Smart 4 I/O

Monitor and Control 4 Digital Inputs & 4 Relay Outputs over Copper or Fiber Ethernet with Real-Time Alerts

Smart 4 I/O

Introduction

The Smart 4 I/O is a programmable Ethernet I/O controller that interfaces with field devices such as sensors, push buttons, alarms, locks, and motors.

Each of the Digital Input and Relay Output channels are configurable through a built-in web management portal, and can be integrated with network management systems, industrial control systems, Internet of Things (IoT) frameworks, and REST-integrated automation platforms.

The Smart 4 I/O supports TLS/SSL encryption, IEEE 802.1X via RADIUS authentication (AAA), role based access control (RBAC), and event logging. The versatile 2-port (1xRJ45, 1xSFP) Ethernet interface offers network access redundancy and segmentation.

It can operate as a standalone unit, independently monitoring and controlling the state of its 4 inputs or 4 relay outputs, or pair with another Smart 4 I/O over a secure TLS/SSL-encrypted tunnel.

This System Pairing feature allows the Smart 4 I/O to transmit I/O bi-directionally across Ethernet between two remote locations.

Features
Monitor and Control 4 Digital Inputs / 4 Relay Outputs
SPDT-style relays simplify Normally Open/Closed relay setup
2-Port Gigabit Ethernet interface featuring 1x RJ45, 1x SFP
User-friendly embedded web management portal
Transport I/O between Smart 4 I/O units via System Pairing
NMS and SCADA/DCS integration options include: SNMPv1/ v2c/3, Modbus TCP, and DNP3
MQTT stack for real-time Publish/Subscribe telemetry
RESTful API with GET/POST/PUT request support
Hardened to operate in -40°F to +158°F (-40°C to +70°C)
DIN rail or wall mount (Wall mount ears included)
Designed, Engineered, and Assembled in the USA
Lifetime warranty

General Safety Practices

Intended Audience

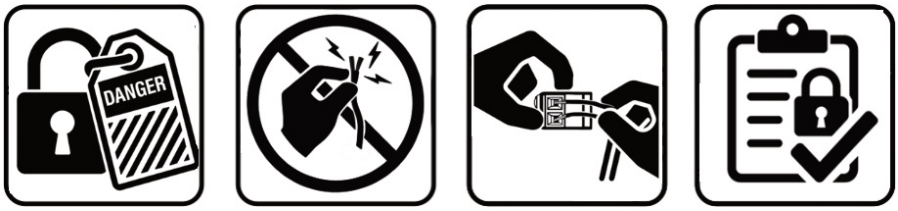
This guide is intended for use by knowledgeable installation, operation and repair personnel. Every effort has been made to ensure the accuracy of the information in this guide. However, due to constant product improvement, specifications and information contained in this document are subject to change without notice.

Electrical Safety

RLH recommends that installation and service personnel be familiar with the correct handling and use of electrical and network equipment prior to use. RLH also recommends that installation and service personnel follow all safety precautions including the use of protective personal equipment as required.

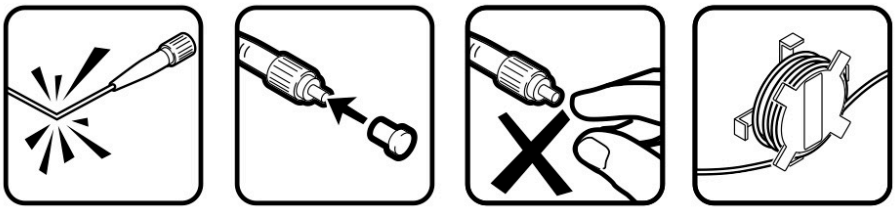
- Never install during a lightning storm or where unsafe high voltages are present
- Wiring leads leads can carry high DC voltages. Use caution when handling copper wiring
- Do not open the enclosure, there are no user serviceable parts

Caution - Severe Shock Hazard



- Always remove source voltage using proper lockout procedures prior to installation and service.
- Never wire any wet inputs without removing source voltage first
- Remove the terminal block when wiring
- Check that all equipment has been properly locked out before restarting or configuring the device

Fiber Cable



- Do not bend fiber cable sharply. Use gradual and smooth bends to avoid damaging glass fiber
- Keep dust caps on fiber optic connectors at all times when disconnected
- Do not remove dust caps from unused fiber
- Keep fiber ends and fiber connectors clean and free from dust, dirt and debris, contamination will cause signal loss
- Do not touch fiber ends
- Store excess fiber on fiber spools at site

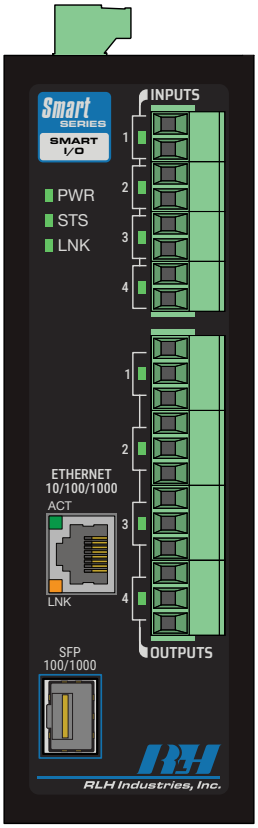
Laser Safety

Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cable connected to a transceiver emit laser light that can cause eye damage.

System Description

Smart 4 I/O

The Smart 4 I/O is a programmable Ethernet I/O controller designed for securely monitoring and controlling remote equipment used in industrial processes, utility (power, water, gas) systems, critical infrastructure, and building automation. Its Input channels detect digital signals (ON/OFF), while its Output channels drive external equipment using onboard mechanical relays.



Smart 4 I/O

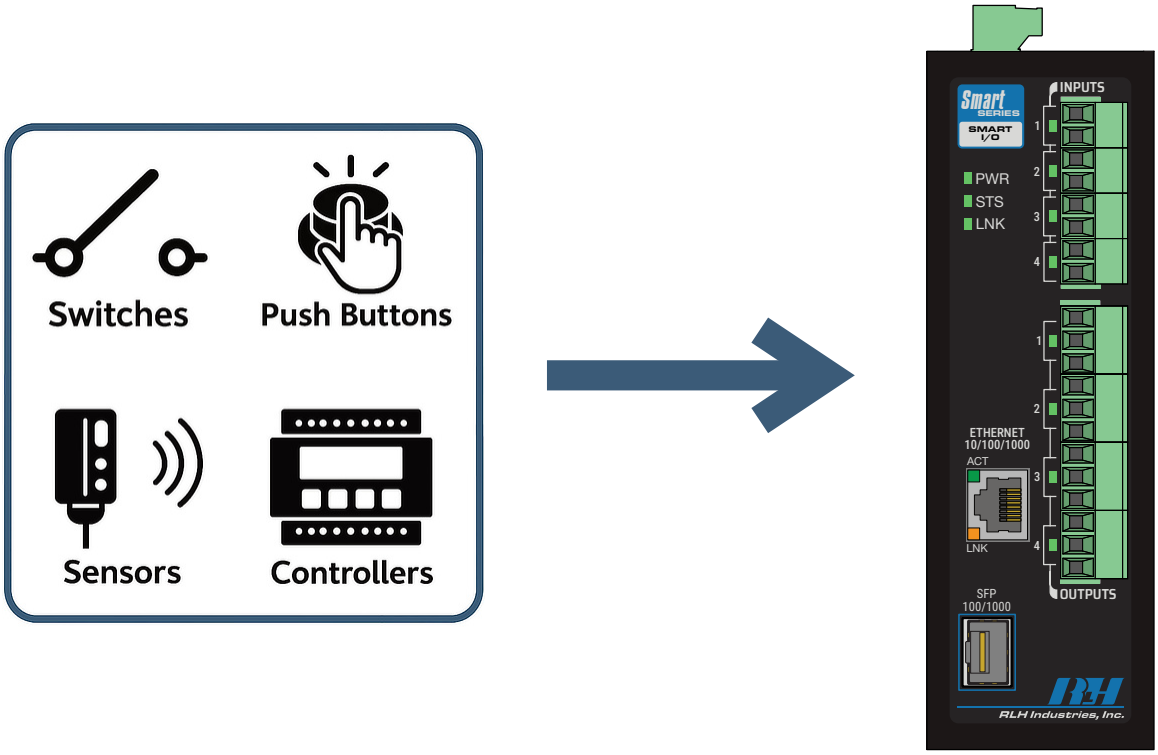
Traditional control system architectures often rely on dedicated wiring from each field device back to a centralized panel ("home-run" wiring). This approach can lead to excessive cabling, crowded panels, and higher installation costs. Additionally, at remote or unmanned sites, verifying a field device's status or diagnosing a fault typically requires sending a technician on-site to investigate.

The Smart 4 I/O overcomes these limitations by offering a network-accessible interface to manage and integrate each I/O point onto a single system. It acts as a bridge between hardwired field devices and Ethernet-based control systems, while also including a self-hosted web management portal. This decentralized architecture significantly reduces wiring needs, and simplifies field device maintenance.

Smart 4 I/O (Field Device Inputs)

Various devices such as limit switches, push buttons, status sensors, or a controller's dry contact outputs, can be wired into the Smart 4 I/O's four available Digital Input channels. The figure below illustrates how the Smart 4 I/O interfaces with field input devices.

Each Digital Input channel detects an ON (closed contact) or OFF (open contact) state from its field device. In this manner, the Smart 4 I/O monitors the status of remote equipment and sensors in real time, converting their hardwired signals into data available across an Ethernet network for remote monitoring and alerts. The system also offers wet input models that instead determine an ON or OFF state based on the voltage applied to a channel's contacts.



Field Device Input Examples

Field Device Examples (Digital Inputs)

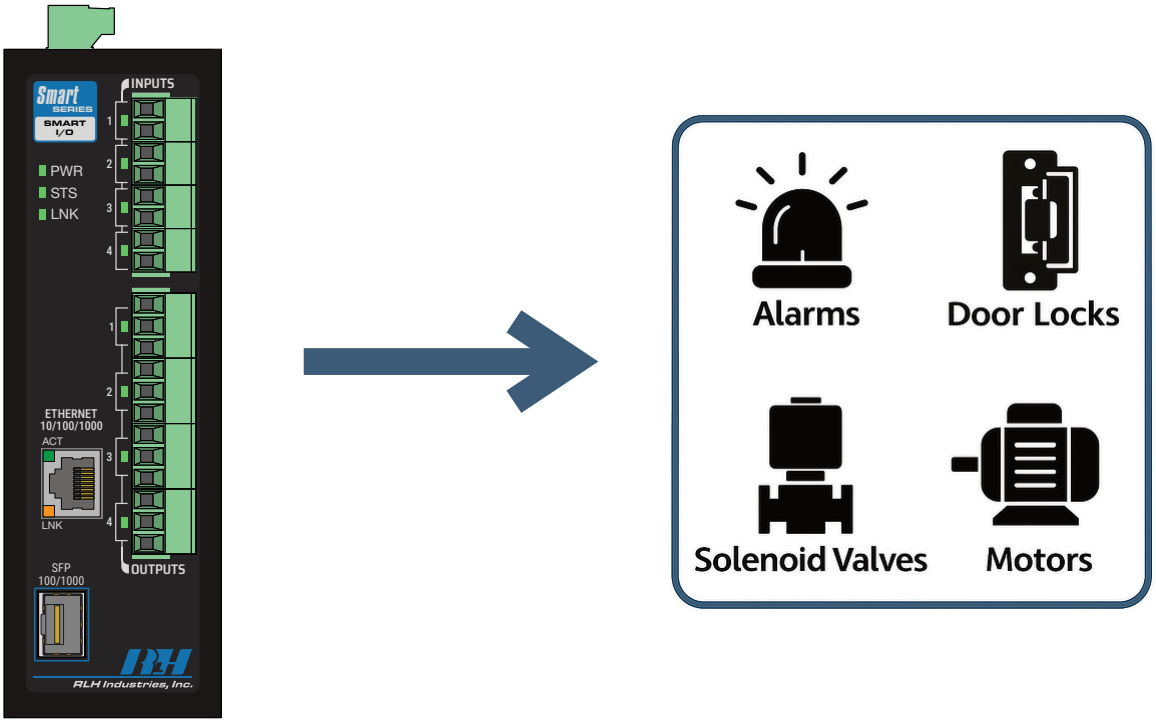
In practice, field devices monitored by the Smart 4 I/O can include:

- **Door / Guard Switch:** Reports when a door, gate, or safety guard has opened
- **Float / Level Switch:** Signals a high-water or sump-full alarm before overflow occurs
- **Generator Run Contacts:** Confirms that a generator has started and is actively running
- **UPS Power-fail Relays:** Reports loss of utility input power to backup systems
- **Temperature Trip:** Detects over-temperature conditions that could damage equipment
- **Cabinet Door Switch:** Triggers when an enclosure or cabinet is opened
- **Emergency-stop Loop:** Reports when an emergency-stop button is pressed, or a loop fault occurs
- **Leak-detection Sensor:** Detects water intrusion or leaks near electrical equipment

Smart 4 I/O (Field Device Outputs)

The figure below illustrates how the Smart 4 I/O interfaces with field device actuators/loads ("relay-controlled outputs"). Each Relay Output channel provides a Form-C (SPDT) relay contact that can be energized (ON) or de-energized (OFF) to switch an external circuit. When a channel turns ON, its NO (Normally Open) contact closes and NC (Normally Closed) contact opens. The contacts will return to their normal state once the channel turns OFF.

Relay Output channels are turned off manually via the system's embedded web management portal, automatically when paired with another Smart 4 I/O, and either manually or automatically via the system's configured protocol integration arrangement (SNMP, Modbus TCP, DNP3, MQTT).



Field Device Output Examples

Field Device Examples (Relay-Controlled Outputs)

In practice, field devices controlled by the Smart 4 I/O can include:

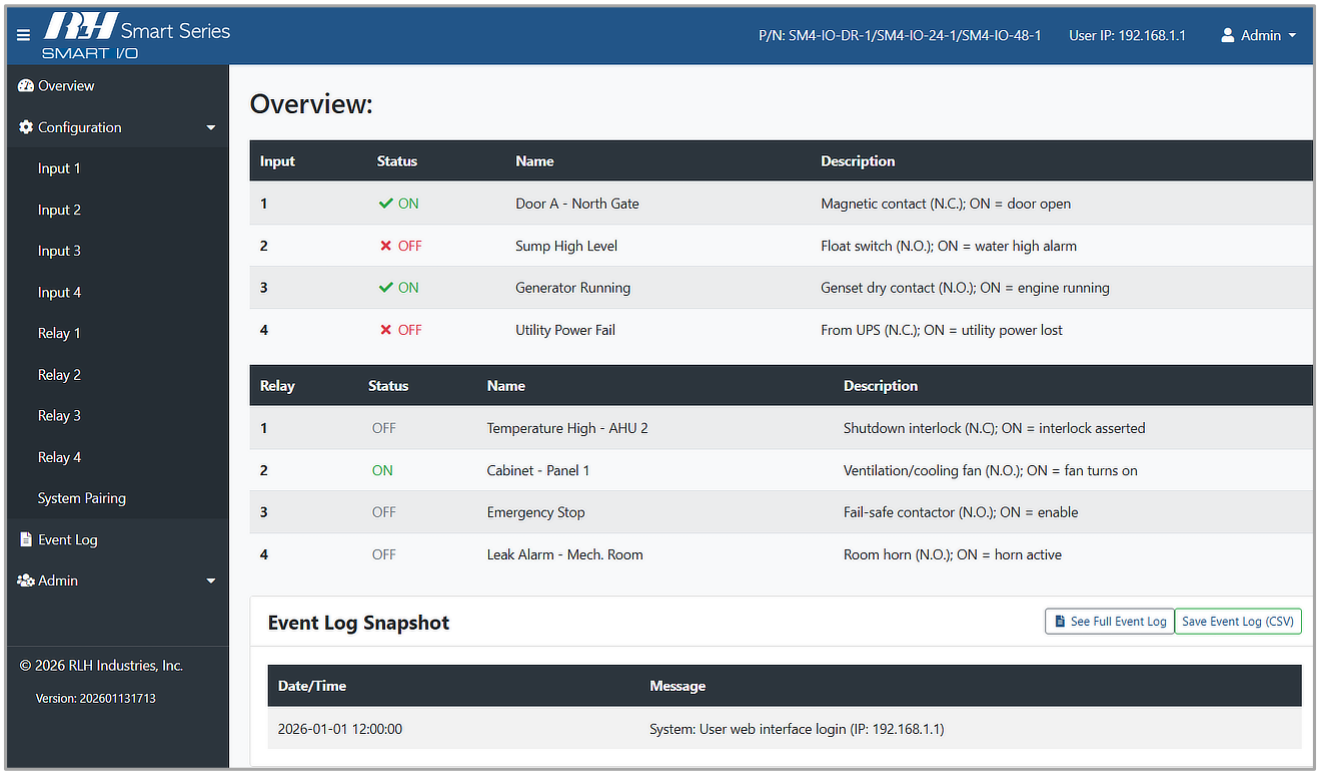
- **Door Lock / Strike:** Releases the latch of an electric strike or maglock to unlock a secured door
- **Sump Pump Starter:** Activates a pump starter to drain excess water from collection basins
- **Run Indicator Lamp:** Illuminates a panel lamp to indicate that a generator is running
- **Alarm / Siren:** Sounds an alarm horn or strobe when a fault (e.g., power loss) is detected
- **Shutdown Interlock:** Triggers a safety trip circuit to shut down equipment that is overheating
- **Ventilation Fan:** Powers a cabinet or panel fan to provide forced cooling and airflow
- **Fail-safe Contactor:** Controls power to machinery in response to an Emergency-stop circuit
- **Horn / Beacon:** Activates a horn with beacon lights to signal an environmental status alarm

Web Management Portal / GUI

This system features an embedded web management portal that centrally administers each I/O channel as a network-accessible, configurable endpoint for remote monitoring and control.

Through this interface, operators can review Input or Output statuses, assign channel names and descriptions, manually toggle channel states as ON or OFF, establish email alerts (SMTP) or traps (SNMP) to trigger upon state changes, configure supported communication protocols, and audit or export system event logs.

