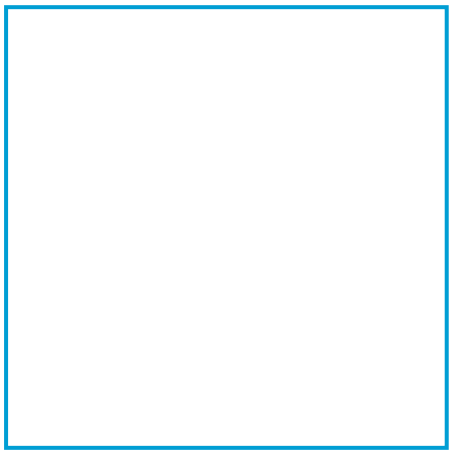
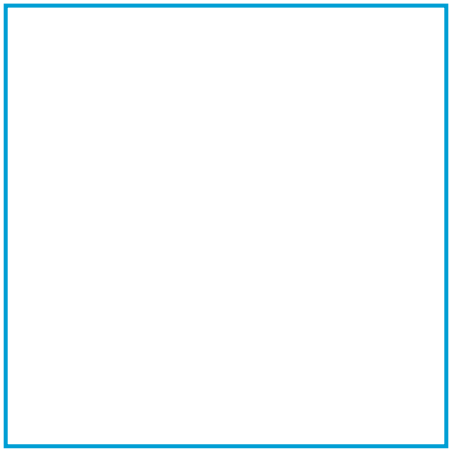
PTB bericht Dos-59
Juli 2017

Harald Dombrowski, Ulrich Grottker, Björn Pullner, Annette Röttger, Roland Zwiener

Sicherheitsvorrichtungen von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen





ISSN 0172-7095
ISBN 978-3-95606-329-9

Physikalisch-Technische Bundesanstalt

Dosimetrie
PTB-Dos-59
Braunschweig, Juli 2017

Harald Dombrowski, Ulrich Grottker, Björn Pullner, Annette Röttger, Roland Zwiener

Sicherheitsvorrichtungen von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen – Anforderungen für die Bauartprüfung nach der Röntgenverordnung –

Leitfaden für Hersteller und Gutachter
Rev. 1.0

ISSN 0172-7095
ISBN 978-3-95606-329-9

Die aktuelle Version dieses Dokuments basiert auf PTB-Bericht PTB-Dos-49 von 2005. Die damaligen Autoren waren Dr. Stefan Neumaier, Dr. Ulrich Grottker, Dr. Harald Dombrowski, Alexander Höhne, Roland Zwiener und Dr. Peter Ambrosi, denen die Autoren der dieser Fassung hiermit herzlich für die geleistete Arbeit danken.

Zusammenfassung

Dieser Bericht beschreibt die Anforderungen der PTB an Sicherheitsvorrichtungen von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen für die Bauartprüfung gemäß Röntgenverordnung. Er enthält detaillierte Anforderungen sowohl an die Hard- als auch an die Software, um das geforderte Sicherheitsniveau zu gewährleisten und richtet sich insbesondere an Hersteller und Gutachter derartiger Röntgeneinrichtungen.

Diese neue Fassung des Leitfadens erläutert grundlegende Prinzipen bei der Schaffung einer Sicherheitsarchitektur nach DIN EN 62061, d. h. es werden Sicherheitsanforderungen und die Prinzipien der Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen sowie spezielle Anforderungen für sicherheitsbezogene Teile von Steuerungen mit programmierbaren elektronischen Systemen beschrieben. Die Beurteilung von Sicherheitsvorrichtungen geschieht gemäß der gleichen Norm, wobei für die Konstruktion und Beurteilung von Teilsystemen auch die Normen DIN EN 13849-1 bzw. DIN EN 13849-2 hinzugezogen werden können. Beide Normen legen Anforderungen für den Entwurf und die Implementierung von sicherheitsbezogenen Steuerungssystemen von Maschinen im Sinne von DIN EN ISO 12100 fest, das für Röntgeneinrichtungen notwendige Schutzniveau für komplexe Systeme wird nur durch die Norm DIN EN 62061 beschrieben. Die DIN EN 62061 beruht auf der sehr umfangreichen DIN EN 61508. Sie enthält neben den Anforderungen für die Auswahl und den Entwurf eines sicherheitsbezogenen elektrischen, elektronischen und programmierbaren elektronischen Steuerungssystems (SRECS) einen informativen Anhang mit einem qualitativen Ansatz zur Risikoabschätzung und Festsetzung des Sicherheits-Integritätslevels bereit, der auf sicherheitsbezogene Steuerungsfunktionen für Maschinen bezogen ist, und im Folgenden für die Sicherheitsvorrichtungen von Röntgeneinrichtungen herangezogen wird.

Abstract

This report describes the PTB requirements for engineered safeguards of basic-protection devices, high-protection devices, full-protection devices and school X-ray devices within the framework of type tests according to the German X-ray Ordinance. It contains detailed requirements for the hard- and software to ensure the required safety level. Especially manufacturers and evaluators of such X-ray tube assemblies are addressed.

Dombrowski, Harald ; Grottker, Ulrich ; Pullner, Björn ; Röttger, Annette ; Zwiener, Roland.
Sicherheitsvorrichtungen von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen. Anforderungen für die Bauartprüfung nach der Röntgenverordnung.
Leitfaden für Hersteller und Gutachter. Rev. 1.0. Physikalisch-Technische Bundesanstalt (PTB), 2017.
Verfügbar unter: https://doi.org/10.7795/110.20171023

Inhalt

1 Einleitung

Dieser Bericht richtet sich an Hersteller und Gutachter von Röntgeneinrichtungen für nichtmedizinische Zwecke im Sinne der Anlage 2 Nr. 2, 3, 4 und 6 der „Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (Röntgenverordnung, RöV)“[1].

Der Betrieb von Röntgeneinrichtungen bedarf nach § 3 RöV grundsätzlich der Genehmigung. Der Gesetzgeber hat im § 4 RöV jedoch eine Reihe von Röntgeneinrichtungen vom Erfordernis der Genehmigung ausgenommen, wenn die Inbetriebnahme der zuständigen Behörde rechtzeitig angezeigt wird. Die Einzelheiten des Anzeigeverfahrens sind in § 4 näher geregelt.

Genehmigungsfrei bei Anzeige ist insbesondere der Betrieb von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen; dies sind bauartzugelassene Röntgeneinrichtungen für nichtmedizinische Zwecke, die den Vorschriften der Anlage 2 Nr. 2, 3, 4 bzw. 6 der RöV entsprechen. Bauartzugelassene Geräte können i. Allg. bereits zwei Wochen nach der erfolgten Anzeige genehmigungsfrei in Betrieb genommen werden. Das Anzeigeverfahren stellt für den Betreiber, im Vergleich zur Genehmigung, ein vereinfachtes Verfahren dar. Die Anforderungen an das organisatorische Strahlenschutzregime und an die Fachkunde des Betreibers sind beim Anzeigeverfahren für nichtmedizinische Röntgeneinrichtungen nur sehr gering. Der Strahlenschutz muss bei diesen bauartzugelassenen Röntgeneinrichtungen deshalb praktisch vollständig durch technische Maßnahmen der Einrichtungen selbst sichergestellt sein.

Nach § 8 RöV hat die Zulassungsbehörde vor ihrer Entscheidung über die Erteilung einer Bauartzulassung auf Kosten des Antragstellers eine Bauartprüfung durch die Physikalisch-Technische Bundesanstalt (PTB) zu veranlassen. Die PTB überprüft im Rahmen dieser Bauartprüfungen die Einhaltung der Bauartanforderungen [2].

Für Basisschutzgeräte, Hochschutzgeräte, Vollschutzgeräte und Schulröntgeneinrichtungen schreibt die Anlage 2 der RöV im Wesentlichen zwei Bereiche von Bauartanforderungen vor:

- **Anforderungen an die Ortsdosisleistung:**
  Es muss sichergestellt sein, dass die Ortsdosisleistung (ODL) in einer Entfernung von 0,1 m von der berührbaren Oberfläche des Schutzgehäuses die in der Anlage 2 der RöV genannten zulässigen Maximalwerte nicht überschreitet. Für Vollschutzgeräte und Schulröntgeneinrichtungen beträgt die maximal zulässige ODL zur Zeit 3 Mikrosievert durch Stunde, für Hochschutzgeräte und Basisschutzgeräte 10 Mikrosievert durch Stunde

- **Anforderungen an das Schutzgehäuse:**
  Es muss sichergestellt sein, dass das Schutzgehäuse außer der Röntgenröhre oder dem Röntgenstrahler auch den zu behandelnden oder zu untersuchenden Gegenstand vollständig umschließt und die Röntgenröhre oder der Röntgenstrahler nur bei vollständig geschlossenem Schutzgehäuse betrieben werden kann. Für Untersuchungsverfahren, die einen kontinuierlichen Betrieb des Röntgenstrahlers erfordern, gelten, soweit das Schutzgehäuse während des Betriebes geöffnet werden kann, analoge Anforderungen für die „Shutter“, die das Strahlenaustrittsfenster verschließen. Bei Vollschutzgeräten müssen die genannten Anforderungen durch zwei voneinander unabhängige Vorrichtungen (im Folgenden auch als Sicherheitsvorrichtungen bezeichnet) sichergestellt sein. Die Anforderungen an das Schutzgehäuse sowie an die beiden Sicherheitsvorrichtungen werden durch einen Beschluss des Länderausschusses Röntgenverordnung beim Bundesumweltministerium (BMU) vom

27. März 2001 präzisiert (siehe Anhang 2), wobei auf die Normen DIN EN 954-1 vom März 1997 und auf die DIN 54113 Teil 2 [3] vom September 1992 Bezug genommen wird.

Mittlerweile ist die DIN EN 954-1 nicht mehr gültig, sodass die Nachfolgenorm DIN EN 62061 [5] herangezogen werden muss. In speziellen Teilaspekten kann auch DIN EN 13849-1 [5] für die Berechnung der Wahrscheinlichkeit für einen gefährlichen Ausfall pro Stunde (Probability of dangerous failure per hour – PFH) verwendet werden. Daraus folgt nach einer Neubewertung gemäß DIN EN 62061, dass insbesondere die zwei Sicherheitsvorrichtungen, neben ihrer Unabhängigkeit, über eine Fehlererkennung verfügen und den Sicherheitsintegritätslevel (SIL) 3 erfüllen müssen (Ableitung des SIL s. Abschnitt 9.1).

Die genannten Anforderungen sollen gewährleisten, dass Bauartzulassungen nur für solche Röntgeneinrichtungen erteilt werden, die dem Stand der Technik entsprechen und beim zugelassenen Einsatz den Erfordernissen des Strahlenschutzes genügen.

Die Bauartprüfungen von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen werden in einem eigenen PTB-Bericht ausführlich beschrieben [2]. Schwerpunkte bilden dabei die rechtlichen, verwaltungstechnischen und physikalischen Grundlagen sowie die Messung der ODL. Der vorliegende Bericht beschäftigt sich dagegen ausschließlich mit den nach der Röntgenverordnung geforderten Sicherheitsvorrichtungen und den damit verbundenen sicherheitstechnischen Fragestellungen.

Da die ODL im Innenraum nichtmedizinischer Röntgeneinrichtungen die oben genannten maximal zulässigen Werte bei weitem überschreiten kann − im Nutzstrahl von Vollschutzgeräten typischerweise um 5 bis 7 Größenordnungen − kommt den Anforderungen an das Schutzgehäuse sowie an seine Sicherheitsvorrichtungen für den Strahlenschutz eine zentrale Bedeutung zu. Wegen der speziellen Anforderungen an die Prüfung der Sicherheitsvorrichtungen wurde dem sicherheitstechnischen Teil der Bauartprüfungen dieser Bericht gewidmet.

Diese Zusammenstellung der Bauartanforderungen und –prüfungen von Sicherheitsvorrichtungen von Basisschutzgeräten, Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen trägt insbesondere dem Wunsch von Herstellern Rechnung, eine detaillierte Darstellung der Anforderungen sowie der zugrunde liegenden Sicherheitskonzepte zu erhalten, um diese frühzeitig bei der Konstruktion neuer Röntgeneinrichtungen berücksichtigen zu können. Ziel dieses „Leitfadens“ ist es deshalb, die Anforderungen an die Sicherheitsvorrichtungen zu schildern und zu erläutern und dabei verbindliche Rahmenbedingungen aufzuzeigen, ohne jedoch konkrete technische Lösungen vorzuschreiben. Der Bericht soll ferner als Arbeitsgrundlage für die Zusammenarbeit zwischen der PTB und Gutachtern dienen, die die PTB bei der Durchführung der vielfältigen und z. T. sehr aufwändigen sicherheitstechnischen Prüfungen unterstützen. Die Darstellung des Ergebnisses dieser Prüfungen sollte sich in Form und Inhalt an dem in Anhang 1 gezeigten Beispiel orientieren.

2 Begriffsbestimmungen

Dieser Abschnitt enthält Erläuterungen der verwendeten Fachbegriffe aus den Bereichen der Sicherheitstechnik und der Röntgentechnik [1].

2.1 Sicherheitstechnik

Ausfall	Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen aufgrund von Verschleiß und anderer physikalischer Effekte oder von Umwelteinflüssen.
Ausfalloffenbarungszeit	Zeit zwischen Auftreten eines Ausfalls und Auslösung der Betriebshemmung.
Betriebshemmung	Verhinderung der Nutzfunktion bei Fehlern, veranlasst und gesteuert durch eine Vorrichtung oder durch Bauelement-Eigenschaften. Bei Röntgeneinrichtungen bedeutet dies, dass ein Wiedereinschalten der Hochspannung nach dem Ausfall einer der Sicherheitsvorrichtungen verhindert wird.
Fehler	Oberbegriff für Ausfälle (Funktionsversagen der Hardware, „zufällige Fehler“) und Abweichungen der System-Realisierung von der geplanten oder gewollten Form (Konstruktionsfehler, Software-Fehler, „Systematische Fehler“).
Fehlerbeherrschung	Erkennung von Fehlern und automatische Auslösung der Betriebshemmung durch bestimmte Schaltungsstrukturen.
Fehlervermeidung	Verwendung von Techniken und Verfahren mit dem Ziel, die Entstehung von Fehlern während jeder Phase des Sicherheitslebenszyklus des sicherheitsbezogenen Systems zu vermeiden.
Gefährdung	Quelle einer möglichen Verletzung oder Gesundheitsschädigung. Anmerkung: Im Bereich des Strahlenschutzes ist darunter auch das Risiko für stochastische Strahlenschäden zu verstehen.
Redundanz	Anwendung von mehr als einem Gerät oder System oder Teil eines Gerätes oder Systems, um sicherzustellen, dass bei Ausfall der Funktion eines Gerätes oder Systems ein anderes verfügbar ist, diese Funktion zu erfüllen.
Risiko	Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.
Sicherheit	Geringe Wahrscheinlichkeit des Auftretens von Gefährdungen.
SIL	Sicherheitsintegritätslevel
Störung	Sporadisch auftretender Verlust der Fähigkeit eines Bauelementes, seine vorgesehene Funktion auszuführen aufgrund von Verschleiß, von anderen physikalischen Effekten oder von Umwelteinflüssen.
Systematische Fehler	Fehler, die grundsätzlich auf konkrete Ursachen zurückgeführt werden können, d. h. Software-Fehler und bezüglich der Hardware Konstruktions- und Fertigungsfehler. Wenn ein derartiger Fehler vorhanden ist, tritt er in jedem serienmäßig gefertigten Exemplar auf.
Zufällige Fehler	Fehler, die ohne eine vorhersehbare physikalische Ursache zu zufälligen Zeitpunkten auftreten. Diese Fehler werden statistisch betrachtet und durch eine „Ausfallrate“ beschrieben.

2.2 Röntgentechnik

Röntgeneinrichtung	Einrichtung, die zum Zweck der Erzeugung von Röntgenstrahlung betrieben wird einschließlich Anwendungsgeräten, Zusatzgeräten und Zubehör, der erforderlichen Software sowie Vorrichtungen zur medizinischen Befundung.
Röntgenstrahler	Bestandteil einer Röntgeneinrichtung, bestehend aus Röntgenröhre und Röhrenschutzgehäuse, bei einem Einkesselgerät auch dem Hochspannungserzeuger.
Basisschutzgerät	Röntgeneinrichtung, die den Vorschriften der Anlage 2 Nr. 6 der RöV entspricht.
Hochschutzgerät	Röntgeneinrichtung, die den Vorschriften der Anlage 2 Nr. 2 der RöV entspricht.
Vollschutzgerät	Röntgeneinrichtung, die den Vorschriften der Anlage 2 Nr. 3 der RöV entspricht.
Schulröntgeneinrichtung	Röntgeneinrichtung zum Betrieb im Zusammenhang mit dem Unterricht in Schulen, die den Vorschriften der Anlage 2 Nr. 4 der RöV entspricht.
maximalen Betriebsbedingungen	Kombination der technischen Einstellparameter, die unter normalen Betriebsbedingungen bei Röntgenstrahlern nach Anlage 2 Nr. 1.1, Röntgeneinrichtungen nach Anlage 2 Nr. 2 bis 4 und 6 und Störstrahlern nach Anlage 2 Nr. 5 zur höchsten Ortsdosisleistung und bei Röntgenstrahlern nach Anlage 1 und Anlage 2 Nr. 1.2 zur höchsten mittleren Ortsdosisleistung führen. Hierzu gehören die Spannung für die Beschleunigung von Elektronen, der Röntgenröhrenstrom und gegebenenfalls weitere Parameter wie Einschaltzeit oder Elektrodenabstand.

