

ProSafe-PLC

Technical Product Description

1 Preface

The ProSafe-PLC system is an Industrial safeguarding system, capable of executing all typical Safety tasks, as well as the related supplementary non-Safety functions. This comprises interfacing with a Man-Machine-Interface (MMI), Distributed Control System (DCS), Sequence of Event Recording (SER), a SCADA system, etc.

This manual will familiarise the reader with the merits of the ProSafe-PLC system, created by the unique system design.

The aspects of Safety and fault-tolerance are discussed, as well as the system structure, configuration, communication capabilities and the specifications.

In particular the powerful ProSafe-PLC SET, System Engineering Tool, is highlighted. It facilitates the engineering, configuration, programming and maintenance procedures; furthermore it creates the project documentation.

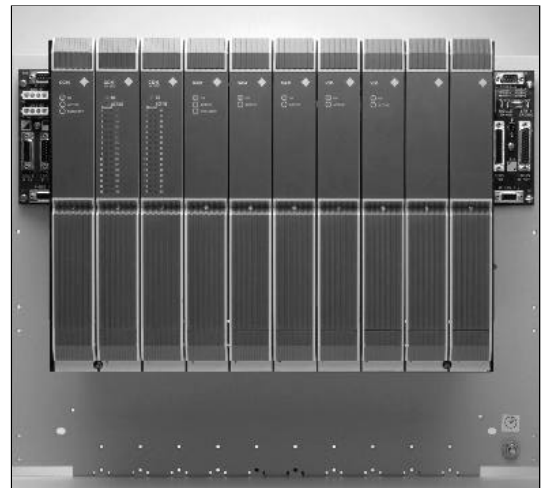


Table of contents

Chapter 1	<i>Preface</i>	2
Chapter 2	<i>Introduction</i>	4
Chapter 3	<i>Safety requirements in Industry</i>	5
	- Introduction to Safety Instrumented Systems (SIS)	5
	- The history of SIS using PLC technology	5
Chapter 4	<i>The ProSafe-PLC system concept</i>	7
	- System structure & design	7
	- Areas of application	11
	- Communication capabilities & SER	12
	- ProSafe-COM and SER	15
Chapter 5	<i>Specifications:</i>	16
	- Modulerack, Unirack	16
	- Powerack	17
	- CCM, Critical Control Module	18
	- CDM, Critical Discrete Module	21
	- SAM, Standard Analogue Module	23
	- EAM, Enhanced Analogue Module	26
	- IDM, Input Discrete Module	28
	- VIM, Voltage Input Module	29
	- RTM, Resistance Temperature Module	30
	- ODM, Output Discrete Module	32
	- SDM+, Standard Discrete Module Plus	33
	- BCM, Bus Continuation Module	35
	- BDM, Bus Diverter Module	35
	- MNI, Module-NET Interface	36
Chapter 6	<i>Project realisation</i>	37
	- The ProSafe-PLC SET, System Engineering Tool	37
Chapter 7	<i>Glossary of terms</i>	39
Chapter 8	<i>Yokogawa ISS serving Industrial Safety</i>	41

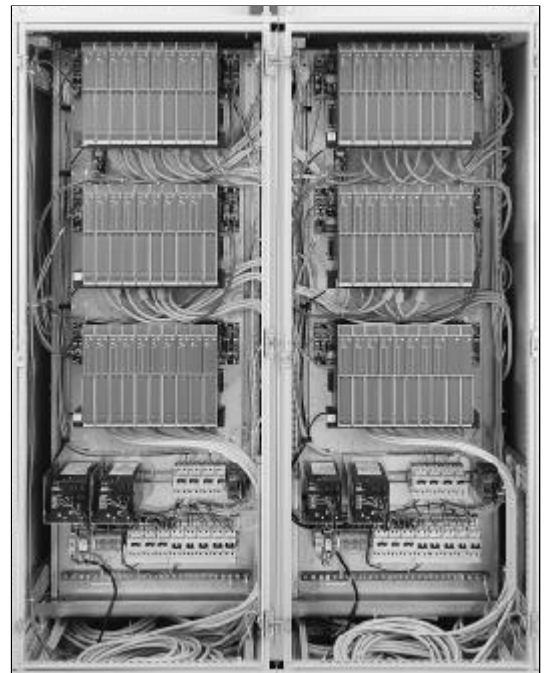
2 Introduction

As a result of a design strategy for superior fault avoidance and fault tolerance, the ProSafe-PLC system in the Quadruple channel architecture outpaces conventional dual PLC's and TMR systems in reliability and availability.

Fault avoidance techniques reduce the system failure-rate, while fault tolerance enables the system to operate successfully, even when a component fails. The Safety critical parts of the ProSafe-PLC system have a Safety certification from the TÜV covering AK1-6 applications.

Typical user applications as a Safety Instrumented System (SIS) are found in the Chemical, Refining and Oil & Gas production industry. This includes the protection of offshore platforms and floating production & storage offshore (FPSO) vessels, such as:

- Emergency Shut-Down systems (ESD) for Safety critical process units;
- Burner Management Systems for incinerator furnaces and steam boilers;
- Compressor protection systems for rotating and piston type compressors;
- Fire & Gas protection systems.



3 Safety requirements in Industry

Introduction to Safety Instrumented Systems (SIS)

The quest for higher Safety

In recent decades, many accidents in industry have been attributed to computer failures, causing loss of life, damage to assets and to the environment. This has strengthened the corporate and public awareness of the need for risk reduction, to create Safety in Industrial processes. The guidelines for safe operation of Industrial installations in the petrochemical, oil and gas production are becoming more and more severe by International Safety standards, developed by the IEC. Safety standards, such as the new IEC 61508/61511, are developed by cooperation of industry groups, Safety certifying agencies and insurance companies, resulting in more stringent regulation and legislation.

The operating companies are aware, that a reliable Safety Instrumented System (SIS) is of great value, not only because of the legal and insurance liability. It serves to provide protection for people, environment and to safeguard the large scale investments, that are involved in today's production processes.

On the other hand, unnecessary interruptions of a production process must be avoided, because this aspect of process "availability" has a direct relation with production yield and cost. Furthermore there also exists an indirect and positive correlation between Availability and Safety. Availability is therefore an integral part of the design of a reliable SIS.

It is important to emphasise that availability by fault-tolerance, is an

other phenomenon than Safety, and to be aware that these two benefits are created by different design strategies. The combination of these two elements in one design requires a specific attention for the facets of common-cause effects and the self-diagnostic capability.

The history of SIS using PLC technology

Regular PLC's were designed around 1970 to create flexibility for process-control and to implement facilities such as PID-loops, calculation, sequencing, etc.

The general trend towards more complex processes and the necessity of "flexibility" during engineering, as well as during operational use, have introduced PLC's as Safety Instrumented Systems (SIS) in the industry. Often also non-Safety related functions have been put in the same systems, because the powerful capabilities.

Today's special Safety-PLC's do all employ a variety of redundant configurations to improve the Safety as well as availability.

- Single PLC's (1oo1), that employ a single signal path from the inputs via a microprocessor to the outputs are unsuitable for SIS systems, since any type of hardware or software failure can create a potentially unsafe situation, if an output switch can no longer be de-energised to perform its protection function. This condition is not likely to be detected by the systems self-diagnostics. Therefore a single PLC does not comply with today's Safety standards and are considered unsuitable for Safety applications.

- **Dual Safety PLC's (2002)** are based on the principle of diagnostics by comparison. Both PLC's execute the same program and in case of a discrepancy between the results of two processors the outputs will be de-energised. The I/O circuits need special provisions for comparison or self-test. This creates an improved Safety performance when compared to a 1001 system, at the expense of increased hardware use, which is responsible for the lower availability or higher false trip rate (FTR) of 2002 systems.
- **A Triple Safety PLC (2003) or TMR systems**, are based on the principle of diagnostics by consensus or majority voting, creating about similar Safety as dual PLC systems, without the need to trip at the first failure. A voting mechanism acts on dynamic changes in order to recognise any differences. However the majority of potential unsafe failures is static and is responsible for 'on-demand failures'. Also the common-cause effects are a source of concern, because in most TMR systems no diversity is applied in the hardware or in software. The higher availability (or low FTR), compared to 2002 systems, is achieved at the expense of fully triplicate hardware.
- **ProSafe-PLC** has a 1001D structure that applies diversity in the dual signal paths, combined with comparison between processors, which is a more effective configuration than a regular 2002 PLC. The architecture denomination 'D' reflects the extensive self-diagnostic 'by reference' capabilities, implemented in each channel and the secondary shutdown path that is controlled by this self-diagnostic. This standard 1001D architecture can be expanded to include optional redundant controllers, providing a low-cost option for redundancy of critical functions.
- **The ProSafe-PLC in 1002D** Quadruple Channel architecture creates full fault-tolerance, by employing the basic 1001D structure in redundancy. At the detection of a first critical failure, the system goes in the 1001D mode and there is no shutdown. An on-line repair can be executed to restore the 1002D structure. When comparing different generic control structures, no other architecture has a lower FTR than this 1002D, according to the IEC 61508/61511 standard. The same conclusion can be found in many other well-documented publications. The Safety and availability performance of 1002D is equivalent, if not better, compared to TMR and furthermore this is achieved at reduced cost.
- **The ProSafe-DSP technology** is employed for the most demanding applications including SIL1-4 or TÜV class AK1-7 and is available as a programmable system, as well as in a solid-state system. The elimination of all system software is a major breakthrough for a programmable system. ProSafe-DSP has eliminated all known sources of unsafe failures by introducing an inherent self-test. This ProSafe-DSP technology can be applied in fault-tolerant configurations (1002 & 2003) for high availability and is described in separate Yokogawa documentation.

Note: The names of the generic SIS configurations: 1001, 1002, 2002, 2003, 1001D, 1002D are assigned to these architectures by the IEC 61508/61511 standard and the ISA SP/TR84.01 technical report.

4 The ProSafe-PLC system concept

System structure & design

Modular Design

The ProSafe-PLC Safety System consists of a range of plug-in modules that includes critical control modules and critical I/O modules. In the ProSafe-PLC architecture these Safety system devices co-operate in a selective and flexible manner. The three categories of modules include control modules, I/O modules and communication modules for plant-wide expansion of the system and interfacing to other networks.

Control modules execute any combination of distinct control languages: function block & ladder logic, while a series of I/O modules act as an interface between the control module and field termination signals. A ProSafe-PLC system is created for a particular application by simply selecting functionality as individual modules and populating the ten-slot MODULRACK shown. Up to 16 racks can be configured in one local area system.

When a module is plugged into a module rack, a connector on the back of the module engages with a receptacle on the MODULRACK backplane. This connection provides the physical communication and power path. When the system is on-line, communication takes effect as soon as the module is inserted. This “hot insert” feature allows on-line replacement of modules, minimising process downtime for system maintenance.

In addition, all slots in a module rack are identical. This allows any module to be plugged into any slot, providing maximum flexibility in initial system design and future expansion.

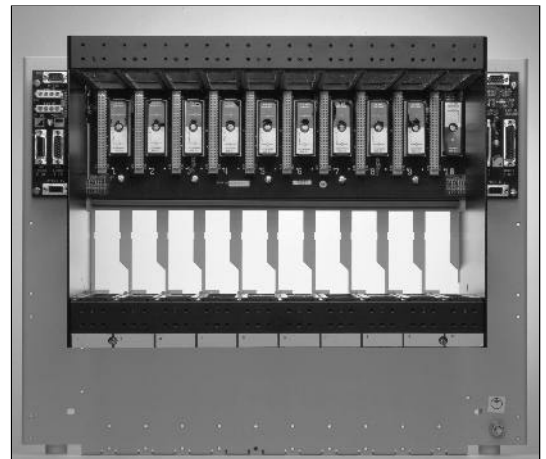


Figure 4.1 ten-slot MODULRACK

High physical strength

The functional Safety is guaranteed by the above described system structure and self-diagnostic capability. On the other hand, fault-avoidance by the rugged design and physical strength enhances the systems reliability and availability, by means of:

- **Cast aluminium housing covering each module serves as a heat sink for the heat producing components and creates a good Safety margin for the operating temperature range;**
- **Coating of all electronic assemblies protects against humidity and chemicals;**
- **Screw-in mounting of modules and clamp-type security protects against shock and vibration;**
- **Isolated I/O and surge protection protect against electromagnetic interference;**
- **FM and CSA approvals allow the use in Class 1, div. 2 hazardous locations;**
- **Multiple levels of access security and version control prevent unauthorised software changes;**
- **Keyed slots for modules and cable connectors avoid replacement errors;**
- **Redundant modules are located on separate hardware, thus minimising common-cause effects.**

It is advantageous to create fully autonomous sub-systems that reflect the sub-unit partitioning of the process plant. It creates “distributed Safety”, and in this way it does avoid unnecessary shutdowns in other process units.

The system structure

The ProSafe-PLC incorporates two separate circuit paths. The standard dual architecture provides unique Guarded Outputs. The Output energy flows through dual switches, executed in diverse-technology. A solid state switch provides the normal controller output and a relay, controlled by built-in diagnostics supplies the second switch.

