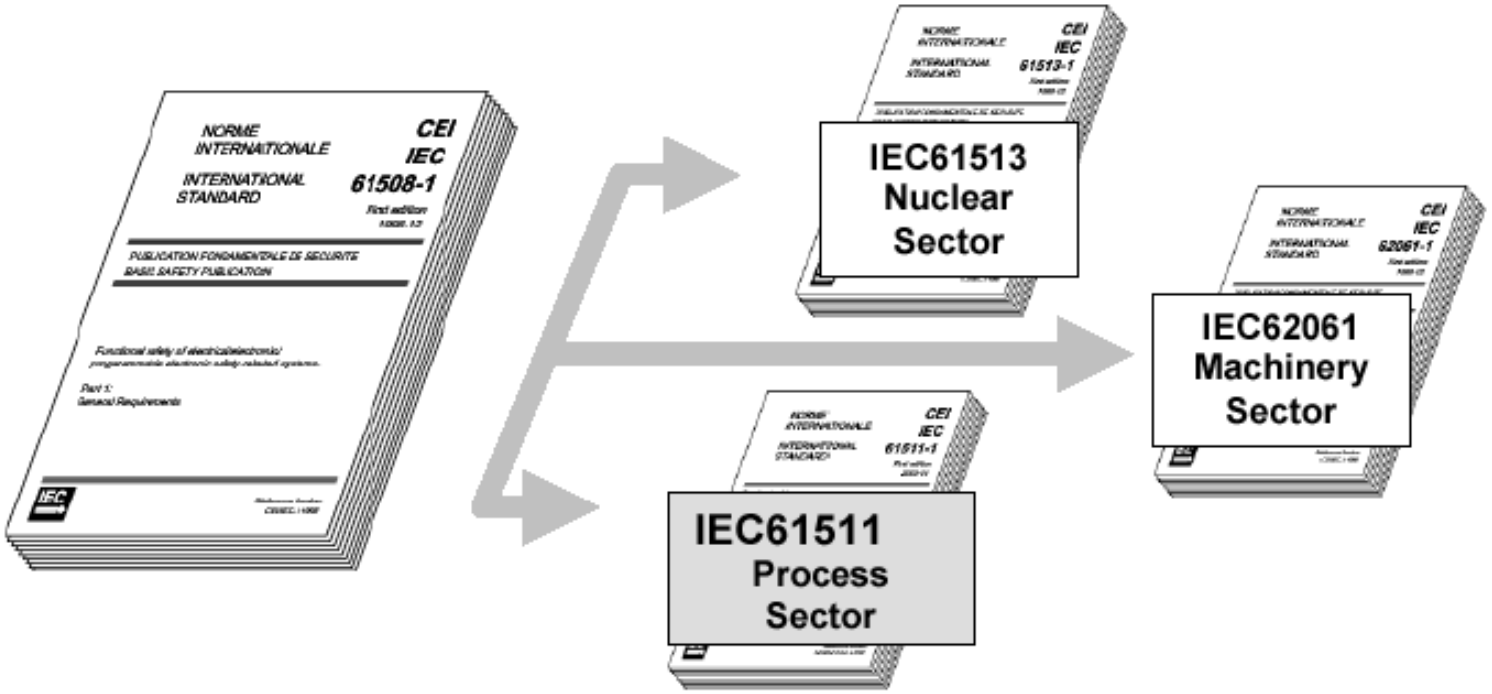
Science For A Better Life

Neue Ausgabe der IEC 61511

(VDE 0810)

23.03.2017 / Dr. G. Schmitt-Pauksztat / Version 1

Einordnung der IEC 61511



Hersteller

Anwender

Stand Veröffentlichung IEC 61511 Ed. 2

Functional safety – Safety instrumented systems for the process industry sector

- IEC 61511-1 Edition 2.0 2016-02
  Part 1: Framework, definitions, system, hardware and application programming requirements
  - IEC 61511-1:2016/COR1:2016-09
  - IEC 61511-1 Edition 2.0 Amend. 1/CDV (Abstimmung bis 2017-01-13)
- IEC 61511-2 Edition 2.0 2016-07
  Part 2: Guidelines for the application of IEC 61511-1: 2016
- IEC 61511-3 Edition 2.0 2016-07
  Part 3: Guidance for the determination of the required safety integrity levels