3 Grundanforderungen an die Sicherheitsvorrichtungen von Vollschutzgeräten

3.1 Allgemeines

Die Anforderungen an die Bauart von Vollschutzgeräten sind in der Röntgenverordnung sowie durch einen Länderausschuss-Beschluss (vgl. Anhang 2) definiert.

Nach Anlage 2 Nr. 3.2 dieser Verordnung muss bei Vollschutzgeräten durch zwei voneinander unabhängige Vorrichtungen sichergestellt sein, dass

- die Röntgenröhre oder der Röntgenstrahler nur bei vollständig geschlossenem Schutzgehäuse betrieben werden kann, oder
- bei Untersuchungsverfahren, die einen kontinuierlichen Betrieb des Röntgenstrahlers erfordern, das Schutzgehäuse während des Betriebes des Röntgenstrahlers nur bei geschlossenem Strahlenaustrittsfenster geöffnet werden kann.

Anmerkung: Bei kontinuierlichem Betrieb wird das Strahlenaustrittsfenster typischerweise mit einem “Shutter“ verschlossen. Der Shutter ist in diesem Fall in die Sicherheitsvorrichtung mit einzubeziehen.

Zusätzlich sind Vollschutzgeräte mit einer Zeitverzögerung zu versehen, die das Öffnen des Schutzgehäuses erst dann ermöglicht, wenn nach dem Abschalten des Gerätes die Beschleunigungsspannung der Röntgenröhre 5 kV unterschritten hat. Diese Anforderung hat i. Allg. die Notwendigkeit des Einbaus einer aktiven Verriegelung zur Folge (siehe Abschnitt 3.2).

Anmerkung: Diese Anforderung dient dazu, eine Strahlenexposition durch „Reststrahlung“ zu vermeiden.

Weitere Anforderungen betreffen die maximal zulässigen Ortsdosisleistungen außerhalb bzw. im Innenraum dieser Geräte. Diese Anforderungen werden im PTB Bericht Dos-47 [2] ausführlich diskutiert. Der vorliegende Bericht beschäftigt sich dagegen im Wesentlichen mit der detaillierten Beschreibung der Sicherheitsanforderungen sowie deren Prüfung im Rahmen der Bauartprüfungen der PTB.

Insbesondere, wenn Sicherheitsvorrichtungen nach anderen Konstruktionsprinzipien realisiert wurden, als explizit in diesem Bericht berücksichtigt , kann außer den im Folgenden genannten Normen bei der Bauartprüfung die Berücksichtigung weiterer Normen und Regelwerke (z. B. der Schutz gegen physikalische Effekte - siehe Abschnitt 4.6.1) erforderlich sein. Eine sicherheitsbezogene Steuerungsfunktion, die den sicheren Zustand einer Maschine (hier: eines Gerätes) aufrechterhält, wird in der DIN EN 62061 abgekürzt als SRCF (Safety-Related Control Function) bezeichnet.

3.2 Aktive Verriegelung

Hierbei handelt es sich um eine elektromechanische Verriegelung, die sicherstellt, dass erst nach Herunterfahren der Spannung an der Röntgenröhre oder nach Schließen eines Röntgenröhrenverschlusses ein Zugang des Nutzers zum Innenraum oder Probenraum des Gerätes möglich ist, dass der Nutzer beim Öffnen einer Tür oder Klappe auch nicht einer Röntgen-Reststrahlung ausgesetzt ist. Die aktive Verriegelung soll so in die Sicherheitskreise eingebaut sein, dass für das Gesamtsystem die Anforderungen des SIL 3 nach DIN EN 62061 erfüllt.

Auf eine aktive Verriegelung kann verzichtet werden, wenn die folgenden drei Bedingungen alle eingehalten sind:

- Bei geöffnetem Schutzgehäuse überschreitet die Ortsdosisleistung in 0,1 m Abstand von der fiktiven berührbaren Oberfläche den Grenzwert der RöV zu keinem Zeitpunkt

und

- ein Hineinfassen in den Nutzstrahl ist unter normalen Betriebsbedingungen ausgeschlossen (z. B. aufgrund sehr kurzer Verschluss-Schließzeiten)

und

- im Fehlerfall überschreitet beim Hineinfassen in das Innere des Gerätes die Teilkörperbelastung der Hände bzw. die lokale Hautdosis den Jahresgrenzwert für die Bevölkerung auch bei maximal anzunehmender Ereigniszahl nicht.

Anmerkung: Die Messungen im Außenraum sind bei geöffnetem Verschluss und mit Streukörper durchzuführen.

Wenn das Gerät auch ohne aktive Verriegelung die Anforderungen nach RöV erfüllt, d. h. die drei obigen Bedingungen einhält, sind bei Anbringung einer zusätzlichen Verriegelung nur die Anforderungen der Kategorie B nach DIN EN 13849-2 [6] einzuhalten.

3.3 Warnleuchten

Es muss mindestens eine Warnleuchte vorhanden sein, die den Zustand Hochspannung eingeschaltet" ("HV On“) signalisiert. Dabei gelten folgende Anforderungen:

- Die Farbe dieser Leuchte muss gelb oder orange sein (nicht rot, nicht blau, nicht grün). Rote Lampen würden fälschlicherweise Gefahr signalisieren, was beim Betrieb umschlossener Strahler aber nicht gegeben ist.
- Diese Leuchte soll ausfallsicher sein. Mindestens ist jedoch eine redundante Auslegung gefordert.
- Die Leuchte muss derart angebracht sein, dass sie mindestens vom Schaltpult (Bediengerät) deutlich zu erkennen ist.

Diese Anzeige darf nicht die durch weitere Statusanzeigen verunklärt werden, insbesondere dann, wenn diese für den Nutzer nicht selbsterklärend sind. Es ist das Ziel, dass klar ersichtlich ist, wann die Röntgenröhre unter Hochspannung in Betrieb ist und wann nicht. Den Anforderungen an die Farbgebung der Leuchten wurde an die EU-Richtlinie 92/58/EWG angelehnt, auf die die Maschinenrichtlinie Bezug nimmt. (Anhang I, 3.) [7].

3.4 Vermeidung einfacher Manipulation

Verriegelungseinrichtungen müssen so gestaltet sein, dass sie nicht auf einfache Weise umgangen werden können (Zitat BGI 575).

Vorkehrungen, die ein Umgehen erschweren:

- Verwendung von codierten Positionsschaltern oder Systemen, z. B. mechanische, elektrische, magnetische oder optische,
- physikalische Hindernisse oder Verdeckungen der Verriegelungseinrichtungen bei geöffneter trennender Schutzeinrichtung.
- gesicherte Verbindungen, die eine Demontage erschweren (z. B. geschweißt, genietet, Einwegschrauben).

Als Umgehen auf einfache Weise gilt nicht ein aufwendiges Unwirksam machen von Schutzfunktionen wie z. B.:

- das Demontieren oder Wegdrehen von Bauteilen der Verriegelungseinrichtungen, z. B. Positionsschaltern und Zuhaltungen oder deren Betätigungsteile,
- das Benutzen eines separaten oder nicht bestimmungsgemäß montierten Betätigungsteils bei Verriegelungseinrichtungen der Bauart 2.

Die Anforderungen an Näherungsschalter für Sicherheitsfunktionen sind in DIN EN 60947-5-3 [16] festgelegt. Weitere Informationen und Hinweise zur Gestaltung von Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen gibt die Norm DIN EN ISO 14119 [20]

4 Anforderungen zur Vermeidung systematischer Fehler

4.1 Allgemeines

In der Sicherheitstechnik werden zwei Arten von Fehlern unterschieden (siehe Kap. 2): *systematische* und *zufällige* Fehler (Ausfälle).

Es ist das Ziel, durch entsprechendes Vorgehen bei Konstruktion und Prüfung von Sicherheitssystemen dafür zu sorgen, dass *systematische* Fehler nicht auftreten. Mit ihnen wird nach erfolgreichem Abschluss der Prüfungen und der Zulassung im praktischen Betrieb nicht gerechnet.

In den Grundanforderungen (Kap. 3) wird verlangt, dass es nur dann möglich sein darf, Röntgenröhre bzw. Röntgenstrahler zu betreiben, wenn das Schutzgehäuse vollständig geschlossen ist. Die Sicherheitsvorrichtung muss so konstruiert sein, dass sie in jeder Betriebssituation eine Gefährdung von Personen durch ionisierende Strahlung sicher verhindert. Dies lässt sich durch die folgenden Konstruktionsprinzipien erreichen:

- Durch Verwendung von Bauelementen hoher Zuverlässigkeit und durch Überdimensionierung,
- durch Schaltungsstrukturen, die gewährleisten, dass nicht der Ausfall eines Bauelementes zum Verlust der Sicherheitsfunktion der Sicherheitsvorrichtung als Ganzes führt und
- durch einfache, leicht nachvollziehbare Schaltungen und Software zur Vermeidung von Konstruktionsfehlern und zur Ermöglichung der effizienten Begutachtung.

Die praktische Realisierung der Sicherheitsvorrichtung weicht von der idealisierten Darstellung eines Schaltbildes ab und birgt noch weitere Fehlermöglichkeiten, verursacht durch unsachgemäße Ausführung (z. B. Kurzschlüsse zwischen Schaltungspunkten, die in der Realisierung räumlich dicht beieinander liegen). **Diese Art von möglichen Fehlern muss durch eine Augenscheinprüfung an einem Baumuster mit dem für die Serienfertigung vorgesehenen mechanischen und elektrischen Aufbau von einem Gutachter ausgeschlossen werden.** Soweit Fehlerquellen dieser Art aufgefunden werden, müssen sie vom Hersteller durch eine Nachbesserung eliminiert werden.

4.2 Grundlegende Konstruktionsprinzipien

4.2.1 Anforderung

Hardware und Software sind entsprechend dem Stand der Sicherheitstechnik zu konzipieren und zu erstellen (siehe Kap. 4.3 bis 4.13). Die Software und Hardware der Sicherheitsvorrichtung darf keinen Konstruktionsfehler enthalten, der in irgendeiner Situation, in der sich noch kein (Hardware-) Ausfall ereignet hat, zum Verlust der Sicherheitsfunktion führt.

Zur Vermeidung von einfacher Manipulation ist die DIN EN ISO 14119 [20] zu berücksichtigen sowie der Abschnitt 4.3.

4.2.2 Erläuterung

Es gelten die grundlegenden Anforderungen der DIN EN 62061 Abschnitt 6.11 bis 6.12 Sicherheitsschaltungen müssen so konstruiert sein, dass systematische Fehler (nach bestem Wissen) nicht vorhanden sind, dass zufällige Fehler, d. h. Ausfälle in der Hardware verglichen mit der Lebensdauer des Gerätes selten auftreten und die Schaltung auch bei Auftreten von zufälligen Fehlern so reagiert, dass keine Gefährdung auftritt. Ein wichtiger Konstruktionsgrundsatz ist dabei die Einfachheit der Schaltung und – falls vorhanden – der Software, denn sowohl der Konstrukteur als auch ein Gutachter müssen in der Lage sein, die Richtigkeit der Konstruktion nachzuweisen. Eine umfangreiche Zusammenstellung von Maßnahmen zur Verhinderung von Fehlern bei der Konstruktion befindet sich in [9], Teil 2, Anhang B (Hardware) und [9], Teil 3, Anhang A (Software).

4.2.3 Prüfung

Die Anforderung wird bei den Prüfungen nach 4.3 bis 4.13 mit geprüft**.**

4.3 Grundsätze bei der Wahl der Bauelemente

4.3.1 Anforderung

Es sind folgende drei Grundsätze bei der Wahl der Bauelemente einzuhalten:

1. hohe Qualität,
2. Überdimensionierung, Einhaltung von Montageregeln und Normen zur Verhinderung von Störbeeinflussungen und
3. Verwendung von Bauelementen mit garantiertem Ausfallverhalten in Schaltungen.

Die Grundsätze 1. und 2. dienen zur Verringerung der Ausfallwahrscheinlichkeit, der Grundsatz 3. zur Fehlerbeherrschung.

4.3.2 Erläuterung

Die Qualität eines technischen Gerätes hängt sehr von der richtigen Auswahl und Dimensionierung seiner Bauelemente ab. Bei einer Sicherheitsvorrichtung gilt dies umso mehr, da hier die Auswahl und Dimensionierung der Bauelemente sowie deren fachgerechte Montage die Fehlerwahrscheinlichkeit und damit die Sicherheit beeinflusst (siehe Anhang 3). Die Bauelementeauswahl muss unter dem Ziel der *Fehlervermeidung* in der Sicherheitsvorrichtung getroffen werden.

Bei Geräten des SIL 3 müssen auch Prinzipien der *Fehlerbeherrschung* berücksichtigt werden: Durch spezielle Schaltungsstrukturen können Ausfälle ermittelt und das Einschalten verhindert werden (siehe Kap. 4.4). Hierzu sind Bauelemente erforderlich, siehe [4] mit Verweis auf DIN EN 61508-4 [9], bei denen bestimmte Fehlerarten ausgeschlossen werden können. Standard-Bauelemente sind hier nicht geeignet, auch wenn sie die eigentliche Nutzfunktion genauso gut erfüllen würden (Beispiel: Verwendung zwangsgeführter Relais statt normaler, damit die Ausfallart „Öffner und Schließer gleichzeitig geschlossen“ nicht auftreten kann).

4.3.3 Prüfung

Die Qualität der Bauelemente wird durch Sichtprüfung der ausgeführten Schaltung beurteilt. Anhand der Datenblätter und Schaltpläne werden die richtige Dimensionierung und gegebenenfalls die Zuverlässigkeitskennwerte insbesondere der sicherheitskritischen Bauteile geprüft. Müssen Bauelemente zur Fehlerbeherrschung bestimmte Eigenschaften haben, so wird anhand der Datenblätter überprüft, ob die verwendeten Bauelemente diese tatsächlich besitzen.

4.4 Geeignete Schaltungsstrukturen

4.4.1 Anforderung

Die *Fehlerbeherrschung* muss als wichtiges Konstruktionsprinzip beachtet werden, d. h. die automatische Fehlererkennung und anschließende Betriebshemmung (Abschaltung der Hochspannung der Röntgeneinrichtung bzw. Verhinderung des Einschaltens der Hochspannung). Als Fehlerursache sind zufällige Hardware-Ausfälle anzusehen. Diese werden in Kapitel 5 behandelt. Beispiele für geeignete technische Lösungen sind in Kapitel 10 zu finden.

Bei Vollschutzgeräten muss die Sicherheitsfunktion (Abschaltung der Hochspannung) durch zwei voneinander unabhängige Vorrichtungen realisiert sein (siehe Kap. 3). Damit sollen systematische Fehler vermieden werden. Die Schaltung muss hierzu nicht unbedingt symmetrisch doppelt ausgeführt sein. „Unabhängig“ bedeutet lediglich, dass in der Schaltung *Fehler gemeinsamer Ursache* nicht möglich sind, die die Sicherheitsabschaltung verhindern (siehe Kap. 4.9).

4.4.2 Erläuterung

Die bei den hier betrachteten Röntgeneinrichtungen zu realisierende Sicherheitsfunktion ist sehr einfach: Die Energieversorgung des Röntgenstrahlers muss abgeschaltet werden, sobald Schutzgehäuse, Hauben, Türen oder Verkleidungen[1] geöffnet werden. Für diese Funktion sind nur wenige Bauelemente erforderlich. Die Zahl der an der Sicherheitsfunktion beteiligten Bauteile sollte nicht unnötig erhöht werden, damit die Fehlerwahrscheinlichkeit in der Sicherheitsvorrichtung niedrig bleibt und die Funktion der Schaltung leichter verstanden und geprüft werden kann.

4.4.3 Prüfung

Die Anforderung wird bei den Prüfungen nach 4.5 bis 4.13 mitgeprüft**.**

[1] Verkleidungen, die vom Betreiber geöffnet werden können.

4.5 Berücksichtigung aller Betriebssituationen

4.5.1 Anforderung

Der Röntgenstrahler bzw. die Röntgenröhre muss beim Öffnen des Schutzgehäuses in jeder Betriebssituation durch die Sicherheitsvorrichtung abgeschaltet werden. Hierbei sind neben den normalen auch ungewöhnliche Betriebssituationen zu berücksichtigen wie

- Einschalt- und Abschaltvorgang,
- Ausfall der Spannungsversorgung zu beliebigen Zeitpunkten und
- Fehlbedienungen durch den Betreiber des Gerätes

4.5.2 Erläuterung

Bei den hier behandelten Geräten sind verschiedene Betriebssituationen möglich. Die Sicherheitsanalyse muss neben den Phasen, in denen der Röntgenstrahler betrieben wird, auch alle anderen Phasen und Betriebszustände lückenlos berücksichtigen, da auch sie Einfluss auf die Sicherheit haben können. Die sichere Abschaltung des Vollschutzgerätes muss in allen ungewöhnlichen Betriebssituationen, u. a. auch bei Fehlbedienung, gewährleistet sein.

