

MicroNet™ Safety Module

Fault-Tolerant Protection System

(Safety PLC with Integrated Overspeed Protection)

Description

The MicroNet™ Safety Module is a safety PLC (programmable logic controller) with integrated overspeed and over-acceleration protection designed to safely shut down any steam, gas, or hydro turbine upon sensing a safety event. The MicroNet Safety Module accepts 10 discrete or analog inputs per module (30 total) and one speed (MPU or PROX) input per module (3 total). It uses custom-programmed logic to determine when a true safety event has occurred, then issues a shutdown command to safely shut down the turbine system.

The MicroNet Safety Module utilizes a triple modular redundant architecture and 2-out-of-3 voting logic to accurately determine unsafe conditions and ensure that no single-point failure will affect system reliability or availability. With this design, system failures (switches, transducers, modules) are detected, annunciated, and allowed to be repaired or replaced while the monitored system continues to operate on-line.

Designed to safely protect high-speed rotating equipment in system-critical applications, this safety PLC's total response time is less than 12 milliseconds for its independent voted output models and 20 milliseconds for its 2-out-of-3 voted models.

Depending on the system design, the MicroNet Safety Module can be purchased with two dual-redundant trip relay outputs using a 2-out-of-3 voted architecture, or with three independent non-voted trip relay outputs (typically used to interface with a 2-out-of-3 based trip block assembly). Programmable inputs and outputs, 4–20 mA speed readouts, and Modbus® * communications make this safety PLC easy to integrate into any MicroNet system, or function as a stand-alone safety system.

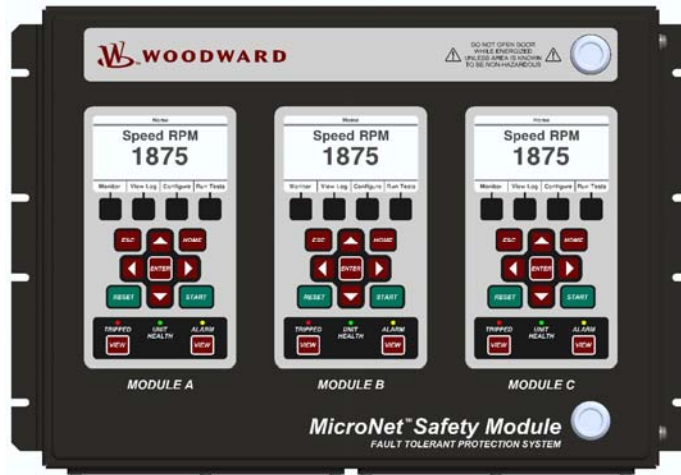
*—Modbus is a trademark of Schneider Automation Inc.

The MicroNet Safety Module is available in flush-mount models designed to be installed within a standard 24" (610 mm) cabinet front door, or models designed to be bulkhead-mounted on a wall or skid near the turbine set. Designed for harsh environments when installed within an enclosure, this device has an ingress protection rating of IP56 (protected against dust and completely protected against jets of water of similar force to heavy seas).

Designed for high reliability, each MicroNet Safety Module's kernel (A, B, C), depending on the purchased model, accepts two high-voltage power inputs (90–240 Vac / 100–150 Vdc) or one high-voltage power input (90–240 Vac / 100–150 Vdc) and one low-voltage power input (18–32 Vdc). This design works on a high-signal-select basis, allowing the unit to fully operate with either or both power sources available.

Applications

The MicroNet Safety Module is designed to be applied as part of a MicroNet control system and function as the safety system for any size steam, gas, or hydro turbine, or plant process equipment. This safety PLC's fast (12 millisecond) response time, 0.5 to 32 000 rpm speed range, and integrated overspeed and acceleration detection/protection functionality, make it ideal for application on critical high speed rotating motors, compressor, turbines or engines.



