PAC8000 SafetyNet

SIL 2 Functional Safety System

A cost-effective functional safety system

GE Intelligent Platforms, through its acquisition of MTL Open System Technologies, has established itself as a leading supplier of process I/O and safety products.

One of the key technologies that GE now offers is PAC8000 SafetyNet – a cost-effective functional safety system that meets the safety needs of today's Emergency Shut Down, Fire & Gas and Burner Management applications.

Certified as suitable for use in SIL 2 safety functions by TÜV Rheinland, PAC8000 SafetyNet incorporates the latest design techniques to achieve compliance with IEC 61508 and IEC 61511. PAC8000 SafetyNet is rugged, reliable and open, and has been used worldwide in many different process applications, including power generation, gas plants, chemical and petrochemical industries, pipelines and in all sectors of the oil and gas industries.

SafetyNet can handle the harshest environments and has received Lloyd's Register approval for marine, offshore and industrial use in Lloyd's environmental categories ENV1, ENV2 and ENV3. With this environmental capability, SafetyNet can be remote mounted in the world's toughest environments – for Alaskan pipelines, Saharan well heads and deep sea FPSOs.

SafetyNet's rugged open control platform incorporates Modbus TCP with built-in Fault Tolerant Ethernet (FTE) for redundant communications, providing simple but secure connections to a wide range of standard software and hardware packages. This offers users flexible migration paths that connect to yesterday's legacy control systems, interface with the most up-to-date instruments and software, and look forward to the products that aren't even developed yet.

A new approach to functional safety

SafetyNet was specifically developed to work with IEC 61508, and to meet the needs of the majority of safety requirements – SIL 2.

IEC 61508 defines a new approach to safety, described as a structured, practical, realistic, understandable and defensible approach for selecting a safety system for any given hazard.

Users must specify more capable safety systems to protect against more dangerous hazards. They must consider the entire safety function lifecycle when they analyze the nature of the hazard and the means to protect against it. And when this analysis results in a high risk process – Safety Integrity Level (SIL) 3 or greater, many users will attempt to redesign that process to reduce its risk.

Manufacturers of safety products must design safety into their products – considering software and other "systematic" faults as well as random hardware failures.

SafetyNet was specifically developed to work with this new approach, and to meet the needs of the majority of safety requirements – SIL 2. Not overspecified. Not under-specified. It's as it should be – fit for purpose.

"The SafetyNet solution provides PCS Nitrogen Geismar an OPEN, user-friendly, adaptable, trustworthy, and cost-effective safety platform."

Kirk Hadeed, *Process Control Engineer*
PCS Nitrogen

A compact, elegant and cost-effective solution for risk reduction

SafetyNet provides a high level of internal and automatic diagnostics – achieving SIL 2 without redundant I/O modules or controllers.

An increased level of safety is achieved either by adding redundancy or increasing diagnostic coverage, or both. Traditionally, the focus was on redundancy, but SafetyNet takes a different path. Comprehensive internal diagnostics mean that redundancy is not needed to meet SIL 2 – giving you a compact and cost-effective safety solution.

The diagnostic testing carried out by PAC8000 SafetyNet is integrated into the product. So you'll find the safety manual simple and straightforward. And when the time comes to make changes, you can focus on the application – you won't need to manage changes to the diagnostics too.

Optional Redundancy for Availability

Though SafetyNet doesn't need redundancy to be safe, it does offer redundancy for increased availability in critical applications. Redundant LANs, power supplies and controllers can all be specified if required. And this is redundancy for continuous processes – truly bumpless transfer, alarming of failed components, automatic re-routing of communication paths. It's everything you need to keep your process running continuously.

Connect SafetyNet to Your Existing Control System

SafetyNet's use of open standards allows for an easy integration of safety instrumented systems with your existing Process Control system. Modbus TCP provides an excellent mechanism for high data transfer rates in real time from SafetyNet to an existing Process Automation System. For those with older legacy systems that don't offer Ethernet connections, the widely used Modbus serial protocol may be an alternative.

