

Nachweisbericht zur Systematischen Eignung (SC)
gemäß IEC 61508/
Report for Proof of Systematic Capability (SC)
acc. IEC 61508

Produkt/Product:

Armaturen-Baureihen mit Antrieben für Anwendungen in
Sicherheitskreisen der Prozessindustrie und der Energieerzeugung
Valve Series for Application in Safety Functions of Process Industry and
Power Generation

Hersteller/Manufacturer:

Holter Regelarmaturen GmbH&Co.KG
Helleforthstraße 58-60
D-33758 Schloß Holte-Stukenbrock

B-Nr./Report-No. 190355

Rev. 1.0

Classification: none

Ersteller/Assessor:

INGENIEURBÜRO URBAN
Dipl.-Ing. Josef Urban

Öffentlich bestellter und vereidigter Sachverständiger für Sicherheitsfragen für programmierbare elektronische Systeme
Anerkannter Sachverständiger für die Prüfung elektrischer Anlagen

Büro Bodensee-Oberschwaben
Kirchstraße 8, D-88239 Wangen i.A.
Tel. +49 171/521-3509

Büro München
Anzingerstr. 24, D-85604 Pöding b. München
Tel. +49 8106/236626 Fax. +49 8106/236624

E-Mail mail@ibu-sv.de
Mobiltel. +49 171/521-3509

B190355_V10_SC-Report_HORA_Produktpalette Armaturen mit Antrieben		Seite 1 von 13
<p>INGENIEURBÜRO URBAN – Dipl.-Ing. J. Urban Öffentl. Bestellung u. Vereidigung ♦ Zeichen für Sachverstand ♦ Unabhängigkeit ♦ Unparteilichkeit Publicly certified ♦ The mark of quality in the expert profession ♦ Independence ♦ Impartiality Certificación pública ♦ Señal de competencia ♦ Independencia ♦ Imparcialidad</p> <p>© INGENIEURBÜRO URBAN Rev. 11.2017</p>		

Inhaltsverzeichnis

0. Vorbemerkungen / Benutzungshinweise	3
0.1 Revisionsindex	4
1. Management Summary	5
1.1 Besondere Hinweise für den Anwender ..	5
2. Beschreibung des Produktes	6
2.1 Allgemeiner Aufbau und Typisierung	6
2.2 Weitere Definitionen und Abkürzungen ...	7
3. Referenzunterlagen	8
3.1 Normen und sonstige Literatur	8
3.2 Ergebnisberichte im Rahmen der SC-Analyse	9
4. Nachweis der Systematischen Eignung (SC)	10
4.1 Methodik der SIL-Fähigkeits-Analyse	10
4.2 Vorgehensweise beim Nachweis der systematischen Eignung.....	10
4.3 Anforderungen an das Management der Funktionalen Sicherheit	11
4.4 Anforderung an die Auslegung und Realisierung des Produkts (Route 1S).....	12
4.5 Anforderungen an den Modifikationsprozess	12
4.6 Bewertung der systematischen Eignung (systematische Sicherheitsintegrität)	12
5. Ergebnisse	13

Contents

0. Remarks/Information for Use	3
0.1 Revision Index	4
1. Management Summary	5
1.1 Special information for the user	5
2. Product Description	6
2.1 General Structure and Type.....	6
2.2 Further Definitions and Acronyms.....	7
3. Reference Documents	8
3.1 Standards and Other Literature.....	8
3.2 Result Reports within the SC-Analysis....	9
4. Proof of Systematic Capability (SC)	10
4.1 Method of SIL Capability Analysis.....	10
4.2 Procedure for Proof of Systematic Capability	10
4.3 Requirements for the Functional Safety Management	11
4.4 Requirements for the Design- and Realization of the Product (Route 1S).....	12
4.5 Requirements for the Modification Process	12
4.6 Evaluation of Systematic Capability (Systematic Safety Integrity)	12
5. Results	13

0. Vorbemerkungen / Benutzungshinweise

Der vorliegende Bericht fasst die Ergebnisse der Bewertung der systematischen Eignung nach IEC 61508 für Armaturenbaureihen der Firma HORA Holter Regelarmaturen GmbH&Co.KG mit und ohne Antrieben zusammen.