If a potential dangerous failure is detected within one output channel, the relay contacts will be opened, de-energising the output to ensure a safe action. (In the 1002D structure the process will remain in operation, controlled by the redundant modules.)

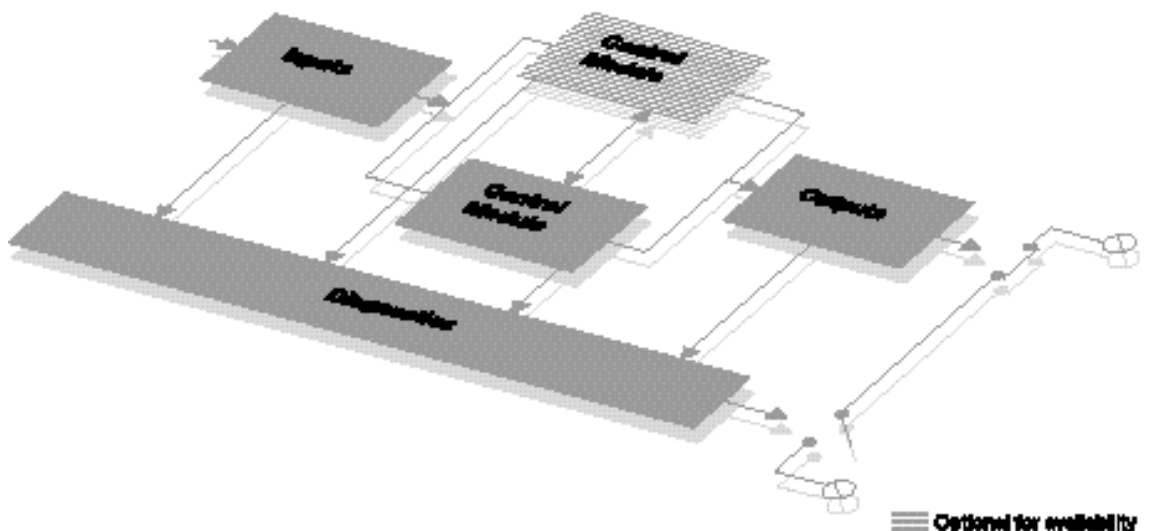
Diversity applied in the dual signal paths, combined with comparison between controllers, has created the ProSafe-PLC, 1001D structure. The architecture denomination ‘D’ reflects

the extensive self-diagnostic capability ‘by reference’, implemented in each channel and the secondary shutdown path controlled by this effective self-diagnostic.

The standard ProSafe-PLC in 1001D architecture features:

- A single controller; single I/O with Guarded Outputs and “fail on” and “fail off” diagnostic output options;
- Redundant power supplies;
- Redundant communication links ;
- Redundant, diverse watchdog timers;
- CPU instruction tests, exhaustive RAM tests;
- Over 1000 different faults can be detected by the diagnostic.

This standard architecture can be expanded to include optional redundant processors, as shown in figure 4.3, providing a low-cost option for redundancy of critical functions. These features come with all the qualities people like about using a PLC for Safety systems, such as advanced logic solving capabilities, modularity, and a rugged design. ProSafe-PLC then adds other features such as fault-tolerance, easy mixing of discrete and regulatory control, and seamless communication with any DCS process control system.



8 Figure 4.2 1001D Configuration with single critical control module for TÜV4 or SIL2

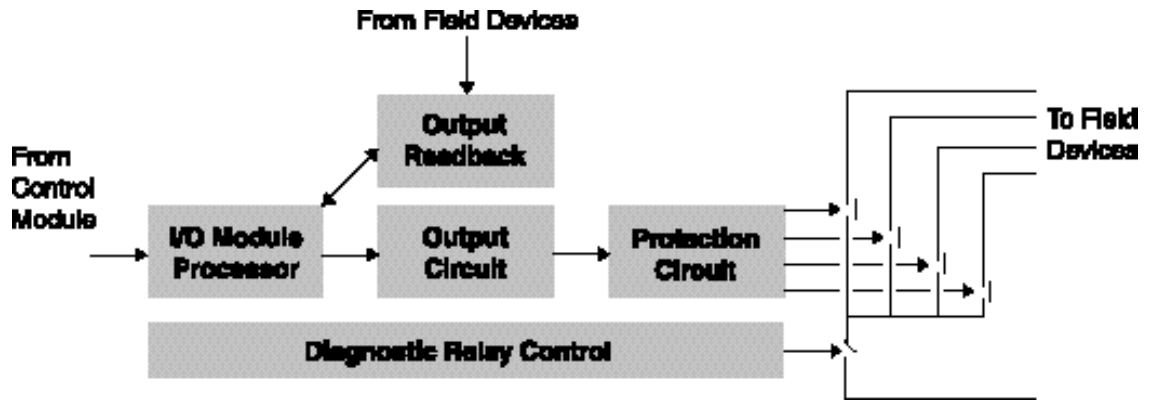


Figure 4.3 shows a block diagram of the standard ProSafe-PLC architecture.

Guarded Outputs

Output modules use a combination of extensive on-line diagnostics and internal “diagnostic cut-off” relays to automatically protect against energised output failures. The block diagram of the standard ProSafe-PLC architecture shows that Output energy flows through “dual-switches” to each load. A solid-state switch provides the normal control module output. A relay, controlled by the built-in diagnostics, supplies the second switch through a set of normally open contacts.

If a dangerous failure is detected within the output channel, the relay contacts will be opened. This action de-energises the output, ensuring the output fails safely.

The Guarded Outputs ensure that no single component failure can prevent a mandatory trip.

Redundancy

While the first priority of a critical control system is Safety, the system must also maintain high system availability to avoid unnecessary shutdowns. ProSafe-PLC achieves high availability through extensive redundancy capabilities, that range from internal standard redundancy features, to redundancy of a single control module, through to full quadruple redundancy.

Standard Redundancy

In its standard form, ProSafe-PLC incorporates a dual architecture and includes redundant communication networks. The M-BUS on which control and communication modules communicate is a secure, redundant, deterministic network. In addition, I/O modules exchange data with control modules over a dedicated redundant bus: the I/O-BUS. Also the Powerbus is a triple redundant bus providing 24 Vdc to all ProSafe-PLC modules.

Module-to-Module Redundancy

The most inexpensive form of redundancy is duplication of a single control module. A control module is made redundant by inserting a second identical module in a slot adjacent to the first, and connecting the two modules via a redundancy cable. (Figure 4.4). All program synchronisation, comparison and control

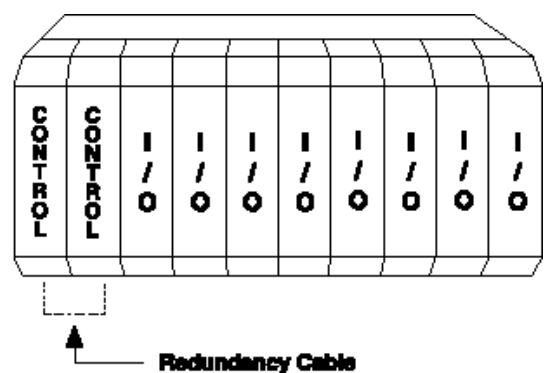


Figure 4.4 Module-to-Module redundancy

arbitration logic is embedded in the control module firmware, while no user programming is required to activate any of the redundancy features.

Quadruple Rack-to-Rack Redundancy

For maximum availability, the ProSafe-PLC “Quadruple” 1oo2D architecture (Figure 4.5) features a parallel combination of Guarded Outputs, thus providing 4 switches for every output. Should the on-line diagnostics detect a failure in one system (input/ processor/output), the other system automatically assumes control and the system remains available.

ProSafe-PLC also offers the option of physically separating redundant systems into separate cabinets. This is called “Rack-to-Rack Redundancy” or “Node-to-Node redundancy”. This minimises the system’s susceptibility to common-cause effects, such as cabinet temperature or cabinet damage.

Power Supply Redundancy

System power (24 Vdc) can be supplied by up to three separate sources. All ProSafe-PLC modules monitor and are connected to and this triplicate power bus.

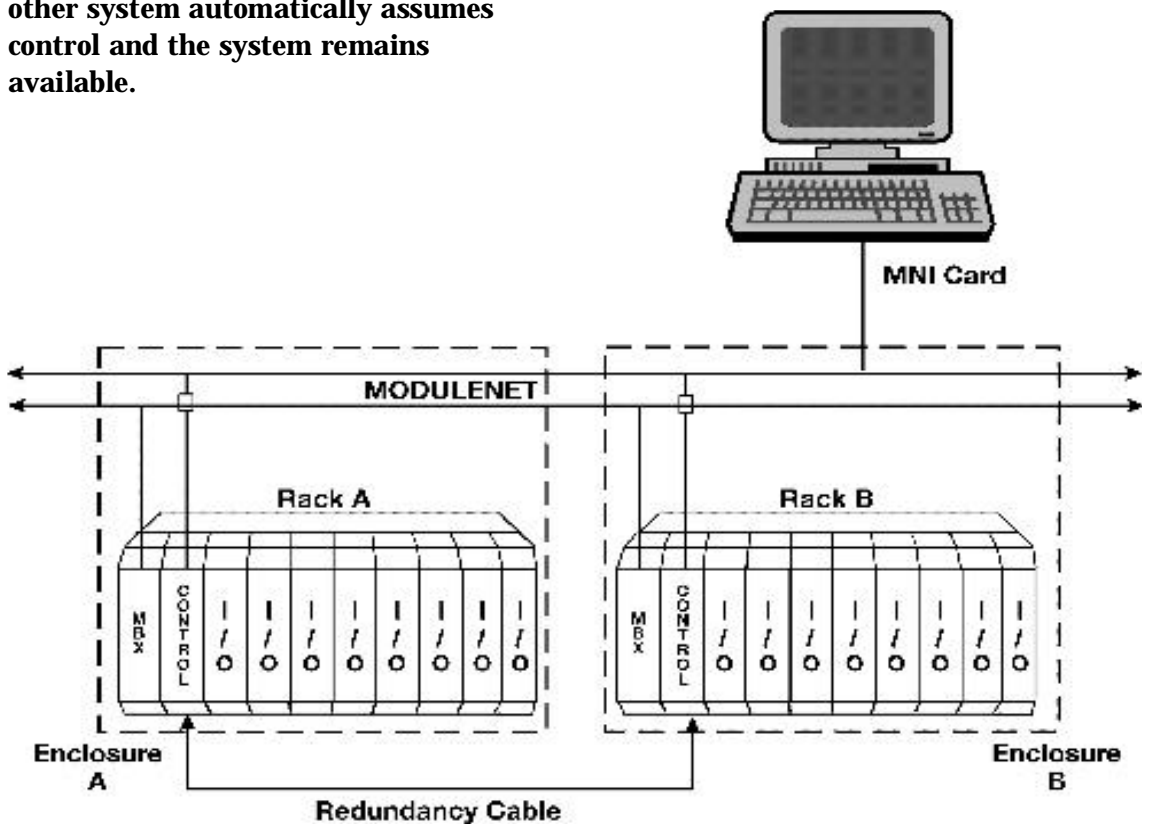


Figure 4.5 ProSafe-PLC “Quadruple” 1oo2D architecture

Areas of application

The ProSafe-PLC system suits all Safety and high availability applications

Because of the flexible system architecture the ProSafe-PLC can be configured to fit a variety of requirements for Safety Integrity

Levels and availability. Figure 4.6 shows the Safety Integrity Levels (SIL's) by which the systems are rated. The ProSafe-PLC covers SIL 1 through 3 and TÜV AK1-6 classification.

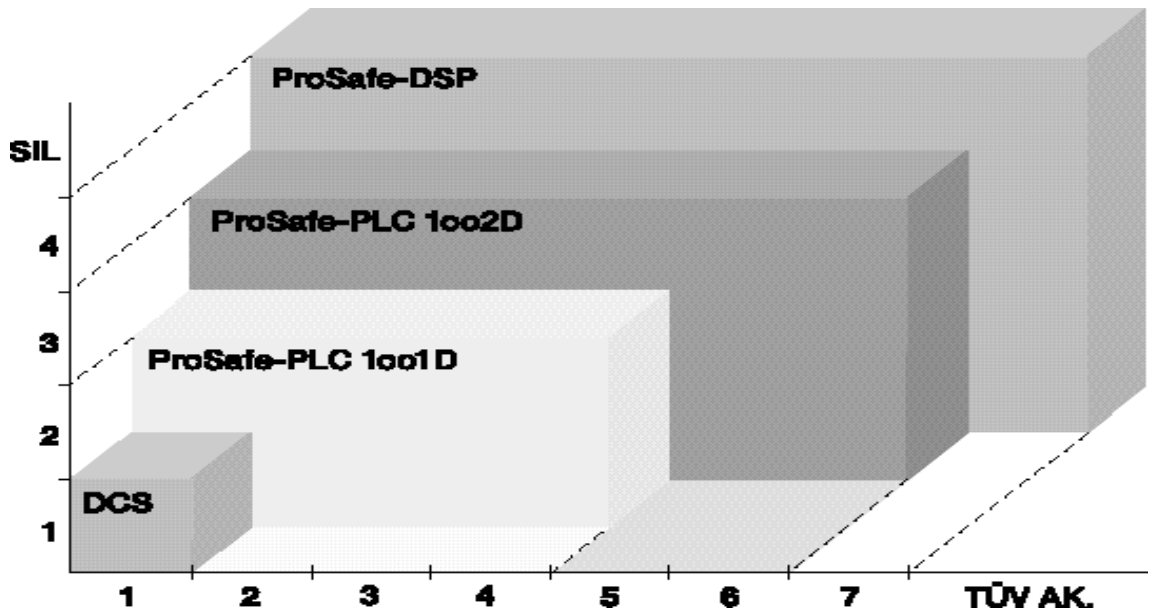


Figure 4.6 The coverage of Safety classification by ProSafe-PLC and ProSafe-DSP systems.

