2 Vorgehensweise

2.1 Fehler- und Gefährdungsanalyse

Die Fehler- und Gefährdungsanalyse ist die Ermittlung aller Fehlfunktionen und Gefährdungen und deren auslösenden Ursachen für das Produkt/System und dessen Komponenten. In der Vorgehensweise sind alle Funktionen zu betrachten bzgl. der Umstände (bestimmungsgemäßer und unsachgemäßer Gebrauch) und der Wirkung auf Personen (Anwender, Service Personal, Unbeteiligte) und oder Sachen (Geräte, Umwelt, Umgebung, Daten). In der Fehler- und Gefährdungsanalyse werden nicht nur direkt vom System verursachte Auswirkungen berücksichtigt sondern auch indirekte, die z.B. durch falsche Informationen zustande kommen.

Die einzelnen Komponenten des Systems und deren Aufgaben im Gesamtsystem sind im Absatz 3 beschrieben. Die einzelnen Funktionen sind im Pflichtenheft [2] detailliert beschrieben.

2.2 Bewertung der Bedeutung

Die in der Fehler- und Gefährdungsanalyse ermittelten Punkte werden entsprechend ihrer Bedeutung klassifiziert. Die Einstufung ist umso höher, je schwerwiegender die Auswirkungen einer Fehlfunktion sind.

Zur Klassifizierung der Bedeutung werden folgende Merkmale verwendet:

Klasse	Auswirkung	Beschreibung der Auswirkungen
1	Keine	Die Fehlfunktion hat keine Einflüsse auf das Systemverhalten. Es ist nicht zu erwarten, daß der Anwender/Kunde die Fehlfunktion bemerkt.
2	Unwesentlich	Die Fehlfunktion hat leichte Einflüsse auf das Systemverhalten. Die Bedeutung des Fehlers löst leichte Unzufriedenheit des Anwenders/Kunden aus.
3	Störend	Die Fehlfunktion hat deutlich merkbare Einflüsse auf das Systemverhalten. Die Bedeutung des Fehlers löst spürbare Unzufriedenheit des Anwenders/Kunden aus.
4	Kritisch	Die Fehlfunktion verhindert eine Arbeit mit/am System. Die Unzufriedenheit des Kunden ist groß, da das System nicht anwendbar ist und/oder seine Arbeitsprozesse stört.
5	Schäden	Die Fehlfunktion verursacht Folgeschäden an Einrichtungen, der Umwelt, an gespeicherten Informationen oder Daten. Die Unzufriedenheit des Kunden ist sehr groß.
6	Sicherheit	Die Fehlfunktion verursacht sicherheitsrelevante Folgeschäden. Die Sicherheit des Anwenders/Kunden, von Unbeteiligten, von Einrichtungen, der Umwelt oder ist nicht gewährleistet. Die Einhaltung des Datenschutzes ist nicht gewährleistet. Vorhandene gesetzliche Vorschriften werden nicht eingehalten.

2.3 Auftretenswahrscheinlichkeit

Jeder dieser Punkte wird zusätzlich unter dem Gesichtspunkt der vermuteten Wahrscheinlichkeit des Auftretens betrachtet. Die Abschätzung der Wahrscheinlichkeit erfolgt gemäß dem Stand der Technik und den vorhandenen Erfahrungen.

Die Auftretenswahrscheinlichkeit einer Fehlfunktion wird in die folgenden Klassen eingeteilt:

Klasse	Wahrscheinlichkeit	Beschreibung der Wahrscheinlichkeit
A	Unvorstellbar	Das Auftreten des Fehlers ist unvorstellbar und tritt nach menschlichem Ermessen und entsprechend der verfügbaren Erfahrungen während der Gebrauchsdauer nicht ein.
B	Unwahrscheinlich	Das Auftreten des Fehlers ist unwahrscheinlich aber möglich.
C	Vorstellbar	Das Auftreten des Fehlers ist entfernt vorstellbar, tritt aber vermutlich nicht auf.
D	Gelegentlich	Tritt wahrscheinlich wenigstens einmal während der Gebrauchsdauer auf.
E	Wahrscheinlich	Tritt wahrscheinlich einige Male während der Gebrauchsdauer auf.
F	Häufig	Das Auftreten der Fehlfunktion ist mit an Sicherheit grenzender Wahrscheinlichkeit gegeben.

Systematische Ausfälle, deren Ursache auf Designfehler zurückzuführen sind (.z.B. falsche Programmierung der Auswerteapplikation) werden hier nicht berücksichtigt, da die einwandfreie Funktion durch die vorgesehenen Tests weitgehend sichergestellt ist. Die Auftretenswahrscheinlichkeit für diese Art von Ereignissen ist daher kaum vorherzusagen.

2.4 Risikobereiche

Für jeden Fehler bzw. für jede Gefährdung ergibt sich aus den o.g. Abschätzungen das Risiko. Dieses Risiko wird in drei Bereiche eingeteilt (siehe auch Abbildung 1).