Die Armaturenbaureihen mit und ohne Antrieb werden in Sicherheitsfunktionen zum Absperrren und Regeln von Stoffströmen in Energieerzeugungsanlagen und Prozessanwendungen verwendet.

Die Armaturenbaureihen werden im Folgenden als „Ventile“ bezeichnet.

Mit der Bewertung der systematischen Eignung auf Grundlage der IEC 61508 wurde der qualitative Nachweis gemäß IEC 61508-1 und IEC 61508-2, Route 1S geführt, dass die Ventile die einem Prozess gemäß IEC 61508 unterliegen grundsätzlich zum Einsatz in sicherheitstechnischen Anwendungen geeignet sind.

Die Bewertung der systematischen Eignung zeigt, dass die grundlegenden Anforderungen an das Management der Funktionalen Sicherheit (FSM), sowie die zutreffenden Anforderungen an die Entwicklung und Auslegung der Ventile erfüllt sind.

Der Bericht liefert den Nachweis der systematischen Eignung (SC) für die untersuchten Armaturenbaureihen und bildet somit gemeinsam mit dem für die jeweiligen Armaturenbaureihen erforderlichen quantitativen SIL-Fähigkeitsnachweis den Nachweis der Eignung der Ventile für den Einsatz in sicherheitstechnischen Anwendungen.

Das Ergebnis kann für den weitergehenden Nachweis der systematischen Eignung von Sicherheitsanwendungen, in denen die Ventile eingesetzt werden, verwendet werden.

Die Ergebnisse sind in Kapitel 1 zusammengefasst.

Wangen/Pöring, den 06. Dezember 2019
INGENIEURBÜRO URBAN



Dipl.-Ing. J. Urban

0. Remarks/Information for Use

This report is summarizing the results of the systematic capability evaluation according to IEC 61508 for vavle series manufactured by HORA Holter Regelarmaturen GmbH&Co.KG with and without drives.

The valve series with and without drive are used in safety functions to close or control mass flow in in power generation plants and process applications.

The valves series are named as “valves” in the following.

With the evaluation of the systematic capability based on IEC 61508, the qualitative proof according to IEC 61508-1 and IEC 61508-2, route 1S has been performed that the valves which are supposed to a process acc. IEC 61508 are basically suitable for use in safety related applications.

The evaluation of the systematic capability shows that the fundamental requirements for the functional safety management (FSM) and the applicable requirements for the design and dimensioning of the valves are fulfilled.

The report delivers the proof of systematic capability (SC) for the analyzed valve series and forms in combination with the quantitative SIL-capability analysis required for the valve series the proof of the capability of the valves to be used in safety related applications.

The result can be used for further demonstration of the systematic capability of safety applications, in which the valves are used.

The results are summarized in chapter 1.

Wangen/Pöring, 6th December, 2019
INGENIEURBÜRO URBAN



Dipl.-Ing. J. Urban

0.1 Revisionsindex

Index	Datum	Abschnitt	Beschreibung der Änderungen
V0.1	23.2019	Alle	Entwurf (Erstfassung)
V1.0	06.12.2019	Alle	Endfassung nach internem Review

0.1 Revision Index

Index	Date	Section	Description of the changes
V0.1	2019-10-23	All	First draft
V1.0	2019-12-06	All	final version after internal review

1. Management Summary

Der Nachweis der systematischen Eignung erfolgte durch ein Audit der beim Hersteller implementierten Prozessabläufe unter Berücksichtigung der grundlegenden Anforderungen gemäß IEC 61508-1 zum Management der Funktionalen Sicherheit (FSM) und gemäß IEC 61508-2, Route 1S für die Entwicklung und Realisierung der Ventile.

