SIL – IEC 61508

D/GB 007 – 09/17

Gerätezulassung nach IEC 61508 – SIL (sicherheitsbezogene Zuverlässigkeit einer elektronischen oder elektrischen Steuerungseinrichtung)

Die von uns hergestellten Geräte basieren auf magnetisch betätigten Reed-Kontakten. Im Schaltrohr befinden sich bistabile Schutzgaskontakte. Wahlweise fest angeordnet oder als Kontaktpatrone einstellbar auf einer Lochleiste montiert. Diese Kontakte 01, 02, 03, 04 sind passive Schaltelemente, die durch den in unserem Schwimmer eingebauten Magneten geschaltet werden. Für diese Funktion wird keine Hilfsenergie oder Steuerstrom benötigt.
Für die Berechnung des SIL-Wertes muss ein ständiger Steuerstrom anliegen. Die in unseren Geräten eingebauten Reedschalter werden nicht regelmäßig betätigt. Bei unseren Niveauschaltern mit diesem Kontaktsystem ist der Kontakt entweder geschlossen oder geöffnet. Dies ist von der Füllstandshöhe abhängig. Dadurch fließt kein permanenter Steuerstrom. Für eine analytische Berechnung des Lebenszyklus ist er jedoch Vorrausetzung.
Durch die unterschiedlichen Anwendungsfälle kann über die Anzahl der Schaltvorgänge keine Aussage gemacht werden. Auf Grund dieser technischen Eigenschaft kann keine SIL-Berechnung durchgeführt werden. Dies gilt für alle Geräte mit Reed-Kontakten.

Technische Merkmale betreffend der Funktionalen Sicherheit:

Schalter mit Reed Kontakt:

Version: 01 / 02 / 03 / 04 / NRA-W

Die Lebensdauer der Niveaukontakte beträgt bei maximaler Belastung 10^5…10^6 Schaltspiele. Die mechanische Lebensdauererwartung beträgt mindestens 10^9 Schaltspiele.

Beim Schalten von Induktiven Lasten ohne Schutzbeschaltung kann sich die Lebensdauer infolge Überschreitens der zulässigen Einschaltströme oder Schaltspannungen reduzieren.

Diese Schalter werden seit über 30 Jahren in verschiedensten Geräten mit höchster Zuverlässigkeit eingesetzt.

Approval for instruments according to IEC 61508 – SIL (Safety Integrity Level)

Our manufactured instruments are based on the magnetic activated reed-contacts. The switching tube contains bistable protective gas contacts. These may be fixed or alternatively mounted as an adjustable contact cartridge on a perforated strip. These contacts 01, 02, 03, 04 are passive switching elements which switch with our float that contains a magnet. These components don't need any emergency current or electric power supply for their function.
The contact in our level regulators which are equipped with these contact system is either normally closed or normally open. This is depended from the filling level. Thereby there is no continuous current.
For the calculation of the SIL data, the permanent electric power supply must basically be guaranteed, otherwise the life time cycle can annalistically not be calculated. Based on this technical character a SIL calculation can not be executed, this counts on all reed-contact based instruments.

Technical features concerning functional safety:

Switch with reed contact:

Version: 01 / 02 / 03 / 04 / NRA-W

The life span of the level contacts amounts by maximum charging 10^5…10^6 switching charges. The mechanical life span amounts at least 10^9 switching charges.

The switching of the inductive loads without the suppressor can reduce the life span due to the overrun of the permissible currents inrush or the switching voltages.

The switches are in use with the highest reliability in various devices for more than 30 years.

GOLDAMMER
REGELUNGSTECHNIK GMBH

Schöllersheider Str. 15 TELEFON 02104/12093
D-40822 METTMANN TELEFAX 02104/12028
POSTFACH 10 02 17 info@goldammer-regelungstechnik.com
D-40802 METTMANN goldammer-regelungstechnik.com

SIL – IEC 61508 (Safety Integrity Level)

In Kürze

Die SIL-Norm dient der Beurteilung elektrischer-/elektronischer-/programmierbarer elektronischer Systeme in Bezug auf die Zuverlässigkeit von Sicherheitsfunktionen und wird nach 4 Sicherheitsleveln definiert. Die Sicherheitsanforderungsstufen stellen ein Mass für die Zuverlässigkeit des Systems in Abhängigkeit von der Gefährdung dar. Die Betreiber von Anlagen mit sicherheitsrelevanten Funktionen legen im Rahmen einer Gefährdungsbeurteilung den Sicherheits-Integritätslevel für die jeweilige Sicherheitsfunktion fest. Bis zum Level 2 kann dies der Hersteller in eigener Verantwortung vornehmen. Ab Level 3 wird dies durch einen unabhängigen Dritten durchgeführt.

Was ist SIL?

