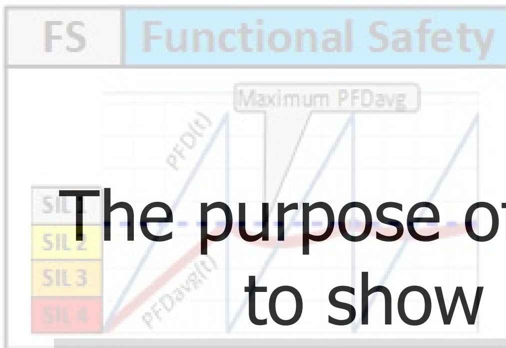


The purpose of this SAMPLE document is to show in the public domain LIUTAIO's criteria for "Reliability data validation" that are being used by:

LIUTAIO "FUNCTIONAL SAFETY SERVICES"

For calculating "Reliability indexes values", like: SFF, PDFavg, PFHavg, STR, MTTF, MTTFspuriously, MTTFdangerously, etc.

Copyright © 2018 LIUTAIO Consulting and Engineering Services

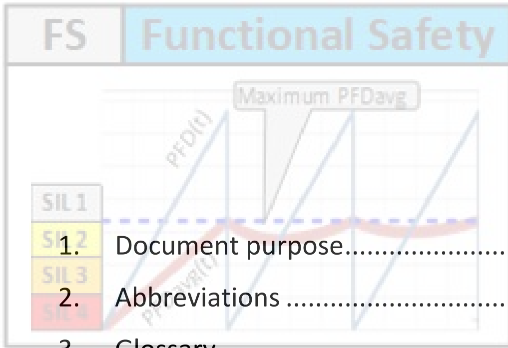
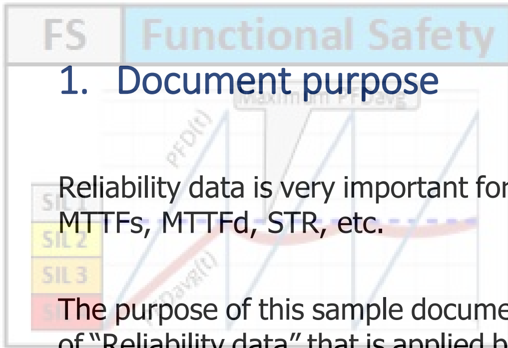


Table of Contents

1. Document purpose 3
2. Abbreviations 3
3. Glossary 3
4. References 3
5. Introduction 4
6. Reliability data outline 5
   6.1 Attributes for Failure classification 5
   6.2 IEC-61508 Failure Model (Reliability data for “SIL verification”) 5
7. Reliability Data Validation (RDV) 8
   7.1 Are “Diagnostics” used in SIF design? 8
   7.2 Are “Diagnostics” used to reduce “Spurious Trip Rate” (STR)? 9

LIUTAIO Functional Safety Services www.LiutaioCES.com 0418H03SD15 Rev.01 Reliability Data Validation - SAMPLE DOCUMENT -

Copyright © 2018 LIUTAIO Consulting and Engineering Services



1. Document purpose

Reliability data is very important for calculating reliability indexes like: SIL rating, PFDavg, PFHavg, MTTFs, MTTFd, STR, etc.

The purpose of this sample document is to show in the public domain an outline about "Validation" of "Reliability data" that is applied by LIUTAIO "Functional Safety Services" before executing above listed calculations.

For preparing this SAMPLE document LIUTAIO experience was used.

2. Abbreviations

Refer to sample document: 0418D10SD01 Abbreviations

3. Glossary

Refer to sample document: 0418D10SD02 Glossary

4. References

[1] IEC-61508:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems

[2] LIUTAIO – Functional Safety Services
0418D10SD01 Abbreviations - Sample Document
Rev.01

[3] LIUTAIO – Functional Safety Services
0418D10SD02 Glossary - Sample Document
Rev.01

[4] LIUTAIO – Functional Safety Services
0418G25SD11 Rev.01 FMEDA Background - Sample Document
Rev.01

LIUTAIO Functional Safety Services www.LiutaioCES.com 0418H03SD15 Rev.01 Reliability Data Validation - SAMPLE DOCUMENT -

Copyright © 2018 LIUTAIO Consulting and Engineering Services

5. Introduction

Reliability data is very important for calculating reliability indexes like:

- "Safe Failure Faction" (SFF),
- "Average Probability of Failure on Demand" (PFDavg),
- "Average Dangerous Frequency of Failure" (PFHavg),
- "Spurious Trip Rate" (STR),
- "Mean Time to Failure Spuriously" (MTTFs),
- "Mean Time to Failure Dangerously" (MTTFd), etc.

