The purpose of this SAMPLE document is to show in the public domain a typical FMDEA assessment For a "Actuator-Positioner-Valve" (APV) arrangement, developed by:

LIUTAIO

"FUNCTIONAL SAFETY SERVICES"

For preparing this SAMPLE report, examples and public data of actuators, positioner and valves was used in combination with

LIUTAIO experience.

However, when this report is prepared for a CUSTOMER, only the authorized or provided information by CUSTOMER will be used, and the report **WILL NOT BE** part of the public domain.

Table of Contents

FMEDA assessment Management Summary

An Actuator-Positioner-Valve (APV) arrangement shall be used as a final element in a "Safety Instrumented Function" (SIF).

It is required to issue the arrangement "SIL Certificate" to determine if the APV arrangement satisfies SIL-3 rating in fault tolerance 0 or 1 configuration.

The following analysis scenarios were considered in this assessment:

1) "Fail Open" APV arrangement (Open to Trip), with FVST.
2) "Fail Open" APV arrangement (Open to Trip), NO FVST.
3) "Fail Open" APV arrangement (Close to Trip), with FVST.
4) "Fail Open" APV arrangement (Close to Trip), NO FVST.

In ALL Scenarios, and according to IEC-61508-4 2010, section 3.6.15, the APV arrangement SIL rating is limited by "Safe Failure Fraction" (SFF) up to:

- SIL 1 in Scenario No.1, and
- In Scenarios No.2, 3 and 4, the APV arrangement **DOES NOT** satisfy event SIL 1 rating.

"FMEDA assessment" results indicate that ONLY in the above Scenario No1, the APV arrangement is capable to satisfy:

- SIL 1 rating, with installed fault tolerant 0.
- SIL 2 rating, with installed fault tolerant 1.
- SIL 3 rating, with installed fault tolerant 2.

Below table shows an outline of the "FMEDA assessment" results.

	Item Description		Eng.Unit	Scenario 1 Fail Open Close to Trip w/FVST	Scenario 2 Fail Open Close to Trip NO FVST	Scenario 3 Fail Open Open to Trip w/FVST	Scenario 4 Fail Open Open to Trip NO FVST
1	SFF Safe Failure Fraction		%	53.3%	37.5%	20.3%	20.3%
2	Device Type (IEC-61508-4 2010, section 3.6.15)		------	Type A	Type A	Type A	Type A
3	Maximum SIL to CLAIM by SFF. Fault Tolerance 0. (IEC-61508-4 2010, section 3.6.15, and Route 1H)		%	SIL 1	SIL 0	SIL 0	SIL 0
4	PFDavg **(NOTE 1)** Probability of Failure on Demand. (1oo1)	1 year	1 / year	1.26E-03	1.68E-03	2.15E-03	2.15E-03
5		2 years	1 / year	2.52E-03	3.37E-03	4.29E-03	4.29E-03

1. Document purpose

The purpose of this sample document is to show in the public domain a typical "FMDEA assessment" developed by **LIUTAIO** "Functional Safety Services", for an "Actuator-Positioner-Valve" (APV) arrangement, as a requirement from a Customer (in this case, typically a Valve VENDOR/Manufacturer).

For preparing this SAMPLE report, examples and public data of actuators, positioner and valves was used in combination with **LIUTAIO** experience.

However, when this report is prepared for a CUSTOMER, only the authorized or provided information by CUSTOMER will be used, and the report **WILL NOT BE** part of the public domain.

In practice, Valve VENDORs/Manufacturers use to SHARE a document/report like this one in the public domain.

2. Abbreviations

Refer to sample document: 0418D10SD01 Abbreviations

3. Glossary

Refer to sample document: 0418D10SD02 Glossary

4. References

4.1 Professional information and Standards

[P1] LIUTAIO – Functional Safety Services
0418D10SD01 Abbreviations - Sample Document
Rev.01

[P2] LIUTAIO – Functional Safety Services
0418D10SD02 Glossary - Sample Document
Rev.01

[P3] IEC-60812 2006 Procedure for Failure Mode and Effects Analysis (FMEA)

[P4] William M. Goble, and Harry Cheddie.
Safety Instrumented Systems Verification - Practical Probabilistic Calculations
ISA 2005.

[P5] LIUTAIO – Functional Safety Services
0418G25SD11 FMEDA Background - Sample Document
Rev.01

4.2 Documents provided by Customer

Not included in this SAMPLE document.

