ProSafe-DSP

with PLS, Programmable Logic Solver
or SLS, Solid-state Logic Solver

Technical Product Description
1 Preface

The ProSafe-DSP system is a Safety Instrumented System (SIS) that was designed for applications, which require the highest Safety Integrity Levels (SIL). For the DSP: ‘Dedicated Safety Processor’ a selection can be made between a programmable logic-solver (PLS) or a solid-state logic-solver (SLS).

Both technologies are 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-DSP system, created by the unique system design, setting it apart from conventional software-based Safety PLC’s. The aspects of Safety and Fault-tolerance are discussed, as well as the system structure, configuration, the communication capabilities and specifications.

In particular the powerful System Engineering Tool (SET) is highlighted. It facilitates the engineering, programming and maintenance procedures; furthermore it creates the project documentation.
# Table of contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Preface</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Safety requirements in Industry</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>- Introduction to Safety Instrumented Systems (SIS)</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>- Inherently fail-safe &amp; fault-tolerant?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>The ProSafe-DSP system concept</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>- The DSP or Dedicated Safety Processor</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>- Comparison Safety PLC's vs ProSafe-DSP</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>- The ProSafe-DSP Availability</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>- The ProSafe-DSP Serviceability</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>- The SLS technology</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>- The PLS technology &amp; system concept</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>The ProSafe-DSP Communication capabilities</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>- The communication interface ProSafe-COM</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>- Sequence of Event Recording</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>- Auxiliary non-safety related Input &amp; Output modules</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>- MMI, Man Machine Interface</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>Project realisation</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>- The ProSafe-DSP SET System Engineering Tool</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>- Test &amp; Maintenance</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>- System Acceptance Testing</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>- Factory Acceptance Testing</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>- Commissioning &amp; proof testing on-site</td>
<td>22</td>
</tr>
<tr>
<td>7</td>
<td>ProSafe-DSP specifications &amp; performance</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>- Generic system specifications</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>- The SLS &amp; PLS modules description</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>- Input modules</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>- Discrete Output modules</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>- Solid-state Output modules</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>- Logic &amp; Timer modules</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>- ProSafe-DSP Auxiliary modules</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>- Clock, power &amp; communication modules</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>- The ProSafe-COM modular communication interface</td>
<td>32</td>
</tr>
<tr>
<td>8</td>
<td>Glossary of terms</td>
<td>35</td>
</tr>
<tr>
<td>9</td>
<td>Yokogawa ISS serving Industrial Safety</td>
<td>37</td>
</tr>
</tbody>
</table>
2 Introduction

The ProSafe-DSP system is based on the Dedicated Safety Processor (DSP), that is employed in a fault-tolerant architecture. Its sophisticated design and superior Safety performance have created the Safety reference standard for programmable as well as for solid-state Safety Instrumented Systems (SIS). The modular design allows fault-tolerant structures to achieve very high Availability, without affecting the superior Safety performance.

A radical improvement provided by the ProSafe-DSP system, is the elimination of software for an operating system and for the self-diagnostics. Instead a unique inherent self-test technology is employed, throughout the safety-related parts of the ProSafe-DSP system.

Furthermore the life-cycle cost is relatively low as a result of a design-lifetime exceeding 15 years, and the powerful engineering and maintenance System Engineering Tool. In addition, by the absence of system software, the need for costly and risky software updates is also non-existent.

Typical user applications are found in the Chemical, Refining, Oil & Gas production and Nuclear & conventional Power industry, such as:

• Emergency Shut-Down systems (ESD) for Safety critical process units;
• High-Integrity Protection Systems (HIPS) for well-heads, pipelines, natural Gas storage installations;
• Chemical process plants for critical process protection;
• Well-head protection systems, also in sub-sea applications;
• Burner Management Systems for incinerator furnaces and steam boilers;
• Compressor protection systems for rotating and piston type compressors;
• Fire & Gas protection systems as found in Oil & Gas installations;
• High-Integrity protection systems in the Nuclear industry.
3 Safety requirements in Industry

Introduction to Safety Instrumented Systems (SIS)

The quest for higher Safety
The guidelines for safe operation of Industrial installations in the Petrochemical and 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 co-operation of industry groups, Safety certifying agencies and insurance companies, resulting in more stringent regulation and legislation.

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 another 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.

‘Eliminating the unexpected’
The current Safety considerations focus on three elements:
• The physical separation of the Safety interlocks and process control systems;
• The nature of the SIS technology used;
• Quantitative risk assessment (QRA) methods, which enable to optimise the links of the Safety chain including the field devices.

This first element is a matter of engineering design practice. Physical separation of process control and Safety interlocks will eliminate common-cause problems that can originate from hardware, software and human causes.

The second element offers essentially two alternatives technologies to consider. One based on PLC’s (Programmable Logic Controllers), typically incorporating test-circuits and test-software. A superior alternative is the use of technology that employs an ‘inherent self-test’ of the ProSafe-DSP, whereby the ‘fail-to-safe’ nature is achieved by this unique technology, without the need for additional hardware or software for self-diagnostics.
In many instances it is advantageous to compose the system from various types of hardware, dedicated to the specific tasks. These 'hybrid' systems make it possible to exploit the advantages technologies. The use of 'inherently fail-safe' technology is creating the highest Safety level. On the other hand, microprocessor based devices provide the flexibility, the interface facilities and additional functionality. The ProSafe-DSP system is in fact such a unique 'hybrid system', that combines the advantages of both technologies.

The third element of contemporary Safety approach is the Safety assessment by QRA, a quantitative risk assessment that calculates realistic figures for Safety (Pfd & SIL) and Availability (MTNF & FTR) for each project. This will make sure that the SIS will perform according to expectations and conforms to the required Safety Integrity Levels. The SIL requirement depends on the Safety risk that is provoked by operating a certain type of process. In practice, it ranks from 1 for the less critical processes, up to 4 for the most Safety critical processes.

Safety standards such as IEC 61508/61511 and DIN/VDE V 19250 that have world-wide recognition have created stringent Safety requirements for process plants. Therefore the operating companies in the process industry are looking for system suppliers, that can offer tightly integrated control and Safety systems. In the Yokogawa ISS project organisation a department of specialists guarantees adherence to Safety standards and can issue a 'certificate of conformity' for an individual project.
Inherently fail-safe & fault-tolerant?

The use of the terms ‘fault-tolerance’ & ‘redundancy’ may give many users a feeling of confidence, which is not always justified. It should be noted that fault-tolerance is only a method to provide an elevated level of Availability if applied properly. Full or partial redundancy with ‘voting’ can be applied in any type of modular technology on the Inputs, the logic-solver and the output modules. In a redundant configuration the voter serves to compare the performance of the system modules and to make a selection, based on the requirement of Safety and/or availability. In general an attempt to increase Safety by redundant modules goes at the expense of Availability, because of increased hardware use and additional software.

Also visa-versa: a configuration for increased Availability creates a lower Safety, because the ‘diagnostic coverage-factor’ in all types of redundant systems has a dominating influence on the system SIL level, if this figure is less than 0.99.

The limiting factors are the undetected failures, common-cause failures, software execution time and hardware reliability. The undetected failures that remain (and can accumulate!) in the system, are due to the limited testability of software and of complex hardware. By definition, redundancy and voting devices are no remedy for this type of un-safe failures.

Since in the ProSafe-DSP system the diagnostic coverage factor 1 for the ‘inherent self-test’ and the safety is not affected by redundancy. By a modular design of the ProSafe-DSP system it can be configured in a fault-tolerant manner, which is done for applications where this is a prerequisite besides un-compromised Safety.

