TeLo

TECHNICAL SAFETY CONSULTING

10 häufige Fehler im Bereich der Funktionalen Sicherheit

TeLo GmbH
office@telo.at
+43 (0) 3113 / 5115–0
Gersdorf an der Feistritz 158
A-8213 Gersdorf an der Feistritz
www.telo.at

INHALT

EINLEITUNG

Die Funktionale Sicherheit (weiters auch „FuSi“) gewinnt im modernen Maschinenbau und speziell in der Industrie 4.0 immer mehr an Bedeutung. Sie ermöglicht es die Maschine und Bediener auf engem Raum sicher zusammenarbeiten zu lassen. Richtig ausgelegt kann gleichzeitig die Sicherheit der Maschine erhöht werden, ohne dass der Produktionsprozess gestört wird. Doch was versteht man nun konkret unter FuSi? Grundsätzlich ist die Funktionale Sicherheit ein Teil der Gesamtsicherheit eines Systems und hat stets das Ziel vor Schäden zu schützen. Dabei ist es irrelevant, ob es um Schäden an Menschen, Umwelt, der Maschine o.ä. geht. Zum Schutz dieser werden Sicherheitsfunktionen eingeführt. Unter einer Sicherheitsfunktion versteht man eine Funktion, die implementiert wird, um einen sicheren Zustand zu erreichen bzw. aufrecht zu erhalten. Mit Hilfe dieses eBooks möchten wir Ihnen 10 häufig gemachte Fehler im Zusammenhang mit der Funktionalen Sicherheit aufzeigen, damit Sie diese in Zukunft vermeiden können. Für eine ausführlichere Beratung bzw. Unterstützung stehen wir natürlich jederzeit sehr gerne zur Verfügung!

1. FALSCHE AUSLEGUNG DER SICHERHEITSFUNKTION

Einer der häufigsten Fehler passiert bereits im Zuge der Risikobeurteilung. Im Rahmen der Risikobeurteilung werden die Sicherheitsfunktionen entsprechend der identifizierten Gefährdung definiert. Die Risikobeurteilung setzt sich grundsätzlich aus der Risikoanalyse und -einschätzung zusammen. Bei der Risikoanalyse werden die Gefahren identifiziert, wohingegen bei der Risikoeinschätzung die Wahrscheinlichkeit des Eintretens sowie das Ausmaß der Gefahr behandelt werden. Der hier gemachte Fehler ist es den falschen Sicherheitslevel für die Sicherheitsfunktion festzulegen. Zum

einen kann dies aus kostentechnischen Gründen sein, da ein mehrkanaliges redundantes System wesentlich teurer ist als ein einkanaliges System. Zum anderen kann dies schlicht auf einer falschen Bewertung der Situation beruhen. Der iterative Prozess der Risikominimierung sollte spätestens bei der Validierung aufzeigen, falls das Risiko und das Sicherheitslevel falsch definiert wurden. Zur Festlegung des Sicherheitslevels kann zum einen der SIL (Safety Integrity Level) nach EN IEC 62061 oder EN 61508 und zum anderen der PL (Performance Level) entsprechend der EN ISO 13849-1/-2 herangezogen werden. Sowohl beim SIL als auch beim PL werden Sicherheitsfunktionen nach ihrer Integrität in diskrete Level unterteilt. Beim SIL von 1-4 beim PL von a-e. Zu berücksichtigen ist hier, dass diese nicht gleich gesetzt werden können! Das heißt SIL 3 entspricht nicht zwangsläufig PL d. Deshalb ist es wichtig die jeweilige Sicherheitsfunktion mit der dazugehörigen Risikoeinschätzung (z.B.: Risikograph, LOPA, ...) zu ermitteln.

2. AUSWAHL DER FALSCHEN NORM

Sich im Normendschungel zurecht zu finden ist nicht immer einfach. Speziell im Bereich der Funktionalen Sicherheit gibt es mehrere Normen, wie zum Beispiel die EN 61508, EN 61511, EN ISO 13849 oder die EN IEC 62061, zur Auswahl. Um hier die richtige Norm zu finden ist es wichtig, den Anwendungsbereich seines Produktes genau abzustecken. Ist dieser definiert, kann nun anhand des Anwendungsbereiches das passende Regulativ zum Produkt ausgewählt werden. Speziell für Hersteller von Maschinen ist die EN ISO 13849 von großer Bedeutung. Diese umfasst, anders als die EN 61508, EN IEC 62061 oder EN 61511, nicht nur elektrische, elektronische und elektronisch programmierbare Komponenten, sondern auch die hydraulischen, pneumatischen und mechanischen Komponenten einer Sicherheitsfunktion. Daher ist die EN ISO 13849 die Grundnorm für den Maschinenbau. Wie ist nun bei der Normenrecherche konkret vorzugehen? Einen

guten Anfang stellt hier unsere Linksammlung unter https://www.telo.at/de/links dar. Dort finden Sie einen guten Überblick über alle relevanten Seiten zur Normenrecherche. Ob es nun die Seite von Austrian Standards bzw. dem Beuth-Verlag für österreichische bzw. deutsche Normen sind, oder die CEN/CENELEC Seite für europäische Normen bzw. die ISO/IEC Seite für die internationalen Normen - hier werden Sie fündig.

