Failure Modes, Effects and Diagnostic Analysis

Project:
MPG**-**, HPG**-**, LCV** and EBV*** valves

Company:
m-tech GmbH
Forchtenberg
Germany

Contract Number: m-tech 22/06-062
Report No.: m-tech 22/06-062 R001
Version V1, Revision R0, January 2023
Philipp Hanzik

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the MPG**-**, HPG**-**, LCV** and EBV*** valves. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the MPG**-**, HPG**-**, LCV** and EBV*** valves. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

Table 1 gives an overview of the different versions that were considered in this FMEDA of the MPG**-**, HPG**-**, LCV** and EBV*** valves.

Table 1 Version Overview

Version	Type	Description
V1	MPG**-**	PN420 Bar – Gaseous media
V2	HPG**-**	PN600 Bar - Gaseous media
V3	LCV**	PN40 Bar- Liquid gas – Cryogen (-196°C)
V4	EBV***	PN16 Bar – Gaseous and Liquid media

The MPG**-**, HPG**-**, LCV** and EBV*** valves is classified as a device that is part of a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. See Section 6.1. Therefore, the MPG**-**, HPG**-**, LCV** and EBV*** valves can be classified as a 2_H device when the listed failure rates are used. When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H.

Based on the assumptions listed in 5.3, the failure rates for the MPG**-**, HPG**-**, LCV** and EBV*** valves are listed in section 5.5.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

The failure rates listed in this report are based on over 350 billion-unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI), see section 5.2.2.

A user of the MPG**-**, HPG**-**, LCV** and EBV*** valves 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).

[1] Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Table of Contents

1 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 MPG**-**, HPG**-**, LCV** and EBV*** valves. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

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.

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500-person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project-oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

m-tech GmbH	Manufacturer of the MPG**-**, HPG**-**, LCV** and EBV*** valves
exida	Performed the hardware assessment.

m-tech GmbH contracted *exida* with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Mechanical Component Reliability Handbook, 4th Edition, 2016	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2016 (pending publication, not publicly available at the time of this report)
[N3]	Safety Equipment Reliability Handbook, 4th Edition, 2015	*exida* LLC, Safety Equipment Reliability Handbook, Fourth Edition, 2015, ISBN 978-1-934977-13-2
[N4]	Goble, W.M., 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	O'Brien, C., Stewart, L., & Bredemeyer, L., 2018	*exida* LLC., Final Elements in Safety Instrumented Systems IEC 61511 Compliant Systems and IEC 61508 Compliant Products, 2018, ISBN 978-1-934977-18-7
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 201	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers

[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N9]	Random versus Systematic – Issues and Solutions, September 2016	http://www.exida.com/Resources/Whitepapers/random-versus-systematic-failures-issues-and-solutions
[N10]	Bukowski, J.V. and Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
[N11]	Bukowski, J.V. and Stewart, L.L., April 2016	Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	*exida* White Paper, Sellersville, PA www.exida.eu
[N13]	Goble, W.M. and Brombacher, A.C., November 1999, Vol. 66, No. 2	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.

2.4 *exida* tools used

[T1]	T-141 V1R13 Mechanical FMEDA	FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by m-tech GmbH

[D1]	HPG_12_NC_NO_de.pdf	Datasheet HPG 12 NC / NO, 24.05.2022
[D2]	HPG_12_PR_de.pdf	Datasheet HP 12 PR, 24.05.2022
[D3]	LCV_DN25_CTE.PDF	Drawing LCV**, 03.03.2021
[D4]	LCV_en.pdf	Datasheet LCV, 27.10.2022
[D5]	EBV_en.pdf	Datasheet EBV***, 27.10.2022
[D6]	MPG 03 NC_masterbinder_SL-de.pdf	BOM MPG 03, 12.12.2008
[D7]	MPG 03 NC_masterbinder_SZ.PDF	Drawing MPG 03, 06.01.2010
[D8]	MPG 03 PR_de.pdf	Datasheet MPG 03 PR, 24.05.2022
[D9]	MPG 12 NC_masterbinder_SZ.PDF	Drawing MPG 12, 25.01.2010
[D10]	MPG 12 NO_masterbinder_SL-de.pdf	BOM MPG 12, 05.12.2008
[D11]	MPG_03_NC_NO_de.pdf	Datasheet MPG 03 NC / NO, 24.05.22
[D12]	MPG_12_NC-NO_de.pdf	Datasheet MPG 12 NC / NO, 24.05.22
[D13]	MPG_12_PR_de.pdf	Datasheet MPG 12 PR, 24.05.2022
[D15]	Ventilbaugruppe 1034_HPG 12 NC_GD SZ SL_dr_en.pdf	BOM, Drawing HPG12 NC, 21.10.2015