4.5.3 Prüfung

Für alle Betriebssituationen wird praktisch und/oder theoretisch an Hand der technischen Unterlagen (Schaltpläne) oder der Software die richtige Funktion der Sicherheitsvorrichtungen geprüft.

4.6 Vermeidung von unzulässigen Beeinflussungen durch physikalische Effekte

4.6.1 Anforderung

Die Sicherheitsvorrichtung muss robust gegen unerwünschte Beeinflussung ausgeführt sein (z. B. EMV-gerechtes Design, elektrisch reichlich dimensionierte Stromversorgung, Sicherstellung des Erhaltes von Fehlerinformationen). Die Einzelheiten werden u. a. in den folgenden Normen definiert:

- DIN EN 60947-5-1, Niederspannungsschaltgeräte, Steuergeräte und Schaltelemente, elektromechanische Steuergeräte [15];
- DIN EN 60204-1, Elektrische Ausrüstung von Maschinen [8];
- DIN EN 50178, Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln [17];
- DIN EN 60664, Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen [18];
- DIN EN 61000-6-2, Elektromagnetische Verträglichkeit (EMV) - Fachgrundnormen Störfestigkeit für Industriebereich [19].

4.6.2 Erläuterung

Zwar bilden die elektrische Schaltung und die Software der Sicherheitsvorrichtung den Kern der Betrachtungen. Es darf jedoch nicht außer Acht gelassen werden, dass diese Vorrichtung mehr oder weniger starken äußeren Einflüssen unterliegt, unter denen die

Sicherheit gewährleistet bleiben muss. Die Einflüsse lassen sich einteilen in physikalische und funktionell-schaltungstechnische, die durch andere Geräte oder Geräteteile hervorgerufen werden. Der Schutz gegen physikalische Einflüsse wird durch die vorstehend genannten Normen beschrieben. Unerwünschte funktionelle Beeinflussungen der Sicherheitsvorrichtung werden in den Kapiteln 4.7 und 4.8 behandelt.

4.6.3 Prüfung

Für alle Einflussgrößen wird die Prüfung gemäß der genannten Normen durchgeführt. Gegebenenfalls kann der Prüfer/Begutachter entscheiden, auf einzelne Prüfungen wie zum Beispiel den EMV-Test zu verzichten, wenn die verwendete Technologie die Erfüllung der Anforderungen sicherstellt.

4.7 Schutz gegen innere funktionelle Beeinflussung

4.7.1 Anforderung

Sind Geräteteile vorhanden, die selbst keine Sicherheitsfunktion erfüllen, so dürfen diese die Sicherheitsvorrichtung nicht beeinflussen können. Dies gilt auch, wenn in den *nicht* sicherheitsrelevanten Geräteteilen Ausfälle auftreten oder Software-Fehler enthalten sind. Die Sicherheitsvorrichtung und andere Geräteteile sollten sich in unterschiedlichen Baugruppen befinden und nur über wenige elektrisch gut entkoppelte Schnittstellen (galvanische Trennung) verbunden sein. Die Beeinflussungsmöglichkeit der Sicherheitsvorrichtung durch Software wird den Abschnitten 4.12.1 d), e), f) und 4.13.1 b), c) behandelt.

4.7.2 Prüfung

Das Gerät wird einer detaillierten Sichtprüfung unterzogen und die technische Ausführung der Konstruktion wird untersucht. Die technischen Daten der Trennelemente werden anhand der Datenblätter überprüft. Ist eine ausreichende Trennung der Sicherheitsvorrichtung von anderen Schaltungsteilen nicht gewährleistet, werden diese in die Sicherheitsprüfung mit einbezogen.

4.8 Schutz gegen äußere funktionelle Beeinflussung

4.8.1 Anforderung

Ist die Röntgeneinrichtung mit anderen Geräten über Schnittstellen verbunden, so dürfen die Sicherheitsfunktionen nicht über die Schnittstellen beeinträchtigt werden können. Dies kann z. B. durch galvanische Trennung in der Schnittstelle erreicht werden. Die Beeinflussungsmöglichkeit der Sicherheitsvorrichtung über die Schnittstellen durch Software wird im Abschnitt 4.13.1 f) behandelt.

4.8.2 Prüfung

Die technischen Daten der Trennelemente werden anhand der Datenblätter überprüft. Ist eine ausreichende Trennung der Sicherheitsvorrichtung an den Schnittstellen nicht gewährleistet, werden die an den Schnittstellen angeschlossenen Geräte in die Sicherheitsprüfung mit einbezogen. Die Prüfung muss – wenn erforderlich – durch praktische Simulation von Ausfällen an der Schnittstelle – wie z. B. Kurzschlüssen zwischen beliebigen Steckerstiften – ergänzt werden.

4.9 Vermeidung von Fehlern gemeinsamer Ursache

4.9.1 Anforderung

Das Gerät muss so konstruiert sein, dass ein beliebiger Ausfall in irgendeinem Bauelement der Sicherheitsvorrichtung nicht weitere Fehler nach sich zieht (Folgefehler), die gemeinsam zu einem Verlust der Sicherheitsfunktion führen.

4.9.2 Erläuterung

Es gelten hier insbesondere die Abschnitte 6.4.1 bis 6.4.2 der DIN EN 62061.

Fehler gemeinsamer Ursache müssen berücksichtigt werden, wenn die Wahrscheinlichkeit für das Auftreten eines solchen Fehlers von Bedeutung ist.

Folgefehler sind Fehler, die aufgrund physikalischer Effekte zwangsläufig (deterministisch) aus dem ersten Fehler resultieren, nicht Fehler, die statistisch unabhängig zufällig zu dem ersten Fehler hinzukommen. Lässt sich ein Folgefehler nicht prinzipiell durch konstruktive Maßnahmen ausschließen, so muss abgeschätzt und entschieden werden, ob das damit verbundene Risiko akzeptabel ist. Das folgende Beispiel beschreibt einen nicht akzeptablen Folgefehler.

> **Beispiel 4-1:** Ein Kurzschluss (erster Fehler) verursacht das Verschweißen von zwei redundanten, in Reihe geschalteten Schließern (Folgefehler), die zur sicheren Abschaltung dieses Stromkreises vorgesehen waren. Verhinderung: Begrenzung des maximalen Stromes durch Widerstände oder Sicherungen.

4.9.3 Prüfung

Im Rahmen der Einzelfehleranalyse wird überprüft, ob sich ein Einzelfehler gefährlich auswirken kann. Jeder Einzelfehler wird daraufhin untersucht, ob er Folgefehler verursachen kann. Dies geschieht anhand der Datenblätter der Bauelemente und anhand des Schaltplanes. Können Folgefehler auftreten, wird die Fehleranalyse auch für die Kombination aus Erst- und Folgefehler durchgeführt oder die Schaltung wird so geändert, dass der Folgefehler nicht auftreten kann.

4.10 Vermeidung des Verlustes der Redundanz aufgrund von Ausfällen

4.10.1 Anforderung

Das Gerät muss so konstruiert sein, dass ein beliebiger Ausfall in irgendeinem Bauelement der Sicherheitsvorrichtung nicht dazu führt, dass ein weiterer unabhängiger Fehler die redundanten Kanäle oder Komponenten *gleichartig beeinflusst,* so dass die Sicherheitsvorrichtung den Röntgenstrahler bzw. die Röntgenröhre nicht mehr abschalten kann.

4.10.2 Erläuterung

Durch Verlust der Redundanz kann sich bereits ein weiterer Fehler so auswirken wie zwei oder mehrere gleichzeitig auftretende Fehler und damit zur Gefährdung führen.

Wird der Fehler, der den Verlust der Redundanz bewirkt, nicht aufgedeckt (d. h. nicht automatisch von der Sicherheitsschaltung erkannt), so muss mit der Kombination aus diesem ersten Fehler und beliebigen anderen gerechnet werden. Gemäß den Anforderungen nach Kap. 5.7 muss die Schaltung so ausgelegt sein, dass außer dem Fehler, der zum Verlust der Redundanz führte, noch mindestens zwei weitere unabhängige Fehler hinzukommen müssen, damit es zu einem Verlust der Sicherheitsfunktion kommt.

Um die Schaltungsstruktur und die Sicherheitsanalyse nicht unnötig zu verkomplizieren ist anzustreben, durch konstruktive Maßnahmen in der Schaltungsstruktur und durch die praktische Ausführung der Schaltung zu verhindern, dass die Redundanz durch Ausfälle überhaupt verloren gehen kann. Zwei Beispiele sollen zeigen, wie Verlust der Redundanz vermieden werden kann:

Beispiel 4-2: Ein Kurzschluss zwischen den Wicklungsanschlüssen von zwei redundanten Relais (Schützen), die die redundanten Schließer im Energiekreis betätigen, wird nicht erkannt. Führt ein zweiter Fehler dazu, dass einer der beiden Schaltkreise zur Steuerung der Relais nicht mehr abschalten kann, wird die Wicklung des zweiten Relais über den Kurzschluss mit erregt und die Spannungsversorgung kann nicht mehr abgeschaltet werden. Es käme zur Gefährdung. Der Verlust der Redundanz muss verhindert werden, indem die Verdrahtung so ausgeführt wird, dass dieser Kurzschluss nicht auftreten kann.

Das folgende Beispiel zeigt einen zu vermeidenden Konstruktionsfehler in einer Digitalschaltung:

Beispiel 4-3: Die Signale, die die Überwachungskontakte eines Schützes einer Vergleicherschaltung zuführen, werden über zwei Halbleiter-Gatter geführt, die sich in einem Bauelement befinden. Z. B. muss innerhalb von integrierten Schaltungen mit Kurzschlüssen zwischen beliebigen Punkten gerechnet werden, auch zwischen den beiden Ausgängen der Gatter. Die Redundanz wäre nach einem derartigen Ausfall nicht mehr gegeben und das Nichtöffnen eines Schließers des Schützes könnte nicht mehr erkannt werden.

Der Verlust der Redundanz lässt sich verhindern, indem die betreffenden redundanten Signale nicht in Gattern ein und desselben Bauelementes, sondern in verschiedenen Bauelementen verarbeiten werden. In einem Vergleicher müssen die Signale beider Kanäle allerdings auf ein Bauelement geführt werden. Deshalb ist eine doppelte Ausführung der Vergleicher in verschiedenen Bauelementen notwendig.

Weitere Maßnahmen zur Verhinderung des Verlustes der Redundanz sind z. B. die Wahl ausreichend großer Leiterbahnabstände, so dass keine Kurzschlüsse auftreten können, oder die Führung redundanter Signale nicht über benachbarte Stifte in Steckverbindern.

4.10.3 Prüfung

Im Rahmen der Einzelfehleranalyse, bei der überprüft wird, dass sich kein Einzelfehler gefährlich auswirken kann, wird parallel bei jedem Fehler untersucht, ob er den Verlust der Redundanz zur Folge hat. Dies geschieht anhand der Datenblätter der Bauelemente und anhand des Schaltplanes. Wird der mögliche Verlust der Redundanz festgestellt, muss die Schaltung so geändert werden, dass dies nicht mehr möglich ist.

4.11 Schutz gegen den Verlust der Redundanz aufgrund von Störungen

4.11.1 Anforderung

Redundante Schaltungsteile, Baugruppen oder Programm-Module dürfen nicht durch (elektrische, elektromagnetische usw.) Störungen ihre Redundanz verlieren, so dass die Sicherheitsvorrichtung Fehler nicht mehr erkennen und damit die Hochspannung des Röntgenstrahlers nicht mehr abschalten kann.

4.11.2 Erläuterung

Durch elektromagnetische und andere physikalische Störungen kann es zum Verlust der Redundanz mit denselben Konsequenzen wie in Kapitel 4.10 beschrieben kommen.

Beispiel 4-4: Die folgende Konstruktion ist problematisch: Eine Schaltung besitzt zwei redundante elektronische Kanäle zur Erkennung des Abfalls von zwei Schließern. Durch eine schlecht ausgelegte Spannungsversorgung wird beim Abschalten der Erregung des Ausgangsschützes ein fehlerhafter Impuls auf beiden Signalleitungen der Schaltung zur Fehlererkennung erzeugt. Dieser Impuls täuscht das Öffnen der Schließer nur vor. Öffnen diese irgendwann einmal wirklich nicht, erkennt die Schaltung dies nicht.

Eine Verhinderung des Redundanzverlustes ist z. B. durch Überdimensionierung von Spannungsversorgungen, Versorgung von redundanten Schaltungsteilen durch getrennte Spannungsversorgungen und EMV-gerechtes Leiterplatten-Design möglich.

4.11.3 Prüfung

Das Layout von Leiterplatten und die Verdrahtung des Gerätes werden einer detaillierten Sichtprüfung unterzogen. Falls es der Prüfer als erforderlich ansieht, kann er Messungen an der Stromversorgung und im Massesystem vornehmen, um die gegenseitige Beeinflussung der Schaltungsteile erkennen zu können. Ein normaler EMV-Test ist nur auf die Nutzfunktionen des Gerätes ausgerichtet und wird einen möglichen Redundanzverlust nicht aufdecken. Der Schaltplan wird analysiert und die Dimensionierung von Bauelementen, die zur Entstörung und Entkopplung dienen, wird kontrolliert.

4.12 Allgemeine Software-Konstruktionsregeln

4.12.1 Anforderungen

Werden sicherheitsrelevante Funktionen durch Software realisiert, so muss die verwendete Programmiersprache vollständig und eindeutig definiert sein. Geeignete Sprachen werden z. B. in DIN EN 61131-3 [12] genannt. Als nicht geeignet gilt u. a. C/C++ [13] sofern der Sprachumfang nicht durch Programmierregeln eingeschränkt ist. Durch Einhaltung der folgenden Regeln a) bis h) kann auch eine nicht ausdrücklich für Sicherheitsanwendungen konzipierte Sprache verwendet werden.

a) Als unsichere oder fehleranfällige Konstrukte im Kontrollfluss, die vermieden werden müssen, gelten:
   - Verwendung von Interrupts, insbesondere geschachtelte Interrupts (es sei denn, aus der Stack-Untersuchung (siehe d)) ergibt sich die Unbedenklichkeit dieser Konstruktion.)
   - Berechnete Sprünge
   - Rekursionen
   - Berechneter Wert für Schleifen-Ende-Bedingung
   - Fließkomma-Arithmetik (wenn in Laufzeitbibliotheken mit nicht offengelegtem Quellcode realisiert)

b) Als unsichere oder fehleranfällige Datenkonstrukte gelten:
   - Dynamische Speicher-Verwaltung
   - Globale Variable
   - Indirekte Adressierung
   - Rekursive Datenstrukturen
   - Mehrfach-Typisierung von Variablen (Varianten, unions, ...)
   - Typumwandlungen (casts)
   - Fehlende Initialisierung von Variablen

c) Funktionen aus Laufzeitbibliotheken (z. B. Stringoperationen, Fließkomma-Arithmetik, trigonometrische Funktionen, ...) dürfen nicht verwendet werden, wenn sie nicht denselben Prüfungen wie die eigentlichen Programme unterzogen werden können (Quellcode muss offengelegt sein). Kann nachgewiesen werden, dass die eingesetzte Version der Laufzeitbibliothek jahrelang in hoher Stückzahl unverändert im Einsatz war, kann von Betriebsbewährtheit ausgegangen werden und die Prüfung der Bibliotheks-Funktionen ist nicht erforderlich.

d) Eine besondere Gefahr stellt der Stack- oder Heap-Überlauf dar, weil er nicht einfach während der Programmierung vorherzusehen ist (deshalb: Vermeidung von Interrupts und Rekursionen). **Es ist eine worst-case Analyse für die Stack-/Heap-Nutzung durchzuführen und nachzuweisen, dass ein Überlauf nicht stattfinden kann.** Interrupt-Steuerung, dynamische Speicher-Verwaltung usw. (siehe c)) können nur akzeptiert werden, wenn dieser Nachweis gelingt.

e) Das Zeitverhalten muss analysiert werden. Es muss bei zeitkritischen sicherheitsrelevanten Funktionen nachgewiesen werden, dass alle sicherheitsrelevanten Funktionen immer rechtzeitig vom Programm ausgeführt werden und dass die Reaktionszeit der sicherheitsrelevanten Programme einen sicheren Betrieb erlaubt.

f) Werden außer den sicherheitsrelevanten Funktionen auch andere Funktionen von der Software realisiert, so muss eine Trennung in einen sicherheitsrelevanten und einen nicht sicherheitsrelevanten Teil erfolgen. Es muss nachgewiesen werden, dass der nicht sicherheitsrelevante Teil der Software den relevanten Teil nicht beeinflussen kann.

g) Der Benutzer der Röntgeneinrichtung muss in der Lage sein, die Identität des sicherheitsrelevanten Programms **vor oder während** des Betriebs festzustellen (Versionsnummer, Checksumme).

h) Die Programme und Datenstrukturen müssen gut dokumentiert werden (zum Zweck der fehlerfreien Wartung und zur Prüfung), z. B. durch
   - Verbale oder formale grafisch unterstützte Gesamtbeschreibung des Programm-Systems
   - Kommentare im Quellcode: Programm-Kopf mit Daten-Eingang / -Ausgang, Funktion des Moduls, Seiteneffekte, Sicherheitsrelevanz ja/nein, Stand (Datum), Änderungshistorie, Autor
   - Ausreichende Kommentierung von Anweisungen im laufenden Quellcode
   - Beschreibung von Datenstrukturen, Data-Dictionary

4.12.2 Erläuterung

Bei der Steuerung von Sicherheitsvorrichtungen durch Software sind einige Besonderheiten zu beachten. Anders als z. B. bei Relaisschaltungen, bei denen eine überschaubare Zahl von Schaltzuständen geprüft werden muss, können in Software-Lösungen nahezu unbegrenzt viele Zustände auftreten. Selbst wenn der Programmierer sehr restriktive Programmierregeln einhält, müssen noch weitere Sachverhalte über die Umgebung der Software bekannt sein, z. B. Eigenschaften von Software-Entwicklungswerkzeugen oder des Betriebssystems, unter dem die sicherheitsrelevante Software läuft. **Im Allgemeinen ist der Prüfaufwand für software-gesteuerte Vorrichtungen um ein Vielfaches höher als für konventionelle Lösungen. Insbesondere für komplexe Programm-Systeme, in denen Sicherheitsfunktionen realisiert sind, kann der Prüfaufwand unvertretbar hoch sein. Diese Gründe sprechen dafür, nach Möglichkeit auf Software-Lösungen für die Sicherheitsvorrichtung ganz zu verzichten, zumal die**

typische Funktionalität bei den betrachteten Röntgeneinrichtungen (Überwachung einer Schutzhaube) im Grunde trivial ist.

