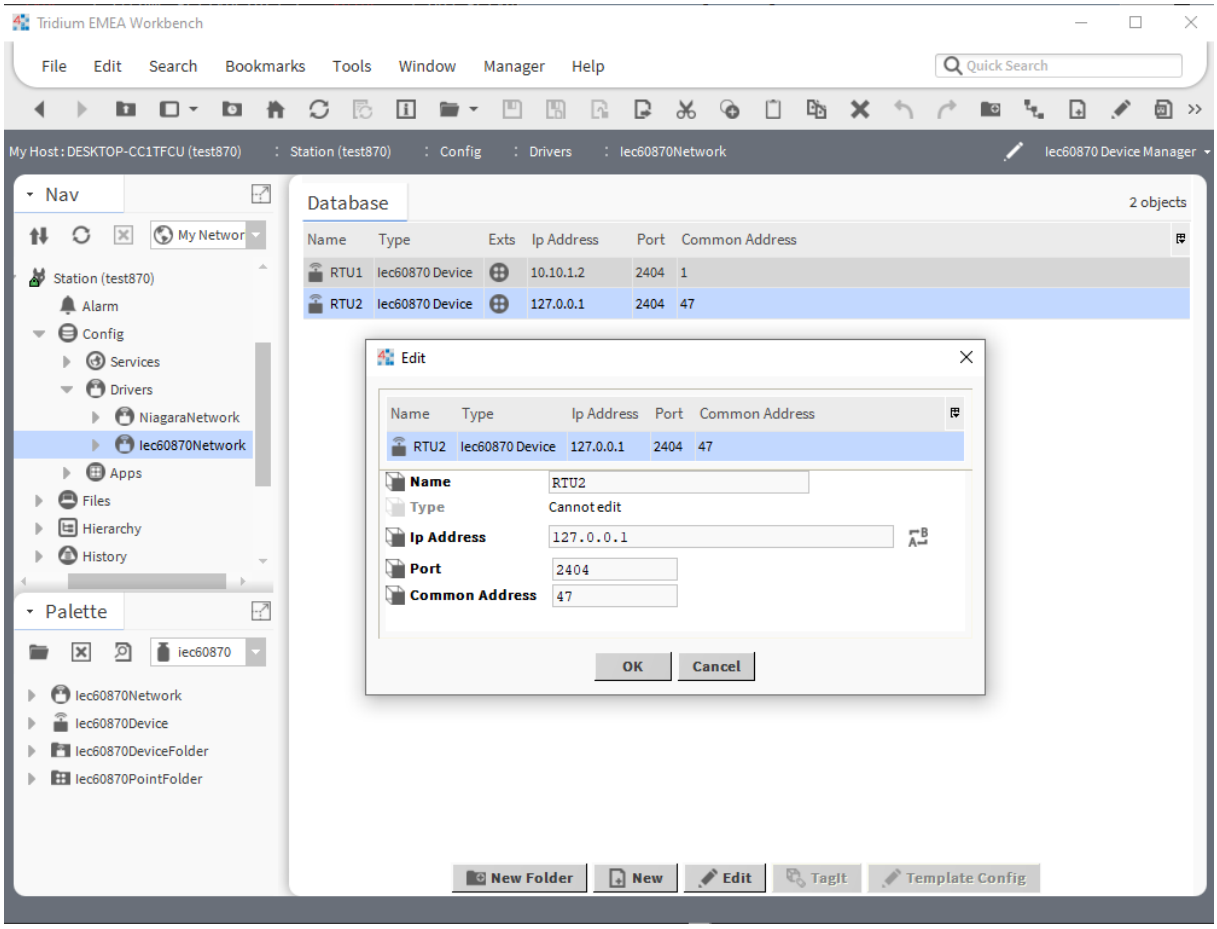

Figure 2: IEC 60870 device manager

6 IEC 60870 Devices

Each **Iec60870 Device** represents one controlled station (server) identified by its address consisting of:

- **Ip Address** – IP address of the IEC 60870-5-104 server.
- **Port** – TCP port number (default 2404).
- **Common Address** – identifies the controlled station (default 1).

