

Trusted TMR 24 Vdc Digital Output Module – 40 Channel

PD-T8451 Issue 15

Rockwell Automation Publication ICSTT-RM280O-EN-P
Superseedes Publication ICSTT-RM280N-EN-P

Rockwell Automation

Reference Manual

Original Instructions

The Trusted® TMR 24 Vdc Digital Output Module interfaces to 40 field devices. Triplicated diagnostic tests are performed throughout the Module including measurements for current, and voltage on each portion of the voted output channel. Tests are also performed for stuck on and stuck off failures. Fault tolerance is achieved through a Triple Modular Redundant (TMR) architecture within the Module for each of the 40 output channels.

Automatic line monitoring of the field device is provided. This feature enables the Module to detect both open and short circuit failures in field wiring and load devices.

The Module provides onboard Sequence of Events (SOE) reporting with a resolution of 1 ms. An output change of state triggers an SOE entry. Output states are automatically determined by voltage and current measurements onboard the Module.

This Module is not approved for direct connection to hazardous areas and should be used in conjunction with Intrinsic Safety Barrier devices.

Features

- 40 Triple Modular Redundant (TMR) output points per Module.
- Comprehensive, automatic diagnostics and self-test.
- Automatic line monitoring per point to detect open circuit and short circuit field wiring and load faults.
- 2500V impulse withstand opto/galvanic isolation barrier.
- Automatic overcurrent protection (per channel), no external fuses required.
- Onboard Sequence of Events (SOE) reporting with 1 ms resolution.
- Module can be hot-replaced online using dedicated Companion (adjacent) Slot or SmartSlot (one spare slot for many Modules) configurations.
- Front Panel output status light-emitting diodes (LEDs) for each point indicate output status and field wiring faults.
- Front Panel Module status LEDs indicate Module health and operational mode (Active, Standby, Educated).
- TÜV Certified IEC 61508 SIL 3.
- Outputs are powered in isolated groups of eight. Each such group is a Power Group (PG).

Description

The TMR 24 Vdc Digital Output Module is a member of the Trusted range of input/output (I/O) Modules. All Trusted I/O Modules share common functionality and form. At the most general level, all I/O Modules interface to the Inter-Module Bus (IMB) which provides power and allows communication with the TMR Processor. In addition, all Modules have a field interface that is used to connect to Module-specific signals in the field. All Modules are Triple Modular Redundant (TMR).

