Technical Information

System Overview ProSafe-COM 3.00

ProSafe-COM

TI48J01A00-00E-N

YOKOGAWA

Yokogawa Europe Solutions B.V.
PO Box 163, 3800 AD, Amersfoort, The Netherlands
Tel: (31) 88-464 1000 Fax: (31) 88-464 1111

TI48J01A00-00E-N

4th Edition Oct 2010

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Preface

Company profile

A part of Yokogawa company is active in the field of design and engineering of control and safety systems. The products are worldwide used as emergency shutdown, process shutdown or fire & gas systems in oil and gas exploration, petrochemical and nuclear industries.

ProSafe safety systems

From its founding days, the safety division of Yokogawa Europe Solutions BV has enterprised solid-state safety systems emerging in a product that is nowadays referred to as ProSafe-SLS. It is a unique, inherent fail-safe technology. It combines a very high safety level with a very high availability level.
The ProSafe-SLS technology is TÜV AK-7 / SIL4 certified.

In 1997 the safety division of Yokogawa Europe Solutions BV introduced the ProSafe-PLC. ProSafe-PLC is TÜV certified up to AK-6 / SIL3. It is highly scalable and can be easily tailored.

To enable communication between the ProSafe systems and other systems like e.g. a DCS, the safety division of Yokogawa Europe Solutions BV has introduced the ProSafe-COM products in 1994.
COM is the abbreviation of 'COMmunication'. A DOS version (MODCOM) and a Windows 2000 based version (MULCOM) are available. The Windows 2000 version allows complete integration with the Yokogawa CS3000 / VP system via V-net and easy linking with the ProSafe-PLC and ProSafe-SLS. Since the functionality of MODCOM and MULCOM functionality partly overlap ProSafe-COM is now introduced, a single platform which can be used to replace both MODCOM and MULCOM. The new ProSafe-COM platform is headless (no moving parts) and comprises an embedded version of Windows XP.

In May 2005 Yokogawa released ProSafe-RS, a new safety system which can be fully integrated with the existing Yokogawa DCS products (CENTUM CS3000 and CENTUM VP).
ProSafe-RS directly connects to the CENTUM control bus, so ProSafe-COM is not required for the integration of ProSafe-RS. However, ProSafe-COM may still be used to integrate legacy ProSafe products with other DCS or SCADA systems.

System overview ProSafe-COM

This booklet is an introduction to ProSafe-COM. It briefly discusses the ProSafe products in general and the context of ProSafe-COM. Thereafter, this booklet focuses on the functions, hardware set-up and interfaces of ProSafe-COM.

Audience

This booklet addresses anyone who wants to get a quick overview of ProSafe-COM and its functions: management, operator, service personnel, etc. This booklet also addresses the system engineer who has to integrate ProSafe-COM into a DCS or SCADA system.

The System overview can be read, without prerequisite knowledge, from the beginning until the desired level of detail is revealed. Though not required, some knowledge of instrumented safety systems is recommended for understanding this booklet.

About this manual

This System overview gives an introduction to ProSafe-COM. The booklet contains nine chapters, two appendices and a glossary list. The basic structure of this booklet is as follows.

Chapter 2	**An introduction to ProSafe-COM** Overview of the ProSafe family products and the main characteristics of ProSafe-COM.
Chapter 3	**ProSafe-COM functions** Detailed description of what data, in which way, can be exchanged between ProSafe-COM and its surrounding systems.
Chapter 4	**ProSafe-COM hardware** Description of available boards in ProSafe-COM.
Chapter 5	**ProSafe-COM interfaces** Functions, hardware provisions and characteristics of: • Printer • User interface • V-net interface • OPC Interface • MODULE-BUS (M-BUS) / MODULE-NET (M-NET) • Ethernet interface • Serial interfaces
Chapter 6	**Functions and hardware design** Explains in more detail how the ProSafe-COM functions are implemented in the hardware.
Chapter 7	**Redundant configurations** Function and characteristics of a redundant configuration.
Chapter 8	**Time synchronisation** Function and realisation of time synchronisation.
Chapter 9	**ProSafe-COM System Engineering Tool** A description of the tool COM SET, used for: • Engineering ProSafe-COM • Commissioning • Test and maintenance
Chapter 10	**EmuTool I/O emulation tool** A description of the tool EmuTool, used for: Emulating I/O
Appendix A	A description of how to integrate ProSafe-COM in the DCS system, using tags. This information is meant for the system engineer of the DCS system that ProSafe-COM has to be integrated in.
Glossary	A glossary of used terms

Note

This *System overview* describes the maximally possible configurations of ProSafe-COM and the ProSafe safety systems. However, in practice ProSafe-COM and the ProSafe safety systems do not need to have all components described.

Other booklets on ProSafe-COM

The ProSafe-COM documentation consists of the following volumes:

- ProSafe-COM General Specification (2 versions)
- ProSafe-COM System overview
- ProSafe-COM Engineering manual
- ProSafe-COM Test & Maintenance manual

The *ProSafe-COM General Specifications* describe high level functionality.

The *ProSafe-COM System overview* gives an introduction for anyone interested in ProSafe-COM.

The *ProSafe-COM Engineering manual* guides engineers through the process of configuring and programming ProSafe-COM. It describes the hardware, system tuning and possible configurations, and points out the strategy for project engineering. The use of the engineering tools is explained in detail.

The *ProSafe-COM Installation, Test & Maintenance manual* provides information for hardware and software installation, for maintenance and for trouble shooting.

Ordering information

The ProSafe-COM 3.0 system documentation can be obtained from any Yokogawa Europe Solutions BV Sales & Marketing department using the volume title and document number:

• ProSafe-COM General Specification (PCI bus only)	GS 48D62Z02-00E-N
• ProSafe-COM General Specification (PCI + PCI-E bus)	GS 48D62A02-00E-N
• ProSafe-COM System overview	TI 48J01A00-00E-N
• ProSafe-COM Engineering manual	IM 48J01G01-00E-N
• ProSafe-COM Installation, Test & Maintenance manual	IM 48J01H01-00E-N

1 An introduction to ProSafe-COM

1.1 ProSafe-COM and the ProSafe family

ProSafe is short for Programmable Safety systems. ProSafe provides for today's and tomorrow's market demand for sound safety solutions. ProSafe comprises a whole family of industrial safeguarding and safeguarding associated products.

A ProSafe safety system can be used as emergency shutdown, process shutdown or fire & gas system in the oil and gas exploration, petrochemical or nuclear industries, to mention some examples. A ProSafe system works autonomously. It shuts down the guarded process (or part of it) without any operator's intervention when the input sensors detect an unsafe situation or when the ProSafe systems diagnose an internal error which may prevent the Safety system from responding correctly when a demand comes from the field.

The ProSafe family can be divided into systems with the following functions:

- Safeguarding
- Communication
- Supervising

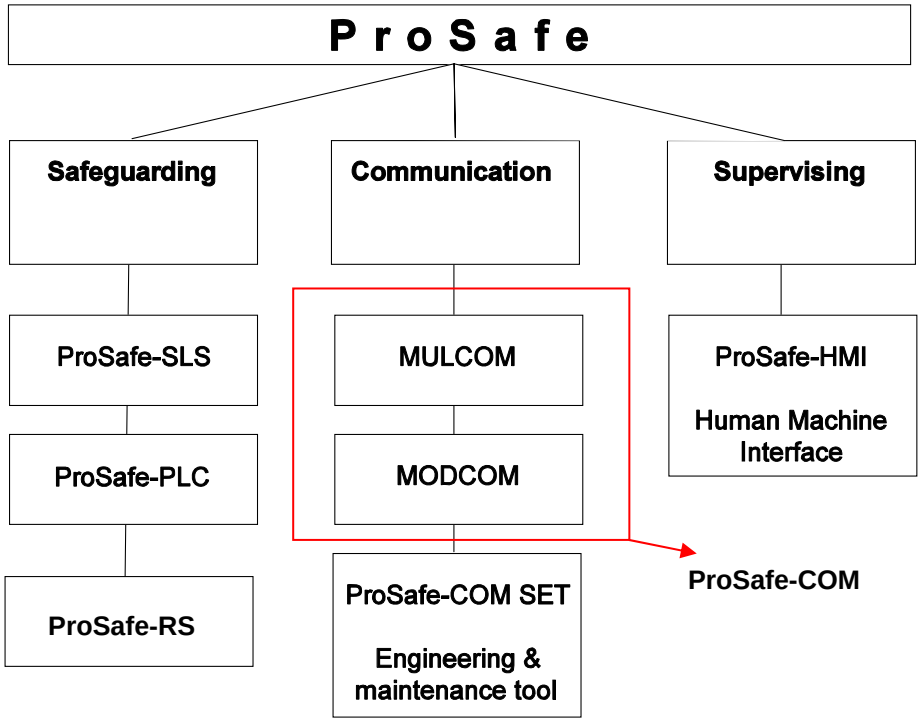

Figure 1: The ProSafe family members

Safeguarding

The kernel of the ProSafe family is the ProSafe safeguarding system. The ProSafe safety system works autonomously, without intervention from operator or other systems. Therefore a ProSafe safety system guarantees a safe industrial system.

The ProSafe safety system can comprise one or more of the following systems:

- ProSafe-SLS: a hard-wired safety system (Solid State Safety)
- ProSafe-PLC: a PLC-based safety system
- ProSafe-RS: a new generation programmable safety system

All these types of safety systems are fail-safe. They can perform the safeguarding function both individually and integrated. Depending on client's wishes, a ProSafe safety system can consist of one or more types of safety systems.

Communication

ProSafe-COM handles the data communication between the ProSafe safety system and various external systems, like CENTUM CS3000 / VP or other supervisory systems.

The data communication can be:

- from ProSafe safety system to ProSafe-COM, and further up to supervisory systems
- from supervisory systems down to ProSafe-COM, and further down to the ProSafe safety system

The basic function of ProSafe-COM is communication. In addition to this, ProSafe-COM can store events (SOE = sequence of event recorder) and perform logical operations.

The engineering and maintenance tool for ProSafe-COM is the ProSafe-COM System Engineering Tool (SET). During commissioning, test and maintenance ProSafe-COM SET is a powerful tool. ProSafe-COM SET can be used for remote inspection and troubleshooting. Especially when long distances need to be covered this can be very useful.

ProSafe-COM supersedes the DOS version (MODCOM) and the Windows NT/2000 version (MULCOM). This booklet describes the ProSafe-COM Windows Embedded POSReady 2009 version.

Supervising

A ProSafe system can be supervised from the Yokogawa CENTUM CS3000 / VP system. Another Distributed Control System (DCS) or SCADA system can be used also. An excellent SCADA solution is provided by Yokogawa System Center Europe's FAST/TOOLS.

ProSafe-COM handles the communication between the ProSafe safety system and the supervising system. ProSafe-COM uploads all relevant process information from the ProSafe system to the supervising system. The ProSafe-HMI (Human Machine Interface), DCS or SCADA system organises and displays this information to the operator.

When connected to a CENTUM system, ProSafe-COM allows a complete integration of the safety system within the CENTUM CS3000 / VP system. ProSafe-COM can automatically send event information to the CENTUM system. Other manufacturer's DCS or SCADA systems have to request for information from ProSafe-COM using OPC or Modbus.

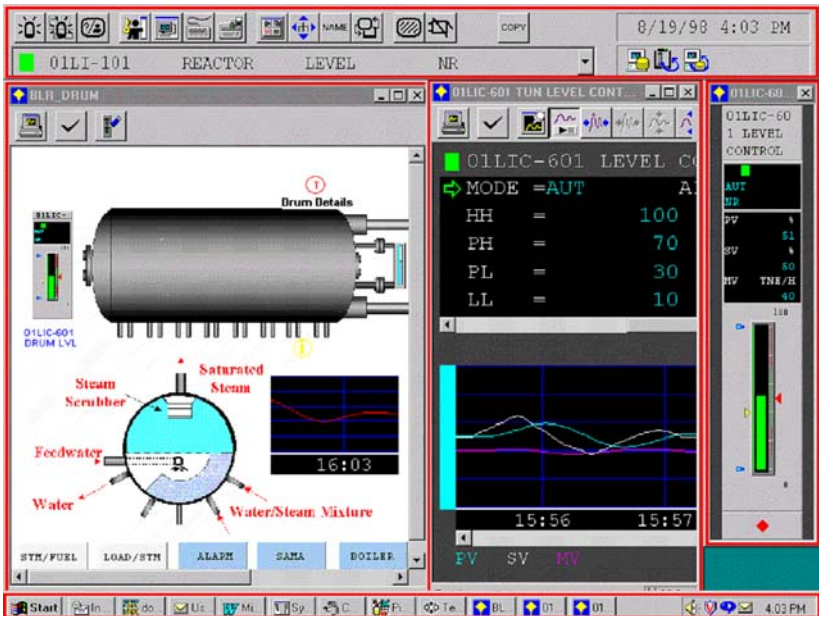

Figure 2: Example of an operator screen on a CENTUM CS3000

1.2 MODCOM / MULCOM versus ProSafe-COM

ProSafe-COM supersedes two earlier versions: MODCOM and MULCOM.
MODCOM is realised on a DOS platform and the DCS interface is based on the Modbus RTU protocol.
MULCOM runs on Windows 2000 and supports multiple interfaces to DCSs (V-net, OPC, Modbus).

Table 1: Main differences between MODCOM/MULCOM and ProSafe-COM

MODCOM	MULCOM	ProSafe-COM
Supervising systems have to request for event and tag information from MODCOM	Full integration with the control backbone of CENTUM (Vnet). MULCOM can send event information to the CENTUM system without a request for it.	Full integration with the control backbone of CENTUM (Vnet) ProSafe-COM can send event information to the CENTUM system without a request for it.
Only RS232 Modbus communication with ProSafe-PLC	Full integration with ProSafe-PLC, via M-BUS/M-NET	Full integration with ProSafe-PLC, via M-BUS/M-NET
Connection to ProSafe-SLS via a single Y-net connection.	Supports two separate Y-net connections to ProSafe-SLS.	Supports two separate Y-net connections to ProSafe-SLS.
Only Modbus communication with DCS or SCADA	Support of Modbus and OPC to connect to OPC enabled supervisory systems.	Support of Modbus and OPC to connect to OPC enabled supervisory systems.
Modbus supports only boolean and 16 bits register types	Modbus supports booleans, 16-bits registers and single precision floats.	Modbus supports booleans, 16-bits registers and single precision floats.
Built on dedicated headless industrial PC using DOS OS.	Built on standard industrial PC (standard hard disk, power supply and processor having fans) using Windows 2000	Built on dedicated industrial PC without moving parts. Flash disk, 24V only, no fans. Using Windows XP compatible Windows Embedded POSReady 2009.
ISA slots only	PCI 2.1 / ISA slots	PCI 2.1 / PCI-E slots

1.3 ProSafe-COM context

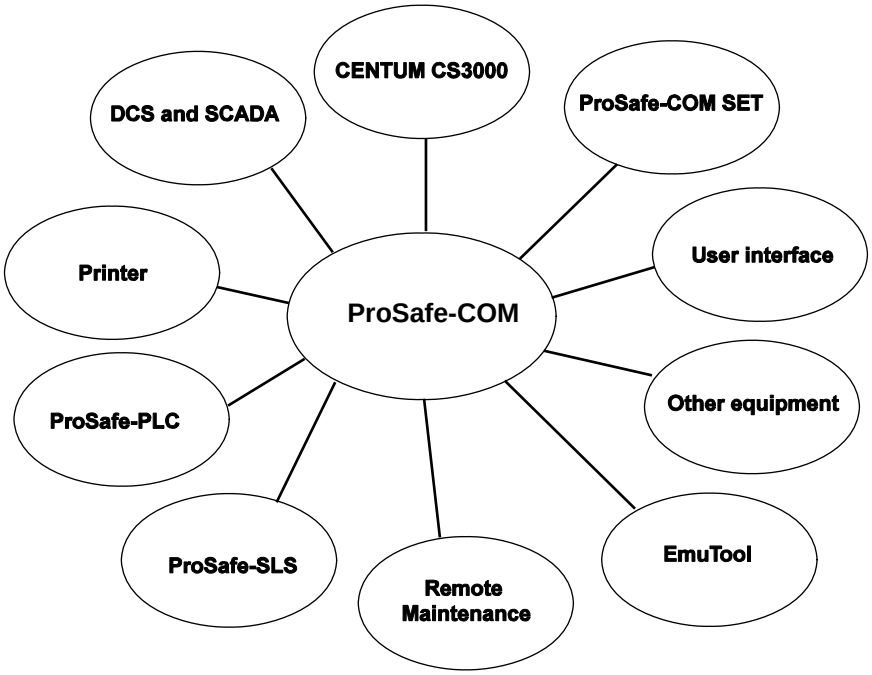

Figure 3: Context of ProSafe-COM

ProSafe-COM

ProSafe-COM is the central communication link between the ProSafe safety system and various other systems. ProSafe-COM communicates data from and to the ProSafe safety system.