2.5.2 Documentation generated by *exida*

[R1]	FMEDA_m-Tech HPGxx-xx.xlsm	Printout Failure Modes, Effects, and Diagnostic Analysis V0R1 of 16.09.2022
[R2]	FMEDA_m-Tech LCV**.xlsm	Printout Failure Modes, Effects, and Diagnostic Analysis V0R1 of 16.09.2022
[R3]	FMEDA_m-Tech MPGxx-xx.xlsm	Printout Failure Modes, Effects, and Diagnostic Analysis V0R1 of 16.09.2022
[R4]	M-Tech Q22-06-062 R001.docx, Sep. 2022	FMEDA report, MPG**-**, HPG**-**, LCV** and EBV*** valves (this report)

3 Product Description

These valves are designed for an operating pressure of 420 bar. The valves of type MPG**-NC (normally closed) and MPG**-NO (normally open) are 2/2-way valves which are externally controlled. When control air is supplied to the valve, it is opened or closed against the spring force, depending on the type of valve. The MPG**-PR are control valves that are externally operated by a positioner.

Figure 1 Example of MPG03- Valve**

These valves are designed for an operating pressure of 600 bar. The valves of the type HPG**-NC (normally closed) and HPG**-NO (normally open) are 2/2-way valves which are externally controlled. When the control air is supplied to the valve, it is opened or closed against the spring force, depending on the type of valve. The HPG**-PR are control valves that are externally operated by a positioner.

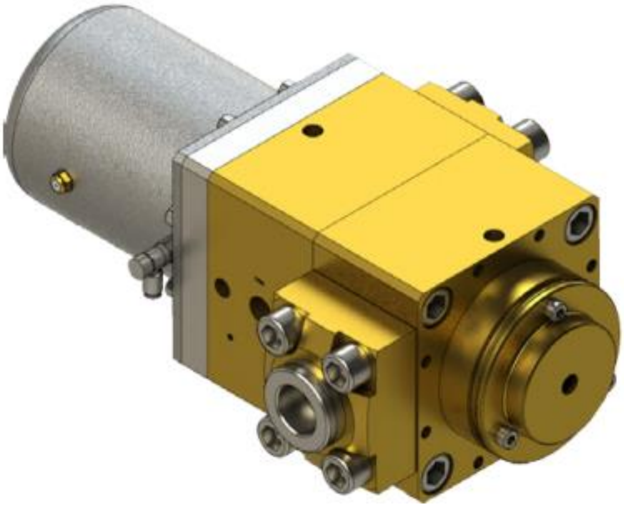

Figure 2 Example of HPG12- Valve**

These valves are designed for an operating pressure of 40 bar. The valve of the type LCV is 2/2-way valves which are externally controlled by an actuator. The valve configuration can be NC (normally closed) or NO (normally open), depending on the actuator mounted. For the control version of a positioner is required.

Figure 3 Example of LCV Valve**

These valves are designed for an operating pressure of 16 bar. The valves of the type EBV are 2/2-way valves which are externally controlled by an actuator. The valves configuration can be NC (normally closed) or NO (normally open), depending on the actuator mounted. For the control version a positioner is required.

Figure 4 Example of EBV* Valve**

4 Description of diagnostic possibilities

4.1 Partial Valve Stroke Testing (PVST)

PVST is the operation of the actuator / valve through a portion of its total stroke range. This short stroke of operation checks that the actuator / valve is not seized in the running position. The limited stroke of the actuator / valve is intended to be short enough so as not to interfere with the operating flow of the system. The purpose of PVST is to provide diagnostic checks inside the MPG**-**, HPG**-**, LCV** and EBV*** valves, which show the possibility to execute the SIF function when demanded.

Partial valve stroke testing is performed at a rate at least ten times faster than the expected demand rate in low demand applications.

5 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation listed in section 2.5.1 and is documented in [R1] – [R3].