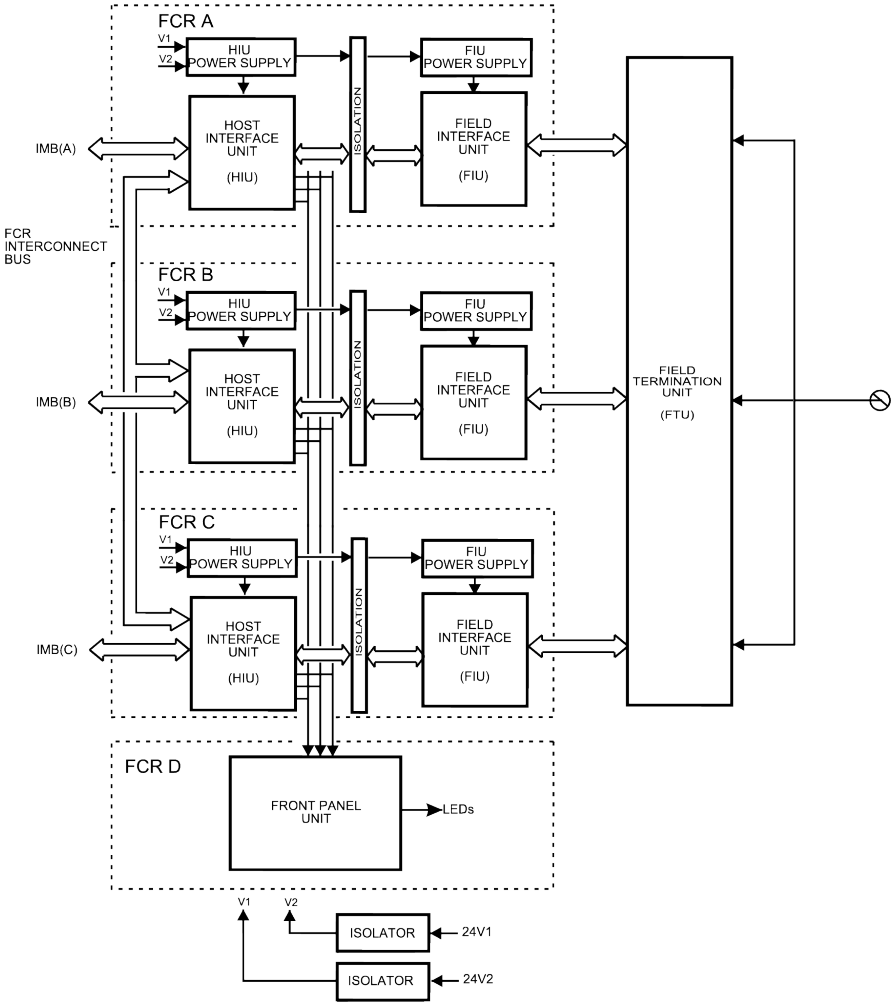


Figure 1: Module Architecture

All High Integrity I/O Modules are made up of four sections: Host Interface Unit (HIU), the Field Interface Unit (FIU), the Field Termination Unit (FTU), and the Front Panel Unit (or FPU).

Figure 2 shows a simplified block diagram of the Trusted 24 Vdc Digital Output Module.