CENTUM CS3000 / VP

The CENTUM CS3000 / VP system is the Yokogawa Process Control System. In many projects the ProSafe safety system is directly connected to the control backbone of the CENTUM CS3000 / VP system. The CENTUM CS3000 / VP system retrieves data from the ProSafe safety system or sends data to it. Sending data (override procedures) may be necessary in case of starting up processes or maintenance.

DCS and SCADA systems

Through the use of the OPC protocol ProSafe-COM can be connected to OPC enabled supervisory systems. OPC runs over TCP/IP Ethernet. Both Data Access and Alarm and Events are supported by the ProSafe-COM OPC servers.

ProSafe-COM has up to 10 serial lines that can be used for Modbus communication with DCS or SCADA systems other than CENTUM. For example, Yokogawa's FAST/TOOLS can provide a SCADA solution.

These systems basically have the same functionality as the CENTUM CS3000 / VP system. However, the DCS or SCADA system has to request for event information from ProSafe-COM. ProSafe-COM cannot be fully integrated on the backbone of DCS and SCADA systems other than CENTUM.

COM SET

ProSafe-COM can be configured and monitored with the engineering tool ProSafe-COM SET. During engineering, the data acquisition and the communication with DCS and SCADA can be simulated. ProSafe-COM SET can also be used for remote first-line maintenance, remote control and remote software upgrading of ProSafe-COM. COM SET can be connected to ProSafe-COM via a serial Modbus connection or via a network connection that supports TCP (Modbus/TCP support).

EmuTool

ProSafe-COM can be run while the actual safety systems (ProSafe-PLC, ProSafe-SLS or Modbus slaves) and DCS interfaces (Vnet, OPC or Modbus master) are not yet or only partly connected.
Yet ProSafe-COM is fully operational with respect to available DCS communication and ProSafe-COM logic program execution. The ProSafe-COM configuration files need not be changed in this situation and are identical to the ones used for the final project. The intention of this I/O emulation is to enable the DCS programmers to fully program the DCS operator's HMI and to test the communication with the safety system. Presence of the safety system is not necessary and project development of safety system and DCS application can be done in parallel.

ProSafe-SLS

Two separate Y-net networks can be connected to ProSafe-COM to support ProSafe-SLS, the solid state solution for the highest safety classes.

ProSafe-PLC

The ProSafe-PLC is a programmable electronic system for use in an automated safety system. The flexibility of the PLC makes it suitable for a large variety of applications. The ProSafe-PLC consists of a range of plug-in modules, including critical control modules and critical I/O modules.

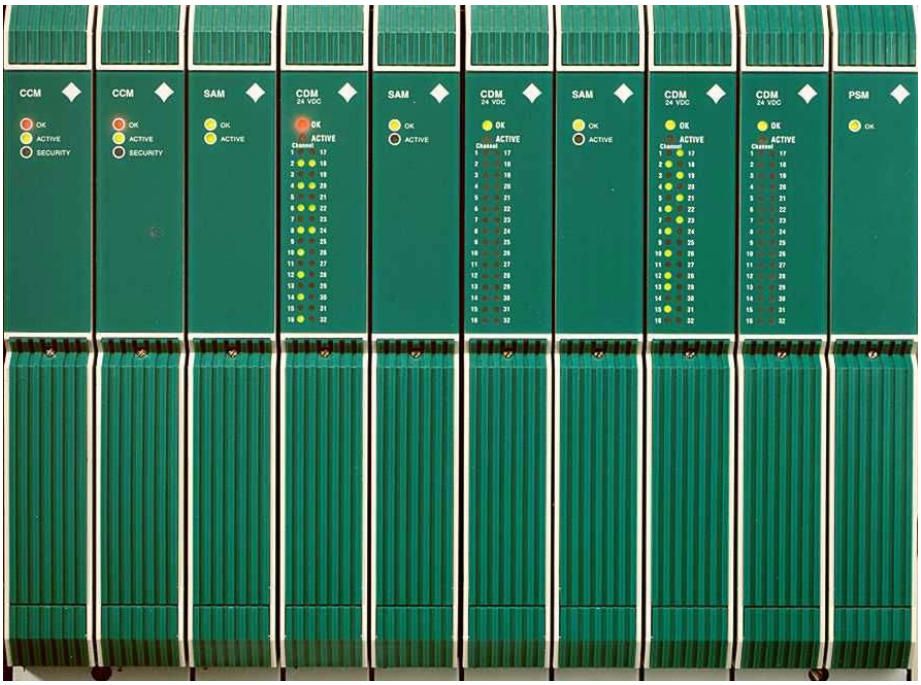

Figure 4: ProSafe-PLC

ProSafe-RS

The ProSafe-RS is the latest SIL3 capable Yokogawa safety system. It has Modbus master and slave capability, so the Modbus links can be used to connect to ProSafe-COM for data exchange with ProSafe-PLC and ProSafe-SLS.

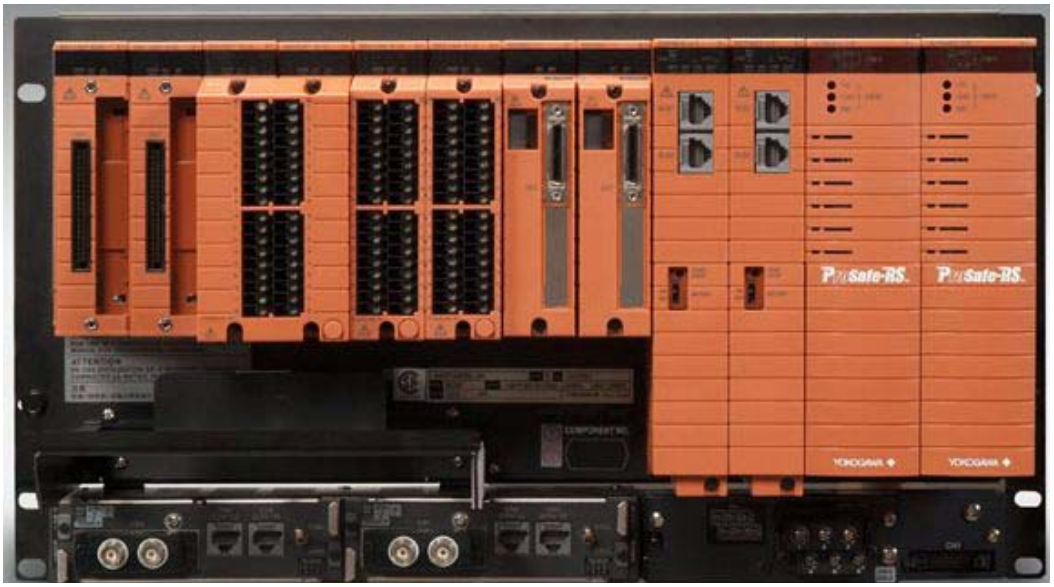

Figure 5: ProSafe-RS

Printer

A printer can be locally connected or connected to another computer in the network to provide a hard-copy of system errors (alarms) and process events.

User interface

Various modules and components of ProSafe-COM and the ProSafe system have LEDs, indicating proper functioning or fault situations. Because ProSafe-COM functions autonomously, no further user interface is required, although connection of a VDU and keyboard is catered for.

Note that engineering, commissioning and maintenance can be done with ProSafe-COM SET.

Other equipment

If required, various other systems can be connected. For example, PLCs other than the ProSafe-PLC can be connected via a serial link. ProSafe-COM can act as a Modbus master station on these serial links. Other equipment can also be connected via the Ethernet link using the Modbus master capability via Modbus/ TCP.

Remote maintenance

Optionally, ProSafe-COM can have an Ethernet connection to allow remote maintenance. The link can be used for on-line inspection and for file transfer. Remote software updates are possible as well.

1.4 ProSafe-COM and CENTUM

ProSafe-COM is the central communication link between the ProSafe safety system and other systems. When used with a CENTUM, ProSafe-COM and the ProSafe safety system present itself as one unit. This unit is called a ProSafe *Safety Control Station* (SCS). The CENTUM is also connected to a *Field Control Station* (FCS). The Field Control Station consists of the non-safety instruments that control and monitor the production process.

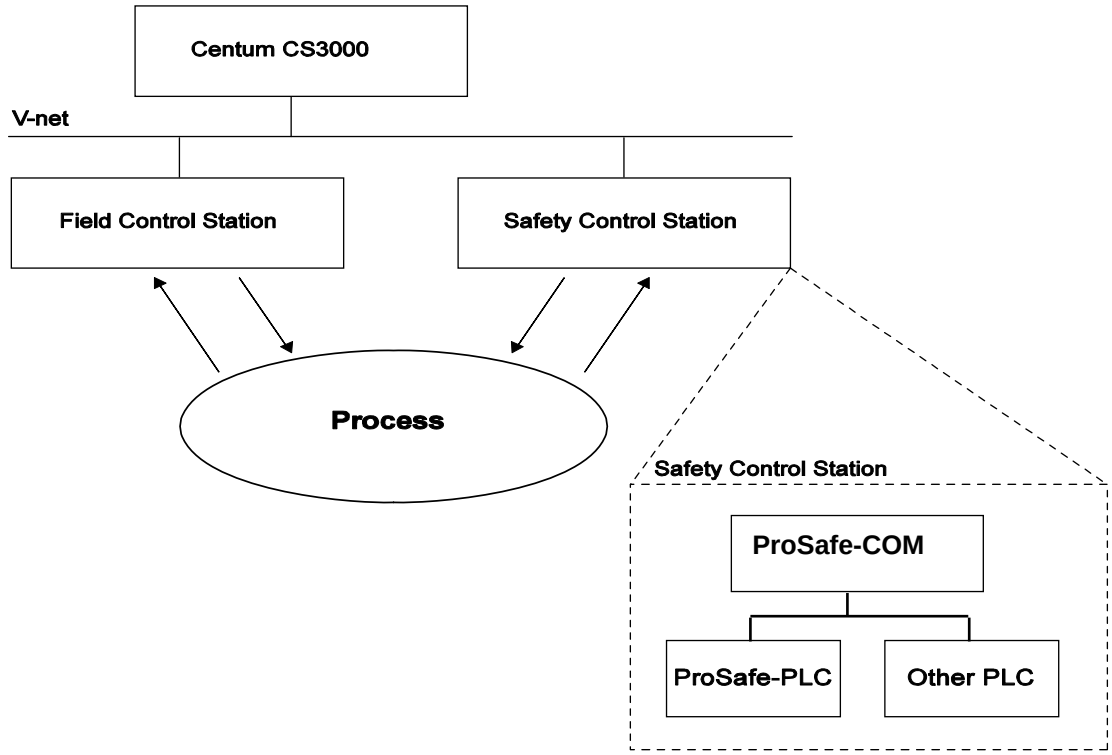

Figure 6: CENTUM and underlying systems

1.5 Functions overview

ProSafe-COM enables communication between the ProSafe safety system and other systems (CENTUM, COM SET, other DCS systems etc.). ProSafe-COM functions autonomously and requires no operator actions. The basic function of ProSafe-COM is to enable communication between the ProSafe safety system and various other systems. The following picture gives a high-level impression of the ProSafe-COM functions.

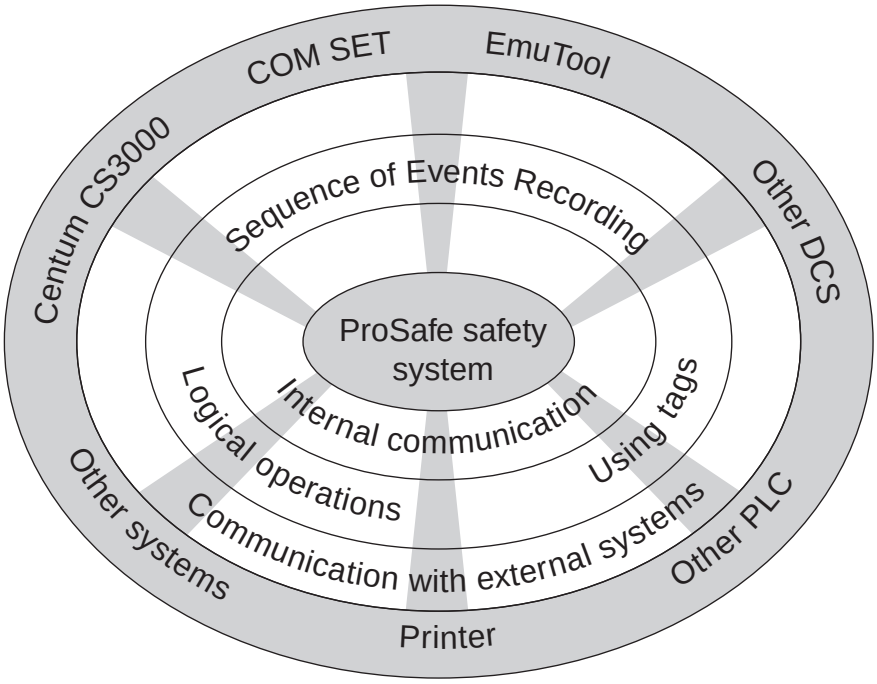

Figure 7: ProSafe-COM functions

Communication with ProSafe safety system

Status of process variables and event messages can be retrieved by ProSafe-COM from the ProSafe safety system. In case of an override procedure, statuses can also be written into the ProSafe safety system.

SER: Sequence of Events Recording

ProSafe-COM keeps track of changes in the ProSafe safety system and maintains a Sequence of Events Recording. All configured signal changes are stored, sorted on time.

Using tags

Tags make communication possible between several systems (for example CENTUM and ProSafe safety system). By means of tags it is easy to design the overall communication between available systems. It is also possible to define which signals are communicated to what system. Not all systems need the same data. So selections can be made by means of groups of tags.

Logical operations

ProSafe-COM has the ability to execute non-safety logic. This facility, for example, can be used to provide a cost-effective solution for the implementation of an operator matrix panel.

Communication with external systems

Status of process variables and event messages can be communicated to a DCS or SCADA system. Status information can also be communicated back to the ProSafe safety system (in case of an override procedure).

