Bureau Veritas
Initiating solutions

For the Benefit of Business and People

TYCO Thermal Controls

PFH Calculations according IEC EN 61508 Standard

Ref.: BN/PTX/CB859/1580190/06/R/216/0

Version	0	1	2
Date	May 31st 2006		
Writer	B. NICOLAS		
Verifier	P. TEIXEIRA		

Table of Contents

1. Introduction

TYCO Thermal Controls is designing and manufacturing a “Leak Detector”. Some of TYCO clients are asking for the PFH (Probability of Failure per Hour) of this equipment according IEC EN 61508 standard.

This report has for objective to demonstrate the PFH reachable by the 2 configurations given below:

⇨ Configuration N°1:
1 component TTC-1 (Detection Module)
1 component FFS (Sensor)
1 cable

⇨ Configuration N°2:
1 component TTC-1 (Detection Module)
6 components FFS (Sensor)
1 cable

This report shows calculations and results in terms of PFH, SFF and the SIL (Safety integrity Level) reachable.

2. References & Glossary

2.1 Standard References

Reference	***Title***
[Ref. 1]	EN/IEC 61508 standard: ✓ Part 1 – 1998-12, 1st edition ✓ Part 2 – 2000-05, 1st edition ✓ Part 3 – 1998-12, 1st edition ✓ Part 4 – 1998-12, 1st edition ✓ Part 5 – 1998-12, 1st edition ✓ Part 6 – 2000-04, 1st edition ✓ Part 7 – 2000-03, 1st edition

2.2 Prisma References

Reference	***Title***
[1]	Trace Tek ⇨ TTC Module de détection à contacts secs TraceTek® Rev 0 ⇨ H53587
[2]	PCB Part Assembly TTC-1 ⇨ 1004-2303 ⇨ Rev G ⇨ 03/09/2006
[3]	Schematic TTC-1 ⇨ 1004-2311 ⇨ Rev D ⇨ 08/24/1990
[4]	Trace Tek ⇨ T-FFS Fiche Technique TraceTek Fast Fuel Sensor
[5]	Schematic TT-FFS ⇨ 1027-0020 ⇨ Rev A ⇨ 06/27/2005
[6]	Failure Evaluation TT-FFS PW.xls given by TYCO Document describing the failure modes of each components, the consequence (dangerous or not), the test performed to detect the failure and the diagnostic coverage.
[7]	Failure Evaluation TT-FFS PW.xls Document describing the failure modes of each components, the consequence (dangerous or not), the test performed to detect the failure and the diagnostic coverage.

2.3 Glossary

Acronym	***Description***
1oo1	1 out of 1 (MooN: M out of N)
DC	Diagnostic Coverage
FMEA	Failure Mode and Effects Analysis
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
PFD	Probability of Failure on Demand
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures
RAMS	Reliability Availability Maintainability Safety
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SFF	Safe Failure Fraction
λ	Failure rate
λ_S	Safe Failure rate
λ_D	Dangerous Failure rate
λ_{DD}	Detected Dangerous Failure rate
λ_{DU}	Undetected Dangerous Failure rate
β	Fraction of undetected failures that have a common cause
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause
μ	Maintenance rate per hour
γ	Failure rate on request

3. Presentation of the system

3.1 Description of the “Leak Detector”

The “Oil Leak Detector” system is made up with one or more sensors, cables and an electronic card.

In this report, only 2 configurations are analysed:

- ⇨ Configuration N°1:
  1 component TTC-1 (Detection Module)
  1 component FFS (Sensor)
  1 cable

- ⇨ Configuration N°2:
  1 component TTC-1 (Detection Module)
  6 components FFS (Sensor)
  1 cable

This system may be considered as a protective system or as part as a protective system as described

3.2 IEC 61508 objectives for 1oo1 system

✓ PFH ([Ref. 1] Part I §7.6.2.9):

The table below gives the objective in terms of PFH (Probability of Failure per Hour) according to [Ref. 1]:

Safety integrity level (SIL)	**High demand or continuous mode of operation** (Probability of a dangerous failure per hour)
1	**$10^{-6} \leq$ PFH $< 10^{-5}$**
2	**$10^{-7} \leq$ PFH $< 10^{-6}$**
3	**$10^{-8} \leq$ PFH $< 10^{-7}$**

- <u>Components Type ([Ref. 1] Part II §7.4.3.1):</u>

The components of the protection system are considered **Type A** as written in [Ref. 1] because:

- For all components of the system, the failure modes are well defined;
- And the behaviour of the system under fault conditions is determined;
- And there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

- <u>Hardware Fault Tolerance & SFF ([Ref. 1] Part II §7.4.3.1):</u>

The protection system has a 1oo1 architecture: there is no hardware fault tolerance.

