your safety... our future
The Logical Solution for Safety

- 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
The Logical Solution for Safety
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
<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Term (units)</th>
<th>Parameter ranges in tables B.2 to B.5 and B.10 to B.13</th>
</tr>
</thead>
</table>
| $T_1$         | 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

<table>
<thead>
<tr>
<th>Term (units)</th>
<th>Parameter ranges in tables B.2 to B.5 and B.10 to B.13</th>
</tr>
</thead>
</table>
| **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 %  |
| **$\beta_D$** 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 %  |
| **$\beta_{DU}$** Dangerous Failure rate (per hour) of a channel in a subsystem | 0.05 $\times 10^{-6}$  
0.5 $\times 10^{-6}$  
5.0 $\times 10^{-6}$  
2.5 $\times 10^{-6}$  
25 $\times 10^{-6}$  |
| **$PFD_G$** 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 $PFD_G$ is equivalent to $PFD_S$, $PFD_L$ or $PFD_{FE}$ 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

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Term (units)</th>
<th>Parameter ranges in tables B.2 to B.5 and B.10 to B.13</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PFH_G$</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>$PFH_S$</td>
<td>Probability of failure per hour for the sensor subsystem</td>
<td></td>
</tr>
<tr>
<td>$PFH_L$</td>
<td>Probability of failure per hour for the logic subsystem</td>
<td></td>
</tr>
<tr>
<td>$PFH_{FE}$</td>
<td>Probability of failure per hour for the final element subsystem</td>
<td></td>
</tr>
<tr>
<td>$PFH_{SYS}$</td>
<td>Probability of failure per hour of a safety function for the E/E/PE safety-related system</td>
<td></td>
</tr>
</tbody>
</table>
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Term (units)</th>
<th>Parameter ranges in tables B.2 to B.5 and B.10 to B.13</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda$</td>
<td>Total Failure rate (per hour) of a channel in a subsystem</td>
<td></td>
</tr>
<tr>
<td>$\lambda_D$</td>
<td>Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0.5 $\lambda$ (assumes 50% dangerous failures and 50% safe failures)</td>
<td></td>
</tr>
<tr>
<td>$\lambda_{DD}$</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>$\lambda_{DU}$</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>$\lambda_{SD}$</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Term (units)</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>( t_{CE} )</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>( t_{GE} )</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>( t_{CE}' )</td>
<td>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)</td>
<td></td>
</tr>
<tr>
<td>( t_{GE}' )</td>
<td>Voted group equivalent mean down time (hour) for 1oo2D architecture (this is the combined down time for all the channels in the voted group)</td>
<td></td>
</tr>
<tr>
<td>( T_2 )</td>
<td>Interval between demands (h)</td>
<td></td>
</tr>
<tr>
<td>( K )</td>
<td>Fraction of the success of the auto test circuit in the 1oo2D system</td>
<td></td>
</tr>
<tr>
<td>( PTC )</td>
<td>Proof Test Coverage</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>High demand or continuous mode only.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Low demand mode only</td>
<td></td>
</tr>
</tbody>
</table>
SIL calculations are easy
Just follow Part 6 of the standard IEC 61508
And the formulae therein.
IEC 61508–2000 Part 6 formulae

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

\[ \text{PFD}_G = (\lambda_{DU} + \lambda_{DD}) t_{CE} \]
\begin{align*}
1002
\quad t_{GE} &= \frac{\lambda_{DU}}{\lambda_D} \left( \frac{T_1}{3} + \text{MRT} \right) + \frac{\lambda_{DD}}{\lambda_D} \text{MTTR} \\
\text{PFD}_G &= 2 \left( (1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU} \right)^2 \ t_{GE} \ t_{CE} \\
&\quad + \beta_D \lambda_{DD} \text{MTTR} + \beta \lambda_{DU} \left( \frac{T_1}{2} + \text{MRT} \right)
\end{align*}
PFD_G = 2 (\lambda_{DU} + \lambda_{DD})t_{CE} = 2 \times 1001
1002D

\[ t_{CE} = \frac{\lambda_{DU} \left( \frac{T_1}{2} + \text{MRT} \right)}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})\text{MTTR}} \]

\[ t_{GE} = \frac{T_1}{3} + \text{MRT} \]

\[ \text{PFD}_G = 2 (1 - \beta)\lambda_{DU} ((1 - \beta)\lambda_{DU} + (1 - \beta_D)\lambda_{DD} + \lambda_{SD})t_{CE} t_{GE} \]

\[ + 2(1 - K) \lambda_{DD} t_{CE} + \beta \lambda_{DU} \left( \frac{T_1}{2} + \text{MRT} \right) \]
\[
PFD_G = 6 \left( (1 - \beta_D) \lambda_{DD} + (1 - \beta) \lambda_{DU} \right)^2 t_{CE} t_{GE} \\
+ \beta_D \lambda_{DD} \text{MTTR} + \beta \lambda_{DU} \left( \frac{T_1}{2} + \text{MRT} \right)
\]
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

\[
\lambda_{DU} = 1 \times 10^{-9}
\]

\[
\lambda_{DD} = 1 \times 10^{-6}
\]

\[
\lambda_s = 8 \times 10^{-6}
\]
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: $\lambda_{\text{TO OPEN}} = 50$ FITS; $\lambda_{\text{TO CLOSE}} = 500$ FITS

Note: 1 FITS = $1.00 \times 10^{-9}$

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)

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

\( \lambda_{DU} = 1 \times 10^{-9} \)
\( \lambda_{DD} = 1 \times 10^{-6} \)

MTTR = MRT = 8hr
If MTTR << MRT

\( T_1 = 1 \text{yr} = 8760 \text{Hr} \)

MTTR = 8hr

\( t_{CE} = 12.3756 \)

\( PFD_G = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} = (1.001 \times 10^{-6}) \times (12.3756) \)

= 1.238 \times 10^{-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):

\[ PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} \]

where

- \( PFD_{SYS} \) is the average probability of failure on demand of a safety function for the E/E/PE safety-related system;
- \( PFD_S \) is the average probability of failure on demand for the sensor subsystem;
- \( PFD_L \) is the average probability of failure on demand for the logic subsystem; and
- \( PFD_{FE} \) is the average probability of failure on demand for the final element subsystem.

![Subsystem structure](image)

**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

\[ \beta = 2\%, 10\% \text{ and } 20\% \]

\[ \beta_D = 2\%, 10\% \text{ and } 20\% \]

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!

© 2001-2005, 61508 Association UK, All rights reserved.
your safety... our future