5.1 Failure categories description

In order to judge the failure behavior of the MPG**-**, HPG**-**, LCV** and EBV*** valves, the following definitions for the failure of the device were considered.

Fail-Safe State:

Valve, Full Stroke	State where the valve is closed.
Valve, Tight-Shut-Off	State where the valve is closed and sealed with leakage no greater than the defined leak rate; Tight shut-off requirements shall be specified according to the application, if shut-off requirements allow flow greater than ANSI class V, respectively ANSI class IV, then Full Stroke numbers may be used.
Valve, Open-To-Trip	State where the valve is open.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
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).
Valve	Failure that prevents the valve from moving to the defined fail-safe state within the normal time span.
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.
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
External Leakage	Failure that causes process fluids, gas, hydraulic fluids or operating media to leak outside of the valve; External Leakage is not considered part of the safety function and therefore this failure rate is not included in any of the numbers. External leakage failure rates should be reviewed for secondary safety and environmental issues.

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

5.2 Methodology – FMEDA, failure rates

5.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress in each application. It combines design FMEA techniques with extensions to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each failure mode category [N13].

5.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] which were derived using over 350 billion-unit operational hours of process industry field failure data from multiple sources and failure data from various databases. The component failure rates are provided for each applicable operational profile and application, see Appendix C. The *exida* profile chosen for this FMEDA was Profile 3 (General Field Equipment) and Profile 6 (Process Wetted Parts) for the Valves process wetted parts as this was judged to be the best fit for the product and application information submitted by m-tech GmbH. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

The failure rates are predicted for a Site Safety Index of SSI=2 ([N10] & [N11]) as this level of operation is common in the process industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from *exida*.

The user of these numbers is responsible for determining the failure rate applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. 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. *exida* has detailed models available to make customized failure rate predictions (Contact *exida*).

Accurate plant specific data may be used to check validity of this failure rate data. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

5.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the MPG**-**, HPG**-**, LCV** and EBV*** valves.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire MPG**-**, HPG**-**, LCV** and EBV*** valves, and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.
- The stress levels are specified in the *exida* Profile used for the analysis limited by the manufacturer's published ratings.
- Materials are compatible with the environmental and process conditions.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- The device is installed and operated per the manufacturer's instructions.
- Worst-case internal fault detection time is the PVST test interval time.
- Loss of the Air Pressure supply is not included in these failure rates.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- The valves are generally applied in relatively clean gas or liquid; therefore, no severe service has been considered in the analysis.
- Valves with Latching and/or Override options are only used in applications where the use of the Latching and/or Override will not put the system in a dangerous condition.
- In order to claim diagnostic coverage for Partial Valve Stroke Testing it is automatically performed at a rate at least ten times faster than the Demand frequency.

5.4 Application specific restrictions

The following application specific restrictions are applicable to the MPG**-**, HPG**-**, LCV** and EBV*** valves and have been considered during the Failure Modes, Effects, and Diagnostic Analysis of the MPG**-**, HPG**-**, LCV** and EBV*** valves. These restrictions shall be included in the safety manual.

- The materials of construction of a MPG**-**, HPG**-**, LCV** and EBV*** valves are specified in the MPG**-**, HPG**-**, LCV** and EBV*** valves brochure. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the MPG**-**, HPG**-**, LCV** and EBV*** valves are used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

5.5 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the FMEDA analysis of the MPG**-**, HPG**-**, LCV** and EBV*** valves.

Table 2 to Table 4 lists the failure rates for the MPG**-**, HPG**-**, LCV** and EBV*** valves according to IEC 61508 with a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix D for an explanation of SSI and the failure rates for SSI of 4 (ideal maintenance practices).