The Smart 4 I/O displays the state of its four Digital Input ("Input") channels, and four Relay Output ("Relay") channels



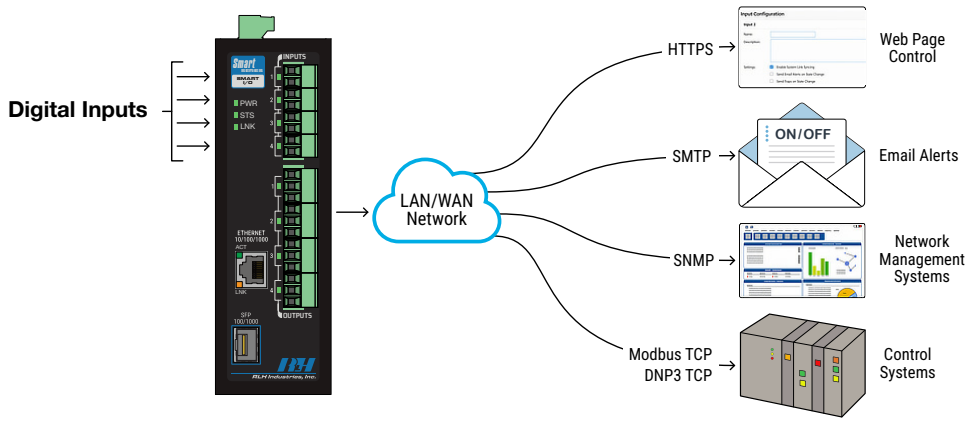
Its I/O summary table will display the detected input state (ON/OFF) for each Input channel, and the energized (ON) or de-energized (OFF) state of each channel's relay, alongside user-configurable labels and descriptions.

Inputs may be logically inverted for testing and commissioning, while Relays can be logically assigned to an ON state, OFF state, or a "mapped" state for automatically adjusting between ON or OFF based upon the Input of another paired Smart 4 I/O unit.

Standalone System Operation

The Smart 4 I/O can operate independently as a standalone system, monitoring and controlling its 4 Digital Inputs or 4 Relay Outputs without requiring a connection to external control systems or an additional Smart 4 I/O module. It may also be integrated through standard SCADA, network management, and telemetry protocols such as Modbus TCP, DNP3, SNMP, or MQTT for polling, event reporting, or cloud publishing.

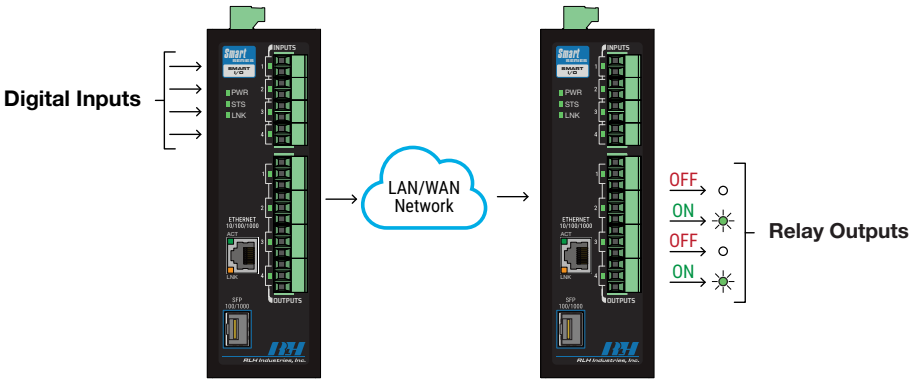
When used independently, the Smart 4 I/O continuously monitors the state of connected field devices, and/or provides remote actuation of connected field devices. All I/O state change activity is recorded within its embedded event log. Email notifications and SNMP trap notifications provide immediate alerts when I/O conditions change. I/O channels can be configured to be polled or published through supported communication protocols.



System Pairing (One-to-One)

In addition to operating as an independent, standalone unit, the Smart 4 I/O can pair together with another Smart 4 I/O module over a secure point-to-point TLS/SSL-encrypted tunnel through System Pairing. When paired, Relay Output channel states can be mapped to a specific Digital Input channel, automatically energizing (ON) or de-energizing (OFF) in response to the mapped input's ON/OFF state. Each participating Relay Output channel will mirror the ON/OFF state of their mapped input within a typical response time of 8ms.

The participation and mapping of Digital Input / Relay Output channels in a System Pairing sync are fully configurable, including support for multiple Relay Outputs to share the same input mapping. System Pairing provides flexibility in designing I/O control paths between two Smart 4 I/O units.



System Pairing Diagram

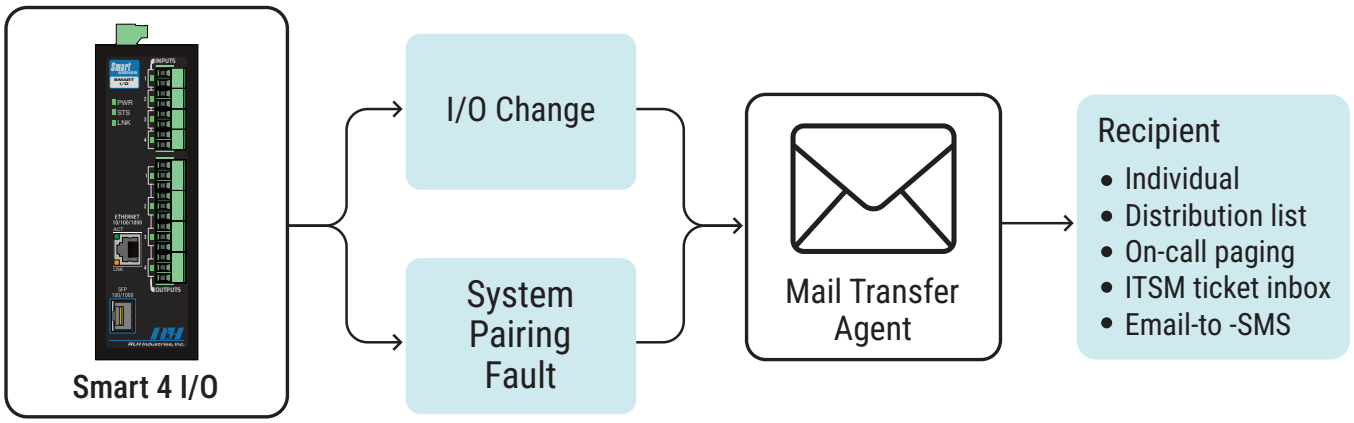
Protocols, Services, & Integration

The Smart 4 I/O features a communication interface and service integration layer that empowers solution architects to leverage existing control system architectures, optimize I/O data transmission across a network, effectively report I/O changes or faults to operators and monitoring systems, and enforce secure access with authenticated and authorized user sessions. Encrypted data transport (TLS) is also supported for applicable services.

Each of the standards-based network protocols, services, and interfaces underpinning this integration layer enables the systems' interoperability with several industrial or enterprise systems, including:

- **Mail Transfer Agents (MTA):** Email notifications via SMTP for I/O activity, and pairing faults
- **Industrial Control Systems (ICS):** SCADA/DCS interoperability via Modbus TCP and DNP3/TCP
- **Network Management Systems(NMS):** Device and I/O monitoring, control, and alerting via SNMPv1/v2c/v3
- **Building Management Systems (BMS):** Poll HVAC, lighting, and alarm points via Modbus TCP
- **Industrial Internet of Things (IIoT):** Upload I/O telemetry to Cloud dashboards via MQTT
- **Port-based Network Access Control (PNAC):** IEEE 802.1X client available on both Ethernet ports (RJ45, SFP)
- **Authentication, Authorization, and Accounting (AAA):** Domain authentication via RADIUS client
- **Application Programming Interfaces (API):** Third-party, external applications via a REST API

Mail Transfer Agents (MTA)



Mail Transfer Agents (MTA)

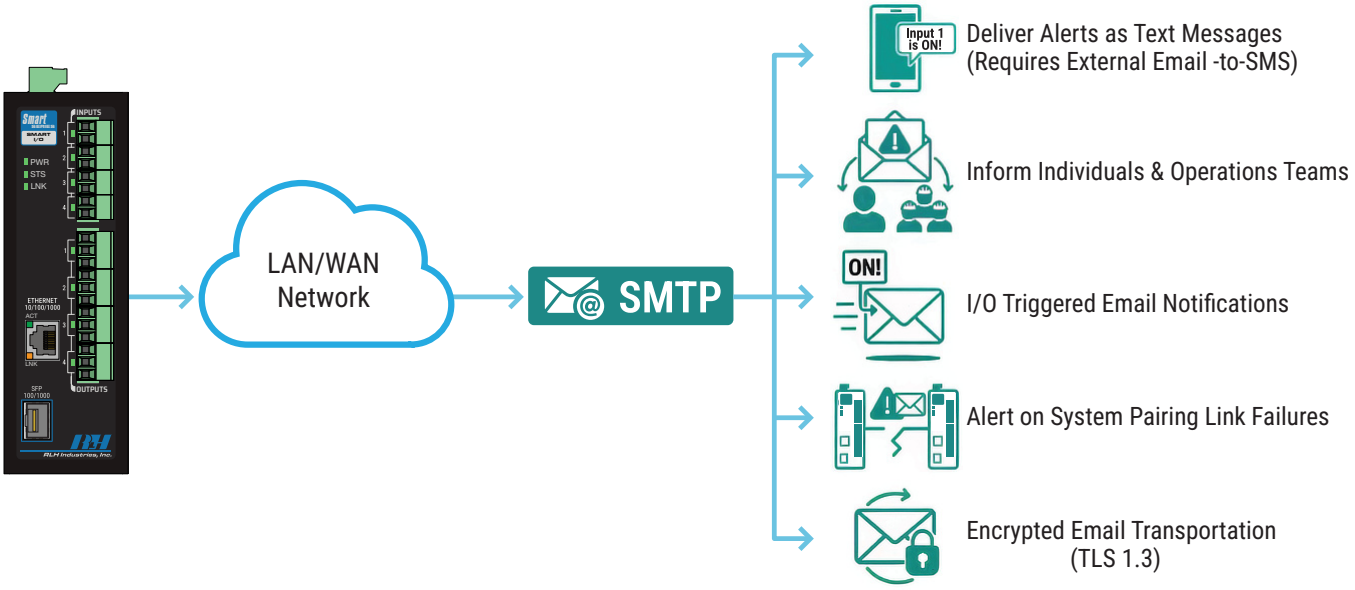
When a Digital Input or Relay Output changes its ON/OFF state, or a System Pairing fault occurs, the device can automatically notify operations staff by generating a notification through an organization's email messaging system. I/O email alerts include the I/O's user-defined name and description, alongside the new ON/OFF state. System Pairing email alerts report the change (ON/OFF) in connection status.

Email notifications can be addressed to individuals, distribution lists, or email-ingestion addresses used by on-call paging and IT Service Management (ITSM) tools. An email-to-SMS gateway can also be used to reach mobile phones, when dashboards are unattended. These alerts are routed through an organization's email server, functioning as a Mail Transfer Agent (MTA) that uses the SMTP protocol.

Simple Mail Transfer Protocol (SMTP)

When an organization's email server is configured on the Smart 4 I/O to support email notifications, the device acts as an email client, composing a concise message for each I/O change event or System Pairing link fault that occurs. The configured email server then distributes those alerts to the email address entered by the user. I/O channels must be individually enabled to transmit email notifications.

Email transportation can be encrypted using the latest version of TLS (TLS 1.3), to ensure message confidentiality and secure delivery through the organization's email infrastructure. A built-in Send Test Email function is available to verify connectivity and authentication settings during initial provisioning, or troubleshooting.



Simple Mail Transfer Protocol (SMTP)

When configuring I/O channels, and enabling email notifications, it is important to use meaningful channel names e.g., "Door A - North Gate", "Sump High Level") and descriptions (e.g., "Magnetic contact (N.C.); ON = door open", "Float switch (N.O.); ON = water high alarm") to ensure that alerts are easy to interpret once received.

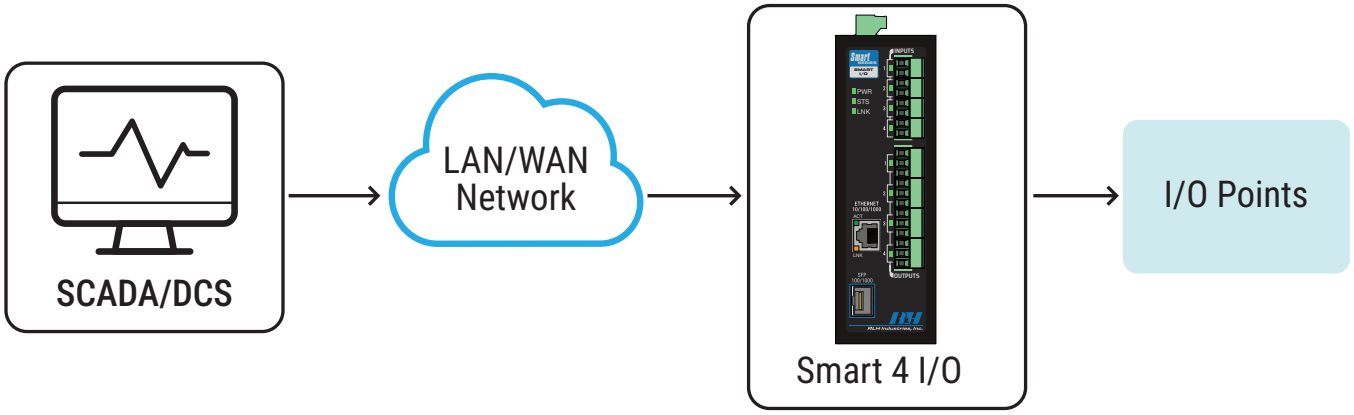
Message Content and Formatting (I/O Change)

- Subject Line: [I/O Channel Name] was changed
- Body: [I/O Channel Name] status was changed to [On/Off].
  Description:
  [I/O Channel Description]
  RLH Industries Smart Bidi Device

Message Content and Formatting (System Pairing Fault)

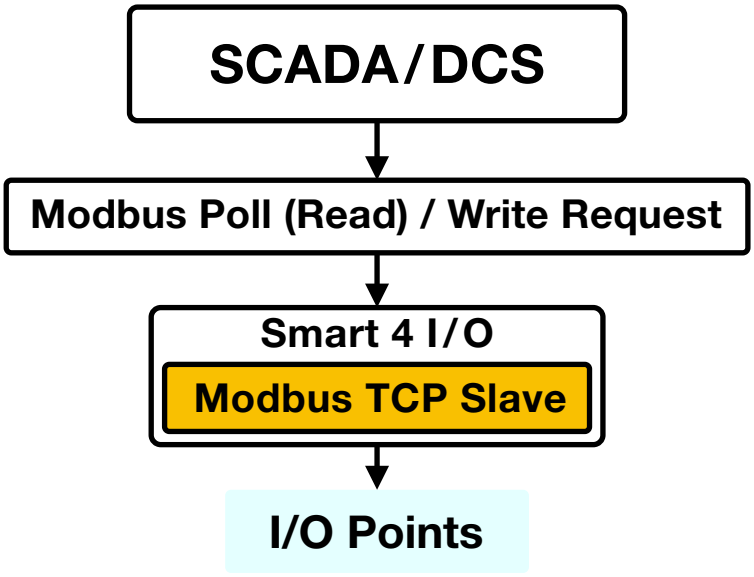
- Subject Line: [I/O Channel Name] was changed
- Body: [I/O Channel Name] status was changed to [On/Off].
  RLH Industries Smart Bidi Device

Industrial Control Systems (ICS)



Industrial Control Systems (ICS)

When an industrial PLC/RTU, HMI, or SCADA/DCS system needs to read I/O statuses from remote cabinets, or actuate equipment at unmanned sites, operators can incorporate the Smart 4 I/O to expose those field I/O points over Ethernet to an existing control system. The Smart 4 I/O may both report discrete statuses (e.g., limit switches, alarms), and execute commands such as starting pumps, enabling fans, or initiating trip/shutdown control sequences.



Modbus I/O Points

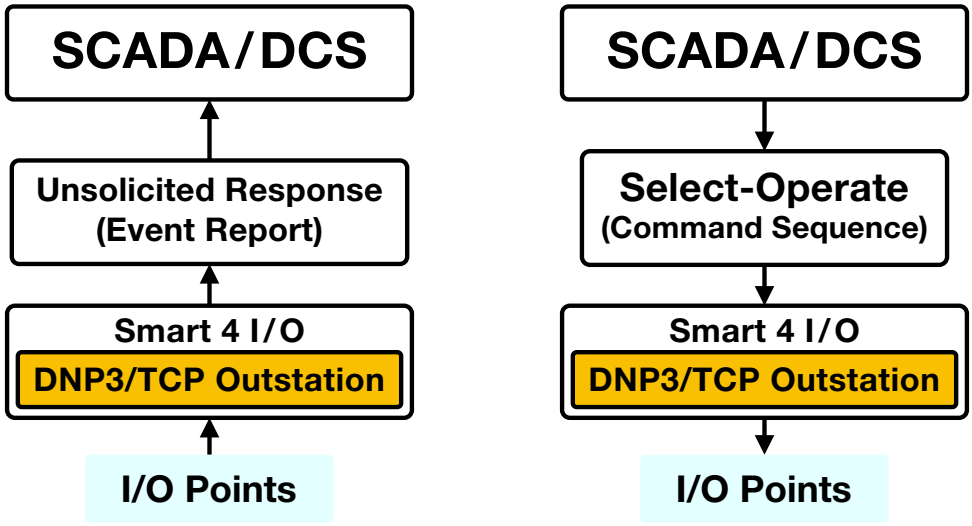
The modules can operate as Modbus TCP slaves (servers), allowing their I/O points to be directly consumed by a Modbus TCP master (client). This is typically a SCADA/DCS host, PLC/RTU controller, or HMI workstation. Clients poll I/O points on a fixed scan and, where permitted, can issue write requests to drive outputs.

The Smart 4 I/O exposes four discrete inputs for read-only operations, and four relay points that are both readable and writable from the Modbus master.

Industrial Control Systems (ICS)

In electric-utility and wastewater treatment environments, supervisory hosts often use DNP3's event-driven reporting model with event classes, unsolicited reporting, and Control Relay Output Block (CROB) operations. The Smart 4 I/O can function as a DNP3 outstation (server) to support these core DNP3 features, and integration with DNP3 masters (clients).

The Smart 4 I/O exposes both Binary Inputs (BI) and Binary Outputs (BO), accepting relay control through CROB-facilitated control functions (e.g., "Select-Operate" execution). When unsolicited reporting is enabled, I/O change-of-state events are automatically pushed to the DNP3 master without requiring a periodic Class 0 poll.