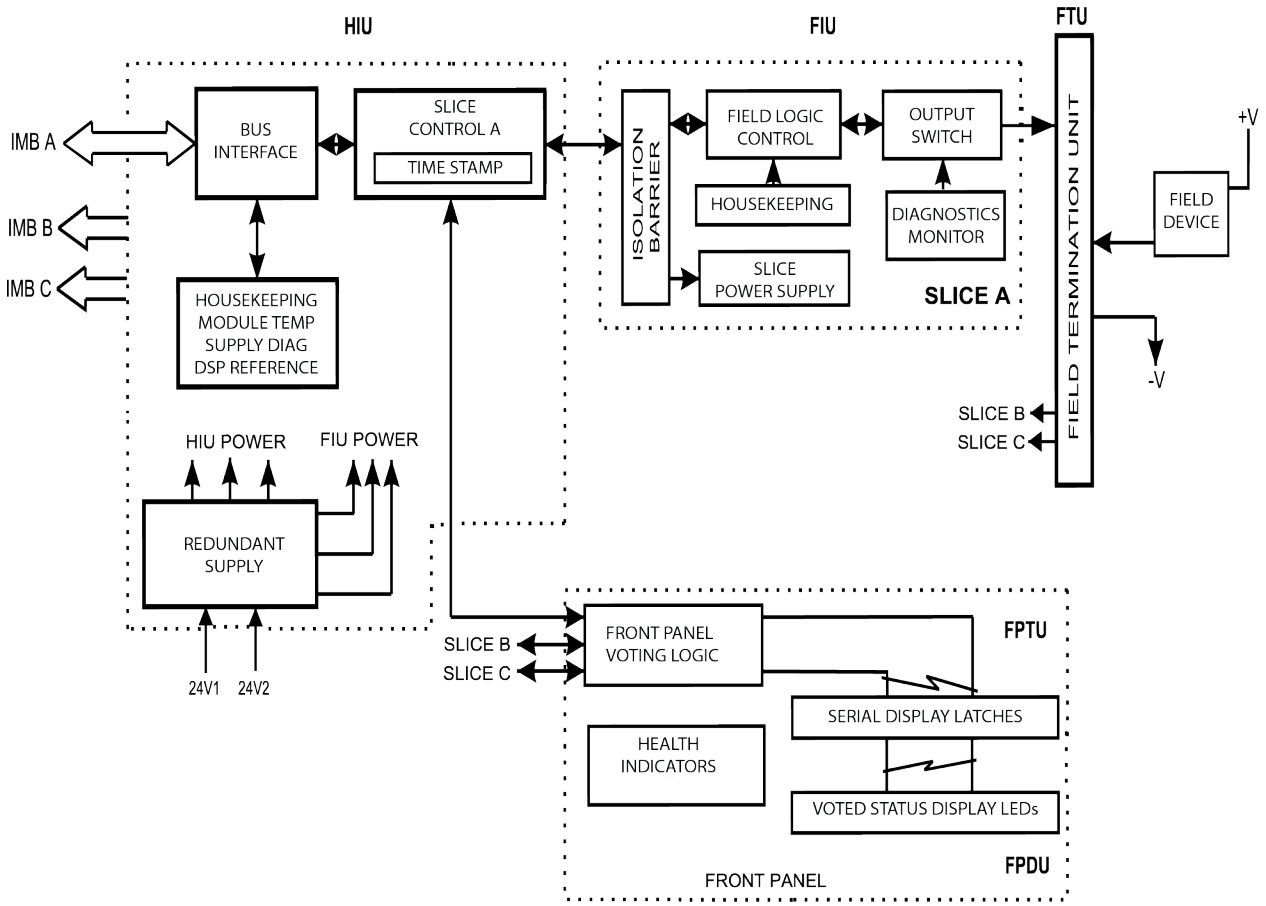


Figure 2: Functional Block Diagram

Field Termination Unit (FTU)

The Field Termination Unit (FTU) is the section of the I/O Module that connects all three FIUs to a single field interface. The FTU provides the Group Fail-Safe Switches and passive components necessary for signal conditioning, overvoltage protection, and EMI/RFI filtering. When installed in a Trusted Controller or Expander Chassis, the FTU field connector interconnects to the Field I/O Cable Assembly attached at the rear of the Chassis.

The SmartSlot link is passed from the HIU to the field connections via the FTU. These signals go directly to the field connector and maintain isolation from the I/O signals on the FTU. The SmartSlot link is the intelligent connection between Active and Standby Modules for coordination during Module replacement.

Field Interface Unit (FIU)

The Field Interface Unit (FIU) is the section of the Module that contains the specific circuits necessary to interface to the particular types of field I/O signals. Each Module has three FIUs, one per slice. For the TMR 24 Vdc Digital Output Module, the FIU contains one stage of the output switch structure,

and sigma-delta (ΣΔ) output circuit for each of the 40 field outputs. Two additional ΣΔ circuits provide optional monitoring of the external field I/O supply voltage.

The FIU receives isolated power from the HIU for logic. The FIU provides additional power conditioning for the operational voltages required by the FIU circuitry. An isolated 6.25 Mbit/sec serial link connects each FIU to one of the HIU slices.

The FIU also measures a range of onboard "housekeeping" signals that assist in monitoring the performance and operating conditions of the Module. These signals include power supply voltages, current consumption, onboard reference voltages and board temperature.

Host Interface Unit (HIU)

The HIU is the point of access to the Inter-Module Bus (IMB) for the Module. It also provides power distribution and local programmable processing power. The HIU is the only section of the I/O Module to directly connect to the IMB Backplane. The HIU is common to most high integrity I/O types and has type dependent and product range common functions. Each HIU contains three independent slices, commonly referred to as A, B, and C.

All interconnections between the three slices incorporate isolation to help prevent any fault interaction between the slices. Each slice is considered a Fault Containment Region (FCR), as a fault on one slice has no effect on the operation of the other slices.

The HIU provides the following services common to the Modules in the family:

- High-Speed Fault Tolerant Communications with the TMR Processor via the IMB interface.
- FCR Interconnect Bus between slices to vote incoming IMB data and distribute outgoing I/O Module data to the IMB.
- Galvanically isolated serial data interface to the FIU slices.
- Redundant power sharing of dual 24 Vdc chassis supply voltage and power regulation for logic power to HIU circuitry.
- Magnetically isolated power to the FIU slices.
- Serial data interface to the FPU for Module status LEDs.
- SmartSlot link between Active and Standby Modules for coordination during Module replacement.
- Digital Signal Processing to perform local data reduction and self-diagnostics.
- Local memory resources for storing Module operation, configuration, and field I/O data.
- Onboard housekeeping, which monitors reference voltages, current consumption and board temperature.

Front Panel Unit (FPU)

The Front Panel Unit (FPU) contains the necessary connectors, switches, logic, and LED indicators for the Front Panel. For every type of Trusted I/O Module, the FPU contains the Slice Healthy, Active/Standby, the Educated

LED indicators, and the Module removal switches. Additional bicolor LEDs provide status indication for the individual I/O signals. Serial data interfaces connect the FPU to each of the HIU slices to control the LED status indicators and monitor the Module removal switches.