PAC8000 SAFETYNET
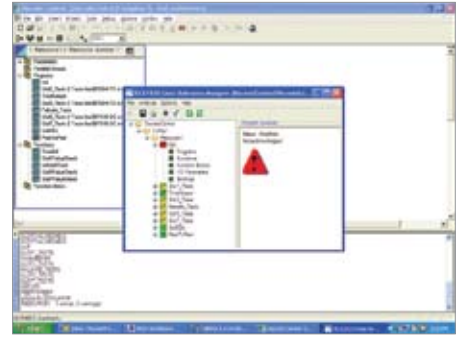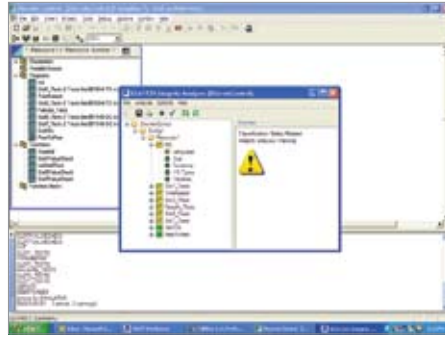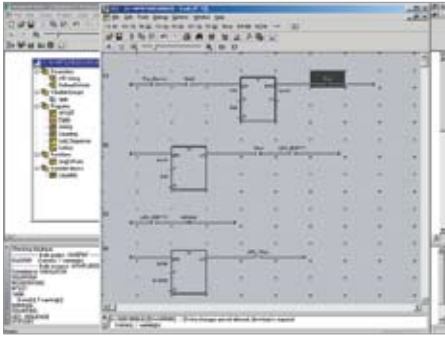
SafetyNet Offers Numerous Key Benefits:

Increased Availability
SafetyNet offers redundant controllers, power supplies and local area networks to increase availability of the SIL 2 safety function and to reduce the rate of nuisance trips.

Safety Certified Peer-to-Peer Communication
SafetyNet P2P, a robust and secure Ethernet protocol, meets the needs of SIL 2 safety functions where inputs and outputs are connected to different nodes.

Live Maintenance
Controllers and I/O modules are designed to be live maintained. With care, you can even replace components live in a Div 2 / Zone 2 hazardous area. Need to modify an application program or download new firmware? You can do this without stopping the process.

HART® Capability
Smart HART field instrumentation has enabled new control and asset maintenance programs, and SafetyNet gives access to these powerful tools.

Normally Energized and De-energized
SafetyNet digital output channels are certified for both normally energized and normally de-energized applications, and can be configured channel by channel.

Safety Manual
The SafetyNet Safety Manual is simple and straightforward – as it should be.

Rapid Application Development
SIL 2 safety applications are developed in the SafetyNet Workbench, using Structured Text (ST), Ladder Diagram (LD), and Function Block Diagram (FBD).

Security and Access Control
The SafetyNet security measures include Password protected user accounts, a Trusted Host table of authorized computers, a Key Switch Tag that blocks and permits access to changes and overrides, and a Controller Password to prevent unauthorized access.

Validation and Verification Software
The SafetyNet Workbench provides tools to test and monitor any changes to the application program.

SafetyNet Logic Static Analysis Tool
The Static Analysis Tool detects structural errors in control strategies, minimizing application issues, reducing the risk of error and cutting software development time.

SafetyNet Logic Differences Utility
The Workbench's Differences Utility can be used to compare a new control strategy with earlier versions and significantly reduce reviews and safety application testing.

Change Control Log
The Workbench maintains a Change Control Log that records all changes to SafetyNet Controllers and modules.

Maintenance Override Capability
SafetyNet's Maintenance Override temporarily suppresses the normal operation of a safety function for maintenance and may also be used to force a system to shut down, or restart the safety system after a shutdown.

Common Platform for Process Control and Process Safety
With SafetyNet, you can combine process control and functional safety in a single platform. SafetyNet's Static Analyzer tools can be used to identify all instances of process control data in the safety controller, helping the safety engineer ensure that the use of process data in the controller does not impact the safety function.