The address must match the server configuration.

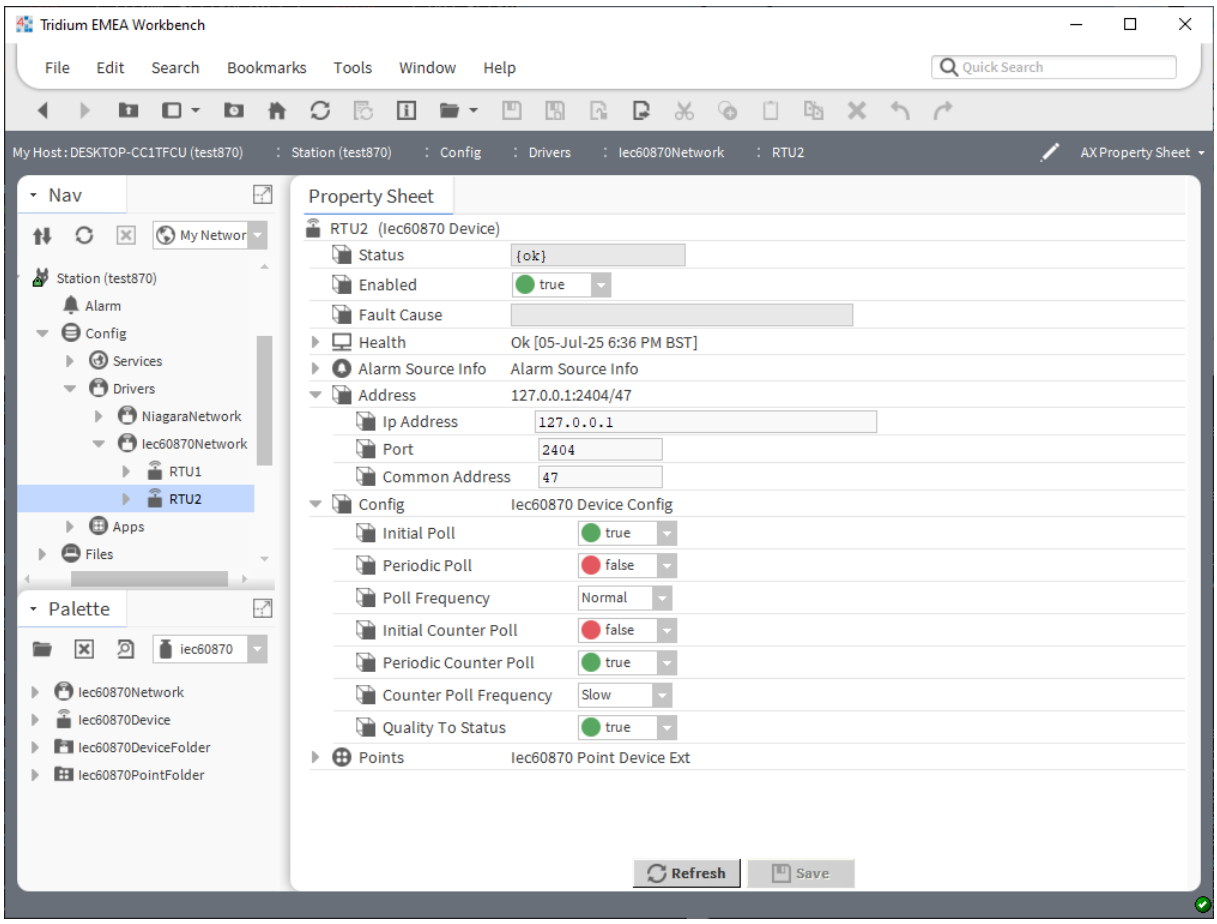

Figure 3: IEC 60870 device properties

Connection Process:

1. TCP connection established to server
2. **STARTDT** (Start Data Transfer) handshake
3. Initial **General Interrogation** (if enabled) for immediate point update
4. **TESTFR** (Test Frame) keepalive mechanism
5. Spontaneous data reception and optional periodic interrogations

7 IEC 60870 Points

IEC 60870-5-104 data points are called **Information Objects** (IO) and are uniquely identified by a combination of:

- **Information Object Address (IOA)** - A 3-byte address (1-16,777,215)

- **Type Identification** - Defines the data format and capabilities

Each Information Object contains:

- **Value** - The actual data (boolean, integer, float, etc.)
- **Quality Descriptor** - Status flags indicating data reliability
- **Timestamp** - Time of measurement/event (optional, depending on type)

7.1 Information Object Types

Information Object types in IEC 60870-5-104 define the structure and meaning of the data being transmitted. Each type determines how the value is encoded, whether it is digital or analog, if it has a timestamp, and how quality information is represented. The main categories are:

- **Single Point Information (M_SP)**: Represents a single binary status, such as the open/closed state of a breaker. Can be with or without timestamp.
- **Double Point Information (M_DP)**: Encodes two bits, often for states like off, on, intermediate, or indeterminate.
- **Step Position Information (M_ST)**: Indicates discrete positions, such as tap changer settings on transformers.
- **Measured Values (M_ME)**: Includes normalized, scaled integer, or floating-point analog measurements. These may represent voltages, currents, temperatures, etc.
- **Bitstring Output Information (M_BO)**: Represents a set of binary output statuses as a bitstring (typically 32 bits), used to convey the status or feedback of multiple binary outputs together with or without timestamp.
- **Packed Single Point Information (M_PS)**: Contains 32 single points packed into one message as a bitstring.
- **Integrated Totals (M_IT)**: Used for counter values, such as accumulated energy or flow totals. Supports counters with and without timestamps.

Each type is further specified by its suffix:

- **_NA**: No timestamp; only the current value is reported.
- **_TA** (for **M_ME** also **_TB** and **_TC**): 3-byte (CP24Time2a) short timestamp: minutes, seconds, and milliseconds only.
- **_TB**, **_TD**, **_TE**, **_TF**: 7-byte (CP56Time2a) full timestamp, precise to the millisecond and including date.

Some vendor documentation might include suffix **_1** at the end, e.g., **M_ME_TA_1**.

7.2 Quality Descriptors

Almost every **Information Object** includes a **Quality Descriptor** byte that indicates the validity and reliability of the data. The main quality flags are:

- **IV (Invalid, bit 7)** – The value is invalid (do not use for operational decisions).
- **NT (Not Topical, bit 6)** – The value is not current (may be stale).
- **SB (Substituted, bit 5)** – The value was substituted (e.g., operator override or test value).
- **BL (Blocked, bit 4)** – The value source is blocked (e.g., maintenance mode).
- **OV (Overflow, bit 0)** – For measured values, the value has exceeded its valid range.

The driver decodes these bits and exposes their meaning in the point's **Quality** field, so operators can quickly determine if a value is trustworthy.

A typical quality byte is structured as follows:

```
7  6  5  4  3  2  1  0
IV NT SB BL -  -  -  OV
```

Where a '1' means the flag is active. For example, 0x80 = IV (invalid), 0x40 = NT (not topical), and 0x01 = OV (overflow).

The driver maps **Quality Descriptor** bits to the Niagara point status as follows:

Flag	Niagara Status	Description
IV	Fault	Invalid value
NT	Stale	Not current
SB	Overridden	Substituted value
BL	Down	Source blocked
OV	Fault	Overflow condition

Note: the device's **Config** object can be used to disable this feature.