Line Monitoring and Output States

The Module automatically monitors the output channel current and voltage to determine the state of the output channel. The numerical output state and line fault status are reported back to the application and are represented in this table:

Table 1 Line Monitoring Fault Status

Description	Numerical Output State	Line Fault Status
Field Short Circuit	5	1
Output Energized (On)	4	0
No Load, Field Open Circuit	3	1
Output De-energized (Off)	2	0
No Field Supply Voltage	1	1

It is recommended to fit a dummy load resistor to unused outputs so that a current is drawn that exceeds the NO-LOAD threshold. This will help prevent the Module from signaling a NO-LOAD fault

Housekeeping

The Output Module automatically performs local measurements of several onboard signals that can be used for detailed troubleshooting and verification of Module operating characteristics. Measurements are made within each slice's HIU and FIU.

Fault Detection/Testing

Extensive diagnostics provide the automatic detection of Module faults. The TMR architecture of the Output Module and the diagnostics performed verify the validity of all critical circuits. Using the TMR architecture provides a Fault Tolerant method to withstand the first fault occurrence on the Module and continue normal output controls without interruption in the system or process. Faults are reported to the user through the Healthy status indicators on the Front Panel of the Module and through the information reported to the TMR Processor. Under normal operations, all three Healthy indicators are green. When a fault occurs, one of the Healthy indicators will be flashing red. It is recommended that this condition is investigated and if the cause is within the Module, it should be replaced.

Module replacement activities depend on the type of spare Module configuration chosen when the system was configured and installed. The Module may be configured with a dedicated Companion Slot or with a SmartSlot for a spare replacement Module.

From the IMB to the field connector, the I/O Module contains extensive fault detection and integrity testing. As an output device, most testing is performed in a non-interfering mode. Data input from the IMB is stored in redundant error-correcting RAM on each slice portion of the HIU. Received data is voted on by each slice. All data transmissions include a confirmation response from the receiver.

Periodically, the TMR Processor commands the onboard Digital Signal Processors (DSPs) to perform a Safety Layer Test (SLT). The SLT results in the DSP verifying with the TMR Processor its ability to process data with integrity. In addition, the DSP uses Cyclical Redundancy Checks (CRC) to verify the variables and configuration stored in Flash memory.

Between the HIU and FIU are a series of galvanically isolated links for data and power. The datalink is synchronized and monitored for variance. Both FIU and HIU have onboard temperature sensors to characterize temperature-related problems.

The power supplies for both the HIU and FIU boards are redundant, fully instrumented and testable. Together these assemblies form a Power Integrity Subsystem.

Sequence of Events Characteristics

The Module automatically measures the field voltage and current to determine the state of each output channel. An event occurs when the output transitions from one state to another. When a channel changes state, the onboard timer value is recorded. When the TMR Processor next reads data from the Output Module, the channel state and real-time clock value are retrieved. The TMR Processor uses this data to log the state change into the system Sequence of Events (SOE) log. The user may configure each output to be included in the system SOE log. Full details of SOE are contained in Trusted Sequence of Events and Process Historian Package Product Description, publication ICSTT-RM243.

Output Switch Structure

The Digital Output Module provides a TMR switch topology where the load is driven by a total of three fully monitored, fail-safe (6 element) switch channels, one physically resident on each FIU in the Module. Any single switch or entire slice failure is designed to leave two of the three fail-safe switch channels operational to power the load.

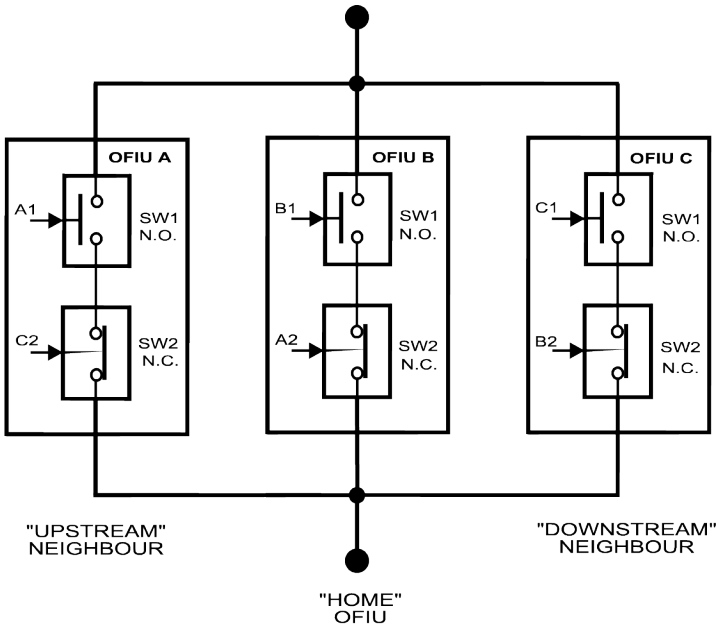


Figure 3: Output Switch Structure

The upper switches as shown in Figure 3 are denoted as N.O. (Normally Open), and are controlled by the FIU on which they are physically resident[1]. The lower switches are depicted as N.C. (Normally Closed), and are controlled by the "upstream" neighboring FIU[2].