Für andere Funktionen der Röntgeneinrichtung kann eine Software-Steuerung sicher sinnvoll sein. Der aus diesem Grunde vorhandene Mikroprozessor sollte aber nicht dazu verleiten, die Sicherheitsfunktionen durch Software zu erledigen. Wird dieser Weg dennoch gewählt, so muss nicht nur die Richtigkeit der sicherheitsrelevanten Programme selbst sondern auch die Unmöglichkeit von Fehlfunktionen in der Umgebung der eigentlichen Programme nachgewiesen werden.

Das Prüfziel ist der Nachweis, dass die sicherheitsrelevante Software keine Fehler enthält (Anforderung gemäß Kap. 4.2). Dieser Nachweis ist meist schwierig und selbst fehleranfällig. Um Fehler bei der Konstruktion und Prüfung zu vermeiden, muss die Software so einfach und klar wie möglich konstruiert werden. Ein Grundsatz der folgenden Software-Anforderungen ist es, durch Reduzierung der Komplexität der Programmiersprache dem Programmierer wie dem Prüfer das Verständnis der Programm-Logik zu erleichtern und die Fehlerwahrscheinlichkeit zu minimieren. Die Nachvollziehbarkeit der Software ist die Grundlage für die Vertrauenswürdigkeit der Prüfaussage. **Die Software legt wesentlich die Eigenschaften des Bauartmusters fest. Deshalb ist die Dokumentation der Software inklusive des Quellcodes bei der Bauartprüfung in der PTB zu hinterlegen.**

Die Einhaltung der folgenden Programmierregeln bewirkt eine weitgehend sequentielle Programm-Struktur und einen sequentiellen zeitlichen Programm-Ablauf, was das Verständnis bei der Prüfung sehr erleichtert. Besonderes Gewicht wurde auch auf die Reduzierung der Einwirkungen der Umgebung auf das sicherheitsrelevante Programm gelegt.

Eine Zusammenstellung von Maßnahmen zur Verhinderung von Fehlern bei der Konstruktion der Software befindet sich in [9], Teil 3, Anhang A und zur Qualitätssicherung der Softwareerstellung in [9], Teil 3, Anhang B sowie [10,11].

4.12.3 Prüfung

Die Einhaltung der Regeln wird an Hand des Quellcodes geprüft.

4.13 Funktionelle Software-Anforderungen

4.13.1 Anforderungen

a) Die Röntgeneinrichtung darf nur in den betriebsfähigen Zustand gehen, wenn das für diesen Zweck zugelassene sicherheitsrelevante Programm aktiv ist und die sicherheitsrelevanten Funktionen ausführt. Werden während des Betriebs der Röntgeneinrichtung die sicherheitsrelevanten Funktionen aufgrund eines Ereignisses nicht mehr ausgeführt, so muss die Sicherheitsvorrichtung die Röntgeneinrichtung unverzüglich automatisch abschalten.

b) Es muss untersucht und nachgewiesen werden, dass das Betriebssystem des Rechners als Umgebung für das zugelassene sicherheitsrelevante Programm geeignet ist. Insbesondere dürfen die sicherheitsrelevanten Funktionen nicht unterdrückt werden und müssen in jeder Situation zeitgerecht ausgeführt werden können.

c) Es muss untersucht und nachgewiesen werden, dass andere Programme, die sich unter Umständen auch auf dem Rechner befinden, das sicherheitsrelevante Programm in keiner Weise beeinflussen, insbesondere die sicherheitsrelevanten Funktionen nicht unterdrücken oder unzulässig verzögern können. Der Benutzer darf nicht die Möglichkeit haben, die sicherheitsrelevanten Programm-Funktionen außer Kraft zu setzen oder zu beeinflussen.

d) Das sicherheitsrelevante Programm muss sich selbst und eventuell gespeicherte Parameter und Daten auf Fehler untersuchen. Nur wenn Programme und Daten fehlerfrei (unverfälscht) sind, darf die Röntgeneinrichtung eingeschaltet werden können.

e) Das sicherheitsrelevante Programm muss prüfen, ob alle für den Betrieb notwendigen Programm-Komponenten, Parameter und Daten vorhanden sind. Nur wenn nichts fehlt, darf es die sicherheitsrelevante Funktion aufnehmen bzw. ausführen.

f) Die Datenübertragung zwischen einem externen Rechner und der Sicherheitsvorrichtung der Röntgeneinrichtung muss sicher sein. Es müssen geeignete Datenübertragungsprotokolle zum Einsatz kommen. Übertragungsfehler dürfen nicht zu einem unsicheren Zustand führen [14]. Die Datenübertragung zu nicht sicherheitsrelevanten Teilen der Röntgeneinrichtung muss nicht gegen Übertragungsfehler gesichert werden.

4.13.2 Prüfung

Die Einhaltung der Anforderungen wird an Hand des Quellcodes geprüft.

5 Anforderungen zur Vermeidung zufälliger Fehler

5.1 Allgemeines

In Abschnitt 4 wurden systematische Fehler und ihre Vermeidung behandelt. Die Fehler der zweiten Art, die zufälligen Fehler, können selbst bei perfekter Konstruktion nicht gänzlich verhindert werden. Durch die im Folgenden erläuterten Konstruktionsprinzipien soll aber erreicht werden, dass Fehler dieser Art keine gefährlichen Auswirkungen haben können.

Die Beherrschung der zufälligen Fehler in der Sicherheitsvorrichtung erfordert einen durchdachten Schaltungsentwurf und meist mehr Aufwand als für die reine Funktion erforderlich. In den einschlägigen Normen werden abgestufte Sicherheitsanforderungen gestellt, die an den jeweiligen Anwendungsbereich oder das Schadensrisiko angepasst sind. Die hier gestellten Anforderungen richten sich nach den Anforderungen der RöV. Die Möglichkeit der Risikoabschätzung und Festsetzung des Sicherheits-Integritätslevels (SIL) nach DIN EN 62061 bei der Betrachtung von sicherheitsbezogenen Steuerungsfunktionen ist zu nutzen. Alternativ können spezielle Anforderungen für sicherheitsbezogene Teile von Steuerungen mit programmierbaren elektronischen Systemen auch nach DIN EN ISO 13849-1 zu behandelt werden.

5.2 Vermeidung des Verlustes der Sicherheitsfunktion durch Einzelfehler (Abschnitte 6, 7 der DIN EN 62061)

5.2.1 Anforderung

Die Schaltung der Sicherheitsvorrichtung muss so aufgebaut werden, dass kein einzelner Ausfall bei irgendeinem Bauelement zum Verlust der Sicherheitsfunktion führt, d. h. dass – solange kein weiterer Ausfall hinzukommt – der Röntgenstrahler bzw. die Röntgenröhre bei Öffnen des Schutzgehäuses in jeder Betriebssituation trotz dieses Ausfalls durch die Sicherheitsvorrichtung abgeschaltet und/oder nach Abschaltung nicht wieder eingeschaltet werden kann (Betriebshemmung).

5.2.2 Erläuterung

Sicherheitsbezogene Teile von Steuerungen müssen so gestaltet werden, dass ein einzelner Fehler in einem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt. Diese Anforderung ist nach Röntgenverordnung bei Vollschutzgeräten durch Redundanz in der Sicherheitsvorrichtung zu realisieren. Diese unabhängigen Vorrichtungen müssen nicht gleichartig sein, sondern können auch in unterschiedlichen Technologien realisiert sein.

> **Beispiel 5-5**: (siehe Abbildung 3, Kap. 10.2): Der Hochspannungsgenerator der Röntgenröhre wird über in Reihe geschaltete Relais-Kontakte geschaltet. Ein Fehler kann bewirken, dass die Kontakte eines Relais (z. B. K2.1s) nicht mehr öffnen. Dieser Fehler ist nicht gefährlich, da das zweite Relais die Hochspannung noch abschaltet. Der zwangsgeführte Kontakt K2.1o schließt nicht, wenn K2.1s nicht öffnet. Dadurch wird der Kondensator C während der Abschaltphase nicht aufgeladen und es kommt zur Betriebshemmung.

Ist ein Mikrocontroller Bestandteil der Sicherheitsvorrichtung, so sind sehr viele Ausfallarten möglich. Die Auswirkungen können vielfach nicht vorhergesehen werden. Die Software muss deshalb den Mikrocontroller überwachen, so dass die Ausfalloffenbarung und Betriebshemmung möglich wird.

Hardwarefehler (Ausfälle) in Mikrocontrollern und in Programm- und Datenspeichern sicherheitsrelevanter Software müssen erkannt werden und zur Betriebshemmung führen. Dies kann z. B. realisiert werden durch:

- Programmlauf-Überwachung durch Watchdog,
- Überwachung, dass alle sicherheitskritischen Punkte im Programmcode rechtzeitig und in der richtigen Reihenfolge passiert werden (Programm-Durchlaufzähler),
- regelmäßig wiederholte Checksummenkontrolle des Programmcodes,
- Überwachung des korrekten Stack-Zeigerstandes,
- Kontrolle von Wertebereichsgrenzen,
- doppelte bzw. redundante Speicherung,
- Test der varianten und der invarianten Speicher beim Einschalten und/oder zyklisch.

Eine weitere akzeptable technische Lösung ist die zweikanalige Ausführung der Rechnerschaltung, wobei Berechnungsergebnisse und Programmstände beider Kanäle regelmäßig miteinander verglichen werden und bei Abweichungen eine Fehlererkennung und Betriebshemmung erfolgt.

5.2.3 Prüfung

Das Schaltbild wird analysiert. Jedes Bauelement wird registriert und es werden nacheinander alle angegebenen Fehlerarten angenommen. Der Prüfer berechnet, schätzt oder simuliert (mit speziellen Programmen) das Verhalten der Schaltung unter dem Umstand des jeweils angenommenen Fehlers und stellt fest, ob eine Gefährdung eintritt. Manche Fehler können auch praktisch durch Ersatz, Überbrückung oder Unterbrechung von Bauelementen simuliert werden, so dass sich die Auswirkung des Fehlers direkt beobachten lässt.

5.3 Fehlererkennung und Betriebshemmung

5.3.1 Anforderung

Die Sicherheitsvorrichtung nach DIN EN 62061 Abschnitt 6.3.2 bis 6.3.3 kann die Fehlererkennung zum Zweck der Betriebshemmung entweder

- durch eine Schaltung unter Ausnutzung garantierter physikalischer (mechanischer, elektrischer) Eigenschaften der verwendeten Bauelemente oder
- durch eine logische Einheit realisieren. Die Software einer derartigen Einheit muss die Anforderung gemäß Kapitel 4.12 und 4.13 erfüllen.

5.3.2 Erläuterung

Wann immer in angemessener Weise durchführbar, muss der einzelne Fehler bei oder vor der nächsten Anforderung der Sicherheitsfunktion erkannt werden.

Diese Anforderung für die Erkennung einzelner Fehler bedeutet nicht, dass alle Fehler erkannt werden. Daher kann die Anhäufung unentdeckter Fehler zu einem unbeabsichtigten Ausgangssignal und zu einem gefährlichen Zustand an der Maschine führen. Typische Beispiele für durchführbare Maßnahmen zur Fehlererkennung sind die zwangsgeführten Relaiskontakte oder die Überwachung von redundanten elektrischen Ausgängen.

Dieses Systemverhalten lässt zu, dass:

- bei Auftreten eines einzelnen Fehlers die Sicherheitsfunktion immer erhalten bleibt;
- einige, aber nicht alle Fehler erkannt werden;
- die Anhäufung unerkannter Fehler zum Verlust der Sicherheitsfunktion führen kann.

„Wann immer in angemessener Weise durchführbar“ bedeutet, dass die erforderlichen Maßnahmen zur Fehlererkennung und der Umfang, in dem diese einbezogen werden, hauptsächlich von den Folgen eines Ausfalls und von der Wahrscheinlichkeit des Auftretens dieses Ausfalls innerhalb der Anwendung abhängig sind. Die verwendete Technologie beeinflusst die Möglichkeiten der Einbeziehung der Fehlererkennung.

Dieser Abschnitt der Norm beinhaltet die Forderung der Fehlererkennung und Betriebshemmung, die in den folgenden Kapiteln 5.4 bis 5.7 für Vollschutzgeräte im Sinne der RöV interpretiert wird (gemäß Kapitel 3).

Anmerkung: Im Allgemeinen ist es möglich, Schaltungsteile hinsichtlich der Fehleranalyse zu gruppieren und Auswirkungen von allen Ausfällen, die innerhalb dieser Gruppe von Bauelementen auftreten können, zusammenzufassen zu fehlerhaften Spannungspegeln an bestimmten Schaltungspunkten. Beispielsweise werden bei der Analyse eines logischen Gatters nicht die Ausfallarten jedes einzelnen Halbleiterelementes

betrachtet, sondern es werden nur 3 fehlerhafte Ausgangspegel stellvertretend für alle möglichen inneren Fehlerzustände angenommen. Genauso kann bei diskret aufgebauten Schaltungen verfahren werden.

5.3.3 Prüfung

Für alle Betriebssituationen wird praktisch und/oder theoretisch an Hand der technischen Unterlagen (Schaltung) die richtige Funktion der Sicherheitsvorrichtungen geprüft. Darin eingeschlossen ist die Prüfung des Quellcodes der Software, wenn das technische Konzept einen Computer oder Mikrocontroller enthält. In Verbindung mit der in 5.2.3 beschriebenen Prüfung wird gleichzeitig untersucht, ob die betreffenden Fehler zu einer Betriebshemmung führen. Hierzu vollzieht der Prüfer entweder die Schaltungsfunktion nach oder er analysiert die entsprechenden Stellen in der Software.

5.4 Ausfalloffenbarungszeit und Betriebshemmung

5.4.1 Anforderung

Die Erkennung eines Ausfalls (Hardware-Fehlers) muss innerhalb kurzer Zeit nach dessen Auftreten erfolgen und sofort oder spätestens beim Versuch, die Hochspannung der Röntgeneinrichtung erneut einzuschalten, zu einer Betriebshemmung führen. Die Zeitspanne bis zum Eintreten der Betriebshemmung gilt als kurz, wenn die Wahrscheinlichkeit für das Auftreten eines weiteren zufälligen Fehlers innerhalb dieser Zeitspanne vernachlässigbar klein ist.

Logische Einheiten zur Fehlererkennung müssen kontinuierlich oder automatisch in regelmäßigen Abständen und vor jedem Einschalten der Röntgeneinrichtung die zu überwachenden Bauelemente prüfen.

Beispiel 5-7: Ein Schaltungs- und Programmkonzept, mit dem eine sichere Betriebshemmung bei einem Fehler im Mikrocontroller zu erreichen ist, ist die Dynamisierung der Ausgangssignale. Ein Relais, das zur Betriebshemmung sicher abgeschaltet werden muss, wird nicht einfach direkt mit dem Ausgangs-Port des Mikrocontrollers verbunden und durch Gleichspannung gesteuert. Vielmehr wird an bestimmten Punkten im Programm, die nur bei korrektem Ablauf erreicht werden, das Ausgangssignal umgeschaltet, so dass eine Wechselspannung entsteht. Diese Wechselspannung wird über einen Transformator geführt und gleichgerichtet und erst die gleichgerichtete Spannung schaltet das Relais. Mit dieser Maßnahme können die typischen und häufigen „Stuck-at-one-fault“ oder „Stuck-at-zero-fault" die Betriebshemmung nicht verhindern. Ein „Stuck-at-fault" muss seine Ursache nicht unbedingt in der Hardware des Ausgangs-Ports haben, sondern kann durch fehlerhaften Programmablauf hervorgerufen werden, der von anderen Hardwareausfällen in der CPU verursacht wurde.