SFF, PFDavg and PFHavg are used to verify if a safety device or "Safety Instrumented Function" (SIF) satisfies or **NOT** a required SIL rating.

BUT, sometimes:

a) A SIF implementation **IS NOT** representative of ALL devices' features, despite of a certificate that indicates installation satisfies required SIL rating, or

b) Traditional black box calculation tools can lead engineering to focus on manipulating software to accept results without question, instead of analyzing data and result according to requirements (SRS) and the way the SIF's devise are implemented.

For example: a device includes "Diagnostics" to reveal detected failures, and this device is selected to be included in a SIF.

The device implementation **DOES NOT** communicate Safety/Control system when a detected failure occurs, even though its "Fault detection capabilities" (Diagnostics) are working properly.

In this case:

- The Operator never knows what is happening, BUT it could be warned (notified).
- "Diagnostics" are a very important to allow a safety device to get SIL rated classification. BUT, implementation **DID NOT** consider the use of "Diagnostics" and therefore SIL requirement of SIF implementation **IS NOT** satisfied.

This document describes how "Reliability Data Validation" (RDV) shall be applied to properly calculate the reliability indexes, to verify if a device and/or SIF satisfies the required SIL rating.

For RDV examples refer to "Examples" No.1 and No.2 in:
http://www.LiutaioCES.com/SampleFunctionalSafety/Index.htm

LIUTAIO Functional Safety www.LiutaioCES.com 0418H03SD15 Rev.01 Reliability Data Validation - SAMPLE DOCUMENT -

6. Reliability data outline

6.1 Attributes for Failure classification

Fail Safe — Failure that causes a "Target System" to move from the NORMAL to the SAFE state. Typically identified as a "Spurious Trip".

Fail Dangerous — Failure that prevents a "Target System" to fail on demand. In other words, when a HAZARD occurs, the "Target System" **CANNOT** perform its automatic protection function and it will remain in the NORMAL state.

Fail Detected — Failure in a "Target System" that can be "Detected" by an automatic diagnostic test, and this test implementation is capable to notify both a Safety/Control system and Operator. An automatic diagnostic test execution frequency **MUST BE** higher than a "Proof Test" execution frequency.

Fail UnDetected — Failure that **CANNOT** be "Detected" in a "Target System" by an automatic diagnostic test. Notification capability **DOES NOT** exist.

No Effect — Failure that has "NO Effect" in a "Target System" automatic protection function. In other words, failure that **DOES NOT** prevent a "Target System" to perform its automatic protection function and **DOES NOT** initiate "Spurious Trip".

Annunciation — Failure that has "NO Effect" in a "Target System" capability to perform its automatic protection function, BUT the "Target System" automatic diagnostic test stop to work.

In other words, this failure **HAS NO** impact in safety, **BUT** "Fault Detection Capabilities" (Diagnostics) **WILL NOT** work.

6.2 IEC-61508 Failure Model (Reliability data for "SIL verification")

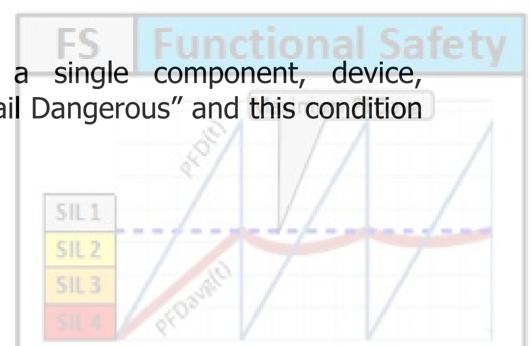
By applying the listed "Attributes for Failure classification" in above section, Figure 1 shows the IEC-61508 failure mode diagram and the diagram elements description is as follows:

Total Failure rate (TFR) — Average frequency of failure, or chance of a single component, device, arrangement or system, to fail within a period of time.