4.3 Document that were developed and delivered by LIUTAIO

[D1] LIUTAIO – Functional Safety Services
0418G25SD12 FMEDA study report - Sample Document
Rev.01

[D2] LIUTAIO – Functional Safety Services
0418G25SD12 FMEDA assessment - Sample Document (**this document**)
Rev.01

[D3] LIUTAIO – Functional Safety Services
0418G25SD14 Rev.01 APV Arrangement "SIL Certificate" - Sample Document
Rev.01

5. Document LIABILITY

LIUTAIO prepares FMEDA reports based on methodologies supported in International Standards. The used data is provided by Customer or from public and available databases and documental references.

Neither **LIUTAIO**, its employees, subcontractors, nor any person acting in **LIUTAIO** behalf makes any warranty, expressed or implied to any third party, with respect to the use of the information contained in this report or assumes any liability to any third party with respect to any use of the information.

LIUTAIO, its employees, subcontractors, and other assigns **CANNOT** individually, or collectively, predict what will happen in the future. **LIUTAIO** has made every reasonable effort to perform the work contained herein in a manner consistent with high professional standards. However, the quality of the work reported in this document is dependent on the accuracy of information provided by the Customer. The responsibility for use and implementation of the recommendations, designs, and procedures contained in this report rests entirely with the Customer.

6. FMEDA assessment

6.1 FMEDA assessment objective and scope of work

An Actuator-Positioner-Valve (APV) arrangement shall be used as a final element in a "Safety Instrumented Function" (SIF).

It is required to issue the arrangement "SIL Certificate" to determine if the APV arrangement satisfies SIL-3 rating in fault tolerance 0 or 1 configuration.

This document is focused in developing the FMEDA assessment, which includes the "SIL Certificate". "SIL Certificate" shall include for each FMEDA analysis scenario:

- Failure rates (LdSD, LdSU, LdDD & LdDU),
- "Safe Failure Fraction" (SFF),
- "Proof Test Effectiveness" (Et) or "Proof Test Coverage" (PTC), and
- Satisfied "SIL rating" for fault tolerance 0 or 1 configuration.
- PFDavg value for "Proof Test Period" of 1 and 2 years (1oo1).

6.2 LIUTAIO – Consulting and Engineering Services (Who we are)

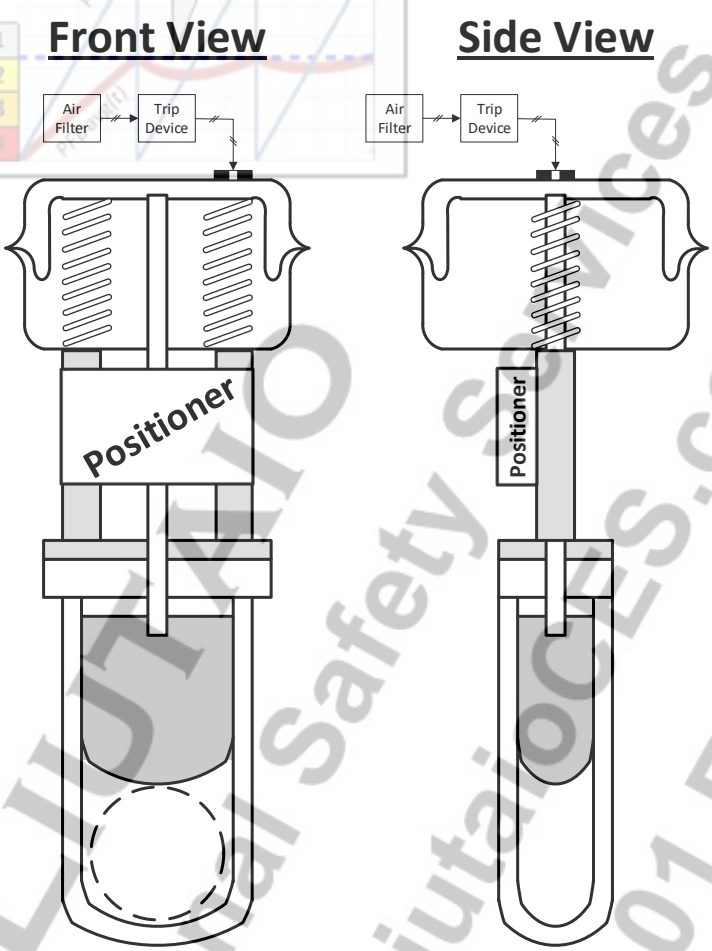
LIUTAIO is an engineering firm focused on Consulting and Engineering Services in the areas of "Process Control", Instrumentation, Simulation and "Functional Safety". Founded by MSc. Claudio Passarella in 2018.