Das Ergebnis, der in diesem Bericht zusammengefassten Untersuchungen, zeigt, dass die Ventile mit einer systematischen Eignung von

SC 3

qualitativ zum Einsatz in sicherheitstechnischen Anwendungen bis SIL 3 geeignet sind.

Die systematische Eignung ist alle fünf Jahre durch ein Re-Audit zu bestätigen.

Die systematische Eignung erlischt, falls sich signifikante Änderungen der zugrundeliegenden Prozesse und Tätigkeiten ergeben oder ein Re-Audit nicht rechtzeitig durchgeführt wird.

Der Hersteller ist dafür verantwortlich, dass die für die systematische Eignung notwendigen Prozesse und Tätigkeiten implementiert, angewendet, erhalten und weiterentwickelt werden.

Der Nachweis der systematischen Eignung bezieht sich nur auf das einzelne Ventil. Der Nachweis der systematischen Eignung des Sicherheitskreises, in dem das Ventil eingesetzt wird, obliegt dem Anwender.

Der Nachweis der systematischen Eignung bezieht sich nur auf die HORA Ventile. Steuerungen, Zukaufteile und Anbauteile die nicht unmittelbar mit den HORA Ventilen geliefert werden, sind nicht Gegenstand dieser Untersuchung.

Der quantitative Eignungsnachweis (quantitative SIL-Fähigkeitsanalyse), gemäß IEC 61508-1, Tabelle 2 bzw. 3 und IEC 61508-2, (Route 1H bzw. Route 2H), ist nicht Bestandteil dieses Berichts und ist gesondert zu führen.

1.1 Besondere Hinweise für den Anwender

Folgende Hinweise sind vom Anwender zu beachten:

- Der Nachweis der systematischen Eignung des sicherheitstechnischen Systems, in dem ein Ventil eingesetzt wird, ist Aufgabe des Anwenders und muss gemäß IEC 61508-2, 7.4.3 bzw. IEC 61511 erfolgen.
- Die Anforderungen an den Einsatz des Ventils in sicherheitstechnischen Anwendungen sind im Sicherheitshandbuch des Ventils dokumentiert. Sie müssen vom Anwender zwingend eingehalten werden.

Für weitere Details Siehe Kapitel 4 dieses Berichts.

1. Management Summary

The proof of systematic capability was provided by an audit of the implemented processes at the manufacturer site considering the general requirements of IEC 61508-1 for functional safety management (FSM) and of IEC 61508-2, route 1S for valve design and realization.

The result of the analysis, summarized in this report, shows, that the valves with a systematic capability of

SC 3

are qualitative suitable to be used in safety related application up to SIL 3.

The systematic capability must be confirmed every five years by a re-audit.

The systematic capability expires, if there are significant changes in the underlying processes and activities or a Re-Audit is not executed in time.

It's manufacturer's responsibility that the required processes and activities will be implemented, applied, sustained and further developed.

The proof of systematic capability takes into account only the single valve. The proof of the systematic capability of the safety loop, within the valve is used, is in the responsibility of the user.

The proof of the systematic capability obtains only the HORA valves. Control units, purchasing parts, and attached parts which are not delivered in combination with the HORA valves are not part of this analysis.

The quantitative proof of capability (SIL capability analysis) following the quantitative criteria of IEC 61508-1, table 2 or 3 and IEC 61508-2, route 1H or route 2H, is not part of this report and must be proceeded separately.

1.1 Special information for the user

The following remarks have to be considered by the user:

- The proof of systematic capability of the safety related system the valve is used within, is task of the user and must comply with IEC 61058-2, 7.4.3 or IEC 61511.
- The requirements for using the valve in safety related applications are documented in the safety manual of the valve. They are mandatory for the user.

For further details, see chapter 4 of this report.



