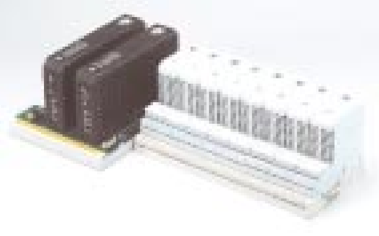
SafetyNet System - Overview



General

The MOST SafetyNet System is a "Programmable Electronic Safety System", certified according to IEC 61508 as suitable for use in safety-related applications up to Safety Integrity Level 2.

The system is suitable for use in emergency shutdown, fire & gas and burner management applications.

New additions to the family

The MOST SafetyNet System uses the same basic structure as the MOST Process Control System, but in addition incorporates specifically developed components. These are:

- SafetyNet Controllers (8851-LC-MT)
- Dedicated Controller Carriers for Earth Leakage Fault Detection (8751-CA-NS)
- SafetyNet IO Modules -Analog Input with HART (8810-HI-TX) and Discrete IO (8811-IO-DC)
- Workbench software tools for use with the SafetyNet System (8841-LC-MT)

Open communications

MTL Open System Technologies products are just that - open. SafetyNet nodes communicate with one another, with standard MOST nodes, historian and asset management packages and with HMI packages over a fault tolerant Ethernet LAN, running at up to 100 Mbit/s.

Peer to peer communication

SafetyNet Controllers can communicate with one another via Ethernet using SafetyNet P2P - which has been certified as suitable for use in SIL 2 applications. Robust checks and controls on access and data corruption ensure the safety of communication and allow safety functions for which the inputs and outputs are widely separated to be easily implemented - both in terms of the software programming and in the hardware design.

Mixing safe and standard

Standard IO Modules can be mounted on SafetyNet Nodes - together with SafetyNet IO Modules - without affecting the node's functional safety performance. Only standard applications can read data from standard Modules, but both standard and SafetyNet applications are allowed to write to standard modules. This flexibility can simplify hardware design, where the physical constraints of the particular locality demand such an approach.

Serial interfaces

The Open approach extends to Modbus serial interface products - which can be connected to any node (SafetyNet or standard) by an RS485 connection.

As with data from standard IO Modules, this data can be read by standard Controllers, but not by SafetyNet Controllers. Both standard and SafetyNet Controllers can write to such devices.

Comprehensive programming tools

The SafetyNet System is programmed using the Workbench software package - in common with the MOST Process Control Products. In addition to providing the options of programming the required safety function in one of three IEC 61131-3 languages (Ladder Diagram, Function Block Diagram and Structured Text) the package also provides many useful tools to assist in testing and commissioning.

Restricted access

Access to modify safety-related parameters within the configuration and application program must be restricted to authorised personnel. The SafetyNet system provides a number of layers and methods of providing this protection. Only users with "Safety Responsibility" can access the safety-related aspects of the Workbench. Only computers that the SafetyNet Controller identifies as "trusted hosts" can download new parameters. A download can only take place when an "over-ride key-switch" is set to the required position. And, if required, each SafetyNet Controller can be protected by its own password - without which access to the safety parameters is denied.

Maintaining field instruments

Maintenance over-rides can be implemented from operator workstations in full compliance with the guidelines from TUV. Users define - as part of the safety application - the actions to be taken to maintain a particular instrument and the SafetyNet System then implements these pre-defined actions.

HART capability

The SafetyNet System allows full access to HART field devices for Emerson's AMS maintenance software. (The first release of SafetyNet will not have full HART capability, contact MTL for further information).

Earth leakage detection

Earth leakage fault detection may be implemented using the 8751-CA-NS Controller Carrier in conjunction with an input channel from an 8811-IO-DC Discrete I/O Module. If ELFD is not required, SafetyNet Controllers can be mounted on 8750-CA-NS Controller Carriers.