Table 2 Failure rates for Static Applications[2] with Good Maintenance Assumptions in FIT @ SSI=2

MPG**-**	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	64	117	68
Tight Shut-Off, Clean Service	0	0	0	102	79	68
Open on Trip, Clean Service	0	4	0	60	117	68
Full Stroke with PVST, Clean Service	0	0	28	36	117	68
Tight Shut-Off with PVST, Clean Service	0	0	28	74	79	68
Open on Trip with PVST, Clean Service	4	0	28	32	117	68

Table 3 Failure rates for Dynamic Applications[4] with Good Maintenance Assumptions in FIT @ SSI=2

MPG**-**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	50	125	66
Tight Shut-Off, Clean Service	0	0	0	95	79	66
Open on Trip, Clean Service	0	6	0	44	125	66
Full Stroke with PVST, Clean Service	0	0	21	29	125	66
Tight Shut-Off with PVST, Clean Service	0	0	21	74	79	66
Open on Trip with PVST, Clean Service	6	0	21	23	125	66

[2] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[3] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[4] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Table 4 Failure rates for Static Applications[5] with Good Maintenance Assumptions in FIT @ SSI=2

HPG**-**	λ_{SD}	λ_{SU}[6]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	50	249	33
Tight Shut-Off, Clean Service	0	0	0	152	148	33
Open on Trip, Clean Service	0	8	0	42	249	33
Full Stroke with PVST, Clean Service	0	0	21	29	249	33
Tight Shut-Off with PVST, Clean Service	0	0	21	131	148	33
Open on Trip with PVST, Clean Service	8	0	21	21	249	33

Table 5 Failure rates for Dynamic Applications[7] with Good Maintenance Assumptions in FIT @ SSI=2

HPG**-**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	39	261	34
Tight Shut-Off, Clean Service	0	0	0	153	148	34
Open on Trip, Clean Service	0	8	0	31	261	34
Full Stroke with PVST, Clean Service	0	0	14	25	261	34
Tight Shut-Off with PVST, Clean Service	0	0	15	138	148	34
Open on Trip with PVST, Clean Service	8	0	14	17	261	34

[5] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[6] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[7] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Table 6 Failure rates for Static Applications[8] with Good Maintenance Assumptions in FIT @ SSI=2

LCV**	λ_{SD}	λ_{SU}[9]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	221	261	42
Tight Shut-Off, Clean Service	0	0	0	279	203	42
Open on Trip, Clean Service	0	4	0	217	261	42
Full Stroke with PVST, Clean Service	0	0	129	92	261	42
Tight Shut-Off with PVST, Clean Service	0	0	129	150	203	42
Open on Trip with PVST, Clean Service	4	0	129	88	261	42

Table 7 Failure rates for Dynamic Applications[10] with Good Maintenance Assumptions in FIT @ SSI=2

LCV**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	59	305	42
Tight Shut-Off, Clean Service	0	0	0	129	235	42
Open on Trip, Clean Service	0	4	0	55	305	42
Full Stroke with PVST, Clean Service	0	0	31	28	305	42
Tight Shut-Off with PVST, Clean Service	0	0	31	98	235	42
Open on Trip with PVST, Clean Service	4	0	31	24	305	42

[8] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[9] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[10] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Table 8 Failure rates for Static Applications[11] with Good Maintenance Assumptions in FIT @ SSI=2

EBV***	λ_{SD}	λ_{SU}[12]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	651	901	14
Tight Shut-Off, Clean Service	0	0	0	1550	2	14
Open on Trip, Clean Service	0	216	0	435	901	14
Full Stroke with PVST, Clean Service	0	0	172	479	901	14
Tight Shut-Off with PVST, Clean Service	0	0	172	1378	2	14
Open on Trip with PVST, Clean Service	214	2	172	263	901	14

Table 9 Failure rates for Dynamic Applications[13] with Good Maintenance Assumptions in FIT @ SSI=2

EBV***	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	548	901	13
Tight Shut-Off, Clean Service	0	0	0	1447	2	13
Open on Trip, Clean Service	0	219	0	329	901	13
Full Stroke with PVST, Clean Service	0	0	125	423	901	13
Tight Shut-Off with PVST, Clean Service	0	0	125	1322	2	13
Open on Trip with PVST, Clean Service	217	2	125	204	901	13

[11] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[12] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[13] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

E = External Leaks

As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure rates do not directly contribute to the reliability of the device but should be reviewed for secondary safety and environmental issues.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (see Section 6.1).

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the MPG**-**, HPG**-**, LCV** and EBV*** valves meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The architectural constraint type for the MPG**-**, HPG**-**, LCV** and EBV*** valves is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

Table 21 and Table 22 lists the failure rates for the MPG**-**, HPG**-**, LCV** and EBV*** valves according to IEC 61508 with a Site Safety Index (SSI) of 4 (perfect site maintenance practices). This data should not be used for SIL verification and is provided only for comparison with other analysis than has assumed perfect maintenance. See Appendix D for an explanation of SSI.