3. VERIFIZIEREN ABER NICHT VALIDIEREN

In allen Normen der Funktionalen Sicherheit müssen die verbauten Komponenten verifiziert werden. Unter einer Komponente versteht man grundsätzlich einen Bestandteil einer größeren Einheit. Verifikation ist der Nachweis, dass ein vermuteter oder behaupteter Sachverhalt wahr ist. Die Frage, die mittels der Verifikation beantwortet werden soll, lautet „Wurde das System richtig gebaut?“. Im Bereich der Funktionalen Sicherheit bedeutet das, dass der Nachweis beweist, dass das geforderte Sicherheitslevel aus der Risikobeurteilung erreicht wurde. Meist wird der geforderte Nachweis mittels Berechnung erbracht. Dies ist aber nur eine Seite der Medaille. Denn so wie die Verifikation in den Normen gefordert wird, so wird auch eine Validierung gefordert. Im Zuge der Validierung soll bewiesen werden, dass das System den vorgegeben Spezifikationen aus der Risikobeurteilung und Anforderungen aus den Normen erfüllt. Damit kann die Frage „Wurde das richtige System gebaut?“ beantwortet werden.

4. UNVOLLSTÄNDIGE VALIDIERUNGSUNTERLAGEN

Wird eine Validierung der Sicherheitsfunktionen durchgeführt, so wird im Zuge dessen häufig nur ein Funktionstest durchgeführt. In den Normen wird unter Validierung aber wesentlich mehr verstanden und auch gefordert. So reicht es nicht lediglich einen Funktionstest durchzuführen, sondern es muss auch die technische Dokumentation, die

Benutzerinformation und die Informationen für die Wartung oder Instandhaltung einer Sicherheitsfunktion und vieles mehr geprüft und validiert werden. Dies kann einen enormen Aufwand bedeuten, da alle Datenblätter und Benutzerhandbücher der Hersteller auf spezielle Hinweise durchsucht werden müssen. Es handelt sich dabei jedoch um eine Vorgabe, welche nicht vernachlässigt werden darf und eingehalten werden muss, um die Einhaltung der herangezogenen Norm bestätigen zu können.

5. NICHTBEACHTUNG DER UMGEBUNGS-BEDINGUNGEN

Ein weiterer häufiger Fehler der Funktionalen Sicherheit ist die Missachtung der speziellen Umgebungsbedingungen. Viele Bauteile, welche in einer Sicherheitsfunktion verbaut wurden, haben einen eingeschränkten Einsatzbereich. Daher ist es unerlässlich alle Bauteile, welche eine Sicherheitsfunktion erfüllen, auf Einschränkungen hinsichtlich den Umgebungsbedingungen zu prüfen. Zum Beispiel sind optische Sensoren in einer sehr staubigen oder schmutzigen Umgebung schlechter geeignet als Radarsensoren. Es ist demnach unabdingbar die Umgebung der Sicherheitsfunktion genau zu analysieren und anschließend die entsprechenden Bauteile auf ihre besonderen Eigenschaften und Einschränkungen zu kontrollieren, um diesen Fehler zu vermeiden.

6. MISSACHTEN VON HERSTELLERVORGABEN

Herstellervorgaben müssen, besonders bei Sicherheitsfunktionen, immer beachtet werden. Da die Betriebsanleitungen von Sicherheitsbauteilen meist sehr umfangreich sind, müssen die wichtigsten Informationen in aufwändiger Recherche der Anleitung herausgefiltert werden. Dabei sind meist spezielle Hinweise, wie zum Beispiel wiederkehrende Überprüfung der Bauteile, sehr versteckt und leicht zu übersehen. Viele

Hersteller verwenden auch mehrere Dokumente für ein Bauteil, sodass es für den Anwender durchaus schwierig werden kann, die für ihn relevanten Informationen zu finden. Nichtsdestotrotz ist auch dieser Schritt essentiell, um über alle Eigenschaften der Sicherheitsbauteile informiert zu sein und diese richtig einsetzen zu können.