In the area of "Functional Safety", **LIUTAIO** offers coaching & mentoring, training, consulting services, HAZOP Conduct/Support, Safety Systems design & FAT/SAT support, SIL determination consulting, SIL verification assessment, FMEA/FMECA/FMEDA assessments and "SIL Certification".

For further information and design SAMPLE documents, refer to: www.LiutaioCES.com

6.3 Description of "Target System"

Figure 1 – Actuator-Positioner-Valve arrangement sketch



The "Target System" under is an Actuator-Positione-Valve (APV) arrangement as shown in Figure 1.

The "Air Filter" and "Trip Device" are OUT OF THE SCOPE in this assessment, and they shall be included as part of a SIF design and "SIL verification".

The safety valve is gate type.

The Actuator is diaphragm pneumatic type, fail to open, installed at the top of a gate safety valve.

The Positioner is installed on the actuator yoke, with a mechanical connection to the actuator stem to measure (monitor) actuator/valve opening position.

Possible installed limit switches to detect Closed/Opened valve positions, and the Positioner **CANNOT** interfere the Actuator-Valve operation in any way.

The Positioner is connected to "Control/Safeguarding system" to monitor de "Valve" position, and to notify Operator when a "Dangerous Detected" failure is revealed.

The APV arrangement installation **MAY** or **MAY NOT** include logic in "Control/Safeguarding system" to execute a "Full Valve Stroke Test" (FVST).

NOTE: Since the "Positioner" is monitoring the valve position, then when the valve moves **WITHOUT** command, the "Positioner" (or installed FVST) can notify Safety/Control System and Operator.

In the APV arrangement:

- A dangerous failure in the "Actuator" will make the valve to fail on demand.
- A dangerous failure in the "Valve" will make the actuator to fail on demand.
- **BUT**, any kind of failure in the "Positioner" may lead to lose of the APV arrangement "Fault Detection Capabilities" only.

In practice any positioner can be used in the APV arrangement, BUT the selected "Positioner" shall comply with the following requirements:

a) Any failure in the "Positioner" **MUST NOT** be able to make Actuator-Valve to fail on demand.

b) Mechanical connection to the actuator stem **MUST NOT** interfere in the Actuator-Valve operation, and any failure in this connection **MUST NOT** be able to make Actuator-Valve to fail on demand.

c) "Positioner" MUST BE able to connect to "Control/Safeguarding system" in order to monitor de "Valve" position, and to notify Operator when a SD or DD failure is revealed.

The possible SD/DD failures to reveal are indicated in reference [D1].

6.3.1 "Target System" structure

In the "Target System", a Dangerous failure in the "Actuator" will make the "Valve" to fail on demand, and vice versa.

Figure 2 shows the "Target System" structure for FMEDA assessment in the form of a very simple "Reliability Block Diagram" (RBD). Notice that the "Positioner" **DOES NOT** appear in the RBD, because any kind of failure in the "Positioner" **WILL NOT** make the APV arrangement to fail on demand. The "Positioner" installation ONLY monitors the valve position, and it **HAS NO** effect in the APV operation.

Figure 2 – APV arrangement "Reliability Block Diagram"

6.4 FMEDA assessment conditions and scenarios

The way the APV arrangement fails in an operation/environment condition CAN CHANGE WHEN THE APV ARRANGEMENT is working in a different operation/environment condition.

"APPENDIX A" and "APPENDIX B" describe the operation/environment conditions which define the scope of work in this FMEDA assessment.

From "APPENDIX A" and "APPENDIX B", the analysis scenarios to consider in this assessment are:

5) "Fail Open" APV arrangement (Open to Trip), with FVST.
6) "Fail Open" APV arrangement (Open to Trip), NO FVST.
7) "Fail Open" APV arrangement (Close to Trip), with FVST.
8) "Fail Open" APV arrangement (Close to Trip), NO FVST.

6.5 Methodology

6.5.1 Failure classification that were used in this FMEDA assessment

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.
Fluid Leakage	Failure that causes a "Process Fluid" leakage in a "Target System".
Air Leakage	Failure that causes an "Air" leakage in a "Target System".