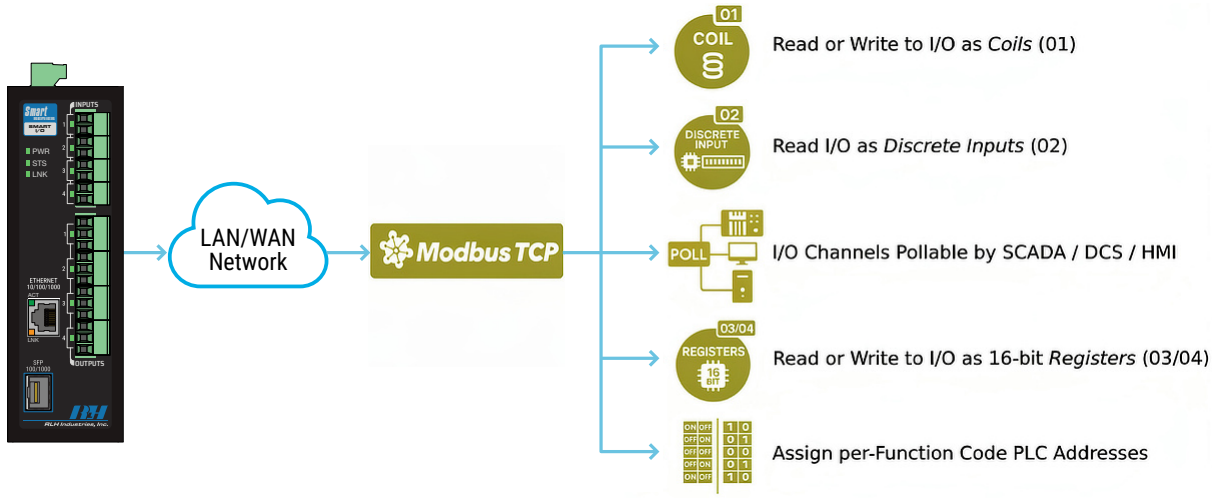
Industrial Control Systems (ICS) I/O Control

When operating as a DNP3/TCP outstation, the Smart 4 I/O offers event-based reporting and remote I/O control capabilities. Instead of relying on fixed-rate scans, the device can automatically send updates when I/O states change, and also accept standard control commands for remote operation.

The Smart 4 I/O's capacity for functioning as a Modbus TCP slave and/or DNP3/TCP outstation extend an Industrial Control System's I/O coverage across networked sites without provisioning a new controller, or installing additional home-run wiring.

Modbus TCP

The Smart 4 I/O can expose its connected field I/O to PLC, HMI, and SCADA/ DCS clients over the Modbus TCP protocol as a Modbus TCP slave. I/O statuses are presented as single-digit data points, or 16-bit registers, for ensuring broad compatibility across different Modbus TCP masters.



Modbus TCP

Modbus Data Object Mapping

I/O is exposed over Modbus TCP as standard Modbus data types: Coils, Discrete Inputs, Holding Registers, and Input Registers. The Smart 4 I/O's object data types are published across eight contiguous, configurable address blocks. The first four addresses correspond to input status readings (read-only), and the last four to relay control/status (read/write).

First Four Addresses (Digital Inputs 1-4): Read-only

- Supports Modbus read function codes: 01 (Coils), 02 (Discrete Inputs), 03/04 (Holding/Input Registers)
- All Modbus write function codes are rejected
- Digital Inputs are mirrored (read-only) onto the Coils (01) and Holding Registers (03) addresses

Last Four Addresses (Relay Outputs 1-4): Read + Write

- Supports Modbus read function codes: 01 (Coils), 02 (Discrete Inputs), 03/04 (Holding/Input Registers)
- Supports Modbus write function codes: 05/15 (Coils), 06/16 (Holding Registers)
- Relay Outputs are mirrored (read-only) onto the Discrete Inputs (02) and Input Registers (04) addresses

Function Code	Operation	Digital Inputs 1~4	Relay Outputs 1~4
01	Read Coils	✔	✔
02	Read Discrete Inputs	✔	✔
03/04	Read Registers (Holding / Input)	✔	✔
05/15	Write Coils (Single / Multiple)	✘	✔
06/16	Write Registers (Single / Multiple)	✘	✔

Modbus TCP Function Codes (Read Requests)

Coils (0x) represent Relay Outputs and Discrete Inputs (1x) represent Digital Inputs. For compatibility with Modbus TCP masters (clients) that can only read one of the two address spaces (0x or 1x), the Smart 4 I/O exposes read-only mirrors of Digital Inputs onto the Coils (0x) mapping, and read-only mirrors of Relay Outputs onto the Discrete Inputs (1x) mapping. Consequently, Coil/Discrete Input values exist for both Digital Input and Relay Output channels.

Function Code 01 (Address Prefix 0x, Hex 0x01): Read Coils

- Returns one or more relay/coil states as single-bit values
- 0 = OFF/de-energized, 1 = ON/energized

Function Code 02 (Address Prefix 1x, Hex 0x02): Read Discrete Inputs

- Returns one or more inputs as single-bit values
- 0 = OFF/open, 1 = ON/closed

Function Code 03 (Address Prefix 4x, Hex 0x03): Read Holding Registers

- Returns one or more 16-bit holding registers
- 0x0000 = OFF/de-energized, 0x00FF = ON/energized

Function Code 04 (Address Prefix 3x, Hex 0x04): Read Input Registers

- Returns one or more 16-bit input registers
- 0x0000 = OFF/open, 0xFF00 = ON/closed

Modbus TCP Function Codes (Write Requests)

Function Code 05 (Address Prefix 0x, Hex 0x05): Write Single Coil

- Writes a single-bit OFF or ON state to a relay/coil
- 0 = OFF/de-energized, 1 = ON/energized

Function Code 06 (Address Prefix 4x, Hex 0x06): Write Single Holding Register

- Writes a 16-bit ON or OFF state to a holding register
- 0x0000 = OFF/de-energized, 0x00FF = ON/energized

Function Code 15 (Address Prefix 0x, Hex 0x0F): Write Multiple Coils

- Writes an OFF or ON state to multiple relays/coils in a byte
- For a single point, 0x0000 = OFF/de-energized, 1 = ON/energized

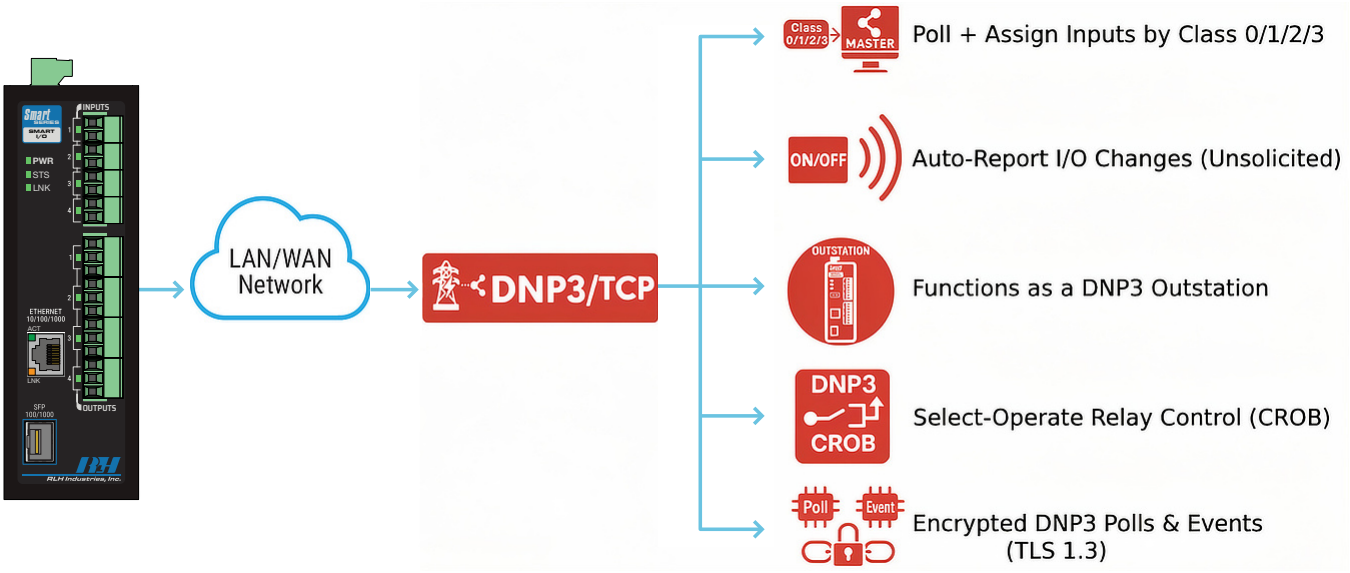
Function Code 16 (Address Prefix 4x, Hex 0x10): Write Multiple Holding Registers

- Returns one or more 16-bit input registers (big-endian)
- For a single point, 0x0000 = OFF/de-energized, 1 = ON/energized

DNP3/TCP

The Smart 4 I/O can operate as a DNP3/TCP outstation, providing time-stamped events and deterministic two-step relay actuation. A SCADA/DCS DNP3 master can perform Class 0 integrity polls (static data) and Class 1/2/3 event polls, while the Smart 4 I/O can also push unsolicited events so alarms appear without waiting for the next scan.

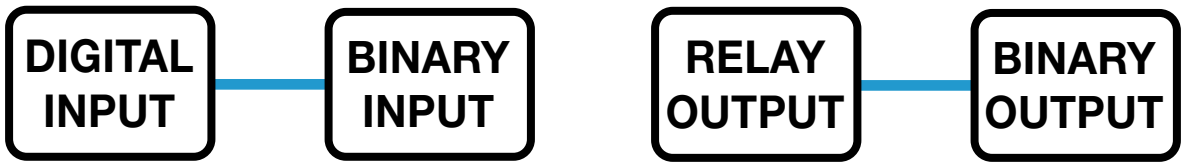
Relay Outputs are controllable using Control Relay Output Block (CROB) commands in a Select-Operate sequence (e.g., LATCH_ON, LATCH_OFF, PULSE_ON, and PULSE_OFF). Transport security is available via TLS 1.3, encrypting DNP3/TCP polls and events. For accurate Sequence of Events (SOE) timestamps, the master should periodically time-sync the Smart 4 I/O when operating as an outstation.



DNP3/TCP

DNP3 Data Object Mapping (Overview)

DNP3 organizes I/O data into standardized objects; each object belongs to a defined Object Group and Variation that specifies the data's encoding, quality flags, and (where supported) timestamps. In this model, Digital Inputs are represented as Binary Inputs (BI) that a DNP3 master can read, while Relay Outputs are represented as Binary Outputs (BO). Binary Outputs may be read as a Binary Output Status (BOS), and controlled through Control Relay Output Block (CROB) operations.



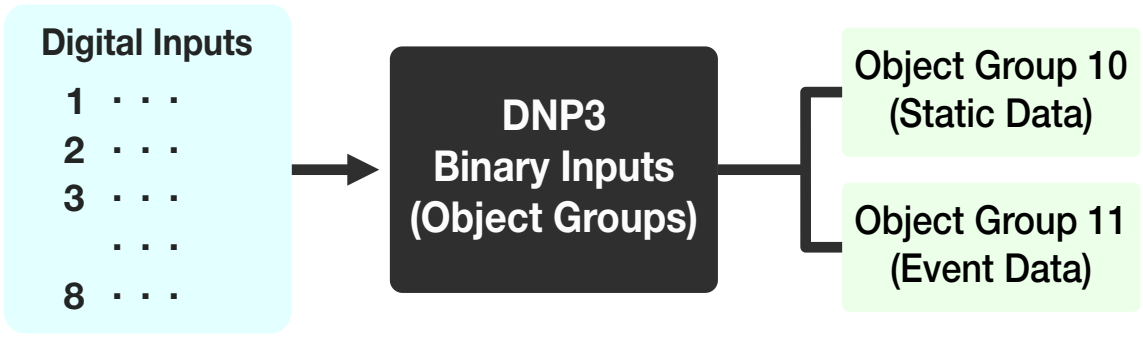
The Smart 4 I/O implements these standardized DNP3 object and control formats for its integration within DNP3-based control and SCADA architectures.

DNP3 Data Object Mapping (Binary Inputs)

Digital Inputs → Binary Inputs (BI)

The Smart 4 I/O's DNP3/TCP implementation maps its Digital Inputs as Binary Inputs (BI). These Binary Inputs are reported using DNP3 Object Groups that either return the current value of each Digital Input (Object Group 1), or instead provide a Change-of-State (COS) event buffer of the Digital Input state transitions that have occurred since the last COS event buffer retrieval (Object Group 2). Timestamps may optionally be included for Object Group 2 Variations.

COS events (Object Group 2) can also be transmitted to a DNP3 master as unsolicited responses, allowing the Smart 4 I/O to report input state changes immediately as they occur, without requiring continuous polling.



Object Group 1 (Binary Input, Static Data)

Binary Inputs may be polled to acquire their current static state using DNP3 Object Group 1. The Smart 4 I/O supports Object Group 1 Variation 1 (Binary Input) and Object Group 1 Variation 2 (Binary Input Status), where Variation 2 contrasts with Variation 1 by including status (quality) flags alongside each point's value. Variation 0, common to all Object Groups, serves as a wildcard request from the DNP3 master, prompting the Smart 4 I/O to respond with its configured or default Variation for that particular Object Group.

When the Smart 4 I/O acts as a DNP3/TCP outstation and receives a poll request for Variation 1 (g1v1), Variation 1 (g1v1), or Variation 2 (g1v2), it will always respond using Variation 2 (g1v2). In this response, each Binary Input is represented by a one-byte flag field. Inputs that are active (ON) have their Point Value bit and Online flag bit set to (1), returning a value of 0x03.

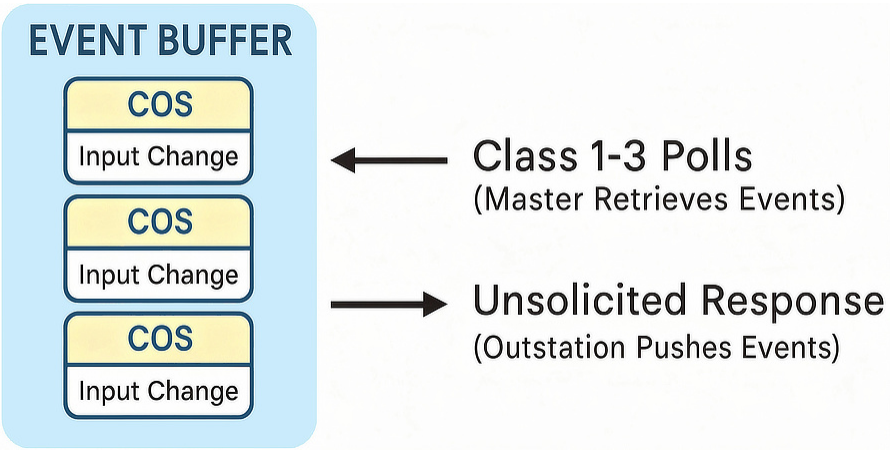
Group 1, Variation 2 (g1v2): Binary Input Status

- Presents the current Binary Input states, with quality flags, in a series of eight bytes
- For a single point, 0x02 = OFF/open, 0x03 = ON/closed

Input State	Online Bit (b1)	Point Value Bit (b0)	Binary Pattern	Returned Byte (Hex)
`OFF / Open Contact`	1	0	00000010	0x02
`ON / Closed Contact`	1	1	00000011	0x03

Object Group 2 (Binary Input, Event Data)

Binary Input Events are reported using DNP3 Object Group 2, which records each Change-of-State (COS) transition that occurs on a Digital Input. Each input can be assigned to a DNP3 Event Class (1, 2, or 3) using the web interface's configuration menu. These Classes define which events are returned during specific Class 1-3 polls from a DNP3 master, while assigning the inputs to Class 0 excludes them from event reporting, making their status only available through static (Object Group 1) reads. Detected COS events are stored in the Smart 4 I/O's internal DNP3/TCP outstation event buffer, and may be retrieved by a DNP3 master via Class 1-3 polls, or transmitted automatically as unsolicited responses.



Timestamps may accompany the events when using Object Group 2 Variation 2 (g2v2) or Variation 3 (g2v3). For ensuring timestamp accuracy, it is important to first establish the device's date and time using the Date & Time webpage.

Group 2, Variation 1 (g2v1): Binary Input Event - Without Time

- Returns COS events without timestamp data
- For a single point, 0x02 = OFF/open, 0x03 = ON/closed

Group 2, Variation 2 (g2v2): Binary Input Event - With Absolute Time

- Appends the absolute time-of-occurrence to each event (UTC from the outstation's synced clock)
- For a single point, 0x02 = OFF/open, 0x03 = ON/closed

Group 2, Variation 3 (g2v3): Binary Input Event - With Relative Time

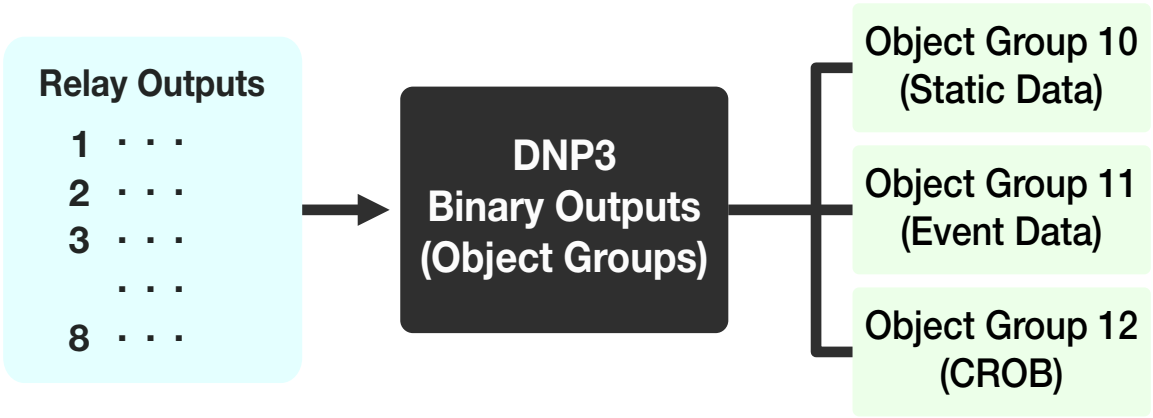
- Sends a Common Time of Occurrence (CTO) once, then each event includes a relative offset (ms)
- The timestamp is based on a Common Time of Occurrence (CTO), in relation to other events
- For a single point, 0x02 = OFF/open, 0x03 = ON/closed

Input State	Online Bit (b1)	Point Value Bit (b0)	Binary Pattern	Returned Byte (Hex)
OFF / Open Contact	1	0	00000010	0x02
ON / Closed Contact	1	1	00000011	0x03

DNP3 Data Object Mapping (Binary Outputs)

Relay Outputs → Binary Outputs (BO)

The Smart 4 I/O's DNP3/TCP implementation maps its Relay Outputs as Binary Outputs (BO). These Binary Outputs are represented using DNP3 Object Groups that either return the current status of each Relay Output (Object Group 10/11), or instead accept Control Relay Output Block (CROB) commands (Object Group 12) from a DNP3 master to control the Relay Output.



