

Statement on Functional Safety

Category: Guidelines and approvals
Product group: All

Dear customers,

Process engineering plants in industry must be operated "safely", as they have a high risk potential for humans and the environment. The standards IEC 61508 and IEC 61511 define functional safety requirements for electrical, electronic and programmable electronic systems. These standards define four Safety Integrity Levels (SIL) 1- 4, whereat SIL 1 is the lowest level and SIL 4 is the highest level. These SIL levels consider the properties of the safety functions of an overall system (consisting of sensor, controller and actuator) and not of individual components. With this consideration the normal operation functions are irrelevant.

Suitability of HEORSE-Valves for use in safety loops acc.to IEC 61508 and IEC 61511:

- **Manually operated valves** cannot be integrated into safety-related systems and are therefore excluded within the scope of application of these standards.
- **Safety valves** are not part of normal operating processes that are tested for functional safety according to SIL. They are not part of the control-related safety loops of normal plant operation but are to be regarded as a purely mechanical final safety device.
- **The electrically or pneumatically actuated valves** are basically applicable for use in safety loops acc.to the above-mentioned standards, presupposed the externally purchased add-on parts (actuator, positioner, etc.) are suitable for use in these safety loops as well in accordance with the manufacturer's declaration.

Therefore, only selected valve types from the product group of Cryogenic Globe Valves can be used in safety loops with requirements for functional safety. Proof of their utilizability is based on a SIL capability analysis acc.to route 2H (IEC 61508-2, 7.4.4.3), a FMEDA (Failure Modes, Effects and Diagnostic Analysis) and an analysis of the Systemic Capability (SC) acc.to route 1S (IEC 61508-2, 7.4.6 f.). These analyzes were carried out in cooperation with TÜV Rheinland Industrie Service GmbH.

These valves do not yet represent a complete system in the sense of a safety loop, which consists of a sensor, controller and actuator. The add-on parts (actuator, positioner, etc.) are only individual components, which only result in a complete system with the valve, add-on parts and the user-side system technology, which forms a closed safety loop within a process engineering plant. A final evaluation of the SIL capability is therefore only possible through a user-side consideration of the safety relevant parameters (e.g. pfd-values) of all components connected in a safety loop.

Furthermore, it should be noted that the safety relevant parameters (e.g. PFDavg) specified in the HEROSE manufacturer's declaration were determined on the assumption that an annual **Diagnostic Test (Proof Test)** is carried out in order to check the safety function. It is assumed that the inspection and maintenance intervals recommended in the operating instructions are observed by the operator.

The safety relevant parameters of other components, such as drives, solenoid valves, etc., as well as descriptions of test procedures and test intervals for the safety function of the third-party components are not taken into account in the HEROSE manufacturer's declaration and the HEROSE operating instructions. The individual operating instructions, manufacturer's declaration and data sheets from the third-party manufacturers apply to these add-on parts. HEROSE makes these documents available to its customers together with the final documentation ordered.

Diagnostic test (proof test)

- The **Diagnostic Test (Proof Test)** on the HEROSE valves should be carried out as a "Full Stroke Test" and based on the test plan drawn up by the operator. This is intended to ensure that the operator regularly checks whether the fitting reliably assumes its **safe state** in the safety loop when requested.
- **Safe State:**
 - Move to the end position defined as "safe" (fully open or fully closed);
 - The maximum permissible internal and external leakage is not exceeded;
- **Test procedure:**
 1. Actuator is supplied with actuating pressure and the valve is in the normal operating situation.
 2. Triggering of the safety function via the safety loop. As a result, the actuator must vent automatically and the valve moves independently (by spring force) to the **safe state**.
 3. Check whether the end position required for a safe state is reached.
 4. Visual inspection of the valve and its mounting parts for damages, completeness and correct installation.
 5. Check for external leaks.

The test is passed if the **safe state** has been reached without any objections. In case of faults in the safety function, which can be traced back to the valve, HEROSE must be informed immediately.


HEROSE GmbH
Stephan Lütjens - QM



Erklärung zur funktionale Sicherheit

Rubrik: Richtlinien und Zulassungen
Produktgruppe: Alle

Sehr geehrte Kunden,

Verfahrenstechnische Anlagen in der Industrie müssen „sicher“ betrieben werden, da sie ein hohes Gefährdungspotenzial für Mensch und Umwelt besitzen. In den Standards IEC 61508 und IEC 61511 sind Anforderungen an die funktionale Sicherheit für elektrische, elektronische und programmierbarer elektronische Systeme hinterlegt. Diese Normen definieren vier Stufen für Sicherheits-Integritätslevel (SIL) 1- 4, wobei SIL 1 die niedrigste Stufe und SIL 4 die höchste Stufe darstellt. Diese SIL Stufen betrachten die Eigenschaften der Sicherheitsfunktionen eines Gesamtsystems (bestehend aus Sensor, Steuerung und Aktor) und nicht einer einzelnen Komponente. Bei dieser Betrachtung spielen die normalen Betriebsfunktionen keine Rolle.