For example, in a High Integrity Process Safety (HIPS) system a 2 out of 3 voting can be applied on the Inputs only. This will improve the reliability of the input process parameters, since the field sensors (transmitters) and actuators (valves) often have a relative high failure-rate and do contribute to the SIL calculation.

The relation between ‘SIL’ and the ‘Mission-time’

The necessary proof-test intervals are becoming shorter if the diagnostic covers less than 100 %. This real coverage-factor does comprise the percentage of un-tested hardware and software!

It is this phenomenon of Safety-degradation necessitates a periodical off-line test of a Safety system. For the user it is important to have a test-interval time that is exceeding the ‘mission-time’ of the process, otherwise a process shut-down is required to do this periodical ‘proof-test’.
Often the quoted diagnostic coverage-factors are ‘an expert’s opinion’, having only a qualitative significance. In the recent decade, scientific developments have created more realistic quantitative validation methods of Safety and the self-test capability of systems. In practice, this figure is dominating the calculation of the Safety Integrity Level (SIL), provided by a system and the field devices.

**Common-cause faults**

Systems that employ redundancy are in particular vulnerable for common-cause faults. Similar redundancy may be a good method to improve the systems availability, for systems that have apparently too many failures. For improving safety, the effect of redundancy is limited, or even counter productive, since it will introduce common-cause failures. In practice, redundant safety PLC systems do apply similar hardware and only single software. Redundancy when applied in parallel brings a degree of fault-tolerance, not to be confused with safety. Fault-tolerance and safety are benefits, which are achieved by dissimilar design strategies.
The DSP or Dedicated Safety Processor

The unique technology of the ProSafe-DSP can employ either the programmable logic solver (PLS) or the solid-state logic solver (SLS). The non-safety functions and computer interfaces are implemented with regular microprocessor technology. The Dedicated Safety Processor has been designed with the objective of an uncompromising safeguarding system, of which the Safety Integrity Level is eminent and verifiable. The unique technology employed in the PLS concept has created today's reference standard for programmable & solid-state SIS systems. The robust safety achievement is originating from its internal architecture and inherent self-test methodology. Also the elimination of all system software is a major breakthrough for a programmable safety system. The DSP design has successfully eliminated all known sources of unsafe failures. In each DSP system the inherent self-test is performed, in every small functional unit, while working with the real functional logic code of the application. This further implies, that the logic processing and self-test are executed at exactly the same moment in time and by the same components of the hardware.

Comparison between Safety PLC’s and the ProSafe-DSP:

<table>
<thead>
<tr>
<th>Safety PLC’s</th>
<th>ProSafe-DSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software for firmware &amp; diagnostics</td>
<td>Megabytes</td>
</tr>
<tr>
<td>Software for application</td>
<td>Megabytes</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>by software &amp; hardware</td>
</tr>
<tr>
<td>Soft-error detection</td>
<td>by voting</td>
</tr>
<tr>
<td>Fault-tolerance</td>
<td>yes</td>
</tr>
<tr>
<td>Redundancy voting</td>
<td>by software &amp; hardware</td>
</tr>
<tr>
<td>'Common-cause' elements</td>
<td>software/voting/synchronisation</td>
</tr>
<tr>
<td>Separation Safety &amp; other functions</td>
<td>no, all in same processor</td>
</tr>
<tr>
<td>Subdivision of systems</td>
<td>possible</td>
</tr>
<tr>
<td>Communication capabilities</td>
<td>yes</td>
</tr>
<tr>
<td>Scan-time</td>
<td>50 - 1000 milliseconds</td>
</tr>
<tr>
<td>Response-time</td>
<td>100 - 2000 milliseconds</td>
</tr>
<tr>
<td>Programming</td>
<td>various languages</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Level</td>
<td>SIL 2 &amp; 3, AK 4-6</td>
</tr>
<tr>
<td>'Mission-time' &amp; test interval</td>
<td>several months</td>
</tr>
</tbody>
</table>
The ProSafe-DSP

**Availability**

Products in the ProSafe-DSP range have been designed from the outset, to give the highest level of reliability required in control Systems where failures can be costly and hazardous. As a result of the simplicity, the low parts count, the components de-rating, the functional tolerance for component parameters drift and last but not least the high EMI immunity, the SLS system also scores very high on the scale of Availability (FTR & MTNF). For extremely high demands regarding Availability the SLS modules can be duplicated freely.

The ProSafe-DSP

**Serviceability**

Serviceability is inherent in the design is a prime feature of all ProSafe Systems.
In case of a detected failure, the faulty module can be replaced quickly without interfering with other subsystems. Modules do not require system specific configuration or addressing when replaced, and all module upgrades are retro-compatible. Normally skilled personnel can easily replace modules on the basis of testing every logic step in the system. Test facilities are permanently integrated in the system and are enhanced when using the ProSafe-COM facility.

The SLS technology

**Safety-by-design**

The essence of the SLS, solid-state logic solver The ProSafe-DSP SLS principle was invented in 1965 and in the mean time has been utilised in a large number of SIS installations in the hydrocarbon, the chemical and the (nuclear) power industry. This technology, formerly known as 'MagLog' has been upgraded using up-to-date components and fabrication methods, without changing the basic inherently-Safety principle.

**ProSafe-DSP SLS Inherently fail-safe**

The SLS technology is called 'inherently fail-safe', meaning that by the self-testing nature of the basic SLS circuit it will act fail-safe, without the necessity of utilising additional test- or diagnostic circuits.
A logical ‘1’-signal status in a SLS system that reflects the ‘safe’ condition of a process parameter is represented by a pulse-train, keeping the SLS circuits dynamic continuously. The logic solver operations are executed by magnetic core elements, while the transistors only serve to restore the energy of the pulse-trains.

**The ProSafe-DSP SLS principle**

The essential element of the SLS circuit is a ring-shaped core of magnetic material with several windings. This basic circuit further consists of a transistor and pulse-shaping circuit that comprises a choke coil and a diode.

The ring-shaped magnetic core is not a normal transformer, since it has a very high hysteresis, which makes it a binary element with two stable positions and it serves a dual purpose. First it can execute logical functions (AND, OR, NOT) and secondly it does provide a galvanic isolation between SLS circuits.
Current pulse-trains are used to magnetise the magnetic cores. The duty-cycle is less than 3%, which keeps the circuit dissipation low. As an extra benefit, as a result of this current principle the low circuit impedances make the circuit immune to high levels of electro-magnetic interference.

The logical '1' input information, from a closed field contact for example, is represented by a pulse-train of 1000 short pulses per second in the SLS circuit; we call them 'A' pulses. Each SLS circuit needs these 'A' as well as phase shifted 'B' pulses, which may come from an other logic input or from the system clock generator. These 'A' and 'B' current pulse-trains have an asymmetrical shape, meaning that the current flows in one direction only and therefore are only capable to magnetise the core in only one direction (clockwise or anti-clockwise). A second wire through the same core, having pulses in the opposite current direction and which are phase shifted, make sure that the almost rectangular hysteresis-loop of the magnetic cores is fully exercised.

The resulting output pulse-train is alternating between positive and negative pulses. Only the positive pulses are capable to make the transistor conduct. Only in case that both 'A' and 'B' pulses are present, an induced current pulse-train will come out of the pick-up winding, during the change of magnetic flux. This pulse-train makes the transistor switch 'on' with each positive pulse, creating an output of this SLS basic circuit with a similar pulse-train.