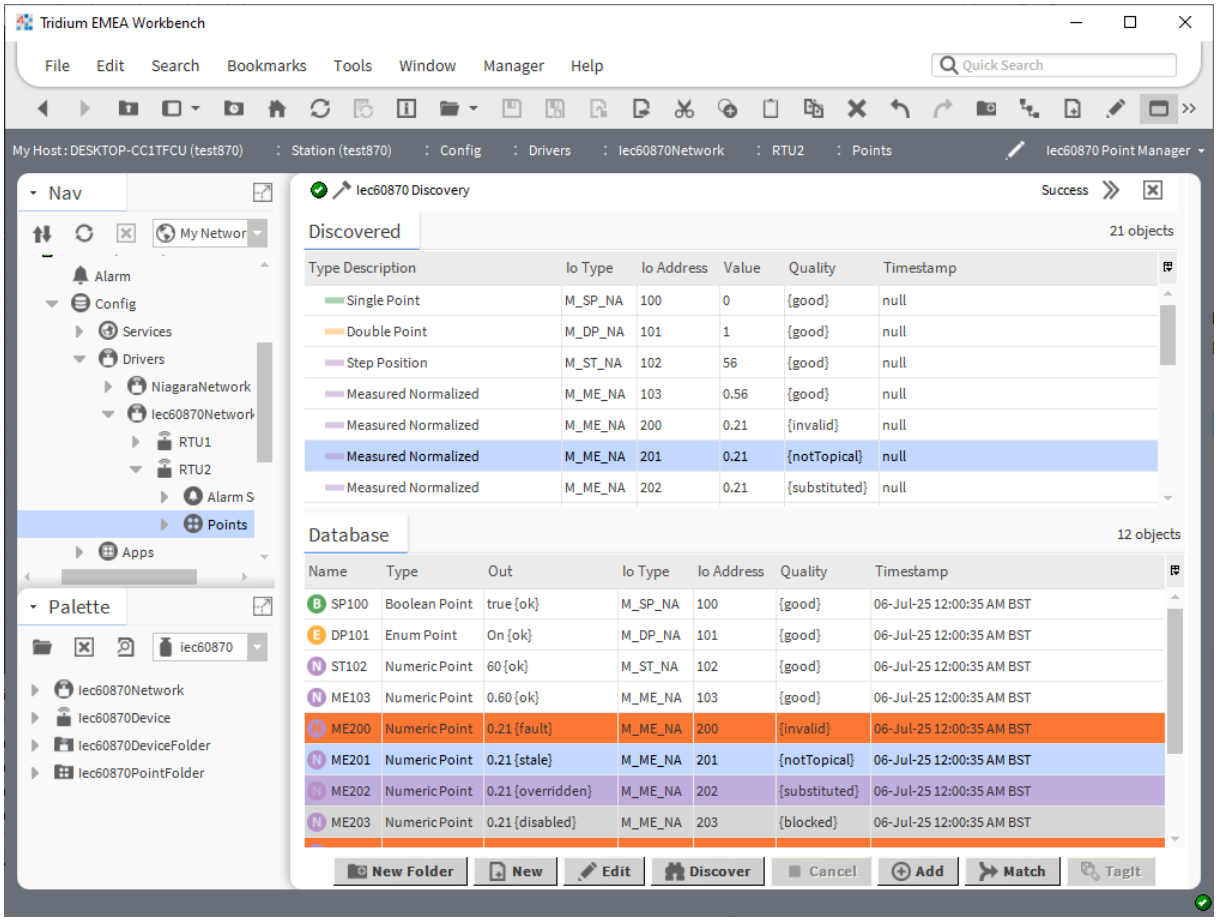

Figure 4: IEC 60870 points

7.3 Point Representation in Niagara

Each **Information Object** can be mapped to a Niagara point. A point is addressed with **Io Type** and **Io Address** properties. In addition to standard **Out** property to show real-time value, **proxyExt** contains **Quality** and **Timestamp** properties for quality flags and a timestamp.

Timestamps are updated with server time for types with timestamps and with local Niagara time for types without timestamps.

