FMEDA REPORT

Failure Modes, Effects and Diagnostic Analysis

Project:
Tecofi Knife Gate Valve

Company:
TECOFI SAS
83 RUE MARCEL MERIEUX 69969, CORBAS CEDEX, FRANCE

Manufacturer:
TECOFI SAS
83 RUE MARCEL MERIEUX 69969, CORBAS CEDEX, FRANCE

Farex (Shanghai) Fluid Control Equipment Co., Ltd.
No.248, Xintuan Rd., Qingpu Industry Zone, Shanghai, P.R.C.

Report No.: MY21-1202-R0
Version V0, Revision R0, June 20, 2022

Catalog

1 Purpose and Scope

This report summarizes the results of a PFD evaluation of the:

- Tecofi Knife Gate Valve

  VG Series, VGS Series, VGH Series, VGP Series

A PFD evaluation was performed, according to IEC 61508-2 and IEC 61511-1, to evaluate the λ values and, consequently, the SFF and the PFDAVG values of the Tecofi Knife Gate Valve.

The PFD evaluation according to IEC 61508-2 is one of the steps to be taken to achieve functional safety certification according to IEC 61508 of a device. Failure rates and Safe Failure Fraction are determined. For full functional safety certification purposes all the requirements of IEC 61508 (Part 1-7), including the Functional Safety Management System and the Safety Life Cycle (with reference to parts 6 and 7 of IEC 61508-1, with application to the product subject of the Certification) must be considered.

The device subject of this assessment report is Tecofi Knife Gate Valve, designed to be used in a Safety Instrumented System for use in low demand application.

Table 1 lists the versions of the Tecofi Knife Gate Valve that have been considered for the hardware assessment.

Table 1 Version overview

Type	DN	Connection	Working Pressure
VG Series	DN50 – DN1200	EN 1092-1 EN 1092-2 ASME B16.5 ASME B16.47	2~10 Bar
VGS Series	DN100 – DN800	EN 1092-1 EN 1092-2 ASME B16.5 ASME B16.47	1~3 Bar
VGP Series	DN50 – DN1200	EN 1092-1 EN 1092-2 ASME B16.5 ASME B16.47	2~10 Bar
VGH Series	DN50 - DN1200	EN 1092-1 ASME B16.5 ASME B16.47	10~25 Bar

The Tecofi Knife Gate Valve is classified as a Type A device according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the criteria for Route 2H. Therefore, the Tecofi Knife Gate Valve can be classified as a 2H device when the listed failure rates are used. When 2H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 3 at HFT = 0 per Route 2H. If Route 2H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1H.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 5.2.2.

A user of the Tecofi Knife Gate Valve can utilize these failure rates in a probabilistic model of a Safety Instrumented Function (SIF) to determine suitability in part for Safety Instrumented System (SIS) usage in a particular Safety Integrity Level (SIL).

Failure rates for the devices are listed in Table 5.

2 Purpose and scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Tecofi Knife Gate Valve. From this, failure rates and example PFD_{avg} values may be calculated.

The information in this report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PFD_{avg}) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

A FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

3 References

3.1 Standards / literature used (Table 2)

[N1]	IEC 61508:2010 (all parts)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook	Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	SN 29500	Failure rates of components
[N4]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629
[N5]	Safety Equipment Reliability Handbook	Safety Equipment Reliability Handbook
[N6]	IEC 61511 (all parts)	Functional safety – Safety instrumented systems for the process industry sector

3.2 Documentation provided by manufacturer (Table 3)

[D1]	ISO 9001 Certificate	CN037811
[D2]	Technical specifications	Provide on 2022-06-19, V0
[D3]	Assembly drawings	VG4400 VGH5450 VGP4400 VGS4400
[D4]	User manual	Provide on 2022-06-19, V0
[D5]	Work instruction	FSM-QC-WI-006 R1 FSM-QC-WI-010 R1
[D6]	Failure mode analysis	MY21-1202F-R0
[D7]	Final inspection records	Provide on 2022-06-19, V0
[D8]	Material certificates	Provide on 2022-06-19, V0

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed based on the documentation obtained from manufacturer.

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level. This resulted in failures that can be classified according to the following failure categories.

4.1 Failure Categories description

In order to judge the failure behavior of Tecofi Knife Gate Valve, the following definitions for the failure of the devices were considered.

Fail-Safe State — State where the valve performs the safety function to open or close (depending on the application).

Fail Safe — Failure that causes the device to go to the defined fail-safe state without a demand from the process.

Fail Safe Undetected — Failure that is safe and that is not being diagnosed by automatic diagnostics (such as Partial Valve Stroke Testing).

Fail Safe Detected — Failure that is safe and is detected by automatic diagnostics.

Fail Dangerous — Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

Fail Dangerous Undetected — Failure that is dangerous and that is not being diagnosed by automatic diagnostics, such as Partial Valve Stroke Testing.

Fail Dangerous Detected — Failure that is dangerous but is detected by automatic diagnostics, such as Partial Valve Stroke Testing.