It will be evident, that the above circuit can be applied as a logical 'AND' gate when 'A' and 'B' represent two logical input signals. An additional wire through the core with 'A'- pulses in the same direction will create a

"A" and "B" pulse-trains are phase shifted.
logical 'OR' gate, assuming that the 'B' pulses come from the system clock. The output will always go to a static de-energised state, whenever any component failure or a wire failure occurs. Because only discrete components are applied, the circuit failure behaviour is fully predictable. The dynamic nature of the circuit takes care of a continuous self-test, by activating all components and electrical connections. The unique combination of the mentioned design aspects make the SLS circuits 'inherently' fail-safe.

The PLS technology & system concept

The PLS programmable logic solver has been designed without any compromise and the Safety Integrity Level is eminent and verifiable. The hardware consists of a kernel that employs virtual hardware diversity and redundancy, while working with the real functional logic code of the application. Input and output circuits apply the inherently fail-safe SLS technology. The PLS logic solver is located in the Logic & Timer or ‘LT’ module, and it executes all functional logic and timer functions, as defined in the application Functional Logic Diagram. The Logic & Timer modules, power supplies, I/O modules and the supporting modules can be structured in a number of configurations. In this way it is possible to further increase the Availability by fault-tolerance, or to choose for a lower safety integrity level for the protection of a less-critical process.

"A" and "B" pulses are needed to go out through the hysteresis loop.
On system level, ProSafe-DSP PLS is organised in independent fully functional units, including I/O modules. These building bricks are called 'boxes', which can be interconnected to construct a system with more I/O capacity. By this approach, there is no technical or practical limitation to the maximum PLS I/O handling capability. On the other hand, a PLS system can be tailor made to the size of any sub-system of the process, creating 'distributed safety' for the total plant.

By the modular approach, the programmable PLS employs the same range of input & output modules and communication interfaces, as the solid-state SLS.

The essence of the PLS, programmable logic solver
The robust safety achievement originates from its internal architecture and inherent self-test methodology. Also the elimination of all system software is a major breakthrough for a programmable safety system. The design guarantees high safety integrity performance. The configuration in a dual or triple (TMR) fault-tolerant architecture provides further increased availability. The PLS logic processor is capable of executing all standard logic and timer functions, within a fixed program execution cycle-time of one millisecond.

The PLS concept is based on the following essential foundations:
• No system software;
• No unnecessary hardware circuit complexity;
• All safety-related circuits and logic code are fully verifiable for safety, not only in normal operation, but in particular, when one or multiple errors have occurred;
• No concessions to safety.

ProSafe-DSP system block diagram.
The PLS design has successfully abandoned the conventional architecture of regular microprocessors and is capable to disarm the well-known internal potential failures. Besides the capability to detect static failures, the PLS is also well equipped to detect dynamic failures or 'soft-errors', which emerge from critical timing, or electromagnetic interference. These soft errors are driven by the moment of operation and cannot be revealed by a regular off-line functional test.

The PLS employs the fundamental principle of blending logic processing with a full inherent self-test, executed at the same moment in time. As a consequence the inherent self-test occurs with real field input-data, while processing the actual functional application logic in 'virtual instruction diversity' and by usage of the same hardware components involved. All logic processing is driven by the system hardware structure. This patented inherent self-testing method applies 'virtual hardware diversity' and transformation of input data from the process and logic programme instructions. Static and all dynamic failures or potential selection failures in registers, are cancelled in this manner. The PLS employs tightly coupled 'state-machines', which are again inherently self-testing by design.

Safety measures on system level
The ProSafe-DSP PLS system design is based on the following design principles:
• The PLS system has totally abandoned the use of system software. Instead, the operation is driven by the hardware structure. The application-code reflecting the FLD functionality, is typically only a few hundred bytes for one PLS 'box';
• The PLS system logic solvers do not have any cross connections by shared control, data or other resources. Also other means of influencing the operation of a peer's logic solver are absent;
• Application instructions are retained twice in EEPROM in a diverse mode;
• No usage of any conventional memory for data retention. Instead the Outputs are set by inherently-safe magnetic cores, that are refreshed every millisecond by the PLS;
• Usage of inherently fail-safe circuits similar to SLS wherever possible.

The above principles remain valid when multiple PLS boxes are interconnected to create more input & output handling capacity. The fully autonomous PLS boxes operate as parallel processors for the total system logic. In this manner the system scan-time of 1 millisecond remains independent of the total I/O count, which is virtually unlimited.

All logic timers are dual-redundant and are built in dedicated hardware, each with an error detection circuit. This detection circuit is activated by any discrepancy between the timers Outputs. Since the ultimate test for a timer is using the timer, this test is similar to the normal operation. For this test, each timer is activated for the programmed time and after its expiration, this procedure is repeated continuously. For regular operation each timer is reset and started instantaneously, by the functional logic.
**ProSafe-DSP PLS system configuration**

The smallest PLS system is called a 'box'. Each PLS 'box' is in essence a complete safety system, containing all modules to create a safety system. A box can accommodate the following modules:

- Two Communication & Power (CP-180) modules, which work in a redundant mode. Besides the system power provision, these modules also support the inter-module communication for status and events;
- A PLS 'box-pair' utilises the CP-180 modules located in the left side box;
- Two inherently fail-safe digital input modules, each with 16 channels;
- Three logic & timer modules, each containing a PLS logic processor;
- Two inherently fail-safe output modules, each with 8 channels.

PLS boxes are mounted two-by-two, in a dual height 19' rack, sharing one back-plane, two redundant power-supplies and the communication interfaces, which are located in the same Communication & Power (CP-180) modules. This assembly is called a PLS 'box pair'.

---

<table>
<thead>
<tr>
<th>Box 1</th>
<th>Box 2</th>
<th>Box 3</th>
<th>Box 4</th>
<th>Box 5</th>
<th>Box 6</th>
<th>Box 7</th>
<th>Box 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-180</td>
<td>CP-180</td>
<td>CP-180</td>
<td>CP-180</td>
<td>CP-180</td>
<td>CP-180</td>
<td>CP-180</td>
<td>CP-180</td>
</tr>
<tr>
<td>CI-16A</td>
<td>CI-16A</td>
<td>CI-16A</td>
<td>CI-16A</td>
<td>CI-16A</td>
<td>CI-16A</td>
<td>CI-16A</td>
<td>CI-16A</td>
</tr>
<tr>
<td>TI-16B</td>
<td>TI-16B</td>
<td>TI-16B</td>
<td>TI-16B</td>
<td>TI-16B</td>
<td>TI-16B</td>
<td>TI-16B</td>
<td>TI-16B</td>
</tr>
<tr>
<td>LO-8B</td>
<td>LO-8B</td>
<td>LO-8B</td>
<td>LO-8B</td>
<td>LO-8B</td>
<td>LO-8B</td>
<td>LO-8B</td>
<td>LO-8B</td>
</tr>
<tr>
<td>FT-8C</td>
<td>FT-8C</td>
<td>FT-8C</td>
<td>FT-8C</td>
<td>FT-8C</td>
<td>FT-8C</td>
<td>FT-8C</td>
<td>FT-8C</td>
</tr>
</tbody>
</table>

The ProSafe-DSP box pair, with an arbitrary selection of modules.
5 The ProSafe-DSP Communication capabilities

The Communication interface ProSafe-COM

The functions of Communication, Sequence of Event Recording (SER) and remote Input and Output functions are realised by the ProSafe-COM modules. The specific functions are implemented by software and dedicated modules of the ProSafe-COM system.