2. Beschreibung des Produktes

2.1 Allgemeiner Aufbau und Typisierung

Die systematische Eignung wurde für folgende Ventile nachgewiesen:

- Ventile die dem grundlegenden Prozess für Sicherheitsanwendungen und dem Functional Safety Management der Fa. HORA unterliegen

verschiedene Ventilserien:

Die Ventilserien für sicherheitstechnische Anwendungen werden in unterschiedlichen Baugrößen und Nenndruckstufen hergestellt. Die angewendeten Design und Fertigungsprozesse, sowie das Functional Safety Management basieren jedoch auf firmeneinheitlichen Prozessen.

2. Product Description

2.1 General Structure and Type

The systematic capability is proofed for the following valves:

- Valves which are supposed to the basic process for safety application and the Functional Safety Management of HORA.

different valve series:

The Valve series for safety applications are manufactured in different sizes and nominal pressure ranges. The applied design and manufacturing processes as well as the Functional Safety Management are based on company corporate processes.

2.2 Weitere Definitionen und Abkürzungen

2.2 Further Definitions and Acronyms

Tabelle 1: Definitionen und Abkürzungen

Table 1: Definitions and Acronyms

Aktor, Komponente / Final element, component	Teil eines sicherheitstechnischen Systems, das die Eingriffe in den Prozess ausführt, um einen sicheren Zustand zu erreichen.	Part of a safety instrumented system, which implements the physical action necessary to achieve a safe state.
System / Teilsystem System / Subsystem	Menge von Elementen, die nach einem Entwurf in gegenseitiger Beziehung stehen. Ein Element eines Systems kann zugleich ein anderes System sein, genannt Teilsystem, welches ein steuerndes oder ein gesteuertes System sein und Hardware, Software und menschliche Eingriffe beinhalten kann.	Set of elements, which interact according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction.
Systematische Eignung / Systematic Capability SC	Maß des Vertrauens (ausgedrückt auf einer Skala von SC 1 bis SC 4), dass die systematische Sicherheitsintegrität eines Elements den Anforderungen des festgelegten SILs hinsichtlich der festgelegten Element-Sicherheitsfunktion entspricht, wenn das Element in Übereinstimmung mit den im Sicherheitshandbuch für konforme Objekte für das Element festgelegten Anweisungen angewendet wird.	Measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.
Management der Funktionalen Sicherheit / Functional Safety Management FSM	Das Management der Funktionalen Sicherheit beschreibt die im Unternehmen implementierten Prozesse zum Erreichen des erforderlichen Levels der Funktionalen Sicherheit (SIL) von Komponenten, Teilsystemen und Systemen zur Erfüllung von Sicherheitsfunktionen.	The management of Functional Safety describes the implemented Processes in a company to achieve the required level of functional safety (SIL) of components, subsystems and systems to fulfill safety functions.
Zufälliger Hardware Fehler / Random Hardware Failure λ	Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften der Bauteile führen	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.
Systematischer Fehler / Systematic failure	Systematisches Versagen/Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann	Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors
Sicherer Zustand / Safe state SS	Zustand/Position, die als sicher für das System definiert worden sind.	Status/position, which is defined as safe for the System.
Sicherheitsfunktion / safety function SF	Funktion verantwortlich für das Halten oder das Erreichen des sicheren Zustands aus der aktuellen Position/ aus dem aktuellen Betriebszustand innerhalb der Sicherheitszeit vom Zeitpunkt der Anforderung der Sicherheitsfunktion ausgehend.	Function responsible to maintain or achieve the safe state from the actual position/mode of operation after request of the safety function within the safety time.
Weitere Abkürzungen und Definitionen siehe IEC 61508-4, IEC 61508-7, und IEC 61511-1		Further acronyms and definitions see IEC 61508-4, IEC 61508-7, and IEC 61511-1