- IEC61508 SIL-3 Certified
- API670 & API612 Compliant
- Overspeed protection
- Acceleration & deceleration protection
- User-programmable logic
 - o 10 inputs
 - o Discrete or analog
 - o Trip/alarm logic
 - o Test logic
- 2-out-of-3 voting
- High availability (TMR)
- On-line testing
- On-line repair
- Auto test routines
- Trip valve health monitoring
- Trip, alarm & test logs
- Modbus communications
- Password security protection (NERC compliant)
- 12 millisecond response time (independent voted models)
- Internal frequency generator

The MicroNet Safety Module's versatile inputs, outputs, programming environment, and communications make it ideal as a safety protection device for use in applications that could possibly reach an unsafe state or condition and that must communicate directly to the plant DCS. Totally segmented from the main MicroNet control system, this safety module is not affected by controller-based faults or errors.

The MicroNet Safety Module is designed for critical applications where both personnel safety and unit availability (operation run time) is a concern or necessity. Certified as an IEC61508 SIL-3 (Safety Integrity Level 3) safety device, the MicroNet Safety Module can easily be applied as a stand-alone IEC61508-based device or within an IEC61511-based plant safety system. A thorough product manual is provided to instruct users on how to apply the MicroNet Safety Module to meet IEC based requirements.

The MicroNet Safety Module's triple modular voting architecture, first-out trip indication, alarm, trip & overspeed logs, valve response monitoring, programmable auto-test routines, coupled with API670 (American Petroleum Institute) and API612 compliance make it ideal for use in petrochemical or power generation applications. The MicroNet Safety Module models with two dual-redundant relay outputs are designed to be applied with simplex or dual-redundant trip block assemblies or trip systems.

The MicroNet Safety Module models with three independent non-voted output models are designed to be applied with special turbine trip block assemblies that perform the 2-out-of-3 voting within their design. Designed for system-critical applications, the MicroNet Safety Module's triple-modular architecture coupled with its on-line testing and on-line repair capabilities give it one of the highest availability and reliability ratings in the industry.

Functionality

Programming—The MicroNet Safety Module functions as a safety PLC, as it accepts 10 discrete or analog inputs per module (30 total), and allows users to create custom safety/protection programs to safely protect site personnel and equipment. Programmers are able to utilize typical logic and testing sequence routines to create their application-specific safety logic and tests.

On-Line Testing—Each MicroNet Safety Module kernel can be tested manually from the module's front panel, Modbus communications port, or automatically via its auto-test routine function. The MicroNet Safety Module allows users to configure overspeed or custom-programmed tests to be performed manually or automatically on a periodic basis. With these test routines, each module (A, B, C) is tested one at a time, and either a successful test result is logged or, upon sensing a fault, the routine is halted and the sensed fault indicated/alarmed.

On-Line Repair—The MicroNet Safety Module's triple modular design allows users to easily replace one of its modules (A, B, C) while the monitored equipment/turbine is on-line and operating normally. Ease of replacement is enhanced by the unit's backplane plug-and-operate structure, and its module-to-module learning function.

Trip, Alarm, & Overspeed Logs—The MicroNet Safety Module log function logs (saves to memory) all trips, alarms, trip valve response times, and overspeed events. The trip log function uses a scrolling buffer and records the last 50 sensed trip or alarm events and the last 20 overspeed events to memory, with associated times. Each log file can be viewed from the unit's front panel, or downloaded to a computer via

the MicroNet Safety Module service tool program. Each module utilizes non-volatile memory to ensure that all logged events are saved, even on loss of power.

Real Time Clock—Each MicroNet Safety Module kernel utilizes a real-time clock to ensure accurate time logging. A special time-averaging function is utilized between modules to ensure module-to-module clock synchronization. Alternatively, the MicroNet Safety Module can be configured to accept a standard IRIG-B time synchronization input signal from a time synch device.

Features

High Resolution Displays—Each module includes a high resolution 4.2" (107 mm) color display and keypad to allow users to locally monitor configuration settings, statuses, system inputs and outputs, and alarm, trip, and overspeed logs.

Automatic Overspeed Test Routine—Optionally, the MicroNet Safety Module can be configured to routinely perform and overspeed test each module/trip solenoid, then log and report the test results. With this test routine, each module is sequenced through its test sequence using an internal frequency generator to simulate an overspeed condition.