It is a must for every Safety system to monitor start-up and shutdown procedures in real system-time and record the associated events for later analysis in a Sequence of Event Recorder. The ProSafe-COM system provides just that 'black box' function, which makes it possible to retrace and analyse the events associated with a particular process situation, with a time resolution of one millisecond.

The SER information, such as sorted events with real-time tags and I/O status with tag names can be presented in a stand-alone configuration on a personal computer and printer. The same information is available for the operator's MMI, via a bi-directional serial link, to display for example the real-time process mimics, events and alarms. In addition, the functionality as found in matrix panels such as alarm handling sequences and overrides may be fulfilled by this MMI. The programmable matrix controller is part of the ProSafe-COM functionality and is very suitable for control of annunciation matrix or mimic panels.
The MMI man machine interface provides the operator with all pertinent information on the screen from the underlying Safety systems and it enables all necessary interventions, protected by authorisation levels, and hardwired override permissions. In practice most functions of an annunciation matrix panel and the ProSafe-COM can be conveyed to this operator MMI. The MMI supervisory system offers extensive report capabilities to summarise all operator and process activities in daily reports.

Sequence of Event Recording

In the ProSafe-COM system, the sequence of event recorder system fulfils the functions of:

- Data communication of:
  - events;
  - status;
  - analogue values;
  - real-time clock setting for synchronisation with the host computer system;
  - override & inhibit capability of Inputs and Outputs via dedicated modules that handle the non-safety I/O.
- High-speed time-tagging of events at input level, for accurate real-time information;
- Data buffer capacity prevents loss of data if communication with the host system is slow or interrupted;
- Fault-isolation is guaranteed by virtue of built-in precautions, for connections to the Safety-related system modules. The safety integrity of these devices is hereby maintained;
- Cost effective modular design, which can be configured for virtually any application;

- Redundant serial data communication with DCS and any other host application system, supporting the Ethernet TCP/IP & ModBus interface protocols;
- Printer output;
- Time resolution of 1 millisecond;
- Max. 5000 signals per ProSafe-COM system;
- Storage buffer for 10,000 events. Virtually unlimited storage capacity in the ProSafe-COM workstation or in the MMI.

Auxiliary non-Safety related Input & Output modules

Additional modules of the ProSafe-COM system can handle non-safety-critical I/O in a cost-effective manner, such as for the control of annunciation matrix and mimic panels:

- Bi-directional serial communication with other systems, operating as a master or as a slave, utilising the ModBus protocol;
- Sequence handling for alarm systems or other non-safety functions;
- Many standard alarm sequences, first-up handling and other function-blocks, which are readily available in the engineering tool.
The MMI, a supervisory VDU workstation

The Man Machine Interface for the operator can supervise all distributed safety systems as well as associated functions during process start-up, normal operation and SER data processing for later analysis. It comprises for example:

• Real-time presentation of process mimics on the VDU;
• Alarm and start-up sequence handling;
• Events presentation and sorting by period and by sub-system;
• First-out indication, also on individual sub-systems;
• Override and disable capability such as:
  - permit control;
  - disable all, disable group;
  - number of overrides limitation;
  - duration limitation.
• Extensive report capabilities;
• Data retention is virtually unlimited in the workstation;
• System-time synchronisation capability with other systems.
Computer Aided Engineering and programming of ProSafe-DSP system applications is fully supervised by the PC based, engineering system working under Windows. It serves to create an engineering environment, where all engineering activities are co-ordinated and documented. The ProSafe-DSP SET does allow the project engineer to fully employ his expertise and preferences for system layout and the creation of autonomous sub-systems.

During the engineering process, the SET is assisting the engineer, by examining the created AutoCAD based system drawings. Messages, warnings and suggestions are generated automatically in case of mismatch of hardware usage, or potential safety conflicts. In order to verify the functional logic, the engineer can simulate the functional design, not only on ProSafe 'box' level, but also through the entire ProSafe-DSP system.

After engineering completion, SET will compile all engineering documentation, including the complementary project documentation, such as mechanical drawings, wire-lists and of course the PLS instruction code files. Not only during engineering, but also extending to the whole useful life of the realised project, the System Engineering Tool organises the consistency of project files. The SET keeps track of all revisions and changes of the application drawing package. In this way, the SET provides up-to-date project documentation, safeguarding not only the quality of engineering, but in particular serving the interest of safety.
PC hardware, minimal requirements:
• Personal Computer, Pentium, with min. 32 MB operating memory;
• The use of a 17 inch colour monitor;
• A function-tablet is recommended. Operation by means of a mouse is also possible.

The SET software employs various software modules that co-operate smoothly to create additional functionality:
• Windows as operating system;
• AutoCAD for the creation of drawings;
• A graphical alphanumeric database;
• The PLS system code compiler and de-compiler for code verification.

Test & Maintenance

Using the SET, Test & Maintenance Tool
Testing and maintenance of a PLS system are supported by the SET, Test and Maintenance Tool that contains the relevant functionality and it can run conveniently on a lap-top PC. The Test & Maintenance Tool enables monitoring of internal functions on bit level and of course, it supports the uploading and downloading of PLS application programs.

A strong feature of System Engineering Tool is the self-documenting capability. This mode is used to trace
the functional design specification
documents (FDS) of the application.
The SET is capable to automatically
read-out actual logic status and to
compare this to the engineering
documentation. This consistency test
can also be executed on the plant site,
after a system modification, or during
scheduled maintenance.
During normal operation, the PLS
system performs various self-tests.
Malfunctions, if any, are
communicated via front panel status
indicators as well as via the
communication interfaces. Remote
system diagnostic is created via a
modem connection and operates via
the ProSafe-COM interface.

Maintenance activities like on-line
changes or module replacement can be
done with a ‘hot’ system. After an on-
line modification only the involved
PLS boxes need to be tested, since all
other boxes remain untouched.
Maintenance activities involving
changes of the PLS application
programs require the proper access
authorisation. For on-line
modifications, the PLS system must
contain the 2003 configuration,
however a temporary upgrade is
creating this capability as well.
Once again, the Test and Maintenance
tool assists and supervises the
modification procedure and makes
sure, that the documentation is
updated. At all times, the ProSafe-DSP
inherently safe 2003 voter remains
untouched. This guarantees the
system safety integrity during these
on-line modifications, or hot repair
activities.

System Acceptance Testing

For the execution of the tests the
manner of working is defined in the
test protocols and the results will be
recorded in test records. All system
testing prior to delivery is performed
at the assembly factory.

Factory Acceptance Testing

The regular FAT tests to be performed
are:
• visual inspection;
• system module test;
• electrical tests: earthing, insulation,
power supply etc.;
• functional tests; verification against
functional design drawings;
• performance tests: system load,
power variations etc.;
• temperature rise test.

In addition the following optional tests
can be performed:
• duration test;
• RFI test;
• heat-soak test;
• duration test at elevated
temperature;
• vibration & earthquake compatibility
test.
Commissioning & integrated proof-testing on-site

On completion of installation and commissioning at site, a final site test will be performed. This test will generally include all tests made in the Factory Acceptance test, using portable simulators or actual plant Inputs and Outputs. The testing may be supplemented by additional tests required as a result of any changes incorporated into the system since the FAT.

The logic-solver of the DSP system utilises inherently fail-safe modules and inherently self-testing dynamic logic, therefore there is no requirement for system input, output and logic testing once the system has been put in operation.

