

Quelle: <https://www.arbeitssicherheit.de//document/af850d9f-c8cd-358d-af78-4ad46182142f>

Bibliografie	
Titel	Praxishandbuch Brandschutz
Herausgeber	Scheuermann
Auflage	2016
Abschnitt	8 Explosionsschutz → 8.16 MSR-Technik im Rahmen von Explosionsschutzmaßnahmen
Autor	Dyrba
Verlag	Carl Heymanns Verlag

8.16.7 Maßnahmen zur Erkennung, Vermeidung oder Beherrschung des Ausfalls der MSR-Einrichtungen mit Sicherheitsfunktion

Allgemeine Anforderungen für ein Klassifizierungsverfahren

Falls für die ordnungsgemäße Funktion der Überwachung das Vorhandensein oder die Vorhaltung von Hilfsenergien (z.B. elektrische Energie) oder Hilfsmedien (z.B. Inertgase oder Druckluft) erforderlich sind, so ist bei Ausfall derselben die dafür festgelegte Sicherheitsfunktion auszuführen. Es ist z.B. eine Alarmierung auszulösen, oder die Hilfsenergie/-medien müssen redundant sein.

Überwachungen dürfen nach Auslösung nicht automatisch zurückgesetzt werden, es sei denn, in der Gefährdungsbeurteilung ist etwas anderes festgelegt.

Sofern manuelle Absperrrichtungen an Prozessanschlüssen von Sicherheitseinrichtungen vorhanden sind, muss deren Fehlstellung erkannt werden und zu Maßnahmen führen oder der Stellungszustand muss leicht erkennbar und gegen unbeabsichtigtes Schließen gesichert sein, z.B. durch Sperrhülsen, Kette und Schloss oder durch Entfernen von Handrädern.

Überwachungen müssen grundsätzlich unabhängig von betrieblich erforderlichen Mess-, Steuer- und Regeleinrichtungen funktionieren.

Zwischen Überwachungen und Betriebseinrichtungen ohne Sicherheitsfunktion, wie z.B. Visualisierungseinrichtungen, ist grundsätzlich Rückkopplungsfreiheit sicherzustellen. Die Überwachung muss von MSR-Betriebseinrichtungen insoweit unabhängig sein, dass bei Ausfällen von Betriebseinrichtungen die Funktion der Überwachung erhalten bleibt (z.B. dürfen Anregesignale der Überwachung zur Verwendung im Regelkreis von MSR-Betriebseinrichtungen nur rückwirkungsfrei ausgekoppelt werden). Andernfalls ist von einer Abhängigkeit auszugehen. Das Signal zur Auslösung der Sicherheitsfunktion muss stets Vorrang vor den Signalen der Betriebseinrichtung haben.

Für einfache Systeme kann in den folgenden Fällen die Klassifizierungsstufe K1 durch bewährte Technik mit regelmäßiger Prüfung in Verbindung mit den allgemeinen Anforderungen nach diesem Kapitel erreicht werden:

- Überwachung betrieblicher Zündquellen
- Überwachung von Maßnahmen zur Vermeidung explosionsfähiger Atmosphäre

Komplexe Systeme können nur verwendet werden, wenn diese durch den Hersteller oder hinsichtlich der Betriebsbewährung durch den Arbeitgeber bewertet sind.

Für komplexe Systeme, die programmierbar sind, müssen die Anforderungen der DIN EN 50495 (VDE 0170-18):2010-10, Kapitel 5.3.3 bei der Erstellung der Anwendersoftware beachtet werden. Dabei gilt insbesondere

- Die Anwendersoftware ist mit einem eindeutigen Stand zu dokumentieren. Die Übereinstimmung zwischen Dokumentation und Anwendersoftware ist nachzuweisen (z.B. durch Signaturen, Versionsnummern).
- Die wesentlichen Inhalte der Dokumentation sind:
 - Programmdokumentation
 - Spezifikation der Schutzfunktionen (Protokoll der Sicherheitsbetrachtung)
 - Spezifikation der Schutzfunktionen (Protokoll der Sicherheitsbetrachtung)

Prozessleitsysteme (PLS) können als komplexe Systeme für die Klassifizierungsstufe K1 eingesetzt werden, wenn für diese die folgenden Bedingungen erfüllt sind:

- Der PLS-Hersteller betreibt zum Zeitpunkt der Herstellung ein Qualitätssicherungssystem.
- Der PLS-Hersteller betreibt ein Änderungsmanagement für die Soft- und Hardware, z.B. gemäß DIN EN 50495 (VDE 0170-18):2010-10 oder DIN EN 62061 (VDE 0113-50):2013-09.
- PLS-Systeme sind in bewährter Technik ausgeführt, wenn sie sich in Standardanwendungen des Arbeitgebers oder vergleichbaren Anwendungen bewährt haben und einem Freigabeverfahren unterzogen wurden.
- Das PLS hat eine dokumentierte Spezifikation (Lastenheft) und muss auch für eine Verwendung in kontinuierlich betriebenen Anlagen der Prozessindustrie geeignet sein.
- Die Hardware ist vor Inbetriebnahme einer dokumentierten Funktionsprüfung zu unterziehen. Die Software ist auf Plausibilität zu prüfen.
- Der Arbeitgeber verfügt über ein Änderungsmanagement für alle Änderungen in der Hard- und Software mit Freigabe zur Änderung sowie genehmigter Spezifikation und anschließender dokumentierter Prüfung.
- Das für die Instandhaltung und Änderungen eingesetzte Personal hat eine geeignete Qualifikation. Diese beinhaltet technisches Wissen, Ausbildung und Erfahrung bezogen auf
 - die verfahrenstechnische Anwendung
 - die eingesetzte PLS-Technologie
 - Sensoren und Aktoren
- Zwischen betrieblichen Einrichtungen und Überwachungen besteht eine hinreichende Unabhängigkeit:

8.16.7 Maßnahmen zur Erkennung, Vermeidung oder Beherrschung des Ausfalls der MSR-Einrichtungen mit Sicherheitsfunktion – Seite 3 – 01.06.2016

- Funktional zusammenhängende Betriebsfunktion und Sicherheitsfunktion sollen nicht auf gleichen Eingangs- und Ausgangskarten liegen. Die Realisierung von Sicherheitsfunktionen im Automatisierungssystem ist grundsätzlich mit separaten Modulen übersichtlich durchzuführen.
- Funktionen von Überwachungen müssen gegenüber Betriebseinrichtungen stets Vorrang haben und sind als solche in der Funktionsspezifikation detailliert festzulegen.
- Nutzung vorhandener Fail-safe-Eigenschaften (z.B. Ruhesignalprinzip, sicherer Zustand bei Ausfall der Spannungsversorgung)
- Prozessleitsysteme dürfen keine Funktion von Gaswarnanlagen wahrnehmen, es sei denn, sie sind nach den Normen für Gaswarnanlagen ausgelegt und geprüft.
- Für die Klassifizierungsstufen K2 bis K3 gilt, dass ein passiver Fehler innerhalb einer Zeitspanne erkannt und beseitigt werden muss, in der vernünftigerweise nicht mit einem weiteren Fehler gerechnet werden muss, der in Kombination mit dem passiven Fehler zu einem unsicheren Zustand führt.

- Bei softwaregesteuerten Geräten (z.B. Frequenzumrichter oder Stellungsregler) sollten sicherheitstechnische Schalthandlungen grundsätzlich ohne deren Softwaresteuerung direkt auf das entsprechende Stellglied einwirken, es sei denn, es liegt der Nachweis der erforderlichen funktionalen Sicherheit vor.

Zusatzmaßnahmen

- Über die allgemeinen Anforderungen hinaus sind, wenn im Einzelnen gefordert, die folgenden Zusatzmaßnahmen einzuhalten:

1. Einhaltung der grundlegenden und bewährten Sicherheitsprinzipien nach ISO 13849-2:2008, insbesondere:
 - Verwendung bewährter und zuverlässiger Installationstechnik
 - Geeignete Auswahl, Kombination, Anordnungen, Zusammenbau und Einbau der Bauteile durch Berücksichtigung der Anwendungshinweise der Hersteller sowie von Erfahrungen mit ähnlichen Bauteilen

2. Übersichtlicher und einfacher Aufbau der Überwachung. Verringerung der Anzahl von Bauteilen

3. Begrenzung von Fehlerauswirkungen durch z.B.

- hochohmige Entkopplung oder
- Kurzschlussfestigkeit oder
- galvanische Trennung.

4. Anwendung des Ruhestrom- bzw. Ruhesignalprinzips für Signalleitungen

8.16.7 Maßnahmen zur Erkennung, Vermeidung oder Beherrschung des Ausfalls der MSR-Einrichtungen mit Sicherheitsfunktion – Seite 4 – 01.06.2016

[<<](#)

5. Verhinderung von Grenzwertveränderungen durch nicht autorisierte Personen

6. Toleranz der Überwachung gegen Abweichungen der Hilfsenergieversorgung (z.B. Steuerluft, elektrische Versorgung usw.). Abweichungen über die für die Versorgung der Geräte zulässigen Grenzwerte hinaus dürfen keinen schädlichen Fehler in der Überwachung zur Folge haben. Z.B. durch:

- entsprechende Eigenschaften der Geräte selbst oder
- Sicherstellung der Hilfsenergieversorgung durch z.B. Redundanzen oder
- automatische Überwachung der Hilfsenergieversorgung mit Melden und Auslösen der Schutzfunktion.

7. Vermeidung von Fehlern gemeinsamer Ursache in redundanten Ex-Einrichtungen

8. Wiederkehrende Prüfungen in Abhängigkeit von der Klassifizierungsstufe nach den Festlegungen der Hersteller und/oder den Erfahrungen des Arbeitgebers. Mit einer Verkürzung der Prüfabstände kann eine höhere funktionale Sicherheit erreicht werden.

- Bei anderen Klassifizierungsstufen als K1 sind zur Erfüllung der erforderlichen Fehlersicherheit, in Abhängigkeit von einer Fehlerbetrachtung, weitergehende Maßnahmen notwendig, z.B.:
 - MSR-Einrichtungen zur automatischen Funktionsüberwachung (z.B. Laufzeit- oder Stellungsüberwachung),
 - Plausibilitätsprüfung,
 - Schritt- und Zeitüberwachung oder
 - Erkennung eines Kurzschlusses oder einer Unterbrechung.

Bearbeitungsdatum: Dezember 2016