Safe Detected (**SD**) Failure rate — Portion of the TFR where a single component, device, arrangement or system will "Fail Safe" and this condition is "Fail Detected".

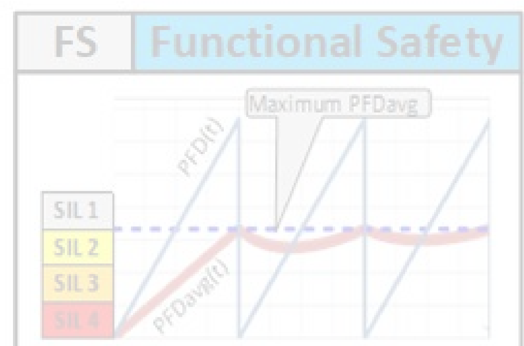
Safe UnDetected (**SU**) Failure rate — Portion of the TFR where a single component, device, arrangement or system will "Fail Safe", **BUT** this condition **IS NOT** "Fail Detected".

Dangerous Detected (**DD**) Failure rate — Portion of the TFR where a single component, device, arrangement or system will "Fail Dangerous" and this condition is "Fail Detected".



Dangerous UnDetected (**DU**) Failure rate	Portion of the TFR where a single component, device, arrangement or system will "Fail Dangerous", **BUT** this condition **IS NOT** "Fail Detected". DU failures can be detected by operator intervention, or FULLY by "Proof Test" if this one can reveal ALL DU failures.
Residual Failure rate	Portion of the TFR that **CANNOT** be classified as SD, SU, DD or DU. "Annunciation" and "No Effect" failures are included in "Residual Failures".
Dangerous UnDetected (**DU-P**) Failure rate, where failures are revealed by "Proof Test"	When "Proof Test" **CANNOT** reveal all DU failures, this is the portion of the DU failures where a single component, device, arrangement or system will "Fail Dangerous", **BUT**: • This condition **IS NOT** "Fail Detected", and • Can be revealed by "Proof Test".
Dangerous UnDetected (**DU-M**) Failure rate, where failures are revealed by Maintenance ONLY.	When "Proof Test" **CANNOT** reveal all DU failures, this is the portion of the DU failures where a single component, device, arrangement or system will "Fail Dangerous", **BUT**: • This condition **IS NOT** "Fail Detected", and • ONLY Maintenance can be reveal the failure.
Proof Test Effectiveness (Et), Or Proof Test Coverage (PTC) **Et = PTC = (DU-P / DU)**	Portion (0-100%) of the DU failure rate revealed by "Proof Test". Applicable when "Proof Test" **IS NOT** capable to reveal all DU failures.

LIUTAIO Functional Safety Services www.LiutaioCES.com 0418H03SD15 Rev.01 Reliability Data Validation - SAMPLE DOCUMENT -



Copyright © 2018 LIUTAIO Consulting and Engineering Services

Figure 1 – IEC-61508 Failure Model diagram

λ
(TFR) **Total** Failure rate

λ_T
Failure Rate for Reliability Indexes calculation

NO Effect Failure rate

Annunciation Failure rate

Residual Failure rate

λ_S
Safe Failure rate

λ_D
Dangerous Failure rate

λ_{SD}
(LdSD)
Safe **D**etected Failure rate

λ_{SU}
(LdSU)
Safe **U**nDetected Failure rate

λ_{DD}
(LdDD)
Dangerous **D**etected Failure rate

λ_{DU}
(LdDU)
Dangerous **U**nDetected Failure rate

Revealed by "Diagnostics"

λ_{DU-P}
Dangerous **U**nDetected Failure rate revealed by "Proof Test"

λ_{DU-M}
Dangerous **U**nDetected Failure rate revealed by Maintenance

LIUTAIO Functional Safety Services
www.LiutaioCES.com
0418H03SD15 Rev.01
Reliability Data Validation
- SAMPLE DOCUMENT -

7. Reliability Data Validation (RDV)

7.1 Are "Diagnostics" used in SIF design?

The IEC-61508 failure rate model (see Figure 1) states that if a SIF Device includes "Fault Detection Capabilities" (Diagnostics), then the Safe and Dangerous failure rates have a portion for failures that can be detected by Diagnostics, and the other portion not. This distribution has positive credit in the "SIL verification" process in favor to make the SIF implementation to easier satisfy the "Safety integrity targets, constraints and other requirements".