On-line changes

Where allowed by local practices - and following adequate testing and approval - new safety programs and configuration can be downloaded on-line and in real time. In some situations, this may be possible without interrupting the operation of the safety function.

SafetyNet Controller - Overview

General

The 8851-LC-MT SafetyNet Controller stores and runs the SafetyNet application program which is downloaded from the Workbench.

It manages a number of communication paths: with the IO Modules mounted on the local node via the internal Railbus; with other entities on the Ethernet LAN (other MOST nodes, PCs running the Workbench programming tools, HMI, historian packages and asset management tools) and with remote mounted serial devices.

The SafetyNet Controller also manages the implementation of the redundancy strategy either as master or standby.

Certification

The SafetyNet Controller is certified for use in safety-related applications up to and including SIL 2. The SafetyNet Controller achieves this Safety Integrity Level with a 1oo1D architecture (i.e. it operates in "simplex" mode, with correct operation ensured by comprehensive internal diagnostics). In such applications the SafetyNet Controller is used in conjunction with the 8811-IO-DC SafetyNet Digital Input/Output Module and the 8810-HI-TX SafetyNet Analog Input Module with HART*. The SafetyNet Controller is mounted on its dedicated Carrier 8751-CA-NS.

*First release of SafetyNet will not have full HART capability.

Safe by design

The SafetyNet Controller has been designed specifically for safety-related applications and is certified on the basis of the excellence of its design. It does not depend for its certification on "proven in use" data.

Diagnostics

If the SafetyNet Controller's internal diagnostics detect a fault that would prevent the SafetyNet System from carrying out its safety function, then it will initiate a controlled shutdown. A controlled shutdown has two objectives - firstly, to ensure that the SafetyNet System enters its failsafe mode; and secondly, to record sufficient data to allow the reason for the shutdown to be determined.

If a SafetyNet Controller enters a controlled shutdown, then all communication with IO Modules is stopped and - when the programmed time delay for each IO module has elapsed - they will enter their safe states.

System size

The SafetyNet Controller can interface with up to 64 locally mounted, 8-channel IO Modules - giving a total capacity of over 500 channels per node. The Ethernet LAN is capable of supporting over 200 nodes, giving a maximum theoretical capacity of over 100 000 channels!

HART pass-through

SafetyNet Controllers can be configured to allow transparent access to the process variables and status information provided by HART field instruments. HART data cannot be used within the SafetyNet application (as - for example - it does not employ sufficiently rigorous data error detection algorithms), but communication with such devices can be achieved by using a "pass-through" command which does not involve, nor interfere with, the safety application. (The first release of SafetyNet will not have full HART capability, contact MTL for further information).

Live maintenance

Once the Ethernet LANs are isolated, SafetyNet Controllers can be removed and replaced - with the local power supplies still connected - even in Division 1, Class 2 or Zone 2 hazardous areas.

Redundant Controllers

SafetyNet Controllers can be used in a master - standby redundant configuration to improve the availability of the safety function, but this is not required for safety. Redundancy is implemented by simply inserting the new Controller in to the free slot on the Controller Carrier.

The SafetyNet system will automatically upload the required SafetyNet application to the new Controller and initiate the redundancy algorithms. Switching between redundant Controllers on detection of a fault is automatic and bumpless.

The standby Controller continually performs the same processing, on the same data and at the same time as the Master and the results are routinely cross-checked. This ensures that the Standby is always ready to take over control from the Master. The redundancy strategy employed is known as "rendezvous redundancy".

The "Change State" button on the Controller Carrier is used to switch a master to being the standby in a redundant pair, to switch a standby offline and to instruct an offline standby Controller to synchronise itself with the Controller and to enter standby.

If a SafetyNet Controller has entered the “Failsafe” state, it can be brought out of this state by use of the “Change State” button.