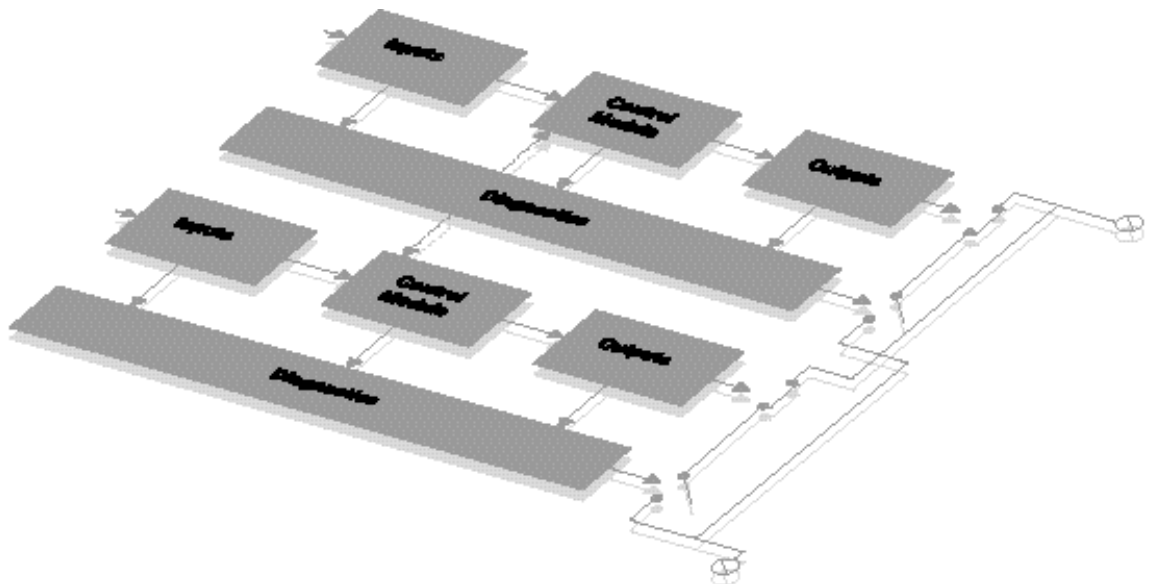
Note: The SIL levels are determined by calculation and include the field devices, based on the IEC 61508/61511 standard. The TÜV-AK classes are a qualitative assessment considering only the Safety Instrumented System, based on DIN19250V.

ProSafe-PLC in high availability applications

In order to create full fault-tolerance, the basic 1001D structure is used in redundancy in the ProSafe-PLC, 1002D Quadruple Channel architecture. At the detection of a first critical failure, the system goes in the 1001D

mode and there is no shutdown. An on-line repair can be executed to restore the fault tolerant 1002D structure.

Full redundancy in 1002D quadruple channel architecture creates complete fault-tolerance. At the same time the system Safety level increases, because each diagnostic protection circuits is capable, upon detection of a failure, to de-energise the associated output circuit. In addition, upon failure of one diagnostic protection circuit, the remaining diagnostic protection circuit will de-energise the redundant output circuit associated with the failing



11 Figure 4.7 1002D Configuration complete redundant system for TÜV5/6 and SIL3 applications.

protection circuit. In this way, a process trip is avoided, while an on-line repair can restore the original healthy situation. The 1002D ProSafe-PLC systems are located in completely separate units or racks; this greatly enhances the common-cause strength. Should the on-line diagnostics detect a critical failure in one system branch, the other system automatically assumes control and the process remains in operation.

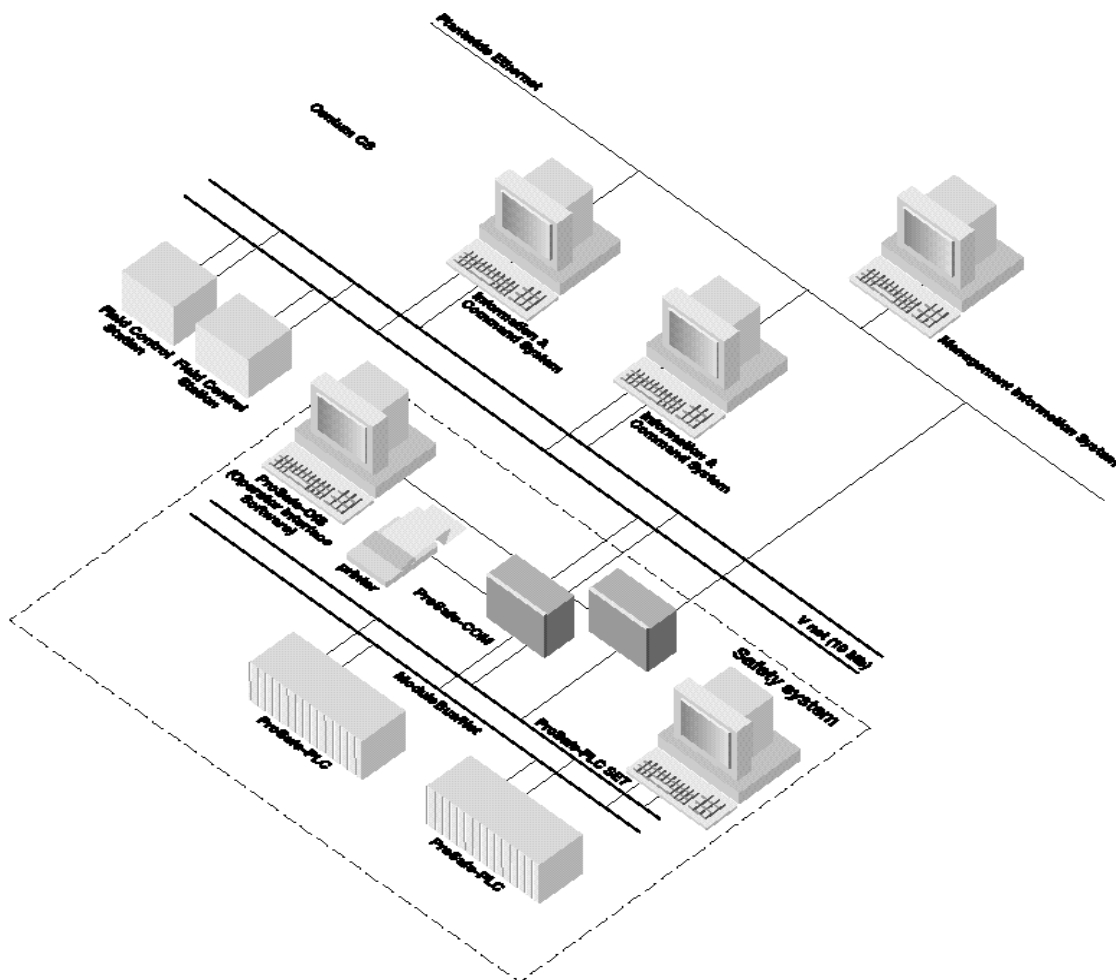
This ProSafe-PLC 1002D structure minimises the amount of hardware required, while providing a parallel combination of Guarded Outputs. This 1002D configuration, as defined by IEC65A/61508-2 and ISA SP84.01, allows the connection of redundant sensors and actuators in a very cost-effective way, without additional hardware.

Communication capabilities & SER

System integration with process control systems

The ProSafe-PLC system operates in harmony with, but independently from the process control system. Interfaces communicate all relevant information, however ProSafe-PLC offers protection through the ability to identify variables, which may not to be overwritten by any type of external communication. In this way the systems interfaces will be “reverse-fault immune” and the autonomous Safety functionality remains untouched.

An open communication structure with other systems is created by the support of commonly used industrial communication standards, such as Ethernet, BIP, Dynamic Data Exchange (DDE) and ModBus



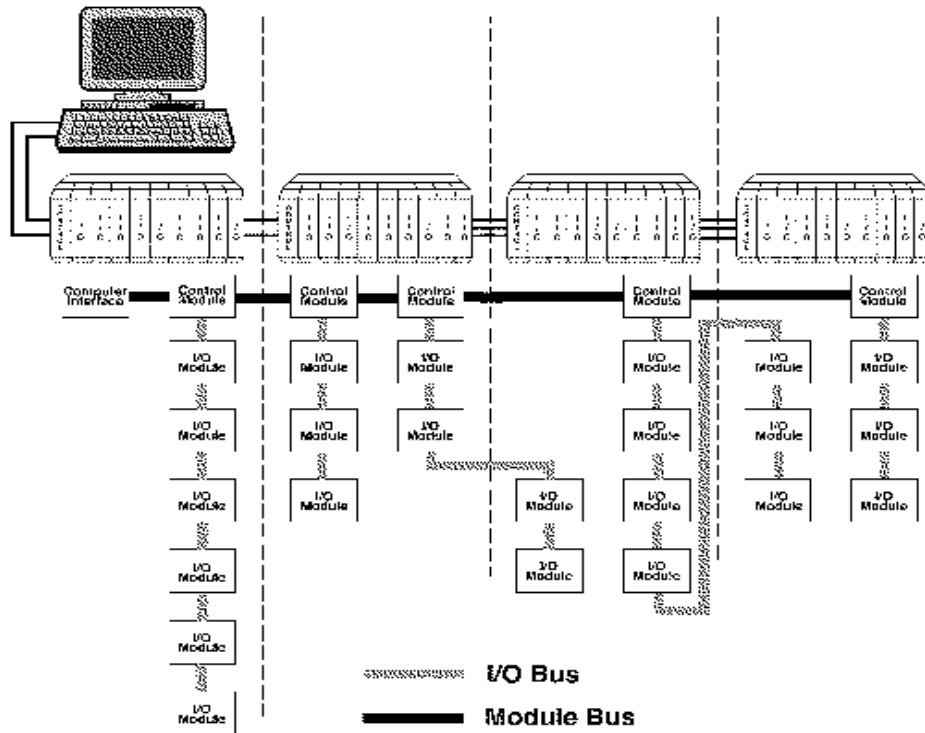


Figure 4.9 MODULE-BUS and I/O-BUS structure

ProSafe-PLC communication capabilities

The ProSafe-PLC system has two communication buses that are used to share process and system information between modules: MODULE-BUS (M-BUS) and the I/O-BUS. The M-BUS is used for communication between control modules and communications modules. I/O modules and their master control module use the I/O-BUS. These redundant communication busses provide high speed and secure communication for all functions within one Safety system, or local area system. A local M-BUS supports up to 32 modules and can be expanded from a local bus into a multiple area network via the M-BUS Expander module (MBX). This module provides communication over a network called MODULNET (M-NET). ProSafe-PLC control modules provide a secure area for reading and writing of process variables to M-BUS. A 'firewall' protection system prevents M-BUS from affecting the Safety critical functions.

The I/O-BUS provides the control module with secure access to I/O points, which are terminated at I/O modules. The I/O-BUS is a redundant bus that has a data transmission rate of 1 mbps. One control module (the master) and 39 slave- I/O modules can be distributed locally or remotely on an I/O-BUS. The remote capabilities include using extension cables and fibre optic repeaters. The fibre optic option supports star configurations for the most cost-effective distribution of I/O modules.

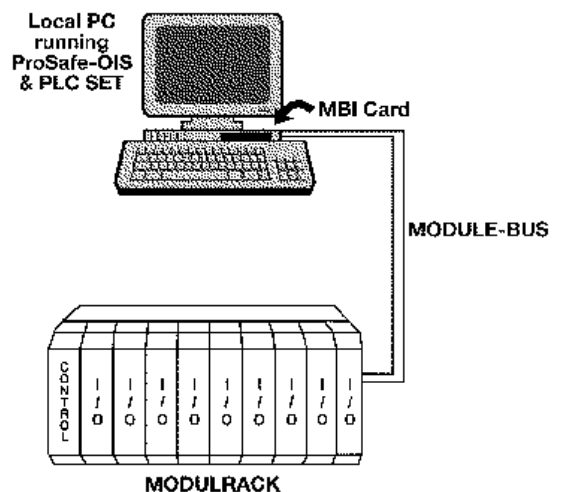


Figure 4.10 Safety system with remote PC workstation using MBI card

Example systems

The modularity of ProSafe-PLC's and the flexible networking allows the creation of various system architectures. In Figure 4.5 Unit Safety System with Remote PC via Network is shown.