7.4 Niagara Point Types

The driver supports comprehensive IEC 60870-5-104 data types organized by category:

Type	Description	Niagara Type	Use Case
M_SP_NA	Single Point	Boolean Point	Current switch/breaker status
M_SP_TA	Single Point	Boolean Point	Status with short timestamp
M_SP_TB	Single Point	Boolean Point	Status with full timestamp
M_DP_NA	Double Point	Enum Point	Position (OFF/ON/Intermediate)
M_DP_TA	Double Point	Enum Point	Position with short timestamp
M_DP_TB	Double Point	Enum Point	Position with full timestamp
M_ST_NA	Step Position	Numeric Point	Tap changer positions
M_ST_TA	Step Position	Numeric Point	Position with short timestamp
M_ST_TB	Step Position	Numeric Point	Position with full timestamp
M_ME_NA	Normalized Value	Numeric Point	Scaled measurements
M_ME_TA	Normalized Value	Numeric Point	Scaled with short timestamp
M_ME_TD	Normalized Value	Numeric Point	Scaled with full timestamp
M_ME_NB	Scaled Value	Numeric Point	Integer measurements
M_ME_TB	Scaled Value	Numeric Point	Integer with short timestamp
M_ME_TE	Scaled Value	Numeric Point	Integer with full timestamp
M_ME_NC	Short Float	Numeric Point	IEEE 754 float values
M_ME_TC	Short Float	Numeric Point	Float with short timestamp
M_ME_TF	Short Float	Numeric Point	Float with full timestamp
M_IT_NA	Integrated Total	Numeric Point	Energy meters, counters
M_IT_TA	Integrated Total	Numeric Point	Counter with short timestamp
M_IT_TB	Integrated Total	Numeric Point	Counter with full timestamp
M_ME_ND	Measured No Quality	Numeric Point	Raw values without quality
M_PS_NA	Packed Single Point	Numeric Point (Bin)	16 binary points
M_BO_NA	Bitstring Output Status	Numeric Point (Bin)	32 binary output statuses
M_BO_TA	Bitstring Output Status	Numeric Point (Bin)	Outputs with short timestamp

Type	Description	Niagara Type	Use Case
M_BO_TB	Bitstring Output Status	Numeric Point (Bin)	Outputs with full timestamp

7.5 Point Discovery Process

IEC 60870 points are discovered automatically through **General Interrogation** and **Counter Interrogation** commands. The **Iec60870 Point Manager** displays discovered points with comprehensive information for effective point management.

Automatic Discovery Sequence:

1. Driver sends **General Interrogation** command with **Station Interrogation** qualifier
2. Server responds with all current point values and their current states
3. Driver automatically creates point entries in discovered pane
4. Same operation is repeated for **Counter Interrogation** command for integrated totals points

7.6 Point Update Logic

The driver supports two types of point updates: spontaneous reporting (sent automatically by the server when data changes) and interrogations (periodic polling requests to refresh all values).

7.6.1 Spontaneous Reporting

Spontaneous reporting consists of messages sent by the IEC 60870 server immediately whenever a point value changes or periodically. This mechanism ensures low-latency reporting without waiting for a polling cycle. The driver listens for spontaneous updates continuously after the STARTDT handshake. When a value changes, the server transmits a message containing the new data, timestamp, and quality flags, and the driver updates the Niagara point in real time.

Note: in some implementations counters (**M_IT** types) are not sent spontaneously and need to be polled.

7.6.2 Interrogations

Interrogations occur when the driver sends a General Interrogation request (for all points) and a Counter Interrogation request (for counters) as per poll scheduler or at startup to retrieve all point

values. The server responds with all current measurements and statuses in a burst of messages. This ensures that slow-changing or infrequently updated data is refreshed even if no spontaneous updates have occurred. Polling is configurable for frequency and can be disabled if not needed.