6 Using the FMEDA Results

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

6.1 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:

> "based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to
>
> - the amount of field feedback; and
> - the exercise of **expert judgment**; and when needed
> - the undertaking 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."

exida 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, ed2, 2010 does not give detailed criteria for Route 2_H, *exida* 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 by *exida*; 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.

7 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
Device	A device is something that is part of an element; but, cannot perform an element safety function on its own.
Dynamic Applications	The movement interval of the final element device is less than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.
Element	A collection of devices that perform an element safety function such as a final element consisting of a logic solver interface, actuator and valve.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
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
High demand Mode	Mode, where the demand interval for operation made on a safety-related system is less than twice the proof test interval.
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
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 frequently than the proof test; therefore, the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption, the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
Severe Service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic 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).

SSI	Site Safety Index (See Appendix D)
Static Applications	The movement interval of the final element device is greater than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2

8 Status of the Document

8.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from *exida* compiled field failure data and a collection of industrial databases. *exida* 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.

Due to future potential changes in the standards, product design changes, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical model number product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three-year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years, contact the product vendor to verify the current validity of the results.

8.2 Version History

Version History:	V1R0	Release, 26.01.2023
	V0R2	Review changes, added EBV*** Valves, 19.12.2022
	V0R1	Initial Draft of 16.09.2022
Authors:		Philipp Hanzik
Review:	V0R1:	Carlos Riveros, m-tech GmbH, 09.12.2022 Stephan Aschenbrenner, *exida.com* GmbH, 09.12.2022

Release Status: Release of 26.01.2023

At request of client.

8.3 Release signatures

B. Eng Philipp Hanzik, Safety Engineer

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner, CEO

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 5.2.2) this only applies provided that the useful lifetime[14] of 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 PFD_{avg} 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 MPG**-**, HPG**-**, LCV** and EBV*** valves per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

A major factor influencing the useful life is the air quality.

Based on general field failure data a useful life period of approximately 15 years (actuators, valves, actuator-valve combinations) is expected for the MPG**-**, HPG**-**, LCV** and EBV*** valves.

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

[14] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 f) of IEC 61508-2, proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The suggested Proof Test consists of a full stroke of the associated device, see Table 10. Refer to the table in B.2 for the Proof Test Coverages.

Table 10 Suggested Proof Test – MPG-**, HPG**-**, LCV** and EBV*** valves**

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the air supply/input to the Actuator to force the Actuator/Valve assembly to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time. Note:-This tests for all failures that could prevent the functioning of the Control Valve as well as the rest of the final control element.
3.	Inspect the Actuator and Valve for any leaks, visible damage or contamination
4.	Re-store the original air supply/input to the Actuator and confirm that the normal operating state was achieved.
5.	Remove the bypass and otherwise restore normal operation.

For the test to be effective the movement of the Valve must be confirmed. To confirm the effectiveness of the test both the travel of the Valve and slew rate must be monitored and compared to expected results to validate the testing.

B.2 Proof Test Coverage

The Proof Test Coverage is the fraction of the dangerous undetected failures that can be detected during a Proof Test. The Proof Test Coverage for the various device configurations with and without PVST (see 4.1) are given in Table 9 to Table 14.

Table 11 Proof Test Results – MPG-** – Static Application**

Application	Safety Function	$\lambda_{DU}PT$[15] (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	22	66%	39%
	Close On Trip – Tight Shutoff	60	41%	19%
	Open On Trip	18	70%	44%

Table 12 Proof Test Results – MPG-** – Dynamic Application**

Application	Safety Function	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	18	64%	38%
	Close On Trip – Tight Shutoff	64	33%	14%
	Open On Trip	12	73%	48%

Table 13 Proof Test Results – HPG-** – Static Application**

Application	Safety Function	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	19	62%	34%
	Close On Trip – Tight Shutoff	120	21%	8%
	Open On Trip	11	74%	48%

Table 14 Proof Test Results – HPG-** – Dynamic Application**

Application	Safety Function	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	18	54%	28%
	Close On Trip – Tight Shutoff	131	14%	5%
	Open On Trip	9.7	69%	43%

[15] **λ_{DU}PT** = Dangerous undetected failure rate after performing the recommended proof test.