5.4.2 Erläuterung

Für Fehler, deren Auftreten nicht wegen anerkannter Betriebsbewährtheit der Komponente ausgeschlossen werden kann, und für die **kein** Ausfalloffenbarungsmechanismus existiert, muss die gesamte Lebensdauer des Gerätes als Zeitspanne angenommen werden[2]. Schon bei einfachen Schaltungen kann dies zu aufwändigen Analysen führen. In diesen Fällen wird als Abschätzung bei der Analyse angenommen, dass dieser Fehler mit Sicherheit eintritt (ungünstigster Fall). Nach Kap. 5.7 ist die Sicherheitsschaltung nur dann in Ordnung, wenn noch mindestens zwei weitere Fehler zu diesem ersten nicht offenbarten hinzukommen müssen, bevor es zur Gefährdung kommt.

[2] Die Eintrittswahrscheinlichkeit eines Fehlers wird abgeschätzt durch das Produkt aus der (vom Hersteller des betreffenden Elementes angegebenen) *Ausfallrate* und der voraussichtlichen Lebenszeit des Gerätes. Bei Baugruppen muss dieser Wert für jedes enthaltene Bauelement berechnet werden; anschließend werden alle diese Werte summiert und ergeben einen Schätzwert für die Ausfallwahrscheinlichkeit der Baugruppe.

5.4.3 Prüfung

Der Prüfer analysiert die Schaltung und berechnet oder schätzt unter Berücksichtigung der in 5.2.3 und 5.3.3 gewonnenen Erkenntnisse, wie lang die Ausfalloffenbarungszeit zwischen Auftreten des Fehlers und Betriebshemmung ist. Erfolgt die Betriebshemmung nicht unmittelbar, muss er im Einzelfall entscheiden, ob der Fehler wegen 5.7 nicht unbedingt erkannt werden muss bzw. ob die Ausfalloffenbarungszeit kurz genug ist. Hierbei berücksichtigt er die Zuverlässigkeit des Bauelementes und die Auswirkung des Fehlers.

5.5 Statusanzeige

5.5.1 Anforderung

Dem Bediener muss der Betriebszustand der Röntgenröhre angezeigt werden (z. B. "Röntgenröhre in Betrieb", "Betriebshemmung", usw.

5.5.2 Erläuterung

Die Anzeige des Betriebszustands der Röntgenröhre an sich stellt noch keine Ausfalloffenbarung im Sinne der Kapitel 5.3 und 5.4 dar. Es ist im Rahmen eines sicheren Betriebs jedoch unerlässlich, dem Bediener den Zustand der Sicherheitsvorrichtung anzuzeigen.

5.5.3 Prüfung

Prüfung des Schaltplans und Inaugenscheinnahme des Gerätemusters im Rahmen der Bauartprüfung.

5.6 Beibehaltung einer Betriebshemmung

5.6.1 Anforderung

Ist ein Fehler einmal erkannt worden, darf die Sicherheitsvorrichtung auch bei Hinzutreten weiterer Fehler oder Störungen (z. B. leitungsgebundene oder elektromagnetische) ein Einschalten des Röntgenstrahlers bzw. der Röntgenröhre nicht wieder zulassen, bis der Fehler behoben worden ist. Insbesondere eine logische Einheit zur Fehlererkennung muss die Information des erkannten Fehlers sicher und redundant über längere Zeiträume bei abgeschalteter Spannungsversorgung speichern können und bei jeder (versuchten) Inbetriebnahme auswerten.

5.6.2 Prüfung

Für alle Betriebssituationen wird praktisch und/oder theoretisch an Hand der technischen Unterlagen (Schaltung) und des Quellcodes der Software geprüft, ob die Betriebshemmung beibehalten wird.

5.7 Bedingungen für Verzicht auf Fehlererkennung

5.7.1 Anforderung

Die Auswahl, für welche Fehler eine Erkennung durch die Schaltungsstruktur gemäß Kapitel 5.3 realisiert wird, darf nicht willkürlich getroffen werden. Folgende Fehler müssen **nicht unbedingt** durch die Sicherheitsvorrichtung erkannt werden:

- zufällige Fehler, die erst zu einer Gefährdung führen, wenn mindestens ***zwei*** *weitere statistisch unabhängige zufällige Fehler* hinzukommen oder bereits vorhanden sind, oder
- zufällige Fehler, die aufgrund langjähriger Erfahrung mit dem betreffenden Bauelement (anerkannter Betriebsbewährtheit) nicht angenommen werden müssen.

Werden Fehler nicht mittels einer Schaltung detektiert, die den Anforderungen der Kapitel 5.3 und 5.4 entspricht, so sind sie in der Dokumentation der Sicherheitsvorrichtung zu nennen und es ist zu begründen, warum auf eine Erkennung verzichtet wurde.

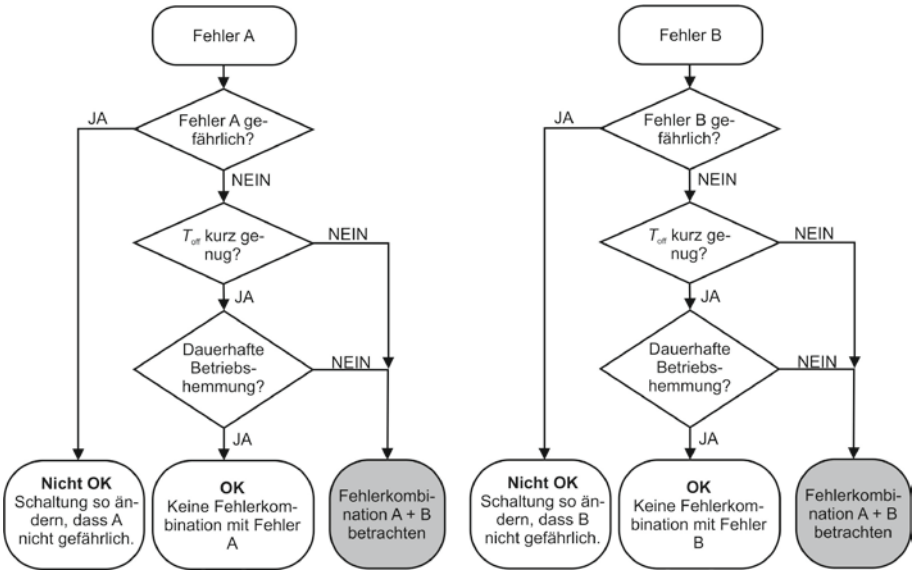


Abbildung 1a: Erkennung von Fehlern, die nicht zur Betriebshemmung führen müssen (T_{off} – Ausfalloffenbarungszeit). Fortsetzung des Laufplans für den Fall „Fehlerkombination A + B betrachten“ in Abbildung 1b.

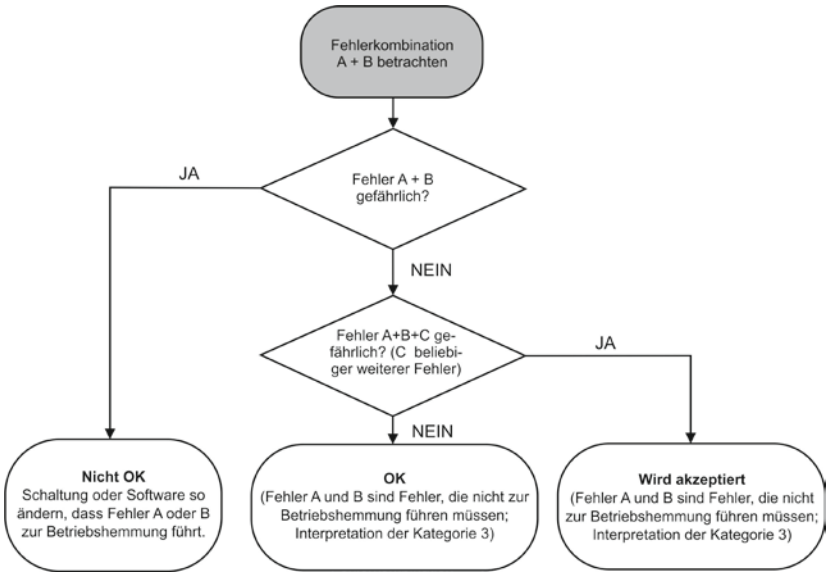


Abbildung 1b: Fortsetzung der Abb. 1a.

5.7.2 Prüfung

Der Prüfer verwendet die Liste der in 5.2.3 registrierten Fehler und betrachtet diejenigen, die nicht zur Betriebshemmung führen. Nun kombiniert er alle Fehlerarten aller Bauelemente dieser Liste paarweise miteinander und betrachtet die Auswirkung der Fehlerkombination. Die Kombination aus zwei Fehlerarten darf sich noch nicht gefährlich auswirken. Ein Versagen der Sicherheitsvorrichtung darf erst beim Hinzukommen eines dritten Fehlers möglich sein (siehe Abbildung 1).

Bei den meisten Fehlerkombinationen ist sofort ersichtlich, dass sie nicht gefährlich sind. Aber bei Fehlerkombinationen in Bauteilen, die funktionell zusammenhängen, können tatsächlich gefährliche Kombinationen verborgen sein. Schon bei einer relativ geringen Zahl von Fehlern, die nicht zur Betriebshemmung führen, kann der Analyseaufwand so groß werden, dass Konzeptänderungen zu empfehlen sind.

6 Überblick über die Anforderungen an Vollschutzgeräte

Die folgende Abbildung gibt einen Überblick über die einzelnen Anforderungen an Vollschutzgeräte und deren Prüfung.

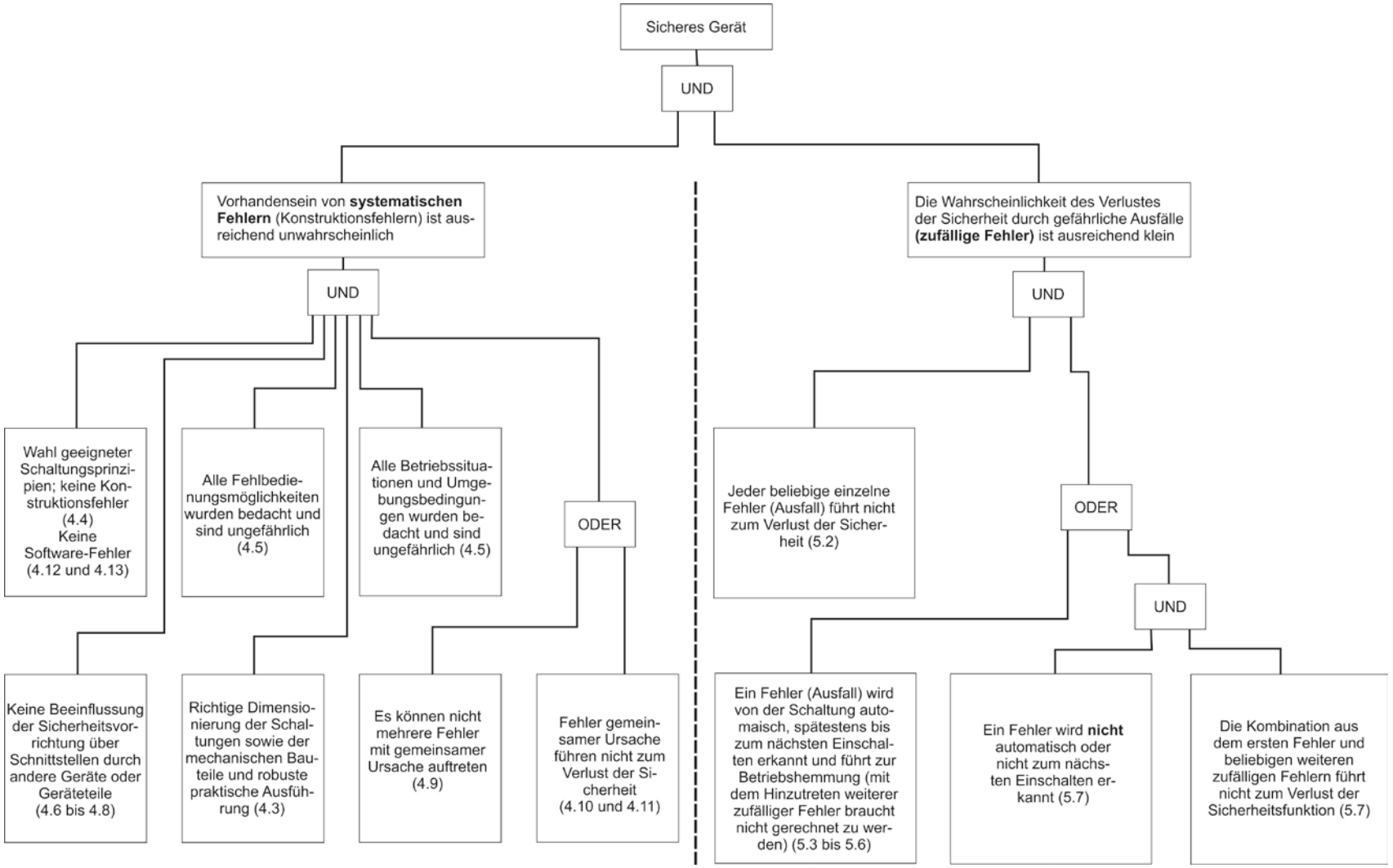


Abbildung 2: Fehlerarten und Prüfpunkte (In Klammern: Verweise auf die relevanten Abschnitte)

7 Grundanforderungen an die Sicherheitsvorrichtungen von Schulröntgeneinrichtungen

Schulröntgeneinrichtungen müssen alle Anforderungen, die an Vollschutzgeräte gestellt werden, erfüllen (Anlage 2, Nr. 4 RöV). Daher gelten alle in den vorangegangenen Kapiteln aufgeführten Anforderungen auch für Schulröntgeneinrichtungen.

Zusätzlich muss bei Schulröntgeneinrichtungen nach Anlage 2, Nr. 4.2 RöV sichergestellt sein, dass die vom Hersteller oder Einführer angegebenen maximalen Betriebsbedingungen nicht überschritten werden können. Folglich dürfen elektronische Schaltungen, die die Röntgenröhre mit Strom und Spannung versorgen, keinen systematischen Fehler enthalten (siehe Kapitel 5). Um zufällige Fehler zu vermeiden sind keine Sicherheitsvorrichtungen gemäß SIL 3 bzw. PL e erforderlich. Weil ein Versagen der Leistungsbegrenzung nicht zu einer Gefährdung von Personen durch den Nutzstrahl führt, reicht zur Absicherung der maximalen Betriebsbedingungen ein Erfüllen der Kategorie B nach DIN EN 13849 aus.

8 Grundanforderungen an die Sicherheitsvorrichtungen von Hochschutzgeräten und Basisschutzgeräten

Die maximal zulässigen Ortsdosisleistungswerte von Hochschutzgeräten und Basisschutzgeräten sind erheblich größer als die von Vollschutzgeräten (siehe Anlage 2 in [1] und Erläuterungen in [2]). Daher dürfen Hochschutzgeräte und Basisschutzgeräte nur betrieben werden, wenn ein Strahlenschutzregime vorhanden ist, was u. a. die Überwachung jedes einzelnen Gerätes durch einen Strahlenschutzbeauftragten beinhaltet. Bei Hochschutzgeräten muss nach Anlage 2, Nr. 2 RöV sichergestellt sein, dass die Röntgenröhre oder der Röntgenstrahler nur bei vollständig geschlossenem Schutzgehäuse betrieben werden kann. Ausnahmen sind in der Anlage 2 Nr. 2 der RöV geregelt (siehe auch den Bericht PTB-Dos-47 [2]). Das Innere eines Schutzgehäuses darf bei kontinuierlichem Betrieb z. B. dann zugänglich sein, wenn die Ortsdosisleistung im Inneren den in 0,1 Meter vom Außengehäuse zulässigen Wert nicht überschreitet.

Anmerkung: Bei kontinuierlichem Betrieb wird das Strahlenaustrittsfenster typischerweise mit einem “Shutter“ verschlossen. Der Shutter ist in diesem Fall in die Sicherheitsvorrichtung mit einzubeziehen (vergl. die Anforderungen an Vollschutzgeräte in Kap. 3).

Die Sicherheitsvorrichtung eines Hochschutzgerätes oder Basisschutzgerätes muss SIL 3 gemäß DIN EN 62061 oder PL e gemäß DIN EN 13849-2 erfüllen. Daher müssen bei der Konstruktion eines Hochschutzgerätes alle Anforderungen erfüllt werden, die in den Kapiteln 4 und 5 aufgeführt sind (Vermeidung von systematischen und zufälligen Fehlern). Jedoch sind die nachfolgend aufgeführten Abweichungen bei der Umsetzung der Anforderungen gemäß Kapitel 5 möglich. Diese Abweichungen beziehen organisatorische Maßnahmen ergänzend zu den technischen Vorkehrungen mit ein.