Operator Interface System

A standard personal computer can be used as the workstation. It can communicate with a rack of modules in one of two ways: via a M-BUS Interface (MBI) card or a standard network card. As shown in figure 4.10, a MBI card plugs into an expansion slot of a PC and provides a M-BUS connection directly to the module rack. This architecture has the added benefit of a redundant, secure highway between the control module and PC. For a connection to a TCP/IP network, the PC includes the appropriate card in an expansion slot. This arrangement allows a variety of cabling options to be used and opens the system to support a connection to an existing plant-wide network.

ProSafe-PLC network architecture specification:

MODULE-BUS (M-BUS)	Max. length	60 ft (18 m)
	Module rack capacity	4
	Module capacity	32
	Electrical specification	Un-modulated IEEE 802.4
	Transmission rate	5 mbps
MBI Network (M-BUS between PC's)	Type	Redundant
	Max. length	550 ft. (167 m) less the length M-BUS across racks
	Number of PC's	4
	Electrical specification	Un-modulated IEEE 802.4
	Type	Redundant
I/O-BUS	Max. lengths	300 ft. (91 m), 1500 ft. (457 m) extended and 7500 ft. (2286 m) fibre optic segments to allow star configurations.
	Max. rack capacity	4
	Module capacity	39
	Electrical specification	RS485
	Transmission rate	1 mbps
	Type	Redundant
	Workstation	Network
MODULNET (M-NET)	Type	Ethernet, Token Ring, etc.
	Max. length	Up to 3000 ft (909 m) without repeaters.
	Electrical specification	IEEE 802.4
	Transmission rate	5 mbps
	Type	Redundant carrier band
	Protocol	TCP/IP
	Transmission rate	Ethernet: 10 mbps;Token Ring: 16 or 4 mbps, depending on cable selection.

ProSafe-COM and Sequence of Event Recording (SER)

It is a necessity for safeguarding systems to monitor start-up and shutdown procedures in real system-time and record these events for later analysis. The Sequence of Event Recorder system provides just that “black box” function, which makes it possible to retrace and analyse the events associated with a particular process situation. As a consequence it is necessary for the Safety system to interface with other process data handling systems.

Status and event data can be communicated with other data handling systems, such as the ProSafe Operator Interface (OIS) and a Distributed Control System (DCS).

The Sequence of Event Recorder (SER) controls and manages data collected by the Critical Discrete Module (CDM), an I/O module capable of high speed event gathering for discrete inputs. If two observed points change status 1 millisecond or greater apart, the CDM will detect that two separate events have occurred, logging them with distinct times. This accuracy level provides the ability to detect what happened, what followed, and the context in which it all occurred. The CDM then sends the information to the Event Recorder in the Critical Control Module (CCM) and the Event Recorder stores the information in a user-specified array, which includes a user-defined description for each string. The array may then be read from the CCM and placed in a text file in the Operator Interface or PC.

5 Specifications

The technique of hardware packaging for the ProSafe-PLC simplifies system installation and long-term maintenance. All hardware for the system's control, I/O, and communication functions are packaged using a single methodology, that includes built-in features for high reliability, while providing the flexibility necessary to meet a variety of needs.

The ProSafe-PLC is based on a modular approach, that allows a unique application to be accommodated in a cost effective manner, by simply selecting and combining individual modules, that are each dedicated to a particular function (e.g. control, I/O, communication).

The ProSafe-PLC modules help the system achieve an unparalleled level of reliability and Safety by providing high strength against physical stresses in a harsh Industrial environment. These stresses include heat, humidity and chemicals, shock and vibration, electrical surge and discharge. Also including operational and maintenance errors.

Modulrack

The ProSafe-PLC modules plug into three standard module rack assemblies: the ten slots MODULRACK, the six slots SIXRACK and the single slot UNIRACK. All racks enable front access for interconnecting cabling and wiring. Any module can be plugged into any slot of the MODULRACK as shown in figure 5.1 or SIXRACK. The UNIRACK is for one I/O module only. Any module can be plugged into any slot of a module rack. After a slot is selected for a specific module type, it can be keyed with holes and fitting plugs to accept only this module type. The modules can be removed and inserted with a module rack fully powered to allow continued on-line operation, while servicing individual modules.

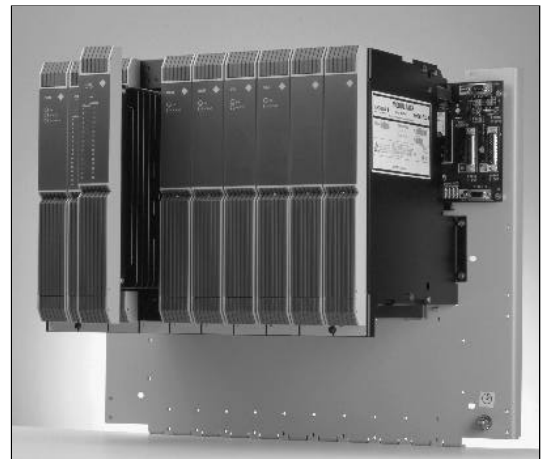


Figure 5.1 Modulrack components

Backplane

Both MODULRACK and SIXRACK can accommodate I/O and communication modules on its backplane. The backplane further provides for three separate power supply connections, the redundant M-BUS and redundant I/O-BUS connections. The I/O-BUS terminator plugs are supplied at each slot to accommodate multiple I/O-BUS architectures. The SIXRACK accommodate Marshalling Termination Assemblies and Rail Termination Assemblies and can be panel mounted or mounted in standard 19" cabinets.

Unirack

The UNIRACK houses a single I/O module. Its backplane provides for 2 two separate power supply connections and redundant I/O-BUS connections. The UNIRACKS accommodate Marshalling Termination Assemblies and Rail Termination Assemblies and can be panel or through panel mounted.

Field termination options for I/O modules

There are different methods of field termination to fit particular applications. These methods are local termination wiring, marshalled termination wiring with a finished cable system and marshalled termination wiring with an unfinished cable end.

Local termination wiring

For this application, the Local Termination Strip is used. This assembly locates terminal blocks directly below a module rack, allowing field wiring to be located local to the module with which it is associated. The terminal blocks are mounted on the Local Termination Panel, which is an extension of the module rack mounting panel that is designed specifically for local termination applications. Extended Transition Boards are required for control and communications module connections, when utilising a local termination.

Marshalled termination wiring

In the marshalled termination-wiring configuration, field wiring is located in an enclosure separate from the I/O module(s). The extension from the module(s) is accomplished via a Marshalled I/O Cable Assembly. This assembly, which comes in several different lengths, is a multiconductor cable with a P2 receptacle, which attaches to the module rack backplane on one end and a finished or unfinished termination end.

The Power Supply Rack, Powerack

This power supply rack (Figure 5.2) is capable of distributing 24 Vdc operating power to ProSafe-PLC modules, through the backplane of a MODULRACK and can typically support four MODULRACKS. The POWERACK consists of a power supply assembly mounted to an "L" bracket that is attached to a rack mount panel. The panel can be mounted to standard 19" cabinet rails. A termination board mounted adjacent to the power supply facilitates AC and DC power connections.

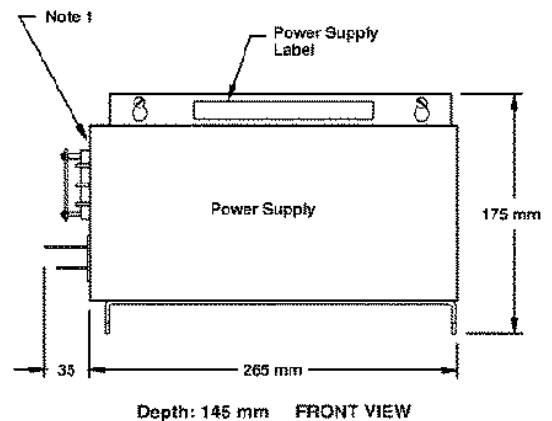


Figure 5.2 Powerack

Protection features: Over Current, Over Voltage, Over temperature, Input under Voltage (Vac). In case of over temperature and input under Voltage to the output is re-established when the condition is back in the specified range. The LED indicators supports the several power status's, known as: 24 Vdc Output OK, Overvoltage, Over-temperature Shutdown, DC Output Voltage is not within specifications.

Specifications:

Model 39PSR4ANAN

Output Voltage 24 VDC

Input Voltage 115/230 VAC, frequency 47- 63 HZ

**Max ratings 25A (525W) @40°C
20A (420W) @60°C**

The Critical Control Module (CCM)

The CCM performs logic solving and advanced control functions, while interfacing with other ProSafe-PLC modules. The CCM (see figure 5.3) also exchanges data with other control and communication modules via the M-BUS.

The CCM:

- Has a “Safety critical rating” by TÜV for AK 1-6 applications;
- Continuously runs extensive diagnostics to quickly detect potentially dangerous failures;
- Provides diagnostics analysed by failure modes and effects analysis (FMEA) and verified by full fault injection testing for easy problem solving;
- Utilises the high strength ProSafe-PLC module packaging for uninterrupted service;
- Eases process Safety management documentation control by maintaining a master graphical configuration within the control module;
- Facilitates efficient and intuitive protection strategy design by allowing standard configuration languages to be mixed within a single module;



- Supports redundant (1oo2D) architecture for SIL3 Safety and highest availability;
- Reduces servicing time by allowing the module to be inserted or removed while powered, without disturbing system wiring;
- Reduces servicing time by supporting on-line replacement of the redundant module, with automatic reconfiguration;
- Complies with the European Community Electromagnetic Compatibility (CE) directive.

Redundancy

In a redundant architecture, inter processor communications necessitate a redundancy cable between CCM's. The CCM control modules in a redundant pair maintain dedicated communications across this redundancy cable that connects to the transition board of each module. Through this cable, the control modules are in constant communication and maintain identical configurations and data values.

The CCM facilitates flexible redundancy options to maximise Safety and availability.

In a module-to-module redundancy structure, a CCM has a redundant twin module located in the adjacent module rack slot and the two CCM's share a common set of I/O modules. This arrangement provides higher availability of the control function in an economical configuration and allows inter processor comparison of critical data and calculation results for increased Safety.

Rack-to-rack redundancy in 1oo2D architecture completely duplicates a CCM and its I/O subsystem, providing high availability. Both the redundant CCM's execute the protection logic simultaneously and compare results and I/O scan data.

Diagnostics

The CCM is Safety critical certified. As such, no known dangerous undetected failures are permitted. And any module malfunction will perform automatic switchover between the 'calculate' and 'verify mode' of both units in a fully redundant (1oo2D) ProSafe-PLC system. If a potential dangerous fault is detected an automatic shutdown is performed of one (redundant) channel, module, or system (for fail-safe operation). However, the redundant I/O modules can avoid a process trip.

Microprocessor diagnostics

The main microprocessor in the CCM is on-line tested, to assure that potentially dangerous failures are detected. In addition two watchdog timers external to the microprocessor monitor execution timing. A series of calculations performed by the diverse microprocessors in I/O modules are compared with identical calculations made by the main processor. Self-checked program execution is provided in the microprocessor. These extra reference diagnostic techniques will detect both transient and permanent failures in the microprocessor circuitry.

Memory diagnostics

The ROM memory in the CCM is on-line tested, by calculating CRC32 test patterns on critical data and program areas and comparing to stored values. The RAM memory within the CCM is internally duplicated. The redundant data is compared by hardware on each read cycle.

This secure memory strategy detects transient and permanent failures.

Communication diagnostics

Bus communications failures for buses directly employed to the PLC, like the M-BUS and I/O-BUS, are detected by a number of diagnostic techniques. As there are CRC32 message integrity checking, Message type and format checking, address verification, time-out checking and sequence verification. In

redundant CCM architectures these message parameters are compared, to assure that all communications are accurately received.

The I/O-BUS is a Safety-critical communication bus. It is Isolated, Single-fault tolerant, constantly switched between channel A or B and it is able to tolerate the failure of an I/O module.

Common circuit diagnostics

The CCM receives power from the power buses in a module rack. Outputs from the on-board power system are monitored for over-voltage and under-voltage failures. Battery voltage is periodically sampled under load to verify the battery status. Redundancy and Safety control signals are on-line checked for invalid bit patterns. These signals are also compared against the same information and diversely sent through communication buses.

Software diagnostics

Special diagnostic techniques are used to detect systematic failures, by comparing interim results with predefined patterns. The CCM on-line software employs program flow control, a technique where the execution of each piece of critical software is measured. The execution time and execution sequence must agree with predefined patterns. CCM software also uses data integrity verification at key points in the execution. This technique requires that critical variables be checked to verify that they are within permitted ranges. Variables within the CCM are data-typed. Data type consistency checking is done for calculations. The CCM maintains a log of current and historical errors that can be reviewed in detail using the Diagnostic Logger Utility or ProSafe-PLC System Engineering Tool (SET) configuration software.