Table 15 Proof Test Results – LCV – Static Application**

Application	Safety Function	$\lambda_{DU}PT$[16] (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	28	87%	70%
	Close On Trip – Tight Shutoff	86	69%	43%
	Open On Trip	24	89%	73%

Table 16 Proof Test Results – LCV – Dynamic Application**

Application	Safety Function	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	12	80%	57%
	Close On Trip – Tight Shutoff	82	36%	16%
	Open On Trip	8	85%	67%

Table 17 Proof Test Results – EBV*– Static Application**

Application	Safety Function	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	393	40%	18%
	Close On Trip – Tight Shutoff	1292	17%	6%
	Open On Trip	177	59%	33%

Table 18 Proof Test Results – EBV*– Dynamic Application**

Application	Safety Function	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage	
			No PVST	with PVST
Clean Service	Close On Trip – Full Stroke	361	34%	15%
	Close On Trip – Tight Shutoff	1259	13%	5%
	Open On Trip	141	57%	31%

[16] **$\lambda_{DU}PT$** = Dangerous undetected failure rate after performing the recommended proof test.

Appendix C *exida* Environmental Profiles

Table 19 *exida* Environmental Profiles

***exida* 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 also applicable for D1	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[17]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[18]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[19]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[20]	G2	G3	G3	G3	G3	Compatible Material
Surge[21]						
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	
EMI Susceptibility[22]						
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	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[23]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[17] Humidity rating per IEC 60068-2-3
[18] Shock rating per IEC 60068-2-27
[19] Vibration rating per IEC 60068-2-6
[20] Chemical Corrosion rating per ISA 71.04
[21] Surge rating per IEC 61000-4-5
[22] EMI Susceptibility rating per IEC 61000-4-3
[23] ESD (Air) rating per IEC 61000-4-2

Appendix D Site Safety Index

Numerous field failure studies have shown that the failure rate for a specific device (same Manufacturer and Model number) will vary from site to site. The Site Safety Index (SSI) was created to account for these failure rates differences as well as other variables. The information in this appendix is intended to provide an overview of the Site Safety Index (SSI) model used by *exida* to compensate for site variables including device failure rates.

D.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 20 details the interpretation of each SSI level. Note that the levels mirror the levels of SIL assignment and that SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site and therefore there is no degradation in safety performance due to any end-user activities or practices, i.e., that the product inherent safety performance is achieved.

Several factors have been identified thus far which impact the Site Safety Index (SSI). These include the quality of:

Commission Test
Safety Validation Test
Proof Test Procedures
Proof Test Documentation
Failure Diagnostic and Repair Procedures
Device Useful Life Tracking and Replacement Process
SIS Modification Procedures
SIS Decommissioning Procedures
and others

Table 20 *exida* Site Safety Index Profiles

Level	Description
SSI 4	Perfect - Repairs are always correctly performed, Testing is always done correctly and on schedule, equipment is always replaced before end of useful life, equipment is always selected according to the specified environmental limits and process compatible materials. Electrical power supplies are clean of transients and isolated, pneumatic supplies and hydraulic fluids are always kept clean, etc. **Note:** This level is generally considered not possible but retained in the model for comparison purposes.
SSI 3	Almost perfect - Repairs are correctly performed, Testing is done correctly and on schedule, equipment is normally selected based on the specified environmental limits and a good analysis of the process chemistry and compatible materials. Electrical power supplies are normally clean of transients and isolated, pneumatic supplies and hydraulic fluids are mostly kept clean, etc. Equipment is replaced before end of useful life, etc.
SSI 2	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.
SSI 1	Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.
SSI 0	None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.

D.2 Site Safety Index Failure Rates – MPG**-**, HPG**-**, LCV** and EBV*** valves

Failure rates of each individual device in the SIF are increased or decreased by a specific multiplier which is determined by the SSI value and the device itself. It is known that final elements are more likely to be negatively impacted by less than ideal end-user practices than are sensors or logic solvers. By increasing or decreasing device failure rates on an individual device basis, it is possible to more accurately account for the effects of site practices on safety performance.