Organisatorische Maßnahmen unterliegen der Verantwortung des zuständigen Strahlenschutzbeauftragten, sofern sie Lücken im technischen Schutzniveau gemäß der Anforderungen 5.2 bis 5.4 oder 5.6 oder 5.7 kompensieren. Die Umsetzung derartiger organisatorischer Maßnahmen ohne Aufsicht des zuständigen Strahlenschutzbeauftragten ist nicht zulässig! Eine regelmäßige Überprüfung der Sicherheitsvorrichtung durch den Hersteller oder Verbringer in zeitlich kurzen Abständen (von wenigen Monaten) ist ggf. eine weitere Möglichkeit, durch organisatorische Maßnahmen eine ausreichende Sicherheit im Strahlenschutz sicher zu stellen. Voraussetzung ist ein Wartungsvertrag, der diese Maßnahmen regelt.

Rein technische Schutzmaßnahmen, d. h. das Erfüllen der Anforderungen des SIL 3, sind der Einbindung organisatorischer Schutzmaßnahmen grundsätzlich vorzuziehen (d. h. Realisierung des SIL 2 zusammen mit organisatorischen Maßnahmen); denn die Bauartprüfung ist bei der Realisierung rein technischer Schutzmaßnahmen einfacher und rein technischer Schutzmaßnahmen erleichtern den späteren Betrieb des geprüften Gerätes. Die Begründung für die Festlegung der erforderlichen SIL findet sich im Kapitel 9.

Abweichung zu Kapitel 3.3:

Basisschutzgeräte, die einen Verschluss besitzen, der den Röntgenstrahl aus dem Probenraum ausblendet, müssen eine Anzeige besitzen, die ausfallsicher erkennen lässt, wann der Nutzstrahl offen in den Probenraum eintritt.

Abweichung zu Kapitel 5.2.1:

Ein einzelner Fehler darf nicht zum Verlust der Sicherheitsfunktion führen. Diese Anforderung ist bei Vollschutzgeräten durch zwei unabhängige Sicherheitsvorrichtungen zu realisieren. Bei Hochschutzgeräten und Basisschutzgeräten kann auch durch organisatorische Maßnahmen ein vergleichbares Schutzniveau erreicht werden.

Abweichung zu Kapitel 5.3.1:

Bei Hochschutzgeräten und Basisschutzgeräten können Fehlererkennung und Betriebshemmung in begrenztem Maße auch durch organisatorische Maßnahmen erfolgen. Dabei ist zu beachten: Das Schutzniveau darf insgesamt nicht verringert werden. Das technisch realisierte Schutzniveau muss mindestens die Anforderungen des SIL 2 nach DIN EN 62061 erfüllen.

Abweichung zu Kapitel 5.4.1:

In Kapitel 5.4.1 ist gefordert: "Die Erkennung eines Ausfalls (Hardware-Fehlers) muss innerhalb kurzer Zeit nach dessen Auftreten erfolgen und sofort oder spätestens beim Versuch, die Hochspannung der Röntgeneinrichtung erneut einzuschalten, zu einer Betriebshemmung führen“. "Logische Einheiten zur Fehlererkennung müssen ... in regelmäßigen Abständen und vor jedem Einschalten der Röntgeneinrichtung die zu überwachenden Bauelemente prüfen." Bei Hochschutzgeräten und Basisschutzgeräten kann ein Teil dieser Prüfungen auch von fachkundigen Personen durchgeführt werden. Wird ein Fehler von einer Person erkannt, muss eine Betriebshemmung manuell herbeigeführt werden.

Abweichung zu Kapitel 5.6.1:

Ist bei einem Hochschutzgerät eine Betriebshemmung manuell herbeigeführt worden, ist der zuständige Strahlenschutzbeauftragte für die Beibehaltung der Betriebshemmung (bis zur Behebung des Fehlers) verantwortlich.

Abweichung zu Kapitel 5.7.1:

Zusätzlich zu den in Kapitel 5.7.1 genannten Fehlern müssen bei Hochschutzgeräten zufällige Fehler, die durch organisatorische Maßnahmen erkannt werden, bevor es zu einer Gefährdung kommt, durch die Sicherheitsvorrichtung nicht unbedingt erkannt werden, so dass das das technische Realisieren des SIL 2 ausreicht.

9 Schadensrisiko und Sicherheitskategorien

9.1 Sicherheitstechnische Einstufung von Vollschutzgeräten und Schulröntgeneinrichtungen

Die Festlegung des erforderlichen SIL gemäß DIN EN 62061 ergibt sich nach Anhang A.2 aus einer Risikoabschätzung der Gefährdung. Diese wird ermittelt anhand einer Beurteilung der Schwere eines möglichen Schadens (S) kombiniert mit der Einschätzung der Wahrscheinlichkeit des Auftretens dieses Schadens. Diese Wahrscheinlichkeit ergibt sich aus der Verknüpfung der Betrachtung der Häufigkeit und Dauer der Exposition (F), der Wahrscheinlichkeit des Auftretens eines gefahrbringenden Ereignisses (W) und der Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (P). Die erwähnte Norm fordert, dass Worst-case-Annahmen bei der Festlegung einzelner Parameter getroffen werden.

Tabelle 1: Matrix der Festlegung des SIL nach DIN EN 62061. Falls andere Schutzmaßnahmen notwendig sind, ist '(AM)' angegeben.

Schwere (S)	Klasse (K)				
	4	5 bis 7	8 bis 10	11 bis 13	14 bis 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(AM)	SIL 1	SIL 2	SIL 3
2			(AM)	SIL 1	SIL 2
1				(AM)	SIL 1

Bei nichtmedizinischen Röntgeneinrichtungen bedeutet der Ausfall der Sicherheitsvorrichtungen, dass der Betreiber ggf. eine erhöhte Dosis ionisierender Strahlung erhalten kann. Aufgrund der sehr hohen Dosisleistungen im Nutzstrahl [2] der verwendeten Röntgenstrahler und erheblicher Streustrahlungsanteile sind bei nicht ordnungsgemäß geschlossenem Strahlenschutzgehäuse Teilkörperexpositionen mit schweren irreversiblen Schädigungen sowie Ganzkörperexpositionen mit deutlich über den zulässigen Grenzwerten liegenden Strahlungsdosen nicht auszuschließen. Letzteres könnte im Einzelfall die Wahrscheinlichkeit für das Auftreten strahlungsbedingter Spätschäden (Krebserkrankungen, genetische Defekte) in inakzeptabler Weise erhöhen. Der Schwere der möglichen Verletzungen (S) wird bei nichtmedizinischen Röntgeneinrichtungen deshalb grundsätzlich als 4 angenommen (irreversibel: Tod, Verlust eines Auges oder Arms, unerlaubt hohe Dosiswerte führen ggf. zum Verlust des Arbeitsplatzes am Röntgengerät).

Häufigkeit und Dauer der Exposition hängen stark vom Einzelfall ab: es gibt z. B. Hochschutzgeräte sowie Schulröntgeneinrichtungen, deren Betriebsdauer nur wenige Tage pro Jahr beträgt und bei denen sich der Betreiber in der Regel nicht unmittelbar am Gerät aufhält. Es gibt andererseits Vollschutzgeräte, die unmittelbar am Arbeitsplatz eingesetzt werden, wodurch Expositionszeiten von 2000 Stunden pro Jahr nicht auszuschließen sind. Schon eine Häufigkeit der Exposition (> 10 min), die oberhalb oder gleich von 1 pro Tag liegt, führt zu einer Festlegung des Parameters F auf 5 gemäß Abschnitt A.2.4.1 der DIN EN 62061. Im Allgemeinen muss diese Expositionshäufigkeit angenommen werden.

Die Wahrscheinlichkeit des Auftretens des gefahrbringenden Ereignisses wird im Abschnitt A.2.4.2 der DIN EN 62061 behandelt. Die Betrachtung geschieht unabhängig von der Wirkung der Sicherheitsvorrichtungen (SRCFs)! Von einem Röntgengerät ohne technische Schutzvorrichtungen geht grundsätzlich eine sehr hohe Gefahr aus, weil selbst fachkundige Nutzer ohne sehr genaue Kenntnis des Gerätes mit Röntgenstrahlen exponiert würden;

denn Röntgengeräte stellen – im Gegensatz zu anderen Maschinen - per se durch das Erzeugen von Röntgenstrahlen hoher Dosis eine Gefahr dar. Folglich ist der Parameter W mit 5 ("sehr hoch") zu bewerten.

Die Möglichkeit, die Gefährdung zu vermeiden, oder den Schaden zu begrenzen, muss bei ionisierender Strahlung als gering angesehen werden. Der Mensch verfügt über kein Sinnesorgan zur Wahrnehmung dieser Strahlung. Die Betreiber von Vollschutzgeräten unterliegen zudem i. Allg. keinem Strahlenschutzregime: Es gibt i. Allg. keinen Strahlenschutzbeauftragten für den Betrieb dieser Geräte, es wird keine Fachkunde des Betreibers gefordert und es wird keine dosimetrische Überwachung durchgeführt. Gemäß Abschnitt A.2.4.3 der DIN EN 62061 ist daher der Parameter P mit 5 anzusetzen ("Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens unmöglich").

Nach diesen Betrachtungen wird die Klasse (K) nach folgender Formel berechnet:

K = F + W + P = 5 + 5 + 5 = 15 kombiniert mit der Schwere 4 ergibt sich nach Tabelle 1 der SIL 3. Selbst wenn man die Schwere mit 3 ansetzen würde, oder einen der anderen Parameter niedriger einstufen würde, ergäbe sich immer noch der SIL 3. Nach Tabelle 3 der DIN EN 62061 entspricht der SIL 3 der Wahrscheinlichkeit eines gefahrbringenden Ausfalls je Stunde von $\geq 10^{-8}$ bis $< 10^{-7}$. Dieser Wahrscheinlichkeitsbereich entspricht nach Tabelle 3 der DIN EN 13849-1 einem Performance Level (PL) von e.

Nach Neuinterpretation des vom Länderauschuss Röntgenverordnung beim BMU geforderten Schutzniveaus, damals basierend auf der Norm DIN EN 954-1, wird jetzt nach den aktuellen Normen DIN EN 62061 der SIL 3 bzw. nach DIN EN 13849-1 der PL e gefordert.

Damit wird insbesondere sichergestellt, dass das Versagen einer Komponente nicht den Ausfall der Schutzeinrichtung zur Folge hat und ein aufgetretener Fehler spätestens beim nächsten Einschalten der Röntgenstrahlung erkannt und ein Einschalten der Strahlung verhindert wird.

Für Vollschutzgeräte, bei denen kein Strahlenschutzregime vorgesehen ist und der Betreiber über keine Fachkunde im Strahlenschutz verfügen muss, ist der SIL 3 oder PL e **ausschließlich durch technische Maßnahmen des Gerätes selbst zu realisieren**. Für Hochschutzgeräte, die nur in Verbindung mit einem Strahlenschutzregime betrieben werden dürfen, kann der Sicherheitsstandard SIL 2 (analog dem PL d) ausreichen, wenn durch zusätzliche organisatorische Maßnahmen der Sicherheitsstandard insgesamt angehoben wird, sodass insgesamt die Gefährdung für Personen nicht höher ist als bei Vollschutzgeräten.

9.2 Sicherheitstechnische Einstufung von Hochschutz- und Basisschutzgeräten

Die Vorgehensweise der Risikobewertung ist analog zu der im vorhergehenden Abschnitt. Die Beurteilung der Schwere von Schäden fällt gleich aus (S = 4), da die Gefahrenquelle Röntgenstrahlung bei allen Röntgengeräten die gleiche ist. Die Häufigkeit der Exposition ist bei einer Worst-case-Betrachtung ebenfalls mit F = 5 einzuschätzen.

Die Wahrscheinlichkeit eines gefahrbringenden Ereignisses (W) kann man jedoch geringer einschätzen, da ein fachkundiger Nutzer (im Sinne der RöV) die Gefahren der Röntgenstrahlung eher einschätzen kann. Allerdings sind gefahrbringende Ereignisse immer noch möglich, sodass sich W = 3 ergibt. Eine Vermeidung oder Begrenzung von Schäden kann auch durch organisatorische Maßnahmen unterstützt werden, da es bei Hochschutz- oder Basisschutzgeräten ein Strahlenschutzregime mit Strahlenschutzbeauftragten und ggf. mit einer dosimetrischen Überwachung gibt. Die Einwandfreie Funktionsweise der Röntgengeräte kann regelmäßig durch fachkundiges Personal überprüft werden. Die Gefährdung

durch Röntgenstrahlen kann Fachpersonal ggf. auch an Warnleuchten und anderen Statusmeldungen erkennen. Diese Maßnahmen müssen so zuverlässig sein, dass eine Vermeidung oder Begrenzung von Schäden wahrscheinlich ist (P = 1).

Damit ergibt sich:

K = F + W + P = 5 + 4 + 1 = 10,

sodass gerade noch der SIL 2 für Hochschutz- und Basisschutzgeräte vertretbar ist.

Es wird jedoch empfohlen, bei zentralen Sicherheitsvorrichtungen immer das Niveau des SIL 3 zu realisieren, da die Beurteilung der Tragfähigkeit von organisatorischen und sonstigen technischen Hilfsmaßnahmen (wie Anzeigelampen) schwierig ist und im Einzelfall oft größerer Aufwände bedarf. Es gilt der Grundsatz, dass technische Lösungen zum Schutz gegen Gefahren zu bevorzugen sind.

9.3 Technischer Hintergrund

Durch Auswahl hochwertiger Bauelemente und durch Überdimensionierung in sicherheitsrelevanten Schaltungen und mechanischen Vorrichtungen kann die Wahrscheinlichkeit für das Auftreten der zufälligen Fehler gering gehalten werden und damit bei geringen zu erwartenden Schäden eine angemessene Sicherheit erreicht werden(Kategorie B nach DIN EN 13849-1).

Das auf diese Weise erzielbare Sicherheitsniveau reicht aber in vielen Fällen nicht aus. Um auch nach Auftreten eines zufälligen Fehlers die Sicherheit eines Gerätes oder einer Anlage gewährleisten zu können, verlangt die Röntgenverordnung für Vollschutzgeräte und Schulröntgeneinrichtungen, dass sicherheitsrelevante Teile der Geräte zweifach vorhanden sind (Redundanz). So kann der Schaltungsteil, der nicht von dem Ausfall betroffen ist, die Funktion des fehlerhaften Teils übernehmen und der Betrieb des Gerätes bleibt sicher.

Bei mittlerem Schadensrisiko genügt bereits die einfache Verdoppelung der betreffenden Schaltungsteile, um eine angemessene Sicherheit zu erreichen (Kategorie 2 nach DIN EN 13849-1). Wird aber eine höhere Sicherheit verlangt, weil große Sachwerte, die Gesundheit von einzelnen Menschen oder gar einer Vielzahl von Menschen von der Sicherheit des Gerätes abhängen, so müssen noch weitergehende Schutzmaßnahmen gegen die Auswirkungen von zufälligen Fehlern in der Sicherheitsvorrichtung getroffen werden. Dies ist notwendig, weil man bei einer einfachen Verdoppelung von Schaltungsteilen ignoriert, dass im Verlauf der Einsatzzeit des Gerätes noch weitere zufällige Fehler auftreten können, die auch den redundanten noch intakten Teil der Sicherheitsvorrichtung betreffen können und damit die Sicherheit des Gerätes gefährden.

Bei größerem Schadensrisiko und erhöhtem Sicherheitsbedarf wird deshalb verlangt, dass ein zufällig aufgetretener Fehler möglichst bald nach seinem Auftreten von der Sicherheitsvorrichtung automatisch erkannt und das Gerät in einen sicheren Zustand überführt wird (Abschaltung, Betriebshemmung, Diagnosedeckungsgrad nach DIN EN 13849-1 ist hoch). Während der Zeit zwischen dem Auftreten des Fehlers und seiner Erkennung bzw. der Abschaltung wird der sichere Betrieb durch die redundanten Teile des Gerätes gewährleistet. Ist die Zeit zwischen dem Auftreten eines zufälligen Fehlers und der Abschaltung des Gerätes bezogen auf die Rate der anzunehmenden Fehler kurz, so braucht mit dem Auftreten eines zweiten zufälligen Fehlers nicht gerechnet zu werden und die Sicherheit ist auch über längere Zeiträume gegeben.

Nach DIN EN 62061 oder DIN EN 13849-1 brauchen nicht alle Fehler automatisch erkannt zu werden und zum Übergang in einen sicheren Zustand führen (Stichwort: Fehlertoleranz eine SRECS). Man nimmt also in Kauf, dass mit einer sehr geringen Wahrscheinlichkeit beide Teile einer redundanten Sicherheitsvorrichtung ausfallen und die Sicherheit nicht mehr gewährleistet ist. Es ist Aufgabe des Gutachters bzw. der PTB, zu bewerten, ob die

vom Hersteller vorgesehene Fehlererkennung die gefährlichsten oder wahrscheinlichsten Fehler aufdeckt und ob die von der Sicherheitsvorrichtung nicht erkannten Fehler akzeptiert werden können. Die mittlere Zeit bis zum gefahrbringenden Ausfall muss in diesem Zusammenhang betrachtet werden. Die Anforderung an einen hohen Diagnosedeckungsgrad lässt jedoch wenig Spielraum bezüglich unerkannter Fehler. Gemäß DIN EN 13849-1 ergibt sich allein schon aus dieser Anforderung der PL e (siehe z. B. Tabelle 7 dieser Norm).