Typical applications of ProSafe-COM

ProSafe-COM is scalable in hardware and software functionality and can easily be tailored according the project's needs. Status acquisition and event recording are just the two basic facilities. All other ProSafe-COM functionality is based on these two features. Figure 8 gives an overview of the possible functionality.

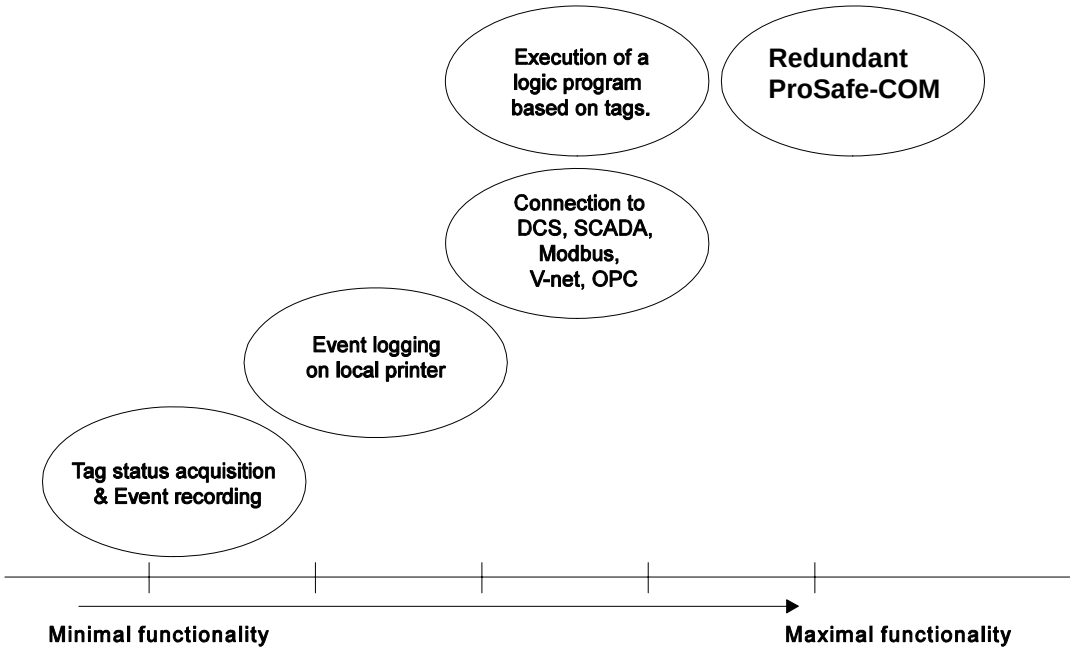

Figure 8: ProSafe-COM application areas

1.6 Hardware overview

ProSafe-COM hardware comprises an industrial PC in 19 inch housing.
The basic configuration has a main CPU board with 4 RS-232 serial interfaces, a parallel printer interface, SATA bus and connections for VDU, keyboard and mouse. Also three Ethernet interface connections and two USB connections are built-in on the CPU board. The IPC is equipped with a solid state flash disk and a Windows XP compatible embedded Windows version (Windows Embedded POSReady 2009).

Hardware modularity

Hardware modularity is achieved by using an (industrial) PC with standard PC interface bus and slots in which the required hardware modules can be fit. Extension boards can be plugged in if necessary. The ProSafe-COM has 3 standard 2.1 version PCI bus connectors (supporting 3.3 and 5 V interface boards) and 1 PCI-E slot. The latter is especially there to be able to use the CENTUM VF702 interface board. The older 2.1 compatible PCI slots support the interface boards for the ProSafe-SLS and ProSafe-PLC safety systems.
The modular set-up of ProSafe-COM enables cost-effective realisation of projects.

1.7 Interface overview

To communicate with the ProSafe safety system and for external communication, ProSafe-COM has the following interface possibilities:

- Printer (maximally 1)
- User interface (keyboard / VDU / mouse / LEDs)
- V-net interface (maximally 1)
- M-BUS/M-NET interface (maximally 4)
- Ethernet interface (maximally 3)
- Serial interfaces (maximally 10)
- Y-net interface (maximally 2)
- USB interface (maximally 2)

The interfacing of ProSafe-COM can be configured with COM SET.

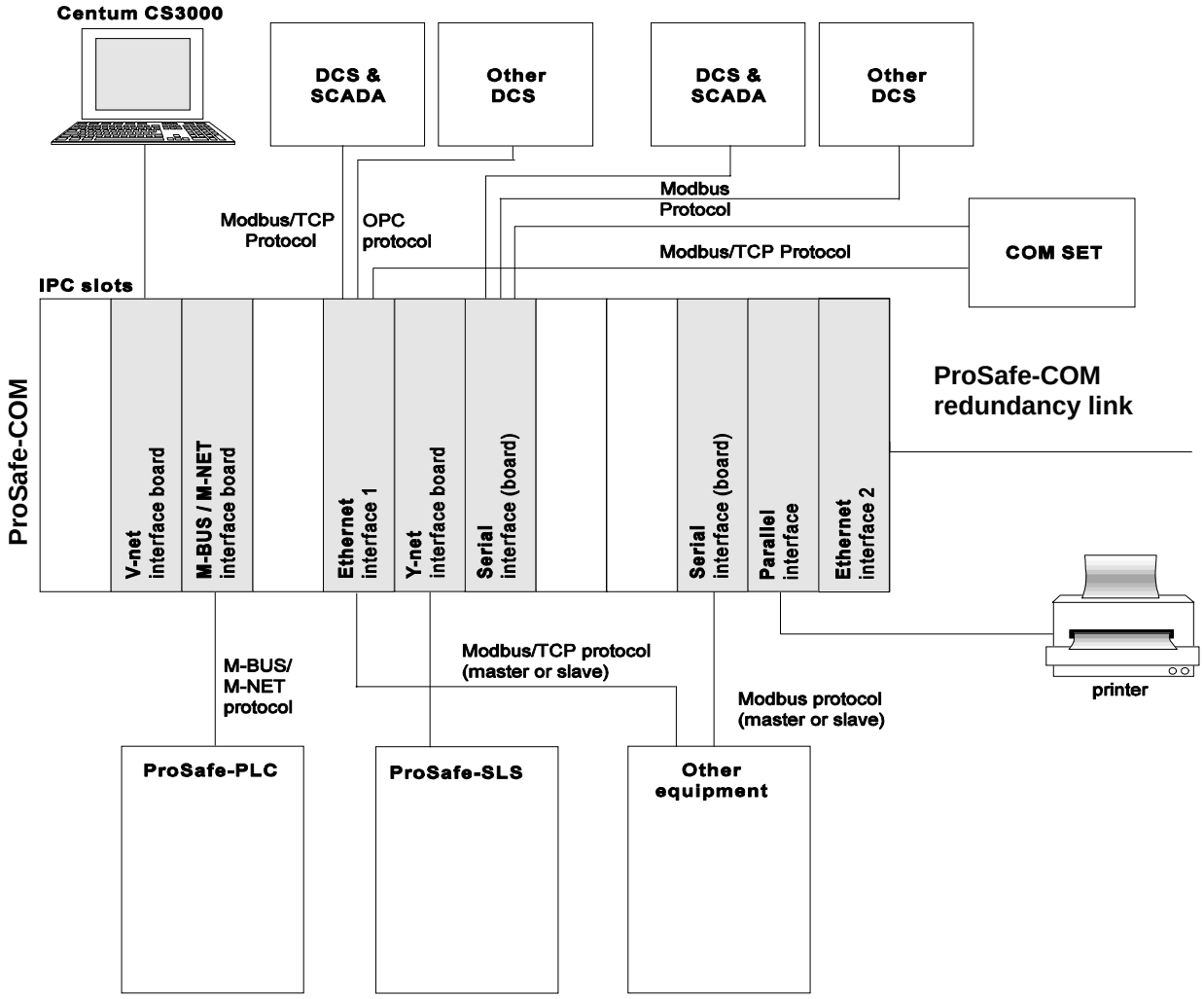

Figure 9: ProSafe-COM interfaces

Printer
If requested a matrix line printer can be connected, for local event printing and assistance to troubleshooting. This printer can also be connected to another computer, provided that ProSafe-COM is connected to the other computer via Ethernet.

User interface

ProSafe-COM can be used without user interface (VDU / keyboard / mouse). The user interface then consists of LEDs on various modules. LEDs give a quick indication of the status and functioning of the system.

V-net interface

V-net is the connection from ProSafe-COM to CENTUM CS3000 / VP. ProSafe-COM has maximally 1 V-net interface.

M-BUS/M-NET interface

The M-BUS/M-NET interface (maximally 4) connects ProSafe-COM to the ProSafe-PLC.

Ethernet interface

The 3 Ethernet interface(s) of ProSafe-COM serve the following purposes:

- Connection to a local network for easy configuration and engineering
- Connection to OPC clients
- ProSafe-COM redundancy link (usually a dedicated Ethernet link, not used for other protocols)
- Connection to ProSafe-COM SET on an engineering PC via Modbus/TCP, for configuring, monitoring and maintenance
- Connection to external equipment (foreign PLC) using Modbus/TCP (either Modbus master or slave)
- Connection to a computer that runs the I/O emulator (EmuTool)

Serial interface

The serial interfaces of ProSafe-COM are used for the Modbus RTU protocol.

ProSafe-COM can have maximally 10 serial interfaces. Four COM ports are available in the standard ProSafe-COM, additional COM ports can be installed using a PCI board.

Connection with a Modbus RTU protocol can be used for:

- Connection to DCS systems other than CENTUM CS3000 / VP
- Connection to other PLCs than the ProSafe-PLC (ProSafe-COM can be both Modbus master or Modbus slave)
- Connection to an engineering PC, for configuring, monitoring and maintenance with ProSafe-COM SET

Y-net interface

The Y-net interfaces of ProSafe-COM are used for the connection of ProSafe-SLS safety systems.

ProSafe-COM can have maximally 2 Y-net interfaces
Y-net is a high speed RS-485 network

Redundancy

An overview of the current status of the ProSafe safety system and of the sequence of events in the guarded process can be of utmost importance for the process operator. Therefore, ProSafe-COM can have single or redundant configurations. A redundant (hot standby) configuration, with doubled components and connections, gives an even higher availability than a single ProSafe-COM configuration.

2 ProSafe-COM functions

2.1 Basic function

The basic function of ProSafe-COM is to exchange data. The term data covers both events and tag status information.

Events are signal changes with the changing time. Events inform about what has happened sequentially. An event can trigger a logic function, if defined so within ProSafe-COM SET.

Status of a *tag* informs about the installation situation. Tag statuses are used for both detection and overrides. A tag can be read, but some can also be set. Setting a tag is sometimes necessary for start-up or maintenance overrides.

Events can be transferred only *upwards*: from ProSafe safety system to ProSafe-COM and further to other systems.
Tag statuses can be transferred *upwards* and *downwards*: from the ProSafe safety system to ProSafe-COM and to the DCS, or the other way round.

Figure 9 shows the information flow of ProSafe-COM with its surrounding systems.

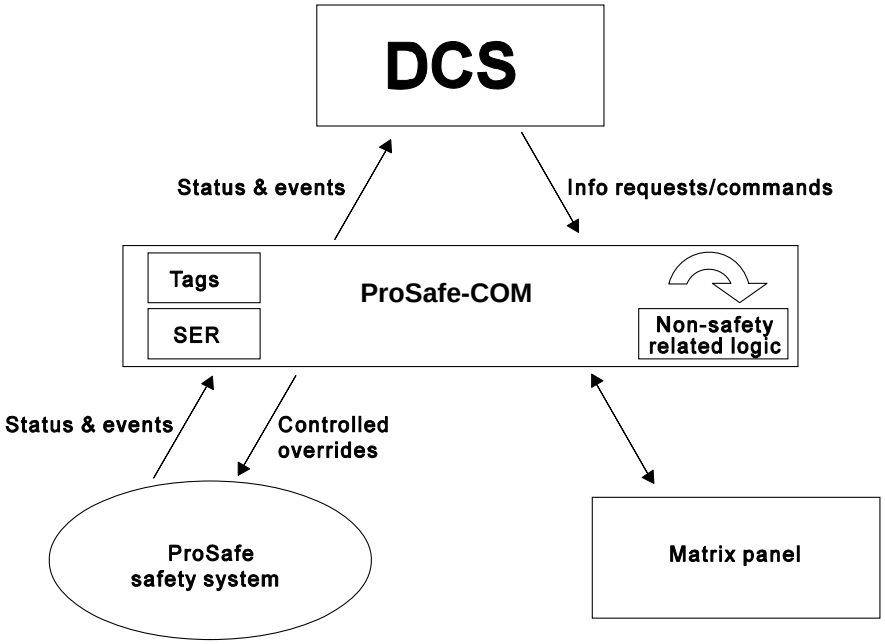

Figure 10: Information flow of ProSafe-COM with surrounding systems

The basic function of exchanging data can be subdivided into:

- Status acquisition
- Sequence of events recording, SER
- Forcing statuses, i.e. override facilities

2.2 Status acquisition

A DCS system is a typical *master* / *slave* application (see figure 11). The master determines when and what kind of information is needed. The slaves only give information on request of the master. In the communication between a DCS system and ProSafe-COM, the DCS system is the master and ProSafe-COM is the slave. In the communication between ProSafe-COM and the ProSafe safety system, ProSafe-COM is the master and the ProSafe safety system is the slave.

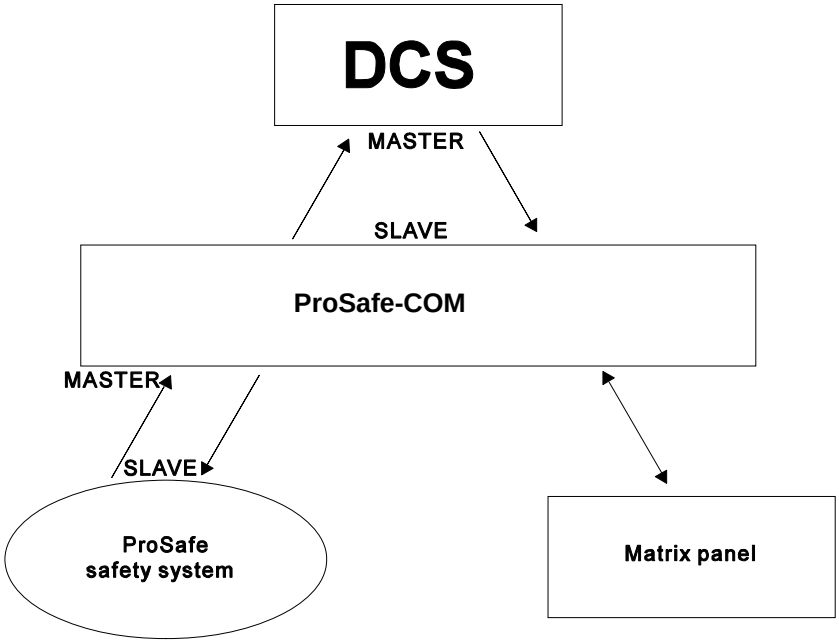

Figure 11: Status acquisition and master-slave relations

In a DCS system an operator can get status information of the actual situation of the ProSafe safety system. ProSafe-COM retrieves the status of the ProSafe safety system, and sends it to a CS3000 / VP when requested. Event information (time-stamped status changes) is automatically sent to the CS3000 / VP. To other DCS or SCADA systems, the event information is only sent on request of the DCS system. For example: an OPC A&E client or a Modbus master station must actively request event information from ProSafe-COM.

