Functional Safety
www.silmetric.com

FMEA Certificate

A failure modes and effects analysis has been performed by SILMETRIC with reference to IEC 61508-2: 2010 clauses 7.4.4 and 7.4.5 to establish the probabilistic hardware failure data for the following product(s):

HBS5500 and HBS5600 universal temperature transmitters

The function performed in safety applications is to convert the input signal to a corresponding 4-20mA output (as specified on the relevant product datasheet)

Summary of failure data from the FMEA and assessment report

Parameter *	Abbreviation	Value
Dangerous diagnosed failure rate	λ_{DD}	1.3E-06
Dangerous undiagnosed failure rate	λ_{DU}	1.8E-07
Safe failure rate	λ_{S}	6.7E-07
No-effect failure rate	λ_{NE}	1.2E-06
Diagnostic coverage	DC	88%
Safe failure fraction	SFF	92%
Hardware fault tolerance	HFT	0
Type		Type B

* Refer to IEC 61508-4:2010 for definition of parameters and IEC 61508-2:2010 for relevance to SIL

Manufacturer: H&B Sensors Ltd
FMEA: FMEA21008-1, rev 1.1
Report: RPT21021-1, rev 1.0
Certificate: C21021-1, rev 1.0
Date: 20th July 2021

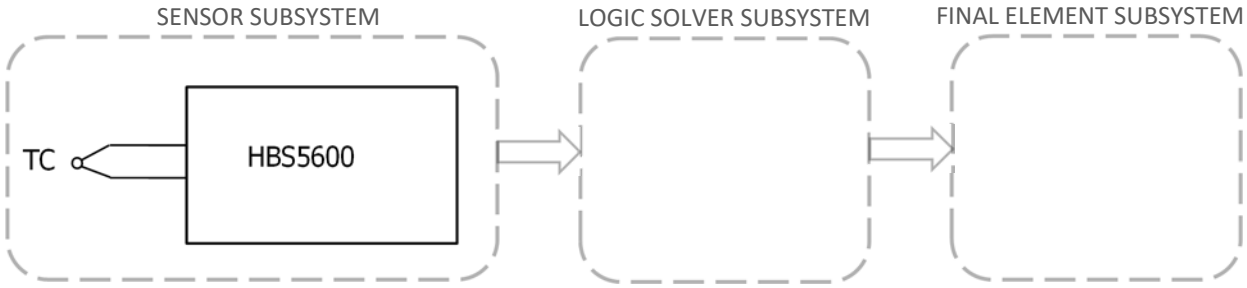
Assessor:

.....
P J Reeve BEng CEng MIET FInstMC

See the following pages for an illustration of how the data can be used in a safety instrumented system, including assumptions in the derivation of the data and conditions of its use.

Illustration of use of the FMEA data in a safety instrumented system

This example uses a single thermocouple connected to a HBS5600 transmitter to form the sensor subsystem in a safety instrumented system (SIS). The safety instrumented function (SIF) is required to trip if the temperature measurement exceeds a pre-set level with a probability of failure on demand (PFD_{AVG}) of less than 0.01 to meet SIL 2. The proportion of the SIL 2 PFD_{AVG} used by the sensor subsystem is required to be less than 35% (leaving 65% available for the other subsystems in the SIS).



PFD_{AVG} for sensor subsystem
35% x 0.01 = 0.0035

For the purposes of illustration only, example TC failure data is shown, together with the FMEA failure data for the HBS5600 from page 1. (Note that failure data quantities are summed to get the corresponding parameter value for the sensor subsystem).

Parameter	TC	HBS5600	Sensor subsystem	Comments
λ_{DD}	9.0E-06	1.3E-06	1.0E-05	e.g., TC open circuit fault, diagnosed by HBS5600
λ_{DU}	1.0E-06	1.8E-07	1.2E-06	e.g., TC short circuit and drift faults, undiagnosed
λ_S	0.0E+00	6.7E-07	6.7E-07	All λ_S classified faults produce the fault condition
DC	90%	88%	90%	
SFF	90%	92%	90%	Reference to IEC 61508-2 table 3 for type B subsystems indicates these parameters impose architectural constraints which limit the SIF to SIL 2
HFT	0	0	0	
Type	A	B	B	

Note that all λ_{DD} and λ_S failures produce a fault indication on the HBS5600 (e.g. <4mA, >20mA) which must be acted upon by the logic solver, e.g., asserting the SIF or by some other appropriate action.