7. FALSCHE MONTAGE VON SICHERHEITSBAUTEILEN

Die Hersteller von Sicherheitsbauteilen geben oft eine Montageart oder -richtung vor. Diese muss unbedingt beachtet werden, da sonst die Funktion der (Sicherheits-)Bauteile vom Hersteller nicht gewährleistet werden kann. Bei Druckschaltern oder Durchflussmessern zum Beispiel spielt die Montagerichtung eine besonders große Rolle. Ist der Druckschalter falsch montiert, kann es sehr leicht zu Fehlfunktionen des Schalters kommen. Bei Durchflussmessern hingegen muss besonders auf eine Beruhigungsstrecke geachtet werden. Das heißt der Durchflussmesser sollte nicht unmittelbar nach einem Rohrleitungsbogen installiert werden. Es kann aber auch versteckte Montagehinweise in der Dokumentation der Hersteller geben. So kann es vorkommen, dass Schütze nur senkrecht und mit mind. 6 mm Abstand zu den geerdeten Elementen verbaut werden dürfen. Auch hier ist eine gewissenhafte und sorgfältige Recherche hinsichtlich der Eigenheiten der Sicherheitsbauteile wichtig.

8. NICHT DURCHGÄNGIGE ZWEIKANALIGKEIT

Oft kommt es bei redundanten Sicherheitsfunktionen zu einem schwerwiegenden Fehler. Während die Sensorseite bis hin zur Logikgruppe in redundanter Bauweise geplant und gebaut wird, wird die Aktorseite meist nur einkanalig behandelt. Unter Redundanz versteht man die Existenz von mehr als einem Mittel zur Ausführung einer

erforderlichen Funktion - dies beschreibt z.B. die Zweikanaligkeit. Als Beispiel kann genannt werden, dass eine zweikanaliger Sensor an ein entsprechendes Auswertegerät angeschlossen wird, welches in sich zweikanalig ist, und der zugehörige Motor nur über ein Hauptschütz abgeschaltet wird. Durch diesen Fehler wird der Sicherheitslevel der Sicherheitsfunktion drastisch verringert, da aus dem zweikanaligen System ein einkanaliges System wird bei dem ein einzelner Fehler (z.B. Nichtöffnen der Schützkontakte) zum Ausfall führt.

9. FEHLENDE ÜBERPRÜFUNG DER SICHERHEITS-FUNKTIONEN IM FEHLERFALL

Bei zwei- oder mehrkanaligen Systemen wird zwar häufig die Sicherheitsfunktion mittels Funktionstest getestet, allerdings nicht die Reaktion bzw. das Verhalten im Fehlerfall. Da bei einem Ausfall eines Kanals die Funktionstüchtigkeit einer Sicherheitsfunktion nicht verloren gehen darf, ist es wichtig bei der Validierung der Sicherheitstechnik die Funktionen auch im Fehlerfall (z.B.: Querschluss oder Drahtbruch) zu überprüfen. Damit kann sichergestellt werden, dass die Sicherheitsfunktion auch im Fehlerfall ordnungsgemäß funktioniert. Die Fehlerfälle können durch eine geeignete FMEA (Failure Mode and Effects Analysis) identifiziert und dokumentiert werden. Die FMEA ist eine Analyse, die potenzielle Fehlerquellen aufzeigen und bewerten soll, um in weiterer Folge daraus geeignete Präventionsmaßnahmen abzuleiten und darzulegen, ob Fehler auch rechtzeitig erkannt werden können. Weitere (detailliertere, bzw. vertiefendere) Möglichkeiten stellen hier die FMECA (Failure Mode and Effects and Criticality Analysis) sowie die FMEDA (Failure Mode and Effects and Diagnostic Analysis) dar.

10. BESTEHENDE ANSÄTZE NICHT HINTERFRAGEN

Oft werden in Unternehmen Sicherfunktionen, welche schon mehrfach verwendet wurden, nicht mehr auf Tauglichkeit evaluiert - streng nach dem Motto „Das haben wir immer schon so gemacht“. Dadurch kann es zu gravierenden Folgefehlern kommen. Auch werden häufig bestehende Sicherheitsfunktionen für einen anderen Anwendungsfall verwendet, für den sie weder konzipiert noch geeignet sind! Gerade im Bereich der Sicherheitstechnik sollten die verschiedenen Lösungsansätze immer revalidiert und evaluiert werden um den Stand der Technik zu gewährleisten.