- europäische Übernahme der Norm durch CENELEC TC 65X zurückgestellt, derzeit gültig: DIN EN 61511-1(VDE 0810):2005

Begriffe und Definitionen

- “Schutzeinrichtung” -> “Sicherheitseinrichtung”
- 3 Betriebsarten:
  - low demand mode (niedrige Anforderungsrate)
    Häufigkeit von Anforderungen nicht mehr als einmal pro Jahr
  - high demand mode (hohe Anforderungsrate)
    Häufigkeit von Anforderungen mehr als einmal pro Jahr
  - continuous mode (kontinuierliche Anforderung)
    PLT-Sicherheitsfunktion Teil des normalen Betriebs

Lebenszyklus (1)

- Kompetenzen von beteiligten Personen (IEC 61511-1 5.2.2):
  - Einsatz von qualifizierten Personen im gesamten Lebenszyklus, dokumentiertes Management der Kompetenzen
  - regelmäßige dokumentierte Prüfung der Kompetenz (inkl. Prozessbeschreibung)
- Management von Änderungen, Rücksprung in frühere Phasen des Lebenszyklus (IEC 61511-1 6.2)
- Anwendungsprogrammierung Teil des Lebenszyklus (IEC 61511-1 6.3/10)
- Lieferanten von Produkten mit Konformität zu IEC 61511-1 müssen ein Managementsystem für Funktionale Sicherheit haben (IEC 61511-1 5.2.5)
- Sicherheitshandbuch erforderlich mit Randbedingungen für Betrieb, Instandhaltung und Fehleraufdeckung der PLT-Sicherheitseinrichtungen sowie typische Geräte-Konfiguration und betriebliche Umfeld (IEC 61511-1 11.2.13)

Lebenszyklus (2)

- Functional Safety Assessments (IEC 61511-1/2 5.2.6)
  begleitend bei Spezifikation / Planung / Bau u. Inbetriebnahme (MoC beachten)
  regelmäßig während des Betriebs
  Erweiterte Anforderungen bzgl. Kriterien und Teilnehmer
- Umgang mit Bestand:
  bestehende PLT-Sicherheitseinrichtungen nach alten Standards überprüfen, ob in sicherer Art und Weise geplant, instandgehalten, geprüft und betrieben
  (IEC 61511-1 5.2.5.4)

Betrieb (1)

- Überwachung der Leistungsfähigkeit der PLT-Sicherheitseinrichtungen / Verfahren zum Sammeln von Daten bezogen auf (IEC 61511-1, 16.2.2 f / 16.2.9)
  - Anforderungsrate
  - Zuverlässigkeitsdaten (Fehler und Fehlermodi)
  - Ursache der Anforderung
  - ergriffene Maßnahmen bei Ansprechen der Sicherheits-einrichtung
  - Ursache und Häufigkeit von Fehlauslösungen (spurious trip)
  - Ausfall von Einrichtungen, die Teil von Ersatzmaßnahmen sind

Betrieb (2)

- Änderungsmanagement erweitert (IEC 61511-1 17.2.4/5):
  - Sicherheitsplanung für Änderungen und Verifikation der Änderung
  - Änderung und Verifikation in Übereinstimmung mit Planung
  - Aktualisierung aller betroffenen Dokumente
- Identifikation und Vorhaltung von Ersatzteilen von PLT-Sicherheitseinrichtungen (IEC 61511-1 16.2.12)
- Anforderungen an Brückung / Ersatzmaßnahmen
  - Weiterbetrieb nur zulässig, wenn Risikominderung der Ersatzmaßnahme ausreichend (IEC 61511-1 16.2.4)
  - Zustand in „Überbrückungs-Logbuch“ (IEC 61511-1 16.2.7)
  - Freigabe, Signalisierung (IEC 61511-1 16.2.7)
  - definierte zeitliche Begrenzung (IEC 61511-1 11.8.4)