10 Beispiele

10.1 Allgemeines

In diesem Abschnitt werden drei Beispiele für mögliche Realisierungen von Sicherheitsvorrichtungen entsprechend SIL 3 beschrieben, die die Anforderungen vom Konzept her erfüllen.

10.2 Sicherheitsvorrichtung mit zwangsgeführten Relais

Die in Abbildung 3 gezeigte Relais-Schaltung zeichnet sich dadurch aus, dass nur sehr wenige Bauelemente zusätzlich zu den für die eigentliche Nutzfunktion notwendigen eingesetzt werden. Bauelemente mit besonderen sicherheitstechnischen Eigenschaften sind die beiden Relais K1 und K2 und die Türschalter S1 und S2, für die der Fehler „Öffner und Schließer sind gleichzeitig geschlossen“ aufgrund der Zwangsführung der Kontakte ausgeschlossen werden kann. Die übrigen Bauelemente können Standard-Bauelemente sein, bei denen Fehler nicht ausgeschlossen werden müssen. Nicht alle Fehler in der Schaltung werden erkannt und führen zur Betriebshemmung. Wie die Fehlerart- und Ausfall-Effekt-Analyse in Tabelle 2 zeigt, sind die Folgen dieser Ausfälle aber vertretbar.

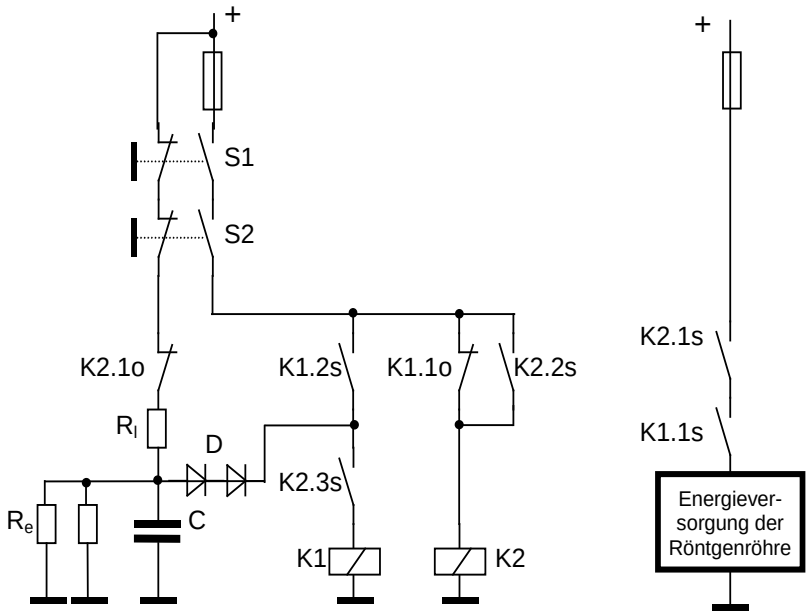


Abbildung 3: Sicherheitsvorrichtung mit zwangsgeführten Relais

Tabelle 2: Fehlerart- und Ausfalleffekt-Analyse für Beispielschaltung nach Abbildung 3.

Nr.	Bauelement	Aus-fallart	Fehlereffekt	Erken-nung
1	Relais K1	NE	Ein Kontakt im Energiekreis bleibt geöffnet.	a)
		NA	Ein Kontakt im Energiekreis bleibt geschlossen. Weil Öffner K1.1o nicht schießt, kann K2 nach erneutem Start nicht anziehen.	b)
2	Schließer K1.1s	NS	Ein Kontakt im Energiekreis bleibt geöffnet.	a)
		NO	Ein Kontakt im Energiekreis bleibt geschlossen. Wg. Zwangsführung schließt K1.1o nach Stopp nicht. K2 kann bei erneutem Start nicht anziehen.	b)
3	Schließer K1.2s	NS	K1 zieht nach Start an, fällt aber nach Entladung von C wieder ab. Kontakt K1.1s im Energiekreis bleibt nicht geschlossen.	a)
		NO	Wg. Zwangsführung schließt K1.1o nach Stopp nicht. K2 kann bei erneutem Start nicht anziehen.	b)
4	Öffner K1.1o	NO	Wg. Zwangsführung bleibt Kontakt K1.1s im Energiekreis geöffnet.	a)
		NS	K2 kann bei erneutem Start nicht anziehen.	b)
5	Relais K2	NE	Kontakt K2.1s im Energiekreis bleibt geöffnet. K1 zieht nicht an. Zweiter Kontakt K1.1s im Energiekreis bleibt auch geöffnet.	a)
		NA	Alle Schließer geschlossen; Kontakt K2.1s im Energiekreis bleibt geschlossen. Wg. Zwangsführung bleibt K2.1o geöffnet und C kann nach Stopp nicht aufgeladen werden. Deshalb zieht K1 bei erneutem Start nicht an.	b)
6	Schließer K2.1s	NS	Ein Kontakt im Energiekreis bleibt geöffnet.	a)
		NO	Kontakt K2.1s im Energiekreis bleibt geschlossen. Wg. Zwangsführung bleibt K2.1o geöffnet und C kann nach Stopp nicht aufgeladen werden. Deshalb zieht K1 bei erneutem Start nicht an.	b)
7	Schließer K2.2s	NS	Start – Anzug K2 – Anzug K1 – Öffnen von K1.1o. Da Selbsthaltung durch K2.2s nicht möglich ist, fällt K2 und danach auch K1 wieder ab. Oszillation bis C entladen ist. Dies geschieht bei jedem Start erneut.	c)
		NO	Wg. Zwangsführung bleibt K2.1o geöffnet und C kann nach Stopp nicht aufgeladen werden. Deshalb zieht K1 bei erneutem Start nicht an.	b)
8	Schließer K2.3s	NS	K1 zieht nicht an. Ein Kontakt im Energiekreis bleibt geöffnet.	a)
		NO	Wg. Zwangsführung bleibt K2.1o geöffnet und C kann nach Stopp nicht aufgeladen werden. Deshalb zieht K1 bei erneutem Start nicht an.	b)
9	Öffner K2.1o	NO	Wg. Zwangsführung zieht kein Schließer von K2 bei Start an. Kein Kontakt im Energiekreis ist geschlossen.	a)
		NS	C wird nicht aufgeladen. Deshalb zieht K1 bei erneutem Start nicht an.	b)
10	Türschalter S1s oder S2s	NS	Kein Relais zieht an.	a)
		NO	Zweiter Türschalter öffnet. Wg. Zwangsführung schließt der zugehörige Öffner S1o bzw. S2o nicht. C wird nicht aufgeladen und K1 zieht bei erneutem Start nicht an.	b)
11	Türschalter S1o oder S2o	NO	Wg. Zwangsführung schließt der zugehörige Schließer S1s bzw. S2s nicht.	a)
		NS	C wird nicht aufgeladen. Deshalb zieht K1 bei erneutem Start nicht an.	b)
12	Widerstand Rl	K	Stärkere Beanspruchung der Kontakte.	d)
		U	C wird nicht aufgeladen und K1 zieht bei erneutem Start nicht an.	b)
13	Widerstand Re	K	C wird nicht aufgeladen und K1 zieht bei erneutem Start nicht an.	b)
		U	C wird nur durch Wicklung von K1 bei Start entladen und behält die Ladung auch nach mehreren Einschaltvorgängen. Nichtabfall von K2.Xs-Kontakten und damit Nicht-Schließen von K2.1o oder S1o, S2o wird solange nicht erkannt (deshalb Verdopplung).	e)
14	Kondensator C	C+	Keine Wirkung (bei richtiger Dimensionierung von C und Re). Die zur Fehlererkennung notwendige minimale Ausschaltdauer (Entladungszeitkonstante Re · C) erhöht sich. Unkritisch, da die Zeitkonstante viel kleiner (Größenordnung 1s) als die reale Ausschaltdauer ist.	nein
		C-	Bei starker Verringerung oder Unterbrechung zieht K1 bei Start nicht mehr an. Kurzschluss wie (13).	b)
15	Diode D	K	C wird über S1s, S2s und K1.2s nach Start geladen. C ist nach Stopp nicht entladen. Bei schnellem Wiedereinschalten wird Nicht-Schließen von K2.1o oder S1o, S2o nicht erkannt (deshalb Verdopplung).	e)
		U	K1 zieht bei Start nicht mehr an.	b)

Abkürzungen für die Ereignisse und Ausfallarten:

Start	-	Start der Vorrichtung: Schließen der Tür
Stopp	-	Öffnen der Tür
NE	-	Nicht-Erregung, Nichtanzug eines Relais
NA	-	Nichtabfall eines Relais
NS	-	Nichtschließen eines Kontakts
NO	-	Nichtöffnen eines Kontakts
K	-	Kurzschluss
U	-	Unterbrechung
C+	-	Kapazitätserhöhung
C-	-	Kapazitätsverringerung

Abkürzungen für die Art der Fehlererkennung:

a) Betriebshemmung sofort
b) Betriebshemmung bei nächstem Start
c) Betriebshemmung bei nächstem Start, verzögert nach anfänglicher Relais-Oszillation.
d) Keine Betriebshemmung. Außer erhöhtem Verschleiß keine weiteren Auswirkungen.
e) Betriebshemmung beim nächsten Einschalten, jedoch nur bei ausreichend langer Pause zwischen Stopp und Start.

Alle Einzelausfälle sind ungefährlich. Zu den Ausfällen c, d und e müssen mindestens noch zwei weitere zufällige Einzelausfälle hinzutreten, damit es zur Gefährdung kommt. Gemäß Anforderung nach Kap. 5.7 wäre deshalb für die genannten Ausfallarten keine Erkennung erforderlich. Im Beispiel wird die Wahrscheinlichkeit für diese Ausfälle durch Verdopplung der betreffenden Bauelemente noch weiter verringert, so dass sogar drei weitere Ausfälle notwendig wären. *Damit führen selbst Mehrfachausfälle in dieser Schaltung nicht zur Gefährdung.*

10.3 Sicherheitsvorrichtung mit vollständiger Software-Steuerung

Bei der Konfiguration gemäß Abbildung 4 zur Überwachung *einer* Tür oder Klappe sind die logischen Verknüpfungen, die zur sicheren Abschaltung der Energieversorgung des Röntgenstrahlers notwendig sind, fast ausschließlich durch Software realisiert (beachte aber auch die Hinweise in den Kapiteln 4.12 und 4.13). Nur bei den auslösenden Schaltern und Schützen handelt es sich notwendigerweise um Hardware.

Die Schaltung ist symmetrisch zweikanalig ausgeführt und besitzt getrennte Stromversorgungen für beide Rechner. Die Zweikanaligkeit ist erforderlich, um zufällige Fehler (Hardware-Ausfälle) erkennen zu können und die Betriebshemmung nach dem Ausfall sicherzustellen.

Die Software ermittelt sämtliche Hardware-Ausfälle durch ständige Abfrage der Zustände der Schalter und Schütze. Der Schaltzustand eines jeden Schützes wird mit Hilfe der Überwachungskontakte vor jedem Einschalten geprüft. Informationen über den Einschaltzustand werden über je einen zwangsgeführten Überwachungskontakt der Schütze kreuzweise an den jeweils anderen Rechner übergeben. Die Software hat volle Sicherheitsverantwortung. Es sind Maßnahmen zur Programmlaufüberwachung realisiert. Der Mikrocontroller führt keine anderen Funktionen aus als die Überwachung der Sicherheitsvorrichtung (keine weitere Steuerung, Regelung oder Diagnose).

Die Information, dass ein Hardware-Ausfall vorliegt, wird in einem nicht-flüchtigen Speicher sicher gespeichert. Bei jedem Neustart des Rechner-Systems werden die Informationen dieses Fehlerregisters vom Programm gelesen. Der Rechner, in dessen Fehlerregister ein noch nicht behobener Fehler registriert ist, schaltet den Schütz für die Hochspannung nicht ein und zeigt ggf. eine Fehlermeldung an.

Die Software erfüllt die Anforderungen der Kapitel 4.12 und 4.13. Die Bauelemente haben besondere sicherheitstechnische Eigenschaften: Die Schütze besitzen zwangsgeführte Kontakte. Zur Reduzierung leitungsgebundener Störungen werden die Eingangssignale z. B. von den Türschaltern und von den Überwacher-Kontakten der Schütze über Optokoppler dem Mikrocontroller zugeführt. Die Ausgänge zu den Schützen werden ebenfalls über Optokoppler geführt.

Hinweis: Das Schaltbild in Abbildung 4 ist vereinfacht; es sind weitere Bauelemente erforderlich, um eine zuverlässige Schaltungsfunktion zu gewährleisten und um eine Überwachung bezüglich der Programmlaufzeit zu realisieren.

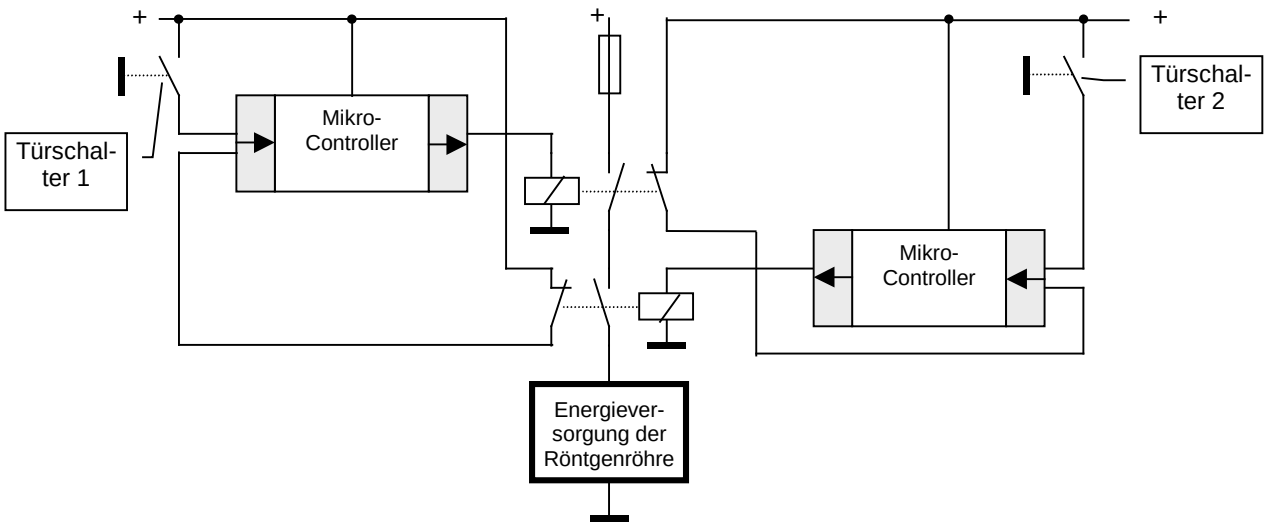


Abbildung 4: Vollständige Software-Steuerung der Sicherheitsvorrichtung zur Überwachung einer Tür (vereinfacht)

10.4 Erkennung von Hardware-Fehlern und Betriebshemmung durch Software

Die Konfiguration gemäß Abbildung 5 ist dadurch gekennzeichnet, dass die Ein- und Abschaltung der Energieversorgung der Röntgenröhre im fehlerfreien Fall nur von zwei redundanten Hardware-Kanälen bestehend aus je einem Schalter und der zu überwachenden Tür und einem Schütz erfolgt. Fehler werden durch Plausibilitätsprüfungen der Türkontakte und der Schütz-Überwachungskontakte von einem Mikrocontroller ermittelt, der die Energieversorgung der Röntgenröhre über ein Relais unterbrechen kann.

Wenn ein Hardware-Ausfall aufgedeckt wurde, wird diese Information in einem nicht-flüchtigen Speicher sicher (doppelt invers) gespeichert. Bei jedem Neustart des Rechner-Systems werden die Informationen in diesem Fehlerregister vom Programm gelesen. Wenn im Fehlerregister ein noch nicht behobener Fehler registriert ist, schaltet der Rechner die Hochspannung nicht ein und zeigt ggf. eine Fehlermeldung an. Dieser Rechner muss nicht mehrkanalig ausgeführt sein und es werden keine höherwertigen Schutzmaßnahmen, wie z. B. eine Überwachung bezüglich der Programmlogik und –laufzeit, verlangt: Sollte sich in der Hardware der Rechner-Schaltung ein Ausfall ereignen, so müssen noch zwei weitere unabhängige Fehler in der Hardware der Türschalter-/Schütz-Kombination eintreten, damit es zu einer Gefährdung kommt.

Die Software muss aber die Anforderungen der Kapitel 4.12 und 4.13 erfüllen.

