SIL 3 Systems
(Part 3)

Version November 2009
- Functional Safety
- Safety Integrity Levels – SIL
- SIL Capability
Functional Safety

- Functional Safety describes the behaviour of a safety device — meaning HW and SW — in case of an internal failure occurring.
- The target is — "reaching a safe state”

**WHAT DOES IT MEAN?**
It means internal faults in the safety device should be detected by the device itself and shall be indicated and signalled.

The only requirement of the standards is safety!
Safety and Availability

- A safety device, which will shut down the monitored production line or better the whole plant.
- In any case of the smallest probability of a potential failure, this is safe and will comply to the standards reaching a high SIL.

*BUT will The Customer be happy with it?*

*What about the system’s availability?*
The standards requires safety ...

... The Customer requests availability

- Safety and availability must not be a contradiction!
- The solution stays in systems with fault tolerance, which is typically related to high SIL
Fault Tolerance

- Fault tolerance means the safety device is still in operation and in measuring mode after the fault situation has been detected.
- Operation will proceed eventually with reduced functionality.

.. which leads to the Emergency Mode
Emergency Mode

- The SIL-standard in gas detection (EN 50402) permits explicitly an “emergency mode”
- Defined for a specified period of time for redundant systems.
- After detection of an internal fault the system is not longer redundant but still fully operational.

This allows time to repair for the safety device without the need to shut down the monitored system.
SIL = Safety Integrity Level

- SIL describes the different levels of “Functional Safety” on a safety device

- The values are defined from SIL-1 (lowest) up to SIL-4 (highest)

- Which doesn’t mean SIL1 is (too) low

Example: A typical gas detection device (system) with ATEX-Certificate including the functional approval according IEC 61779, with regular maintenance is equivalent to SIL-1
Typical examples of SIL levels

- **SIL 1**: A typical gas detection device / system with ATEX-Certificate

- **SIL-2**: Typically reached by
  - self testing facilities for HW.
  - reduced maintenance intervals
  - specific SW requirements and documentation.
Typical examples of SIL levels

- **SIL-3**  The main requirement: One failure shall not cause an unsafe state

  *Therefore a SIL 3 is a fail-safe system*

  - Step SIL 2 – SIL 3 is typically reached by redundancy
  - Specific SW requirements are added

- **SIL-4**  Sometimes requires triple redundancy
**Different Classes of Faults**

- Safe detected
- Safe undetected
- Dangerous detected
- Dangerous undetected

Above classification important in design to determine the “Safe Failure Fraction”, specific for each SIL level

Which may be classified as:

- Random faults
- Systematic faults
Different Classes of Faults

- Random faults – occur occasionally
- Systematic faults – occur at specific conditions
  Reproducible should the same conditions apply

*HW features both random and systematic faults*

*SW features only systematic faults*
SIL - Capability of modules

- Simple modules –
  - Relays
  - Sensor element
  - any simple analogue electronics circuit

- Complex modules
  - microprocessor based systems
In a complex system different modules are combined together

- SIL capability is determined by the modules combination
  - series modules – “weakest” module gives the combination SIL
  - parallel modules – SIL capability may increase by one level
SIL – Capability of a Safety function

Safety function – the combination of modules
In a gas detection system:
Ex. Gas detection system: combination of modules
from gas inlet (sensor) to the output device (relay)

- Different options in the modules combinations lead
to different safety functions

HW and SW combinations are evaluated in
different ways
SIL – Capability of a Safety function

In combination

HW  SIL-2
SW  SIL-2

HW  SIL-3
SW  SIL-2

SIL 2
SIL – Capability of a Safety function

HW SIL-2
SW SIL-3

In combination

HW SIL-3
SW SIL-3

SIL 3

HW SIL-2
SW SIL-3

Pre-requisites
Logical consequences for a new system

- To increase the availability, redundancy should be implemented – double processor system.
- If one processor is faulty – emergency mode – still fully operational
- SW developed according to SIL 3
- With redundant detectors and redundant relays the systems may reach SIL 3

... as a consequence, the items above describe Galileo Multisystem
The new control unit GALILEO Multisystem was designed in accordance with the SIL standard, so the system hereby presented would comply with the various SIL levels according to the standard EN 50402.