Eignung von HEROSE-Armaturen für den Einsatz in Sicherheitskreisen nach IEC 61508 und IEC 61511:

- **Handbetätigte Armaturen** können nicht in sicherheitsgerichtete Systeme eingebunden werden und fallen damit nicht in den Anwendungsbereich dieser Normen.
- **Sicherheitsventile** sind kein Bestandteil normaler Betriebsprozesse, die nach SIL auf Funktionssicherheit hin überprüft werden. Sie sind kein Bestandteil der regelungstechnischen Sicherheitskreise des normalen Anlagenbetriebes, sondern sind als rein mechanisches letztes Sicherheitsorgan zu betrachten.
- **Die elektrisch oder pneumatisch angetriebenen Armaturen** sind grundsätzlich in Sicherheitskreisen gemäß den o.g. Normen einsetzbar, vorausgesetzt, die für die Sicherheitsfunktion relevanten fremd zugekauften Anbauteile (Antriebe, Stellungsregler, etc.) sind gemäß Herstellerdeklaration für den Einsatz in diesen Sicherheitskreisen geeignet.

Somit sind nur ausgewählte Armaturentypen aus der Produktgruppe der Tieftemperatur-Durchgangsventile in Sicherheitskreisen mit Anforderungen an die funktionale Sicherheit einsetzbar. Der Nachweis über deren Einsatzfähigkeit basiert auf einer SIL Fähigkeitsanalyse gemäß Route 2H (IEC 61508-2, 7.4.4.3), einer FMEDA (Failure Modes, Effects and Diagnostic Analysis) und einer Analyse der systemischen Sicherheitsintegrität (SC) gemäß Route 1S (IEC 61508-2, 7.4.6 f.). Diese Analysen wurden in Kooperation mit der TÜV Rheinland Industrie Service GmbH durchgeführt.

Diese Armaturen stellen noch kein Gesamtsystem im Sinne eines Sicherheitskreises dar, welcher aus Sensor, Steuerung und Aktor besteht. Auch die Anbauteile (Antrieb, Stellungsregler, etc.) sind nur einzelne Komponenten, welche erst in Kombination aus Armatur, Anbauteile und der anwenderseitigen Anlagentechnik ein Gesamtsystem ergeben, welches einen geschlossenen Sicherheitskreis innerhalb einer verfahrenstechnischen Anlage bildet. Eine abschließende Bewertung der SIL-Fähigkeit ist somit erst durch eine anwenderseitige Betrachtung der sicherheitstechnischen Kennwerte (z.B. PFD-Werte) aller in einem

Sicherheitskreis verbundenen Komponenten möglich. Daher beziehen sich die in der Herstellererklärung von HEROSE angegebenen sicherheitstechnischen Kennwerte nur auf die Armatur als einzelne Komponente.

Des Weiteren ist zu beachten, dass die in der Herstellererklärung von HEROSE angegebenen sicherheitstechnischen Kennwerte (z.B. PFD_{avg}) unter der Annahme ermittelt wurden, dass ein jährlicher **Diagnosetest (Proof Test)** durchgeführt wird, um die Sicherheitsfunktion zu überprüfen. Es wird vorausgesetzt, dass die in der Betriebsanleitung von HEROSE empfohlenen Prüf- und Wartungsintervalle vom Betreiber eingehalten werden.

Die sicherheitstechnischen Kennwerte weiterer Komponenten, wie z.B. Antriebe, Magnetventile etc., wie auch Beschreibungen zu Prüfverfahren und Prüfintervallen der Sicherheitsfunktion der Fremdkomponenten werden in der Herstellererklärung und der Betriebsanleitung von HEROSE nicht berücksichtigen. Für diese Anbauteile gelten im Einzelnen die Betriebsanleitungen, Herstellererklärung und Datenblätter von den Fremdherstellern. Diese Dokumente stellt HEROSE seinen Kunden, zusammen mit der bestellten Enddokumentation, zur Verfügung.

Diagnosetest (Proof Test)

- Der **Diagnosetest (Proof Test)** an den HEROSE-Armaturen soll als „Full Stroke Test“ und anhand des vom Betreiber aufgestellten Prüfplans durchgeführt werden. Hierdurch soll durch den Betreiber regelmäßig überprüft werden, ob die Armatur auf Anforderung zuverlässig ihren **sicheren Zustand** im Sicherheitskreis einnimmt.
- **Sicherer Zustand:**
 - Verfahren in die als „sicher“ definierte Endlage (vollständig geöffnet oder vollständig geschlossen);
 - Die maximal zulässige innere und äußere Leckage wird nicht überschritten;
- **Testablauf:**
 1. Antrieb ist mit Stelldruck versorgt und die Armatur befindet sich in der normalen Betriebssituation.
 2. Auslösen der Sicherheitsfunktion über den Sicherheitskreis. Als Folge muss der Antrieb automatisch entlüften und die Armatur verfährt selbstständig (durch Federkraft) in den **sicheren Zustand**.
 3. Prüfen, ob die für den sicheren Zustand geforderte Endlage erreicht wurde.
 4. Visuelle Prüfung der Armatur und deren Anbauteile auf Beschädigungen, Vollständigkeit und korrekte Montage.
 5. Prüfen, ob äußere Leckagen erkennbar sind.

Der Test ist bestanden, wenn der **sichere Zustand** ohne Beanstandungen erreicht wurde. Bei Störungen der Sicherheitsfunktion, welche auf die Armatur zurückgeführt werden, ist HEROSE umgehend zu informieren.

i.A. Stephan Lütjens
HEROSE GmbH
Stephan Lütjens - QM