Status information can be represented in two different ways: digital and analogue. Digital data can be represented in the form of bits (Boolean: output is true or false). Analogue data can be presented in several formats. Some modules of the ProSafe safety system use digital status acquisition, others use analogue status acquisition.

ProSafe-COM supports a functionality called “soft marshalling”. It means that a DCS can access a tag using a logical address which hides the actual physical address of the tag in the safety system. The match between the physical address and the logical address is configured in the ProSafe-COM tag list.

ProSafe-COM tags are by default read / write accessible (except for certain ProSafe-COM diagnostics tags). However, it is possible to configure tags as read-only for additional security.
The DCS and ProSafe-COM logic cannot write the tag anymore. Another possibility is to define a tag as “read-only for DCS, but read / write for ProSafe-COM logic”.

2.3 Sequence of events recording

It is essential for safeguarding systems to monitor start-up and shut-down procedures in real system time and record these events for later analysis. The SER provides just that 'black box' function, which makes it possible to retrieve and analyse the events associated with a particular process situation.

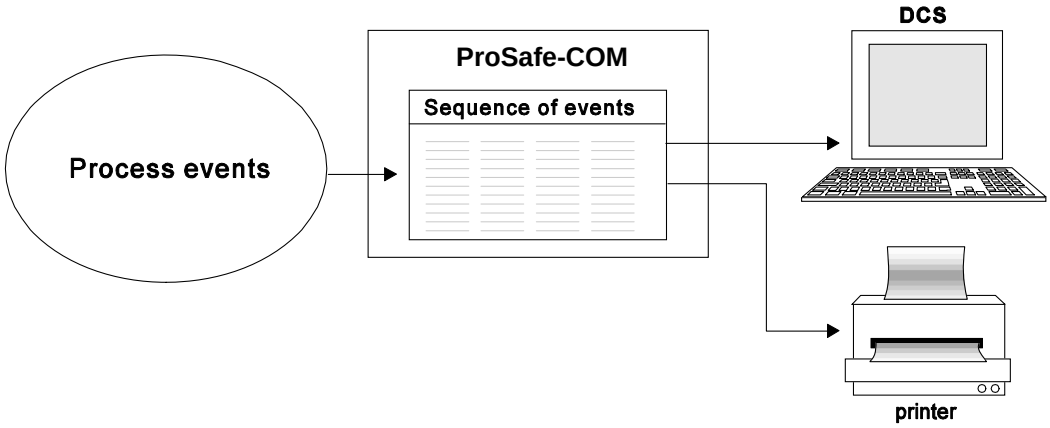

Figure 12: Sequence of events recording

All data is communicated with other members of the ProSafe family or a 'host' system. Many interfaces are available using proprietary protocols as well as industry standards.

ProSafe-COM maintains an event list in memory. All ProSafe safety system events are kept and sorted on time stamp. This list can be printed or made available to the process engineers for thorough process investigations or analysis of process shutdown sequences. The event time stamps of the ProSafe safety system digital field I/O have a resolution of 1 millisecond, sequence of events can be guaranteed with accuracy in the order of 10 to 20 msec.

The size of the event list is configurable, with a maximum of 10.000 events. The most recent events are saved on disk and can be inspected after a recovery from a power-down situation. Maximal 10% of the available events will be stored on disk. For example, if the configured event list in memory is 10.000 events long, then 1000 events will be saved on disk during a power outage.

2.4 Forcing statuses

A ProSafe safety system works autonomously. However, in start-up and maintenance procedures overrides may be necessary. By using overrides, situations that are normally faulty can be temporarily ignored by the ProSafe safety system.

In case of a start-up procedure, an override may be necessary in order to put the ProSafe safety system to work. When an override is set, the values read via the I/O modules are temporarily ignored in order to proceed. If no override is used, the start-up procedure probably will be terminated immediately because a situation occurs that is not normally allowed.

When the process has started up properly, the override procedure can be terminated and the I/O will be checked again in the normal way.

A maintenance override is necessary to temporarily disable the I/O that can activate a shut down. This may be necessary when testing or maintaining the ProSafe safety system.

Override procedures always require a double action: a manual enable with a key, and an override command from e.g. a DCS or matrix panel.

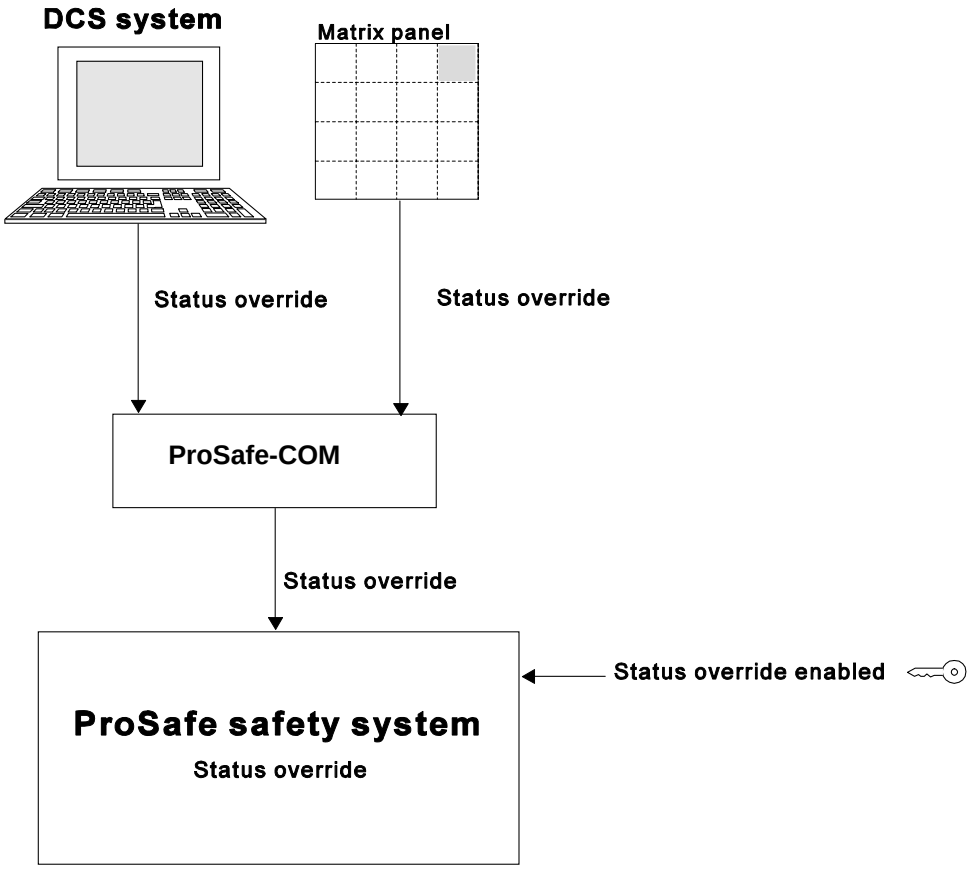

Figure 13: Forcing status

The override can be switched off manually by a system operator. But a logic program can also automatically reset the override. The latter is more secure and has more possibilities. The logic file of ProSafe-COM can be configured to automatically end overrides after a certain time or in case of a certain condition. The logic file can also limit the number of overrides that can occur simultaneously.

2.5 Configuring ProSafe-COM

The software running on ProSafe-COM must be configured. The functionality of ProSafe-COM and the way it exchanges data can be defined beforehand.

Configuring is done by making three configuration files with the COM SET. These files are compiled and loaded into ProSafe-COM. ProSafe-COM interprets these files at start-up time.

The configuration files are:

- Configuration file
- Tag file
- Logic file

The configuration file and the tag file are mandatory. The logic file is optional.

Configuration file

When the ProSafe-COM executable starts up, it must know its hardware environment. In the configuration file two major hardware groups can be defined:

- Group 1: the hardware of the ProSafe-COM PC itself
  Examples: Availability of a V-net, Y-net or OPC interface, number of COM-ports and their baud rates, presence of a parallel printer, etc.
- Group 2: the layout of the ProSafe-SLS networks and the scan rates of the different modules; the available PLCs on the PLC-network, plus address information of tags in these PLCs. Moreover, the configuration file defines exactly what the scan rates will be for each PLC (network tuning).

Tag file

The communication of ProSafe-COM with other systems is based on tags. A tag is a name for a process variable (a status in the ProSafe safety system).

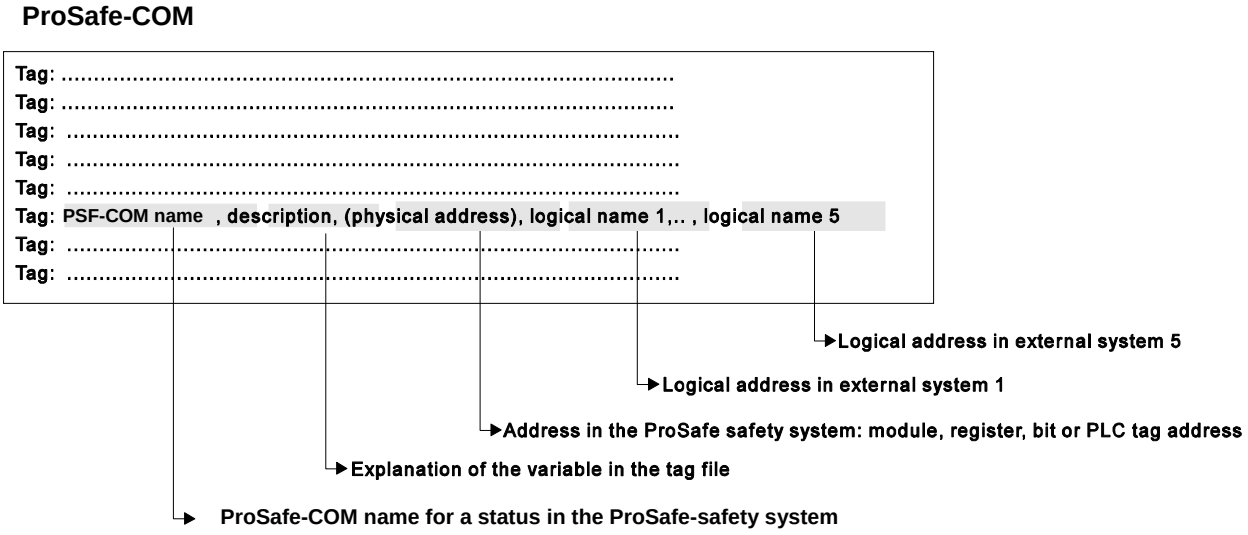

Figure 14: Tag definition

The tag file defines per tag:

- The tag name in ProSafe-COM.
- A description of the variable, for clarification in the tag file
- The physical address.
  The 'original name / addresses' for the process variable. More precisely, the position / definition of the process variable in the safety system. (i.e. ProSafe-PLC or ProSafe-SLS I/O point, etc)
- The logical name of the tag for the different communication channels.
  Each physical address can have 1 up to 5 logical addresses. This is also called 'soft-marshalling'. It means that external systems can give their own addresses (and name) to a process variable in the ProSafe safety system and are not bothered by the physical position and address of the actual tag.
- Event filtering.
  It can be defined per communication channel and per tag if events must be transferred.
- Analogue scaling, in various types.
  Analogue values can be scaled to values that are common in the DCS or external equipment. Scaling goes per tag and per communication link.
- Write boundary values (minimum and maximum value that can be written)
- Read / write or read-only accessibility

Tags are not only the purely hardware related points (I/O modules). Tags can also be software related items in ProSafe-COM. For example, the status of the modules of the ProSafe-PLC can be tags. Other examples are the network load, or the settings of the communication parameters of the serial communication lines. These tags are referred to as “diagnostics tags” or “system tags”.

All tags must be defined in the tag file before the tags are externally accessible or usable in the ProSafe-COM logic program.

Tags can be read but they can also be written (depending on the accessibility attribute in the tag file). A DCS or other external equipment can force the status of a certain tag, or group of tags. ProSafe-COM directly communicates with the appropriate modules via the M-BUS/M-NET, Y-net or Modbus links and sets the outputs of the modules.

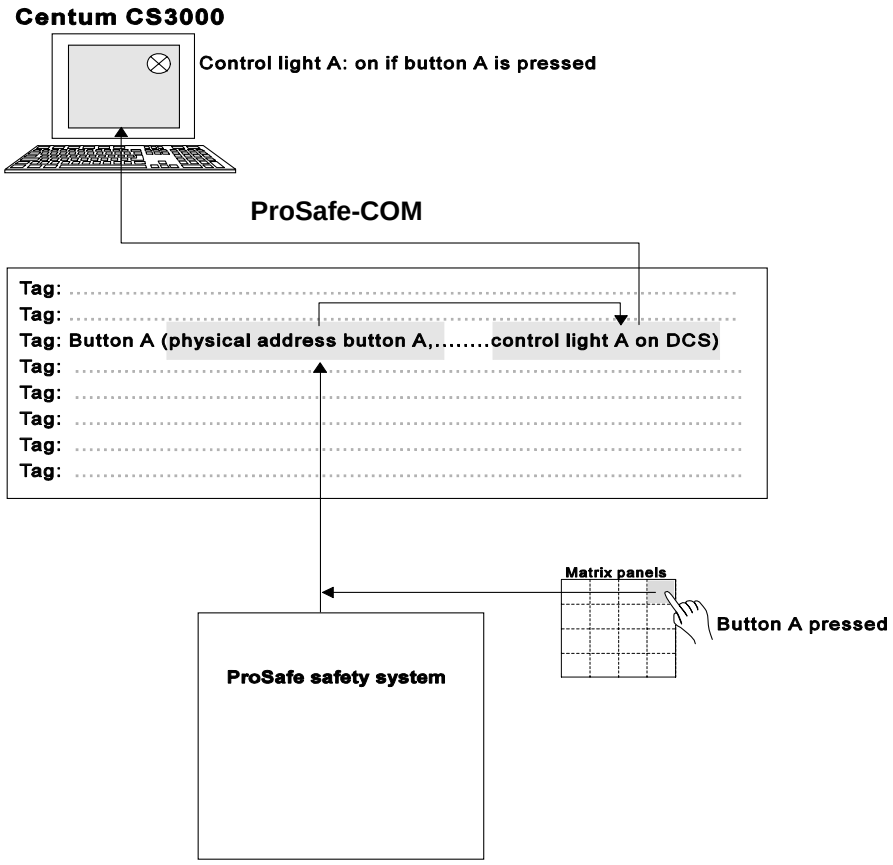

Figure 15: Communication with tags

Tag file and event filtering

Event information can be read via the external communication lines of ProSafe-COM. ProSafe-COM offers the possibility to define event filtering per communication line and per tag, because different external systems probably will be interested in different sets of events. So a ‘next event’ request via one communication line can return an event, while the same request via another communication line yields nothing, because the event is filtered for that communication line. This facility is configured in the tag file.