3. Referenzunterlagen

3.1 Normen und sonstige Literatur

Tabelle 2: Referenzunterlagen, Normen und sonstige Literatur

3. Reference Documents

3.1 Standards and Other Literature

Table 2: Referenced documents, standards and other literature

No.	Title	remarks
[1]	IEC 61508-1 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Part 1- General requirements	
[2]	IEC 61508-2 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems	
[3]	IEC 61508-3 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Software Requirements	
[4]	IEC 61508-4 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Definitions and abbreviations	
[5]	IEC 61508-5 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Examples of methods for the determination of safety integrity levels	
[6]	IEC 61508-6 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Guidelines on the application of IEC 61508-2 and IEC 61508-3	
[7]	IEC 61508-7 Edition 2.0 /2010: Functional safety of electrical/electronic/programmable electronic safety-related systems: Overview of techniques and measures	
[8]	IEC 61511-1/2016: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements	
[9]	IEC 61511-2/2016: Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1:2016	
[10]	IEC 61511-3/2016: Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels	



3.2 Ergebnisberichte im Rahmen der SC-Analyse

3.2 Result Reports within the SC-Analysis

Tabelle 4: Referenzunterlagen – Auditbericht

Table 4: Reference documents – Audit Reports

No.	Title	remarks
[11]	INGENIEURBÜRO URBAN: Audit-Report for Functional Safety Assessment acc. IEC 61508, HORA Valve Series for Safety Application in Power Generation and Process Industry Applications, Report No.: B190354, Version 1.0 File name: B190354_V10_Audit-Report_HORA_Product ValveSeries for Safety Application	

4. Nachweis der Systematischen Eignung (SC)

4.1 Methodik der SIL-Fähigkeits-Analyse

Beim Analysegegenstand von SIL-Fähigkeits-Analysen handelt es sich immer um Komponenten von Sicherheitskreisen, d.h. nicht um den gesamten Sicherheitskreis. Das Analyseergebnis ist daher stets nur ein Nachweis, dass die jeweilige Komponente für den Einsatz in Sicherheitskreisen, die einem bestimmten Safety Integrity Level (SIL) genügen müssen, geeignet ist.

Die SIL-Fähigkeitsanalyse besteht aus folgenden Teilschritten:

- Nachweis der probabilistischen Sicherheitsintegrität (rechnerischer Nachweis, quantitative Verifizierung, gemäß IEC 61508-1, Tabelle 2 sowie IEC 61508-2, Route 1H oder 2H)
- Nachweis der systematischen Sicherheitsintegrität (systematische Eignung, qualitative Verifizierung, gemäß IEC 61508-1, FSM sowie IEC 61508-2, Route 1S oder 2S)

Der vorliegende Bericht dient als Nachweis der systematischen Eignung der Ventile zum Einsatz in sicherheitstechnischen Anwendungen. Der Nachweis der systematischen Eignung erfolgt anhand der IEC 61508-1, Anforderungen an das Management der Funktionalen Sicherheit (FSM) sowie anhand der IEC 61508-2, Route 1S.

Der quantitative Eignungsnachweis (quantitative SIL-Fähigkeitsanalyse), gemäß IEC 61508-1, Tabelle 2 und IEC 61508-2, Route 1H bzw. Route 2H ist nicht Bestandteil dieses Berichts und ist separat zu führen.

4.2 Vorgehensweise beim Nachweis der systematischen Eignung

Der Nachweis der systematischen Eignung gemäß IEC 61508 basiert auf

- einem Audit der für die Funktionale Sicherheit relevanten Produktdokumentation sowie
- einem Audit des Functional Safety Management Systems.

Dabei werden die in Kapitel 4.3-4.5 des vorliegenden Berichtes aufgeführten grundlegenden Anforderungen überprüft.

Da es sich bei Ventilen mit und ohne Antrieb generell um mechanische Komponenten handelt, werden die normativen Anforderungen der IEC 61508-1/-2 für die Bewertung der systematischen Eignung an die Ventile und deren Komplexität angepasst (Tailoring) und Mindestanforderungen definiert.

Mit Erfüllung der Mindestanforderungen ist die systematische Eignung nachgewiesen.

Die Bewertung der systematischen Eignung kann über die Mindestanforderung hinausgehende weitere Maßnahmen empfehlen, die die Funktionale Sicherheit in der Produktentwicklung und/oder Realisierung

4. Proof of Systematic Capability (SC)

4.1 Method of SIL Capability Analysis

Scope of SIL capability analysis are always components of safety loops and mostly not the overall safety loop. The result of the analysis therefore is only the proof that the analyzed component will fit for use in safety loops, which must fulfill the requirements of a certain Safety Integrity Level (SIL).

