

PLANTSAFE 8000 SAFETY SYSTEM



*Cutting-edge, open
safety system solutions,
at a fraction of the cost.*

NET  **SAFETY**
MONITORING INC.





PlantSafe 8000 – A Cost-Effective Functional Safety System

PlantSafe 8000 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, PlantSafe 8000, powered by SafetyNet, incorporates the latest design techniques to achieve compliance with IEC 61508 and IEC 61511.

PlantSafe 8000 shares the same virtues as the rest of the Net Safety detection offerings – rugged, reliable performance. The PlantSafe 8000 system's open control platform incorporates Modbus TCP with



built-in Fault Tolerant Ethernet (FTE) for redundant communications, providing you simple but secure connections to a wide range of standard software and hardware packages.

This unique open approach allows users flexible migration paths. Connect to yesterday's legacy control systems, interface with the up-to-date instruments and software packages and look forward to the products that aren't even developed yet – knowing that PlantSafe 8000 will connect to them.

And as with our other products, we believe in straightforward pricing. Pay for our Workbench engineering suite once and you can use it for as many projects as you like, with as many I/O points. We think surprises should only be the pleasant kind. See how PlantSafe 8000 can provide you with a compelling solution for your next safety project.



A New Approach to Functional Safety

IEC 61508 defines a new approach to safety. It's not mandatory - but it is the way forward. IEC 61508 describes a structured, practical, realistic, understandable and – crucially – 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.

PlantSafe 8000 is suited to work with this new approach, and to meet the needs of the majority of safety requirements – SIL 2. Not over-specified. Not under-specified. It's as it should be – fit for purpose.



Integration of Process Control and Safety

PlantSafe 8000 is a certified functional safety system that provides a cost-effective solution for process safety applications, including emergency shutdown and burner management. The system, certified to SIL 2 by TÜV Rheinland, complies with IEC 61508 and IEC 61511 standards. PlantSafe 8000 is a fully scalable system, addressing needs ranging from standalone boilers to extensive shutdown applications. PlantSafe 8000 utilizes the existing MTL open control environment, allowing for the integration of process control, functional safety and plant monitoring.

A tightly integrated platform shortens development times, simplifies the work of the operator, minimizes mistakes, reduces spare part requirements and saves space, weight and money. No wonder end users are demanding a common platform!





Safety Essentials

An increased level of safety is achieved either by adding more redundancy or increasing diagnostic coverage; or doing both. Traditionally, the focus was to add redundancy, but this inevitably means more hardware, more cabinet space and therefore more cost. PlantSafe 8000 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 comprehensive diagnostic testing carried out by PlantSafe 8000 is such that the requirements of IEC 61508 for SIL 2 safety functions are met without the need for redundant IO modules and controllers. (To use the language of IEC 61608, PlantSafe 8000 provides a safe failure fraction of >90% and - as a Type B system - can be used in SIL 2 safety functions with a hardware fault tolerance of 0).

Increased Availability

The effectiveness of an Emergency Shut Down system is measured by its ability to prevent the occurrence of hazardous situations, but it should also be measured on its operational availability. "Nuisance trips" impact production, but can also affect safety – operators begin to view the safety system as a hindrance to their work, not a help – and the pressure to over-ride essential safety mechanisms can be intense.

PlantSafe 8000 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

Safety functions with widely distributed inputs and outputs can be implemented using PlantSafe 8000's certified communication - MTL Safety Net P2P, a robust and secure protocol that meets the needs of SIL 2 safety functions where inputs and outputs are connected to different nodes.

HART Capability

The development of smart HART field instrumentation has opened up new techniques for implementing control and safety strategies and maintenance programs. PlantSafe 8000 gives access to these powerful tools. Each HART input channel can "acquire" up to 4 dynamic variables and device status – allowing this information to be used directly in the safety application. Industry leading asset management solutions can transparently access HART instruments connected to PlantSafe 8000 HART inputs. This allows remote interrogation and configuration of the smart instruments. Be careful though! Access to such powerful tools needs to be carefully controlled in a safety environment.



Normally energized or normally de-energized?

Emergency shut down applications will typically require normally energized outputs – where the output is immediately de-energized on detection of a process problem or an internal fault. Fire and gas applications typically require normally de-energized – where the output is only energized if a fire or gas leak is detected. PlantSafe 8000 digital output channels are certified for both applications – and can be configured on a channel by channel basis.