7.6.3 Update Configuration

The **Config** properties include:

- **Initial Poll**: whether to perform an initial General Interrogation after connection.
- **Periodic Poll**: whether to periodically re-poll all data points.
- **Poll Frequency**: the interval between periodic polls.
- **Initial Counter Poll**: whether to perform an initial Counter Interrogation.
- **Periodic Counter Poll**: whether to periodically poll counters.
- **Counter Poll Frequency**: the interval for periodic counter polling.
- **Quality To Status**: whether to map Quality Descriptor bits into Niagara point status (Fault, Stale, Down, Overridden).

These options are configured in the device's Config Property sheet, as shown in the configuration screenshot.

8 Troubleshooting

8.1 Systematic Troubleshooting Methodology

Step 1: Connection Verification

1. Verify basic network connectivity (ping test)
2. Test TCP port accessibility (telnet or netcat)
3. Check firewall rules on both client and server
4. Verify server is running and listening on port 2404

Step 2: Configuration Validation

1. Verify Common Address matches server configuration
2. Check IP address and port settings
3. Validate timeout parameters are appropriate for network
4. Confirm license is valid and not expired

Step 3: Protocol Communication

1. Monitor connection establishment (STARTDT sequence)
2. Verify TESTFR keepalive is functioning
3. Check for protocol errors in logs
4. Analyze sequence number behavior

Step 4: Data Flow Analysis

1. Verify General Interrogation success
2. Check point discovery process
3. Monitor spontaneous data reception
4. Validate point subscription status

8.2 Connection Problems

Connection Failed - Network Issues:

- **Symptoms**: "Connection refused" or timeout errors
- **Diagnosis**:
  - Test: `ping <server_ip>`
  - Test: `telnet <server_ip> 2404`
  - Check: Network routing and firewall rules
- **Solutions**:
  - Verify server is running and listening on port 2404
  - Check firewall allows TCP port 2404 bidirectional
  - Verify network routing between client and server
  - Test with different network interface if available

Connection Failed - Protocol Issues:

- **Symptoms**: Connection established but no data exchange
- **Diagnosis**:
  - Check STARTDT sequence completion
  - Monitor for protocol error messages
  - Verify sequence number progression
- **Solutions**:
  - Increase Response Timeout for slow networks
  - Check server protocol compliance

  - Verify Common Address configuration
  - Review server logs for protocol errors

8.3 Discovery Problems

No Points Discovered:

- **Symptoms**: Empty point list after discovery
- **Diagnosis**:
  - Check Common Address matches server configuration
  - Verify General Interrogation command acceptance
  - Monitor server response messages
- **Solutions**:
  - Confirm server supports General Interrogation (C_IC_NA_1)
  - Check server has configured data points
  - Verify server Common Address setting

9 FAQ

9.1 Can the driver control IEC 60870-5-104 devices?

No, this driver is read-only for safety in critical infrastructure environments. It supports monitoring only.

9.2 What is the maximum number of points supported?

Point limits depend on license type. Contact vendor for specific requirements.

9.3 Can multiple Niagara stations connect to the same IEC 60870-5-104 server?

This depends on the server implementation. Many servers support multiple concurrent client connections.

9.4 Does the driver support time synchronization or file transfer?

No, the current version focuses on real-time data monitoring only. Time synchronization commands and file transfer are not implemented.

9.5 How often should periodic general interrogation be used?

Use sparingly (Normal/Slow rates) as most data should come via spontaneous reporting. Use only for backup data collection or slow-changing values.

9.6 What happens if the server connection is lost?

The driver will automatically attempt to reconnect and re-establish data transfer. Point values will show as down until connection is restored.

9.7 Can I use custom port numbers?

Yes, configure the port in Comm Config. Standard port 2404 is recommended for compliance.

9.8 How do I know if my server is compatible?

The server must support IEC 60870-5-104 TCP/IP with General Interrogation. Most modern RTUs and PLCs with IEC 60870-5-104 interfaces are compatible.