Hardware Fehler Toleranz (HFT)

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand mode or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

(IEC 61511-1 Kapitel 11)

- Vereinfachung auf eine HFT-Tabelle
- Kriterium für Safe Failure Fraction (SFF) entfällt
- Vorgehensweise nach IEC 61508 weiterhin zulässig

Auswahl von Geräten

Einsatz von Geräten in Sicherheitseinrichtungen (IEC 61511-1 11.5.2.1)

- betriebsbewährte Geräte “prior use” und/oder
- Geräte entwickelt nach IEC 61508-2/3

Geräte müssen für den Anwendungsfall geeignet sein.

Differenzierung der Betriebsbewährung

- proven in use (IEC 61508 / Hersteller)
- prior use (IEC 61511 / Anwender)
  - Firmen- oder betriebsspezifische Auswahl von Geräten in verschiedenen Anwendungen, Fokus auf Prozess und Prozessanschluss
  - Nachweis der Einsatzfähigkeit in Sicherheitseinrichtungen (IEC 61511-1, 11.5.3)
    - Berücksichtigung des Herstellers (Qualität / Management System)
    - Nachweis der Leistungsfähigkeit des Geräts
    - Umfang der Betriebserfahrung
  - Geräte unterliegen einem Änderungsmanagement (IEC 61511-1, 11.5.3.3)

Quantifizierung zufälliger Ausfälle

- berechnete Ausfallwert muss berücksichtigen u.a. (IEC 61511-1 11.9.2):
  - die Prüf-Abdeckung (PTC) jeder wiederkehrenden Funktionsprüfungen, die zugehörige Prüfvorschrift und die Zuverlässigkeit der Prüfeinrichtungen und der Prüfvorschrift
- Anforderung an Zuverlässigkeitsdaten zur Quantifizierung zufälliger Ausfälle müssen (IEC 61511-1 11.9.3):
  - belastbar
  - dokumentiert
  - nachvollziehbar
  - begründet
  - auf Felddaten für ähnliche Geräte in einer ähnlichen Betriebsumgebung beruhen
- Berücksichtigung von Unsicherheiten der Zuverlässigkeitsdaten (z.B. durch Wahl des Konfidenzintervalls)
- Vorgehensweise bei Nicht-Erreichen des Zielwertes (IEC 61511-1 11.9.5)

Verifikation (Test und Testplanung)

Nachweis durch Überprüfung, Analyse und/oder Test, dass die im Verifikationsplan festgelegten Tätigkeiten durchgeführt wurden (IEC 61511-2 7.2)

- in Anforderungsspezifikation / Planung der Verifikation im Voraus (IEC 61511-1 7.2)
- Planung für die Integration des Anwendungsprogramms, der Hardware und der Feldgeräte, einschließlich der Integration von Teilsystemen, die anderen Normen unterliegen (wie Maschinen oder Feuerungsanlagen)
- Prüfumfang (Beschreibung des Testaufbaus, Art des Tests einschließlich des Tests für die Hardware, des Anwendungsprogrammes und des Programmiergerätes)
- Prüffälle und Prüfdaten (spezifische Testszenarien)
- Prüfumgebung, einschließlich Werkzeuge
- Prüfkriterien und Umgang mit Abweichungen
- Prüfung der Rückwirkungsfreiheit von nicht-sicherheitsgerichteten Funktionen

IT-Sicherheit / Security

Risikobewertung zur IT-Sicherheit muss durchgeführt werden (IEC 61511-1 8.2.4)