AA Bereich (allgemein akzeptabel)

In diesen Fällen ist die Bedeutung des Fehlers oder der Gefahr und(oder die Auftretenswahrscheinlichkeit so gering, daß das Risiko im Vergleich zu anderen Gefährdungen, die allgemein akzeptiert werden, genügend klein ist. Maßnahmen zur Risikoreduzierung sind nicht erforderlich.

GVM Bereich (so gering wie vernünftigerweise möglich)

Die Risiken sind unter Abwägung der Vorteile aus der risikobehafteten Funktion einerseits und der Nachteile einer weiteren Risikoreduzierung, wie z.B. Funktionseinschränkung andererseits auf das niedrigste praktikable Niveau reduziert.

Jedes Risiko muß auf ein Niveau zurückgeführt werden, welches “so gering wie vernünftigerweise möglich” (GVM) ist. Weitere Maßnahmen sind in der Regel dann erforderlich, wenn das Risiko nahe am nicht akzeptablen Bereich liegt, selbst wenn damit zusätzlicher Aufwand verbunden ist.

NA Bereich (nicht akzeptabel)

In diesem Fall ist das Risiko so hoch, daß es nicht vertretbar wäre. Solche Risiken sind durch weitere Maßnahmen zu reduzieren, welche die Bedeutung und/oder die Auftretenswahrscheinlichkeit verringern.

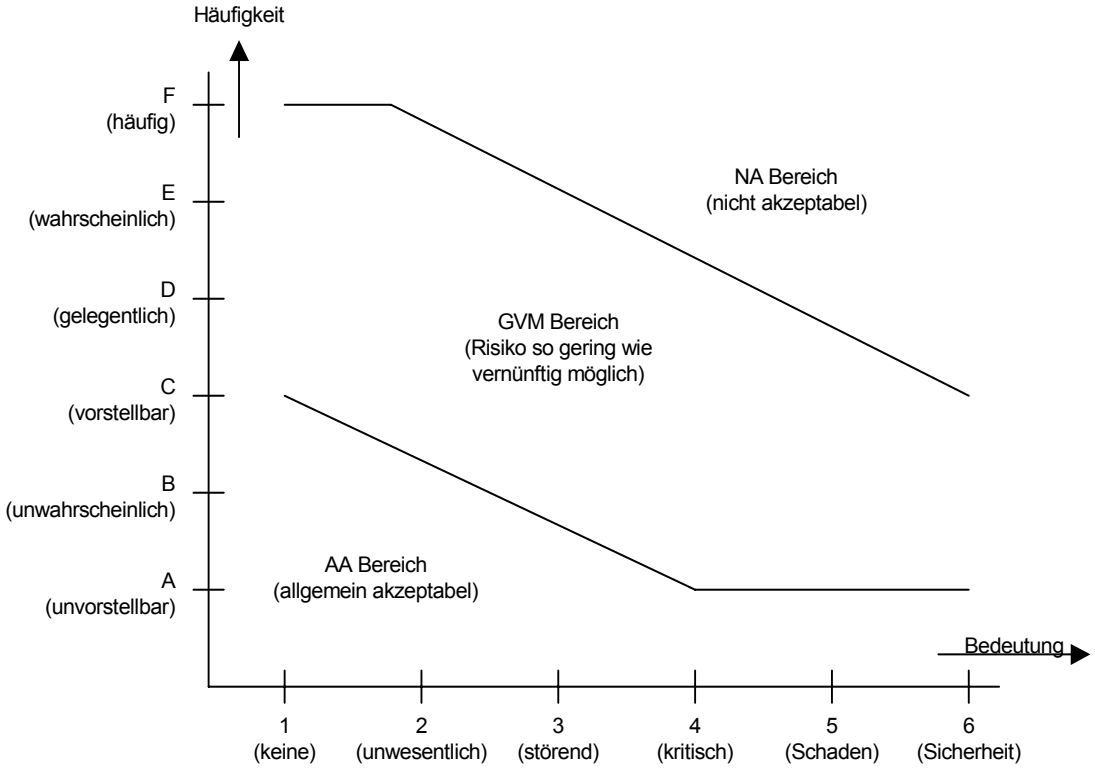

Abbildung 1: Risikobereiche.

2.5 Ablauf

Schritt 1: Betrachtung aller Funktionen

Die Risikobetrachtung beginnt mit einer Auflistung aller relevanten Funktionen und/oder aller Funktionskombinationen der einzelnen Komponenten und den daraus resultierenden Fehler- oder Gefährdungsmöglichkeiten. Die Identifizierung der Fehler- oder Gefährdungsmöglichkeiten ist unabhängig davon, ob Hardware- oder Softwarekomponenten oder auch menschliches Versagen (wie z.B. Fehlbedienungen) für den Fehler oder die Gefährdung verantwortlich sind.

Die wesentlichen Funktionsblöcke sind im Kapitel 3 beschrieben.

Schritt 2: Feststellen der Auswirkungen

Als nächstes wird festgestellt, welche möglichen Fehlfunktionen oder Gefährdungen auf die zu untersuchende Funktionseinheit einwirken können oder von dieser ausgehen können. Für jede der relevanten Funktionen und/oder aller Funktionskombinationen müssen alle Fehlfunktionen oder Gefährdungen aufgelistet werden.