Die Sicherheitsanforderungsstufe ist ein Begriff aus dem Gebiet der Funktionalen Sicherheit und wird in der Internationalen Normung gemäß IEC 61508 auch als **Sicherheits-Integritätslevel (SIL)** bezeichnet. Er dient der Beurteilung elektrischer-/elektronischer-/programmierbarer elektronischer Systeme in Bezug auf die Zuverlässigkeit von Sicherheitsfunktionen.

In der nationalen Sicherheitsnorm DIN EN-61508, entstanden aus der internationalen Norm IEC 61508, wird der Sicherheits-Integritätslevel wie folgt definiert:

Vier Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität von Sicherheitsfunktionen, die dem Sicherheitsbezogenen System zugeordnet werden, wobei der „Sicherheits- Integritätslevel 4“ die höchste Stufe der Sicherheitsintegrität und der „Sicherheits-Integritätslevel 1“ die niedrigste darstellt.

Bei Systemen die keinerlei Sicherheitsanforderungen genügen müssen, hat sich die Bezeichnung „Sicherheits-Integritätslevel 0“ eingebürgert.

Sicherheitsfunktionen dienen in der Industrie dem Schutz der Gesundheit der dort Beschäftigten, der Umwelt und von Gütern. Diese Sicherheitsfunktionen werden durch einen Regelkreis, der aus Sensoren, Steuerungskomponenten und Aktoren besteht, realisiert. Die Sicherheitsanforderungsstufe stellt ein Mass für die Zuverlässigkeit des Systems in Abhängigkeit von der Gefährdung dar. Prozesse mit einer geringeren Gefährdung werden durch einen Sicherheitskreis mit geringerem Level aufgebaut als Prozesse mit höherer Gefährdung, bei denen z.B. Menschen getötet werden können. Typische Sicherheitsfunktionen sind Notausschaltungen, Abschalten überhitzter Geräte oder auch die Überwachung gefährlicher Bewegungen.

Eine Risikoabschätzung lässt sich anhand eines Risikographen durchführen. Hier werden mehrdimensional Faktoren betrachtet, die die Höhe des zu erwartenden Risikos einer Anlage beeinflussen können. Diese sind:

- **Schadensausmaß**

  S1: leichte Verletzung einer Person, kleinere schädliche Umwelteinflüsse

  S2: schwere irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person, vorübergehende grössere schädliche Umwelteinflüsse

  S3: Tod mehrerer Personen, lange andauernde grössere schädliche Umwelteinflüsse

  S4: katastrophale Auswirkungen – sehr viele Tote (Seveso, Tschernobyl, Bhopal) GAU

- **Aufenthaltsdauer von Personen im Gefahrenbereich**

  A1: selten bis öfter A2: häufig

  bis dauernd

- **Möglichkeit der Gefahrenabwendung**

  G1: möglich unter bestimmten Bedingungen

  G2: kaum möglich

Die Betreiber von Anlagen mit sicherheitsrelevanten Funktionen legen im Rahmen einer Gefährdungsbeurteilung den Sicherheits-Integritätslevel für die jeweilige Sicherheitsfunktion fest. Entsprechend dieser Festlegung werden die dafür geeigneten Geräte ausgewählt und zu einem System zusammengeführt.
Die Gerätehersteller beurteilen innerhalb eines Assessments ihre Geräte entsprechend der Normen. Bis zum Level 2 kann dies der Hersteller in eigener Verantwortung vornehmen. Ab Level 3 wird dies durch einen unabhängigen Dritten durchgeführt, der nach erfolgreicher Zertifizierung ein entsprechendes Zertifikat ausstellt.

Für die Festlegung der Stufe der Sicherheitsintegrität ist zum einen eine Betrachtung des Ausfallverhaltens der betrachteten Baugruppe notwendig. Weiterhin wird in dem Assessment genau beurteilt ob redundante Strukturen vorliegen, wie das Verhältnis zwischen sicheren Fehlern und unsicheren Fehlern ist und ob die Sicherheitsfunktion kontinuierlich oder auf Anforderung zu betrachten ist. Aus diesen Angaben werden dann die Ausfallraten bestimmt. Diese Kennwerte dienen einer Beurteilung des Sicherheitsintegritäts-Levels entsprechend der Vorgaben

der Norm.
Die Betrachtung der Kennzahlen ist aber für die Einstufung der Geräte nicht hinreichend. Es ist noch eine Betrachtung des Lebensdauerprozesses des Gerätes notwendig. Hierbei werden z.B. die Sicherheitsgerichtete Konstruktion und ähnliche Bereiche betrachtet. Das Normenwerk gibt hier gesonderte Massnahmen für die einzelnen Stufen der funktionalen Sicherheit an. Eine besondere Bedeutung hat dieser Bestandteil bei der Betrachtung von Betriebsmitteln mit komplexen Baugruppen, dies sind z.B. Mikroprozessoren, die über ein internes Programm verfügen. Hier werden in den Normen separate Massnahmen dargelegt um auch auf Programmierfehler reagieren zu können. Ein spezielles Problem stellen hier z.B. Fehler dar, die nicht durch eigene Entwicklungstätigkeiten entstehen, sondern schon in Softwarewerkzeugen wie Compilern und ähnlichem enthalten sind. Erst die Betrachtung aller Punkte lässt eine Einschätzung zu, ob sich das Betriebsmittel in einem Sicherheitskreis der entsprechenden Sicherheitsanforderungsstufe einsetzen lässt.