6.5.2 IEC-61508 Failure Model

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 ONLY by "Proof Test" or operator intervention.
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".
Proof Test Effectiveness (Et), Or Proof Test Coverage (PTC)	Portion (0-100%) of the DU failure rate revealed by "Proof Test". Applicable when "Proof Test" **IS NOT** capable to reveal all DU failures.

6.5.3 FMEDA

A "Failure Mode and Effects Analysis" (FMEA) is a methodology to identify ways a product, safety device, process or system can fail.

A "Failure Mode, Effects and Diagnostic Analysis" (FMEDA) is a systematic detailed procedure that is an extension of the classic FMEA procedure, which purpose is to calculate the failure rates of a safety device or group of safety devices.

This technique was first developed for electronic devices and recently extended to mechanical and electro-mechanical devices.

A FMEDA assessment of a hardware device or arrangement (group of devices) provides the required failure data (or Reliability data) needed for "SIL verification", "SIL Certification" or to calculate the device contribution in a "Safety Instrumented Function" (SIF) when the SIF's SIL rating is calculated.

6.6 Premises and Assumptions

1) Failure rates are constant, wear-out mechanisms are not included.
2) A "Service Life" (SLf, or mission time) of 10 years was used.
3) The end user will operate and maintain the APV arrangement according to Customer instructions.
4) "Positioner" is excluded as a device in the FMEDA assessment, because any failure in "Positioner" **WILL NOT** make APV arrangement to fail on demand.
5) The APV arrangement selection as part of a "Safety Instrumented Function" (SIF) shall be done to properly satisfy the required application, and this "APV arrangement" shall be installed, operated and maintained according to Customer documentation and instructions.
6) The APV arrangement is used within the indicated limits in "APPENDIX A" and "APPENDIX B".
7) Data to prepare this FMEDA assessment is taken from reference [D1].

6.7 Assessment Results

Table 1 – Calculated Failure rate values per assessment scenario for APV arrangement

	Item Description	Scenario 1 Fail Open Close to Trip w/FVST		Scenario 2 Fail Open Close to Trip NO FVST		Scenario 3 Fail Open Open to Trip w/FVST		Scenario 4 Fail Open Open to Trip NO FVST	
		[1 / h]	[FIT]	[1 / h]	[FIT]	[1 / h]	[FIT]	[1 / h]	[FIT]
1	Safe Detected (**SD**) Failure rate	1.19E-08	11.9	0.0	0.0	0.0	0.0	0.0	0.0
2	Safe UnDetected (**SU**) Failure rate	2.22E-07	221.6	2.33E-07	233.5	1.26E-07	126.5	1.26E-07	126.5
3	Dangerous Detected (**DD**) Failure rate	9.86E-08	98.6	0.0	0.0	0.0	0.0	0.0	0.0
4	Dangerous UnDetected (**DU**) Failure rate	2.91E-07	291.1	3.90E-07	389.8	4.97E-07	496.8	4.97E-07	496.8
5	Residual Failure rate	2.25E-08	22.5	2.25E-08	22.5	2.25E-08	22.5	2.25E-08	22.5
6	**Total Failure rate**	**6.46E-07**	**645.7**	**6.46E-07**	**645.7**	**6.46E-07**	**645.7**	**6.46E-07**	**645.7**

Table 2 - Reliability Index values related ti "SIL rating" per assessment scenario for APV arrangement

	Item Description		Eng.Unit	Scenario 1 Fail Open Close to Trip w/FVST	Scenario 2 Fail Open Close to Trip NO FVST	Scenario 3 Fail Open Open to Trip w/FVST	Scenario 4 Fail Open Open to Trip NO FVST
6	SFF Safe Failure Fraction		%	53.3%	37.5%	20.3%	20.3%
7	Device Type (IEC-61508-4 2010, section 3.6.15)		------	Type A	Type A	Type A	Type A
8	Maximum SIL to CLAIM by SFF. Fault Tolerance 0. (IEC-61508-4 2010, section 3.6.15)		%	SIL 1	SIL 0	SIL 0	SIL 0
9	PFDavg **(NOTE 1)** Probability of Failure on Demand. (1oo1)	1 year	1 / year	1.26E-03	1.68E-03	2.15E-03	2.15E-03
10		2 years	1 / year	2.52E-03	3.37E-03	4.29E-03	4.29E-03

NOTE 1: PFDavg calculation with NO Maintenance effect (TD=0, MTTR=0, MRT=0).