The SIL capability analysis consists of following steps:

- Proof of the probabilistic safety integrity (proof by calculation, quantitative verification, according to IEC 61508-1, table 2 and IEC 61508-2, route 1H or 2H)
- Proof of the systematic safety integrity (systematic capability, qualitative verification, according to IEC 61508-1, FSM and IEC 61508-2, route 1S or 2S)

This report serves as proof of systematic capability of the valves for usage in safety related applications. The proof of the systematic capability has been performed considering IEC 61508-1, requirements to the functional safety management (FSM), and follows the IEC 61508-2, route 1S.

The quantitative proof of capability (SIL capability analysis) following the quantitative criteria of IEC 61508-1, table 2 and IEC 61508-2, route 1H or route 2H is not part of this report and must be proceeded separately.

4.2 Procedure for Proof of Systematic Capability

The proof of systematic capability according to IEC 61508 is based on

- an audit of the relevant product documentation, which is necessary for functional safety, and on
- an audit of the Functional Safety Management System.

Hereby the basic requirements listed in the chapters 4.3-4.5 of this report have been verified.

Valves are generally mechanical components. Thus, the normative requirements of the IEC 61508-1/-2 are tailored to the valve and the valve complexity for systematic capability evaluation (Tailoring) and minimum requirements are defined.

By fulfilling the minimum requirements, the systematic capability is proven.

The evaluation of the systematic capability may recommend further measures in addition to the minimum requirements, which improve functional safety in the design and/or realization phase.



verbessern.

Die Erfüllung der systematischen Eignung ist regelmäßig durch Re-Audits (alle 5 Jahre) nachzuweisen. Der Hersteller ist für die Veranlassung der regelmäßigen Re-Audits verantwortlich.

4.3 Anforderungen an das Management der Funktionalen Sicherheit

Gemäß IEC 61508-1, Kapitel 5 und 6 muss der Hersteller sicherheitsgerichteter Produkte grundlegende Anforderungen auf Managementebene erfüllen (im Sinne des Managements der Funktionalen Sicherheit (FSM)):

- Die Verantwortlichkeiten für Tätigkeiten im Zusammenhang mit Produkten für sicherheitstechnische Anwendungen müssen festgelegt sein.
- Die Maßnahmen und Methoden zum Erreichen der Funktionalen Sicherheit von Produkten (Ziel: Herstellererklärung für SIL-Produkte) müssen festgelegt sein.
- Eine eindeutige Spezifikation der sicherheitsrelevanten Merkmale und Funktionen des Produkts (Safety Requirements Specification = SRS) muss in den Maßnahmen und Methoden enthalten sein.
- Die Festlegung von Tätigkeiten zur Validierung, Verifizierung und Produktdokumentation muss in den Maßnahmen und Methoden enthalten sein.
- Es muss ein Nachweis der fachlichen Eignung aller am Entstehungsprozess von sicherheitsrelevanten Produkten Beteiligten (Ausbildungs- und Schulungsnachweise) geführt werden.
- Der Art und Umfang der sicherheitstechnischen Dokumentation (Safety Case) z.B. SRS (Safety Requirements Specification), Auslegungsdokumentation, Fertigungsdokumentation, Prüfdokumentation, Sicherheitshandbuch, muss festgelegt sein.

Die erforderlichen Prozesse und Verfahren können in einem eigenen Functional Safety Management System (FSM) dokumentiert werden oder auch in ein integriertes Managementsystem (QM, UM, ASM, FSM) implementiert werden.

The fulfillment of the systematic capability must be verified regularly (every 5 years) by Re-Audits. The manufacturer is responsible to initiate the regularly re-audit.