PlantSafe 8000 Platform

Power Supplies (not shown)

- 90-250 VAC 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



PlantSafe 8000 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
- MTL SafetyNet P2P for certified peer-to-peer communications
- On-line reconfiguration

PlantSafe 8000 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
- LEDs indicate channel and module status
- “Hot swapping” does not affect adjacent modules
- Keying stops modules from being installed 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 $+70^{\circ}\text{C}$
- 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 provided at terminals – no daisy chained power connections
- Integral tagging system



Safety Manual

Sophistication shouldn't mean complexity. PlantSafe 8000 is technologically advanced – but that doesn't mean it should be complicated and difficult to use. A safety system's complexity is apparent when you read the Safety Manual – which defines what you can do, can't do and must do. The Safety Manual is simple and straightforward – as it should be.

Rapid Application Development

The PlantSafe 8000 Logic Workbench uses the same programming environment as the standard MTL Logic Workbench. The Workbench is used to develop, download, simulate, debug, monitor and edit application programs. It's also used to configure the IO Modules, the Controllers and the Network. SIL 2 safety applications are developed in the PlantSafe 8000 Workbench, using one of three safety approved IEC61131-3 programming languages.

Structured Text (ST) is an intuitive, high level structured language that is mainly used to implement complex procedures that are not easily expressed with graphical languages.

Ladder Diagram (LD) is one of the familiar methods of representing logic equations and simple safety applications.

Function Block Diagram (FBD) is a graphical language that allows the user to build complex procedures by connecting pre-defined function blocks together on the screen.

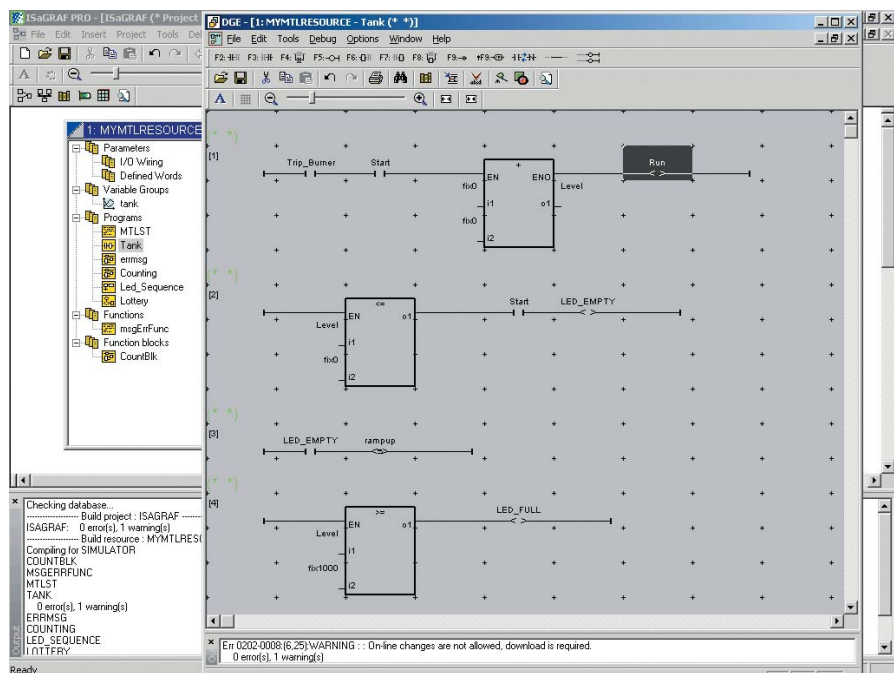
Security and Access Control

Only personnel with appropriate training and authority, using the appropriate tools, should be able to make changes to a safety application or its configuration. The PlantSafe 8000 system provides a number of tools and levels of security to prevent unauthorized access.

Password protected user accounts restrict access to the PlantSafe 8000 Workbench – only users with "safety authority" have the right to make changes.

Further protection is provided for each PlantSafe 8000 Controller by a number of features:

- The Trusted Host Table lists the LAN computers that are authorized to communicate with each controller
- Key Switch Tag locks out / permits access to make changes and implement over-rides
- Optional Controller Password prevents access unless the password is known





Validation and Verification Software

Experience shows that accidents often happen because of mistakes in the specification, design and modification of the application program.