Object Group 10 (Binary Output, Static Data)

Binary Outputs may be polled to acquire their current static state using DNP3 Object Group 10. When the Smart 4 I/O acts as a DNP3/TCP outstation and receives a poll request for Variation 0 (g10v0), it will respond using Variation 2 (g10v2). Object Group 10, Variation 1 (g10v1), is not supported. In this Variation 2 response, each Binary Output is represented by a one-byte flag field. Outputs that are active (energized) have their Point Value bit and Online flag set to (1), returning a value of 0x81.

Group 10, Variation 2 (g10v2): Binary Output Status

- Presents the current Binary Output states, with quality flags, in a series of eight bytes
- For a single point, 0x01 = OFF/de-energized, 0x81 = ON/energized

Object Group 11 (Binary Output, Event Data)

Binary Output Events are reported using DNP3 Object Group 11, which records Change-of-State (COS) transitions and stores them in the Smart 4 I/O's internal DNP3/TCP outstation event buffer. These event objects may be delivered automatically as unsolicited responses. Only Variation 2 (g11v2) is supported.

Group 11, Variation 2 (g11v2): Binary Output Status Event

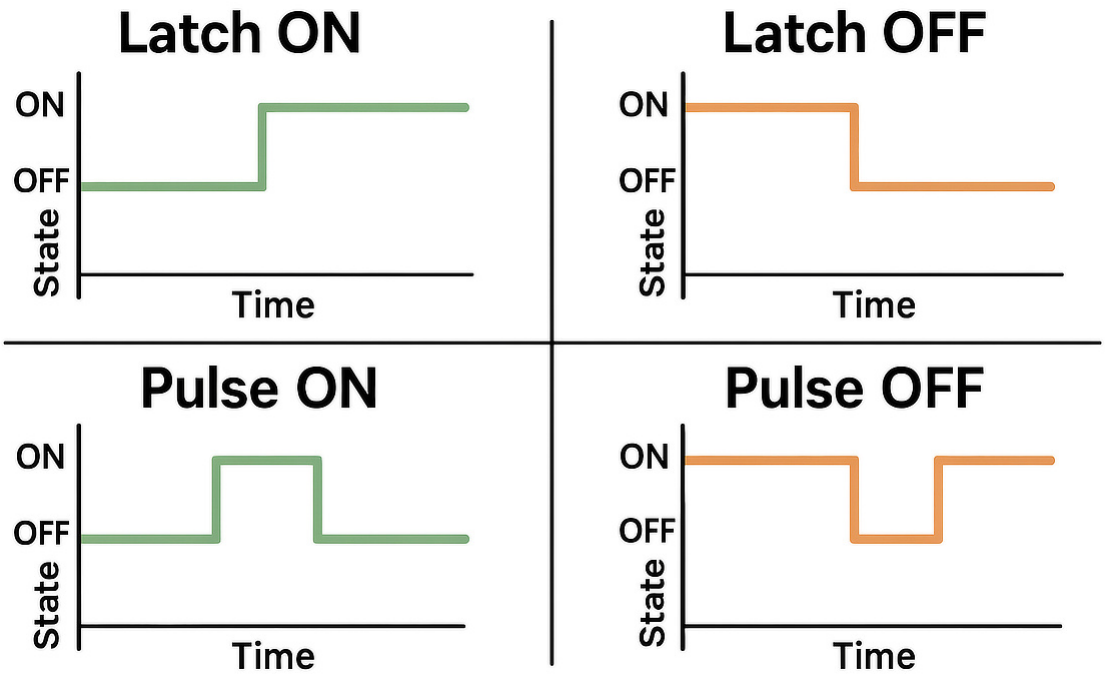
- Presents the current Binary Output states, with quality flags, in a series of eight bytesOnline Bit (b7)
- For a single point, 0x01 = OFF/de-energized, 0x81 = ON/energized

Input State	Point Value Bit (b7)	Online Bit (b0)	Binary Pattern	Returned Byte (Hex)
OFF / De-energized	0	1	00000001	0x01
ON / Energized	1	1	10000001	0x81

Object Group 12 (Control Relay Output Block / CROB)

Binary Output control operations are performed using DNP3 Object Group 12, which is dedicated to Control Relay Output Block (CROB) operations. This Object Group defines how a DNP3 master issues commands to a DNP3 outstation (i.e., the Smart 4 I/O) to operate or pulse a Relay Output. Each CROB request contains the control code, timing parameters, and execution method, for the command.

CROB operations are generally categorized as latching or pulsing actions. Latching commands change and hold the Binary Output in a new state until another command reverses it (e.g., Latch ON or Latch OFF), whereas pulsing commands momentarily energize or de-energize the Binary Output for a defined On-Time interval before automatically returning it to its previous state.



Both Variation 1 (g12v1) and Variation 2 (g12v2) of Object 12 implement Control Relay Output Block (CROB) functionality. Variation 1 provides the full CROB structure, allowing a DNP3 master to specify the control code, count, and precise On-/Off-Time durations for each operation. Variation 2 instead uses a compact format that omits timing (On-/Off-Time) and repetition (Count) fields.

Supported CROB control codes are as follows:

Code (Hex)	Action	Description
0x01	Latch ON (lon)	Energizes the Relay Output, and holds an ON state
0x02	Latch OFF (loff)	De-energizes the Relay Output, and holds an OFF state
0x03	Pulse ON (pon)	Energizes the Relay Output momentarily (On-Time defines duration)
0x04	Pulse OFF (poff)	Momentarily de-energizes the Relay Output

Each Control Relay Output Block (CROB) command can be executed in one of several modes, depending on how the DNP3 master issues it:

- Select-Before-Operate (SBO): Two-step sequence that validates commands before execution
- Direct Operate: Single-step command executed immediately
- Direct Operate No Ack: Same as Direct Operate, but omits confirmation

Group 12, Variation 1 (g12v1): Control Relay Output Block

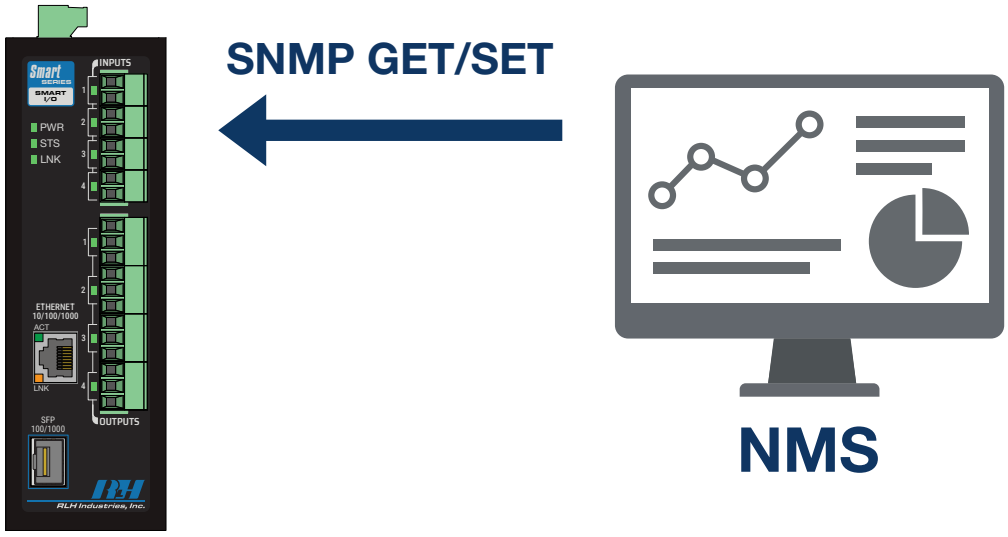
- Provides full CROB capability including control code, count, on-time, off-time, and command status

Field	Description
Control Code	Defines the Relay Output action (Latch ON, Latch OFF, Pulse ON, Pulse OFF)
Count	Number of operation repetitions
On-Time	Duration (ms) that the Relay Output remains energized
Off-Time	Delay (ms) between repeated operations

Network Management Systems (NMS)

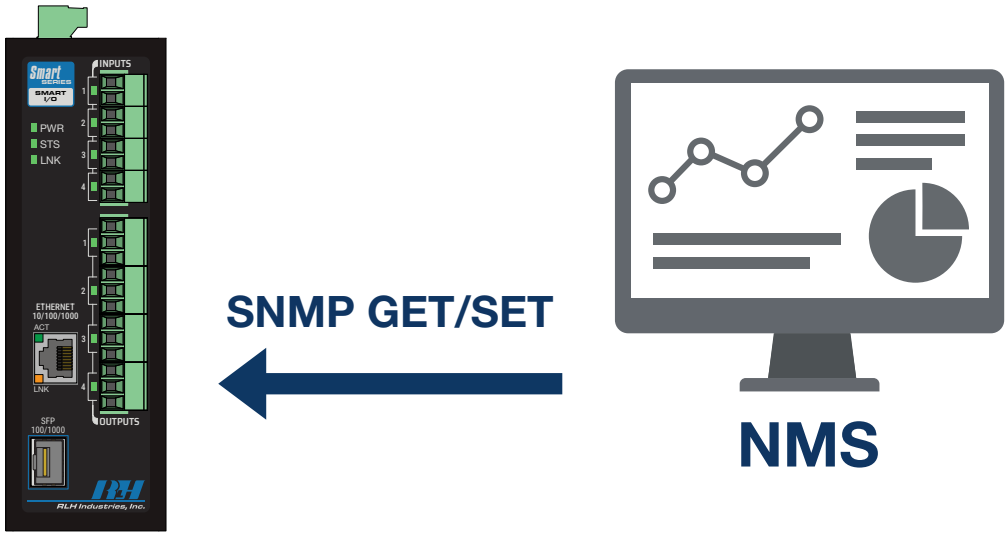
Network Management Systems (NMS) monitor and supervise network-connected infrastructure nodes such as Ethernet switches, routers, and power systems. When integrated into an NMS environment, the Smart 4 I/O functions as a managed SNMP-enabled node capable of providing real-time operational visibility, event-driven I/O state notifications, and configuration management.

An NMS may poll the Smart 4 I/O for information regarding its current system-configured parameters, and per-channel Digital Input statuses. It may also modify the system's configuration parameters, or invert the state of a Digital Input channel from OFF to ON, or ON to OFF.



SNMP Enabled Smart 4 I/O (Digital Inputs)

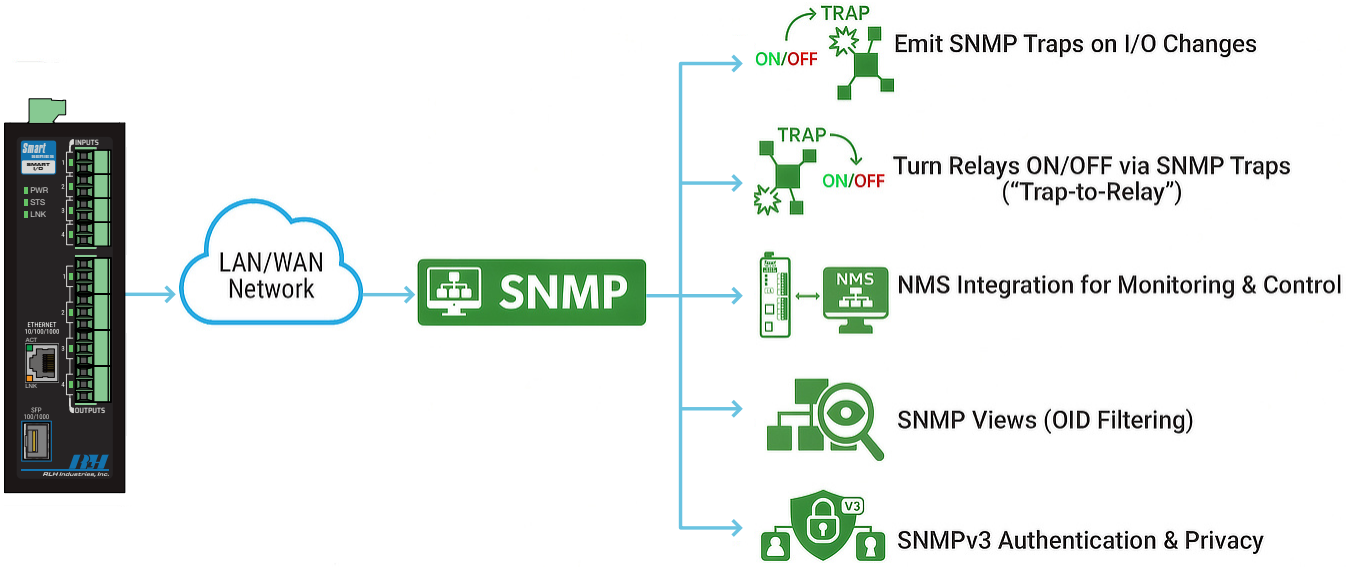
An NMS may also similarly interact with the Smart 4 I/O to poll or modify its device configuration setup, and per-channel Relay Output statuses.



SNMP Enabled Smart 4 I/O (Relay Outputs)

Simple Network Management Protocol (SNMP)

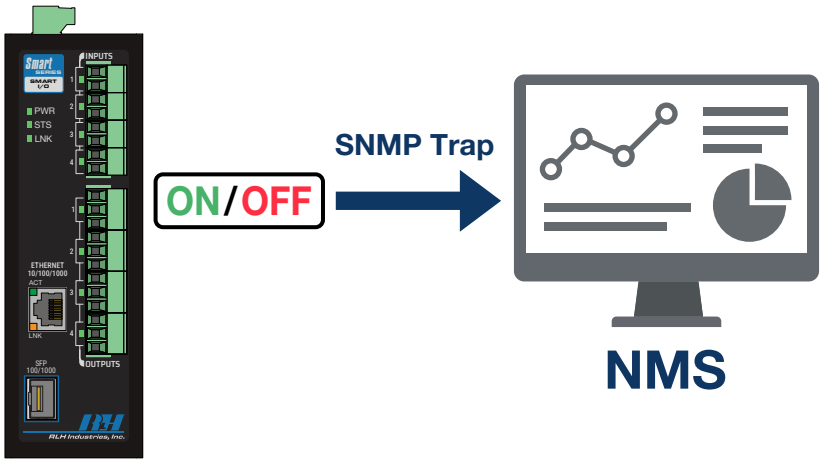
The Smart 4 I/O can operate as an SNMP agent on a network, exposing device configuration information and I/O data to an NMS platform. SNMP communication may use SNMPv1 or SNMPv2c for community-based access, or SNMPv3 to authenticate with user accounts that leverage USM (User-based Security Model) for enhancing security with encryption and authentication.



The Smart 4 I/O also hosts a downloadable model-specific SNMP MIB (Management Information Base) for interacting with all SNMP-accessible device parameters, accessible from within the web portal or on the products' webpage via fiberopticlink.com. Access to each OID sub-tree contained within the MIB may also be filtered via user-configurable SNMP Views.

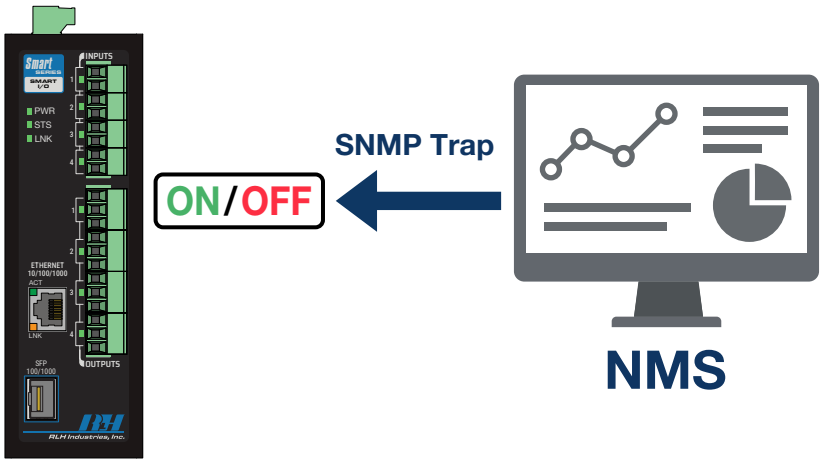
SNMP Trap Notifications

The Smart 4 I/O may transmit SNMPv2c or SNMPv3 traps to an NMS platform upon I/O state changes, when configured on an individual channel.

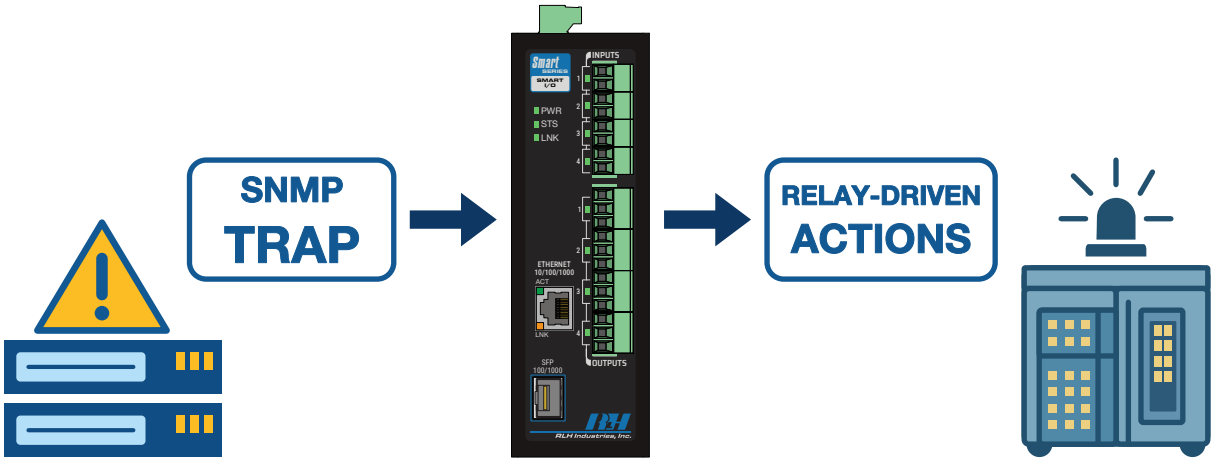


SNMP Trap Receiver

Additionally, the Smart 4 I/O may optionally act as an SNMP Trap Receiver, allowing it to change Relay Output statuses in response to the SNMP traps received from other networked equipment or NMS platforms. Each Relay Output channel can be configured to listen for up to two specific SNMP trap messages: one mapped to drive the relay ON (energize it), and one mapped to drive the relay OFF (de-energize it).