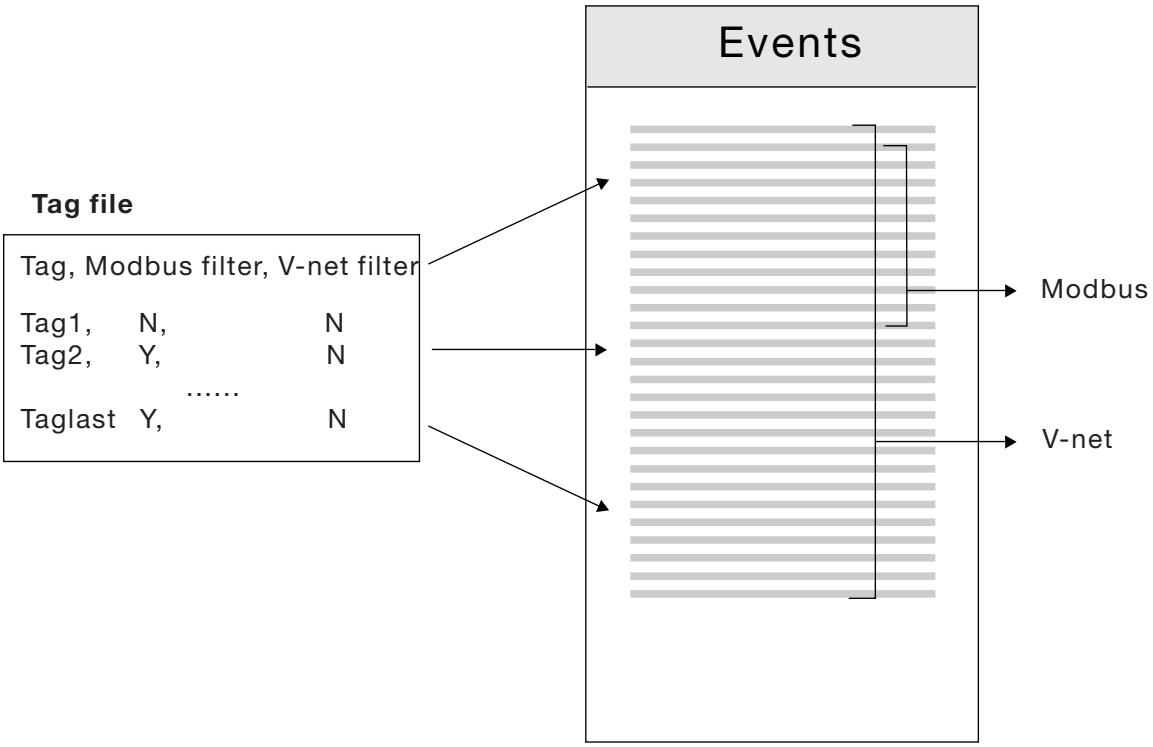

Figure 16: Tag file and event filtering

Logic program file

ProSafe-COM has the ability to execute a logic program, just like a PLC. It reads inputs, performs logic (an application program) and writes outputs. The inputs can be virtually anything. For example the status of tags in the ProSafe safety system, inputs from the matrix panel push buttons, the current status of any output, arithmetic calculations, or the status of a local ProSafe-COM tag that is set externally via a DCS command. The logic program can logically combine all these inputs and write the result to any output (provided that the output tag is not defined as read-only type).
COM SET supports almost the entire set of logical and arithmetic operations that is common in modern programming languages. The source program is written as an ASCII text file. The syntax strongly resembles that of the modern programming languages.

3 ProSafe-COM hardware

3.1 Hardware concept

ProSafe-COM comes as an industrial PC with flash disk. Use of a desktop PC is not recommended due to worse specifications and short PC's life cycle. ProSafe-COM can easily be expanded with additional modules to fit any client's specification. An extensive set of modules is available, ranging from various types of I/ O boards to various interface boards.

This chapter discusses the various hardware components of ProSafe-COM. It also describes the modules required at the ProSafe safety system side for communication, and the modules required for matrix panels.

3.2 19 inch housing with modules

The industrial PC version of ProSafe-COM is a 19 inch rack chassis with built-in single board computer. PCI bus interface boards can be plugged into the 4 spare PCI slots. The IPC comes in two versions: one version with four 2.1 version PCI slots (3.3. and 5 V support). The second type has three 2.1 PCI slots and one PCI-E slot. The PCI-E slot is needed to house the CENTUM VF702 interface board.

Figure 17: ProSafe-COM IPC

ProSafe-COM can have the following modules:

- Max. 1 V-net interface board (VF701 in 2.1 PCI slot or VF702 in PCI-E slot)
- Max. 4 M-BUS/M-NET interface board (in version without PCI-E slot)
- A serial interface board with maximally 8 connections (a maximum of 10 COM ports is supported, including the four on-board COM ports)
- Max 2 Y-net interface boards

3.3 Main board

The main board is the Central Processing Unit (CPU) of ProSafe-COM. It executes the ProSafe-COM software.
Characteristics of the IPC version are:

- Celeron M 1.0 GHz
- Up to 1 GByte ECC RAM
- Built-in serial RS-232 (4), parallel (1), USB 2.0 (2) and Gigabit Ethernet (3) interfaces
- SATA interface for 16 Gigabyte flash disk
- Monitor (DVI-I), PS/2 keyboard and mouse

3.4 V-net interface board

The V-net interface board is used to enable communication between the CENTUM CS3000 / VP system and the ProSafe-COM. V-net is a token-bus network and forms the backbone of the CENTUM CS3000 / VP DCS.

3.5 M-BUS/M-NET interface board

The M-BUS/M-NET interface is used for communication between ProSafe-COM and ProSafe-PLC. A PCI interface board is available for either M-BUS or M-NET.
The M-NET interface provides the same functionality as the M-BUS interface, but supports longer distances and greater ProSafe-PLC configurations.

3.6 Ethernet interfaces

An Ethernet interface has the ability to run several concurrent protocols at the same time. Therefore it can be used for different types of communication.

Ethernet connections can be used for:

- Connecting ProSafe-COM to the customer's network during project engineering.
- First-line maintenance, revision management, solving bugs and software upgrading.
- Connecting ProSafe-COM to a DCS running OPC client software.
- Interconnecting redundant ProSafe-COMs
- Connecting to an engineering PC running the ProSafe-COM SET tool.
- Connecting to a PC running the I/O emulator tool (EmuTool)
- Connecting external equipment (i.e. foreign PLCs) via the Modbus/TCP protocol.

3.7 Serial interface board

ProSafe-COM has a number of serial communication ports (COM-ports). Up to 10 ports can be available, four of which are integrated in the IPC's single board computer.

The serial ports can be used for:

- Modbus status and event queries (either Modbus master or Modbus slave).
- Connection to the ProSafe-COM SET

3.8 Y-net interface board

ProSafe-COM can be equipped with the Y-net interface. Up to 2 interfaces can be available.
The Y-net interfaces are used for:

- Connection of a ProSafe-SLS safety system
- Connection of an operator's matrix panel

3.9 ProSafe-COM and ProSafe safety system modules

Specific modules are used for the communication between ProSafe-COM and the ProSafe safety system.

Because the functioning of ProSafe-COM strongly depends on these modules, these modules are discussed in this *System overview*. Note however that these modules are not part of ProSafe-COM itself.

ProSafe-COM directly communicates with the following modules in the ProSafe safety system:

Table 2: ProSafe-COM communication modules

Module	Application	Module Function
CCM	ProSafe-PLC	PLC central processing unit
MBX	ProSafe-PLC	PLC M-NET interface unit to M-BUS
MC-562 / MC-573 / MC-576	ProSafe-SLS	Analogue input / Digital input / Digital output
MI-983 / MO-986	Matrix panel	Matrix panel input / Matrix panel output
Serial interface supporting Modbus slave (ProSafe-COM is Modbus master)	Foreign PLC or auxiliary equipment	Tag (status) interface
Ethernet interface supporting Modbus/ TCP slave (ProSafe-COM is Modbus master)	Foreign PLC or auxiliary equipment	Tag (status) interface

ProSafe-PLC: CCM-module

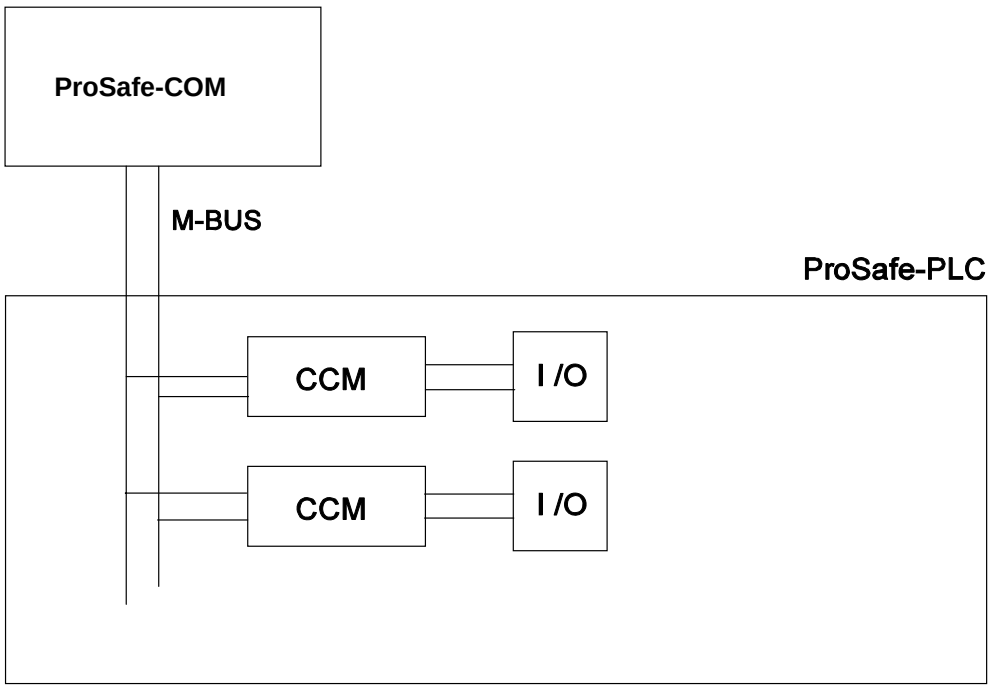

Figure 18: ProSafe-PLC: M-BUS and CCM modules

The Critical Control Module (CCM) is the Central Processing Unit of the ProSafe-PLC. It communicates with ProSafe-COM via M-BUS or M-NET. The CCM module performs the actual control in the ProSafe-PLC. Through the PLC I/O modules, it retrieves values from the inputs and sends appropriate signals to the outputs. The MBX module is the intermediate between ProSafe-COM and the M-BUS.