Serial communications

Each SafetyNet Controller provides two serial ports - one of which is physically connected via the Controller Carrier, the other directly on the Controller itself. The two ports can be configured to be entirely independent, or can be made to work redundantly, either as redundant connections to the same serial link or as redundant connections to redundant links.

When redundant ports of a single Controller are configured as Modbus masters, redundancy issues are handled automatically by the SafetyNet Controller (deciding when to switch to the standby port, alarming failures in the standby).

When redundant ports of a single Controller are configured as Modbus slaves and multi-dropped on a single serial link, the SafetyNet Controller will again manage the redundancy (deciding which port respond to the Modbus master and alarming a fault in the standby port).

When redundant Controllers are used, this adds additional availability to the arrangements above. It is not possible to use the ports on the standby Controller as additional serial connections.

SafetyNet Controller

8851-LC-MT

- *Certified for use in SIL 2 safety applications, according to IEC 61508*
- *Comprehensive internal diagnostics provide basis for safety architecture 1oo1D*
- *Optional redundancy with bumpless transfer for increased availability*
- *Dual redundant high speed fault tolerant Ethernet LAN*
- *Two connections to serial devices*
- *On-line configuration and re-configuration*
- *Communicates with up to 64 I/O modules*
- *Communicates on peer-to-peer basis with other SafetyNet and standard Controllers*
- *Can write to standard output modules without compromising safety function*
- *Live maintainable and hot-swappable - even in Class 1, Div 2 or Zone 2 hazardous areas*
- *HART pass-through of process and status variables*
- *Event logging up to 8000 events*
- *12Vdc Controller power required from 8913-PS-AC*

CONTROLLER SPECIFICATION

See also System Specification

LAN INTERFACE

Transmission medium	100BaseTX or 10BaseT Ethernet™
Transmission protocol	SafetyNet P2P*
Transmission rates	10 - 100 Mbits/s
LAN connector type (x2)	RJ 45 (8-pin)
LAN isolation (dielectric withstand)	1500 V
Action on software malfunction	Halt CPU / Reset CPU

* SafetyNet P2P is a modified form of Modbus™ certified as suitable for use in SIL 2 safety related applications that require peer-to-peer communication.

SERIAL INTERFACES (COM 1 & COM 2)

Transmission rates	1.2 – 115.2 kbits/s (async.)
Transmission standard	RS485 half-duplex
COM 1 connector (on carrier)	9-pin D-type connector (F)
COM 2 connector (on controller)	9-pin D-type connector (M)

HAZARDOUS AREA SPECIFICATION

Protection Technique	EEx nL IIC T4
Location (FM and CSA)	Class 1, Div.2, Grps A,B,C,D T4

POWER SUPPLIES

Controller Power Voltage	12V dc (from 8913-PS-AC)
Controller Power Supply	0.4A (typical), 0.5A (max.)
System Power Supply	15mA (max.)

MECHANICAL

Module dimensions	69 (w) x 232 (l) x 138 (h) mm
Weight (approx.)	1.35kg

Ethernet™ is a trademark of Xerox Corporation
Modbus™ is a trademark of Schneider Automation Inc
HART® is a registered trademark of the HART Communication Foundation

SafetyNet Analog IO Module – Overview

General

The SafetyNet Analog Input Module with HART provides the interface to 8 channels of 4-20 mA input signals.

The SafetyNet Analogue Input Module is certified for use in safety-related applications up to SIL 2. In such applications the module is used with the 8851-LC-MT SafetyNet Controller and 8811-IO-DC SafetyNet Discrete Input/Output Module.

Diagnostics

The SafetyNet Analogue Input Module carries out a number of diagnostic checks to confirm the accuracy of the measurement reported and the correct operation of the module.

In addition to the primary measurement, a second diagnostic measurement is made using different internal circuitry. The two values are then compared. The primary measurement is reported as faulty if it differs from the diagnostic measurement value by more than 2%.

Further tests are carried out on internal supply and references voltages.