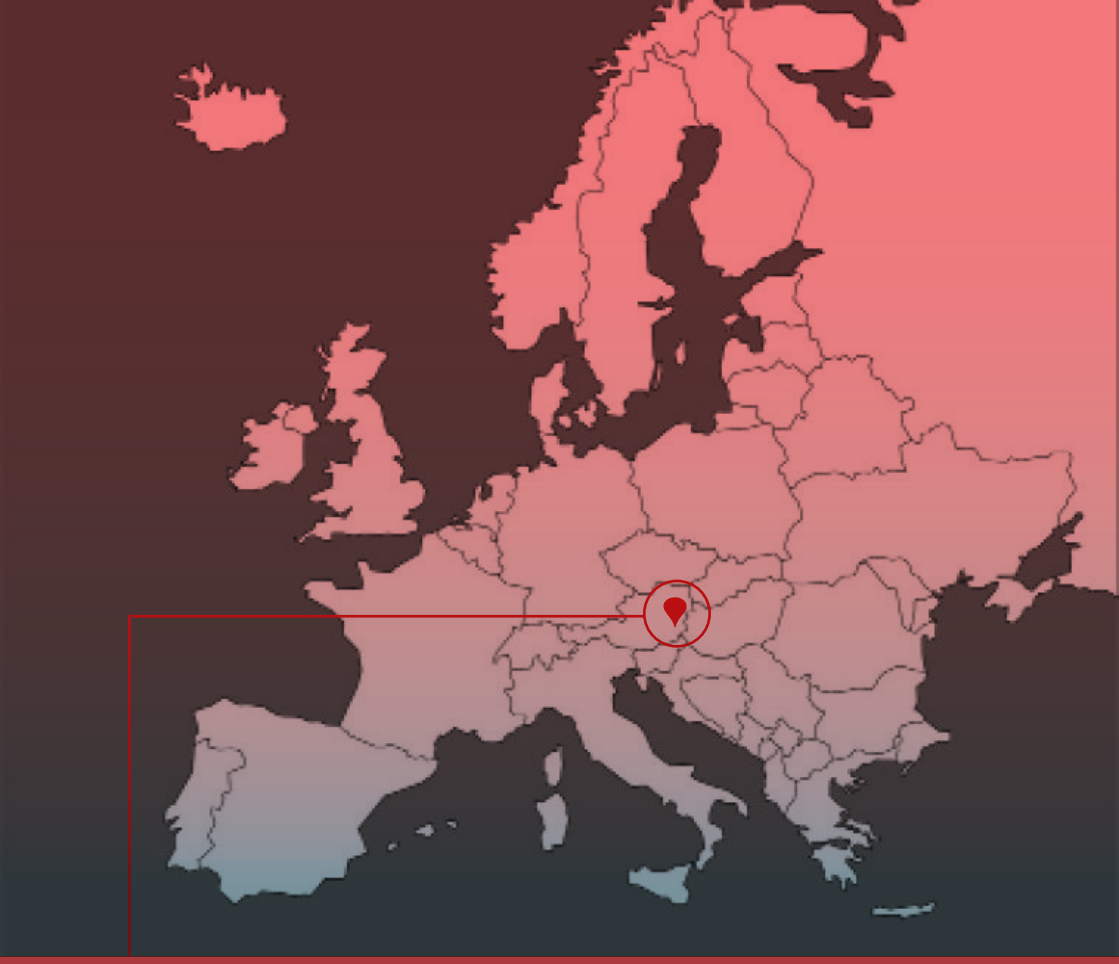
GEMEINSAM ANS ZIEL

Sie benötigen Unterstützung und Beratung bei Fragen im Bereich der Funktionalen Sicherheit? Dann nützen Sie unsere langjährige Erfahrung. Wir sind der richtige Ansprechpartner und helfen Ihnen darüber hinaus bei der Verwirklichung kostengünstiger Lösungen.

Neben der persönlichen Beratung bieten wir auch Schulungen zum Thema Funktionale Sicherheit an. Hier ist es uns besonders wichtig Schulungen mit vielen Praxisbeispielen zu gestalten und auf Ihre ganz individuellen Wünsche und Fragen einzugehen. Unsere Schulungen und Workshops werden von verschiedensten FachexpertInnen sowie hochkarätigen GastlektorInnen gehalten. Selbstverständlich ist es auch möglich das Training speziell auf Ihre Bedürfnisse in Ihrem Unternehmen anzupassen. Melden Sie sich einfach unter anmeldung@telo.at und wir stellen eine individuelle Lösung für Sie bereit - egal ob virtuell oder bei Ihnen vor Ort! Gerne kombinieren wir hierzu auch angebotene Schulungen.

Unsere Schulungen im Bereich der Funktionalen Sicherheit:

- Einführung in die Funktionale Sicherheit
- Funktionale Sicherheit von Maschinen und Anlagen
- FMEA | Failure Mode and Effects Analysis



Kontaktieren Sie uns!

Wir haben ein offenes Ohr für all Ihre Anliegen.
Unsere Flexibilität und Kompetenzen machen uns zu
einem starken Partner für Ihre Projekte!

TeLo GmbH
office@telo.at
+43 (0) 3113 / 5115–0
Gersdorf an der Feistritz 158
A-8213 Gersdorf an der Feistritz