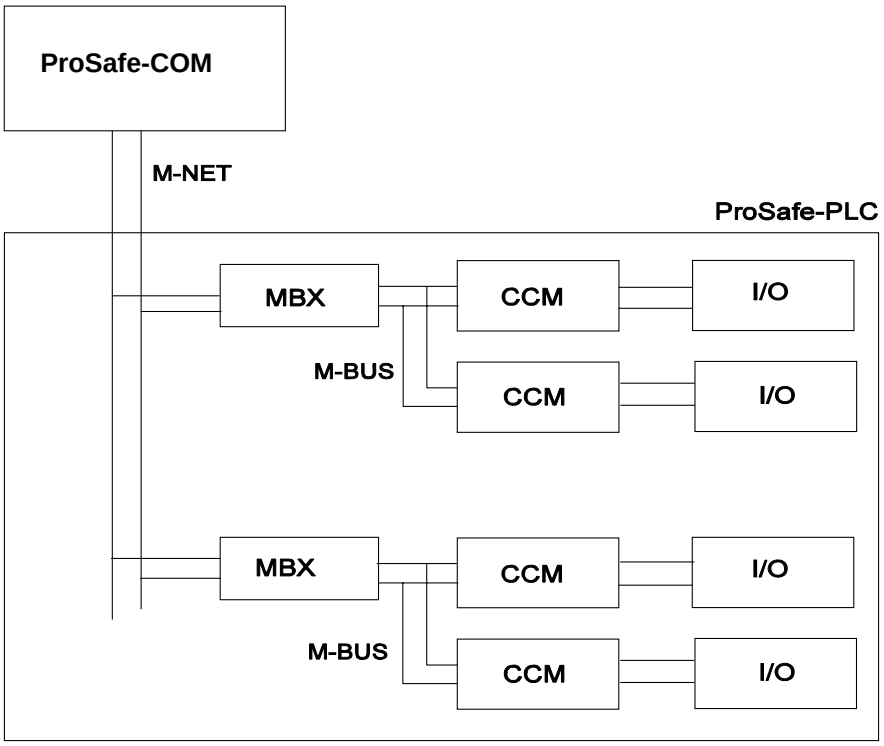

Figure 19: ProSafe-PLC: M-NET, MBX module and CCM modules

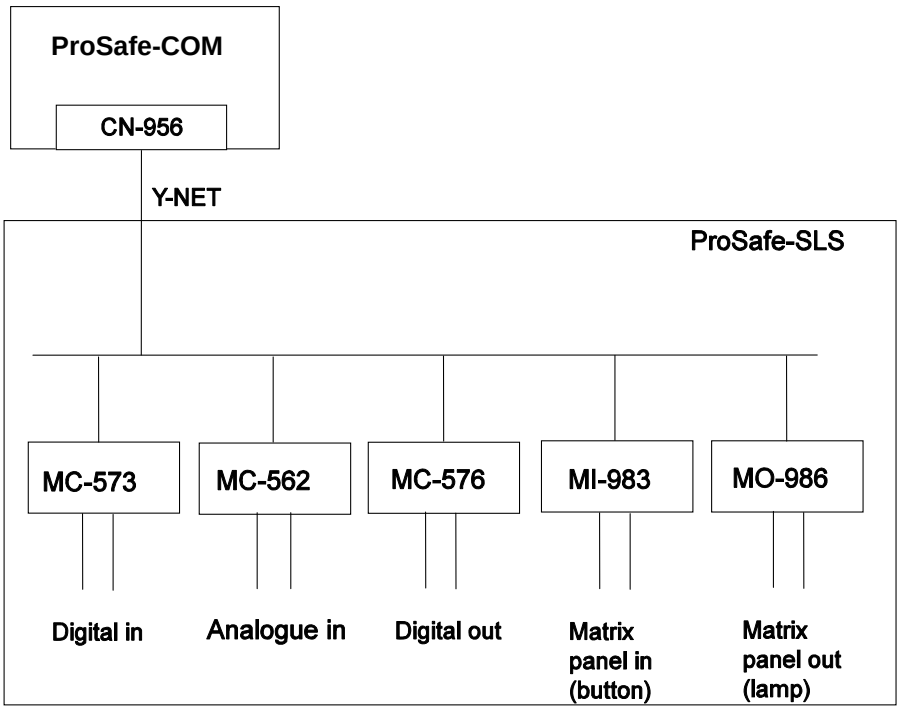

Figure 20: ProSafe-SLS: Safety system and matrix panel connections

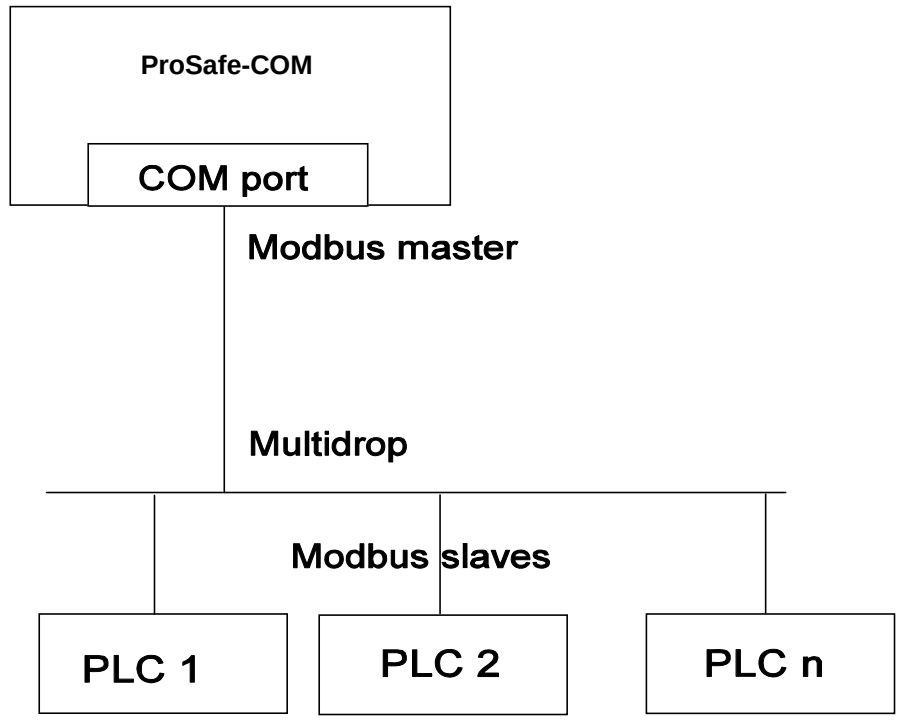

Figure 21: ProSafe-COM as Modbus master in a network with Modbus slaves

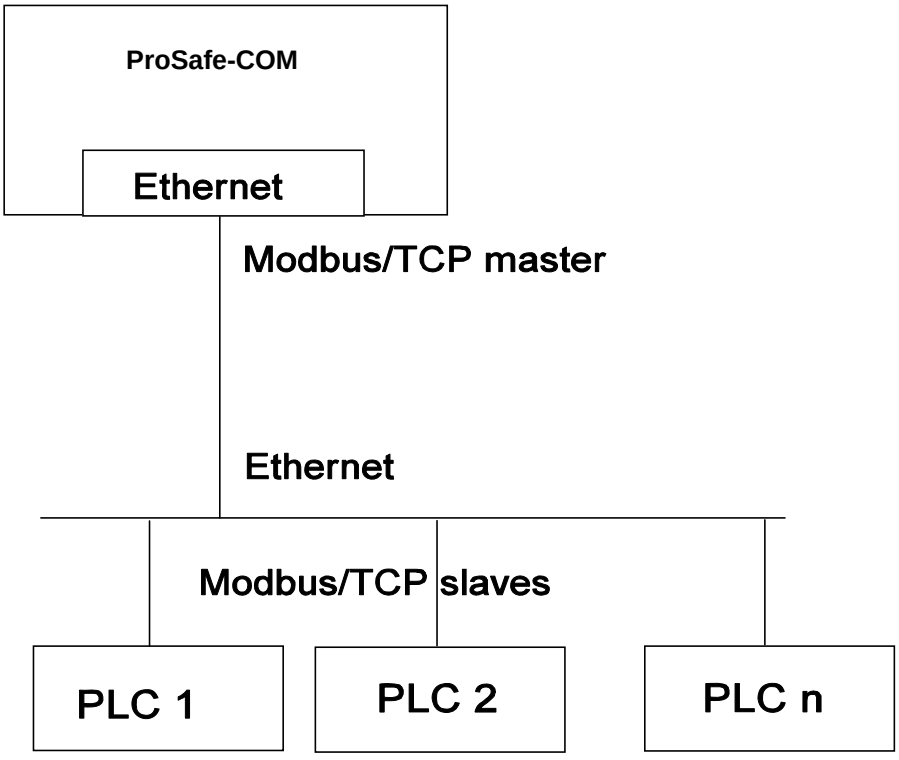

Figure 22: ProSafe-COM as Modbus/TCP master in a network with Modbus/TCP slaves

4 ProSafe-COM interfaces

4.1 Access to status map and event list

The ProSafe-COM interfaces give access to the status map and event list in ProSafe-COM. Statuses and events can be viewed. Statuses of ProSafe-COM outputs can also be changed, e.g. in case of overrides.

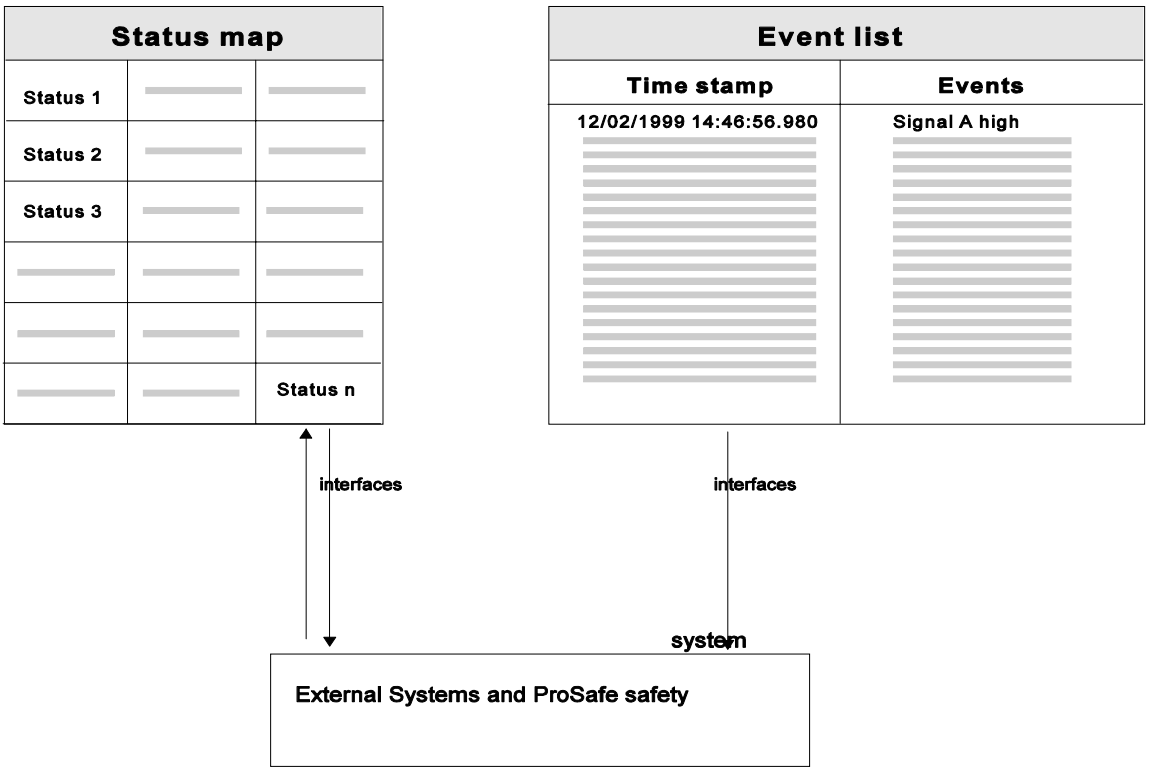

Figure 23: Interfacing ProSafe-COM

This chapter describes the interfacing of ProSafe-COM.

For each interface is described:

- Function (interface to what)
- Hardware provisions
- Characteristics (features of the way the interface works)

4.2 Printer

Function

Events, or a predefined selection of events, can be printed. Furthermore, diagnostic and error information can be printed. This helps maintenance and troubleshooting. Statuses (actual values of tags) can not be printed.

Hardware provisions

The printer is connected to the parallel interface port. The matrix printer can be connected to another computer in the network. ProSafe-COM must then be able to contact the other computer via the network (Ethernet).

Characteristics

- A printer is especially useful when ProSafe-COM is used locally, without connection to an external system like a DCS.
- With the tag file and configuration file, it can be set which events are printed. This requires ProSafe-COM SET. There is no interactive setting of what can be printed.
- System error messages (malfunctions in ProSafe-PLC , ProSafe-SLS or ProSafe-COM modules, etc.) can be printed. Error messages can easily be interpreted and help an operator, engineer or service personnel with fixing problems.
- The printer is a local printer, directly connected to ProSafe-COM's parallel port or to the parallel port of another computer in the network. Only line printers are supported.

4.3 User interface

The various modules and components in the ProSafe system have LEDs. LEDs give a quick indication of the proper functioning of the network and fault situations. In ProSafe-COM, the V-net board, Y-net board and Ethernet connections have LEDs.
A keyboard, mouse and VDU can be connected optionally.

4.4 V-net interface

Function

To make communication possible between the CENTUM CS3000 / VP system and the ProSafe safety system, a V-net interface is used.

Hardware provisions

- V-net interface board, PCI board (VF701)
- Thin Ethernet cable (10Base2)
- Maximum distance of a segment: 185 meters
- A maximum of 2 InterRepeater Links (IRL) is allowed between devices; maximum cable length is 925 meters
- V-net/IP interface board, PCI-E board (VF702) connects to a standard Ethernet network.

Characteristics

- V-net is a Yokogawa proprietary product. V-net is the control backbone of the CENTUM CS3000 / VP
- V-net is a token-passing network

- V-net is a redundant bus
- V-net interface complies with IEEE 802.3 / 10Base2
- V-net allows event information to be sent automatically to the CENTUM CS3000 / VP system, without a request from the CENTUM CS3000 / VP
- V-net allows quick reading and sending of status information from and to the ProSafe safety system (e.g. for operator's display updates and override signals)
- V-net/IP has the same characteristics as V-net, but then on a Gigabit Ethernet network

4.5 M-BUS/M-NET interface

Function

The M-BUS/M-NET interface enables data exchange between ProSafe-COM and the data acquisition modules within ProSafe-PLC.

Hardware provisions

M-BUS The M-BUS can be extended up to a maximum of 18 meters, across up to 4 Modulracks.

In M-BUS the maximum allowable combined Standard MBI Cable and Extension Cable length used to connect PCs (ProSafe-COM, ProSafe configuration) to the M-BUS is 168 m.

M-NET If the maximum allowable combined Standard MBI Cable and Extension Cable length exceeds 168 meters and more than 4 PLC racks are used, an M-NET interface is necessary. In M-NET, the whole network has a maximum bus distance of 914 m.

Characteristics

- Redundant Token passing interface
- Status acquisition, sequence of events recording, and forcing statuses.

4.6 Ethernet interface

Function

The Ethernet connection enables communication using standard network protocols supported by Windows 2000.

Hardware provisions

- UTP class 6 Ethernet cables are needed to achieve the 1 Gigabit bandwidth.

Characteristics

- Used for connection of OPC clients (DCS).
- Used as interlink in redundant ProSafe-COM configuration.
- It can be used to connect to a company's network to enable simple file transfer during the engineering phase.
- Used to connect to an engineering PC running COM SET using the Modbus/TCP protocol.
- Used to connect to a PC that runs the I/O emulation (EmuTool).
- Used to connect to foreign equipment using the Modbus/TCP protocol (either Modbus master or slave).

4.7 Serial interfaces

Function

A serial connection enables Modbus communication (master or slave) with other DCS systems, ProSafe-COM SET and other equipment.

Hardware provisions

An RS-232 connection, the baud rate can be set up to 57600.

Characteristics

- Supported protocol: Modbus RTU.

  A serial interface using a Modbus RTU protocol can be used to:
  - communicate with DCS systems other than CENTUM CS3000 / VP (ProSafe-COM is Modbus slave)
  - communicate with COM SET for configuring and monitoring (ProSafe-COM is Modbus slave)
  - interrogate any piece of equipment with Modbus slave interface (ProSafe-COM is Modbus master)

  To make communication possible, a combination of function and exception codes is used. A function code tells the slave what kind of command the master has given. E.g. one function code tells the slave to give data from a module; another will tell the slave to force an output. Exception codes give information about the message itself.

Table 3: Supported Modbus codes

Supported function codes (standard)	*Supported slave function codes (not standard)*	*Supported exception codes*
Read coils (01, 02) Read registers (03, 04 *) Force single coil (05) Force single register (06) Loopback test (08) Force multiple coils (0F) Force multiple registers (10 *).	Upload (63) Download (64) System reset (41) etc.	Illegal function (01) Illegal data address (02) Illegal data value (03) Failure in associated device (04)

Note *: Multiple read/write register function codes are used to transport 32-bits (single precision) floats in ANSI/IEEE Standard 754-1985 format. Both the standard and Modicon PLC type are supported.

4.8 Y-net interface

Function

The Y-net interface enables data exchange between ProSafe-COM and the data acquisition modules within ProSafe-SLS. Furthermore the matrix panel controllers can be connected to the same network.

Hardware provisions

Y-net The Y-net can support up to 120 I/O modules. Modules for safety system I/O and matrix panel control can be mixed.
The Y-net is divided in segments; each segment can contain 32 modules.
The segments are separated by bus repeaters. Either fibre optic or standard bus repeaters can be used and concatenated. Distances up to 15 km are possible.

Characteristics

- RS-485 communication
- Status acquisition, sequence of events recording, and forcing statuses

5 Functions and hardware design

5.1 Realisation of functions

This chapter details how the three basic functions of ProSafe-COM are realised in the ProSafe-COM hardware. The three basic functions of ProSafe-COM subsequently reappear in this chapter:

- Status acquisition
- Sequence of events recording
- Forcing statuses

5.2 Status acquisition on M-BUS / M-NET

A status informs about the installation situation. Statuses are used for both detection and overrides. To inform a DCS system about the installation situation, a status of the safety related systems can be read. In an M-BUS / M-NET configuration the status of the ProSafe-PLC can be scanned at regular time intervals.

Two kinds of status data can be collected:

- Digital data
  Typically the Critical Discrete Module (CDM) will execute the digital data acquisition and overrides
- Analogue data
  Typically the Critical Analogue Module (CAM) will perform the Analogue status acquisition.

This paragraph describes some more details of this mechanism for the ProSafe-PLC safety system.

For each ProSafe-PLC I/O-bus, one CCM and a maximum of 39 I/O modules can be connected. The CCM scans all the status information of the connected I/O modules. ProSafe-COM scans all CCMs connected through M-BUS / M-NET.
The scan time of the ProSafe-COM scanning the ProSafe-PLC systems can be configured to be different for each CCM. Typically the scan time of the ProSafe-COM is equal or greater than the scan-time of each CCM connected. A scan yields a list of changed tags. ProSafe-COM only retrieves status of changed tags to achieve quick access and low network load.

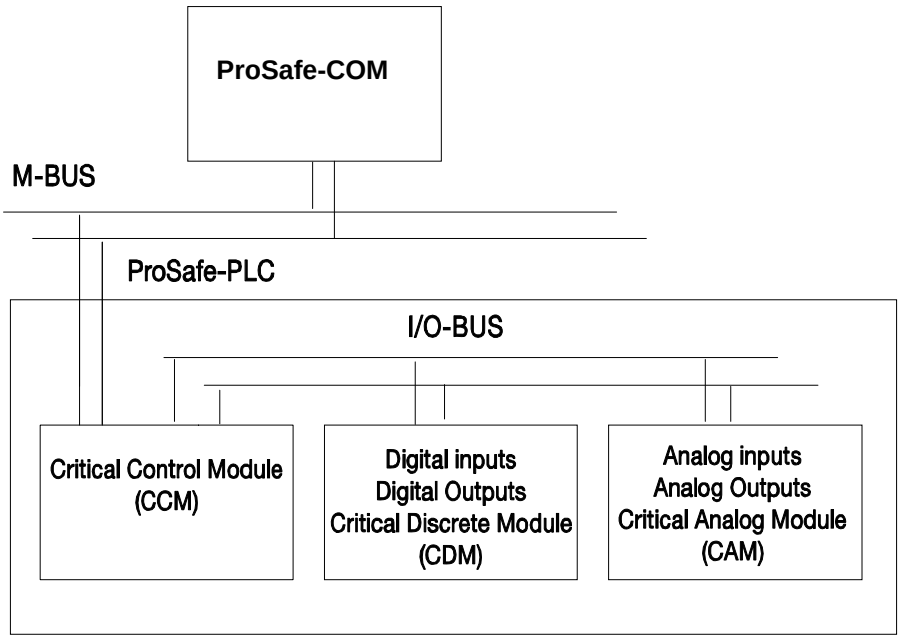

Figure 24: ProSafe-PLC status acquisition modules

5.3 ProSafe-PLC event storage

In a ProSafe-PLC safety system, events are stored with a milliseconds resolution, which yields a very good understanding of cause and effect.
In the ProSafe-PLC safety system, discrete events are recorded in the CCM (Critical Control Module).