Where not detailed in the above mentioned standard, the various chapters of the IEC61508 were followed, especially:

- IEC61508 - 2 for the E/E/PES
- IEC61508 – 3 for the SW requirements
All decisions are taken at the CPU level
Configuration data are redundant and may be found at three levels:
  - CPU
  - Module
  - Detector – where available intelligent detector
Devices to be monitored may be
  - standard 4..20mA analogue output devices
  - addressable devices communicating in RS485 loop
  - simple switches through digital inputs
Full system structure is based on RS485 communication loop
Main features 1/2

- 4 RS485 loops;
- up to 256 programmable field inputs;
- up to 512 programmable field outputs;
- Mother Board redundancy;
- Loop redundancy - optional;
- RS232 PC interface;
- Display/Signalling user interface;
Main features – 2/2

- “Low battery” supervising circuit and “NO battery” signalling.
- Auxiliary power outputs 12/24VDC fuse protected;
- Output modules with relays.
- Loop configuration self-check.
- 6 main operating conditions, implemented in accordance with the CEI standards and EN50402
Operation states 1/2

Three operation states:

- Normal – usual operative state, no particular events, everything working properly;
- Alarm – one or more channels are exceeding one or more of the gas alarm levels;
- Emergency – any of the situations which guide to degrading from SIL3 or SIL2 system to SIL2 or SIL1 respectively.
And three special states:

- Fault – one or more devices in the system are in fault condition or malfunctioning state;
- Test/Maintenance– this status is up to the operator in order to test various parts of the installation and for Calibration purpose also;
- Unset – total or partial unset of the various parts or the system.
4 serial ports RS485 and the whole capacity to all loops as follows:

- 256 analogue inputs and addressable detectors
- 64 digital inputs
- 256 analogue outputs – further development
- 512 relay outputs.
System configurations 2/3

All devices connected in loop will be galvanic isolated so that the loop may be automatically closed if any discontinuity occurs (mechanical cut-off, or open/short circuit):

- Analogue inputs module;
- Loop modules
- Relay outputs modules;
- Analogue outputs modules – further development
- Monitor module – further development
There are several options to connect the field modules to CPU:

1. 2 closed loops, redundant one to the other, case in which the system will feature whole capacity per each loop, monitoring both the same modules.
The Main Board’s architecture is designed around two microprocessor which are making redundancy one to the other.

Each microprocessor is monitoring one loop.

On the two corresponding loops are connected all the field modules.

This way both microprocessors are monitoring in the same time all field devices.
Details CPU

- External Printer
- External PC
- Power supply 1
- Power supply 2
- Control Unit
- System
- Signalling Interface
- LED’s
- 8 RELAYS
- User Interface
- \( \mu P_1 \)
- \( \mu P_2 \)
- Galvanic isolation

- OVER-RANGE
- ALARM 3
- ALARM 2
- ALARM 1
- UNDER-SCALE
- FAULT
- BATTERY
- FAULT
- BATTERY
- UNSET
- TEST
- POWER

- LOOP 1 (RETURN)
- LOOP 1-0
- LOOP 2-0
- LOOP 2-1 (RETURN)
Signalling interface
- front-end LED signalling -

- Signal LED's
- System LED's

- OVER-RANGE
- ALARM 3
- ALARM 2
- ALARM 1
- UNDER-SCALE
- FAULT

- FAULT
- EMERGENCY
- UNSET
- TEST
- POWER

- 3 red LED - three general ALARM thresholds.
- 1 red LED - "Over-Range" situation
- 1 yellow LED - "Under-Scale" situation.
- 1 yellow LED - loop FAULTS.

- 1 yellow LED - general FAULT.
- 1 yellow LED - general "Unset".
- 1 yellow LED - general Test/Maintenance.
- 1 green LED - power supply.
- 1 yellow LED - Emergency Mode.
3 programmable relays corresponding to the three general alarm thresholds.

2 relays - general Fault (System Fault) – 1 relay redundant for the other

1 relay - Test/Maintenance mode.

2 relay - Emergency Mode – 1 relay redundant for the other.
General Philosophy

- The two µP are communicating one to each other in the way that each one is updated with the other’s status.
- NONE of the two µP can switch off the other one;
- Yet EACH of the two µP can decide to switch off itself if something goes wrong.
- In the case on µP is switching off, the other one continues monitoring also the second loop by means of the redundant microprocessors on all field modules.
Provided with peripherals - responsible for the management of:

- external PC – by means of an RS 232 port;
- external printer by means of a parallel port;
- signalling LED’s on the front panel;
- basic relays on central unit’s level;
- two serial loops LOOP A / LOOP A RETURN - RS 485 ports.
Provided with peripherals - responsible for the management of:

- graphical display LCD – by means of an RS 232 port;
- 24 keys keypad;
- signalling LED’s on the front panel;
- basic relays on central unit’s level, by means of a SPI port;
- two serial loops LOOP B / LOOP B RETURN - RS 485 ports.
Loop devices

All loop devices are addressable, each address identifies uniquely one input or output, as follows:

- Analogue inputs module AIM – 8 analogue + 2 digital address points (out of the 256 + 64 system inputs);
- Loop module – programmable 32 addressable detectors on local loop + 2 digital inputs (out of the 256 + 64 system inputs);
- Relay outputs module – 8 or 16 address points (out of the 512 relay outputs) - basic board or basic + extension respectively)
- Analogue outputs module – 8 address points (out of the 256 analogue outputs) – further development
- Monitor module – 1 address point (out of the 256 + 512 system outputs) – further development
Analogue Inputs Module – AIM 1|5

This module is designed to accommodate 8 analogue inputs (4-20mA type) and two digital inputs.