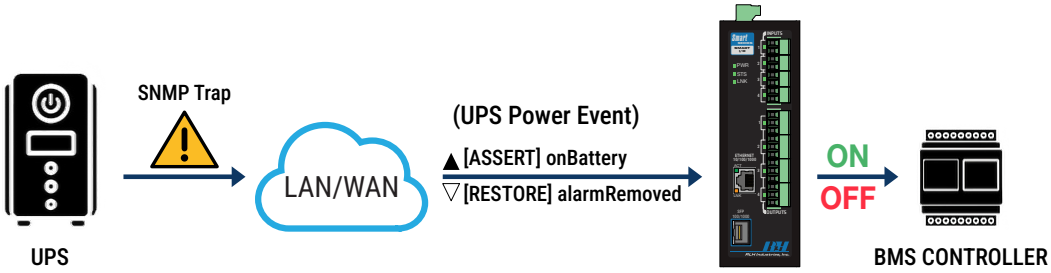


When the Smart 4 I/O receives one of these mapped SNMP traps, it immediately translates the event into a physical relay action. This "Trap-to-Relay" behavior allows network alarms or equipment fault conditions to drive real-world outputs for activating buzzers, lights, control panels, or other connected devices. In this way, SNMP-based events may trigger automated, deterministic responses at the physical layer.



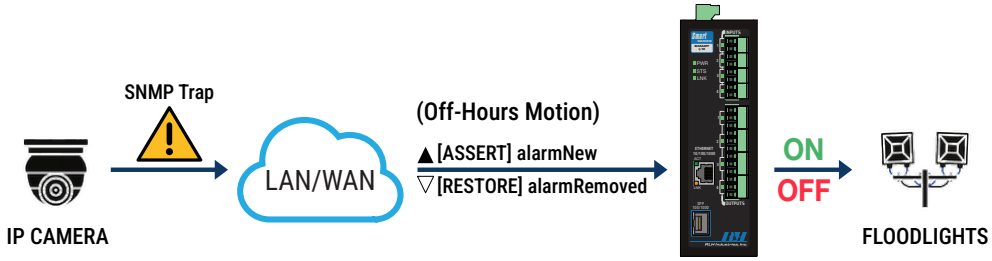
SNMP Trap Receiver

The below examples illustrate how SNMP traps from network devices can drive the system's relay outputs, converting network events into deterministic outputs throughout building management, security lighting, and SCADA system environments:



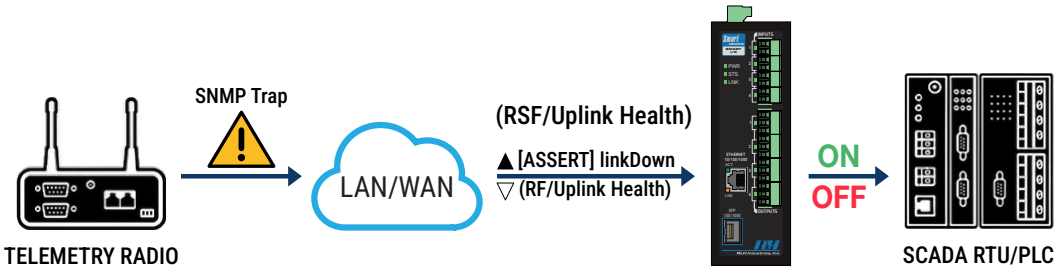
(UPS) - UPS Power Event → BMS Controller

A network-connected Uninterruptible Power Supply (UPS) experiences a loss of utility power, and is consequently running on battery. The UPS sends an SNMP trap to the Smart 4 I/O, energizing a mapped relay output wired to a Building Management System (BMS) controller's alarm input contact. When utility power is restored, the UPS sends another trap for the Smart 4 I/O to de-energize the relay.



(IP Camera) - Off-Hours Motion → Floodlights

An IP security camera monitors a perimeter using a built-in motion detection alarm rule for off-hours. The camera sends an SNMP trap whenever this alarm rule is triggered to the Smart 4 I/O, which energizes a mapped relay wired to a lighting control circuit for triggering floodlights to turn on. After motion stops in this area, another trap is sent by the camera for the Smart 4 I/O to de-energize the relay.



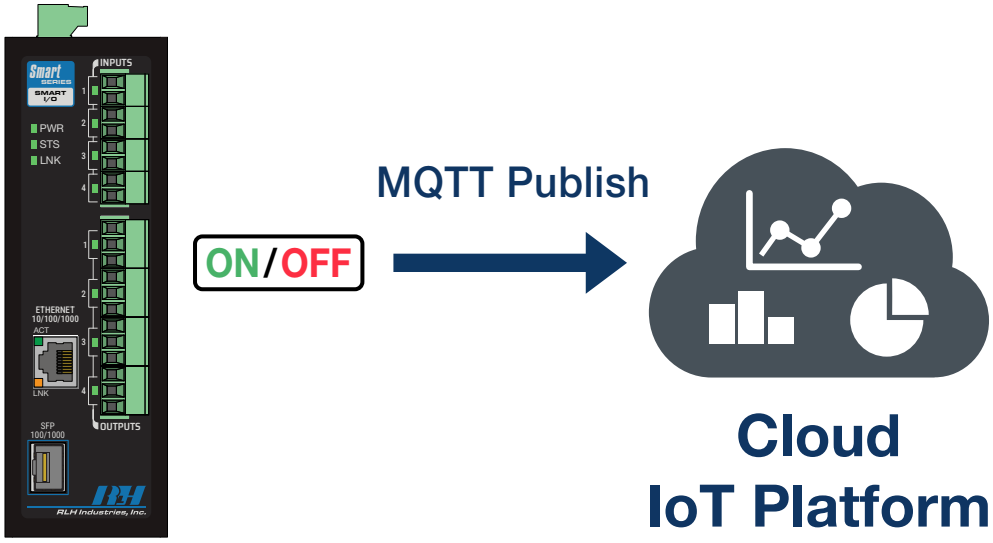
(Telemetry Radio) - RF/Uplink Health → SCADA RTU/PLC

A remote telemetry radio is used for backhaul communications in a SCADA system. The Smart 4 I/O keeps a relay normally energized and connected to a RTU/PLC for the SCADA system to actively monitor the radio link's health. When the wireless uplink fails, the radio sends a trap for the Smart 4 I/O to de-energize the mapped relay, alerting the underlying SCADA system that the link is down. Once the wireless uplink returns online, another trap is sent for the Smart 4 I/O to re-energize the relay.

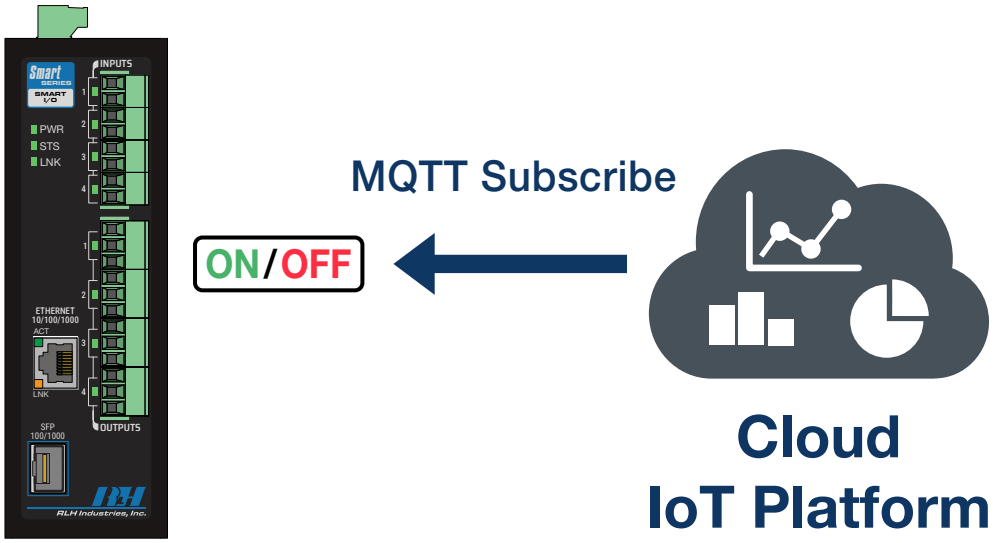
Industrial Internet of Things (IIoT)

The Smart 4 I/O supports full integration into Industrial Internet of Things (IIoT) ecosystems through its built-in MQTT broker and client capabilities. It may operate as an MQTT client, publishing and/or subscribing to user-defined topics, and host an MQTT broker in deployments where an external broker is not available.

When the Smart 4 I/O is configured as an MQTT publisher, it transmits its ON/OFF state changes for selected Digital Input channels to an MQTT broker for downstream MQTT subscribers, such as IoT platforms, SCADA middleware, or other Smart Series modules (e.g., Smart 4 I/O and Smart 8 Relay Output), to receive and act on this data.

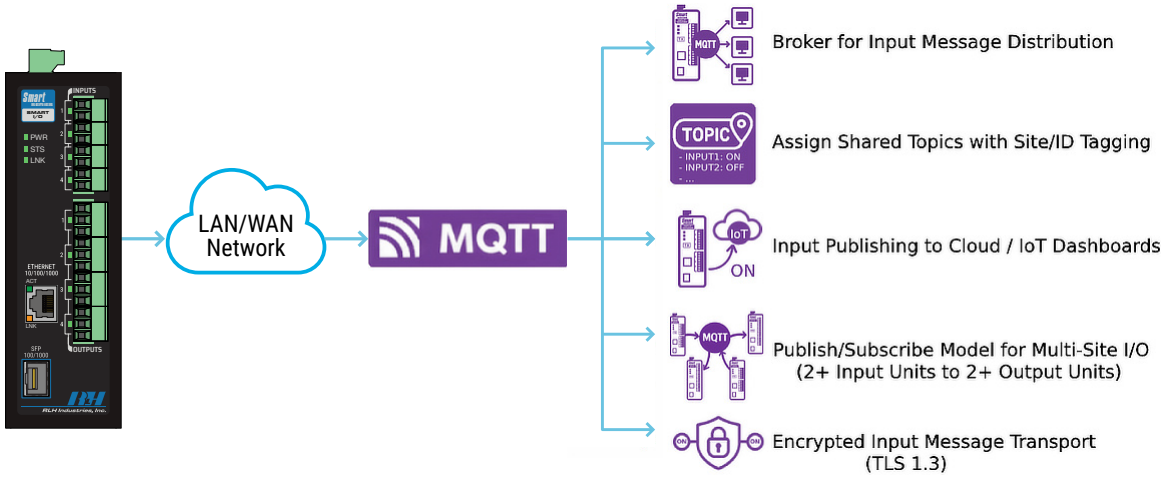


When the Smart 4 I/O is configured as an MQTT subscriber, it listens to defined MQTT topics and converts incoming MQTT payloads into deterministic relay actions. This MQTT subscriber service accepts JSON or plaintext payloads, which are filtered by the source IP address of the MQTT publisher.



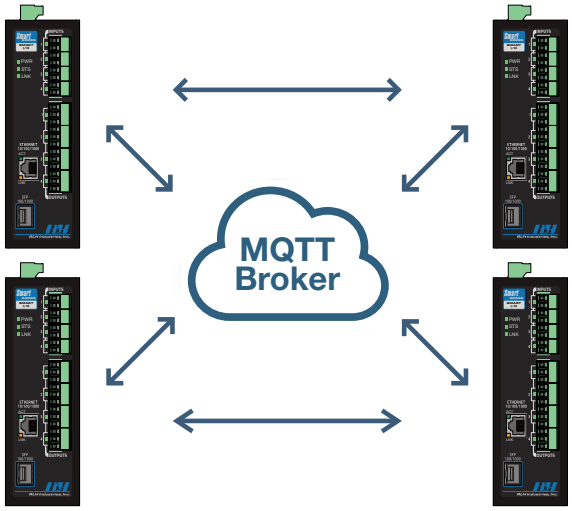
MQTT (Message Queuing Telemetry Transport)

The MQTT (Message Queuing Telemetry Transport) protocol enables lightweight, event-driven communication across distributed industrial systems, allowing field I/O changes to be captured, transported, and acted upon by enterprise IoT platforms or automation systems. The Smart 4 I/O may connect to an external MQTT broker, or operate with its own embedded broker to support local message distribution, multi-site I/O architectures, and secure TLS-encrypted MQTT sessions.



MQTT (Many-to-Many)

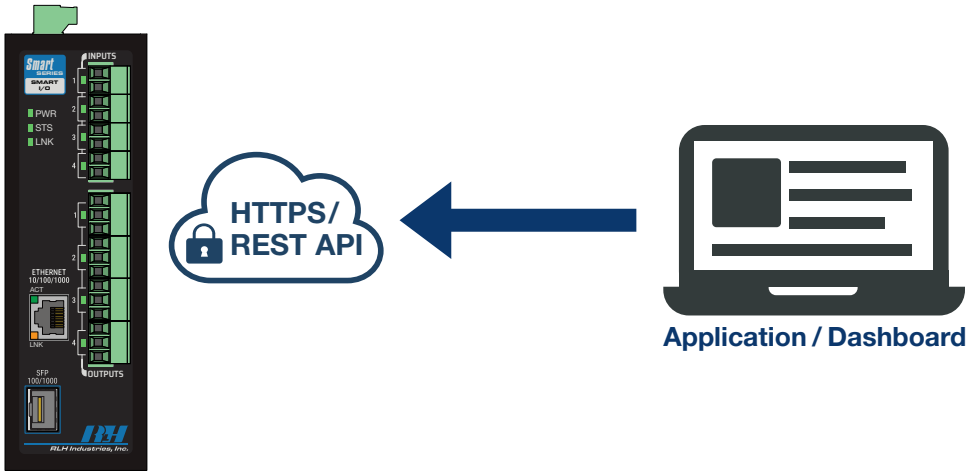
The system's MQTT implementation also uniquely supports a "Many-to-Many" architecture, in which multiple Smart 4 I/O units may publish input state changes to, or subscribe to input states from, other Smart 4 I/O modules.



- Enables multiple Digital Inputs to actuate the same mapped Relay Output channel
- Enables I/O distribution across geographically multiple dispersed input and output sites
- Enables interoperability with Smart 8 Input Sensor (**SM8-IN-XX-1**) and Smart 8 Relay Output (**SM8-OUT-1**) modules
- Updates Relay Outputs in response to the "last acquired state", as opposed to the synchronization facilitated by System Pairing

Application Programming Interface (API)

The Smart 4 I/O also includes a lightweight, REST-based HTTP/HTTPS API that allows external applications, automation software, and custom integration tools to query or configure the systems' I/O states. Authentication is facilitated via a bearer token, which is located in the device's web interface and may be regenerated.



By conforming to REST architectural principles, the system's REST API operates in a language-agnostic manner, allowing any HTTP-capable client environment to interface with the API. This includes, but is not limited to, applications written in JavaScript, Python, PHP, or other languages.

This REST API exposes the following endpoints:

Digital Inputs

- **GET /inputs** Returns the input channel and status (ON/OFF) for all digital inputs (Inputs 1-4)
- **GET /status** Returns the input channel and status (ON/OFF) for all digital inputs (Inputs 1-4), with a timestamp

Relay Outputs

- **GET /relays** Returns the relay channel and status (ON/OFF), for all relay outputs (Relays 1-4)
- **GET /relays/{id}** Returns the relay channel and status (ON/OFF) for a specific relay output (Relay [1-4])
- **PUT /relays/{id}** Updates the relay channel status (ON/OFF) for a specific relay output (Relay [1-4])
- **POST /relays** Updates the relay channel status (ON/OFF) for all relay outputs (Relays 1-4)
- **GET /status** Returns the relay channel and status (ON/OFF) for all relay outputs (Relays 1-4), with a timestamp

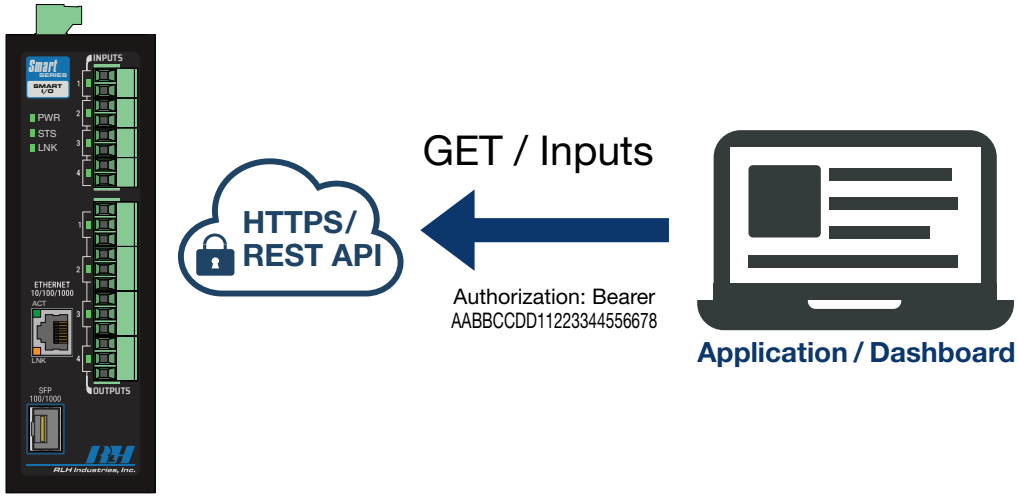
API Help Feature

Appending **?help** to a supported REST endpoint (e.g., /relays**?help**, /inputs**?help**, /status**?help**) returns API usage information that includes each available endpoint, HTTP request method examples, common control scenarios, and troubleshooting guidance.