4.3 Requirements for the Functional Safety Management

According to IEC 61508-1, chapter 5 and 6, the manufacturer of safety related products must fulfill basic requirements in the sense of the functional safety management (FSM):

- The responsibilities for activities concerning products for safety related applications must be defined.
- The procedures and methods for achieving functional safety of products used in safety related applications (products with SIL-manufacturer declaration) must be specified.
- Within the procedures and methods, the specification of safety related features and functions (Safety Requirements Specification = SRS) of the product must be included.
- Within the procedures and methods, the activities for validation, verification and product documentation must be defined.
- Evidence of the technical expertise of all parties involved in the development process of safety-related products (training and training certificates) must be provided.
- The content and storage of safety related documentation must be defined. Safety related documents are e.g. the safety requirements specification (SRS), the design documentation, manufacturing documentation, test protocols and the safety manual.

The required processes and procedures for the FSM can be implemented in a separate management system or in an integrated management system (QM, EM, HSM, FSM).



4.4 Anforderungen an die Auslegung und Realisierung des Produkts (Route 1S)

Gemäß IEC 61058-2, Route 1S sind folgende Mindestanforderungen an die Produktrealisierung zu erfüllen:

- Es muss eine vollständige und gepflegte Produktdokumentation verfügbar sein (IEC 61508-2, 7.2).
- Maßnahmen zur Beherrschung und Vermeidung systematischer Fehler in der Produktentwicklung, Fertigung, Inbetriebnahme, während des Betriebs und der Wartung müssen installiert sein (IEC 61508-2, 7.4, 7.6).
- Die sicherheitstechnischen Funktionen des Produktes müssen validiert werden (IEC 61508-2, 7.7).

4.5 Anforderungen an den Modifikationsprozess

Gemäß IEC 61508-2, 7.8 sind folgende Mindestanforderungen an den Modifikationsprozess zu erfüllen:

- Der Hersteller muss einen Modifikationsprozess für Änderungen am sicherheitsrelevanten Produkt während der Lebenszyklusphasen Entwicklung, Inbetriebnahme, Betrieb und Wartung installieren um unerwünschte Auswirkungen von Änderungen auf die funktionale Sicherheit des Produkts zu vermeiden.
- Modifikationen müssen min. auf dem gleichen Niveau (technisch, organisatorisch) durchgeführt werden wie die ursprüngliche Entwicklung.
- Änderungen des Produkts müssen durch den Hersteller nachvollziehbar dokumentiert sein.
- Der Hersteller muss ein Verfahren zur Behebung von bekannten Fehlern des Produkts im Feld installiert haben (Korrekturmaßnahme im Feld, Field Safety Corrective Action).

4.6 Bewertung der systematischen Eignung (systematische Sicherheitsintegrität)

Die Bewertung der systematischen Eignung des Produkts zum Einsatz in sicherheitsgerichteten Anwendungen erfolgt auf der Basis von Auditergebnissen.

Das Audit umfasste die Stichprobenüberprüfung der Anforderungen in den Kapiteln 4.3 – 4.5 dieses Berichtes anhand der bereitgestellten Herstellerdokumentation für die in Kapitel 2.1 genannten Ventile.

Die Bewertung berücksichtigt die Komplexität und die Beschaffenheit der jeweiligen Ventile anhand einer ingenieurmäßigen Bewertung der einzelnen Anforderung sowie deren Relevanz zur Funktionalen Sicherheit des Produkts. Ggf. werden Maßnahmen zur Verbesserung der funktionalen Sicherheit des Produktes empfohlen.

4.4 Requirements for the Design- and Realization of the Product (Route 1S)

According to IEC 61508-2, Route 1S the following minimum requirements to the product realization must be fulfilled:

- A complete and maintained product documentation must be available (IEC 61508-2, 7.2).
- Measures for controlling and avoiding systematic faults during product design phase, manufacturing, commissioning, operation, and maintenance must be installed (IEC 61508-2, 7.4, 7.6).
- The safety related functions of the product must be validated (IEC 61508-2, 7.7).