Volt free contact (VFC) Outputs and timer cards are the only components requiring periodic testing due to their non inherently fail-safe characteristics, though full reliability data is available for these modules to support reliability predictions.

Testing of field input loops is provided by applying overrides to the relevant Inputs and simulating a trip in the field. The logic allows the true detected state to be monitored and handed off for recording if desired. Testing of output devices should be based on confirmation that they will trip on demand. This requires that Outputs should allow individual manual trip functions, whilst not permitting Outputs to be prevented from tripping. This can be provided by switches on the 24Vdc., supplied to each output circuit where a purpose built test facility is desired. A low cost option is simply to open the isolating pins in the field termination.

Where there is a specific desire for output defeats, then these can be applied to allow a full system trip to be carried out on-line. If the ProSafe-COM system is included in the system, then a full event log of the test is available in the SER, for comparison against an original record.
## 7 ProSafe-DSP specifications & performance

### Generic system specifications:

<table>
<thead>
<tr>
<th><strong>Principle of operation:</strong></th>
<th>Magnetic Core Transistor Logic-solver;</th>
</tr>
</thead>
<tbody>
<tr>
<td>in SLS:</td>
<td>in PLS: Hardware-driven logic-solver for max. 375 machine instructions per PLS box;</td>
</tr>
<tr>
<td>in both:</td>
<td>Inherent self-test and Fail-safe Inputs &amp; Outputs.</td>
</tr>
</tbody>
</table>

#### Special Features:

- Inherently fail-safe;
- Low heat dissipation;
- High immunity to EMI;
- Galvanic separation of logic-solver and I/O;
- Auxiliary microprocessors for:
  - Communication;
  - SER diagnostics;
  - Monitoring;
  - Annunciation.

### Operating environmental conditions:

- **Temperature:** operating -20 C to +70 C.
- **Relative humidity:** 0 – 98 % ‘non condensing’.
- **Shock:** 10g, 16 millisecond
- **Vibration:** 10 - 200 Hz at 1.5g.
- **System:** Seismic qualification.
- **Pollution:** SO2, H2S. < 0.7 PPM.
- **Mechanical:** SLS: Eurocard modules. PLS: double-height Eurocard modules, 266mm. assembly in: 19’ racks. cabinets: 800x2100x600 (or 800)mm, (wxhxd).

### Maximum number of Inputs & Outputs:

- **Inputs:** unlimited.
- **Outputs:** unlimited.
- **Timers:** unlimited.

### Noise immunity conforms to:

- CE: Conformité Européen;
- EN 50081-2 & 50082-2;
- ENV 1954, IEC 1131-2;
- C.I.S.P.R. 16;
- DIN IEC 801-2, 3, 4.

### Input range:

- **Discrete:** 24 VdC
- **Analogue:** 0-20 mA, 0-10 V or 0-5 VdC, set point & measured transmitter value readable by serial link;
- **Thermocouple & R.T.D. Communication:** by signal conditioning before analogue input;
- **DSP Inputs via ModBus and Ethernet.**

### Output range:

- **Relay:** DC and AC
- **Fail-safe:** 5 Watts & 20 Watts; 24 VdC or 110 VdC
- **Serial links:** by ModBus

### Timer range:

- **Multipurpose timer:** 7 millisecond to 70 hours.
- **Dual fail-safe timer:** 1.5 to 310 seconds.
In addition, the ProSafe-DSP system was assessed for Safety and Availability by the following organisations:
• SINTEF;
• TNO;
• WIB;
• KEMA;
• SIREP Evaluation Report E 1699 S 91;
• University of Twente CAIRO study;
• University of Eindhoven RIFIT study.

The ProSafe-DSP system satisfies the recommendations of the following guidelines for SIS systems:
• IEC standards 61508 & 61511;
• ISA SP84 recommendations;
• Department of Energy - Guidance note 91, on Design of Offshore Installations;
• HSE Health & Safety Executive, PES/SIS documents 1 and 2;
• EEMUA Publication 160 - ‘Category 1’ applications;
• API R14C.

Logic processing:
- Scan-time: 1 millisecond for I/O scan and logic processing
- Response time: 1 millisecond per logic element.
- Typically, 25 msec. end-to-end includes I/O delay

Communication:
- Serial link standard via: ModBus protocol (RS 232) or Protocol to customer specifications.
- Point-to-point: via Input & Output modules.

Self diagnostic:
- ProSafe-COM microprocessor system with SER LED’s on modules.

Programming & Engineering:
- For PLS: ProSafe-DSP SET using IEC or ISA logic symbols.
- For SLS: Engineering by ProSafe-DSP SET, also for software programming of the auxiliary microprocessor functions including ProSafe-COM.
- Hardwired programming of the Safety interlocks with protected cold crimp-contacts (IP 20).

Troubleshooting:
- Self-diagnostic by sequence of event recorder and LED status indicators on all modules.

Safety certifications:
- TÜV: AK 6-7
- Factory Mutual: SIL 3 - 4

Typical cabinet layout.
Field I/O termination
Field termination is realised by means of connector-blocks for direct plug-in of system cables, or by terminal rows that facilitate marshalling.

The SLS and PLS modules description

For a ProSafe-DSP SLS system we summarise the various categories of available modules:
- Input modules;
- Logic & Timer modules;
- Output modules;
- Auxiliary modules;
- Communication & Interface modules.

The next chapters describe the functionality in more detail. For a detailed technical specification, we refer to the individual datasheet of each module.

Input modules

Digital input module DI-511 for the SLS
The discrete Input module has 8 channels and converts field voltage Inputs to inherently fail-safe, pulse-train signals. The module performs continuous self-test every millisecond. It has the following characteristics:
- 8 digital Inputs at nominal 24 Vdc;
- status indication per channel by LED's at the front;
- Input current of 8.5 mA, at 18 - 32 Vdc;
- each individual input is galvanically isolated;
- monitoring circuit for interfacing with the ProSafe-COM.

Digital input module DI-110 for the PLS
The inherently fail-safe digital input module DI-110 converts 16 digital field Inputs into 16 pulse train signals. The signal conversion uses inherently fail-safe technology, with all Inputs galvanically isolated. The module has the following features:
- a continuous inherent self-test is executed every millisecond;
- 16 digital Inputs at nominal 24 Vdc;
- LED status indication per channel at the front;
- input current of 8.5 mA, at 18 - 32 Vdc;
- each individual input is galvanically isolated.

The data communication circuit for status and sequence of event monitoring also executes a continuous self-test. It will report the healthiness of the communication-related part to the Clock-Power module CP-180 on a routine basis. Diagnostic information is indicated at the front panel and any abnormal condition will result in an alarm indication on the common alarm line, contained on the bus reserved for this purpose. The module communication responds to communication requests from the communication subsystem located in the clock-power module CP-180 and reports status and event information.

Besides the communication information for status and event-data, the module also responds to create the following system-messages:
- event time stamp;
- communication reset;
- status of communication related part of the module;
- module identity code and communication of the software version code.

Each PLS box can accommodate a maximum of two DI-110 digital input modules, each with 16 input circuits. Therefore, the maximum number of digital fail-safe Inputs for a ProSafe-DSP Box is 32.
Analogue Inputs AI-517 & AI-917
Either the AI-517 discrete trip-amplifier, or the AI-917 programmable trip-amplifier, dependent on the application can process analogue Inputs. Line monitoring can be integrated with the input module for analogue Inputs. For Safety critical applications (SIL 3 or 4 Systems), it is generally recommended that field transmitters are redundant and voted 1-out-of-2 or 2-out-of-3. The logic system performs the voting functions and can provide repeat signals of the measured value to a host system. This communication can be either hardwired via isolators, or via the ProSafe-COM system on a serial link using the MC-562 module.