Safe failure fraction	**Hardware fault tolerance**		
	0	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3
60%≤ SFF <90%	SIL 2	SIL 3	SIL 4
90%≤ SFF <99%	SIL 3	SIL 4	SIL 4
SFF ≥ 99%	SIL 3	SIL 4	SIL 4

<u>Table 2</u>: Architectural constraints on type A safety related subsystems

- <u>In conclusion, the 1oo1 “Leak Detector” system has to meet the following objectives depending on the SIL:</u>

	SIL 1	**SIL 2**	**SIL 3**
PFH to reach	PFH < 10^{-5}	PFH < 10^{-6}	PFH < 10^{-7}
SFF to reach	SFF < 60%	SFF ≥ 60%	SFF ≥ 90%

4. Calculations

4.1 Failure Rates Calculations Description

4.1.1 Reliability data for electronics

The reliability calculations are performed according UTE C 80810 Standard: this standard is the most relevant standard to use currently to calculate electronic reliability.

The definitions are extracted from UTE C 80-810:

MTBF	Mean Time Between Failures
RAMS	Reliability Availability Maintainability & Safety
Tac	Average Ambient Temperature of printed circuit board near the components
Tae	Average Outside Ambient Temperature surrounding the equipment
τon	Total annual ratio of time for the PCB, in permanent working mode with supply.
τoff	Total annual ratio of time for the PCB, in non working or storage/dormant modes.
Ni	Annual number of thermal cycles seen by the components of the PCB, corresponding to the ith phase of the mission profile with an average swing *ΔTi*
ΔTi	Average swing of the thermal variation seen by the components of the PCB, corresponding to the i^{th} phase of the mission profile.
λ	Failure Rate per hour = 1/MTBF

The standard asks to create a **Mission Profile** to model the lifecycles of the components. The mission profile we have used is given below with the following assumptions:

- ✓ 1 cycle per day: 365 per year
- ✓ Temperature 2 : 60°C

PHASES		Number of cycles per year	ΔT(°C)	Tae(°C)	Tac(°C)	τ
Description	**Type**					
Working	Permanent	365	10	60	70	1

4.1.2 Reliability data for other components

The reliability of other components is given hereafter:

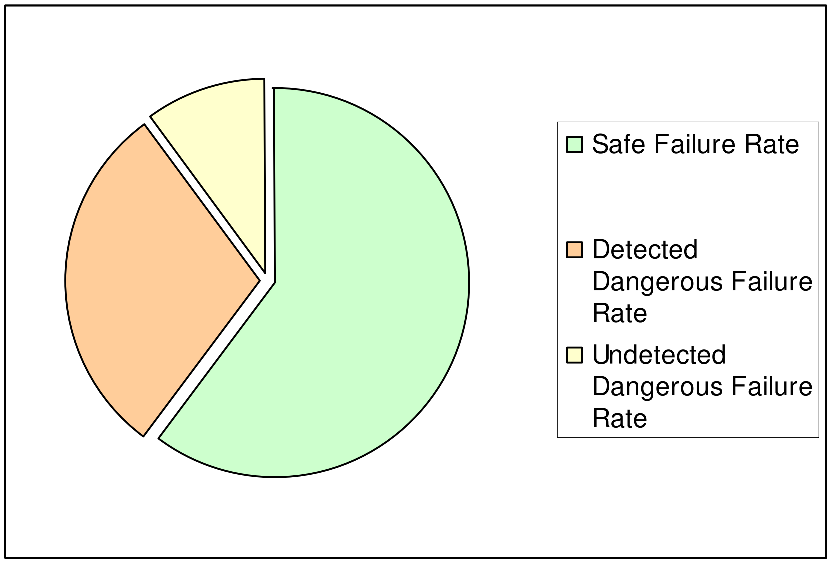
✓ Reliability of the cable:

The reliability of the cable is given in a database “NPRD 1991”:
λ = 1,09 x 10-8 / h

4.2 PFH & SFF Calculations Description

Hypotheses & Formulas:

✓ **Types of Failures:**



✓ **Diagnostic Coverage:**
The diagnostic coverage will be performed by the integrated circuit.
The diagnostic coverage numbers have been given in [6] & [7] by TYCO.

✓ **The formulas are given hereafter:**

PFH (1oo1) = λ_{Du}

SFF = $(\lambda_{DD} + \lambda_S) / \lambda$

4.3 Results of Failure Rates

The following results have been calculated:

- ✓ For TTC1 : λ = 5,96 x 10-7 / h
- ✓ For TT-FFS : λ = 1,76 x 10-7 / h

4.4 Results of the PFH & SFF

The results of PFH & SFF are given below for the 2 configurations:

	Configuration 1	**Configuration 2**
PFH	1,98 x 10-7	2,41 x 10-7
SFF	75 %	87 %
SIL Reachable	**Maximum SIL 2**	**Maximum SIL 2**

5. Conclusion & Limits of the report

5.1 Conclusion

According to the field calculations based on the documents given by TYCO, the following configurations of "Pneumatic Leak Detector" systems have PFH & SFF suitable to use **in safety loops SIL 2**:

⇨ Configuration N°1:
1 component TTC-1 (Detection Module)
1 component FFS (Sensor)
1 cable

⇨ Configuration N°2:
1 component TTC-1 (Detection Module)
6 components FFS (Sensor)
1 cable

5.2 Limits of the Report

The limits of the report are given below:

✓ Only the calculations part has been analysed. Software, process & quality control, documentation & modification management, competencies… have not been analysed.

APPENDIX 1: Calculations Sheets