Table 21 to Table 22 lists the failure rates for the MPG**-**, HPG**-**, LCV** and EBV*** valves according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 21 Failure rates for Static Applications[24] with Ideal Maintenance Assumption in FIT (SSI=4)

MPG**-**	λ_{SD}	λ_{SU}[25]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	32	70	41
Tight Shut-Off, Clean Service	0	0	0	51	47	41
Open on Trip, Clean Service	0	2	0	30	70	41
Full Stroke with PVST, Clean Service	0	0	14	18	70	41
Tight Shut-Off with PVST, Clean Service	0	0	14	37	47	41
Open on Trip with PVST, Clean Service	2	0	14	16	70	41

Table 22 Failure rates for Dynamic Applications[26] with Ideal Maintenance Assumption in FIT (SSI=4)

MPG**-**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	25	75	39
Tight Shut-Off, Clean Service	0	0	0	48	47	39
Open on Trip, Clean Service	0	4	0	22	75	39
Full Stroke with PVST, Clean Service	0	0	11	14	75	39
Tight Shut-Off with PVST, Clean Service	0	0	11	37	47	39
Open on Trip with PVST, Clean Service	4	0	11	11	75	39

[24] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[25] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[26] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Table 23 Failure rates for Static Applications[27] with Ideal Maintenance Assumption in FIT (SSI=4)

HPG**-**	λ_{SD}	λ_{SU}[28]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	25	149	20
Tight Shut-Off, Clean Service	0	0	0	76	89	20
Open on Trip, Clean Service	0	5	0	21	149	20
Full Stroke with PVST, Clean Service	0	0	10	15	149	20
Tight Shut-Off with PVST, Clean Service	0	0	11	65	89	20
Open on Trip with PVST, Clean Service	5	0	10	11	149	20

Table 24 Failure rates for Dynamic Applications[29] with Ideal Maintenance Assumption in FIT (SSI=4)

HPG**-**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	20	156	20
Tight Shut-Off, Clean Service	0	0	0	76	89	20
Open on Trip, Clean Service	0	5	0	16	156	20
Full Stroke with PVST, Clean Service	0	0	8	12	156	20
Tight Shut-Off with PVST, Clean Service	0	0	7	69	89	20
Open on Trip with PVST, Clean Service	5	0	8	8	156	20

[27] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[28] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[29] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Table 25 Failure rates for Static Applications[30] with Ideal Maintenance Assumption in FIT (SSI=4)

LCV**	λ_{SD}	λ_{SU}[31]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	111	156	25
Tight Shut-Off, Clean Service	0	0	0	139	122	25
Open on Trip, Clean Service	0	2	0	109	156	25
Full Stroke with PVST, Clean Service	0	0	65	46	156	25
Tight Shut-Off with PVST, Clean Service	0	0	64	75	122	25
Open on Trip with PVST, Clean Service	2	0	65	44	156	25

Table 26 Failure rates for Dynamic Applications[32] with Ideal Maintenance Assumption in FIT (SSI=4)

LCV**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	30	183	25
Tight Shut-Off, Clean Service	0	0	0	65	141	25
Open on Trip, Clean Service	0	2	0	28	183	25
Full Stroke with PVST, Clean Service	0	0	16	14	183	25
Tight Shut-Off with PVST, Clean Service	0	0	16	49	141	25
Open on Trip with PVST, Clean Service	2	0	16	12	183	25

[30] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[31] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[32] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

Table 27 Failure rates for Static Applications[33] with Ideal Maintenance Assumption in FIT (SSI=4)

EBV***	λ_{SD}	λ_{SU}[34]	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	325	541	8
Tight Shut-Off, Clean Service	0	0	0	775	1	8
Open on Trip, Clean Service	0	130	0	217	541	8
Full Stroke with PVST, Clean Service	0	0	85	240	541	8
Tight Shut-Off with PVST, Clean Service	0	0	86	689	1	8
Open on Trip with PVST, Clean Service	129	1	85	132	541	8

Table 28 Failure rates for Dynamic Applications[35] with Ideal Maintenance Assumption in FIT (SSI=4)

EBV***	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Full Stroke, Clean Service	0	0	0	274	540	8
Tight Shut-Off, Clean Service	0	0	0	723	1	8
Open on Trip, Clean Service	0	132	0	165	540	8
Full Stroke with PVST, Clean Service	0	0	62	212	540	8
Tight Shut-Off with PVST, Clean Service	0	0	62	661	1	8
Open on Trip with PVST, Clean Service	131	1	63	102	540	8

[33] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[34] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[35] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.