Using typical end user parameters, the PFD_{AVG} for the example sensor subsystem can be calculated:

Parameter	Value	Comments
Proof test interval (T)	8,760 h	Typical value, chosen for illustration
Mean time to repair (MTTR)	24 h	As above
Mean repair time (MRT)	24 h	As above
PFD_{AVG} sensor subsystem	8.2E-04	Using the equation for 1oo1 in IEC 61508-6, B.3.2.2.2: $PFD_{AVG}=(\lambda_{DU}+\lambda_{DD})t_{CE}$ Where $t_{CE}=(\lambda_{DU}/\lambda_D)(T/2+MRT)+(\lambda_{DD}/\lambda_D)MTTR$

The PFD_{AVG} for the sensor subsystem in this example is <0.0035 which supports the probabilistic failure target of <0.01 for a SIF required to meet SIL 2. Using the failure data in redundant architectures (e.g., 1oo2, 2oo3, etc) can support higher SILs, as described in IEC 61508-6.

Identification of design(s) analysed

The product(s) listed on page 1 are based on the following electronic circuits; note that the same circuit diagrams apply to both products; changes to these circuits will invalidate the FMEA data:

- S5304_01_02 Main PCB Circuit (Certification)
- S5308_01_01 Display PCB Circuit (Certification)

FMEA assumptions and conditions of data validity

The following specific assumptions have been used in the FMEA, on which validity of the data relies:

1) Configurable settings (and any changes to them) made via the USB or HART interface shall be independently verified (e.g., by manual checks during installation/commissioning)
2) The USB interface shall not be used when the safety instrumented system is operational
3) The HART protocol shall not be used when the safety instrumented system is operational
4) Diagnosed sensor or transmitter failures (λ_{DD}) are indicated by the fault condition (under or over-range) which will require an appropriate system response with regard to the safety function
5) The user shall comply with all recommendations and conditions in the product User Guide(s)
6) Failure data is for 'ground benign' conditions and an operational temperature range of -40 to +85°C

General assumptions used in the FMEA model:

1) Failure rates in the FMEA tables are per hour
2) Failure rates used are constant over the lifetime of the item (sometimes termed 'useful life')
3) FMEA only models random hardware failures; systematic failures need to be addressed through design and development (e.g., software, design calculations, performance testing, verification, validation, documentation, etc.) and by the user adhering to the manufacturer's instructions (e.g., conditions or restrictions in use, environmental limits, materials compatibility, etc.)
4) Where a probability of failure on demand (PFD_{AVG}) is stated, this is dependent on user proof test intervals and mean repair times which are given for illustration; if different intervals are used the PFD_{AVG} must be re-calculated
5) Where safe or dangerous diagnosed failure modes are indicated, this assumes the system designer shall ensure the logic solver performs the appropriate response (e.g., by ensuring the safe state of the EUC or by undertaking repairs within the MRT)
6) Any components that are not involved in performing the safety function and do not fit the definition of safe or dangerous failures (defined as 'no effect' failures) are not included in the safe failure fraction calculation. Refer to IEC 61508-4:2010 for definitions of these failure types
7) Failure rates are generally taken from the component supplier data sheets where available, the Siemens SN 29500 or the Technis FARADIP.THREE databases (as indicated in the FMEA tool) taking into account the specified environmental specifications of the unit
8) IEC 62061 is used as a guide for judging the component failure mode distributions unless otherwise indicated by the failure database
9) Each component failure mode is analysed on its own; the probability of multiple failure propagation is not considered, unless the analysis indicates that one failure mode will directly lead to another in which case these are considered together as a single failure mode