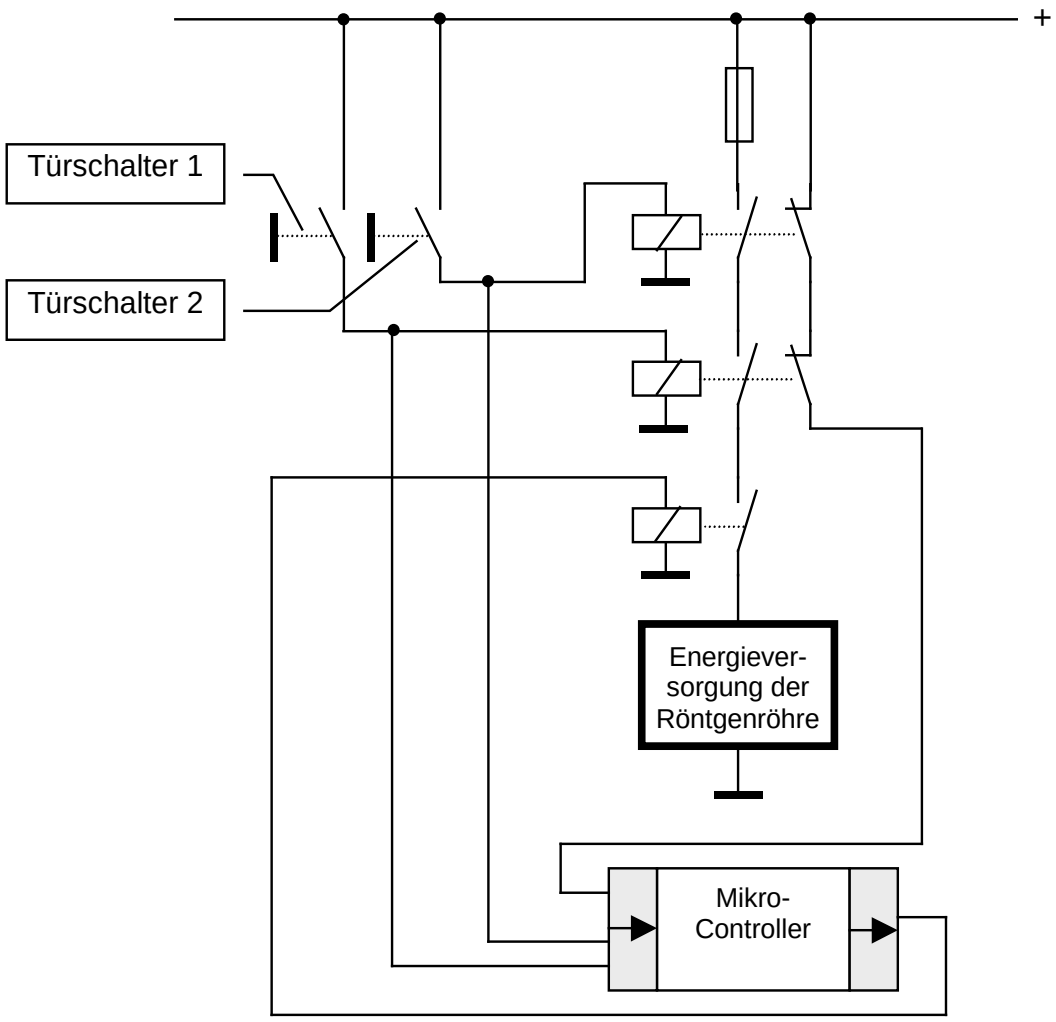


Abbildung 5: Erkennung von Hardware-Fehlern und Betriebshemmung durch Software (vereinfacht).

Die Bauelemente haben besondere sicherheitstechnische Eigenschaften: Die Schütze besitzen zwangsgeführte Kontakte. Die Eingangssignale von den Türschaltern und von den Überwacher-Kontakten der Schütze werden über Optokoppler dem Mikrocontroller zugeführt. Die Ausgänge zu den Schützen werden ebenfalls über Optokoppler geführt. Hinweis: Das Schaltbild in Abbildung 5 ist vereinfacht; es sind weitere Bauelemente erforderlich, um eine zuverlässige Schaltungsfunktion zu gewährleisten, damit Fehler, die in Beispiel 4-3 genannt wurden, nicht auftreten können.

11 Danksagung

Dieser Leitfaden wurde unter der tatkräftigen Unterstützung von Jörg Kretzer, Karsten Kahnt und Susanne Niemeyer erstellt. Wir bedanken uns ferner bei einer Reihe externer Kollegen, die sich mit sicherheitstechnischen Gutachten beschäftigen für die konstruktiven Diskussionen.

Den Kollegen Stefan Neumaier, Ulrich Grottker, Harald Dombrowski, Alexander Höhne, Roland Zwiener und Peter Ambrosi, die den Bericht in der vorherigen Fassung erstellt haben sei für ihre Vorarbeit gedankt. Außerdem möchten wir uns bei Frau Susanne Niemeyer für die Unterstützung bei dem Qualitätsmanagement bedanken.

12 Literatur

[1] Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (Röntgenverordnung – RöV) vom 08. Januar 1987 in der Fassung der Bekanntmachung vom 30. April 2003 (BGBl. I, S. 604), die zuletzt durch Artikel 6 der Verordnung vom 11. Dezember 2014 (BGBl. I S. 2010) geändert worden ist.

[2] P. Taschner, G. Nolte; R. Zwiener; U. Grottker und S. Neumaier: *Bauartprüfungen von Hochschutzgeräten, Vollschutzgeräten und Schulröntgeneinrichtungen im Rahmen der Röntgenverordnung,* Bericht PTB-Dos-47, Wirtschaftsverlag NW, Bremerhaven (2004).

[3] DIN 54113-2:2005-04, *Zerstörungsfreie Prüfung - Strahlenschutzregeln für die technische Anwendung von Röntgeneinrichtungen bis 1 MV - Teil 2: Sicherheitstechnische Anforderungen und Prüfung für Herstellung, Errichtung und Betrieb*, Beuth-Verlag, Berlin (2005).

[4] DIN EN 62061:2016-05; VDE 0113-50:2016-05, *Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme* (IEC 62061:2005 + A1:2012 + A2:2015, Deutsche Fassung EN 62061:2005 + Cor.:2010 + A1:2013 + A2:2015), Beuth-Verlag, Berlin (2016).

[5] DIN EN ISO 13849-1, *Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze* (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015, Beuth-Verlag, Berlin (2016).

[6] DIN EN ISO 13849-2, *Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung* (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012, Beuth-Verlag, Berlin (2013).

[7] Richtlinie 92/58/EWG des Rates über Mindestvorschriften für die Sicherheits- und/oder Gesundheitsschutzkennzeichnung am Arbeitsplatz (Neunte Einzelrichtlinie im Sinne von Artikel 16 Absatz 1 der Richtlinie 89/391/EWG) vom 24. Juni 1992 (ABl. EU Nr. L 245 S. 23) zuletzt geändert durch Artikel 1 der Richtlinie 2014/27/EU vom 26. Februar 2014 (ABl. L 65 S. 1) in Kraft getreten am 25. März 2014 (1992).

[8] DIN EN 60204-1:2014-10; VDE 0113-1:2014-10, *Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen, Teil 1: Allgemeine Anforderungen* (IEC 44/709/CDV:2014); Deutsche Fassung FprEN 60204-1:2014), Beuth-Verlag, Berlin (2014).

[9] DIN EN 61508-4:2011-02; VDE 0803-4:2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen* (IEC 61508-4:2010)*; Deutsche Fassung EN 61508-4:2010*, Beuth-Verlag, Berlin (2011).

[10] J. Jacobsen, H. Carlsson, M. Ohlsson: *Safety Validation of Computer-Based Machine Control Systems*, SP Report 1997-12. Swedish National Testing and Research Institute, Borås, Schweden (1997).

[11] G. Rabe, H. Bezecny, D. Inverso, V. Maggioli, A. Weinert: *Guidelines for the use of Programmable Logic Controllers in Safety-related Systems*, European Workshop on Industrial Computer Systems EWICS, TC7, Position Paper 6012 (1998).

[12] DIN EN 61131-3:2014-06, *Speicherprogrammierbare Steuerungen - Teil 3: Programmiersprachen* (IEC 61131-3:2013); Deutsche Fassung EN 61131-3:2013, Beuth-Verlag, Berlin (2014).

[13] W. A. Halang, A. H. Heinke Frigeri, R. Lichtenecker, U. Steinmann, K. Wendland: *Methodenlehre sicherheitsgerichteter Echtzeitprogrammierung*, Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Fb 813, Dortmund / Berlin (1998).

[14] H. Gall, T. Steffens, K. Kemp: *Anwendung der Bussysteme in der Anlagensicherheit der Chemie-Industrie*, Forschungsvorhaben 35/00, TÜV Anlagentechnik GmbH.

[15] DIN EN 60947-5-1:2010-04; VDE 0660-200:2010-04, *Niederspannungsschaltgeräte - Teil 5-1: Steuergeräte und Schaltelemente - Elektromechanische Steuergeräte* (IEC 60947-5-1:2003 + A1:2009); Deutsche Fassung EN 60947-5-1:2004 + Cor.:2005 + A1:2009, Beuth-Verlag, Berlin (2010).

[16] DIN EN 60947-5-3:2014-12; VDE 0660-214:2014-12, *Niederspannungsschaltgeräte - Teil 5-3: Steuergeräte und Schaltelemente – Anforderungen für Näherungsschalter mit definiertem Verhalten unter Fehlerbedingungen (PDDB)* (IEC 60947-5-3:2013); Deutsche Fassung EN 60947-5-2:2013, Beuth-Verlag, Berlin (2014).

[17] DIN EN 50178:1998-04; VDE 0160:1998-04, *Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln; Deutsche Fassung EN 50178:1997*, Beuth-Verlag, Berlin (1998).

[18] DIN EN 60664-1:2008-01; VDE 0110-1:2008-01, *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen - Teil 1: Grundsätze, Anforderungen und Prüfungen* (IEC 60664-1:2007); Deutsche Fassung EN 60664-1:2007, Beuth-Verlag, Berlin (2008).

[19] DIN EN 61000-6-2:2016-05; VDE 0839-6-2:2016-05, *Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche* (IEC 77/488/CDV:2015); Deutsche Fassung FprEN 61000-6-2:2015, Beuth-Verlag, Berlin (2016).

[20] DIN EN ISO 14119:2014, *Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für die Gestaltung und Auswahl* (ISO 14119:2013); Deutsche Fassung EN ISO 14119:2013; Beuth-Verlag, Berlin (2014).

[21] DIN EN ISO 12100:2011-03, Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010; Deutsche Verfassung EN ISO 12100:2010

Anhang 1
Beispiel für Struktur und Inhalt eines Gutachter-Prüfberichts

Die folgende Gliederung eines Prüfberichtes soll den Gutachtern, die die PTB bei der Durchführung der sicherheitstechnischen Prüfungen von nichtmedizinischen Röntgeneinrichtungen unterstützen, als Beispiel dienen. Die genannten Angaben müssen mindestens enthalten sein.

Deckblatt

- Berichtsnummer
- Berichtsdatum / Datum der Prüfung
- Bezeichnung des geprüften Objektes
- Name und Anschrift des Herstellers
- Name und Anschrift des Gutachters
- Kurzfassung des Prüfergebnisses: Bestanden / Nicht bestanden

Inhaltsverzeichnis

8 Beschreibung der Sicherheitsvorrichtung

- Informelle oder formalisierte Schaltungsbeschreibung bzw. Wirkungsweise der Schaltung ODER

  Bezug auf entsprechenden Abschnitt der Herstellerdokumentation
- Schematisierte Darstellung der sicherheitsrelevanten Software und deren Wirkungsweise ODER

  Bezug auf entsprechenden Abschnitt der Herstellerdokumentation

9 Ergänzende Unterlagen, die die Prüfergebnisse dokumentieren und nachvollziehbar machen:

- FMEA, Fehlerbaumanalyse o. ä.
- Liste der Fehler, die nicht automatisch von der Sicherheitsvorrichtung erkannt werden und zur Betriebshemmung führen; Bewertung der Zulässigkeit bei jedem der genannten Fehler.
- Bewertung der Beeinflussbarkeit der sicherheitsrelevanten Software durch andere Software-Teile oder Geräteteile oder durch ein eventuell vorhandenes Betriebssystem
- Bewertung der Stack-Heap-Analyse
- Bewertung der Beeinflussbarkeit der sicherheitsrelevanten Software über Schnittstellen
- Bewertung der Sicherheit gegen gefährliche Fehlbedienungen
- Bewertung ...
- Checkliste

10 Zusammenfassung

- Ggf. Empfehlungen und Auflagen
- Bei Nichtbestehen: ggf. notwendige Korrekturmaßnahmen

Anhang 2
Länderausschuss-Beschluss[3]

Auszug aus dem Protokoll der 44. Sitzung des Länderausschusses Röntgenverordnung (LARöV) am 27./28. März 2001

Beschluss:

Nach Anlage III der Röntgenverordnung (RöV) vom 8. Januar 1987[4] muss für Schulröntgeneinrichtungen und Hochschutzgeräte, sowie im Falle von Vollschutzgeräten[5] durch zwei voneinander unabhängige Einrichtungen, sichergestellt sein, dass die Röntgenröhre oder der Röntgenstrahler nur bei vollständig geschlossenem Schutzgehäuse betrieben werden kann. Die zur Realisierung dieser Forderung eingesetzten Schutzeinrichtungen müssen dem Sicherheitsgrad „Kategorie 3“ der Norm DIN EN 954-1 vom März 1997 genügen. Außerdem sind die diesbezüglichen Regelungen der Norm DIN 54113 Teil 2 vom September 1992 zu erfüllen. Damit wird sichergestellt, dass das Versagen einer Komponente nicht den Ausfall der Schutzeinrichtung zur Folge hat und ein aufgetretener Fehler spätestens beim nächsten Einschalten der Röntgenstrahlung erkannt und ein Einschalten der Strahlung verhindert wird.

Zusätzlich wird festgestellt, dass nach dem Abschalten der Beschleunigungsspannung der Röntgenröhre wegen der je nach Bauart unterschiedlich langsam sich abbauenden „Reststrahlung" Vollschutzgeräte, Schulröntgeneinrichtungen und Hochschutzgeräte mit Inkrafttreten der novellierten RöV[6] mit einer Zeitverzögerung versehen werden müssen, so dass die Öffnung der Geräte erst dann möglich ist, wenn die Beschleunigungsspannung der Röntgenröhre 5 kV unterschritten hat.

[3] Die in diesem Länderausschussbeschluss erwähnten Normen sind veraltet. Insbesondere die Norm DIN EN 954-1 ist nicht mehr gültig. Daher wurde das Sicherheitsniveau in diesem Leitfaden unter Nutzung der aktuellen Normen DIN EN 62061 und DIN EN 13849-1 und unter Berücksichtigung der damaligen Zielsetzung neu festgelegt. Aus heutiger Sicht besteht die wesentliche Aussage dieses Beschlusses darin, dass (indirekt) eine aktive Verriegelung gefordert wird. Diese Anforderung lässt sich nicht unmittelbar aus Normen ableiten.

[4] In der aktuellen Version der Röntgenverordnung - in der Fassung der Bekanntmachung vom 30. April 2003 (BGBl. I, S. 604), die zuletzt durch Artikel 6 der Verordnung vom 11. Dezember 2014 (BGBl. I S. 2010) handelt es sich um die Anlage 2.

[5] Seit der Novelle der Röntgenverordnung im Jahr 2002 müssen alle Anforderungen an Vollschutzgeräte auch für Schulröntgeneinrichtungen gelten.

[6] D. h. seit 18. Juni 2002.

Anhang 3
Beispiele für Maßnahmen zur Fehlervermeidung

Ermittlung der zu erwartenden Beanspruchung und Auswahl geeigneter Bauelemente.

- Schalter, Relais:
  - Schalthäufigkeit
  - Bemessung des Schaltstromes so, dass Selbstreinigung der Kontakte gewährleistet ist,
  - Berechnung der maximalen Ströme
  - Auswahl des Kontaktmaterial
  - Schaltelemente zur Funkenlöschung vorsehen
- Widerstände, Halbleiter:
  - Maximale Umgebungstemperatur
  - Maximale Verlustleistung der Schaltelemente, Berechnung von Kühlkörpern
- Kondensatoren:
  - Maximale Gleichspannung
  - Prüfung, ob bei polarisierten Kondensatoren (Elektrolytkondensatoren) zu einem Betriebszeitpunkt eine falsche Polung der Gleichspannung eintreten kann
- Leiterbahnen, Kabel, Leitungen:
  - Querschlussfestigkeit
  - Isolationsfestigkeit
  - Sicherheit gegen Übersprechen
  - Ausreichender Querschnitt

Bundesministerium
für Wirtschaft
und Energie

Die Physikalisch-Technische Bundesanstalt, das nationale Metrologieinstitut, ist eine wissenschaftlich-technische Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Energie.

Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Bundesallee 100
38116 Braunschweig

Presse- und Öffentlichkeitsarbeit

Telefon: (0531) 592-93 21
Fax: (0531) 592-30 08
E-Mail: presse@ptb.de
www.ptb.de

Vertrieb:
Fachverlag NW in der
Carl Schünemann Verlag GmbH

Zweite Schlachtpforte 7
28195 Bremen

Telefon: (04 21) 369 03-0
Fax: (04 21) 369 03-63
www.schuenemann-verlag.de