The discrete events can have a variety of sources: field inputs (or outputs), CCM logic, foreign devices that communicate with the CCM via the serial ports (e.g. a Modbus PLC), and any device that communicates with the CCM via the M-BUS and M-NET.

There are two main methods of Sequence of Events (SOE) Recording: control module resolution recording and higher speed I/O module resolution recording. When the CCM is the source of the events, the resolution of the event recording is subject to the scan rate of the CCM (typically 100-500 ms). When the source of the events is exclusively field I/O, the CDM (Critical Discrete input/output Module) can sense the events at 1 ms resolution, and report those events to the CCM.
In either case, the list of recorded events is stored in the CCM using special SOE function blocks.
The ProSafe-COM will retrieve the event information from the CCM. Both I/O module and control module resolution SOE functions can be used simultaneously in a CCM.

In the case of I/O module resolution recording, the CDM senses the events and sends them to a Sequence of Events Recorder (SOE_REC) function block in the CCM for recording. The CDM has a large circular buffer (up to 1000 events per channel), so many fast-occurring events can be stored while the SOE_REC block retrieves them at a slower rate. Each SOE_REC block communicates with one CDM; when the CDM module senses a new event (or events) the event information is sent to the SOE_REC block. The SOE_REC block stores the events in a circular buffer of its own: a string array variable configured as an input of the SOE_REC block.

This string array is read by the ProSafe-COM. After all events have been read the array is cleared.

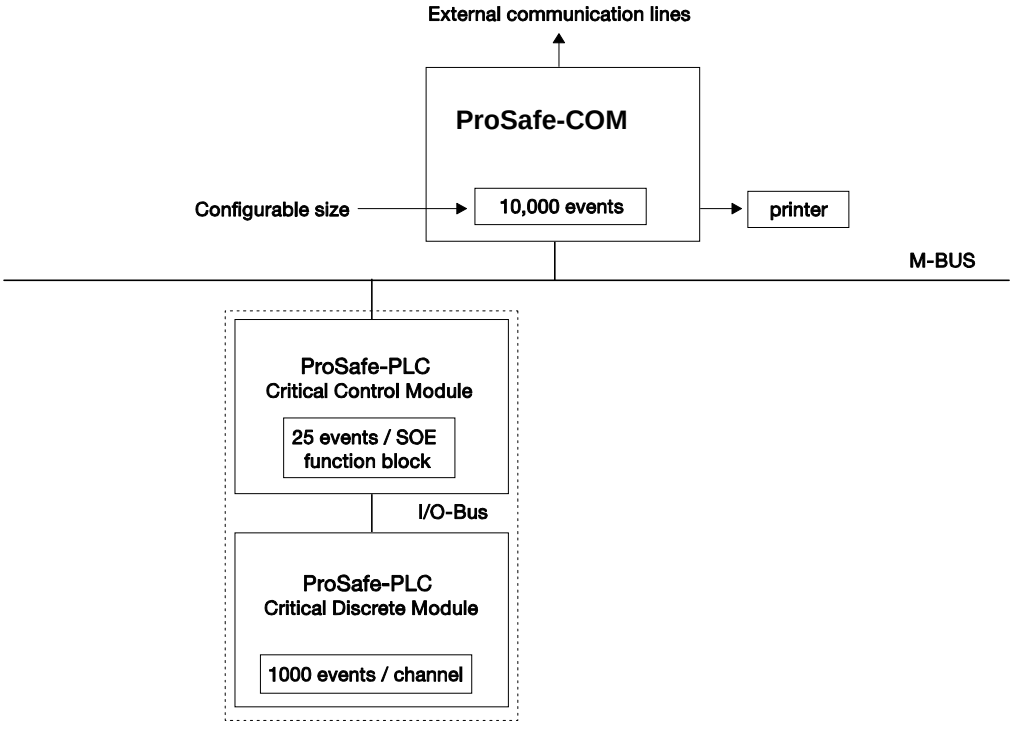

Figure 25: ProSafe-PLC event list concept

5.4 ProSafe-PLC forcing statuses

ProSafe-PLC has software facilities to enable forcing statuses.
The Fail-safe enable is typically connected to an input channel of a CDM. This input will typically be linked to logic in the CCM (basically a logical AND gate) to which also the override output from the ProSafe-COM is connected (originating from external communication lines)
The CCM is connected to the M-BUS and receives write commands from the ProSafe-COM. The following picture gives an impression:

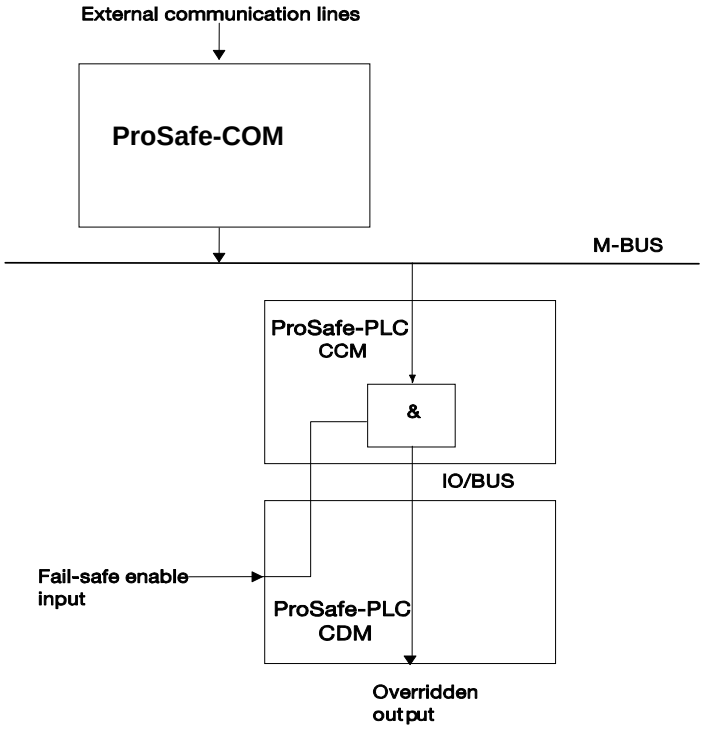

Figure 26: Override facility in ProSafe-PLC

5.5 Status acquisition on Y-net

In a Y-net configuration the status of the ProSafe-SLS can be scanned at regular time intervals.

Five different kinds of status data can be collected:

- Digital input data
  The digital input module (MC-573) performs Digital data acquisition.
- Digital output data
  The digital output module (MC-576) executes write commands.
- Analogue input data
  The analogue input module (MC-562) will perform the Analogue status acquisition.
- Matrix panel input
  The matrix panel input controller (MI-983) reads operator's input.
- Matrix panel output
  The matrix panel output controller (MO-986) sets lamp outputs.

This paragraph describes some more details of this mechanism for the ProSafe-SLS safety system.

Each Y-net can support maximally 120 ProSafe-SLS or matrix panel control modules. ProSafe-COM scans all Y-net modules through the Y-net.

The scan time of the ProSafe-COM scanning each Y-net module can be configured to be different for each module. A scan of a full network is typically performed in less than a second.

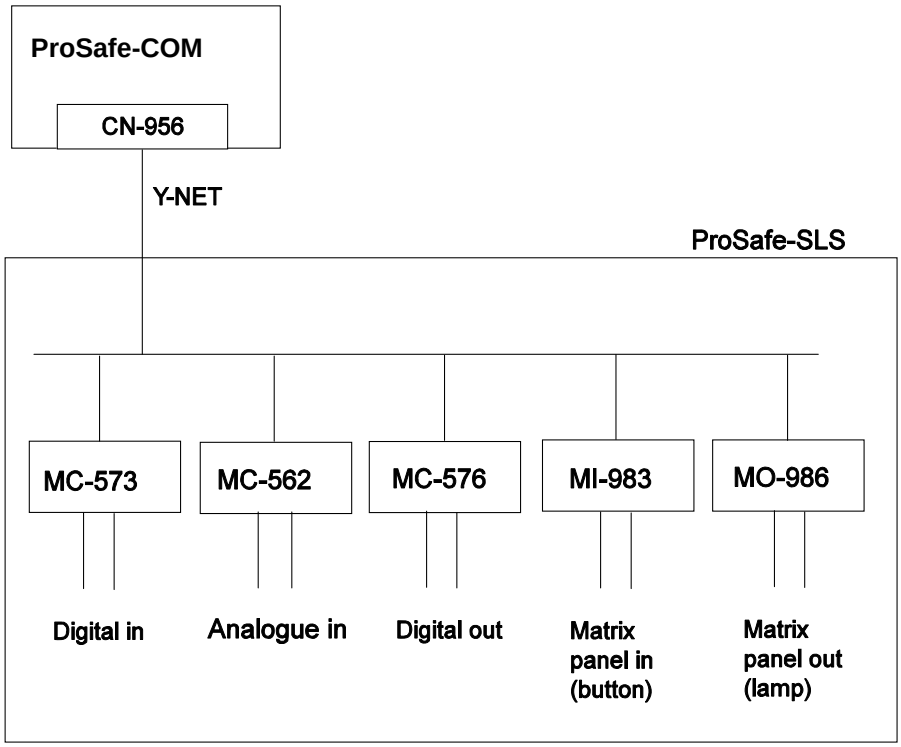

Figure 27: Status and event acquisition in Y-net (ProSafe-SLS)

5.6 ProSafe-SLS event storage

In a ProSafe-SLS safety system, events are stored with a milliseconds resolution, which yields a very good understanding of cause and effect.
The discrete events are stored in the I/O and matrix panel control modules (MC-573, MC-576, MI-983 and MO-986). The analogue input module (MC-562) does not record events.

The I/O modules buffer the events till these are read by the ProSafe-COM Y-net controller. The Y-net controller (CN-956) buffers the events from all I/O modules in Dual Ported Memory. The ProSafe-COM application will retrieve the event information from the DPM and sort the events in the overall ProSafe-COM event list.

5.7 ProSafe-SLS forcing statuses

The digital output module MC-576 can be used to force statuses in a ProSafe-SLS safety system.
The fail-safe enable input of the MC-576 is typically driven by an override enable switch from the safety system. Then it is possible to write maintenance or start-up override signals to the MC-576.

6 Redundant configurations

A ProSafe safety system works autonomously and is fully independent of its communications (apart from start-up and maintenance override situations).

However, an overview of the current status of the ProSafe safety system and of the sequence of events in the guarded process can be of utmost importance for the process engineer. Therefore, ProSafe-COM allows single or redundant configurations.

A redundant ProSafe-COM configuration has double components and/or connections. Communication channels can be redundant, i.e. two Modbus links, or a Modbus link acting as backup of a V-net connection.
It is also possible to use two ProSafe-COM IPCs in a hot stand-by mode.

A redundant ProSafe-COM configuration can be built from the normal hardware components.

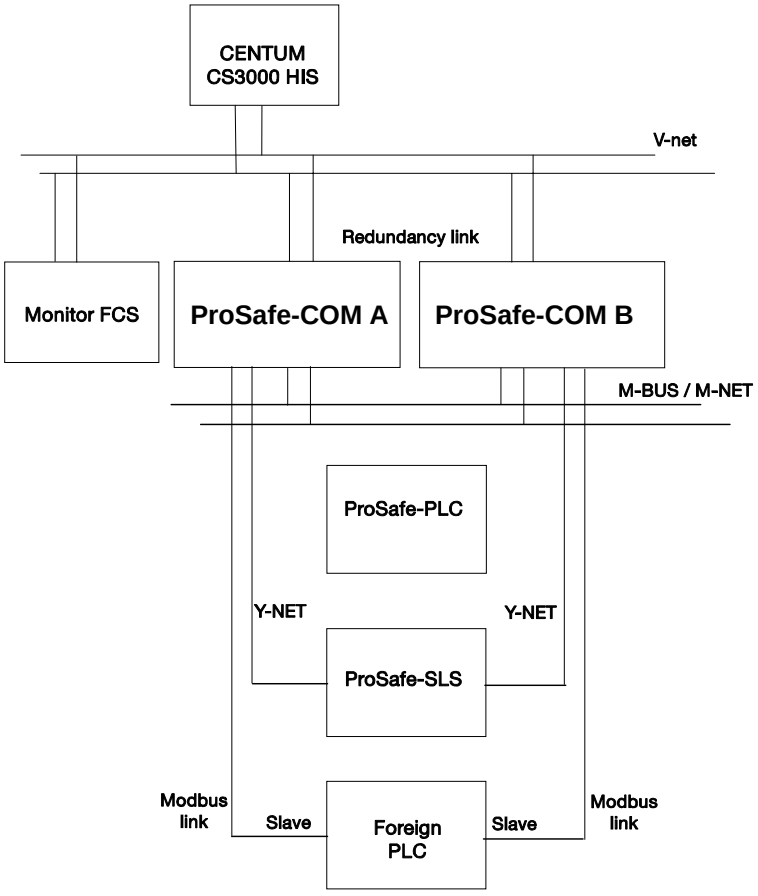

Figure 28: Redundant ProSafe-COM on V-net

Each ProSafe-COM gathers diagnostic information about itself and about its environment. This diagnostic information is available as tags and can be read via the V-net, OPC or Modbus interfaces.
The DCS or SCADA system must decide which ProSafe-COM acts as active and which as back-up. ProSafe-COM has a special tag for redundancy control, which must be written by DCS or SCADA.

A dedicated CENTUM CS3000 / VP software package is available for ProSafe-COM redundancy control.

7 Time distribution and synchronisation

7.1 Realisation of functions

This chapter describes the time aspects in ProSafe-COM. The two basic functions of ProSafe-COM in relation to time are:

- Time distribution
- ProSafe-PLC event time stamp correction

7.2 Time distribution

Function

Within a DCS system data is acquired at multiple locations. Data is acquired by the ProSafe safety system, but also by various other instruments that monitor and control the production process.

Acquired events are time-stamped and stored in the sequence of events list. Both ProSafe-COM and the CENTUM CS3000 / VP DCS system (or other DCS system) record a sequence of events. For these sequence of events to be fully integrated, the time-stamping must be synchronised. Only in an integrated system, synchronised sequence of events causes and effects can be traced back in the right way.

Realisation

Time distribution requires a time master. Other systems must be time slaves to this time master. The time master can be realised as follows:

- When ProSafe-COM is connected to V-net and CENTUM CS3000 / VP, the V-net time master is the time master for ProSafe-COM. ProSafe-COM is the time master for ProSafe-PLC and ProSafe-SLS.
- When ProSafe-COM is not connected to V-net, the time master for ProSafe-COM is the DCS that is connected via Modbus. Again, ProSafe-COM is the time master for ProSafe-PLC and ProSafe-SLS.
- When ProSafe-COM is running stand-alone, then ProSafe-COM is the time master. ProSafe-COM is the time master for ProSafe-PLC and ProSafe-SLS.