**Configuration:**

- Each of the 8 inputs on the board is seen individually by CPU, therefore each AIM is occupying 8 addresses in the loop.
- Each input is separately programmable by means of the software.
- The maximum number of such boards in this configuration is 32.
Analogue Inputs Module – AIM 215

Such board will accommodate:

- 4-20mA output gas detectors – on the analogue inputs

NOTE: RS485 communication provided for all 8 channels – 5 poles connection provided for each channel

- used for setting up the detector’s configuration at system setup and to retrieve further details in case of FAULT

- remote push buttons or switching outputs – on the digital inputs
AIM’s architecture is designed also around two microprocessors making redundancy to each other.

- the two µP of AIM are connected separately on two loops.
- the two µP are sharing status data to each other, by means of I2C bus;
- NONE of the two µP is physically connected also to the second loop.
- Each µP has an internal A/D converter;
- All 8 analogue inputs connected to both µP through 2 external MUX, switching the communication to the 8 channels, one at a time;
- EACH of the two MUX is connected to BOTH microprocessors on board;
- RS 485 MUX will point towards µP № 1 ONLY;
Analogue Inputs Module – AIM 4/5
The module is designed so that it might be used also as an independent central unit. Therefore it is be provided also with the possibility of being connected to:

- an external PC – RS 232 port on µP № 1;
- digital display – RS232 port on µP № 2;
- LED’s board – connected through SPI ports on both µP;
- Relays board - connected through SPI ports on both µP;
- Keypad – parallel port on µP № 2.
- Same as in the system, the two µP are sharing status data to each other, by means of I2C bus;
Loop Module 1/5

- Designed to accommodate one loop of 32 addresses. The loop cycle expected is 0.5s.
- In plus two digital inputs are available.

Configuration:
- Each of 32 addressable detectors on loop will be seen individually, therefore each such board is occupying 32 addresses in the main loop of the system.
- This way each input will be set separately by means of the software.
- The maximum number of such boards in this configuration is 8.
- Such board will accommodate addressable gas detectors SMART type.
- Local loop is a closed loop, RS485 type.
Loop module 2/5

Such board will accommodate:

- addressable SMART gas detectors – on the local loop
- remote push buttons or switching outputs – on the digital inputs
Loop module’s architecture is designed around two microprocessors making redundancy to each other.

- the two µP of Loop module are connected separately on two loops.
- the two µP are sharing status data to each other, by means of I2C bus;
- NONE of the two µP is physically connected also to the second loop.
- The two ends of the local loop are connected each one to one µP through RS485 ports;
- This way BOTH microprocessors see the local loop;
Loop Module 4/5

Loop Module

Galvanic isolation

Control Unit

LOOP Module

μP1

μP2

LOOP 1-0

LOOP 2-0

LOOP 2-1 (RETURN)

LOOP 1-1 (RETURN)

CLOSED LOOP 32 Detectors
The module is designed so that it might be used also as an independent central unit. Therefore it is be provided also with the possibility of being connected to:

- an external PC – RS 232 port on µP № 1;
- digital display – RS232 port on µP № 2;
- LED’s board – connected through SPI ports on both µP;
- Relays board - connected through SPI ports on both µP
- Keypad – parallel port on µP № 2.
- Same as in the system, the two µP are sharing status data to each other, by means of I2C bus;
The module is meant to be used as output device, managing up to 16 relays.

Basic board is microprocessor based, provided with 2 microprocessors each being connected to one of the two loops coming from the central unit.

- Each of the 8 outputs on the board will be assigned an individual address from 1 to 512, therefore such board will occupy 8 addresses (or 16 in case basic board is provided with extension module of 8 relays).

- Each output will be this way separately set, by means of the programming software.

- The maximum number of such boards is 32 (or 16 in case basic board is provided with extension module of 8 relays).
Relay Module 2/3

- 2 µP’s on board, connected separately on two loops, and none of them physically connected on the second loop
- both µP’s are managing 8 relays on the basic board or 16 relays in case the extension board is used.
  - On the main board - 8 relays, rated 4A@250V; DIP switches for each of the 8 relays to set the NO/NC operation mode;
  - On the extension board - 8 relays, rated 16A@250V;
- galvanic isolated connection with the two loops communicating with the central unit;
- provided with connectors to accommodate superposed extension board with additional 8 relays;
Relay Module 3/3
Loop A redundant with loop B

µP № 1 redundant with µP № 2

NO redundancy on detectors level
Loop A redundant with loop B
- μP № 1 redundant with μP № 2
- Redundancy on detectors level
SIL configurations - option

- Loop A redundant with loop B
- μP № 1 redundant with μP № 2
- Redundancy on detectors level
Whole system configuration is done by means of PC software.