Note: In this context, N.O. is defined as being in the off state in the absence of control signal power, and similarly, N.C. is the on state in the absence of control signal power. These switches are constructed from enhancement mode MOSFETs and are both guaranteed to be off in the absence of Module power to create gate voltage signals to bias them on[3] (unlike electromechanical relays for example).

The reason that the lower switches are specified to be on in the absence of control signal power is to allow two channels to power the load should an entire slice fail. Even if an entire slice fails, the surviving output circuits will carry the necessary control.

[1] Their “home” FIU.

[2] The home FIU, supplies an independent control signal for the “downstream” FIU FSS.

[3] For an unfaulted transistor.

This is the structure of each FIU output:

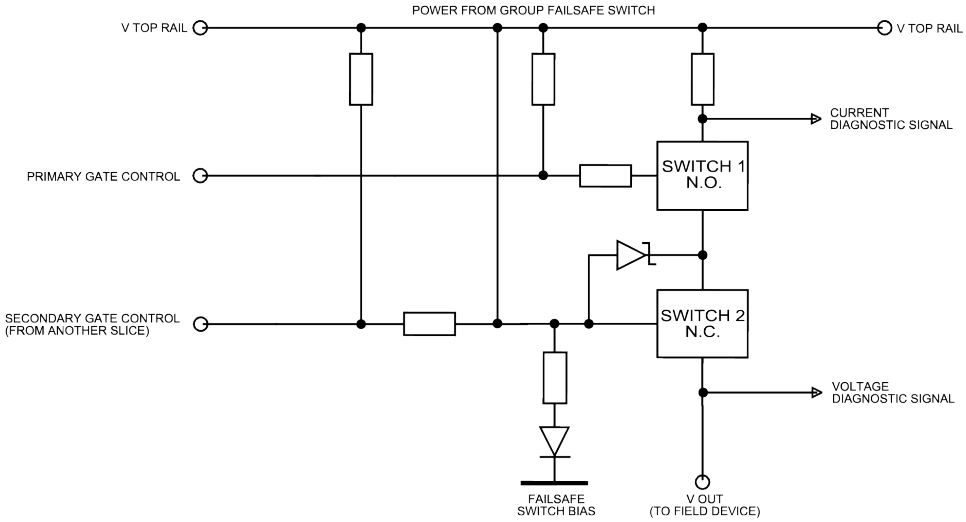


Figure 4: Simplified Switch Circuit Diagram

A resistor provides a means of continuously monitoring the switch current. A signal transistor is used to drive the gate of Switch 2. It provides Switch 2 with a negative gate voltage, to minimize its on resistance, and serves to hold Switch 2 on in the event that the secondary gate control loses power.

The Zener diode between the gate of Switch 2 and the source is only required to protect the gate from large voltage spikes on the drain that might capacitively couple through when Switch 1 and Switch 2 are in the off state.

The resistors in series with the gate of Switch 1 and the signal transistor serve to protect the drive logic in the event of a malicious switch failure. The pull-up resistors define the gate voltages in the absence of power.

Switch Diagnostics

During normal operation, Switch 1 and Switch 2 are maintained on. In this state, Switch 1 and Switch 2 exhibit a low resistance.

To determine the ability of the system to control the load via Switch 1 and Switch 2, their gate voltages are modulated, one at a time. As the gate voltages are modulated, the monitoring signals synchronously change in a predictable fashion. The local DSP analyses the relative amplitude and phase of these small AC signals, to determine the on resistance and threshold voltages of each switch.

The current to the load does not need to be completely interrupted in order to obtain a level of confidence in the ability of the transistors to turn off. For the TMR switch configuration in the on state, only one fail-safe switch at a time needs to be modulated, while the other two bear the load current.

Short Circuit Protection

Output channels are classified as protected under IEC 61131-2, specifically ‘Protected Outputs Requirements’.

While energized, the channel output current is monitored to protect the channel switches from damage by a sustained overcurrent condition. Having detected a sustained overcurrent condition, a short-circuit fault state is latched and the output is de-energized.