The LED's support local trouble shooting without an operator interface. The module includes three LED's, which indicate the several module states.

Configuration

The CCM is configured using the ProSafe-PLC SET. This System Engineering Tool allows a control strategy to be defined using any mix of 4 languages, which are based on the IEC specification for programmable controllers IEC 1131-3. These languages are function blocks, ladder logic, sequential function charts, and structured text. Note that only ladder logic and function blocks have been TÜV certified for Safety related parts of the SIS application, The other languages may be used for communication, alarming, etc. A CCM's configuration can be created off-line and transferred to the module, or a configuration can be created within an on-line, during the initial design phase. On-line configuration is possible because all of the information needed to configure a CCM is stored in

its database, thus eliminating the need to have a disk-based master database for viewing or editing a configuration. The CCM's security can be programmed, so no unauthorised or inadvertent changes are made to a configuration. Several different access restriction levels are available. When this security feature is activated, a configuration can be opened in "read " mode only, ensuring that no further changes are made to the control strategy. The CCM also includes features to simplify start-up, should operation be disrupted. A configuration is battery-backed, so that the configuration for a CCM and its I/O is maintained also when power is lost. Also the real-time clock continues to run, so that warm start and cold start states can be determined and acted upon once power is restored.

Termination

The CCM's termination strip facilitates the connection to a redundant CCM. The CCM termination strip can be short or long, depending on the choice made for termination of the I/O.

CCM Specifications:

Supply voltage range	24 Vdc, ±5%
Maximum supply current	0.9 A
Immunity, electrostatic discharge (ESD)	IEC 801-2, Level 4, Contact discharge: 8 kV Air discharge: 15 kV air
Immunity, radiated electromagnetic interference (RFI)	IEC 801-3 10 V/m; 30 KHz to 1000 MHz
Immunity, power lines & I/O, fast transients	IEC 801-4, Level 3 I/O: 2 kV
Heat dissipation (typical)	16 Watt or 53 BTU/hour
Operating temperature	-25 to 60°C (32 to 140°F)
Operating humidity	5 to 95 %, non-condensing
Storage temperature	-25 to 85°C (-4 to 185°F)
Agency approvals	TÜV approved AK1-6; CE conformity; CSA and FM approval pending for Class I, Div.2, Group A, B, C, & D; ABS approved

The Critical Discrete Module (CDM)

This CDM (see figure 5.4) is an intelligent microprocessor based, configurable module that interfaces discrete DC sensors and actuators with the I/O-BUS.

The CDM:

- Provides fail safe control of outputs with unique Guarded Outputs;
- Has a “Safety critical rating” for TÜV rated AK 1-6 applications;
- Detects shorts and open loops in field wiring with optional Safety Rated Switch Adapter (SRSA)
- Includes an electronic-fuse feature, to protect individual output channels against short circuit and overload conditions, caused by field wiring problems;
- Supports Sequence of Events Recording (SER) functions, by sensing and recording events at 1 ms resolution;
- Improves error checking with a per channel built-in output monitor, that eliminates the need to wire and program additional input channels for error detection;
- Includes dynamic threshold detection circuits to diagnose failed input channels;
- Supports redundant architecture for highest level of availability;
- Supports low and high temperature operation (-25 to 60C), with internal temperature diagnostics, that detect if the module is operating outside of these limits;
- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing system wiring. Isolates field faults by electrically isolating all I/O channels from the backplane and ground;
- Complies with the European Community Electromagnetic Compatibility (CE) directive.

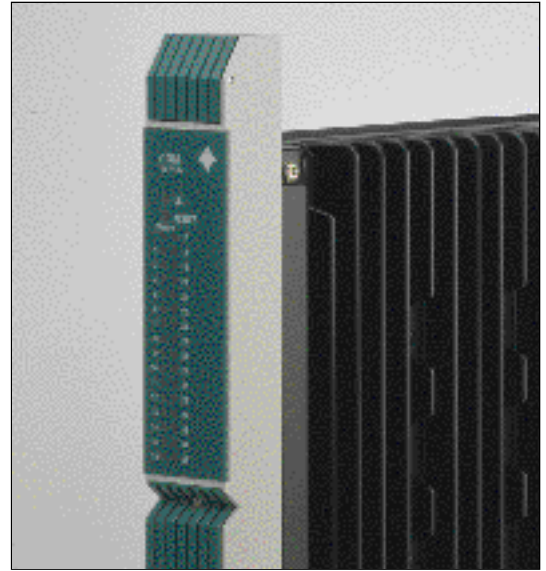


Figure 5.4 CDM-module

Channel types

The CDM provides 32 channels, each of which can be configured to be a discrete input, a discrete output, or a discrete pulse output. The configurable channels reduce hardware costs and spare parts requirements, by allowing one module to accommodate several I/O requirements.

Intelligent Fuse

The ProSafe-PLC Intelligent Fuse feature contains an over-current detection circuit that switches an individual output off, before damage can occur. It protects the CDM output channels against over-current conditions, caused by field wiring and field device problems. In each channel the diagnostics report the “blown” fuse channel and permit clearing the blown fuse from an operator interface. In addition, a push button located on the module allows local resetting of blown fuses. The Intelligent Fuse feature provides equivalent protection as hard fuses; permits remote on-line “repair,” and eliminates the need for stocking spare fuses.

Guarded Outputs

The CDM uses a combination of extensive on-line diagnostics and an internal “diagnostic cut-off relay” to automatically protect against energised output failures. If any dangerous failure is detected, the relay contacts are opened. This action de-energises the output, ensuring the output fails in a safe manner. Using this technique, CDM Guarded Outputs ensure that outputs fail safe, even in the presence of faults.

Diagnostics

The CDM is Safety critical certified the same as the CCM. The goals of the diagnostics are to:

Notify the appropriate personnel of a module malfunction or wiring error, perform automatic switchover in a fully redundant 1oo2D mode of a ProSafe-PLC system and performing of automatic shutdown of a channel or module, if a dangerous fault is detected (for fail-safe operation). There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules and those that cover individual channels.

Overall module performance diagnostics

Diagnostics for overall module performance include failure detection in the communications, processor, and common circuits. These diagnostics include:

- Power supply diagnostics monitor the three 24 Vdc power input busses for under-voltage and the on-board isolated power supply for voltages tolerances;
- Over temperature diagnostics check the module for over-temperature conditions via an on-line monitor;
- Memory diagnostics running a complete IEEE published test on RAM memory at module start-up.

Input & Output circuit diagnostics

Full self-diagnostic capability including field wiring faults, when used with the SRSA circuit. Full diagnostic coverage is obtained by a combination of test pulses that superimpose bipolar dynamic signals onto the input.

A comparator circuit has a variable analogue threshold that allows the CDM processor to test the voltage at the input terminal. This combination of dynamic test pulses and analogue monitoring allows detection of electronic component failures and field wiring faults, such as open circuits, short circuits and even short circuit failures between channels.

The circuit is optimised for normally energised output usage and provides full self-diagnostic capability.

Diagnostics use a combination of pulse testing, voltage & current measurement, and constant switching between CCM's in the 1oo2D architecture.

Momentary pulse-off testing provides a dynamic signal that allows detection of open circuit, short circuit, and diagnostic circuit failures.

The LED's support local troubleshooting without an operator interface. The module includes three LED's, which indicate the several module states.

Termination

The field I/O can be terminated locally or remotely according to user needs and preferences.

The CDM also supports direct, plug-in connection to 32 SPDT relays. This application uses a Relay Marshalled Termination Assembly.

CDM Specifications:

Module	Backplane operating voltage	Voltage 24 Vdc, -10%, +20%	
	Backplane current	0.233 Amps. maximum	
	Electrical isolation	Dielectric tested with 2640 Vac	
	Operating (I/O) voltage	24 Vdc, ±5%	
	I/O Channel loop resistance	< 25 Ohm	
	Heat dissipation	27 Watts max., or 92 BTU/hour	
	Operating temperature	-25 to 60°C (-13 to 140°F)	
	Operating humidity	5 to 95%, non-condensing	
	Storage temperature	-25 to 85°C (-13 to 185°F)	
	Storage humidity	0 to 100%, condensing	
	Agency approvals	TÜV AK1-6; CE conformity; CSA and FM pending for Class I, Div. 2, Groups A, B, C, & D; ABS approved.	
	Inputs	Input delay filter time	OFF-ON: 41 ms, ON-OFF: 25 ms
		Input wetting current	9.96 mA @ 24 Vdc
“ON” state voltage range		15.51 V to 30.0 Vdc	
“OFF” state voltage range		-0.5 to 14.02 Vdc	
Maximum “OFF” state current		5.76 mA	
Outputs	Output current channel	0.6 amps max.	
	Total output current per module	12.8 amps max. at 30°C (86°F) or 4.0 amps at 60°C (140°F)	
	Intelligent Fuse trip	1.53 amps	
	Surge current	2.0 amps max. for 10 msec	

The Standard Analogue Module (SAM)

The SAM (see figure 5.5) is an intelligent microprocessor based, configurable module that interfaces both analogue and discrete I/O signals to the I/O-BUS. The SAM provides a low-cost and high capacity module for standard I/O types.

The SAM:

- Has software-configurable channels functions: analogue input, analogue output, discrete input, or discrete output;
- Provides fail-safe control of outputs with unique Guarded Outputs;
- Provides diagnostics analysed by failure modes & effects analysis (FMEA) and verified by fault injection testing for easy problem resolution;
- Includes current limiting to protect individual channels against short circuit and overload conditions, caused by field wiring problems;
- Supports a redundant architecture for high availability;
- Simplifies maintenance by software configurable channels, that eliminate the need for DIP switches or jumpers;
- Reduces servicing time by allowing the module to be inserted or removed, while powered without disturbing field wiring;
- Isolates field faults by electrically isolating all I/O channels from the backplane and ground;
- Complies with the European Community Electromagnetic Compatibility (CE) directive.

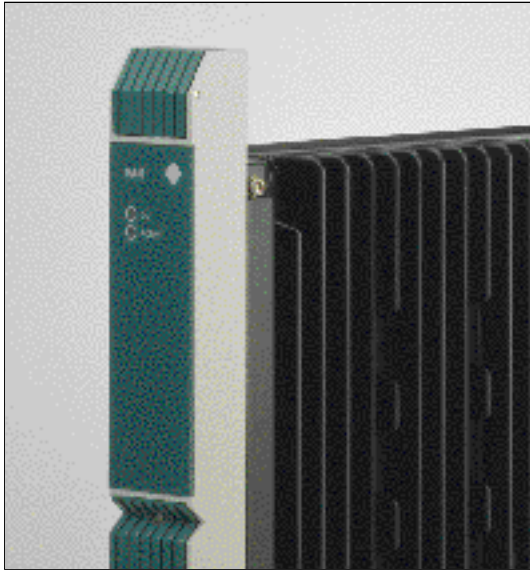


Figure 5.5 SAM-module

Channel types

The SAM provides 32 channels, each of which can be configured to be a two-wire transmitter analogue input (4-20 mA), an analogue output (4-20 mA or 0-20 mA), a discrete input, or discrete output. The configurable channels drastically reduce hardware cost and spare parts requirements, by allowing one module to accommodate input as well as output requirements.

Guarded Outputs

The SAM uses a combination of extensive on-line diagnostics and an internal “diagnostic cut-off switch” to automatically protect against energised output failures. If a potential dangerous failure is detected, the switches are opened. This action de-energises the output, ensuring the output fails in a safe manner. Using this technique, SAM Guarded Outputs ensure that outputs are fail-safe, even in the presence of faults.

Diagnostics

The SAM is designed to provide years of trouble free service. However, in the event of unexpected operation, the SAM is equipped with extensive self-diagnostics verified by full FMEA and fault injection testing. The goals of these diagnostics are to:

- Notify the appropriate personnel of a module malfunction or wiring error;
- Perform automatic switch-over in a fully redundant (1oo2D) ProSafe-PLC system;
- Perform automatic shutdown of a channel or a module if a dangerous fault is detected;
- The control module and the SAM maintain a log of current and historical errors, that can be reviewed using the Diagnostic Logger Utility or the ProSafe-PLC System Engineering Tool (SET) configuration software. Implementations of the diagnostics are monitoring the overall module performance, which are common to all I/O modules, and others cover individual input channels.

Overall module performance diagnostics

Diagnostics for overall module performance include failure detection in the communications, processor, and common circuits such as:

- Power supply diagnostics, that monitor the three 24 Vdc power input busses for under-voltage and the on-board isolated power supply for voltages tolerances;
- Over-temperature diagnostics, that check the module via an on-line detector;
- Memory diagnostics run a complete IEEE published test on RAM memory at module start-up;
- Detect RAM failure modes in the optimal amount of time, and verify critical RAM data and ROM memory on-line, with cyclical redundancy checking (CRC);
- Communication diagnostics verify I/O-BUS communications for each message via CRC;
- Redundancy diagnostics monitor logic signals for valid combinations, compare redundancy status information from the I/O-BUS with logical signals on the module, reporting any discrepancies.