Nevertheless, even though if a related SIF Device includes "Diagnostics", BUT such "Diagnostics" **ARE NOT** used, or **NOT** considered, in the SIF implementation/installation, then **NO CREDIT** on "Diagnostics" shall be taken in the "SIL verification" process.

For example, Table 1 shows the "Failure Rate" data for a SIF Device. It is indicated that the SIF Device includes "Fault Detection Capabilities" (Diagnostics).

BUT, if the SIF implementation/Installation **DOES NOT** use, or **DOES NOT** take advantages of, the Device Diagnostics, then these Diagnostics have **NO CREDIT** in the "SIL verification" process. In this case, data in Table 2 shall be used for "SIL verification", instead of data in Table 1.

Table 2 is the RDV result which indicates that even though the device is **capable** to use "Diagnostics", the benefits from such "Diagnostics" **DO NOT perform** in the SIF/IPF implementation/installation.

Table 1 - Example of "Failure Rate" information of a SIF Device

	Safe	Dangerous	
Detected	λ_{SD}, or LdSD = 75.0 FIT	λ_{DD}, or LdDD = 170.0 FIT	**Type B** device SFF = 95.2% Max CLAIM SIL 2
UnDetected	λ_{SU}, or LdSU = 150.0 FIT	λ_{SU}, or LdDU = 20.0 FIT	

*Table 2 – Adjusted data from Table 1 for "SIL verification", when SIF implementation/Installation **DOES NOT** use, or **DOES NOT** take advantages, of the SIF Device Diagnostics*

	Safe	Dangerous	
Detected	λ_{SD}, or LdSD = 0.0 FIT	λ_{DD}, or LdDD = 0.0 FIT	**Type B** device SFF = 54.2% Max CLAIM SIL 0
UnDetected	λ_{SU}, or LdSU = 150.0 + 75.0 **= 225.0 FIT**	λ_{SU}, or LdSU = 20.0 + 170.0 **= 190.0 FIT**	

Since the maximum SIL rating that a device can CLAIM is determined by SFF (See IEC-61508-4:2010, section 3.6.15), after adjustment in Table 2 the referred SIF device **DOES NOT** satisfy the required SIL rating.

From above paragraph, change in a SIF device SFF will affect SIF's SIL rating, because the maximum SIL rating a SIF can CLAIM is determined by "Route 1H (or 2H)" (See IEC-61508-2:2010 section 7.4.4).

Copyright © 2018 LIUTAIO Consulting and Engineering Services

7.2 Are "Diagnostics" used to reduce "Spurious Trip Rate" (STR)?

Strictly speaking, the "Spurious TRIP Rate" (STR) calculation for a SIF depends ONLY on:

a) ALL SIF "Decision Logics" where the SIF Device is used (use MTTR in calculation), and
b) The SIF Devices' "Safe Detected" (SD) and "Safe UnDetected" (SU) failure rate values.

Nevertheless, if "Fault Detection Capabilities" (Diagnostics) are used in the SIF implementation, then one(1)or both of the following considerations may apply:

NOTE: any of the below considerations **SHALL NOT** affect each device maximum SIL rating that can be CLAIMED by SFF. In fact, ONLY the use of "Diagnostics" makes the below "considerations" to have sense.

>> CONSIDERATION 1:

By default, when a "Safe Detected" (SD) failure occurs in a SIF device, Operator is notified, and then this device condition shall change to initiate a SIF "Spurious TRIP" as well.

If the SIF Device "Fault Detection Capabilities" (Diagnostics) are used to detect SD failures in a Device located in the "Input Channel", then SIF implementation can STOP the "Spurious TRIP" and still warn the Operator. Technically, NO "Spurious TRIP" occurred. This action decreases the SIF STR, making it more reliable.

Consequence of application: SIF Device "Safe Detected" (SD) failure rate (λ_{SD}, or LdSD) **IS NOT** used on "Spurious TRIP Rate" (STR) calculation, BUT it is included in the SIL rating calculation, then reliability data from Table 1 shall be adjusted as shown in Table 3 for "SIL verification" calculation.