PAC8000 SafetyNet Platform

Power Supplies (not shown)
- 85-264VAC and 24Vdc power supplies
- Supplies power for I/O and controllers
- Redundant power supply options
- Mounting options simplify panel design
- Power supply monitor alerts controller when a power supply fails
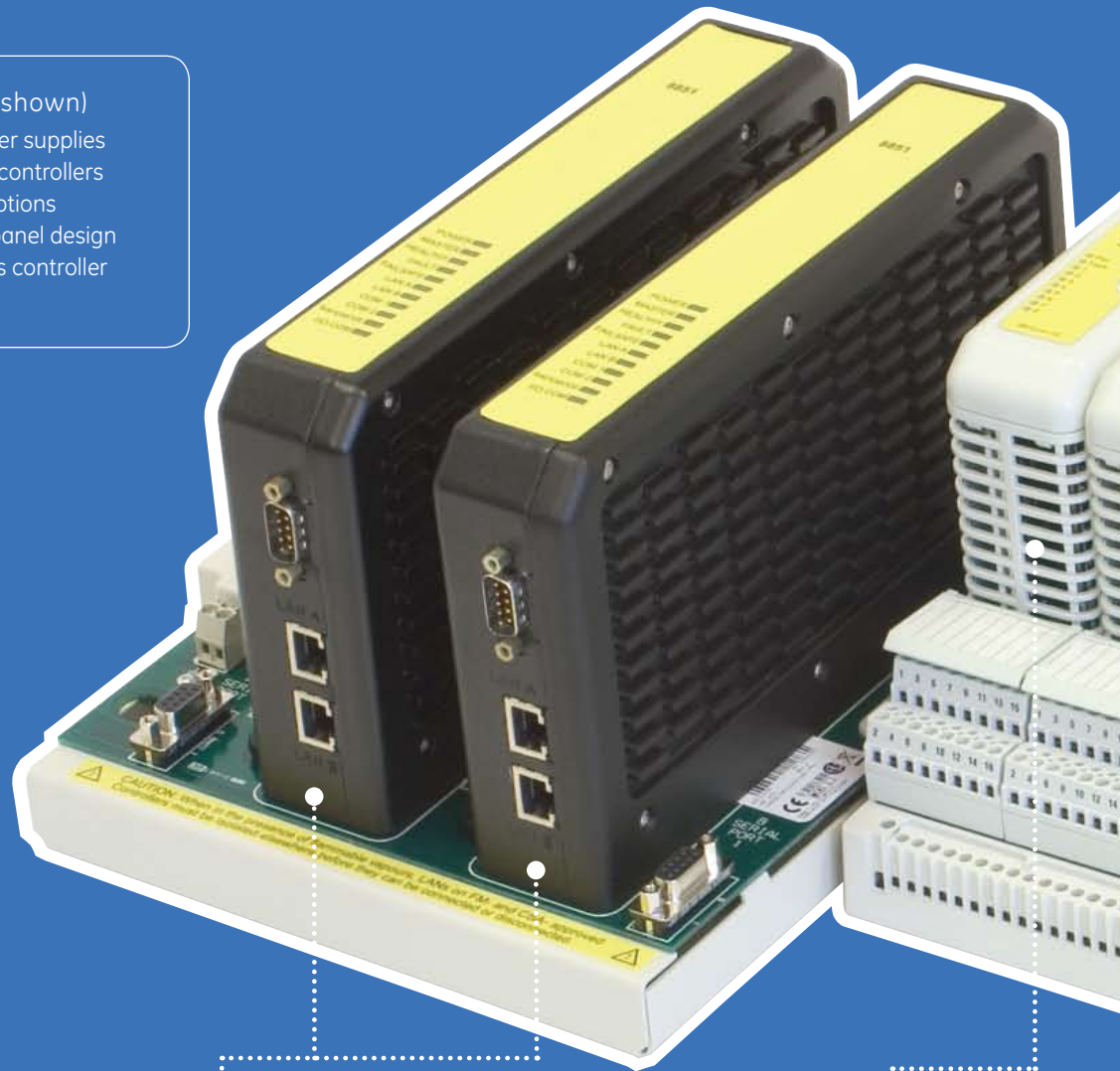
PAC8000 SafetyNet Controllers
- SIL 2 certified with a single controller
- Redundant controllers increase system availability
- Field mountable safety control system
- Controls up to 64 eight-channel modules
- SafetyNet P2P for certified peer-to-peer communications
- On-line reconfiguration

PAC8000 SafetyNet I/O Modules
- Analog input modules offer HART capability
- Discrete modules – individual channels can be configured as inputs or outputs
- Integrated HART support enables remote configuration and interrogation of smart devices
- Mix SafetyNet and Process I/O modules on the same carrier
- LEDs indicate channel and module status
- Live "hot swapping"
- Keying stops modules from being inserted in the wrong position
- Isolation between I/O bus and field wiring

Environment

- Mounts in and connects to Div.2 / Zone 2 hazardous areas
- Operating temperature ranges –40°C to + 70°C
- Resistant to corrosive gasses and salt mist
- Robust operating shock and vibration specifications

Carriers

- DIN rail or surface mounting
- Carries communications between I/O modules and controllers and distributes System and Bussed Field Power
- Choice of 4-module and 8-module carriers
- Cable ground and shield terminals along front edge
- Replacement modules are configured automatically, so maintenance is simplicity itself
- Field power can be supplied through connectors on the back of the carrier

Field Terminals

- Unique, removable terminals for fast wiring and field replacement
- Modules can be replaced without disturbing field wiring
- Optional fuses and disconnects – no interposing terminals required
- Field power routed to terminals – no daisy chaining at the field terminals
- Integral tagging system

GE Intelligent Platforms Contact Information

Americas: **1 800 433 2682** or **1 434 978 5100**
Global regional phone numbers are listed by location on our web site at **www.ge-ip.com/contact**

www.ge-ip.com/safetynet