- Beschreibung der beteiligten Komponenten PLT-Sicherheitseinrichtungen, PLT-Betriebseinrichtungen oder sonstige verbundene Systeme
- Beschreibung der identifizierten Risiken, die zu Sicherheitsvorfällen führen (einschließlich absichtlicher Angriffe auf die Hardware, das Anwendungsprogramm und zugehöriger Software sowie unbeabsichtigter Ereignisse durch menschliche Fehler)
- Beschreibung möglicher Auswirkung und Eintrittswahrscheinlichkeit
- Berücksichtigung aller Phasen im Lebenszyklus
- Festlegung der Anforderungen zur weiteren Risikoreduzierung

Ausfallsicherheit vor den erkannten Risiken muss gegeben sein (IEC 61511-1 11.2.12)

PLT-Betriebseinrichtungen mit Sicherheitsfunktion (1)

Anforderungen PLT-Betriebseinrichtungen mit Sicherheitsfunktion:

- Risikominderung ≤10 (IEC 61511-1 9.3.2)
- Begrenzung der Anzahl der Maßnahmen für ein Risiko: (IEC 61511-1 9.3.4)
  - nicht mehr als 1 PLT-Betriebseinrichtung, falls PLT-Betriebseinrichtung Auslöser für Anforderung der Sicherheitseinrichtung ist
  - nicht mehr als 2 PLT-Betriebseinrichtungen, falls PLT-Betriebseinrichtung nicht Auslöser für Anforderung der Sicherheitseinrichtung ist
- Unabhänigigkeit (IEC 61511-1 9.3.5):
  - PLT-Betriebseinrichtung unabhängig und getrennt von auslösender Quelle des Risikos, sodass Risikominderung nicht beeinträchtigt
  - PLT-Betriebseinrichtung unabhängig und getrennt von jeder anderen Schutzebene, sodass Risikominderung nicht beeinträchtigt

PLT-Betriebseinrichtungen mit Sicherheitsfunktion (2)

Anforderungen an PLT-Betriebseinrichtungen mit Sicherheitsfunktion (IEC 61511-2)

- Spezifikation
- Änderungsmanagement
- Brückungsverfahren
- Rückwirkungsfreiheit von Änderungen im Leitsystem auf Maßnahme
- Quantitativer Nachweis der Risikoreduzierung (z.B. durch Stördatenmanagement)

Zusammenfassung

- Berücksichtigung der Kompetenzen der eingesetzten Personen
- Überwachung der Leistungsfähigkeit der PLT-Sicherheitseinrichtungen
- Reduzierung auf eine Tabelle zur Hardware-Fehler-Toleranz
- Berücksichtigung IT-Sicherheit / Security
- Anforderungen an PLT-Betriebseinrichtungen mit Sicherheitsfunktion

Zukunftsgerichtete Aussagen

Diese Website / Presse-Information / Präsentation kann bestimmte in die Zukunft gerichtete Aussagen enthalten, die auf den gegenwärtigen Annahmen und Prognosen der Unternehmensleitung von Bayer beruhen.

Verschiedene bekannte wie auch unbekannte Risiken, Ungewissheiten und andere Faktoren können dazu führen, dass die tatsächlichen Ergebnisse, die Finanzlage, die Entwicklung oder die Performance der Gesellschaft wesentlich von den hier gegebenen Einschätzungen abweichen. Diese Faktoren schließen diejenigen ein, die Bayer in veröffentlichten Berichten beschrieben hat. Diese Berichte stehen auf der Bayer-Webseite www.bayer.de/ zur Verfügung.

Die Gesellschaft übernimmt keinerlei Verpflichtung, solche zukunftsgerichteten Aussagen fortzuschreiben und an zukünftige Ereignisse oder Entwicklungen anzupassen.

Forward-Looking Statements

This website/release/presentation may contain forward-looking statements based on current assumptions and forecasts made by Bayer management.

Various known and unknown risks, uncertainties and other factors could lead to material differences between the actual future results, financial situation, development or performance of the company and the estimates given here. These factors include those discussed in Bayer's public reports which are available on the Bayer website at http://www.bayer.com/.

The company assumes no liability whatsoever to update these forward-looking statements or to conform them to future events or developments.

Science For A Better Life

Thank you!