- **Watchdog timer diagnostics detect processor operation failures via external and CPU hardware timers and monitor I/O-BUS and scanning operation via additional timers;**
- **CPU diagnostics run manufacturer-supplied tests on CPU components, where results from the instruction sequences must match predetermined values;**
- **Software diagnostics verify program flow control to ensure that software functions execute in proper sequence and time, perform data integrity checks, and compare data to predetermined ranges;**
- **Addressing diagnostics compare module slot/rack addresses against their addresses at start-up.**

Input & Output circuit diagnostics

To detect failures in the analogue to digital (A/D) converter, input filters, and multiplexer circuitry, a series of precision reference voltages are scanned on-line and the readings are compared with predetermined values. Linearity and calibration are also monitored on-line, to detect failures in the A/D and its amplifier circuitry. Open and short-circuit conditions are monitored, as well.

Digital to analogue (D/A) circuitry is on-line tested by full scale ramping with direct A/D read back, while process outputs are held with a sample/hold circuit. In addition, full analogue output loops are monitored with constant A/D read back. These read back values are then compared with expected results. The module includes two LED's that indicate various module & communication states.

Configuration

Like all ProSafe-PLC I/O modules, the SAM is configured using the ProSafe-PLC SET software. The configuration is loaded via the CCM into the module's memory, and a copy of the configuration is stored in the associated non-volatile memory. This approach allows the module to be removed and replaced on-line without the need for reconfiguration. During configuration, ProSafe-PLC SET is used to assign a type to each channel and related parameters, which vary according to channel type.

Analogue Input channel parameters:

- **Minimum and maximum scale;**
- **Bias (in Engineering Units);**
- **Engineering units;**
- **Open-circuit test;**
- **Digital filter time constant;**
- **Shutdown channel.**

Discrete Output channel parameters:

The I/O-BUS fault state defines the state to which the channel changes, if communication with I/O-BUS is lost:

- **Guarded Output;**
- **Read back;**
- **Shutdown channel.**

Termination

Local terminations reside directly below the SAM. Marshalled Termination Assemblies or Rail Termination Assemblies provide for terminations up to 100 feet (30.5 m) away from the SAM.

SAM Specifications:

Module	Module supply voltage	24 Vdc, ±10%
	Supply current	1.0 amps
	Electrical isolation	Tested at 2640 Vac
	Maximum input	±30 Vdc
	Heat dissipation	12,9 Watt or 44 BTU / hour
	Operating temperature	0 to 60°C (32 to 140°F)
	Operating humidity	5 to 95 %, non-condensing
	Storage temperature	-20 to 85°C (-4 to 185°F)
	Storage humidity	0 to 100%, condensing
	Linearity	0.035% of span (1 LSB)
	Ambient temp. effect	#.001% of span per 1_C (100 ppm/°C)
	Min. module scan time	50 msec. (with all channels configured)
	Agency approvals	TÜV AK 1-6; CE conformity; ABS approved; CSA and FM Class I, Div. 2, Gr.A, B, C, & D
	Analogue Inputs	Input range
Calibration range (span)		4 to 20 mA
Resolution		12 bits
Accuracy		0.1% of span at 25°C (77°F)
Repeatability		±0.05% of span
Discrete Inputs	Input filter delay time	9 msec.
	Input current	10 mA
Discrete Outputs	Max. output current	23.6 mA
	Min. "ON" state voltage	20.2 V

Enhanced Analog Module (EAM)

The Enhanced Analog Module (EAM) is a microprocessor-based, configurable module that can interface both analog and discrete I/O signals with the I/O-BUS.

The EAM features:

- Minimal hardware costs with 16 software-configurable channels (analog input, analog output, frequency input, totalizer input, discrete input, or discrete output);
- Improved accuracy with an individual sigma-delta A/D converter per channel and selectable resolution on analog inputs (13, 14, 15, or 16 bits) and frequency inputs (10, 12, 14, or 16 bits);
- Fail-safe control of outputs by unique Guarded Outputs;
- Enables faster response to field problems by providing detection of open-circuit, short-circuit, overrange or underrange conditions;
- Includes current limiting to protect individual output channels against short circuit and overload conditions caused by field wiring problems;
- Improves error-checking with a per channel built-in output monitor that eliminates the need to wire and program additional input channels for error detection;
- Supports redundant architecture for high availability;
- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing field wiring;
- Isolates field faults by electrically isolating all I/O channels from the backplane, ground, and other channels;

- Complies with the European Union's Electromagnetic Compatibility (CE) directive.

Channel Types

The EAM provides 16 channels, each of which can be configured to be an analog input, analog output, frequency input, totalizer input, discrete input, or a discrete output. The EAM has configurable channels that reduce hardware costs and spare parts requirements by allowing one module to accommodate several I/O requirements.

Guarded Outputs

The EAM uses a combination of extensive on-line diagnostics and an internal "diagnostic cut-off switch" to automatically protect against energized output failures. Output energy flows through "dual-switches" to the load. A solid-state switch provides the normal output. A switch controlled by the built-in diagnostics, supplies protection. If any dangerous failure is detected, the switches are opened. This action de-energizes the output, ensuring the output fails in a safe manner. Using this technique, EAM Guarded Outputs ensure outputs fail-safe, even in the presence of faults.

Diagnostics

The EAM is designed to provide years of trouble-free service. However, in the event of unexpected failure, the EAM is equipped with extensive self-diagnostics verified by full FMEA and fault injection testing. The goals of these diagnostics are to:

- Notify the appropriate personnel of a module malfunction or wiring error
- Perform automatic switchover in a fully redundant (1oo2D) ProSafe-PLC system
- Perform automatic shutdown of a channel or module if a dangerous fault is detected.

Any errors detected by these diagnostics are reported to the associated control module. The control module and the EAM maintain a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the PLC SET engineering software. In addition, the LED's indicate various errors.

There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules and those that cover individual I/O channels.

Configuration

Like all ProSafe-PLC I/O modules, the EAM is configured using the PLC SET software. The configuration is loaded into the module memory, and a copy of the configuration is stored in the associated control module's non-volatile memory. This approach to configuration allows the module to be removed and replaced on-line without the need for reconfiguration.

During configuration, PLC SET is used to assign a type to each channel (input, output, or pulse) and relevant parameters, which vary according to the channel types:

- High-Level Analog Input Channel Parameters
- Analog Output Channel Parameters
- Frequency Input Channel Parameters
- Discrete Input Channel Parameters
- Discrete Output Channel Parameters.

Input Discrete Module (IDM)

The Input Discrete Module is an microprocessor-based, configurable module that interfaces discrete 115 or 230 Vac input devices with the I/O-BUS. It has the following features:

- Minimized hardware costs with 32 software-configurable AC input channels;
- Provides extensive diagnostics analyzed by failure modes and effects analysis (FMEA) and verified by fault injection testing for easy problem resolution;
- Provides flexibility in field wiring by isolation of eight groups of four channels each;
- Supports redundant architecture for high availability;
- Supports high temperature operation (0 to 60°C) with diagnostics that detect if the module is operating outside of these limits;
- Simplifies maintenance with software configurable channels that eliminate the need for DIP switches or jumpers;
- Reduces servicing time by allowing the module to be inserted or removed while powered;
- Isolates field faults by electrically isolating channels from the backplane and ground;
- Complies with the European Union's Electromagnetic Compatibility (CE) directive.

Channel types

The IDM supports 32 AC inputs in eight isolated groups of four channels each. This allows AC inputs from different power sources to be connected to the same module. In addition, each channel is electrically isolated from the module's CPU, I/O-BUS and ground.

Diagnostics

The IDM is designed to provide years of trouble-free service. However, in the event of unexpected operation, the IDM is equipped with extensive self-diagnostics verified by full FMEA and fault injection testing.

The goals of these diagnostics are to:

- Notify the appropriate personnel of a module malfunction or wiring error;
- Perform automatic switch-over in a fully redundant (1oo2D) ProSafe-PLC system;
- Perform automatic shutdown of a channel or a module if a dangerous fault is detected.

Any errors detected by the IDM diagnostics are reported to the associated control module. The control module and the IDM maintain a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the PLC SET configuration software. In addition, the module LED's indicate various errors. There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules and those that cover individual input channels.

Overall module performance diagnostics

Diagnostics for overall module performance include failure detection in the communications, processor, and common circuits. The LED's support local troubleshooting without an operator interface. The module includes one LED per channel to indicate its status and two LED's, which indicate the various module status's. These diagnostics include:

- Power supply diagnostics monitor the three 24 Vdc power input busses for under voltage and the onboard isolated power supply for voltages within tolerance;
- Over temperature diagnostics check the module for over temperature conditions via an online monitor;

- **Memory diagnostics** run a complete IEEE published test on RAM memory at module startup, detect RAM failure modes in the optimal amount of time, and verify critical RAM data and ROM memory online with cyclical redundancy checking (CRC);
- **Communication diagnostics** verify I/O-BUS communications for each message via CRC;
- **Redundancy diagnostics** monitor logic signals for valid combinations, compare redundancy status information from the I/O-BUS with logical signals on the module, reporting any discrepancies as errors;
- **Watchdog timer diagnostics** detect processor operation failures via external and CPU hardware timers and monitor I/O-BUS and scanning operation via additional timers;
- **CPU diagnostics** run manufacturer-supplied tests on CPU components, where results from the instruction sequences must match predetermined values;
- **Addressing diagnostics** compare module slot/rack addresses against their addresses at startup.

Input circuit diagnostics

The circuit utilizes redundant optocouplers to provide diagnostic coverage of a faulty input circuit. A fault is reported any time the redundant optocouplers disagree during three microprocessor scans. The reported data is configurable; however the default selection is fail-safe for a deenergize-to-trip operation.

The Voltage Input Module (VIM)

This VIM I/O module (see figure 5.6) is an intelligent microprocessor-based configurable module, which interfaces thermocouple and voltage input signals with the I/O-BUS.

The VIM features:

- **16 software-configurable channels** for thermocouple or voltage input;
- **Calibration and cold junction compensation;**
- **Facilitates fast response to field problems** with a configurable burnout detection feature, up or down scale;
- **Provides protection against short circuits** via individually isolated channels;
- **Supports redundant architecture** for high availability;
- **Reduces servicing time** by allowing the module to be inserted or removed while powered without disturbing field wiring;
- **Isolates field faults** by electrically isolating all input channels from the backplane and ground;
- **Complies with the European Community Electromagnetic Compatibility (CE) directive.**



Figure 5.6 VIM-module

Several standard features allow the VIM to accommodate many input types with simplified configuration and high accuracy, such as:

- Automatic linearization for thermocouple types;
- Cold junction compensation provided for all thermocouple input measurements;
- Autoranging circuitry for thermocouple inputs, eliminating the need to specify a temperature range while maintaining high accuracy;
- Self-calibration feature eliminating the need for field calibration;
- Integral burnout detection to determine if a thermocouple has opened or, if due to ageing, its resistance has increased.

In addition, the VIM has configurable channels that reduce hardware costs and spare parts requirements, by allowing one module to accommodate several input requirements.

Diagnostics

The VIM is equipped with extensive self-diagnostics. The goals of these diagnostics are to:

- Notify the appropriate personnel of a module malfunction or wiring error;
- Perform automatic switch-over in a fully redundant (1oo2D) ProSafe-PLC system;
- Perform automatic shutdown of a channel or a module if a dangerous fault is detected.

Any errors detected by these diagnostics are reported to the associated control module. The control module and the VIM maintain a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the ProSafe-PLC SET.

There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules and those that cover individual input channels. VIM has the same functionality as the SAM for the overall module performance diagnostics and LED indications.

Input circuit diagnostics

Redundant thermal sensors on the termination strip are compared to detect failures. To detect excessive drift failures, duplicate voltage references are also compared, while amplifiers and A/D converter circuits are continually automatically recalibrated on-line. Any component failures that require abnormal calibration correction are also detected. Input source impedance is monitored for up and downscale thermocouple burnout detection and fault detection for other components.

Configuration

Voltage input channel parameters

- Input Range; any range between -10 and 10 Vdc
- Minimum and maximum Scale
- Digital filter time constant
- Engineering units
- Step response time.

Resistance Temperature Module (RTM)

The Resistance Temperature Module is a microprocessor-based configurable module, which interfaces RTD and other resistance input signals with the I/O-BUS and it has the following features:

- Minimal hardware costs with 16 software-configurable channels;
- Simple configuration with integral linearization;
- Provides protection against short circuits via isolation of eight groups of two channels each;
- Facilitates fast response to field problems with field wiring fault detection and overrange/underrange reporting;
- Protects the process with a user-defined fault state for each channel;
- Supports redundant architecture for high availability;

- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing field wiring;
- Isolates field faults by electrically isolating all I/O channels from the backplane and ground;
- Complies with the European Union's Electromagnetic Compatibility (CE) directive.