If a particular channel fails a test, then that channel is made inactive. If the failed test indicates that the Module is not working correctly, it will enter Controlled Shutdown.

Live maintenance

The field wiring connections to the SafetyNet Analogue Input Module are classified as non-incendive and can therefore be live worked in a Class 1, Division 2 or Zone 2 hazardous area.

(Note the Bussed Field Power connection must be isolated before the module is removed or replaced).

Input sampling and filtering

Each input channel is sampled once every 25ms and is filtered by 1st order hardware and software filters. The software filter can be disabled or set to a number of different values according to the filtering requirements of each channel.

HART capability

The HART capabilities of the Analogue Input Module allow acquisition of secondary variables – which can be used by a standard (but not SafetyNet) application program. The Module also allows Emerson's AMS package to communicate with any HART field device transparently, using HART pass-through. (The first release of SafetyNet will not have full HART capability, contact MTL for further information).

LED's

For the operation of the Power and Fault LED's see IO Module Overview.

Module 'Channel' LED's (yellow)

On – Channel in range (4-20mA)
Off – Channel inactive

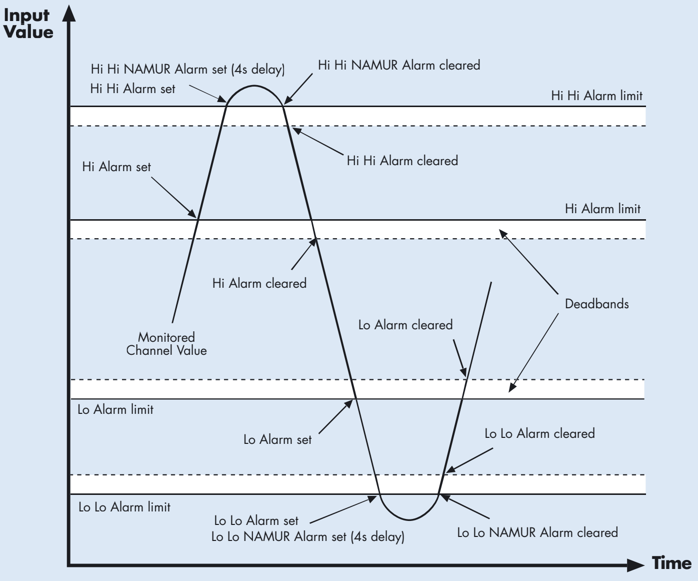
Flashing (equal:mark space ratio) – Any of the following, with an active channel: line fault (indicated by the input measurement being outside the 4-20mA range), loss of HART signal, Hi-Hi or Lo-Lo alarm.

Alarms, Deadband, Dead Zone

The Analogue Input Module has a number of configurable parameters for managing setting and clearing alarms and triggering the reporting of a new input value.

Hi, Hi-Hi, Lo and Lo-Lo alarms can be configured – together with a Deadband through which the input must move before the alarm is cleared. The relationship between these parameters is shown in the diagram below.

A Dead Zone can also be configured, which is the value by which an input measurement must change before it is reported as a new value.



SafetyNet Discrete Input/Output Module

8-channel combination

8811-IO-DC

General

The SafetyNet Discrete Input/Output Module provides the interface to 8 channels that may be configured in any combination of discrete inputs and outputs.

The SafetyNet Discrete Input/Output Module is certified for use in safety-related applications up to SIL 2. In such applications the module is used with the 8851-LC-MT SafetyNet Controller and 8810-HI-TX SafetyNet Analogue Input Module with HART.

Combined inputs and outputs

Each of the 8 channels of the SafetyNet Discrete Input/Output Module may be configured, on a channel-by-channel basis, as either an input or an output.

When configured as an input, the channel is suitable for use with dry contacts – with power supplied from the Module.

When configured as an output, the channel is capable of switching up to 2.0A (maximum of 6.0A continuous per module). Output channels are used with solenoids, valves and alarms

Diagnostics

Comprehensive diagnostic tests are performed on the module and each of its channels, including tests for stuck ON and stuck OFF output switches.

