HIMA-SELLA

HIMA-SELLA LIMITED

SAFETY CONTROL & AUTOMATION SYSTEMS

your **safety**… our **future**

- Burner Management (BMS)
- Emergency Shutdown System (ESD)
- Fire & Gas Detection (F&G)
- High Integrity Pressure Protection Systems (HIPPS)
- Integrated Control & Safety System (ICSS)

- Control Panels
- Marshalling Cabinets
- Instrument Cabinets
- PLC Panels
- DCS / SCADA
- Tiled Mosaics

- Train Control Systems – selective door opening
- Customer Information Systems (CIS)
- Radio Remote Control
- Locomotives
- Cranes
- Telemetry
- SCADA

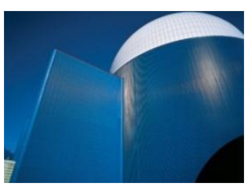
Hima-Sella is an independent market specialist, designing and supplying integrated safety, control and automation systems to the following industries :

- **Chemical**

- **Petrochemical**

- **Defence**

- **Power**

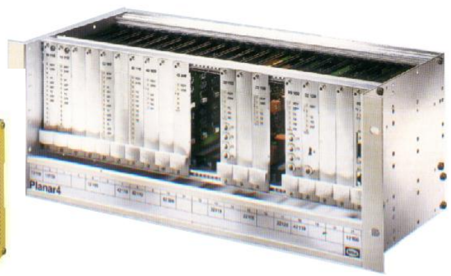


- **Nuclear**

- **Steel**

- **Oil & Gas**

- **Transport**



HIMatrix F30 **Planar4** **HIQuad** **HIMax**

SIL Calculations

Easy or Difficult

Presentation by
Ian Parry Functional Safety Specialist

SIL calculations are easy

Just follow Part 6 of the standard IEC 61508

Abbreviations	Term (units)	Parameter ranges in tables B.2 to B.5 and B.10 to B.13
T_1	Proof test interval (h)	One month (730 h)[1] Three months (2 190 h)[1] Six months (4 380 h) One year (8 760 h) Two years (17 520 h)[2] 10 years (87 600 h)[2]
MTTR	Mean time to restoration (hour)	8 h Note MTTR=MRT=8 hours based on the assumptions that the time to detect a dangerous failure, based on automatic detection is << MRT
MRT	Mean repair time (hour)	8 h Note MTTR=MRT=8 hours based on the assumptions that the time to detect a dangerous failure, based on automatic detection is << MRT
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)	0 % 60 % 90 % 99 %

Abbreviations	**Term (units)**	**Parameter ranges in tables B.2 to B.5 and B.10 to B.13**
β	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_{D)}$	2 % 10 % 20 %
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta D$)	1 % 5 % 10 %
β_{DU}	Dangerous Failure rate (per hour) of a channel in a subsystem	0.05×10^{-6} 0.25×10^{-6} 0.5×10^{-6} 2.5×10^{-6} 5.0×10^{-6} 25×10^{-6}
PFD_G	Average probability of failure on demand for the group of voted Channels (If the sensor, logic or final element subsystem comprises of only one voted group, then *PFDG* is equivalent to *PFDS*, *PFDL* or *PFDFE* respectively)	
PFD_S	Average probability of failure on demand for the sensor subsystem	
PFD_L	Average probability of failure on demand for the logic subsystem	
PFD_{FE}	Average probability of failure on demand for the final element subsystem	
PFD_{SYS}	Average probability of failure on demand of a safety function for the E/E/PE safety-related system	

Abbreviations	Term (units)	Parameter ranges in tables B.2 to B.5 and B.10 to B.13
PFH_G	Probability of failure per hour for the group of voted channels (if the sensor, logic or final element subsystem comprises of only one voted group, then PFH_G is equivalent to PFH_S, PFH_L or PFH_{FE} respectively)	
PFH_S	Probability of failure per hour for the sensor subsystem	
PFH_L	Probability of failure per hour for the logic subsystem	
PFH_{FE}	Probability of failure per hour for the final element subsystem	
PFH_{SYS}	Probability of failure per hour of a safety function for the E/E/PE safety-related system	

Abbreviations	Term (units)	Parameter ranges in tables B.2 to B.5 and B.10 to B.13
λ	Total Failure rate (per hour) of a channel in a subsystem	
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0,5 λ (assumes 50 % dangerous failures and 50 % safe failures)	
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)	
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)	
λ_{SD}	Detected safe failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected safe failure rates within the channel of the subsystem)	

Abbreviations	Term (units)	Parameter ranges in tables B.2 to B.5 and B.10 to B.13
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)	
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)	
$t_{CE'}$	Channel equivalent mean down time (hour) for 1oo2D architecture (this is the combined down time for all the components in the channel of the subsystem)	
$t_{GE'}$	Voted group equivalent mean down time (hour) for 1oo2D architecture (this is the combined down time for all the channels in the voted group)	
T_2	Interval between demands (h)	
K	Fraction of the success of the auto test circuit in the 1oo2D system	
PTC	Proof Test Coverage	
1	High demand or continuous mode only.	
2	Low demand mode only	

SIL calculations are easy

Just follow Part 6 of the standard IEC 61508

And the formulae therein.

IEC 61508–2000 Part 6 formulae

1oo1

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$$

1oo2

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{GE}\, t_{CE}$$

$$+ \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

2oo2

$$PFD_G = 2\,(\lambda_{DU} + \lambda_{DD})t_{CE} = 2 \times 1oo1$$

1oo2D

$$t_{CE}^{l} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})}$$

$$t_{GE}^{l} = \frac{T_1}{3} + MRT$$

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}^{l}\, t_{GE}^{l}$$

$$+ 2(1-K)\lambda_{DD}\, t_{CE}^{l} + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

2oo3

$$PFD_G = 6\ ((1-\beta_D)\lambda_{DD} + (1-\beta)\ \lambda_{DU})^2\ t_{CE}\ t_{GE}$$

$$+\ \beta_D\,\lambda_{DD}\ MTTR + \beta\,\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

SIL calculations are easy

Just follow Part 6 of the standard IEC 61508

And the formulae therein.