Channel types

The RTM provides 16 channels, each of which can be configured to be an RTD input or a resistance input (e.g. slidewire, potentiometer). The RTM has configurable channels that reduce hardware costs and spare parts requirements by allowing one module to accommodate several input requirements. The RTM supports the following RTD elements:

- 100 Ohm platinum (US or IEC);
- 200 Ohm platinum (US or IEC);
- 100 Ohm nickel (IEC);
- Linear resistive element (e.g. copper).

Diagnostics

The RTM is equipped with extensive self-diagnostics. The goals of these diagnostics are to:

- Notify the appropriate personnel of a module malfunction or wiring error;
- Perform automatic switchover in a fully redundant ProSafe-PLC (1002D) system;
- Perform automatic shutdown of a channel or module if a dangerous fault is detected.

Any errors detected by these diagnostics are reported to the associated control module. The control module and the RTM maintain a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the PLC SET configuration software. In addition, various errors are indicated by the LED indicators.

There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules and those that cover individual input channels.

Diagnostics for overall module performance include failure detection in the communications, processor, and common circuits. The RTM has LED's to support local troubleshooting without an operator interface.

RTD Input channel parameters

- RTD Type 100 Ohm platinum, 200 Ohm platinum, 100 Ohm nickel, or a linear resistive element;
- Alpha for linear RTD;
- Resistance for linear RTD;
- Bias in engineering units;
- Engineering units (°C, °F, °K, °R);
- Minimum and maximum range;
- Scale to percent;
- Input fault state defines the value to which the channel changes if detected failures occur;
- Digital filter time constant;
- Response time defines the time to reduces periodic noise and improves repeatability and resolution.

Resistance Input channel parameters

- Minimum and maximum range;
- Minimum and maximum scale;
- Engineering units;
- Bias in engineering units;
- Input Fault State defines the value to which the channel changes if detected failures occur;
- Digital filter time constant;
- Step response time.

Output Discrete Module (ODM)

The Output Discrete Module (ODM) is a microprocessor-based configurable module that interfaces discrete AC devices with the I/O-BUS. The ODM has the following features:

- Minimal hardware costs with 32 software-configurable AC output channels;
- Provides fail-safe control of outputs with unique Guarded Outputs;
- Provides a 1.0 amp capacity per output;
- Supports redundant architecture for high availability;
- Improves error-checking with a per channel built-in out-put monitor that eliminates the need to wire and program additional input channels for error detection;
- Simplifies maintenance with software configurable channels that eliminate the need for DIP switches and jumpers;
- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing field wiring;
- Isolates field faults by electrically isolating all I/O channels from the backplane and ground;
- Complies with the European Union's Electromagnetic Compatibility (CE) directive.

Channel types

The ODM minimizes hardware costs by providing 32 channels, each of which supports an AC output. These channels include many features, which facilitate a long, trouble-free life. The ODM has 32 outputs that are isolated in four groups of eight channels each, which allows each group to use a separate AC power supply. Each group is individually fused with a replaceable 5 amp fuse, which protects the group from a short-circuit in the field wiring and prevents the short-circuit from affecting other channel groups on the module. In

addition, every output circuit is electrically isolated from the CPU, I/O-BUS and ground to isolate field faults.

Guarded Outputs

The ODM uses a combination of extensive on-line diagnostics and an internal "diagnostic cut-off relay" to automatically protect against energized output failures. Output energy flows through "dual-switches" to the load. A solid-state switch provides the normal output. A relay, controlled by the built-in diagnostics, supplies the second switch through a set of normally open contacts. If any dangerous failure is detected, the relay contacts are opened. This action de-energizes the output, ensuring the output fails in a safe manner. Using this technique, ODM Guarded Outputs ensure outputs fail-safe, even in the presence of faults.

Diagnostics

The ODM is designed to provide years of trouble-free service. However, in the event of unexpected operation, the ODM is equipped with extensive self-diagnostics. The goals of these diagnostics are to:

- Notify the appropriate personnel of a module malfunction or writing error;
- Perform automatic switch-over in a fully redundant (1oo2D) ProSafe-PLC system;
- Perform automatic shutdown of a channel or a module if a dangerous fault is detected.

Any errors detected by the ODM's diagnostics are reported to the associated control module. The control module and the ODM maintain a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the PLC SET configuration software. In addition, errors are indicated by the LED indicators, which indicate the module status.

There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules and those that cover individual output channels.

The circuit is optimized for normally energized usage and provides complete self-diagnostic capability. Diagnostic circuitry measures several voltage signals at the indicated points in the drawings, allowing detection of the following faults:

- Output channel failed ON or OFF;
- Group-fuse blown;
- Group I/O power out of tolerance.

Standard Discrete Module plus (SDM+)

The Standard Discrete Module Plus (SDM+) is a microprocessor-based, configurable module that interfaces discrete DC sensors and actuators with the I/O-BUS. The SDM+:

- Provides fail safe control of outputs with unique Guarded Outputs;
- Supports Sequence of Events Recording (SER) by sensing and recording events at 1 ms resolution;
- Includes a Intelligent Fuse feature to protect individual output channels against short-circuit and overload conditions, caused by field wiring problems;
- Allows the Intelligent Fuse trip to be restored to service remotely or locally, without removing the module from the rack;
- Provides extensive diagnostics analyzed by failure modes and effects analysis (FMEA) and verified by fault injection testing for easy problem resolution;
- Improves error-checking with a per channel built-in output monitor that eliminates the need to wire and program additional input channels for error detection;

- Includes dynamic threshold detection circuits to diagnose failed input channels;
- Supports redundant architecture for high availability;
- Supports low and high temperature operation (-25 to 60°C) with internal detector that detect if the module is operating outside of these limits;
- Simplifies maintenance with onscreen configurable channels that eliminate the need for DIP switches and jumpers;
- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing system wiring;
- Isolates field faults by electrically isolating all I/O channels from the backplane and ground;
- Complies with the European Union's Electromagnetic Compatibility (CE) directives.

Channel types

The SDM+ provides 32 channels, each of which can be configured to be a discrete input (standard or SER), a discrete output (standard or SER), or a discrete pulse output. The SDM+ has configurable channels that reduce hardware costs and spare parts requirements by allowing one module to accommodate several I/O requirements. The variety of I/O types supported also allows related signals, such as the I/O for a particular motor or shut-off valve, to be grouped together, decreasing the time needed to find and respond to faults.

Intelligent Fuse feature

ProSafe-PLC has an Intelligent Fuse feature that protects the SDM+ output channels against over-current conditions caused by field wiring and field device problems. Each channel contains an over-current detection circuit that switches the output off before damage can occur. Diagnostics report the “blown” fuse channel and permit clearing the blown fuse from an operator interface. In addition, a pushbutton located on the module allows local resetting of blown fuses. The Intelligent Fuse feature provides equivalent protection of individual hard fuses, permits remote online “repair,” and eliminates the need for stocking spare fuses.

Guarded Outputs

The SDM+ uses a combination of extensive on-line diagnostics and an internal “diagnostic cut-off relay” to automatically protect against energized output failures. Output energy flows through “dual-switches” to the load. A solid-state switch provides the normal output. A relay, controlled by the built-in diagnostics, supplies the second switch through a set of normally open contacts. If any dangerous failure is detected, the relay contacts are opened. This action de-energizes the output, ensuring the output fails in a safe manner, even in the presence of faults.

Diagnostics

The SDM+ is equipped with extensive self-diagnostics verified by full FMEA and fault injection testing. The goals of these diagnostics are to:

- **Notify the appropriate personnel of a module malfunction or wiring error;**
- **Perform automatic switchover in a fully redundant (1002D) ProSafe-PLC system.**

Any errors detected by the SDM+ diagnostics are reported to the associated control module. The control module and the SDM+ maintain a log of current and historical errors that can be reviewed using the Diagnostic

Logger Utility or the PLC SET configuration software. In addition, the module have LED indicators that indicate errors.

There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules, and those that cover individual input/output channels.

Overall module performance diagnostics

Diagnostics for overall module performance include failure detection in the communications, processor, and common circuits.

A series of precision voltages are scanned online and the readings are compared with predetermined values to detect failures in the analog-to-digital (A/D) converter, input filters, and multiplexer circuitry. To detect excessive drift, reference voltage source readings are checked against values stored at the time of manufacture. Failed ON and failed OFF conditions are also monitored. Analog read back constantly monitors the digital-to-analog (D/A) circuitry. These values are compared with expected results for quick failure detection.

The LED's support local troubleshooting without an operator interface. The module includes one LED per channel to indicate its status and two LED's that indicate a combination of the module status's.

Input & Output circuit diagnostics

The circuit is optimized for normally-energized sensor inputs and offers self-diagnostic capability. Diagnostics use a combination of voltage & current measurement and constant switching in the 1002D architecture. Circuitry measures several voltage and current levels at the indicated points in the drawing, which allows detection of short circuit and diagnostic circuit failures.

Configuration

The configuration tool ProSafe-PLC SET is used to assign a type to each channel (input, output, or pulse). In addition, for some channels, additional parameters can be defined.

Discrete Input channel parameters
Input Fault State, if an input channel fails to change state when tested, the input will report the state defined by this parameter.

Discrete or Pulse-Output channel parameters

- The state of an output is automatically “read back” by input circuitry on the same channel as a way to diagnose and report faults;
- Guarded Output; if a Guarded Output channel fails when instructed to de-energize, the SDM+ will disable all of its output circuits.
- The duration of a pulse output channel can be specified to be between 10 discrete and 2000 milliseconds;

The Bus Continuation Module (BCM)

A BCM is an empty module and mounts in a single MODULRACK slot. It is used in spare positions between the other modules. The BCM serves to:

- Enhance the appearance of a partially filled MODULRACK;
- Protect unused MODULRACK backplane connectors;
- Preserve continuity of the I/O-BUS loop signal on unused backplane connectors.

The BCM is required in a rack-to-rack redundant system, when slots intentionally left vacant disrupt the continuity of the ‘OK’ loop redundancy switchover signal.

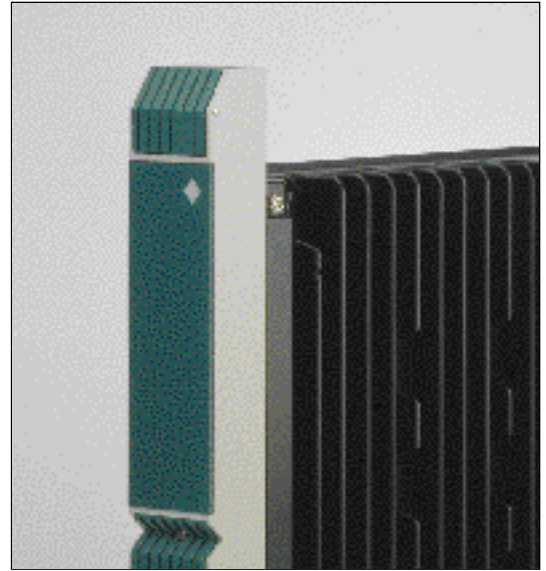


Figure 5.7 BCM-module

In a non-redundant system slot(s) left intentionally empty will not inhibit operation of the system; therefore a BCM may be added for cosmetic purposes or to protect the unused backplane connector.

Bus Diverter Module (BDM)

The BDM occupies a single MODULRACK slot. The top connector at the rear of the module mates with MODULRACK backplane connector P1 for access to I/O-BUS redundancy signals. The I/O-BUS is diverted via a printed circuit board to the bottom connector (P2), which mates with a BDM Transition Board or Extended Transition Board, to allow the I/O-BUS and redundancy signals to exit the MODULRACK at any slot, where the BDM is installed.

The BDM can support both module-to-module and rack-to-rack redundancy. Combinations of non-redundant CCM's and BDM's can be installed in a MODULRACK to create up to five individual I/O-BUSES.

The MODULE-BUS Expander module (MBX)

An MBX module communicates with other MBX's by sending and receiving M-BUS communications across the redundant M-NET. It permits plant-wide expansion of the redundant M-BUS, interconnecting Local Area Systems over short or long distances. An MBX is installed at each Local Area System and each pair of MBX's is linked by coaxial cable. This plant-wide carrier band redundant network is called a M-NET.

The MBX is a node on both the M-BUS and M-NET. It is a communications repeater that:

- Receives M-BUS serial data, converts it and broadcasts it over the M-NET;
- Receives M-NET data, then converts it and transmits that data over the local M-BUS.

The MBX contains two separate, but identical communications systems identified as sides "A" and "B", which accommodate the redundant M-BUS and M-NET. System communications normally alternate between both sides. A permanent switch-over occurs only when a fault is detected.

Rack-to-Rack redundancy

Two MODULRACKS are involved, each with an MBX. The racks must be identical with respect to module selection and slot location. Different System Node Addresses are assigned to the two MBX's; M-NET A and M-NET B are connected to both MBX modules.

Module-to-Module redundancy

One MODULRACK is involved with two MBX's occupying adjacent MODULRACK slots. They are assigned the same System Node Address. One MBX will serve M-NET "A" and the other M-NET "B". The unused side of each MBX will not be connected to the M-NET. When module-to-module redundant MBX's are employed, they must occupy adjacent slots and be assigned identical SNA's (slot & node, addresses).