Residual — Failure of a component that is part of the safety function but that has no effect on the safety function.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore, they are not used for the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks which was derived using over 100 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match Profile 3

(General Field Equipment) and Profile 6 (Process Wetted Parts) for the Valves process wetted parts, see Appendix B. The profile chosen was judged to be the best fit for the product and application information submitted by the device manufacturer. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air hydraulic fluid quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related wear-out failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. Environmental Profiles listing expected stress levels can be found in Appendix B. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the units of Tecofi Knife Gate Valve.

- Only a single component failure will fail the entire Valve.
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer’s instructions.
- Failures during parameterization are not considered.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- External power supply failure rates are not included.
- Only the described versions are used for safety applications.
- Materials are compatible with process conditions.
- The measurement / application limits (including pressure and temperature ranges) are considered.
- Due to the failures are usually reported during commissioning or beginning stage, the actuator with complaint are considered delivered in the same year of complaint reported.

5 PFD$_{AVG}$ Calculation

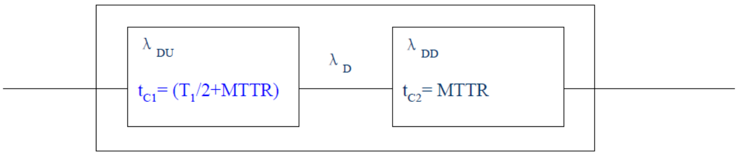
The following section(s) describe how to apply the results of the above data.

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. ISA recommends the accurate *Reliability Block Diagram* tool for this purpose.

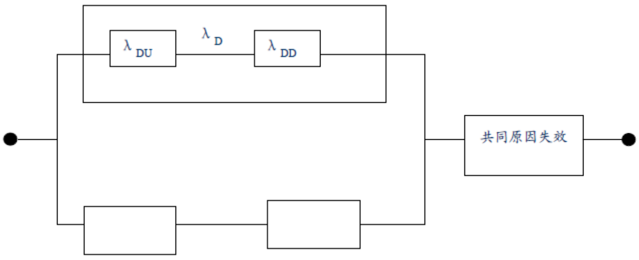
The following results must be considered in combination with PFD$_{AVG}$ values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

5.1 PFDAVG Calculation – Reliability Block Diagram

Reliability Block Diagram is a kind of traditional reliability analysis method. It represents the series-parallel relationship of internal components of the system in a graphical way, and converts the connection relationship of voting mode into series-parallel relationship. It is simple, clear and intuitive. Reliability block diagram is also called reliability network.



$$PFD_{avg} = \lambda_{DU}\left(\frac{TI}{2}+MTTR\right)+\lambda_{DD}MTTR$$



$$PFD_{avg} = 2((1-\beta)\lambda_{DU})^2\left(\frac{TI}{2}+MTTR\right)\left(\frac{TI}{3}+MTTR\right) \quad +\beta\lambda_{DU}\left(\frac{TI}{2}+MTTR\right)$$

The calculation hypothesis:

- Tests intervals: 12 months
- MTTR: 24 h
- SF1: Open or close on demand
- Design life: 15 year
- DC: 90%
- The mode of operation is “Low demand”, which means less than 1 trip demand each year.

5.2 Failure Rate

According to the Sales and After-Sales Data from Manufacturer. And the failure rate is as listed in following table 5.

Table 5 Failure rates

Tecofi Knife Gate Valve	Intermediate results		
	Failure Rate	Undetected dangerous failure rate	Undetected safety failure rate
	1.11E-07	3.34E-09	1.11E-07

5.3 Statistical Approach for Cases with Failure Occurrence

In case one or more failures occurring within the observation period (total operational time or total hours), the steps of the method are the following:

$$\hat{\lambda} = \frac{n}{\tau}$$

Then it was considered the index of confidence of 90% as required by the standard IEC 61508-2 and it is possible to obtain the uncertain range as, in case of occurrence failure:

$$\left(\frac{1}{2\tau}\chi^2(0{,}95, 2n), \frac{1}{2\tau}\chi^2(0{,}05, 2(n+1))\right)$$

Table 6 Confidence interval calculation

Q*h [h]	n. failure dangerous (D)	Confidence %	1/2τ	χ^2 (0,95,2n)	χ^2 (0,05,2(n+1))	λLOW [1/h]	λestimate [1/h]	λUP [1/h]
898259808	3	90%	5.566E-10	1.6354	15.5073	9.10E-10	3.34E-09	8.63E-09
898259808	97	90%	5.566E-10	162.7763	229.6632	9.06E-08	1.11E-07	1.28E-07

Table 7 Final failure rates

Tecofi Knife Gate Valve	Intermediate results		
	Failure Rate	Undetected dangerous failure rate	Undetected safety failure rate
	2.14E-07	8.63E-09	1.28E-07

5.4 SFF

The performing of a regular program of such activities of Full Functional Proof Tests, allows to classify as detected (D) several failure modes that could not be self-detectable.