Eine Klassifizierung der einzelnen Baugruppen entsprechend dem Sicherheits-Integritätslevel ist nicht sinnvoll, da sich die Normenforderungen auf die Sicherheitskreise beziehen. Dies bedeutet, dass die Festlegung der Stufe erst für die bekannte Zusammenschaltung der verschiedenen Betriebsmittel wie Sensoren, Aktoren, Steuerungskomponenten etc. getroffen werden kann.

Zu beachten gilt es, dass eine SIL - Einstufung nicht vor einer gewissenhaften Einstufung nach anderen Normen oder den EMV-Vorschriften entbindet.

SIL – IEC 61508 (**S**afety **I**ntegrity **L**evel) D/GB – 007- 09/17

In brief

The SIL standard is used to evaluate electrical / electronic / programmable electronic systems in reference to reliability of safety functions and is defined according to 4 safety levels. The safety requirement levels represent a measurement for the reliability of the system depending on the risks. Operators of systems with safety-relevant features define the safety integrity level for each safety function within the scope of a risk assessment. This can be performed by the manufacturer at his responsibility up to level 2. From Level , this will be performed by an independent party.

What is SIL?

The safety requirement level is a term from the field of functional safety and is known in international standards in accordance with IEC 61508 as **Safety Integrity Level (SIL)**. It is used to evaluate electrical / electronic / programmable electronic systems in terms of the reliability of safety functions.

In national safety standard EN-61508, derived from the international standard IEC 61508, the safety integrity level is defined as follows:

Four levels to specify the requirements for the safety integrity of safety functions that are allocated to the safety-related system, whereby "Safety Integrity Level 4" represents the highest level of safety integrity and “Safety Integrity Level 1“ the lowest.

The term "safety integrity level 0" has become accepted for systems which do not meet any safety requirements.

Safety functions are used in industry to protect the health of the employees, the environment and goods. These safety functions are implemented by a control loop, consisting of sensors, control components and actuators. The safety requirement level represents a measurement for the reliability of the system based on the risk. Processes with a lower risk are set up by a safety circuit with a lower level than processes with higher risks, in which people can be killed. Typical safety functions are emergency stops, switching off overheated equipment or monitoring dangerous movements.

A risk assessment can be performed based on a risk graph. Multidimensional factors that may affect the magnitude of the expected risk of a system are observed here. These are:

- **Extent of damage**

  S1: slight personal injuries, minor adverse environmental impacts

  S2: severe irreversible injuries to one or more persons or death of a person, temporarily greater adverse environmental effects

  S3: Death of several persons, long-term major adverse environmental impacts

  S4: catastrophic consequences - very many deaths (Seveso, Chernobyl, Bhopal) MCA

- **Length of stay of persons in the danger zone**

  A1: Seldom to often

  A2: Frequently to continuous

- **Possibility of risk aversion**

  G1: possible under certain conditions

  G2: hardly possible

Operators of systems with safety-relevant features define the safety integrity level for each safety function within the scope of a risk assessment. According to this definition, suitable devices are selected and integrated into one system.

The equipment manufacturers evaluate their equipment within an assessment according to standards. This can be performed by the manufacturer at his responsibility up to level 2. From Level 3, this will be performed by an independent third party, who issues a certificate after a successful certification.

An observation of the failure behavior of the observed assembly is required to determine the level of the safety integrity on one hand. Furthermore, a precise evaluation is made in the assessment whether redundant structures are present, how the relationship between safe and unsafe defects and errors is, and if the safety function must be considered as continuous or on demand. The failure rates are then determined from this information. These characteristic values are used for an assessment of safety integrity level according to the requirements of the standard.

The observation of the characteristic values is not sufficient for the classification of the devices. Another observation of the service life process of the equipment is still needed. For example, the safety-oriented design and related areas are observed here. The standards here provide separate measures for each level of the functional safety.

This element has special significance in the observation of equipment with complex assemblies; these are, for example, microprocessors, which have an internal program.
Separate measures are presented here in the standards for also responding to programming errors. Errors that are not caused by own development activities, but are already included in software tools, such as compilers and the like, represent a specific problem. Only the observation of all points allows an assessment of whether the equipment can be used in a safety circuit of the related safety level.

A classification of the individual modules corresponding with the safety integrity level is not useful, since the standard requirements relate to the safety circuits. This means that the level can only be defined for the well-known interconnection of various equipment such as sensors, actuators, control components, etc..

It is important to note that a SIL - classification does not exempt a conscientious classification according to other standards or EMC-regulations.