Modulnet (M-NET) Interface card, MNI

The M-NET Interface Card (MNI) is a 16-bit ISA compatible add-on card, occupying one slot in a Pentium PC and operates in a Windows environment. It enables that computer to run ProSafe-PLC applications such as ProSafe-SET System Engineering Tool or ProSafe-OIS and to communicate with ProSafe-PLC systems by means of the plant-wide redundant M-NET. The MNI Card interfaces the personal computer to the M-NET. Maximum cable length is 50 meters (163 ft.).

6 Project realisation

The ProSafe-PLC SET, System Engineering Tool

ProSafe-PLC SET (SET) is a graphical, self-documenting software package used to configure Safety strategies to be implemented in the ProSafe-PLC system. The graphical programming format is based on the international standard IEC 1131 part 3, following the IEC specification. SET provides an integrated set of configuration tools. The configuration tools support two programming languages for function block & ladder logic, which are allowed for use of Safety critical functions. In addition sequential function charts and structured text are supported for non-Safety related functions, such as communication. These languages are implemented using a graphical format that is easy to learn and provides intuitive documentation. This design makes ProSafe-PLC equally adaptable to continuous and discrete functions, or any mix therein, without requiring custom software or hardware extensions for unusual requirements. It also provides an unprecedented level of consistency and familiarity, which reduces training requirements and accelerates the configuration process.

Software and hardware platform
A basic hardware platform for ProSafe-PLC SET is an IBM® (or compatible) PC running the MS-Windows 3.1/Windows 95 or NT operating system. The minimum hardware requirements are a 386/20 MHz processor and 8 MB of RAM. ProSafe-SET runs on desktop as well as on laptop PC's.

Windows environment

The SET operates within a Microsoft Windows® environment. This environment provides all the tools needed to streamline configuration. Menus, dialogue boxes, and function keys simplify the configuration process by providing quick access to commands and facilitating logical responses. In addition, the System Engineering Tool includes an extensive on-line help file, offering details regarding reported diagnostics and common configuration questions.

Windows also provides a very flexible configuration platform. Configuration windows can be realised, moved, or made into icons. (Icons are freezing a window of graphic configuration at the current level of detail and make additional space in the configuration window, by creating a symbol at the bottom of the screen for quick recall).

Like in other Windows® applications, the user can open multiple SET windows from one or more configurations at the same time. This flexibility allows complex tasks to be easily performed. For instance, pieces of a configuration can be cut, copied, and pasted from one window to others on the same screen.

Graphical configuration

Configuring a drawing sheet consists of placing graphical symbols by using a point and click method with a mouse and a menu bar, or using function keys and 'wiring' the symbols together. This graphical configuration method provides intuitive documentation and is stored as such in the controller, which eliminates the need for off-line documentation altogether.

Configuration hierarchy

A configuration is usually much larger than a single sheet. Therefore, to simplify configurations and maintenance, sheets can be configured and organised in a hierarchical relationship that is similar to a directory structure. Within this hierarchy the variables can be passed from sheet to sheet if needed. They can also be declared global and used anywhere in the configuration. These capabilities integrate the overall configuration. This flexible, user-defined hierarchy allows the organisation of a configuration to reflect the physical organisation of process equipment. The Safety related portion of the configuration should be separated from the non-Safety-related portion of the configuration.

Tag-based configuration

User-defined tags identify all variables in a database. Every tag starts with assignment to the screw terminals of an I/O module and is carried through the configuration. It also makes tracing values from software to hardware during troubleshooting a simple task.

Programming by Function Block & Ladder Logic

The function block language is used to configure function block networks and consists of a series of function blocks connected to perform a regulatory control application. Each function-block within the network is processing input variables and provides one or more outputs.

- Ladder logic programming provides traditional ladder logic network techniques for high performance discrete control and interlocks. The ladder logic elements provide connections between the power rails to software coils.

Off-line & On-line modes

ProSafe-PLC SET can run in an off-line or on-line mode. The off-line mode provides a configuration environment. The on-line mode presents the running hardware configuration and provides tools for troubleshooting and testing. This means one package can be used for configuration, testing, start-up, and maintenance, eliminating the relearning of software.

On-line editing & Forcing of values

Each real-time value can be forced to a new, user-defined value. The effect of the change within the control module can be analysed to help troubleshoot the configuration. This function is particularly valuable because it provides cause & effect information before start-up. Thus, changes can be made to the configuration ahead of time, reducing troubleshooting time during start-up.

On-line changes can range from a simple tag name edit, to adding a few function blocks, to creating new sections in a configuration. During on-line editing, the SET does not require a compilation step, which allows changes to take effect immediately. In Safety systems this feature should not be used or with the utmost care.

7 Glossary of terms

availability: The probability that a system is capable to fulfil its function at some instant of time. Practically it is often assumed to be constant and expressed in the “FTR”.

cause & effect diagram: A matrix drawing showing the functional process Safety interlocks between inputs and outputs of a Safety system. (See also at “FLD”).

common-cause failures: Failures originating from the same external or internal conditions. (See also at “systematic failures”).

coverage factor: The efficacy of the self-diagnostics of a SIS, which makes it possible that a system successfully recovers (safely) from a specific type of component or software fault. It can be expressed in a probability or in a factor that is always smaller than 1 (i.e. $C = 0.95$). The C-factor comprises the percentage of failures in modules, software, external wiring, internal wiring, cables, interconnections and other functions that are detected by the built-in test functions, or by a suitable test program.

covert failure: A non-revealed defect in a system that is not detected by the incorporated test mechanisms. It will cause the system to fail to act properly, when a “demand” for a process shutdown comes from the Safety critical process parameters.

de-energised safe condition: In this context: the electrical or pneumatic valves, which can shutdown the guarded process, are energised during the normal (safe) process situation. If an unsafe condition arises, the (spring-loaded) valve will close, because the energy is cut off.

DCS: Distributed (or Digital) Control System. A process control system based on computer intelligence and using a data-highway to distribute the different functions to specialised controllers.

dynamic logic circuit: In this context: the valid logic-state can only exist and perform logic control, if the circuit is activated continuously, using alternating logic signals.

Emergency Shutdown: Commonly used terminology to refer to the safeguarding systems, that comprise the Safety interlocks and start-up & regular shutdown sequences. The system is especially suited to shutdown a plant in case of a process parameter limit-excess. These systems are also referred to as Safety Related Systems (SRS), or SIS, which stands for a Safety Instrumented System.

EMI: Electrical-Magnetic Interference.

EMC: Electrical-Magnetic Compatibility

event: A change of state of inputs or outputs, as well as intermediate logic status.

fail-safe: A control system that, after one or multiple failures, lapses into a predictable de-energised safe condition.

failure: Loss of function of a single component, system part, or of the entire system.

fault-tolerant: A system that continues to fully perform its functions without interruption, in spite of component failures.

FMEA: Failure Mode and Effect Analysis.

FLD: Functional Logic Diagram. A graphical representation of the system functions, showing the logic-gates and timers as well as the logic signal interconnections.

FTR: False Trip Rate. It equals $1/MTNF$. Also refer to “Availability” & “nuisance failure”.

HIPS: High Integrity Protection Systems.

HIPPS: High Integrity Pressure Protection System. Also called “Over Pressure Protection System” or OPSS.

host system: A computer such as a DCS, a mainframe, workstation or PC that communicates with the ProSafe PLC via the serial interface.

hot repair: Replacement of printed circuit boards or modules in a fully functioning system, without affecting the controlled process.

IEC: International Electronic Committee.

inherently: Existing in something as a natural and inseparable quality. (synonyms: inbred, inborn, internal, and ingrained).

inherently fail-safe: A particular designed dynamic logic principle that achieves the fail-safe property, from the principle itself and not from additional components or test circuits.

intermittent fault: An error that occurs only occasionally due to installed hardware, EMI, varying software status, or software bugs. Also referred to as “soft-error”. See also under “undetected failure”.

MTTR: Mean Time To Repair. The mean time between the occurrence of a failure and the return to normal failure-free operation after a corrective action. This time also includes the time required for failure detection, failure search and re-starting the system.

MMI: Man Machine Interface or “operator interface”, usually a computer screen to present the actual process and system status. It offers the possibility for regular system interventions, data handling and storage.

nuisance failure: A failure arising out of an erroneous assessment of the situation. A shutdown is initiated, though no real impairment of Safety exists. Also referred to as “false trip”.

Pfd: The probability of a failure on demand, to shutdown the process coming from the Safety parameters of the process. This parameter is degrading during the mission time, test interval time. Therefore the average figure Pfd average is used in calculations.

PLC: Programmable logic Controller. Also PES, meaning Programmable Electronic System.

proof-test: A 100% functional system test. In practice, this is only possible when the SIS system is disconnected from the process.

redundancy: Use of elements identical in design, construction and in function with the objective to make the system more robust for self-revealing failures. Sometimes referred to as “similar redundancy”, which is the opposite of “diverse redundancy”. It can apply to hardware as well as to software.

reliability: The probability that no functional failure has occurred in a system during a given period of time.

revealed failure: A failure in a system that is detected by the systems self-diagnostics.

reverse-fault immune: The usage of special design methods, that are sometimes referred to as a “firewall”. This implies that any fault in a particular system module cannot affect the safe operation of the SIS. Also called “interference free”, or in German: “Rückwirkungsfrei”.

Safety: Freedom from unplanned adverse effects on the safe use, operation and maintenance of a system.

Safety interlocks: The functional relationship between system inputs and outputs in the operational mode of the plant. It is installation oriented, reflecting mechanical relationships. In logic terminology, the “and” & “or” gates represented by the Cause & Effect diagram (see also at “FLD”).

scan-time: The time required to execute the complete application program.

SCADA: Supervisory Control and Data Acquisition.

SER: Sequence of Events Recorder, based on real-time state changes of events in the system (see also at “event”).

SIL: Safety Integrity Level as proposed by the IEC defining a Pfd by order of magnitude, which is related to the risk (Pfd) involved in various types of processes. In practice the SIL range is from 1 to 4 for most Industrial processes.

soft-error: See at “intermittent fault”.

solid-state logic: An adjective used to describe circuits whose functionality depends upon electronic components as semiconductors, resistors, capacitors, magnetic cores, etc. and which is not depending on any software.

systematic failures: Failures occurring in identical parts of a (redundant) system due to similar circumstances. History shows that also errors in specification, engineering, software and environmental factors, such as electrical interference or maintenance errors must be comprised.

TMR: Triple Modular Redundancy. A solution to achieve fault-tolerance by a 2 out of 3 voting configuration. Also referred to as 2oo3 voting.

trip: A shutdown of the process by the Safety system.

TÜV: Technische Überwachungs Verein. A testing laboratory in Germany that certifies Safety of equipment, according to the standards issued by the IEC, VDE and DIN.

unrevealed failure: A failure that impairs the system Safety, but remains undetected (see also under “covert failure”) It is related to the risk (Pfd) involved in various types of processes. This type of failures can accumulate in a Safety system, causing a degradation of the Safety performance (SIL), as a function of time.

8 Yokogawa ISS serving Industrial Safety

The company

Founded in 1962, Yokogawa Industrial Safety Systems is one of the world's most experienced Safety and Control firms. Today Yokogawa ISS with its headquarters in The Netherlands provides services to clients on a global scale.

Yokogawa ISS is a company on the move, one that stays in touch with its customers and remains at the forefront of technology by co-operation with technical universities and certifying bodies. Further by active participation in standardisation committees, that are involved in the development of international Safety standards (like the IEC61508), stays abreast of the evolution of the profession of Industrial Safeguarding.

Yokogawa ISS, as one of the four "Centres of Excellence" within the Yokogawa Corporation, is committed to offer protection systems of the highest Safety Integrity Level (SIL) for the oil & gas, chemical process, nuclear and conventional power industries. The Yokogawa ISS project organisation operates on a world-wide basis and is ISO9001 certified. The activities comprise the realisation of turnkey projects, after sales service and technical customer training. Yokogawa remains at the forefront of technology and the development of international Safety standards by participation and co-operation with technical universities, standardisation committees, certifying authorities and inspection agencies.

Yokogawa ISS is a subsidiary of Yokogawa Electric Corporation, a major player in the world of Measurement, Control and Safety. The company employs over 11000 people world-wide and offers the financial backing that will support continued growth through strategic acquisitions and products innovation.

The ProSafe Family of products

The ProSafe Family of products is capable of covering all functionality as found in today's Safety and Process Control systems. Each ProSafe Family member covers one or more specific aspects of the total system functionality. This ranges from the High Integrity Protection Systems HIPPS, ESD, PSD, and F&G systems, up to the Man Machine Interface, Distributed Control Systems and very large supervisory "SCADA" systems. By a policy of continuous innovation, the ProSafe Family of products will remain up-to-date with the imminent developments in International Regulations, such as the IEC61508 and customer requirements. The governing design criteria remain the creation of superior and comprehensive Safety system solutions, at minimal "cost of ownership", prepared for a long useful lifetime.