Discrete Output modules

Inherently fail-safe Output modules
Fail-safe Outputs provide individual fail-safe power to the final elements in the field. In practice, these field devices (valves) will be normally energised, representing the normal safe-operating condition of the process. If a process trip is necessary, the output will be de-energised, resulting in the necessary safe action in the field, i.e. closing of a valve. The valve will often be moved by a spring-load, which is released by compressed air.

All of the inherently fail-safe output modules convert pulse-train signals into power to the Outputs that can directly energise the field actuators (valves). Each output channel has an individual power supply with a fuse and is galvanically isolated. Individual LED's indicate the Output status for each channel.

Inherently fail-safe output modules exits in the following versions:
FO-526 inherently fail-safe output module
This module is for 3 channels providing 24 or 48Vdc, max. 20 Watt.

FO-528 inherently fail-safe output module
This module is for 2 channels providing 24 or 110 Vdc, max. 35 Watt.

FO-529 inherently fail-safe output module
This module is for 4 channels providing 24 Vdc, max. 0.5 Watt.

FO-120 & FO-121 inherently fail-safe output module
Both modules are designed for the programmable PLS and have eight channel fail-safe Outputs, nominal 24 Vdc at the front and LED status indication. The module contains also the voting circuit for redundant logic-pulses, coming from the LT-150, Logic & Timer modules. The unique inherently fail-safe technology is also applied for the voting of the logic Outputs entering from the LT-modules. The logic-pulses are voted 2 out of 3, or 2 out of 2 depending on the chosen configuration. The module contains a communication interface that serves to transfer the status and it stores all events of the DC field Outputs. In addition, the fuse-status of each field power supply is monitored via the communication module. Diagnostic information about the communication is shown at the front panel. Any error condition activates the common alarm on the bus.

The Power supply capacity of each channel is 5 Watt for FO-120 and 20 Watt for FO-121. The PLS Box can accommodate a maximum of two fail-safe power output modules, either 2 each 8 channel 5 Watt, or one 8 channel 20 Watt, or one of each type. Therefore the maximum number of inherently fail-safe Outputs for a PLS Box is 16.

Solid-state Output modules

Matrix panel lamp drivers & Relay output modules:

IO-547 lamp-driver module
This module is designed to control matrix panel lamps or LED’s. It has 8 circuits with the following characteristics:
• 24 Vdc. Inputs;
• 24 Vdc. current sink Outputs;
• 8 LED’s indicate the activated Outputs;
• galvanic isolation by opto-couplers;
• inverted or direct acting;
• common lamp test and flash input;
• shift-register for the ProSafe-COM interface.

DO-523 relays Output module
This module is intended for use as a lamp or relay-driver and converts 8 pulse-train Input signals in solid-state Outputs for 8 channels. Inputs & Outputs are galvanically isolated. Each output includes a protection diode and a fuse. LED’s indicate the activated Outputs.

RE-520 relays Output module
The module is intended for the connection of medium and low power loads. It converts 24Vdc. Input signals into Outputs for 8 channels, voltage free, double throw contacts, rated for 24 Vdc., 0.5 Amp. The channel input status is indicated by LED’s. The Inputs and Outputs are galvanically isolated.

DO-521 relays Output module
This module is intended for the connection of high loads. It converts 6 pulse-train signals into voltage-free output contacts, rated for 2.5 Amp. The channel input status is indicated by LED’s. The Outputs are galvanically isolated.
**RE-522 relays Output module**
This module is applied as a contact-multiplier for 4 channels and can be configured in various ways. Contacts are rated for 0.5 Amp., 24 Vdc. The input status is indicated by 4 LED's.

**DO-524 relays Output module**
This module is intended for the connection of small loads. It converts 8 pulse-train signals into voltage-free output contacts, rated for 0.5 Amp. The channel input status is indicated by LED's. The Outputs are galvanically isolated.

**FG-525 normally de-energised Output**
For Outputs that are normally de-energised or 'energise-to-trip' this module is applied. It provides failure detection in the OFF-state on the board as well as field loop line monitoring both for open and short-circuit. A common fault-annunciation output will hold a memory until the next reset.
The input of pulse-train signals for 2 channels is converted into 24 Vdc., 20 watt. The 6 LED's indicate for 2 channels: Output voltage, normal operation and error.
This module is designed for use in Fire & Gas systems for deluge and other extinguisher Outputs.

**Logic & Timer modules**

**Logic-function modules**
The logic function modules for the SLS have different combinations of predefined logic-elements and serve to execute the functional logic of the ESD system, as laid down in the Functional Logic Diagrams or the process cause & effect diagrams, representing the process safety interlocks. Various different modules exist, each containing a different combination of single and multiple logic gates.
Individual LED's indicates the output status; also an interface for the ProSafe-COM is incorporated on each module.
The FLD function is programmed by interconnection of the logic gates that are ready-made on these standard building-bricks:
- FM-550
- FM-551
- FM-552
- FM-553
- FM-556
- FM-557.

![ProSafe-DSP SLS logic modules](image-url)
**TI-540 redundant timer module**
The module contains two multiple-function timers with logic pulse-train input & output. The operating principle is based on counting the system clock pulses. For fail-safe applications the two timers should be used in a 2 input AND gate. The range can be set between 7 msec. and 70 hours by means of strapping on the mating connector. The various timer states are indicated by 7 LED's.

**TI-544 inherently fail-safe timer module**
This module contains a single channel inherently fail-safe timer for AK7 applications. The operating principle is based on the discharge of a capacitor and generates a logic pulse-train signal at the output. By the limited stored energy in the capacitor, the time can never exceed the pre-set time in a faulty condition.
The range of 1.5 to 310 seconds is set by the strapping on the mating connector. The operation states are indicated by 3 LED's.

**Logic-Timer module LT-150**
The module LT-150 for the PLS processes the safety-related logic and can be used in redundancy, in a dual or TMR configuration, for increased availability. The input signals come either from fail-safe input modules, analogue trip amplifier or from logic interconnections, which are Outputs from other LT-150 modules, located in other PLS boxes. Outputs signals are again either connected to fail-safe Outputs, or interconnected to other PLS boxes.
The LT-150 module can operate in the following modes: 'operational', 'disabled' and 'down-load', while only the relevant functions can be carried out in each mode. In the download mode an application program can be loaded across the serial interface and stored. If the module is not running in the operational mode, all the Outputs are disabled. In every mode it can handle 40 digital Inputs and 24 digital Outputs according to the program representing the necessary logic instructions, including AND, OR, NOT, TIMER and covering all combinations hereof. In the operational mode a full inherent self-test and diagnostics are executed continuously. Any voting error results in a permanent switch-off, within a few milliseconds.
The application program is stored in EEPROM. In the 'down-load' mode acceptance of status-data transfer is allowed via the communication bus. This updates the LT-150 module during a 'hot-repair' procedure. Logic data processing is driven by the hardware structure and consists of the execution of a fixed number and fixed sequence of logic instruction steps, comprising 'Load', 'And', 'Or' and 'Set' (LAOS). The entire processing sequence is executed every millisecond. After every processing cycle, all output results are cleared, and recalculated during the next scan-time of 1 millisecond. For the timer functions a limited number of safety timers is available, as well as a large number of multi-purpose timers. Timer ranges from 1 sec to 10.5 hours.