Automatic Test Routines—Optionally, the MicroNet Safety Module can be configured to routinely perform custom tests of each module/trip solenoid, then log and report the test results. With this test routine, each module is sequenced through a programmed test sequence to simulate, test, and log the results of each safety even condition.

Acceleration/Deceleration Detection—Optionally, the MicroNet Safety Module can be configured to protect a turbine from high acceleration/deceleration events. The derivative of the speed signal is used to detect turbine acceleration/deceleration and issue an associated trip command.

MPU Detection—Each module's speed sensor input uses special MPU open-wire detection circuitry to validate that the MPU is properly connected before turbine operation, and special loss-of-speed detection logic to validate MPU functionality during turbine operation.

Sulfur Contamination Resistant—Utilizes special conformal coating material that has demonstrated excellent long-term protection against H₂S and SO₂ gases at levels classified in international standard IEC 721-3-3 1994 - environment Class 3C2.

Configurability

The MicroNet Safety Module is programmed through a software service tool, allowing users to customize the safety device's inputs, outputs, and operation to a specific application. Designed specifically as a safety PLC, the MicroNet Safety Module includes safety-based logic, testing functions, testing sequences, and trip/alarm event logging. As IEC safety standards dictate routine testing of all safety systems, this device can be configured to automatically perform self and system tests, and to annunciate and log the results of each test.

Typical programmable logic functions (AND, NAND, OR, NOR, XOR, XNOR, NOT, analog comparators, timers, delays, etc.) are available with which to use to create application-specific safety programs. To simplify configuration of all three modules, a special copy function is available within each module, which allows a module to copy its exact configuration to another module if desired. NERC-compliant password protection is used to protect each module from accidental or malicious configuration changes.

Installation Information

- Approximate dimensions, including faceplate: 330 x 445 x 159 mm (13 x 17.5 x 6.25")
- Depending on part number ordered, designed to be bulkhead mounted on a wall or skid, or flush-mounted vertically within a panel or cabinet
- Rated for IP56 (ingress protection level 5-6) based locations
- Operating / storage temperature range: -20 to +60 °C

Input Signals

Power Source (2 Redundant)

- High Voltage Power Supply (88–264 Vac/47–63 Hz; 90–150 Vdc) @ 90 W
- Low Voltage Power Supply (18–32 Vdc) @ 100 W

Speed Signals (1/kernel, 3 total)

Inputs can be configurable to accept signals from:

- MPUs (100–32 000 Hz) @ (1–35 Vrms)
- Proximity probes (0.5–25 000 Hz) @ 24 Vdc
- Gear Tooth Range (1–320 teeth)

Analog/Discrete Inputs (13/kernel, 39 total)

- Alarm/Trip Reset Command (Discrete Input, one per kernel)
- Start Command (Discrete Input, one per kernel)
- Speed Fail Override Command (Discrete Input, one per kernel)
- Analog or Discrete Inputs—Configurable (10/kernel, 30 total)

Output Signals

Discrete Output Relays (model dependent)

- Voted Relay Models only—Shutdown relay output (2 total, 2-out-of-3 voted)
 - o Rated for 8 A @ 220 Vac or 8 A @ 24 Vdc
- Independent Relay Models only—Shutdown relay output (2/kernel, 6 total)
 - o Rated for 1 A @ 24 Vdc

- Programmable relay outputs (3/kernel, 9 total)
 - o Rated for 1 A @ 24 Vdc
 - o Functions—Alarm, trip speed switch, analog switch, test status, etc.)

4–20 mA Analog Output (1/kernel, 3 total)

- Dedicated to function as a speed meter readout

Communication Ports (1/kernel, 3 total)

- Serial RS-232, RS-422, RS-485 Modbus port

Regulatory Compliance

North American Compliance:

- **CSA:** CSA Certified for Class I, Division 2, Groups A, B, C, and D, T3 at 60 °C Ambient for use in Canada and the United States
- **NERC CIP** Cyber Security Standards

European Compliance:

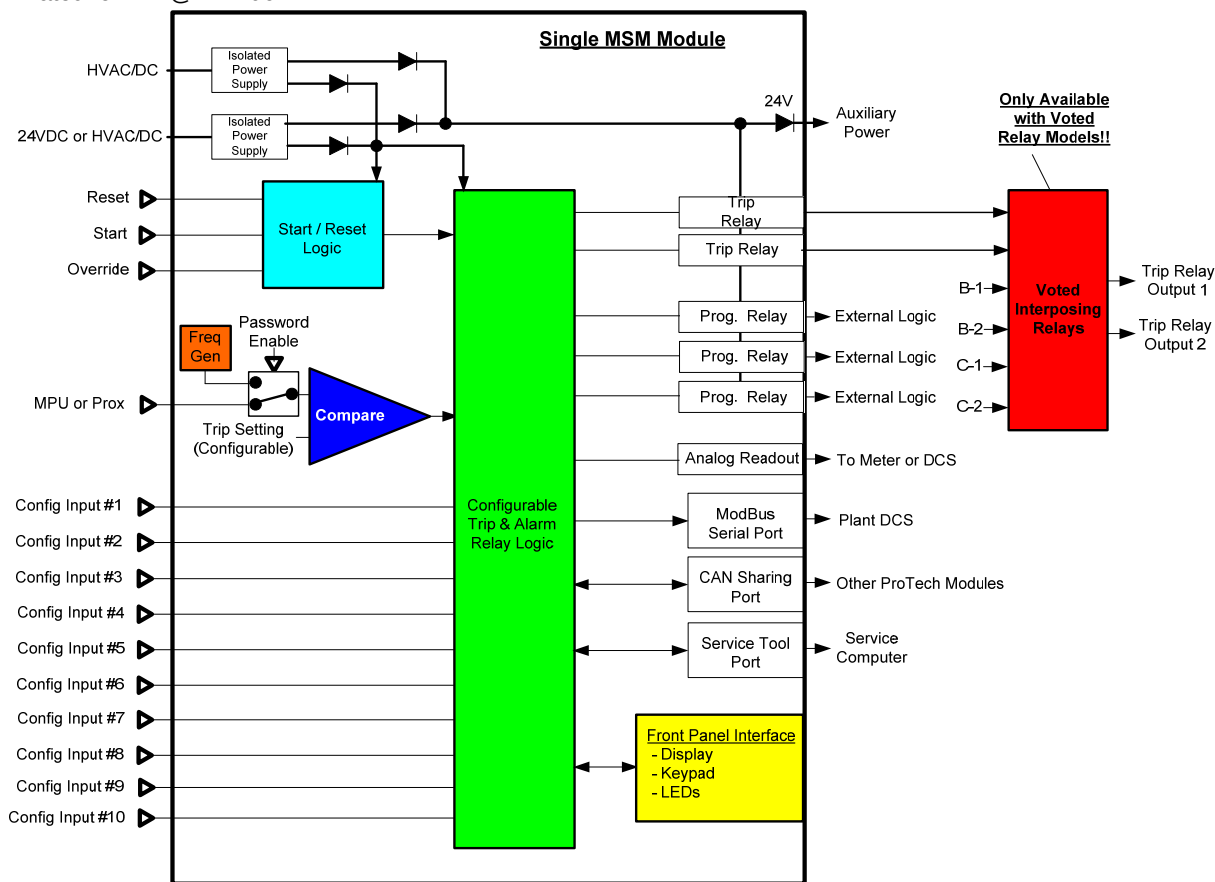
- **EMC Directive:** 2004/108/EC
- **ATEX Directive:** 94/9/EC Zone 2, Category 3, Group II G, Ex nA II T3

Other International Compliance:

- **TÜV:** TÜV certified for SIL-3 per IEC 61508 Parts 1-7, Function Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems
- **C-Tick:** Declared to Australian Radiocommunications Act of 1992 and the New Zealand Radiocommunications Act of 1989.

Other Compliance:

- **IEC60068-2-60:** 1995 Part 2.60 Methods 1 and 4 (conformal coating)
- **API670 & API612** compliant
- **RoHS Exempt** per Annex IA of Directive 2002/96/EC referring to "monitoring and control instruments" within the meaning of Category 9



Single Module Functional Diagram