The PlantSafe 8000 Workbench provides tools to test and monitor changes to this critical aspect of safety system implementation.

Logic Static Analysis Tool

The Static Analysis Tool is used to detect structure errors in control strategies, minimizing safety application issues. This tool helps reduce the time spent in reviewing application logic and reduces the risk of error, making your software development more efficient.

Logic Differences Utility

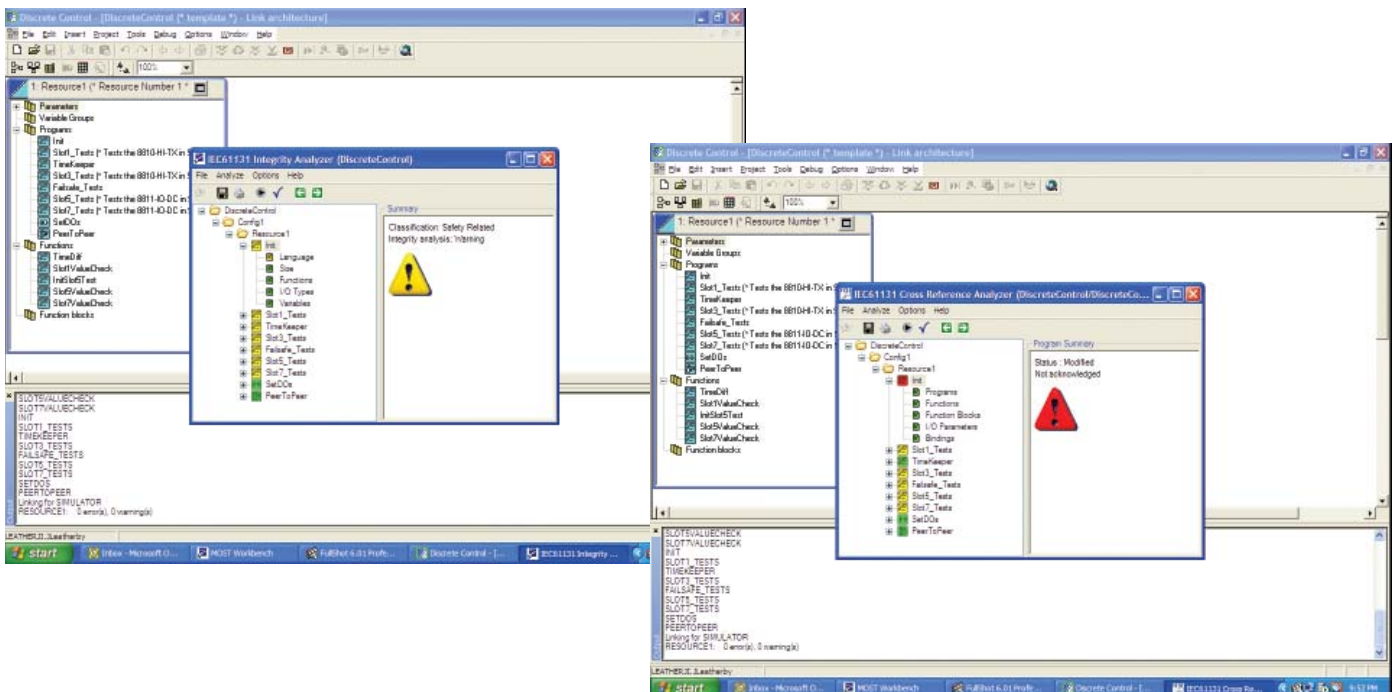
A Download Report is generated when a control strategy is downloaded to the controller. The Workbench's Differences Utility can be used to compare this report with earlier versions of this report to quickly identify a summary of changes. The Difference Utility can significantly reduce the time spent in reviews and safety application testing.

Controller Change Control Log

The Workbench maintains a Change Control Log that records all changes to PlantSafe 8000 Controllers. These changes include changes to IO Modules, IO Tags and configuration parameters, communications parameters, strategy updates and successful strategy downloads. The Change Control Log records the user, date, time and the instance of the application used as well as the detail of the change made, providing a useful audit trail of all changes.