Indication of a voting-error condition occurs, when at least one of the 16 voted signals coming from the output modules, differs from the corresponding output value on the logic module itself. This results in the disabling of the involved output. Data processing and diagnostics are executed simultaneously and continuously, when running in the operational mode. Any abnormal condition will result in an alarm indication on the common error output line and will be indicated by the corresponding LED at the front of the module and via the CP-180 and the ProSafe-COM.

Data communication across the system-bus functions in the active modes.
DSP Auxiliary modules

For additional functionality auxiliary modules are available that do not interfere with the Safety performance of the SLS or PLS system.

FD-509 for separation between Safety & non-safety system parts
This module can be used for separation between the safety-related parts of a DSP system and the other modules if necessary. The module contains 10 de-coupling circuits for pulse-train Inputs & Outputs that are galvanically isolated. A failure in the non-safety parts can never jeopardise the safety of the safety-related parts.

AF-533 for fuse-monitoring
The AF-533 module is user to monitor fuses by a fail-safe circuit. Also fuses that normally have no current are monitored continuously.
A common relay contact on each module provides remote alarming of a faulty fuse. At the front of the module, a LED provides indication of which circuit has failed. Fuses are replaceable from the front panel of the module. The module contains circuits for 6 fuses on the front and individual LED status indication.

AC-534 for line-monitoring normally energised loops
Output & input loops can be monitored continuously by this module. It will detect an open-loop or a short-circuit of 4 loops by means of a low test current. It provides galvanic isolation of each loop and individual LED indication.
A common annunciation contact will retain a memory until the next reset.

AC-535 for line monitoring of Inputs that are normally de-energised.
Performance similar to AC-534 module.

SA-539 system alarm module
This module provides a centralised fault-annunciation via alarm lights and a relay. Eight categories of faults are distinguished, including power supplies, clock/timers, fuses, circuit breakers, etc. At the front 8 LED’s show the fault categories; the same information is available via the COM interface.

AO-543 annunciation module
This module has two independent annunciation circuits to handle system fault signals and operator actions (acknowledge, reset, etc.). Common Outputs like an audible alarm or flash signal are possible in combination with the KA-549 module. Each circuit is connected to one indication light. The module has following characteristics:
• Inputs can be either logic pulse-trains or DC
• galvanically isolated Inputs
• various annunciation sequences are supported (A, M, F 2A, F 3A)
• first-failure detection
• LED and lamp output
• interface for ProSafe-COM.

DR-546 multi-purpose module
This empty printed circuit board can be used for additional components in max. 20 independent circuits. The C1 version of this module contains multi-purpose diodes. The D1 version contains pre-installed diodes and resistors and is typically used for inter-trip connections, when one output is connected to several Inputs.

KA-549 annunciation auxiliary module
This module is for use in combination with module AO-543; it contains a horn driver circuit as well as two reflash and a single flash generator circuit. Status indication by 4 LED’s.
TP-591 test print
This test print is provided with 2x9 LED’s and can be used to check the TI-540 timer settings. It contains a reference list, which is printed on the card.

Clock - power & communication modules

CP-180 Clock & Power supply module
The PLS Clock & Power module is also a communication module. It generates system logic-pulses and creates several galvanically isolated voltages, sufficient for one box pair. Two CP-180 modules can be configured in a redundant mode for fault-tolerance. The power-supply is protected for over-voltage and over-current and has frequency error detection for the logic-clock. For redundant use, the Outputs are coupled by diodes to the power-bus. The logic-clock pulse distribution is monitored, while the status is displayed at the front panel of the module. A common fault indication is provided via the activation of a contact. For controlled replacement of this Clock-Power module, a disable switch is mounted at the front. The module has a bi-directional communication (RS-485 Combus) with all modules in other PLS boxes. This data bus collects input/output, status, events and error information. In addition, the CP-180 provides the ProSafe-COM system interface, which can be connected simultaneously to the maintenance interface and the DCS. The second function is the information exchange between logic modules in case of ‘warm’ start-up after replacement of a logic module. The third function is to transfer safety-related data, for use by the non-safety-related logic modules. These two communication ports can operate simultaneously.

BP-190 Back plane module
The back plane for the PLS serves for all the standard interconnections between modules in a 19 inch rack. The back plane is suitable to accommodate one ‘box pair’ and has following characteristics:
• The back plane is a multi-layer printed circuit board mounted with 28 connectors, mating with the installed modules. It interconnects the following electric signals:
  - the system bus containing all signals necessary for other modules;
  - the logic connections from Digital Inputs to the Logic-Timer modules;
  - the logic connections and supervision feedback signals between Logic-Timer modules and fail-safe Output;
  - system clock for logic signals;
  - power distribution from redundant power supplies;
  - data communication;
  - system error and alarm signals;
  - strapping signals for module identification.

PS-502 power supply module
The power for the SLS logic-solver is generated by this module. It derives 20 Volt, galvanically isolated, from the 24 Volt field power. The module has an electronic over-current protection. LED’s indicate the presence of the input & output voltages. The version A1 has a 24 Volt output.

CL-530 system clock module
The clock module generates the pulse-trains ‘A’ and the phase-shifted ‘B’ pulses, as used in all modules that contain the basic SLS-circuit, such as for the logic-solver, input modules, etc. Also the ProSafe-COM employs this clock for data-collection and timestamping. LED’s indicate the presence of A & B pulses and various module conditions.

The A2 version of the clock module is designed for redundant use and has a ‘hot’ repair capability.
**MC-569 Power supply for data collection modules**
This module provides the necessary stabilised voltages such as 8, -12, +12 Volt, derived from the 24-Volt field supply. It supplies power for up to 32 modules from the MC-5xx range. LED's indicate the presence of the 3 voltages.

**PS-903 main power supplies module**
For maximum reliability, the 24-Volt output is stabilised using the ferro-resonance principle. The nominal output current is 20 Amps with 'fold-back' limitation at 30 Amps. The input voltages are 110, 120, 220 or 240 Vac, at 50 Hz or 60 Hz. An incorporated diode allows the use in parallel to increase the power handling capacity, or for power redundancy. Failure will be indicated by a LED and a relay output contact.

---

**The ProSafe-COM modular communication interface**

The ProSafe-COM is the system name that covers the SER and all interface functions between the ProSafe-DSP and other Data Processing systems, such as the MMI, DCS, etc. As a result of the modular structure, it can be configured to fit a particular application.

The ProSafe-COM system employs the following communication modules:

**MC-562 Analogue communication Input module**
Analogue to digital conversion with 8-bit resolution for 8 channels Inputs after filtering by a low-pass filter of 3 Hz. The voltage Inputs are isolated from the communication processor that interfaces with the local RS-485 network. LED's indicate the proper functioning of communication.

---

ProSafe-DSP system network.
MC-573 Data collection module
The module can collect data from max. 12 modules. The scan interval is 1 millisecond. Data changes are stored with a time-stamp and communicated to the ProSafe-COM system. LED’s indicate the proper functioning of communication with the local RS-485 network.

MC-576 Output driver module
Via the RS-485 local network, 12 pulse-train Outputs can be controlled that create logic Inputs for the ProSafe-DSP system. At the front panel LED’s indicate the proper functioning of communication.

MC-581 Digital input module
For interfacing additional DC signals, this module converts 16 Inputs at 24 Volt for communication with the MC-573 data collection module.

MC-582 Pulse-train input module
For interfacing 16 additional Pulse-train signals, this module communicates with the MC-573 data collection module.