Live maintenance

The field wiring connections to the SafetyNet Discrete I/O Module are classified as non-sparking and can only be worked on in a Class 1, Division 2 or Zone 2 hazardous area once the Bussed Field Power connection has been isolated.

Note: the Bussed Field Power connection must also be isolated before removing or replacing the module.

Input configuration

Input channels are used to interface to volt free contacts. Line fault detection can be turned OFF or can detect open circuits or both open and short.

Input filtering

A change in the input state is recorded only if the states observed at the start and end of the filter time interval are the same. If they are different the previous state is maintained. (This reduces the chance of noise being incorrectly interpreted as a change of input value).

The filter time interval can be configured between 0 and 8s, in 1ms intervals.

Input transition counting

A counter can record the number of filtered transitions of a particular type. Depending on the polarity setting, the counter will either count transitions from 0 to 1, or from 1 to 0. The counter "wraps around" from 65 535 to zero without indication.

Transitions are counted even if the channel is configured to "latching".

Earth leakage detection

Where earth leakage fault detection is required, a single channel of an 8811-IO-DC module must be configured to monitor earth leakage and wired to the appropriate terminals of an 8751-CA-NS Controller Carrier.

Input latching

Inputs can be configured to "latch" a particular (filtered) input transition and maintain the output in the latched state until the latch is cleared. "Normal Polarity" will latch a transition from 0 to 1 as 1, "Inverse Polarity" will latch a transition 1 to 0 as 0. The operation is described in **figure 1**.

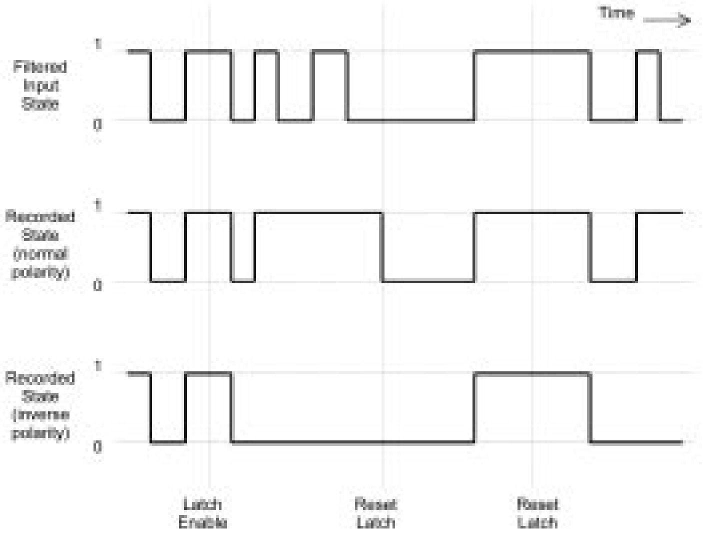

Time
Filtered Input State
1
0
Recorded State (normal polarity)
1
0
Recorded State (inverse polarity)
1
0
Latch Enable
Reset Latch
Reset Latch

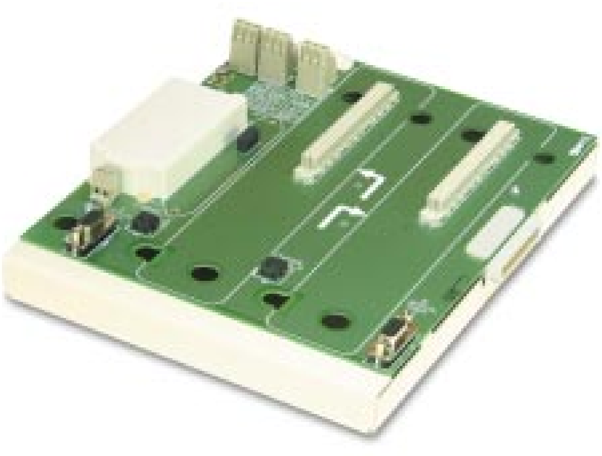
Figure 1 - recording of input states

Controller Carrier

ELFD Controller Carrier

8751-CA-NS

- *terminals for earth leakage fault detection*
- *accommodates two SafetyNet Controllers*
- *accommodates Power Supply Monitor module*
- *two serial port connections*
- *manual " change state" buttons*