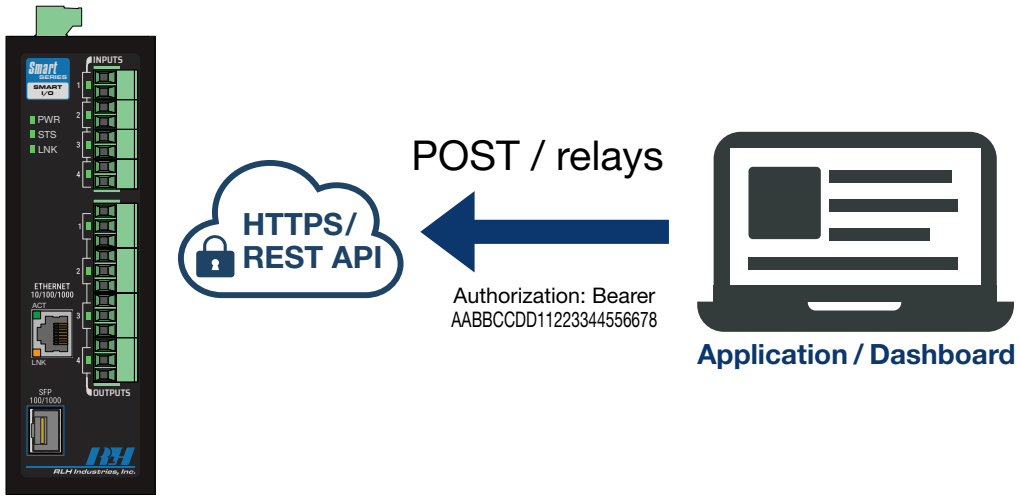
API Request Examples

The Smart 4 I/O's REST API implementation supports GET requests for retrieving channel-specific or aggregated I/O states. It may additionally update Relay Outputs states (ON/OFF) when receiving valid PUT or POST requests.

Example HTTP request methods that may be issued to the systems' REST APIs are presented below using the syntax of curl, a widely used command-line utility capable of issuing HTTP requests. The IP address used in these examples corresponds to the default IP address of the model's Copper (RJ45) port.



- (**Get Inputs 1-4**) curl -H "Authorization: Bearer AABBCCDD1122344556678" 'http://192.168.1.203/inputs'
- (**Get Inputs/Relays 1-4 + timestamp**) curl -H "Authorization: Bearer AABBCCDD1122344556678" 'http://192.168.1.203/status'



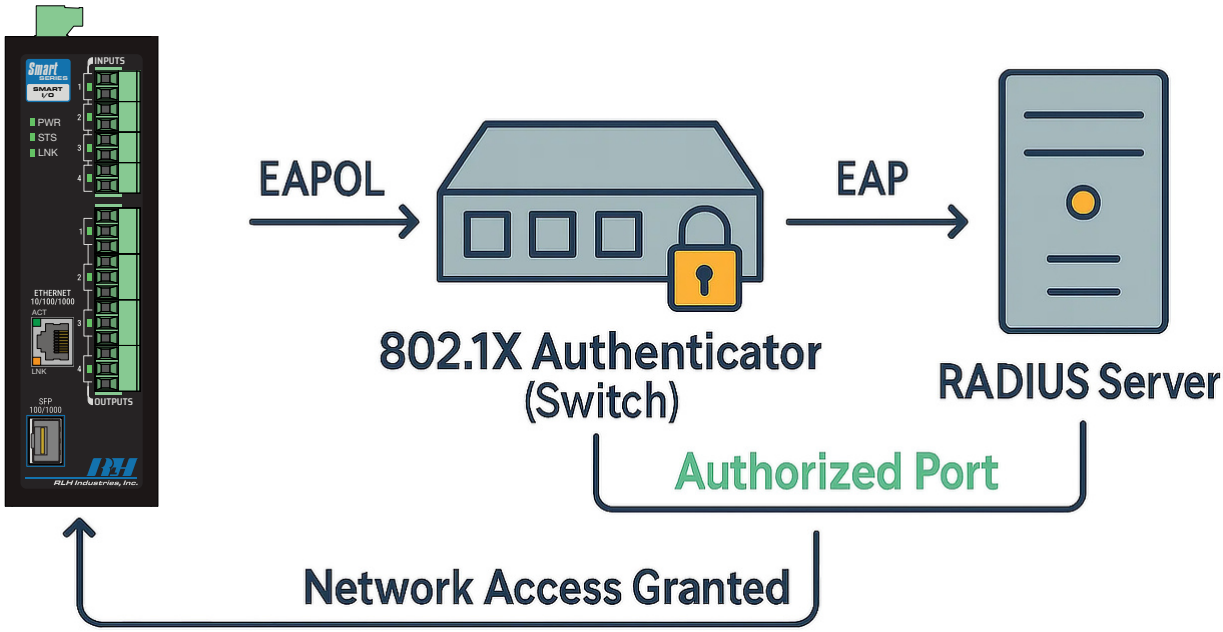
- (**Get Relays 1-4**) curl -H "Authorization: Bearer AABBCCDD1122344556678" 'http://192.168.1.203/relays'
- (**Set Relay 1 to ON**) curl -X PUT -H "Authorization: Bearer AABBCCDD1122344556678" -H 'Content-Type: application/json' -d '{\"status\":\"ON\"}' 'http://192.168.1.203/relays/1'
- (**Set Relay 1 ON, and Relay 2 OFF**) curl -X POST -H "Authorization: Bearer AABBCCDD1122344556678" -H 'Content-Type: application/json' -d '{\"Relay-1\": \"ON\", \"Relay-2\": \"OFF\"}' 'http://192.168.1.203/relays'

Port-based Network Access Control (PNAC)

Port-based Network Access Control (PNAC) enables the Smart 4 I/O to authenticate itself before gaining network access, over either or both of its available Ethernet ports (RJ45/SFP).

To facilitate PNAC, IEEE 802.1X is used as the enforcement mechanism, where the Smart 4 I/O operates as an IEEE802.1X supplicant, requiring successful credential validation through an organization's RADIUS server before permitting data exchange on the enabled Ethernet interface.

Once authenticated, the Ethernet interface transitions from a blocked state to an authorized state, allowing the system's network services (e.g., HTTP/HTTPS server) to operate normally. If authentication fails or the RADIUS session expires, the interface is restricted to prevent unauthorized access to the network.



IEEE 802.1X - EAP (Extensible Authentication Protocol)

To facilitate IEEE 802.1X-based authentication, the Smart 4 I/O supports multiple EAP (Extensible Authentication Protocol) methods for accommodating a wide range of RADIUS deployments.
The systems' supported EAP methods include:

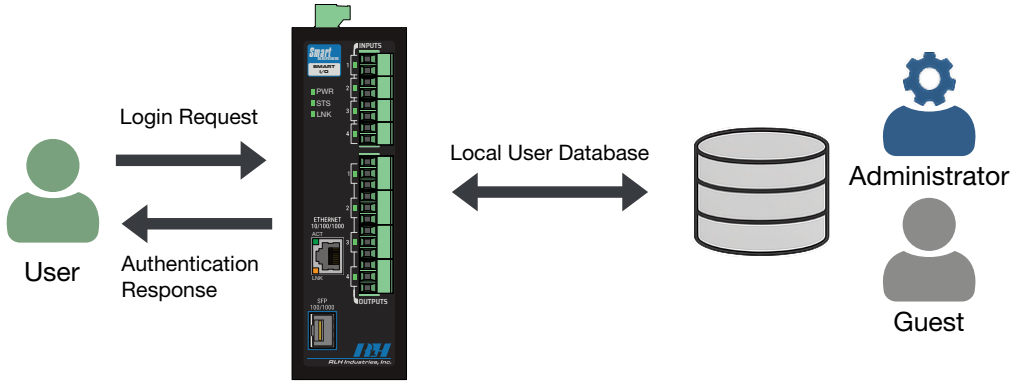
- **EAP-TLS:** Uses TLS/SSL certificates to authenticate with the RADIUS server
- **EAP-TTLS:** Uses an inner EAP authentication method (MSCHAPV2, PAP, CHAP, MD5) inside a TLS tunnel
- **EAP-PEAP:** Uses an inner EAP authentication method (MSCHAPV2, GTC) inside a TLS tunnel
- **EAP-MD5:** Uses an unencrypted pair of credentials for EAP authentication.
- **EAP-LEAP:** Uses an unencrypted pair of credentials for EAP authentication. Also known as EAP-Cisco.

Certificate-based authentication (EAP-TLS) provides the highest authentication level by relying on mutual authentication, whereas tunneled methods such as EAP-TTLS and EAP-PEAP allow encrypted credential exchange. Simpler password-based options such as EAP-MD5 and EAP-LEAP are available for supporting legacy infrastructures.

Web Access Method - Local Authentication

The Smart 4 I/O supports a flexible Web Access Method model that allows organizations to use the systems' local credentials (Admin, Guest), or an external RADIUS authentication server.

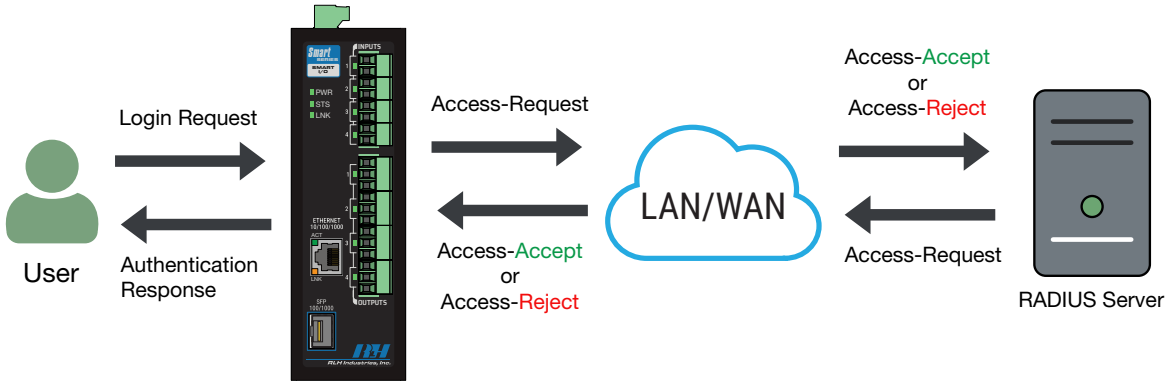
By default, web portal logins are authenticated against the systems' built-in Administrator account and Guest account (if enabled), which are stored inside an internal Local User Database. The Administrator and Guest accounts may be reconfigured to implement a user-defined, non-default password. Additional user accounts can't be provisioned onto the device's Local User Database; only Administrator and (optionally) Guest are supported.



Web Access Method - RADIUS Authentication

For larger-scale or security-sensitive environments, local accounts alone may not meet organizational requirements. To accommodate this, RADIUS Authentication is available as an alternative Web Access Method.

When RADIUS Authentication is enabled, the built-in Administrator and Guest accounts are disabled, deferring login access to the user-configured RADIUS server as the authoritative source for validating all web-portal login attempts. Organization-specific RADIUS client certificates may be uploaded to the Smart 4 I/O's TLS/SSL certificate management store.



User Authentication & Access Control

Role-based access control (RBAC) is a foundational security mechanism that restricts system functions based on user roles. In industrial control systems (ICS), RBAC ensures that only authorized personnel with appropriate permissions can interact with critical devices, minimizing the risk of unauthorized changes or sabotage. Aligned with this principle, the system implements a layered user authentication and access control to safeguard its configuration and operations.

The system provides two built-in local user accounts that enforce basic RBAC: an Administrator account with full read-write privileges, and a Guest (read-only) account. The Guest account is disabled by default.

The Administrator account maintains exclusive rights to modify and manage the system in its entirety, and should only be assigned to trusted personnel. In contrast, the Guest account is intended for operator or observer use, providing read-only access to a restricted view of the Overview dashboard, and the ability to update its credentials.

Administrator - Read-write role, unrestricted access to all system features

- The Administrator can update their account's credentials, configure all I/O channels, modify all system settings, fully access the Event Log, and perform all maintenance tasks.

Guest - Read-only role, access restricted to limited version of Overview Navigation Panel

- The Guest can update their account's credentials, and access a limited Overview dashboard to view the system's Firmware version and Part Number, and the User's IP address.

Feature	Administrator	Guest
User Profile	Full access (Credentials, Guest Enable)	Able to update credentials
Navigation Menu	Full access to all Navigation Panels	Only the Overview Navigation Panel
I/O Table	Full access (I/O Table is read-only)	Full access (I/O Table is read-only)
Event Logs	Full access to Snapshot, Full Log, Save Log	No access to Snapshot, Full Log, or Save Log
Version, P/N	Full access (information is read-only)	Full access (information is read-only)
User IP	Full access (information is read-only)	Full access (information is read-only)

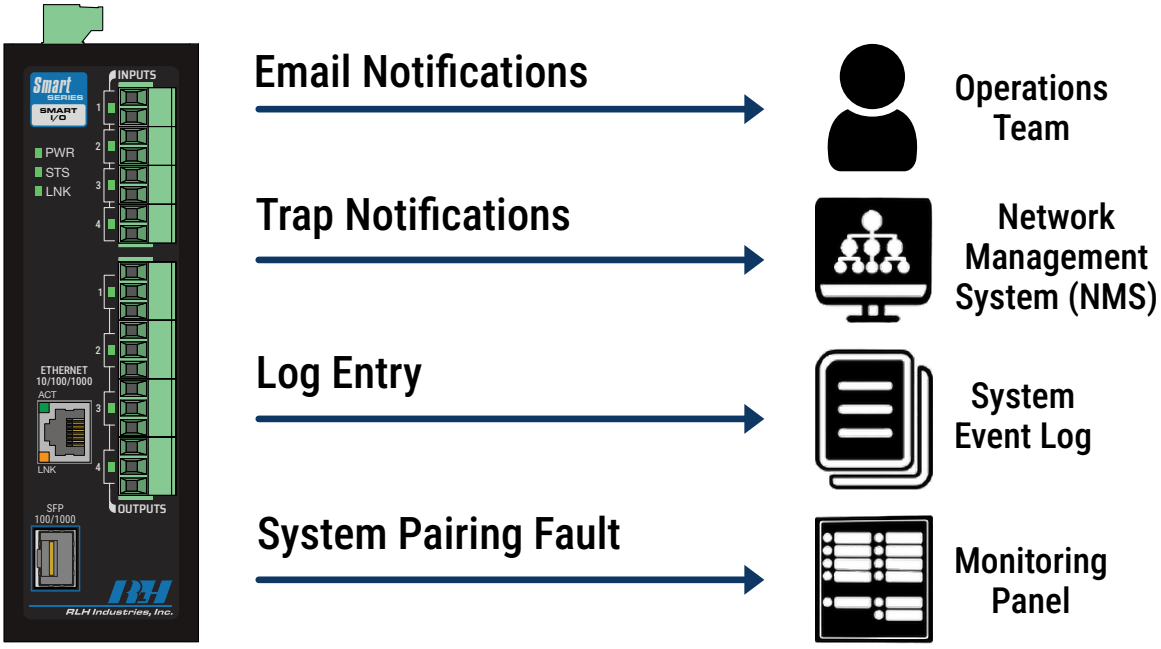
These roles guarantee the ability for administrators to retain sole control over system initialization, while non-admin users can safely observe field equipment operation. This separation of privileges upholds the principle of least privilege, preventing accidental or malicious misconfigurations by users in observer roles.

Alarming & Event Notifications

The Smart 4 I/O provides multiple alarm and event-driven notification mechanisms to communicate critical status changes and faults to on-site staff or remote operations teams. Together, these mechanisms create a layered model of visibility:

- Network protocols (SNMP and SMTP) for delivering alerts to centralized systems and remote operators
- An embedded Event Log that automatically records a time-stamped history of system events
- An SPDT alarm relay that supplies a hardwired signal interface to local alarms or monitoring systems

This combination ensures that notable events are seen in real time, stored for later review, and physically signaled directly in the field when network services may not be available.



Alarming & Event Notifications Architecture

When I/O channels change state, the system can generate Email Notifications (via SMTP) to alert on-call personnel or distribution lists. These emails are sent through a user-defined SMTP server, with support for TLS encryption. Email notifications can also be sent for System Pairing failures between two Smart 4 I/O modules.

Both systems may function as SNMP Trap Senders, transmitting traps to SNMP Managers during I/O state changes, when enabled on an I/O channel. This enables alarms to be captured and parsed by Network Management Systems (NMS) for providing network operators with a centralized view of I/O alerts.

Alarming & Event Notifications (Event Log)

All notable system events are recorded in the device's Event Log, which documents a persistent record of I/O state or system configuration changes. Each Event Log entry is timestamped in reference to the system clock, which may be modified on the 'Date & Time' webpage. The system clock should be configured first, to ensure accurate timestamps.

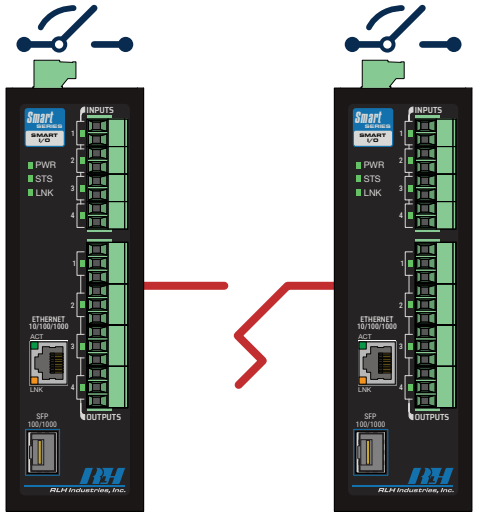
The full Event Log can store up to 150 entries at once, and may be exported as a CSV file for further analysis or archiving. In addition to I/O state or I/O channel configuration changes, Event Log entries will generate for System Pairing connection failures, network service configuration updates, and Event Log database resets.