While de-energized, the output may optionally be configured to detect short-circuit field faults (resistance less than 24 Ω) through System.INI file configuration. The detection of short-circuits while de-energized relies upon a partial energizing of the field circuit to determine the channel load resistance. The partial energizing of a field circuit is designed to constrain any change in field voltage or current to less than 2V or 100 mA, respectively.

A latched short-circuit fault state can be cleared by operating the system Fault Reset button or by transitioning the commanded channel state.

The output also includes a non-replaceable fusible link for absolute protection.

Group Fail-Safe Switches

To support safe operation, the Output Module is equipped with a series of switches that provide source power to a group of eight output channels, a Power Group. The Output Module Group Fail-Safe Switch (GFSS) is intended as a final control switch, which can de-energize any outputs that cannot be de-energized in the normal way. For safety, the presence of two or more faults within the Output Module will cause the Group Fail-Safe Switches to de-energize, resulting in all of the outputs in its group to de-energize.

There are three switches in parallel, which comprise the GFSS, one associated with each 'slice' of the power group. The GFSS' are controlled via a signal from one of the other two neighboring slices. This means that if one slice determines from the output states that an output is not in a de-energized state when it should be, then it can command its own GFSS and those of the other slices GFSS to de-energize. This results in two of the three elements of the GFSS structure to de-energize, leaving only one GFSS element energized. If two slices do the same thing, then the last GFSS output will de-energize. For example, this would occur if two or more output switch elements fail in a 'stuck-on' state such that the output cannot de-energize.

The GFSS control signal is generated by a charge pump driven from the comms clock to the slice power group. If the clock fails, then the GFSS bias collapses. This means that even if the ability of the slice to communicate with a power group is lost, the GFSS can still be de-energized by stopping the comms clock. If a slice fails, the watchdog on the HIU will time out and reset the slice, this will shut down the FIU power supply and the associated GFSS control signal will also de-energize.

Specifications

Specifications

This table lists the module specifications:

Item	Description
Backplane (IMB) Supply	
Voltage	20V DC to 32V DC
Power	27 W
Field Supply	
Voltage	18V DC to 32 V DC
Maximum Current	40 A limited to 8 A per power group (T_A = 50 °C max) 30 A limited to 6 A per power group (T_A = 60 °C max)
Power Dissipation	
Field Supply at maximum power group current.	128 W (T_A = 50 °C max) 96 W (T_A = 60 °C max)
System Supply	27 W
Module Location	T8100, T8300 I/O Module Slot
Isolation	
Power Group to Power Group	50V Reinforced (continuous)[4] [Type tested at 1411V DC for 60 s].
Field Common	50V Reinforced (continuous)[5] 250V Basic (fault)[6] [Type tested at 2436V DC for 60 s].
Channel to Channel	None
Fusing	Not user serviceable
Number of Outputs	40
Number of Power Groups	5 Each Power Group comprises 8 channels
Output	
Output On State resistance	1.6 Ω
Maximum Current Rating (Continuous)	2 A per channel
Minimum On State Load Current	50 mA
Current Measurement Range	0 A to 2.7 A ±5% / ±5 mA[7]
Voltage Measurement Range	0V DC to +30V DC ±2V DC
Maximum Withstanding	-1V DC to +40V DC
Channel to Channel Crosstalk	< 1%
Maximum Load Capacitance	3000 µF
Output Short Circuit Protection	Electronic latching

[4] 50V rms Secondary circuit derived from Mains, OVC II up to 300V.

[5] 50V rms Secondary circuit derived from Mains, OVC II up to 300V.

[6] 250V rms Mains circuit, OVC II up to 300V. Exposure to voltages at these levels shall be temporally constrained consistent with the system MTTR.

[7] Tolerance is ±5 mA up to 1.8 A, thereafter is ±5%.

Item	Description
Sequence of Events	
Event Resolution (LSB)	1 ms
Time stamp Accuracy	±10 ms
Operating Temperature	0 °C to +60 °C (+32 °F to +140 °F)
Storage Temperature	-25 °C to +70 °C (-13 °F to +158 °F)
Relative Humidity – Operating and Storage	10% – 95%, noncondensing
Environmental Specifications	Refer to Document ICSTT-TD003
Dimensions	
Height	266 mm (10.5 in)
Width	31 mm (1.2 in)
Depth	303 mm (12.0 in)
Weight	1.3 kg (2.7 lb)