SIL (**S**afety **I**ntegrity **L**evel)

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/IEC 61511 auch als **Sicherheits-Integritätslevel (SIL)** bezeichnet. Er dient der Beurteilung elektrischer-/elektronischer-/programmierbarer elektronischer (E/E/PE) 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 E/E/PE-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 (SSPS) 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.