Table 3 – Other Reliability Index values per assessment scenario for APV arrangement

	Item Description	Eng.Unit	Scenario 1 Fail Open Close to Trip w/FVST	Scenario 2 Fail Open Close to Trip NO FVST	Scenario 3 Fail Open Open to Trip w/FVST	Scenario 4 Fail Open Open to Trip NO FVST
1	Et Proof Test Effectiveness PTC Proof Test Coverage	%	92.4%	88.9%	92.4%	92.4%
2	DCs Diagnostic Coverage Safe	%	5.1%	0.0%	0.0%	0.0%
3	DCd Diagnostic Coverage Dangerous	%	25.3%	0.0%	0.0%	0.0%
4	MTTF Mean Time to Failure	hour	1.60E+06	1.60E+06	1.60E+06	1.60E+06
5		year	185.7	185.7	185.7	185.7
6	MTTFd Mean Time to Failure Dangerously	hour	2.57E+06	2.57E+06	2.01E+06	2.01E+06
7		year	297.0	297.0	233.0	233.0

APPENDIX A – Operational/Working conditions to consider for APV arrangement FMEDA assessment

#	Operation/Working conditions	Included in assessment	Excluded from assessment	Remarks	#
1	Effect of Abrasive fluid passing through valve (erosion).		Excluded		1
2	Effect of Corrosive fluid passing through valve.		Excluded		2
3	General Liquid fluid passing through valve.	YES			3
4	Orientation installation of Fluid passing through valve.	**Not Applicable**		flow through valve plug top to bottom, or vice versa.	4
5	General Gas fluid passing through valve.		Excluded		5
6	Single phase or steam flow through valve		Excluded		6
7	Flow is flashing (vaporization) through valve		Excluded		7
8	Multi-Phase phase flow through valve		Excluded		8
9	Pressure	General Operation	High Pressure service	Above 6.4 MPa (64 Bar), or above ANSI CLASS 900	9
10			Low Pressure service	Below atmospheric pressure	10
11	Temperature.	General Operation 0-400°C (32-752°F)	High Temperature service	Above 400°C (752°F)	11
12			Cryogenic service	Below -150°C (-238°F)	12
13	Daily temperature excursion (peak to peak)	10°C (50°F)			13
14	Use of Hydraulic fluid to move valve actuator.		Excluded	Hydraulic package **IS NOT** included.	14
15	Use of Pneumatic fluid to move valve actuator.	YES		Instrument Air system **IS NOT** included.	15
16	Hydraulic, Pneumatic, or any other trip device to move the Actuator-Valve from NORMAL to SAFE state (Opened or Closed).		Excluded		16
17	Use of Electrical actuator to move valve.		Excluded		17
18	Use of handwheel to move the valve.		Excluded		18
19	Fail Close valve (Close to trip)		Excluded		19
20	Fail Open valve (Open to trip)	YES			20
21	Fail Close valve (Open to trip)		Excluded		21
22	Fail Open valve (Close to trip)	YES			22
23	Fail lock-in-last position valve		Excluded	Typically, double acting actuator	23
24	Tight-Shutoff valve		Excluded		24
25	FVST – Full Valve Stroke Test	YES			25
26	PVST – Partial Valve Stroke Test		Excluded		26

APPENDIX B – Environment and site installation conditions to consider for APV arrangement FMEDA assessment

#	Environment/Site conditions	Included in assessment	Excluded from assessment	Remarks	#
1	Surrounding Environment Temperature	0-40°C (32-104°F)			1
2	Surrounding Pressure	Atmospheric			2
3	Typical field industrial installation at grade, or at Deck elevation.	YES			3
4	APV arrangement is installed in Vertical or horizontal position	YES			4
5	Dusty environment		Excluded		5
6	Exposed to Elements / Weather condition changes	Moderate (Light rain)		Heavy rain, Thunder (Lightning), Typhon, Tornado or Hurricane **IS NOT** included.	6
7	Explosive/Inflammable area installation location	YES			7
8	Outdoors installation location	YES			8
9	Indoors @ Factory building		Excluded		9
10	Sheltered installation location		Excluded		10
11	Underwater installation location		Excluded		11
12	Underground installation location		Excluded		12
13	Humidity. Non-Condensing environment	YES		5-95% relative humidity	13
14	Humidity. Condensing environment		Excluded		14
15	Vibration at installed location	No-Vibrations			15
16	Solar radiation.	YES		Arrangement under shade in worst case.	16
17	Electromagnetic interference		Excluded		17