On the basis of the above-mentioned hypotheses, taking into account the performing of a periodic Full Proof Test, the Safe Failure Fraction results to be **SFF 93.7%**.

5.5 PFD$_{avg}$ calculation

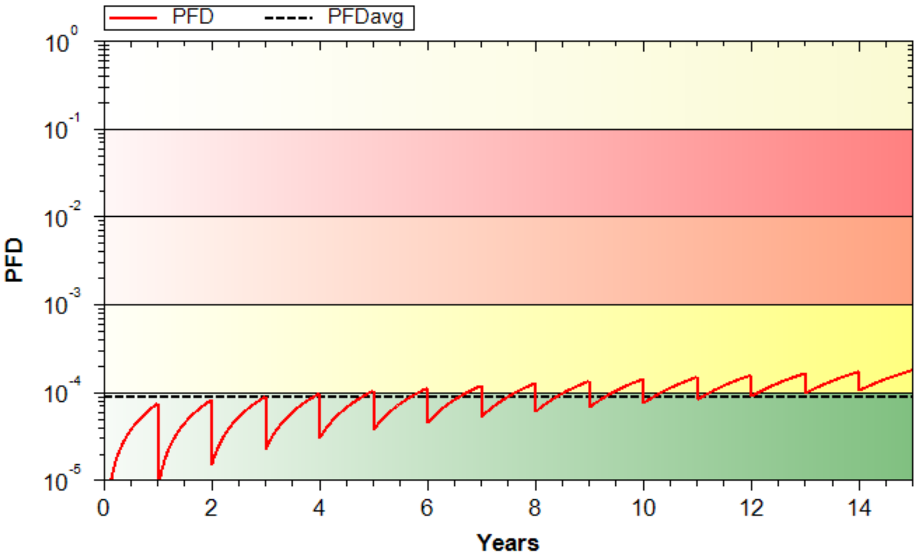
An average Probability of Failure on Demand (PFDAVG) calculation is performed for a single (1oo1) Valve with the analysis tool. The failure rate data used in this calculation is displayed in section 5.4. A mission time of 15 years and a Mean Time To Restoration of 24 hours has been assumed. Table 6 lists the proof test coverage used for the various configurations as well as the results when the proof test interval equals 1 year.

Table 8 Sample PFDAVG Results

Application	Proof Test Coverage	PFDAVG
Tecofi Knife Gate Valve	90%	9.06E-05

The resulting PFDAVG graphs generated from the analysis tool for a proof test interval of 1 year are displayed in Figure1.

Figure 1



5.6 Route 2H Criteria

IEC 61508-2010 describes the Route 2H alternative to Route 1H architectural constraints. The standard states:

"based on data collected in accordance with published standards and, be evaluated according to

• the amount of field feedback; and

• the exercise of expert judgment; and when needed

• the undertake of specific tests,

in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508-2010 does not give detailed criteria for Route 2H, has established the following:

1. field unit operational hours of 100,000,000 per each component; and

2. a device and all of its components have been installed in the field for one year or more; and

3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and

4. failure definitions, especially "random" vs. "systematic" are checked; and

5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.

6 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time (1x10-9 failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval
PVST	Partial Valve Stroke Test - It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Stroke Testing also has an impact on the Safe Failure Fraction.
Proof Test	Periodic test performed manually to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s)
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7. Status of the document

7.1 Liability

SHOCERT prepares reports based on methods advocated in international standards. Failure rates are obtained from client databases or from a collection of industrial databases. SHOCERT accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Revision:	R0	
History:	R0 Initial release	Date: 2022-06-20
Release status:	Released to client	
Authors:	Simon Jiang	

Appendix A Lifetime of Critical Components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime6of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFDAVG 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 the responsibility of the end user to maintain and operate the device per manufacturer’s instructions. Furthermore regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 15 years is expected for the device.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

Appendix B Environmental Profiles

Table 9 Environmental Profiles

Profile	1	2	3	4	5	6
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock	10 g	15 g	15 g	15 g	15 g	N/A
Vibration	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion	G2	G3	G3	G3	G3	Compatible Material
Surge						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	N/A
EMI Susceptibility						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	N/A
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	N/A
ESD (Air)	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

Appendix C Determining Safety Integrity Level

This section provides a detailed overview of the Safety Integrity Level verification performed for Safety Instrumented Function New SIF Tecofi Knife Gate Valve. In order to perform the reliability calculations part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time:	15 years
Startup time:	24 hours
Proof Test Interval:	12 months
Proof Test Coverage:	90 [%]

The SIF operates in Low demand mode.

Table 10 shows the reliability data used during the SIL verification of final element group Valve.

Table 10 Reliability Data Final Element Group Knife Gate Valve

Component	**Failure Rates [1/h]**					**PFD$_{avg}$**	**Arch. Type**
	DD	**DU**	**SD**	**SU**	**Residual**		
MAC 55 series	0	8.63E-09	0	1.28E-07	/	9.06E-05	A

(END)