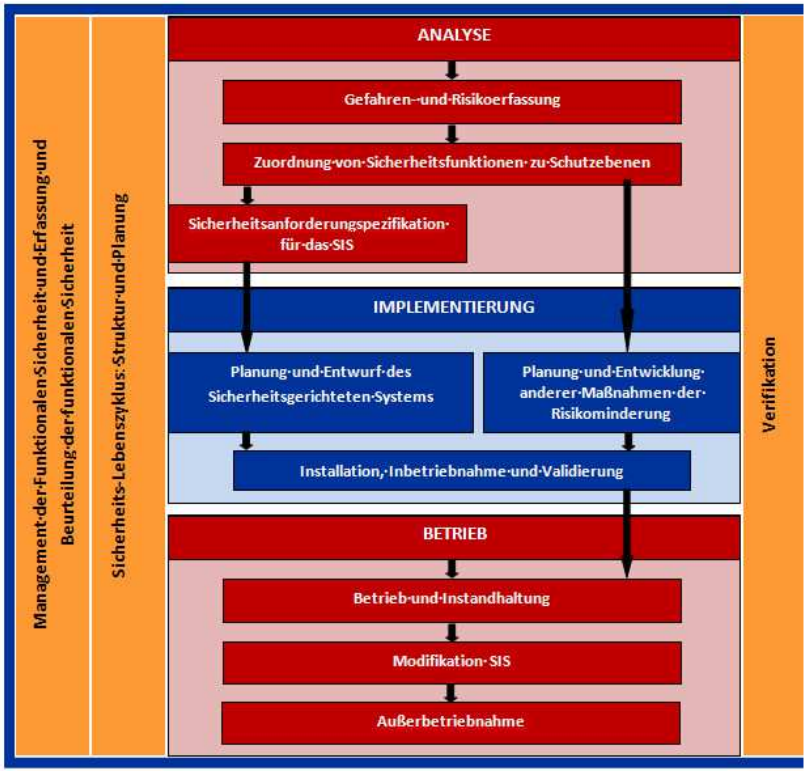
Was Betreiber zur Erfüllung der IEC61511 bedenken müssen

Hintergrund

Ist als Engineering-Prozess definiert, der alle notwendigen Schritte zur Erreichung von Funktionaler Sicherheit beinhaltet.
Enthält alle **notwendigen Aktivitäten** für die Implementierung von sicherheitsgerichteten Systemen, angefangen mit der Konzeptphase des Projekts über die Implementierung bis hin zur Außerbetriebsetzung des sicherheitsgerichteten Systems.
Die Erfüllung der IEC61511 erfordert zudem eine **Organisation beim Betreiber**, um den Lebenszyklusprozess in jeder Ebene einzuführen.



IEC61511 nennt 12 Kernaktivitäten bezogen auf das Management des Sicherheitslebenszyklus (siehe Diagramm). Vereinfacht lässt sich der Ablauf in drei Hauptphasen gruppieren: **Analyse, Implementierung und Betrieb**. Die Managementaktivitäten sind durchgehend in jeder Phase anzuwenden.

Dieses Dokument fasst die wichtigen Aspekte für ALLE SIS-Beteiligten zusammen und nennt spezifische Anforderungen für jede Lebenszyklusphase. Es ist keine vollständige Liste, soll aber als Leitfaden für den Nachweis zur Erreichung der Funktionalen Sicherheit dienen.

Management der Funktionalen Sicherheit

Was auch immer IEC61511 verlangt: ein Plan, eine Prozedur und ein dokumentierter Nachweis, dass beide Dokumente beachtet wurden, müssen sein!
Was auch das Thema ist:“ Wie kann ich sicher sein?“ und „Wie kann ich das beweisen?“

Kompetenz

Jeder Einzelne im SIS Lebenszyklus muss kompetent sein, die Arbeit ausführen. Kompetent sein in einer Sache bedeutet nicht kompetent zu sein in einer anderen. Kompetenz ist Teil des Zertifizierungssystems, in dem die Rollen und Aufgaben definiert sind und der Status aller kompetenten Personen kontinuierlich nachverfolgt wird.

Planung für Funktionale Sicherheit

Die Planung für die Ausführung einer Aktivität muss dokumentiert werden und muß folgende Punkte berücksichtigen: Arbeitsvorgaben, Ressourcen, Werkzeuge, Autorisation, Freigabe, Arbeitsergebnisse. Ohne Berücksichtigung dieser Punkte ist es unmöglich nachzuweisen, ob das Ergebnis der Erwartung entspricht.

Lieferantenbewertung

Alle Anforderungen an das Management der Funktionalen Sicherheit gelten ebenso für Endkunden / Betreiber wie auch für alle am SIS beteiligten Produkt- / Dienstleistungslieferanten. Es sollen nur bewertete Lieferanten berücksichtigt werden, deren Kompetenz in Organisation und Personal nachgewiesen ist.

Verifikation

Verifikation ist der Nachweis, dass eine Aktivität das erwartete Ergebnis erbracht hat. Verifikation erfordert einen Verifikationsplan mit den vordefinierten Akzeptanzkriterien.