Date/Time	Message
2025-01-15 11:12:45	System: Configuration change submitted from web interface Input 3 configuration page
2025-01-13 14:03:23	Input_2 status changed to Off
2025-01-13 14:03:21	System: Configuration change submitted from web interface Input 2 configuration page
2025-01-10 07:32:32	Input_1 status changed to Off
2025-01-10 07:32:30	System: Configuration change submitted from web interface Input 1 configuration page
2025-01-07 13:40:45	System: Configuration change submitted from web interface DNP page
2025-01-01 09:23:17	Input_3 status changed to On
2025-01-01 09:23:15	System: Configuration change submitted from web interface Input 3 configuration page
2025-01-01 09:10:58	Input_2 status changed to On
2025-01-01 09:10:56	System: Configuration change submitted from web interface Input 2 configuration page

Alarming & Event Notifications (System Alarm Relay)

For hardware-level alerting, both systems host a dedicated SPDT alarm relay that energizes when the unit detects a System Pairing connection failure between two corresponding Smart 4 I/O modules.

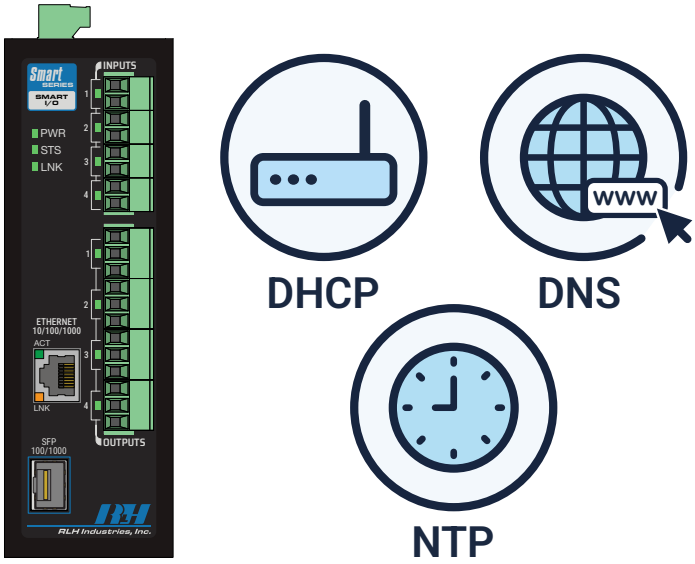
If a System Pairing connection is established ("Connected"), and later transitions into a failed ("Not connected") state,the System Alarm Relay will energize. This SPDT relay includes NO (Normally Open), NC (Normally Closed), and COM (Common) contacts for driving external signaling equipment, or interfacing with supervisory and fail-safe control circuits.



System Alarm Relay Diagram

Network Infrastructure Services

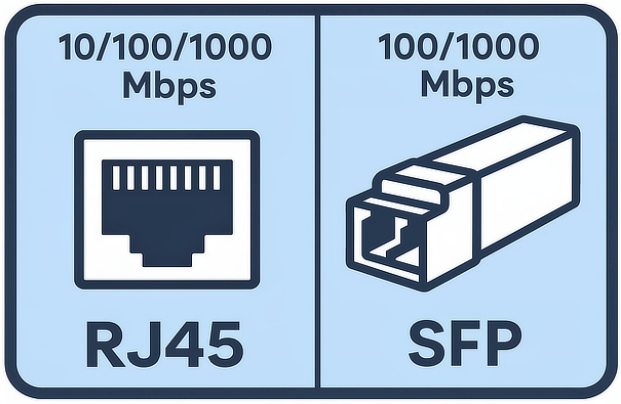
In addition to supporting industrial control system and network management protocols, both systems also host a set of essential network service clients commonly utilized in enterprise environments. These include DHCP for dynamic IP address assignment, DNS for domain-based name resolution, and NTP for time synchronization.



Ethernet Interfaces

The Smart 4 I/O incorporates a two-port Gigabit Ethernet interface, consisting of one RJ45 copper port and one SFP port. The RJ45 port supports 10/100/1000 Mbps Ethernet (10/100/1000BASE-T) over standard twisted-pair copper cabling, up to 100 meters (328 ft). The SFP port supports 100 Mbps (100BASE-X) and 1000 Mbps (1000BASE-X) Ethernet, with its maximum transmission distance limited by the installed SFP.

Both interfaces use auto-negotiation to establish their link speed and duplex mode with the connected network device. Negotiated link parameters are displayed in the web management interface, where each interface's IP settings may be configured. Link speed and duplex mode are determined exclusively by auto-negotiation, and cannot be set manually.



Ethernet Interfaces (Connectivity)

This 2-port Ethernet interface design provides physical-medium flexibility for deployments over copper, fiber-optics, or both, depending on site requirements.

For remote sites that depend on fiber-only connectivity, or require electrical isolation, the Smart 4 I/O's built-in SFP interface enables a seamless integration into an existing fiber-optic infrastructures. The inclusion of this SFP interface also removes the need for deploying external copper-to-fiber media converters.

The RJ45 and SFP interfaces may be used simultaneously, allowing short-range connections to nearby networking equipment over twisted-pair copper, while also utilizing a fiber-based backhaul for electrically isolated communication to a centralized network core. This is approach is common in industrial control panels or cabinets, where networked devices often coexist with Ethernet switches, protocols gateways, and RTUs.

For deployments that rely exclusively on fiber-optic connectivity, the RJ45 port's presence offers on-site technician with a convenient method of accessing the device locally through a service terminal or field laptop.

The SFP port is also engineered to accept copper-based SFP transceivers with an RJ45 connector, enabling the systems to functionally operate with two RJ45 interfaces, when required.

Ethernet Interfaces (Operation)

In addition to physical media flexibility, this 2-port interface offers network access segmentation and redundancy by allowing each port to maintain their own independent IP address configuration.

If both interfaces are used for accessing the device, but one Ethernet link becomes unavailable, the system will still remain accessible through the other active port's IP address. Redundant access is also possible when both ports share the same physical downstream path, and/or subnet assignment, depending on the network environment.

Each port's IP endpoint can also be assigned to separate, isolated networks. For example, one port may reside on a SCADA network for monitoring and collecting the system’s I/O telemetry, while the other connects to an IT/OT management network for system provisioning, configuration, and event log access.

This approach allows the system to participate in distinct network zones, without forcing both onto a shared subnet. It also supports concurrent access, enabling SCADA operators and IT/OT administrators to log in and interface with the system through their respective ports simultaneously.

Please note that this 2-port interface does not function as a 2-port Ethernet switch; network traffic is not forwarded or routed between the RJ45 and SFP ports. Inbound traffic can't be daisy-chained through the RJ45 port to the SFP port, or vice-versa.

Installation

Prior to Installation

- Check for shipping damage
- Check the contents to ensure correct model and fiber type
- Have a clean, dry, installation environment ready

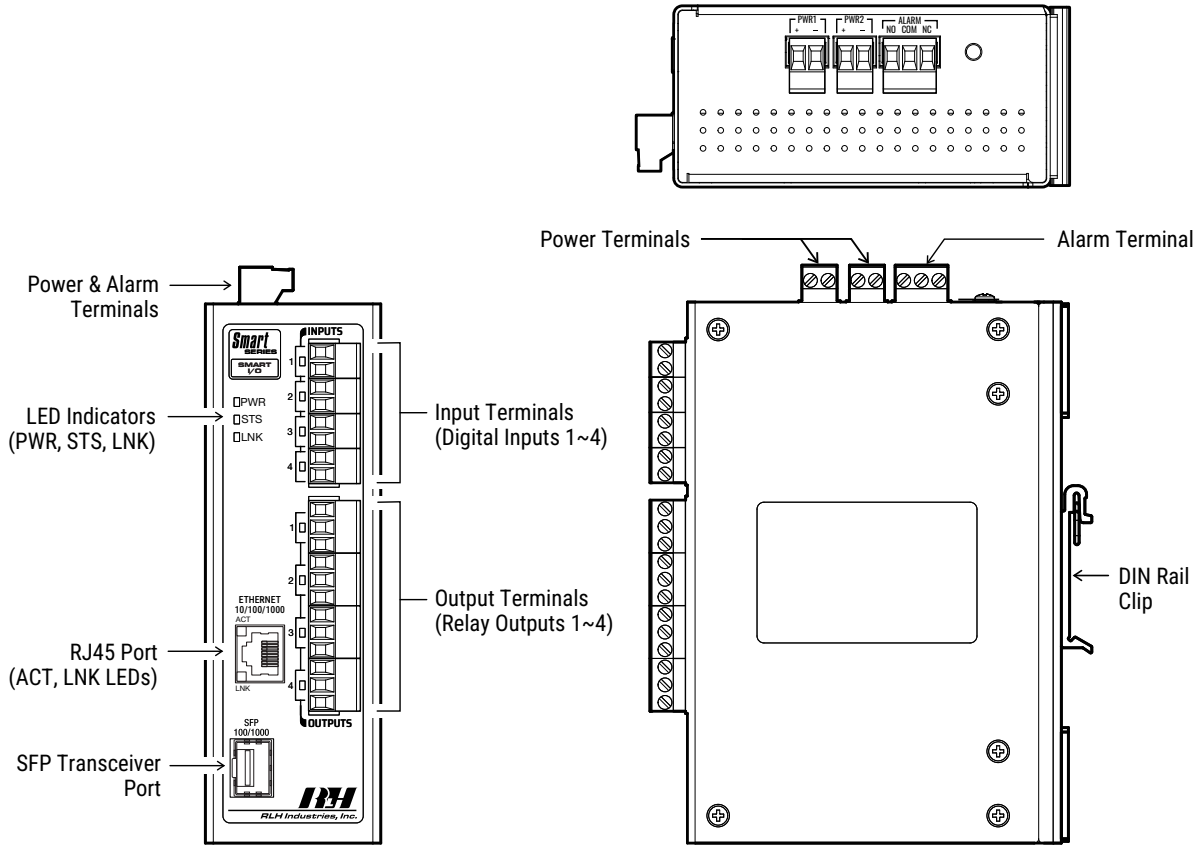
Required for installation

- 12-48 VDC Power Source, or 125VDC Power Source for -A models
- T35 DIN rail or suitable wall mount location
- A weatherproof enclosure is required for outdoor use

Measure the DC voltage of the source power to ensure that it is at least 12VDC. All electrical and fiber optic connections are made directly onto the unit.

Physical layout

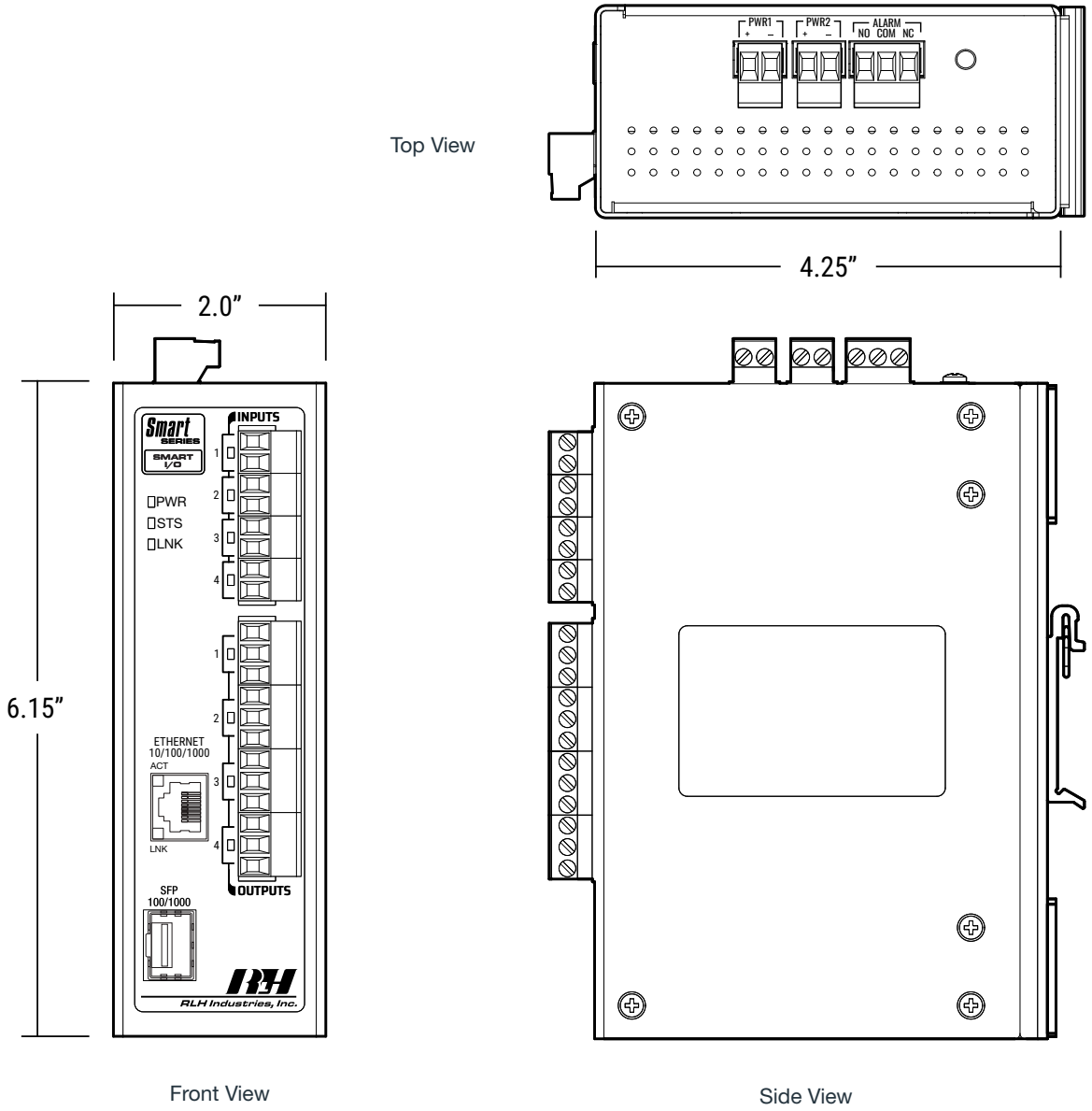
The front panel contains the contact terminals, LEDs, and Ethernet ports (1x RJ45, 1x SFP). The top panel contains the power and alarm terminals.



Smart 4 I/O

Physical layout

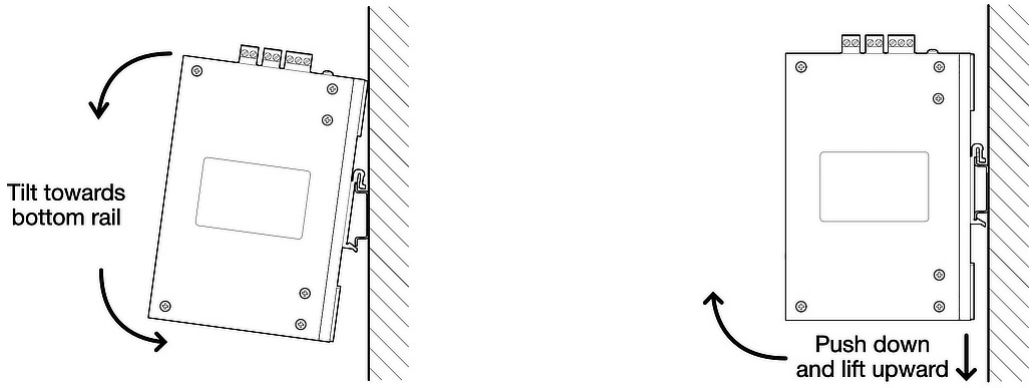
The front panel contains the contact terminals, LEDs, and Ethernet ports (1x RJ45, 1x SFP). The top panel contains the power and alarm terminals.



Physical Layout

DIN Rail Mounting

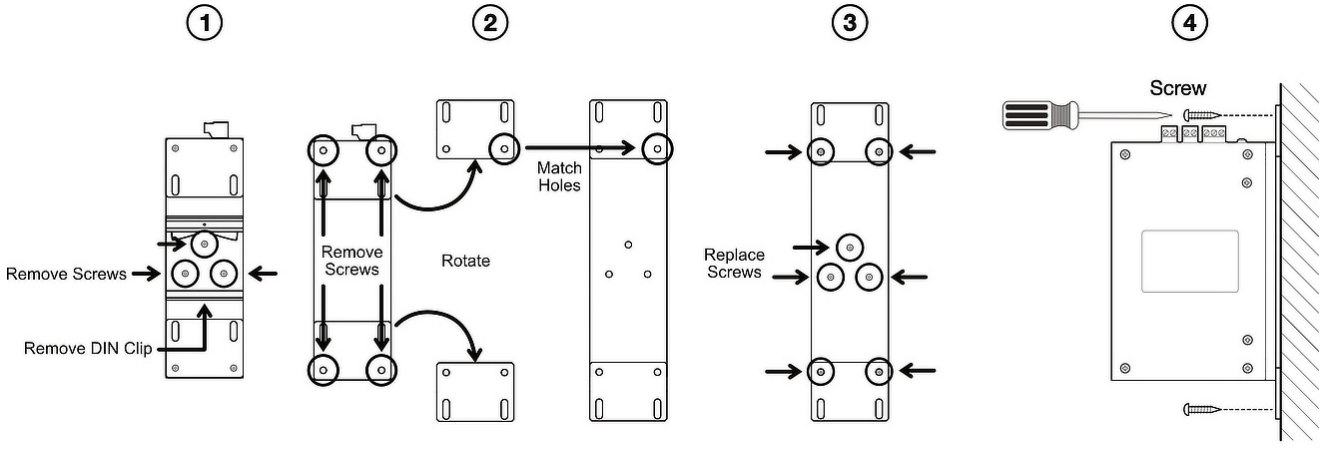
The DIN clip for mounting the system is mounted onto the rear panel. Hook the DIN clip on the top flange of the DIN rail, press down and rotate to the locked position to install. To remove, push down to depress the spring latch and rotate off of the DIN rail.



DIN Rail Mounting

Wall Mounting

The system can be easily wall mounted by attaching the provided wall mount ears and hardware. Attach the wall mount ears by following the instructions below.



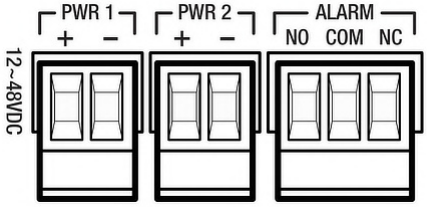
Wall Mounting

Power Input Wiring

Ensure the power supply is OFF prior to wiring the system. Connect a 12-48VDC power supply to the screw-down terminals located on the top of the unit, or a 125VDC power supply for -A models.