"Consideration 1":

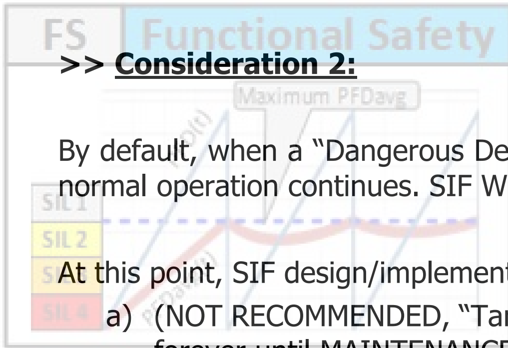
- Device **performs** to avoid "Spurious Trips" from SD failures ("Logic Solver" shall recognize Diagnostic fault result),
- Decreases "Spurious Trip Rate" (STR),
- No effect on device maximum "SIL" rating to claim,
- BUT increases device contribution on SIF "SIL" rating.

Table 3 - Adjusted data from Table 1 for "SIL verification", when SIF implementation/Installation uses "Diagnostics" to identify SD failures in an "Input Channel" device to STOP the "Spurious TRIP"

	Safe	Dangerous
Detected	λ_{SD}, or LdSD = 0.0 FIT	λ_{DD}, or LdDD = 75.0 + 170.0 **= 145.0 FIT**
UnDetected	λ_{SU}, or LdSU = 150.0 FIT	λ_{SU}, or LdSU = 20.0 FIT

NOTE: By design, MAINTENANCE shall have a chance of MTTR time to repair detected SD failure, else safety shall apply. This means that If the "Consideration 1" applies in the SIF design/implementation, when a SD failure occurs in the referred SIF device, SIF implementation shall STOP "Spurious TRIP", BUT a demand shall be initiated to set the SIF FSE in the SAFE state after MTTR time.

LIUTAIO Functional Safety www.LiutaioCES.com 0418H03SD15 Rev.01 Reliability Data Validation SAMPLE DOCUMENT



>> Consideration 2:

By default, when a "Dangerous Detected" (DD) failure occurs, then Operator is notified, and the normal operation continues. SIF WILL fail on demand. **NO** "Spurious TRIP" occurs.

At this point, SIF design/implementation has the following choices:

a) (NOT RECOMMENDED, "Target System" is unprotected) Operator is notified and SIF waits forever until MAINTENANCE is applied to repair SIF device in failure.

b) To allow operation to continue for MTTR time, and Operator is notified. When MTTR expires, SIF implementation shall initiate a demand to set the SIF FSE in the SAFE state. Technically, **NO** "Spurious TRIP" occurred.

c) SIF implementation shall initiate a demand at once the DD failure is detected, and Operator is notified. Technically, a "Spurious TRIP" occurred.

ONLY in the above point "c", the SIF implementation behavior is the same default one as when a SD failure occurs (see above "Consideration 1").

Consequence of application of above Choice 'c': Let's assume the referred SIF device "Reliability data" is shown in Table 1. SIF Device "Dangerous Detected" (DD) failure rate (λ_{DD}, or LdDD) is IN FACT used on "Spurious TRIP Rate" (STR) calculation, but **NOT** in "SIL verification". As consequence of this consideration, reliability data from Table 1 shall be adjusted as shown in Table 4.

"Consideration 2":

- No effect on device maximum "SIL" rating to claim,
- Device **performance** increases "Spurious Trips" (now DD failures can initiate a "Spurious Trip"),
- BUT decreases device contribution on SIF "SIL" rating.

Table 4 – Adjusted data from Table 1 for "SIL verification", when SIF implementation/Installation uses "Diagnostics" to identify DD failures in a SIF device, and when DD failure occurs a "Spurious Trip" is initiated at once

	Safe	**Dangerous**
Detected	λ_{SD}, or LdSD = 75.0 + 170.0 **= 145.0 FIT**	λ_{DD}, or LdDD = 0.0 FIT
UnDetected	λ_{SU}, or LdSU = 150.0 FIT	λ_{SU}, or LdSU = 20.0 FIT

For examples of application of above "Considerations 1 & 2", refer to "Example" No.2 in:
http://www.LiutaioCES.com/SampleFunctionalSafety/Index.htm

Copyright © 2018 LIUTAIO Consulting and Engineering Services