SIL calculations are easy

So we have following failure rate data

$\lambda_{DU} = 1 \times E-09$

$\lambda_{DD} = 1 \times E-06$

$\lambda_{S} = 8 \times E-06$

What does ‘safe’ and ‘dangerous’ mean?

Terms “safe failure”, “dangerous failure” and hence the “safe failure fraction” for an instrument are only relevant with respect to the declared **specific application**

For example, if: $\lambda_{TO\ OPEN} = 50$ FITS; $\lambda_{TO\ CLOSE} = 500$ FITS

Note : 1 FITS = 1.00×10^{-9}

Then : SFF can be either 50/(50+500) = 9% or 500/(50+500) = 91%

(depending on which failure mode is the safe one for your application)

Don’t reject a certificate for an instrument where your specific safety context is not defined and hence no SFF is given – this might be totally appropriate!

1oo1 (Tx, logic solver, valve)

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$\lambda_{DU} = 1 \times E{-}09$

MTTR = MRT = 8hr
If MTTR << MRT

MRT = 8hr

$\lambda_{DD} = 1 \times E{-}06$

$T_1 = 1yr = 8760Hr$

$t_{CE} = 12.3756$

$$PFD_G = (\lambda_{DU} + \lambda_{DD})\, t_{CE} = (1.001 \times E{-}6) \times (12.3756)$$

$$= 1.238 \times E{-}5$$

B.3.2.1 Procedure for calculations

The average probability of failure on demand of a safety function for the E/E/PE safety-related
system is determined by calculating and combining the average probability of failure on
demand for all the subsystems which together provide the safety function. Since in this annex
the probabilities are small, this can be expressed by the following (see figure B.2):

$PFD_{SYS} = PFD + PFD + PFD$

where

- *PFDSYS* is the average probability of failure on demand of a safety function for the E/E/PE safety-related system;
- *PFDS* is the average probability of failure on demand for the sensor subsystem;
- *PFDL* is the average probability of failure on demand for the logic subsystem; and
- *PFDFE* is the average probability of failure on demand for the final element subsystem

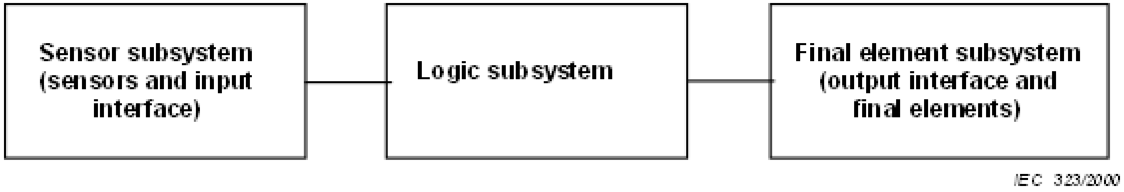


Figure B.3 – Subsystem structure

REMEMEBER

SIL calculations

Come as two calculations!!!!!

PFD or PFH

AND

Safe Failure Fraction – SFF

AND

HARDWARE FAULT TOLERANCE – HFT

So it is that easy

All you need to do is the calculations

Now the DIFFICULT

Voting configurations?

DATA source?

β Beta Factors?

Proof Test Intervals?

Voting configurations!

1oo1 / 2oo3 easy

1oo2

Is it either one to maintain operation or any one out of two to trip

2oo2

Is it either both to maintain operation or two out of two to trip

DATA Sources

1) Supplier SIL data/ Certification Reports

2) Proven in Use

3) OREDA/ EXIDA/FARADIP data bases

β Beta Factors

Beta factors are utilised in the voting configurations and are the common cause factors

The standard defines three values

β = 2%, 10% and 20%

β_D = 2%, 10% and 20%

Normal value is either 10 % or 20%
2% is usually only valid if advised by the supplier.

Proof Test Interval

This is usually allocated as 1 year (8760hrs)

However this value should be supplied by End User as it a function of the site testing routine.

Also sometimes when claiming compliance with a SIL level we have seen proof test intervals of 1 month applied by suppliers.

Ideally unless there is a pressing reason and the End User is in agreement then the PTI should not be less than 1 year.

BE CAREFUL the PTI should not be more than 50% of the demand rate.

So while the calculations are EASY

There are other considerations which also need to be addressed
To ensure the system is compliant with the allocated SIL level.

These are the difficulties as it requires a competent person to make supportable decisions that will have an influence on the systems SIL capability.

Discussion

As always the questions are:

What?

Why?

When?

WHow?

Where?

Who?

With thanks to Rudyard Kipling

61508 Association Toolbox talks available on our website www.61508.org
for free and unlimited distribution so long as acknowledgment of source is included.

- Hymn sheets
  - Directors
  - Senior management
  - Purchaser
  - Project Manager
  - Project Engineer
  - Inspection and QA
  - Operations
  - Maintenance
  - Service Engineer
  - Sales Person
  - Installers
- Other important information
  - What is Functional Safety Management
  - Proven In use, Prior use claims
  - Functional Safety management cross-reference between IEC 61508 and IEC 61511
- SAFETY INSTRUMENTED SYSTEMS are too important to leave to chance!

HIMA-SELLA

HIMA-SELLA LIMITED

SAFETY CONTROL & AUTOMATION SYSTEMS

your **safety**… our **future**