The ELFD Controller Carrier provides a mounting platform for up to two SafetyNet Controllers (8851-LC-MT). It can also accommodate a Power Supply Monitor module (8410-NS-PS) which can monitor the health of up to two 8913-PS-AC, four 8914-PS-AC power supplies and the 12V supply to Intrinsically Safe Modules (when these are used). For each Controller there is a serial port connector and a manually operated ""Change State" button. The Carrier also provides terminals that are used when earth leakage fault detection is required.

CARRIER SPECIFICATION

See also System Specification

CARRIER MOUNTING MODULES

SafetyNet Controller (x2) 8851-LC-MT
Power Supply Monitor Module 8410-NS-PS

ELECTRICAL CONNECTIONS

Railbus connector ....male out
Serial port connectors........................9-pin, D-type (female) (x2)
Power Fail connections........................screw terminals (x7 pairs)
Ground connection ....M4 screw terminal (x1)
BFP0V connection ....M4 screw terminal (x1)
Earth leakage fault detection connections
....screw terminals (1 pair)
System Power connections.....................................6-Pin (male)
(Note: this does not provide power to the SafetyNet Controllers)

MECHANICAL

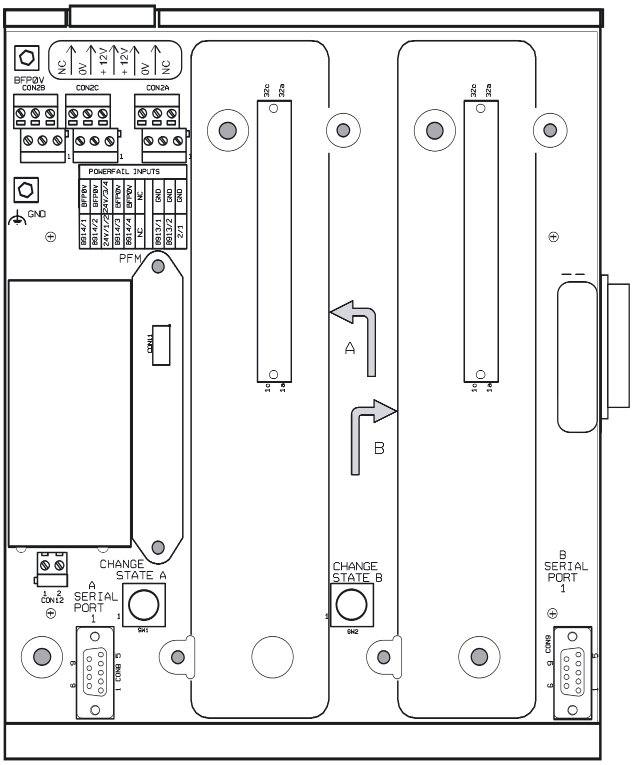
Dimensions ....200 (w) x 253 (d) mm (footprint)
Height ....28 mm (top of circuit board)
....55 mm (overall)
Weight ....1.43 kg (approx.)
Mounting methods ....flat panel (4 fixings)

USER CONTROLS

Two " change state" buttons, one for each SafetyNet Controller, are provided on the carrier. The state change depends upon the controller state before the button is pressed. See table below for effects.

State	Effect
Master	Change to standby if current standby is healthy
Standby	Change to offline state
Backup	Re-synchronise and return to standby

CONTROLLER CARRIER LAYOUT



January 2007