7.3 ProSafe-PLC event time stamp correction

Function

Earlier versions ProSafe-PLC (before October 2001) did not support time synchronisation in the millisecond domain between the ProSafe-COM system clock and the CCMs (times could differ seconds). So the events emerging from different CCMs could not be directly sorted in the ProSafe-COM event list. Dedicated event time stamp correction mechanisms of ProSafe-COM compensated for the differences in absolute time in the connected CCMs.
There were two possibilities:
a) ProSafe-COM sent a synchronisation pulse each minute to calculate all CCM clock deviations with respect to the ProSafe-COM clock.
b) A GPS clock provided a sync pulse each minute, which enabled ProSafe-COM to calculate the CCM clock deviations with respect to the absolute time.

The current version of ProSafe-PLC has the possibility (using time sync function blocks) to keep CCM clocks synchronised within a millisecond and all CCMs synchronised with the ProSafe-COM clock within 5 to 25 milliseconds. Event time stamp correction is no longer needed when an accuracy of 25 millisecond is sufficient.

Realisation of the time synchronization pulse mechanism (classical way)

All CCMs receive a common trigger at regular time intervals, either from ProSafe-COM or from an external source (GPS system). The resulting time stamped events enable ProSafe-COM to calculate the correction factor per CCM.
The function is realised as follows:

- One ProSafe-PLC has a dedicated common trigger output that can be controlled (written) by ProSafe-COM (assuming that ProSafe-COM generates the common trigger pulse; an external GPS receiver is the alternative).
- Each ProSafe-PLC has one dedicated input for the event time stamp correction
- Common trigger output and all time stamp inputs are physically connected
- ProSafe-COM or the GPS generates a pulse at a known moment in time
- ProSafe-COM calculates the correction factor of each different ProSafe-PLC after receiving the common trigger time stamped events.
- Future events from all ProSafe-PLCs are corrected with the calculated time differences.

Realisation using the time synchronization function blocks in the ProSafe-PLC (modern way)

A special time synchronization function block is put in the logic program of all CCMs. All CCM clocks and the ProSafe-COM system clock are synchronised using a high priority protocol. All events in the CCM are time-stamped with the local CCM clock and can directly be used by ProSafe-COM.
The function is realised as follows:

- All CCMs use a special time synchronisation function block in their logic program.
- The CCM time sync function blocks automatically negotiate who will act as the time sync master on the M-BUS/M-NET.
- The CCM time sync master synchronises all other CCM clocks using a high priority M-BUS/M-NET protocol (within a millisecond).
- A new CCM time sync master is automatically appointed when the CCM time sync master is stopped or out of order.
- ProSafe-COM communicates at regular intervals with the CCM time sync master and synchronises the ProSafe-COM clock and the CCM time master clock.
- Events from all CCMs are correctly time-stamped and can be used by ProSafe-COM without any correction.

7.4 ProSafe-SLS event time stamping

Events from the I/O and matrix panel control modules are automatically related to the ProSafe-COM system time. If the ProSafe-COM time is kept synchronised with the DCS time, then the Y-net related events are directly synchronised.

8 ProSafe-COM System Engineering Tool

8.1 COM SET

COM SET is the engineering tool for ProSafe-COM and MODCOM. COM SET is a powerful tool during engineering, commissioning, test & maintenance of ProSafe-COM. Engineering, monitoring and diagnosing ProSafe-COM can be completely done with COM SET.
COM SET and ProSafe-COM can either communicate via a COM port using the Modbus RTU interface, or via a network that supports TCP (Modbus/TCP).

Platform COM SET

COM SET is a Windows-based, graphically oriented software package. It comprises editors, compilers and diagnostics capabilities. The package runs on any modern PC with Windows NT or newer.

8.2 Engineering

In brief the COM SET engineering steps are as follows:

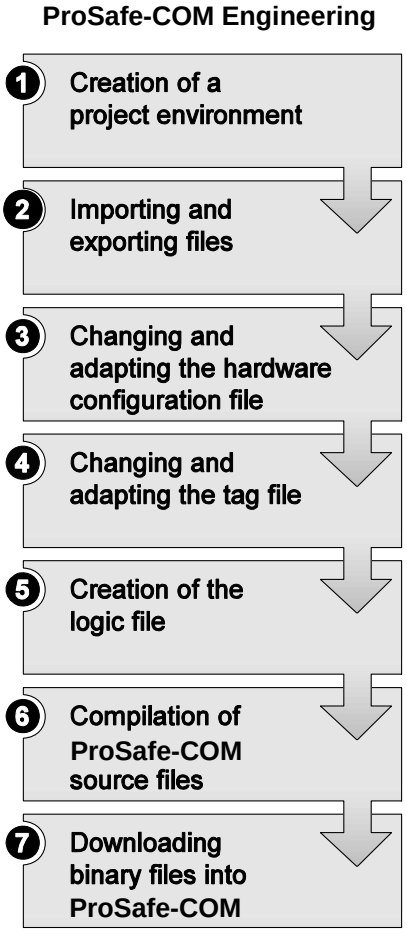

Figure 29: ProSafe-COM engineering

In case of re-engineering the same steps have to be executed. For a more detailed description refer to the *ProSafe-COM Engineering* manual.

8.3 Commissioning, test and maintenance

COM SET can be used also for diagnostic purposes. It can provide status and event overviews of ProSafe-COM. It can create reports for test, maintenance and repair.

Monitoring can be done:

- on line with COM SET
- off line via an error-log file

Preparations and restrictions

To make communication possible between COM SET and ProSafe-COM, one or more communication lines have to be defined in COM SET (serial connection). Therefore, the ProSafe-COM tag file must at least have one communication channel (preferably COM 1) that has logical addresses defined for all tags and that enables events for all these tags.
A dedicated Modbus/TCP connection can be used between ProSafe-COM SET and ProSafe-COM when ProSafe-COM and the engineering PC are connected to the same network.

ProSafe-COM SET can upload the current tag configuration from the ProSafe-COM. This makes it possible to set up a local database containing the available tags in the running ProSafe-COM. The great advantage is that ProSafe-COM SET can monitor any ProSafe-COM system, even if the project database is not present or if the status of the program in the ProSafe-COM is not exactly known.

Status overviews

ProSafe-COM SET can present the actual status of tags in the system. A number of interesting tags are selected from the entire list of tags and grouped into a browse screen. The selections can be saved on disk for later use. Several selection groups can be created and the ProSafe-COM SET engineer can choose which selections must be presented.
The status overviews are frequently refreshed. Output tags can also be written in the browse screens to force overrides, etc.

Statuses can also be diagnostic information.

Event overviews

COM SET reads the available events and creates a local database in which the events are stored. The events can be browsed and inspected and filtered to focus on specific tags. Reports can be created from the event lists for off-line investigations and verifications.

Test

A ProSafe-COM system can be tested even when it is not yet fully integrated in a DCS system. Using ProSafe-COM SET and the I/O emulation all interfaces with ProSafe-COM can be tested easily and early in project development.

In case of error handling ProSafe-COM presents system errors in a log file on disk. The errors can be inspected by uploading the error log file with ProSafe-COM SET for further investigation.
If ProSafe-COM has a parallel printer, then a setting can be made in the configuration file to print system error information on the printer.

Maintenance

The error log file or printer output should be checked regularly, because it might show ProSafe-PLC modules that fail occasionally or permanently and that require maintenance. Note that it is possible to assign ‘internal ProSafe-COM tags’ to the individual module statuses and to the overall ProSafe-COM status. This status can be queried by the DCS at regular time intervals and present an error indication on the DCS’s operator screen.

9 I/O emulation tool

9.1 EmuTool

EmuTool is an engineering tool that emulates the safety systems or the DCS interfaces.
The ProSafe-COM can be fully tested without having the safety system or DCS connected. ProSafe-COM is loaded with the normal configuration files.
All other non-emulated interfaces and ProSafe-COM functions are fully operational.
So the DCS engineers can develop their mimics and control functionality and test the communication with the safety system without having a connection to the actual safety system.
Changes in I/O tags and event generation are invoked via the EmuTool.
The EmuTool can either run on the ProSafe-COM (provided that VDU and keyboard are connected), or on another PC in the network.

Platform EmuTool

EmuTool is a Windows-based, graphically oriented software package. The package runs on any modern PC with Windows NT or higher.

Appendix A: Integrating DCS and ProSafe-COM

This appendix provides a more detailed description of the way ProSafe-COM communicates with other systems. This appendix is especially useful for the engineer of the DCS system. The communication between DCS system and ProSafe-COM can easily be configured by exporting to, or importing from, the tag file.

Communication by using tags

The communication between ProSafe-COM and other systems is configured by defining tags in the tag file. Tags can be read and also be written to.

Tag names can be given to physical addresses in the ProSafe safety system, but also to software items in ProSafe-COM.

A tag consists of:

- the ProSafe-COM name (maximally 25 characters)
- the physical address in the ProSafe safety system (ProSafe-PLC), or the address of the ProSafe-COM software item (maximally 25 characters)
- Tag data type and event information
- 1 up to 5 logical addresses (maximally 25 characters)

Each logical address is connected to a specific communication channel of ProSafe-COM. Communication channels are for example V-net, OPC or the serial Modbus RTU interfaces.

Advantages of using tags

Configuring the communication with tags has the following advantages:

- Each physical address or software item can be assigned to one or more logical addresses. Thus one and the same physical address or item can easily be addressed by different external systems, with different logical addresses. One logical address can be e.g. a Modbus address, another a V-net address.
- The communication connection between ProSafe-COM and external systems is configured in the tag file. This allows flexible, concurrent engineering of ProSafe-COM and external systems. The communication connection can be made, for example, when both DCS system and ProSafe-COM are completely engineered.

Tag definition in a tag file

Tags are defined in the tag file. Part of a tag file is shown below.

```
%-------------------------------------------------------------------------------+
| Module specification                                                          |
+-------------------------------------------------------------------------------+

Description   : ProSafe-COM tag and logical address definition file.

+-------------------------------------------------------------------------------+
| ProSafe-COM Identification definition                                         |
+-------------------------------------------------------------------------------%
[Ident]
    delimiter = "#";              % Redefine the text delimiter from " to # %


[Taglist]
```

```
%-------------------------------------------------------------------------------+
| This part of the tag file defines logical addresses for some digital and      |
| diagnostics tags in a PLC. The first logical address is a Modbus address,     |
| the second one is a V-net address and the third an OPC logical address.       |
+-------------------------------------------------------------------------------%
#MBUS_INPUT_1#, ##, (MBU, 1,1,#input_16#) (Y,N,B,N, 1), B 100 (N,0),
            WB 0112 01 PV    (N , 0 ,   ,          ,  ,  ,    , 1 ),
            #/plc/in_01#  VT_BOOL (N ,   ,   ,#1/8bytes#,  ,  ,  10, 0 );

#CCM1_PRESENT#, ##, (SYS, 4,1,0)          (Y,N,B,N), R 0x5000:1 (N,0),
              WB 0113 02 PV    (N , 0 ,   ,          ,  ,  ,    , 1 ),
              #/sys/in_01# VT_BOOL (N ,   ,   ,#1/8bytes#,  ,  ,  10, 0 );

[EOF]
```

Some explanation to the tag file

- #MBUS_INPUT_1# is the actual ProSafe-COM tag name (maximally 25 characters)
- between ## a description can be given (maximally 25 characters)
- (MBU,1,1, #input_16#) is a physical ProSafe-PLC address on CCM 1, pathid (program sheet) 1 and tag “input_16”
- (Y,N,B,N,1) defines event generation, event generated by hardware, data type, ProSafe-COM start-up output write value and read-only access
- B 100 is a logical Modbus bit address, with (N, 0) indicating event filtering off and the way of scaling (not applicable for boolean)
- R 0x5000:1 is a logical Modbus register address
- WB 0112 01 PV (N,0,,,,,,1) is a logical V-net address defining a boolean, with (N,0,,,,,,1) indicating event filtering off, no scaling and no write boundary checking and event message category 1 (CENTUM CS3000 / VP historical overview only).
- #/plc/in_01# VT_BOOL (N , , ,#1/8bytes#, , , 10, 0) is an example of an OPC logical address.

Connecting logical address and interface
The link between logical address set and a specific interface is set in the configuration file. See below for part of a configuration file, where the link is set. The logical address sets are linked to the various COM ports and to V-net and OPC. The engineer of the ProSafe safety system will set these links.

```
+-------------------------------------------------------------------------------+
| Communication definition                                                      |
+-------------------------------------------------------------------------------%

[Communication]

    %-------------------------------------------------------------------------+
    | Port  | Slave | Logic  | Baud   | Word  |  Parity | Stopbits |Master|
    |       |       | address|        |       |         |          |      |
    |       |       | set    |        |       |         |          |      |
    +-------+-------+--------+--------+-------+---------+----------+------%
      COM 1 ,   1  ,    1   ,   9600 ,   8    ,  None   ,     1    ,  N;

     Vnet 2;
     OPC 3;
```

Importing and exporting tag names
The tag file can be imported and exported from and to the engineering work station (EWS) of the CENTUM CS3000 / VP.
This makes it easy to guard the integrity of tag names used in ProSafe-COM and the CENTUM CS3000 / VP.

It is strongly recommended to use the same names for identical entities as much as possible. This applies to both naming within the tag file as to naming across the various systems.

Abbreviations

CCM	Critical Control Module
COM SET	ProSafe COMmunication System Engineering Tool
DC	Direct Current
DCS	Distributed Control System
EMC	Electro Magnetic Compatibility
EWS	Engineering Work Station (CENTUM CS3000 / VP)
Exn	Regulations for electrical equipment in flammable atmospheres
FCS	Field Control Station
IPC	Industrial Personal Computer
MBI	Module Bus Interface
M-BUS	Module Bus
M-NET	Module Net
Modbus	Gould Modicon serial interface protocol
MODCOM	MODBus COMmunication interface
MULCOM	MULtiple protocol COMmunication interface
HMI	Human Machine Interface
ProSafe	Programmable Safety system
ProSafe-COM	ProSafe COMmunication
ProSafe-RS	ProSafe Responsive System
ProSafe-SLS	ProSafe Solid state Logic Solver
ProSafe-PLC	ProSafe Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCS	ProSafe Safety Control Station
SER	Sequence of Event Recorder
V-net	CENTUM CS3000 / VP proprietary network
V-net/IP	CENTUM CS3000 / VP proprietary network based on Gigabit Ethernet
Y-net	ProSafe-SLS proprietary communication network

Glossary

DCS	Distributed Control System. System consisting of various control and monitoring components, connected by a proprietary network.
Event	Signal change with the corresponding changing time.
Field Control Station	Instruments for non-safe control and monitoring of a production process.
Forcing a status	Setting a status to a specific value.
Logical name (address)	The name for a process variable in another system.
Matrix panel	Panel for local control with push buttons and control lights.
OPC	OLE for Process Control, a standardised method of accessing data and event information.
Physical address	The name for a process variable in the system in which the process is generated.
ProSafe-PLC	Safety system based on a PLC.
Redundancy	Multiplying components or connections, for extra reliability of functioning and communication.
Safety Control Station	Safety system, consisting of ProSafe-COM and ProSafe-PLC.
SCADA	Supervisory Control And Data Acquisition A SCADA system is a system similar to a DCS system. However, a SCADA system is usually built from standard available hardware and software, integrated by a software package.
Sequence of events recording	Recording of various events, sorted on their ‘time stamp’.
Soft marshalling	Giving different logical names to a physical address. In this way, various systems can access a physical address by their own logical name.
Status	Specific situation value in a system or in software. A status can be read and written.
Tag	Identification of a process variable. A tag consists of a ProSafe-COM name, a physical address and 1 up to 5 logical addresses.
Y-net	Proprietary RS-485 network for the communication between ProSafe-COM and ProSafe-SLS.