# FMEDA – Report
# Failure Modes, Effects and Diagnostic Analysis

Device Model Number:

**LB/FB7x04, LB/FB4x06, LB/FB4x02x2, LB/FB4x05x2**

Project:

**Remote I/O LB/FB**

**Pepperl+Fuchs GmbH**

**Mannheim**

**Germany**

Reviewers:

| Role |
|---|
| Project Leader (PL) |
| Product Management |
| Functional Safety Manager |

History of this document:

| Revision of this document | Changes since last version |
|---|---|
| Index 0<br>dated 2008-Apr-08 | Newly created |
| Index A<br>dated 2018-Mar-26 | Adapted to new format, corrected values |

# 1 Report Summary

This report summarizes the results of the FMEDA hardware assessment according to IEC 61508 carried out on the Remote I/O LB/FB System of backplanes equipped with devices LB4x02x2, LB4x05x2, FB4x02x2, FB4x05x2, LB4x06, FB4x06, LB7x04, FB7x04. The hardware of the different versions is considered to be sufficiently similar.

Failure rates used in this analysis are basic failure rates from the Siemens Standard SN29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in Low demand mode has to be < $10^{-2}$ for SIL2 safety functions. For Systems operating in High demand or continuous mode of operation the PFH value has to be <$10^{-6}\ h^{-1}$. However, as the modules under consideration are only part of an entire safety function they should not claim more than 10% of this range, i.e. they should be lower than $10^{-3}$ for SIL2 in Low Demand Mode respectively lower than $10^{-7}\ h^{-1}$ for SIL2 in High Demand Mode.

The Remote I/O LB/FB systems are considered to be Type A components with a hardware fault tolerance of “0”.

Since the device circuit has a hardware fault tolerance of “0” and they are considered to be Type A devices, the SFF must be >60% according to table 2 of IEC 61508-2.

# 2 Functional description of the remote I/O LB / FB devices.

The devices are used in conjunction with a backplane that is integral part in the safety function. The remote I/O devices act as interface between signals from the hazardous area (Ex area) and the safe area (non-Ex area).
The backplane also takes care of the distribution of power, the power supplies used may offer a maximum voltage of 32 V DC.

The safety function that can be implemented with the devices is influencing outputs of a device group on the backplane. On the backplanes, an emergency stop may be attached at a terminal (see connector X3 in example fig. 1). When pushed, the power supply for the safety circuit is cut off, switching off the outputs of all devices installed on the output group.

All device outputs are galvanically isolated from the inputs. The outputs are not polarized and share a common reference potential of the supply. The supplies of emergency stop and outputs may be based on different potentials, as the signals are galvanically isolated from each other.

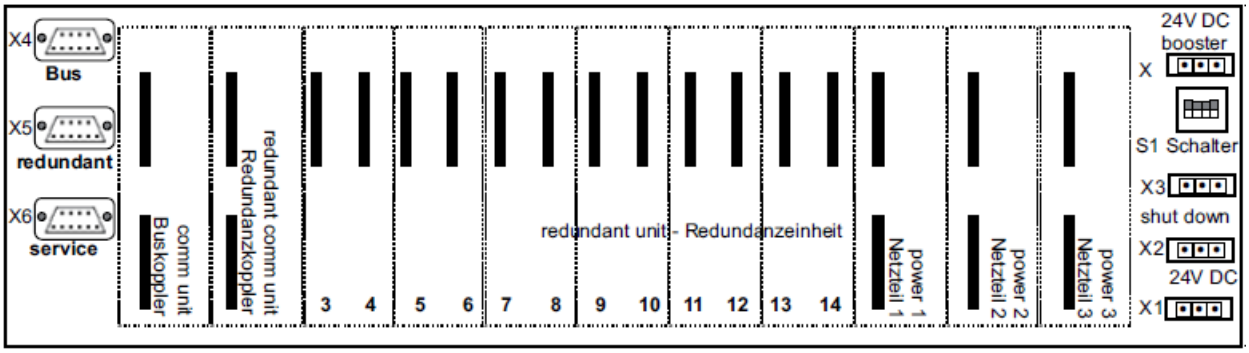


Fig. 1: Typical backplane including connectors

# 3 Definition of the failure categories

The FMEDA was done and is documented in the Pepperl+Fuchs EDM.

In order to judge the failure behaviour of the Remote I/O devices, the following definitions for the failure of the product were considered:

**Fail-safe state:**
The respective output is switched to de-energized state.

**Safe failure:**
Causes the system to go to the fail-safe state without a demand from the emergency stop.

**Dangerous failure:**
When the respective output does not respond to a demand from the emergency stop circuit (not able to switch off the device output).

**“No effect” failure:**
Failure of a component that is part of the safety function but has no effect on it.

**“Not part” failure:**
Means that this component is not part of the safety function, but part of the circuit diagram and is listed for completeness. For this evaluation, only components that are part of the safety circuit were treated.

# 4 Assumptions

The following assumptions were made for the FMEDA of the Remote I/O LB/FB system devices.