Die Auflistung der Fehlfunktionen oder Gefährdungen sind im Kapitel 4 beschrieben.

Schritt 3: Ermittlung der Ursachen und Klassifizierung

Zu einer Fehlfunktion oder Gefährdung können verschiedene Ursachen beitragen. Diese Ursachen sind zu ermitteln und zu beschreiben. Zu jeder Fehlfunktion oder Gefährdung ist die Bedeutung und die Auftretenswahrscheinlichkeit zu ermitteln. Aus diesen beiden Kriterien ergibt sich unter Verwendung der Grafik aus Abbildung 1 der Risikobereich.

Wird bereits in diesem Schritt das Risiko als aktzeptabel eingestuft, so sind keine weiteren Schritte für diese Funktion durchzuführen.

Die Beschreibung der Ursachen und die Klassifizierung befindet sich in Kapitel 5.

Schritt 4: Unmittelbare Reduzierbarkeit der Risiken

Es ist zu klären, ob durch unmittelbare Maßnahmen (System-Architektur, Hardwareeinsatz, Softwaremeachanismen, etc.) die Bedeutung der Fehlfunktion oder Gefährdung und/oder die Auftretenswahrscheinlichkeit reduziert werden kann. Falls Maßnahmen durchzuführen sind, so sind diese zu beschreiben.

Sind die Maßnahmen bereits in der Anforderungsspezifikation [2] an das Produkt/System definiert, so ist eine Referenz auf die Funktion im Pflichtenheft durch Angabe des oder der Requirement Keys herzustellen.

Sind die Maßnahmen noch nicht adressiert, so sind diese in die Maßnahmenliste aufzunehmen. Die Abarbeitung der Maßnahmenliste ist durch Aufnahme in den Testplan sicherzustellen.

Die durchzuführenden Maßnahmen sind in Kapitel 5 beschrieben. Die Maßnahmenliste befindet sich im Kapitel 6.

Schritt 5: Reduzierbarkeit durch Schutzmaßnahmen

Es ist zu klären, ob durch zusätzliche Schutzmaßnahmen (regelmäßige Funktionsüberwachungen, redundante Technik, gespiegelte Datenhaltung, etc.) die Bedeutung der Fehlfunktion oder Gefährdung und/oder die Auftretenswahrscheinlichkeit reduziert werden kann oder das System bzw. die Funktion beim Auftreten einer Fehlfunktion wenigstens in einen sicheren oder unkritischen Bereich gebracht werden kann.

Sind die Maßnahmen bereits in der Anforderungsspezifikation [2] an das Produkt/System definiert, so ist eine Referenz auf die Funktion im Pflichtenheft durch Angabe des oder der Requirement Keys herzustellen.

Sind die Maßnahmen noch nicht adressiert, so sind diese in die Maßnahmenliste aufzunehmen. Die Abarbeitung der Maßnahmenliste ist durch Aufnahme in den Testplan sicherzustellen.

Die durchzuführenden Maßnahmen sind in Kapitel 5 beschrieben. Die Maßnahmenliste befindet sich im Kapitel 6.

Schritt 6: Reduzierbarkeit durch Warnhinweise

Wenn sowohl unmittelbare als auch mittelbare Maßnahmen nicht möglich sind oder nicht ausreichen, ist zu prüfen, ob durch Alarmfunktionen oder beschreibende Sicherheitstechnik (Gebrauchsanweisung, Online-Hilfe, Aufkleber, Warnhinweise, Schulung, etc.) das Risiko angemessen reduziert werden kann.

Sind diese Maßnahmen noch nicht adressiert, so sind diese in die Maßnahmenliste aufzunehmen. Die Abarbeitung der Maßnahmenliste ist durch Aufnahme in den Testplan sicherzustellen.

Die durchzuführenden Maßnahmen sind in Kapitel 5 beschrieben. Die Maßnahmenliste befindet sich im Kapitel 6.

Schritt 7: Bewertung des Restrisikos

Das durch die theoretische Durchführung der Schritte 4 bis 6 verbleibende Restrisiko muß unter den gleichen Gesichtspunkten neu bewertet werden. Ist das Restrisiko auch nach Anwendung mehrerer Maßnahmen nicht vertretbar, so muß über die weitere Vorgehensweise im Rahmen der Produktentwicklung entscheiden werden. Gegebenenfalls muß nachgewiesen werden, daß das Restrisiko bei Abwägung des Nutzens für den Kunden vertretbar ist.

Die Beschreibung der Bewertung der Restrisiken befindet sich in Kapitel 5.

Schritt 8: Zusätzliche neue Fehlfunktionen bzw. Gefährdungen

Es ist zu prüfen, ob durch die aus den Schritten 4 bis 6 evtl. neu aufgenommenen Maßnahmen bzw. Anforderungen neue oder andere mögliche Fehlfunktionen oder Gefährdungen hervorgerufen werden. Diese müssen dann zusätzlich untersucht und auf die gleiche Weise betrachtet werden.

Die Beschreibung neu entstandener Fehlermöglichkeiten befindet sich in Kapitel 5.