- Requires one (1) power supply; use a second power source for redundant power
- The PWR and ALARM terminal blocks are removable, and accept wire sizes 16~26 AWG
- Fully seat the terminal blocks back into the connector before operating the system

Note: The power inputs are polarity insensitive; connect the + and - conductors of the wire pair in either order. The + and - labels are included on the housing to simplify the installation process.



Power and Alarm Terminals

System Alarm Wiring

The System Alarm can be configured in the Web Portal to activate after losing a System Pairing connection. When the System Alarm activates, the ALARM terminal's relay will energize: COM-NO closes, and COM-NC opens. If a System Pairing connection is lost, the local unit is unable to form an Ethernet link with the remote/paired unit(s).

System Alarm Relay				
Alarm	**Condition**	**Relay Coil**	**Relay Contact States**	
OFF	Default (Idle, or Unpowered)	De-Energized	**NO-COM** = Open	**NO-COM** = Closed
OFF	System Pairing Active	De-Energized	**NO-COM** = Open	**NO-COM** = Closed
ON	System Pairing Inactive	Energized	**NO-COM** = Closed	**NO-COM** = Open

Note: The ON Alarm Status is only available after enabling the System Alarm feature in the Web Portal

A lost System Pairing connection can indicate any of the following on the local or remote/paired unit(s):

- Change in System Pairing settings (Endpoint Mode/Remote IP/Remote Port/TLS Encryption)
- Change in TLS/SSL certificates used for System Pairing (when TLS Encryption is enabled)
- Change in IP configuration of the network interface used in System Pairing
- Change in the underlying network's ability to route traffic between each unit in System Pairing
- Change in network interface(s)'s physical connectivity (e.g., removal or damage of copper/fiber cabling)

Terminate wiring at NO/COM/NC as required for when the System Alarm is ON:

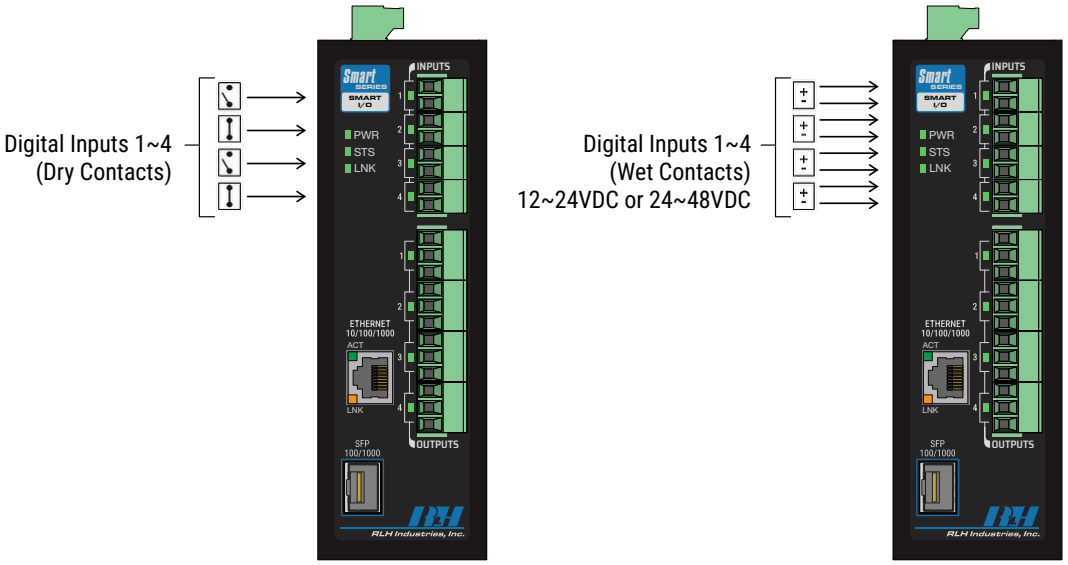
- Use NO and COM to activate an externally connected alarm when the System Alarm is ON
- Use NC and COM for monitoring systems that expect a normally-closed loop;
- the loop will open when the System Alarm is ON

Digital Input Terminal Wiring

Terminate the field device's input wires at the screw-down contact terminals of the desired Digital Input channel(s).

DO NOT APPLY VOLTAGE to the input terminals without verifying that the unit is a Wet Input model, or the system can become damaged.

- The 4 Channel input terminal block is removable, and accepts wire sizes 16~26 AWG
- Fully seat the terminal block back into the connector before operating the system



Digital Input Terminal Wiring

Dry Input Model (SM4-IO-DR-1)

- Each channel operates as a sourcing input, supplying a small sensing current onto the input terminals' contacts to detect the closure of a connected dry contact (open = OFF status, closed = ON status)
- Verify that the DC loop resistance of the connected pair does not exceed 100Ω for reliable input detection
- Do not apply voltage to the input terminals, or the system can become damaged

Wet Input Models (SM4-IO-24-1, SM4-IO-48-1)

- Each channel operates as a sinking input, receiving voltage within a specified range to signal an ON status:
  - Wet Input Model **SM4-IO-24-1**: 12-24VDC (8~27VDC / 5mA) = ON status
  - Wet Input Model **SM4-IO-48-1**: 24-48VDC (20~52VDC / 5mA) = ON status
- Verify that the DC input voltage is within the model's specified range
- Remove all DC voltage when initially connecting a wire pair to the input terminals
- The input terminals are polarity insensitive; connect the + and - conductors of the wire pair in either order

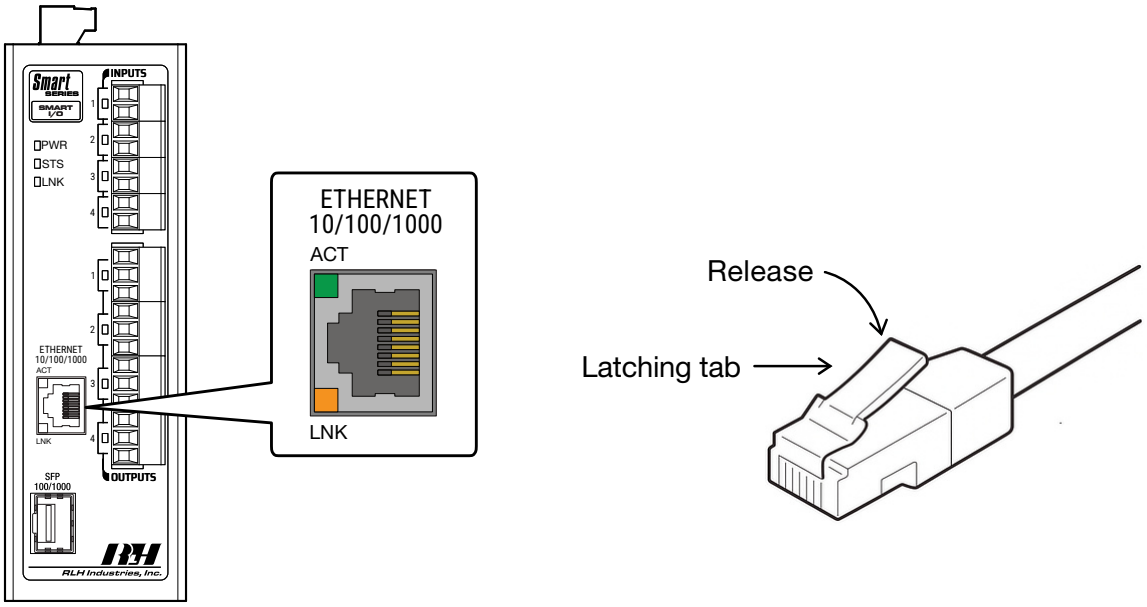
Ethernet Connections

The system's network interface features two Ethernet ports: one copper RJ45 port, and one fiber-optic SFP port. The RJ45 port supports 10/100/1000 Mbps Ethernet over twisted-pair cabling, while the SFP port is dual-rated to accept either 100 Mbps-rated or 1000 Mbps-rated SFP transceivers. Both ports use auto-negotiation to determine and establish the highest supported data transmission speed with their link partner (e.g., Ethernet switch).

RJ45 Ethernet Port (Copper)

This interface requires a standard Ethernet cable (twisted-pair, terminated per T568A or T568B). For reliable performance in environments with electrical noise or electromagnetic interference (EMI), shielded twisted-pair (STP) cables are recommended. Unshielded (UTP) Cat6 patch cables are sold separately.

- Ensure the cable length does not exceed 100 meters (328 feet)
- Use Ethernet cables rated for Cat5e and above for supporting Gigabit-rated bandwidth
- Straight-through or crossover cables can be used; the port automatically adjusts via Auto-MDIX
- Insert the RJ45 plug of the cable firmly into the Ethernet port until the retention tab audibly clicks
- To remove the cable, press down on the latching tab and gently release the connector out



RJ45 Ethernet Port

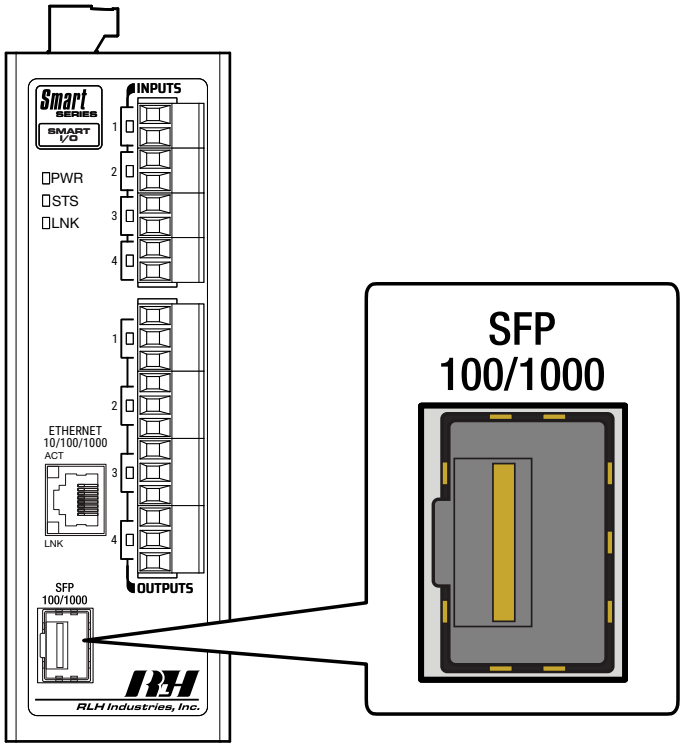
LED	Name	Status	Condition
ACT (Green)	Ethernet Activity	Flashing	Port is sending or receiving data
		OFF	Port is not sending or receiving data
LNK (Amber)	Ethernet Link	ON	Link established
		OFF	Link not established

RJ45 Ethernet Port LEDs

SFP Ethernet Port (Fiber)

This interface requires MSA-compliant fiber-optic SFP transceivers supporting 100 Mbps (Fast Ethernet) or 1000 Mbps (Gigabit Ethernet). For reliable performance across the system's full operating temperature range (-40℃ to +70℃), industrial-grade SFPs are recommended. SFP transceivers are sold separately.

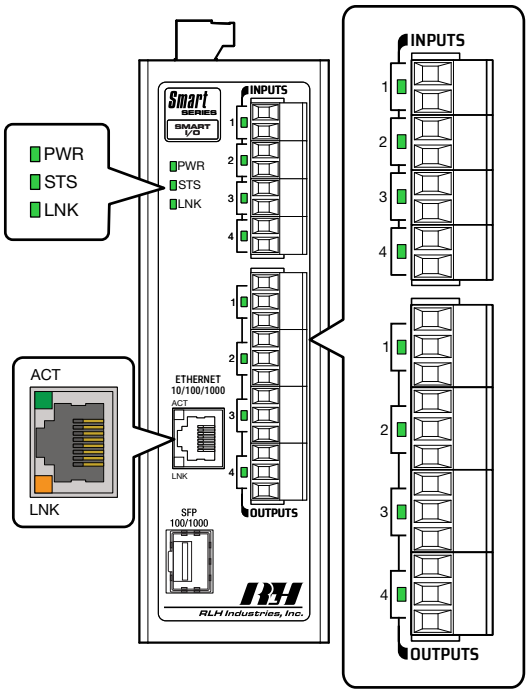
- This system requires MSA compliant, fiber optic SFP transceivers. An Industrial-grade SFP is recommended.
- Dual fiber systems require identical SFP transceivers
- Single fiber systems require a matching pair, side A and side B
- Close clasp and slide the SFP transceiver into the port
- To remove, pull the clasp back to release it, and then slide it out



SFP Ethernet Port

- Use a Cat5e twisted-pair cable or above for supporting Gigabit-rated bandwidth
- Shielded twisted-pair cables are recommended for environments with excessive noise or EMI
- Ensure the cable length does not exceed 100 meters (328 feet)
- Straight-through or crossover cables can be used; the port uses Auto-MDIX to detect both pinouts
- Insert the RJ45 plug of the cable firmly into the Ethernet port until the retention tab audibly clicks
- To remove the cable, press down on the latching tab and gently release the connector out

Front Panel LEDs



LED	Name	Status	Condition
PWR	Power Indicator	ON	DC input power is OK
		OFF	DC input power fault (insufficient or absent)
STS	CPU Status	Flashing	CPU operating normally
		Solid	CPU fault detected
LNK	System Pairing	ON	Paired (connected)
		OFF	Not Paired (disconnected)
INPUTS 1-4	Digital Inputs	ON	Input active / signal detected
		OFF	Input inactive / signal absent
OUTPUTS 1-4	Relay Outputs	ON	Relay is Energized
		OFF	Relay is De-energized
ACT (Green)	Ethernet Activity	Flashing	Port
		OFF	Port inactive
LNK (Amber)	Ethernet Link	ON	Link established
		OFF	Link not established

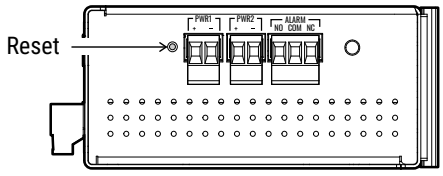
Smart 4 I/O Front Panel LEDs

System Reset

The System Reset feature allows the device to perform a controlled restart and re-initialization by using the Reset button present on the unit's housing, adjacent to the PWR1 terminal. This will reset all system configuration settings to factory-default.

To initiate the System Reset feature, perform the following steps:

1. Press and hold the Reset button for five (5) seconds
2. Release the Reset button.
3. Confirm that the STS LED turns OFF.
4. Wait approximately one minute for the system to re-initialize.



When the STS LED returns to a blinking state, the System Reset process is complete.

Ethernet I/O Specifications

Digital Inputs 1~4	Model: SM4-IO-DR-1	Dry Contacts (0-100 ohms) contact closure		
	Model: SM4-IO-24-1	Wet Contacts (8~27VDC / 5mA) contact closure		
	Model: SM4-IO-48-1	Wet Contacts (20~52VDC / 5mA) contact closure		
	Optical Isolation	3.5kV		
Digital Relay Outputs 1~4	Relay Type:	Mechanical, SPDT Relay, Form C, Normally Open/NO or Normally Closed/NC		
	Relay Ratings:	Max. Power	Max. Voltage	Max. Current
		60W / 125VA	220VDC / 250VAC	2A AC/DC
Ethernet Interface	1x RJ45 Port (10/100/1G), 1x SFP Port (100/1G) *Data Transmission is auto-negotiated			
Compliant IEEE Standards	IEEE 802.3 10Base-T (Ethernet)		IEEE 802.3u 100Base-TX/FX (Fast Ethernet)	
	IEEE 802.3ab/z 1000Base-T/X (Gigabit Ethernet)		IEEE 802.1X (Port-Based Network Access Control)	
Network Protocols	HTTP/HTTPS, SMTP, DHCP, DNS, NTP, IEEE 802.1X/RADIUS, TLS/SSL Encryption			
	SNMPv1/v2c/v3, Modbus TCP, DNP3, MQTT, RESTful API			
System Pairing Topologies	One-to-One: 1x Smart 4 I/O to 1x Smart 4 I/O			
System Pairing Latency	One-to-One: (TCP) Typical 8ms, Maximum 45ms			
	* Latency specification listed is based on direct connections between two Smart 4 I/Os			

General Specifications

LED Indicators	Power, CPU Status, System Pairing, Digital Inputs 1~4, Relay Outputs 1~4, Ethernet Link/Activity			
Power	Power Input	12-48VDC (11-53VDC)		
	Dual redundant power options - Polarity insensitive			
	Power Consumption	6 Watts Maximum		
DC Input Isolation (In/Out)	1.5kV	*For -A power option models only		
Overcurrent Protection	1.0A	Automatic Recovery		
System Status Alarm	Relay Type:	Mechanical, SPDT Relay, Form C, Normally Open or Normally Closed		
	Operational Limits:	Max. Power	Max. Voltage	Max. Current
		60W / 125VA	220VDC / 250VAC	2A AC/DC
Operating Temperature	-40˚C to +70˚C (-40˚F to +158˚F)			
Storage Temperature	-40˚C to +85˚C (-40˚F to +185˚F)			
Dimensions	H 4.93" x W 2.0" x D 3.93" (125mm x 51mm x 100mm) - not including DIN clip			
Weight	1.6 lbs. (0.73kg)			
Mounting	Standard T-35 DIN rail clip and wall mount ears (Included)			
Humidity	95% non-condensing			
Compliance	Reach, RoHS			
Warranty	Lifetime - Visit www.fiberopticlink.com for warranty information and coverage details			

Ordering Information

Description	Part Number
Smart 4 I/O, 4 Digital Inputs (Dry), 4 Digital Outputs, Powered by 12-48VDC	**SM4-IO-DR-1**
Smart 4 I/O, 4 Digital Inputs (Wet 12-24V), 4 Digital Outputs, Powered by 12-48VDC	**SM4-IO-24-1**
Smart 4 I/O, 4 Digital Inputs (Wet 24-48V), 4 Digital Outputs, Powered by 12-48VDC	**SM4-IO-48-1**

- Add -A to the end of the part number for 125 VDC input power option

Contact

Mail:	ATTN: Sales RLH Industries, Inc. 936 N. Main Street Orange, CA 92867	
Phone:	**Local**	714-532-1672
Sales/Service	**Toll Free**	800-877-1672
Email:	info@fiberopticlink.com	
Fax:	714-532-1885	

Support

Email:	support@fiberopticlink.com
Phone:	Toll Free 855-754-2497