- Failure rates based on the Siemens standard SN29500.
- Failure rates are constant, wear out mechanisms are not included.
- All modules are operated in the Low demand mode or High demand mode of operation.
- The device shall claim less than 10 % of the total failure budget for a SIL2 safety loop.
- For a SIL2 application operating in Low Demand Mode the total $PFD_{avg}$ value of the SIF (Safety Instrumented Function) should be smaller than $10^{-2}$, hence the maximum allowable $PFD_{avg}$ value would then be $10^{-3}$.
- For a SIL2 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than $10^{-6}$ per hour, hence the maximum allowable PFH value would then be $10^{-7}$ per hour.
- Since the circuit has a Hardware Fault Tolerance of zero and is considered to be a type A component, the SFF must be > 60 % according to table 2 of IEC 61508-2 for SIL2 (sub)system.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 ºC. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 ºC, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- The appearance of a safe error (e. g. output in safe state) is repaired within 8 hours (e. g. remove sensor burnout).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (for example: substitution by an equivalent device).
- Different channels of one device can fail based on one common failure. Do not use multiple channels of one device for one safety function.
- On some backplanes, switches are included that allow easy bridging of the emergency stop. To prevent from manipulation, covers are available from Pepperl+Fuchs that prevent easy access to these switches. These covers must be used as described in the safety manual.
- For further limitations to the use of these devices refer to the instructions in the manual and the limitations in the data sheets.

# 5 Results of the Assessment

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 7.1.18 by exida.com.

**Table 1:**
**LB/FB7x04, LB/FB4x06, LB/FB4x02x2, LB/FB4x05x2 used in a 1oo1 structure**

| Parameters acc. to IEC61508 | Variables |
|---|---|
| Device type | A |
| Demand mode | Low Demand Mode or High Demand Mode |
| Safety Function | DTS (de-energize-to-safe) |
| HFT | 0 |
| SIL | 2 |
| $\lambda_s$ [1] | 15.7 FIT |
| $\lambda_{dd}$ | 0 FIT |
| $\lambda_{du}$ | 9.4 FIT |
| $\lambda_{total\ (Safety\ function)}$ | 25.1 FIT |
| $\lambda_{no\ effect}$ | 8.1 FIT |
| $\lambda_{not\ part}$ | 0 FIT |
| SFF[1] | 62 % |
| PTC | 100 % |
| MTBF[2] | 3437 years |
| PFH | $9.42 * 10^{-9}$ 1/h |
| $PFD_{avg}$ for $T_1$ = 1 year | $4.13 * 10^{-5}$ |
| $PFD_{avg}$ for $T_1$ = 2 years | $8.25 * 10^{-5}$ |
| $PFD_{avg}$ for $T_1$ = 5 years | $2.06 * 10^{-4}$ |
| Safety Response Time[3] | 100 ms |

[1] "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the safety values / SFF.
[2] acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.
[3] Time from failure detection to failure reaction.

# 6 Possibilities to Reveal Dangerous Undetected Faults During the Proof Test

The Proof test shall reveal the dangerous undetected (du) faults, which have been noticed during the FMEDA.

Dangerous failures are limited to incorrect reaction on pushing the emergency stop. There are no dangerous failures if the reaction on the emergency stop is coming within the expected time. To test this, the maximum load within the application must be switched off and the timing must be observed. By this, all dangerous undetected failures are revealed.

Assuming 10% of the failure budget of a safety loop to be available for the Remote I/O device results in a proof test interval of 24 years. It is possible that the device is used in other environments than specified within the assumptions for the FMEDA assessment so a different calculation is necessary. The calculations for the safety loop can also reveal that the device may claim a different amount of the PFD value (standard is 10%). Both effects have an influence on the proof test time.

It is the responsibility of the operator to select a suitable proof test time.

# 7 Useful life time

Although a constant failure rate is assumed by the probabilistic estimation this only applies, if the useful lifetime of components is not exceeded. Beyond this useful lifetime, the result of the probabilistic calculation is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, the electrolytic capacitors can be very sensitive to the working temperature).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore, it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

However, according to IEC 61508-2, a useful lifetime, based on experience, should be assumed. Experience has shown that the useful lifetime often lies within a range period of about 8 ... 12 years.

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and operator can extend the useful lifetime. Our experience shows that the useful life time of a Pepperl+Fuchs product can be higher if the ambient conditions support a long life time, for example if the ambient temperature is significantly below 60 °C.

Please note that the useful lifetime refers to the (constant) failure rate of the device. The effective lifetime can be higher.

# 8 Abbreviations

| | |
|---|---|
| FMEDA | Failure Modes, Effects and Diagnostic Analysis |
| PFD | Probability of dangerous failure on demand |
| PFH | Probability of dangerous failure per hour |
| SFF | Safe Failure Fraction |
| HFT | Hardware Fault Tolerance |
| SIL | Safety Integrity Level |
| MTBF | Mean Time Between Failure |
| $T_{proof}$ | Proof time |
| AVG | Average |

# 9 Literature

**Manufacturing Documents**

FS-0007PF-26A V5 dated 2017-Dec-19, FMEDA excel sheet for the LB/FB4x0x/7x04
01-8712B from 2011-Jul-26, circuit diagram for the LB/FB shunt voltage regulator
01-8704E from 2015-Mar-18, circuit diagram for the LB/FB7x04 power supply

**Standards**

IEC 61508-2:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Requirements
SN 29500 parts 1 – 13, Failure rates of components
FMD-91, RAC 1991 Failure Mode / Mechanism Distributions
FMD-97, RAC 1997 Failure Mode / Mechanism Distributions