MC-584 & MC-585 Parallel interface
The 32 discrete Outputs can be used to present status information that originate from the ProSafe-DSP system, to external equipment such as a DCS or SCADA system. The time-resolution is 1-millisecond. The Inputs for the MC-584 are maximum four (8-bits) shift-registers from any other DSP module. The MC-585 is the rail-mounted termination connector that contains 32 LED’s for status indication.

CO-950 Basic Communication module
This communication processor is an industrial PC, which consists of a 5 slots bus-board carrying standard PC modules: CPU, dual ported COM ports and a local network controller. The CO-950 can be equipped with up to 4 serial ports (default 2) and runs the standard or extended ModBus protocol for status & event retrieval and override commands. A fifth serial COM port is used for configuration and maintenance, or can be connected to the optional LCD display & keyboard CP-953. The ProSafe-DSP modules are interrogated via a dedicated Local Network.

Depending on the application additional modules can be added. This industrial PC hardware platform supports the following (non-safety) functionality:
• Presentation of the ProSafe-DSP status to DCS and other equipment;
• Communication & scaling of the analogue Inputs from ProSafe-DSP;
• Creating Inputs for overrides, etc., in the ProSafe-DSP;
• Sequence of Event Recording;
• Time-stamp of the Events from the ProSafe-DSP system;
• Synchronising the real-time with i.e. DCF-77, GPS or other source;
• Presentation of diagnostic information.

CS-951 Serial interface module
By adding this module to the CO-950 the total number of serial ports will be four.

CP-952 Printer interface module
A parallel printer port is provided by this module.

CP-953 LCD & keyboard interface module
This module is meant to create access to ProSafe-COM for the process operator or maintenance engineer.
**CE-954 Ethernet Controller module**
The CE-954 will create an Ethernet interface using either the TCP/IP or UDP/IP protocol.

**CN-955 Local-Network controller module**
For large ProSafe-DSP systems or redundant systems this module creates a second Local-Network, that interrogates the DSP modules.

**MI-983 & MO-986 Matrix-controller input & output module**
For interfacing with solid-state matrix-panels these modules will monitor the Inputs from push-buttons & key-switches and create Outputs for signal lamps. The communication with the basic CO-950 is via the dedicated Local Network. Proper operation is indicated via LED's on the front panel.

**BR-987 & BR-988 Local-Network repeaters**
The dedicated Local RS-485 Network segment connects a maximum of 32 DSP modules and has a length that may not exceed 300 meters. If more segments are required, the BR-987 can be used to create another isolated segment. Up to five BR-987 may be cascaded.
The BR-988 is a fibre-optic bus repeater and is designed to extend the Local-Network over a long distance of maximum 3000-meter and has redundant fibre-optic ST-connections.
Glossary of terms

2003: see at 'TMR'.
availability: The probability that a system is capable to fulfill its function at some instant of time. Practically it is often assumed to be constant and expressed in the 'FTR'.
cause & effect diagrams: 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 causing coincident failures of two or more separate channels in a redundancy system, leading to system failure. (See also at 'Systematic failures').
covered 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. demand: The excess of a process safety-parameter beyond the safety limit, necessitating a trip of the process by intervention of the SIS.
demand-rate: The frequency of a process trip demand.
diagnostic coverage factor: The percentage of failures detected by manual or automatic diagnostic tests. It can be expressed 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.
dangerous failure: A failure which has the potential to put the safety-related system in a dangerous or fail-to-function state.
decided: See at 'voter'.
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 move to the safe position, because the energy is cut off. Larger valves are moved by releasing compressed air by means of the electrically de-energised valve.
demand: DCF-77: Accurate time signals broadcasted from Germany, Frankfurt, with a range of approximately 1000 km. Comparable time signals, with different coding are available in the USA, Fort Collins and in the UK, Rugby.
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
error: A detected discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition. An error is that part of the system state, which is liable to lead to a failure.
event: A change of state of Inputs or Outputs, as well as intermediate logic status.
fail-safe: The built-in capacity of a system such that predictable equipment failure modes only cause system failures in which the system reaches and remains in a safe fall-back state. - A control system that, after one or multiple failures, goes into a predetermined safe condition.
failure: Loss of function of a single component, system part, or of the entire system.
fault: An abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
fault-avoidance: The use of techniques and procedures, which aim to avoid the introduction of faults during any phase of the safety system lifecycle.
fault-tolerant: A system that continues to fully perform its functions without interruption, in spite of component failures or errors.
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.
FPSO: Floating Production & Storage & Offloading.
FTR: False Trip Rate. It equals 1/MTNF. Also refer to 'Availability' & 'Nuisance failure'.
GPS: Global Positioning System with absolute time-synchronisation capability.
HIPPS & HIPS: High Integrity (Pressure) Protection System. Also called: 'Over Pressure Protection System' or 'OPPS'.
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.
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 bug. Also referred to as ‘soft-error’. See also under ‘undetected failure’.
LED: Light Emitting Diode.
Maglog: A former name for the solid-state and inherently fail-safe technology, which employs magnetic cores as logic-gate elements. This technology is used in the ProSafe-DSP system.
MTTR: Mean Time To Repair. The mean time between the occurrence of a failure and the return to normal failure-free operation after corrective action. This time also includes the time required for failure detection, failure search and re-starting the system.

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

Safety Integrity: The probability of a SIS satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. See at 'SIL'.

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.

Viack: A failure that impairs the system Safety, but remains un-detected. 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. By definition redundancy and voting devices are no remedy for this type of un-safe failures. (see also under ‘covert failure’).

Validation: Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

VDU: Video Display Unit.

Verification: Confirmation by examination and provision of objective evidence that the requirements have been fulfilled.

VFC: Voltage Free Contact.

Voter: In a redundant system configuration this decider hardware (and/or software) is applied to compare the performance/results of modules and to make a selection based on fault-tolerance for detected-faults. The structure of the voting device will determine whether this will improve the safety and/or the availability of the system. (See also at: ‘un-detected failure’).

SIS: Safety Instrumented System.

soft-error: See at ‘intermittent fault’.

solid-state logic: An adjectival 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.

state-machine: Also called a ‘finite state-machine’ is used to build sequential logic circuits, that is are capable to execute a (small) control task fully autonomously. The hardware is characterised by ‘present state’ and ‘next state’, with ‘conditional transitions’, opposing to the technology as found in traditional combinatory gate/logic, employed in conventional microprocessors.

systematic failures: A failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

TMD: Triple Modular Redundancy. A solution to achieve fault-tolerance by 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 the standards issued by the IEC, VDE and DIN.

un-detected failure: A failure that impairs the system Safety, but remains un-detected. 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. By definition redundancy and voting devices are no remedy for this type of un-safe failures. (see also under ‘covert failure’).

Validation: Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

VDU: Video Display Unit.

Verification: Confirmation by examination and provision of objective evidence that the requirements have been fulfilled.

VFC: Voltage Free Contact.

Voter: In a redundant system configuration this decider hardware (and/or software) is applied to compare the performance/results of modules and to make a selection based on fault-tolerance for detected-faults. The structure of the voting device will determine whether this will improve the safety and/or the availability of the system. (See also at: ‘un-detected failure’).
9 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 we stay abreast of the evolution of the profession of Industrial Safeguarding.

Yokogawa ISS, as one of the four ‘Centres of Excellence’ within the Yokogawa Corporation, we are committed to offer protection systems of the highest Safety Integrity Level 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 a subsidiary of Yokogawa Electric Corporation is 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 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.