Überprüfung der Funktionalen Sicherheit

Überprüfung der Funktionalen Sicherheit bedeutet eine vorgeschriebene Bewertung durch (eine) unabhängige Person(en) zur Überprüfung, ob die Funktionale Sicherheit und die Sicherheitsintegrität erreicht sind.

Audits

Audits müssen geplant und deren Ergebnis nachverfolgt werden. Audits sind der Beweis zur Einhaltung der IEC61511.

EMERSON.
Process Management

Die Phasen des Lebenszyklus

Analyse

Gefahren- und Risikoabschätzung

Der bekannte HAZOP-Prozess und die daraus folgenden Aktionen müssen in eine Prozedur überführt und überprüft werden inkl. aller Revisionen.

SIL Bestimmung

Das Risiko einer Gefährdung ist zu quantifizieren, um die Sicherheitsfunktion (SIF) und den geforderten SIL zu bestimmen. Risikograph und LOPA sind zwei halb-quantitative Verfahren. Beide benötigen ein klares Verständnis der Eintrittswahrscheinlichkeit und der Konsequenzen. Ebenso muß der Risikograph aus dem Standard vor seiner Verwendung kalibriert werden.

Sicherheitsanforderungsspezifikation (engl. SRS)

Einige Unternehmen verwenden für die Prozesssicherheitsanforderungen Beschreibungen und verlassen sich dabei auf die ingenieurmäßige Interpretation. Eine klare SRS ist erforderlich und hilft bei dem Verständnis der Designmerkmale und deren Wichtigkeit.

Implementation

Auswahl der Ausrüstung, SIF Design, Konfiguration der Hardware und Software

Das sind die Detailspezifikationen. Die Eignung der Komponenten ist nachzuweisen. Es ist sicherzustellen, dass die Konfiguration den kontrollierten und verifizierten Prozeduren folgt. Die Produktzertifizierung und die Organisation des Lieferanten unterstützen in großem Maße bei dem Nachweis der Einhaltung.

Validierung

Validierung und Verifikation haben verschiedene, spezifische Bedeutungen in der IEC61511. Ein SIS sollte nicht in Betrieb gehen, ohne dass eine formale Validierung die Überstimmung mit allen Anforderungen der SRS nachweist.

Selbsteinschätzung der IEC61511-Erfüllung

Hat jeder eine klar definierte Rolle?
Sind alle meine HAZOP Aktionen komplett?
Entspricht meine SRS den aktuellen Anforderungen?
Bin ich kompetent für die für mich vorgesehene Tätigkeit?
Existiert ein Nachweis der SIS Validierung gegenüber der SRS?
Sind meine Inspektionen detailliert und dokumentiert?
Erreichen meine Prüftests den geforderten Deckungsgrad?
Kann ich alle Änderungen bis zum Originaldokument nachverfolgen?
Wann ist die nächste Überprüfung der Funktionalen Sicherheit?

Antwort „Nein“ bei einer Frage? Emerson kann helfen!

Betrieb

Konfigurationsmanagement

Eine Definition im IEC61511 Standard, bedeutet die Kontrolle von jeglicher Ausrüstung mit Einfluss auf die Funktionale Sicherheit einschließlich der unabhängigen Schutzebenen. Die (Ausrüstungs-) Liste inkl. der Hardware/Software Versionen darf sich nur durch kontrollierte und autorisierte Prozeduren ändern.

Prüftest und Inspektion

Zum Auffinden verborgener Fehler oder externer Effekte an der Installation muß jedes Gerät in vorgeschriebenen Intervallen inspiziert und getestet werden. Diese Aktivität erfordert eine gerätespezifische Planung und Dokumentation zur Sicherstellung einer konsistenten Implementierung und Aktenlage.

Leistungsanalyse

Für die Vorhersage der Sicherheitseigenschaften einer SIF sind viele Annahmen erforderlich. ALLE diese Annahmen müssen in einer sorgfältigen Analyse der SIS-Ereignisse und der Wartungsaufzeichnungen über die Zeit nachgewiesen werden.

Änderungen

Jede SIS Änderung soll mit der gleichen Ernsthaftigkeit wie das Originaldesign behandelt werden. Die Auswirkungsuntersuchung einer Änderung weist auf den Punkt im Lebenszyklus hin, ab dem die Folgeschritte zur Komplettierung erforderlich sind. Dieses erfordert eine angemessene Verifikation der Vorgänge und die Validierung der installierten Änderung.

Denken Sie daran: Alle zuvor genannten Anforderungen im *Management der Funktionalen Sicherheit* sind auf jede dieser Aktivitäten im Sicherheitslebenszyklus anzuwenden.

„Haben Sie alle Fähigkeiten und Ressourcen, welche Sie für die Einhaltung der IEC61511 benötigen?

Informieren Sie sich bei Emerson über SIS-Lösungen und Dienstleistungen im Lebenszyklus.

Ihr Ansprechpartner: Kai Henkel
SIS Consultant
+49-(0)2129-553-198
kai.henkel@emerson.com

EMERSON.
Process Management