4.5 Requirements for the Modification Process

According to IEC 61508-2, 7.8 the following minimum requirements to the modification process must be fulfilled:

- The manufacturer must install a modification process for modification of safety related products during the lifecycle phases design, commissioning, operation and maintenance to avoid unintended effects of modifications to the function safety of the product.
- Modification must be implemented at the same level (technically, organizationally) as the original development.
- Modification of the product must be documented verifiably by the manufacturer.
- The manufacturer must have implemented a procedure for field correction of known failures of the product (field safety corrective action).

4.6 Evaluation of Systematic Capability (Systematic Safety Integrity)

The evaluation of the systematic capability of the product for usage in safety related applications is based on the audit results.

The audit contains sample inspection of the requirements as defined in chapter 4.3. to 4.5 based on the provided manufacturer documentation for the valves named in chapter 2.1.

The evaluation considers the complexity and the design of the specific valves. The tailoring was done by engineering judgement of the single requirement and the relevance to functional safety of the product. Further measure for improvement of function safety of the product may be recommended.



5. Ergebnisse

Das Management der Funktionalen Sicherheit (FSM) des Herstellers wurde auditiert und erfüllt die grundlegenden und anwendbaren Anforderungen gemäß IEC 61508-1.

Die produktspezifischen Entwicklungs- und Realisierungsprozesse wurden auditiert und erfüllen die Mindestanforderungen gemäß IEC 61508-2, Route 1S. Der Hersteller hat geeignete Maßnahmen zur Vermeidung systematischer Fehler getroffen.

SIL-Produkte sind im allgemeinen Entwicklungsprozess der Fa. HORA, der im QM-System definiert ist, explizit berücksichtigt. Dieser Prozess und die dazugehörigen Arbeitsanweisungen unterliegen dem ständigen Aktualisierungsprozess des QM-Systems. Die Ergebnisse des Erstaudits sowie der Folgeaudits zur systematischen Eignung sind entsprechend diesem Prozess zu berücksichtigen und innerhalb der im Auditbericht gesetzten Fristen zu bearbeiten.

Der Hersteller der Ventile verfügt über ein geeignetes Verfahren zur Modifikation gemäß IEC 61058-2, 7.8. Der Änderungsprozess beinhaltet alle notwendigen Schritte um die Sicherheit bei Modifikationen der Ventile zu gewährleisten.

Das Ergebnis, der in diesem Bericht zusammen gefassten Untersuchungen, zeigt, dass die Ventile mit einer systematischen Eignung von

SC 3

qualitativ zum Einsatz in sicherheitstechnischen Anwendungen bis SIL 3 geeignet ist.

Die systematische Eignung ist alle fünf Jahre durch ein Re-Audit zu bestätigen.

Es ist zu beachten, dass die Bewertung der sicherheitstechnischen Eignung eines gesamten Systems auch von der systematischen Eignung der anderen Komponenten sowie von der quantitativen SIL-Bewertung abhängt.

5. Results

The functional safety management (FSM) of the manufacturer has been audited and meets the requirements acc. to IEC 61508-1.

The product specific design and realization processes have been audited and fulfill the minimum requirements according to IEC 61508-2, route 1S. The manufacturer has installed suitable measures to avoid systematic failures.

SIL-products are explicitly considered in the general design process of HORA company, defined in the QM-system. This process and the corresponding working instructions are part of the continuous process of rework of the QM-system. The results of the primary audit as well as of the follow-audits for systematic capability must be respected and handled according this process within the timeline defined in the audit report.

The manufacturer of the valves has a suitable method for modifying the turbine according to IEC 61508-2, 7.8. The modification process contains all required steps to ensure safety in case of valve modification.

The result of the analysis, summarized in this report, shows, that the valves with a systematic capability of

SC 3

is qualitative suitable to be used in safety related application up to SIL 3.

The systematic capability must be confirmed every five years by a re-audit.

It must be considered that the evaluation of the safety integrity of an overall safety system depends also on the systematic capability of the other components and on the quantitative SIL-verification.