Maintenance Over-ride Capability

Maintenance Over-ride capability allows sensors and actuators to be maintained, by temporarily suppressing the normal operation of a safety function. Maintenance over-rides may also be used to meet other requirements – such as forcing a system to shutdown or restarting the safety system after a shutdown has taken place.





An Integrated Control and Safety Solution

Historically, the emphasis for Control and Safety was on diversity - to reduce the probability of "common" failures affecting both operational and protection systems simultaneously. More recently though, the trend has been towards closer integration between the two - as users have realized that complexity and confusion have a detrimental affect on actual, practical and real-world safety. For others, there simply isn't the space to implement two systems with different and possibly conflicting cabinet layouts.

Net Safety PlantSafe 8000 and MTL MOST Control give you a number of options for integration - but at all times provide the necessary separation between the two to ensure that safety is never compromised. (In the language of functional safety, MTL MOST Control is guaranteed to be "non-interfering" with safety functions implemented in PlantSafe 8000).

For example, values read by PlantSafe 8000 Input channels can also be used as inputs to control loops. The values being passed to the control application by peer-to-peer communication between PlantSafe 8000 and conventional Controllers. Also, PlantSafe 8000 nodes can

be used as "data concentrators" for local conventional I/O and local serial communication devices. The data is sent and received to the PlantSafe 8000 node by peer-to-peer communication and, again, this is guaranteed to be "non-interfering".

Our vision of integration encompasses process and discrete control, functional safety, fire and gas detection, combustion control, burner management, remote I/O and so on.

Connect PlantSafe 8000 to Your Existing Control System

PlantSafe 8000'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 PlantSafe 8000 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.





Net Safety Systems Division

Net Safety Systems Division offers fit-for-purpose technology solutions for F&G (Fire & Gas) Systems with up to SIL 3 certification. What sets us apart is the ability to provide a specialized engineering solution within a wide range of specifications. We design your entire system utilizing the most efficient and cost-effective combination of products for your specific application.

Our extensive knowledge and expertise in fire and gas detection allows us to provide a system solution custom-made to meet your application requirements while ensuring the safety and well-being of your plant and personnel. Every system offered by Net Safety is proven in the industry worldwide and engineered to the strictest global standards. Designed with a modular approach, our solutions offer complete expansibility while utilizing the latest technology available.

Net Safety Monitoring Inc.

Net Safety Monitoring Inc. is a global leader in the engineering and manufacturing of a full range of industrial safety systems and F&G detection equipment. Net Safety maintains office locations in Calgary, Houston, Dubai and Singapore which are supported by our international distribution and service network. Our corporate vision remains focused on providing premium quality products, with dedicated service and support, at a cost that is highly competitive.

**Redundant Control
System Network
(Fault Tolerant Ethernet)**

PlantSafe



Net Safety Monitoring Incorporated - Corporate Headquarters

2721 Hopewell Place NE, Calgary, AB Canada T1Y 7J7
Direct: (403) 219 0688 | Facsimile: (403) 219 0694
Email: sales@net-safety.com | www.net-safety.com

Net Safety Systems Division

Dayanidhi Lakshmiopathy - Director
Direct: (403) 219 2640 | Facsimile: (403) 219 0694
Email: systems@net-safety.com

CANADA

Larry McGee, Director of Sales
Telephone: (403) 717 2639
Mobile: (403) 608 6097
Fax: (403) 219 0694
larrym@net-safety.com

UNITED STATES

Brian Ledebner, Director of Sales
Telephone: (281) 380 2265
Fax: (281) 419 5844
brianl@net-safety.com

EUROPE

Bruce Curlock, President
Telephone: (403) 717 8201
Mobile: (403) 471 2859
Fax: (403) 219 0694
brucec@net-safety.com

MIDDLE EAST/INDIA

Darshan Behl, Director of Sales
Telephone: 971 4 265 3277
Mobile: 971 50 272 2487
Fax: 971 4 265 3447
darshanb@net-safety.com

ASIA PACIFIC

Adrian Low, Director of Sales
Telephone: (65) 6 561 5671
Mobile: (65) 9 630 8418
Fax: (65) 6 567 0301
adrianl@net-safety.com

LATIN AMERICA

Mauricio Romero, Director of Sales
Telephone: (403) 219 0688
Mobile: (403) 619 9775
Fax: (403) 219 0694
mauricio@net-safety.com