Funktionale Sicherheit des Plasmasystems PB3/PS2000

Sicherheitsbetrachtung angelehnt an EN ISO 13849

Durch Systemabgrenzung, Identifikation der Gefährdung und Risikoabschätzung lässt sich durch entsprechende Maßnahmen der Risikominderung eine sichere Plasmaanlage aufbauen, die mindestens ein Performancelevel D erreicht.

Sicherheitssysteme

Sicherheitssysteme sind aktive oder passive Anlagenkomponenten, die technische Anlagen für den Menschen sicher machen sollen.

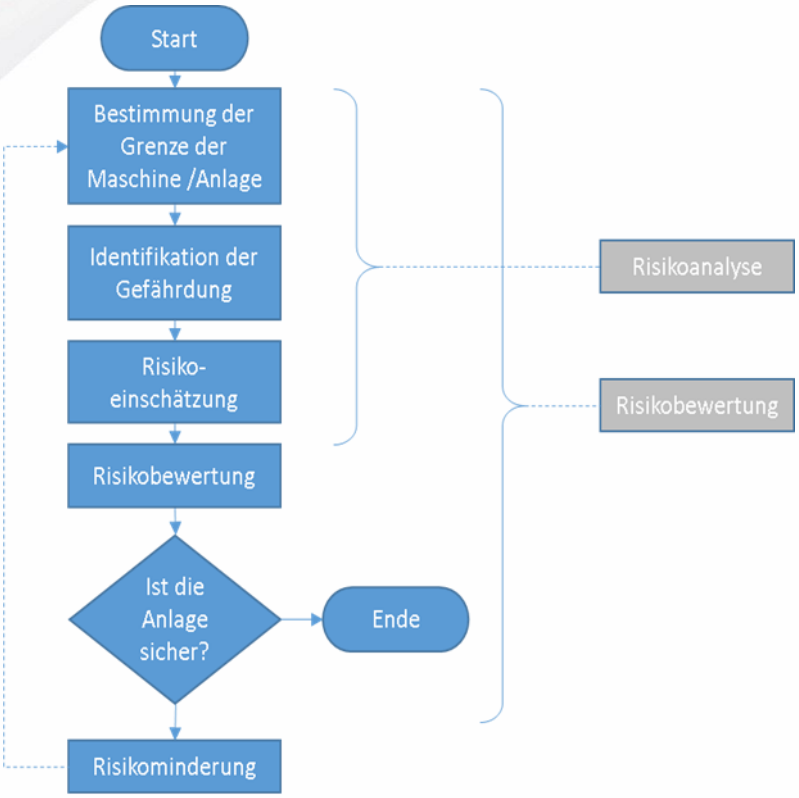

Abbildung 1 Flussdiagramm zur Risikoabschätzung

Von Maschinen, Anlagen und allen anderen technischen Einrichtungen gehen Gefahren für den Menschen aus. Dabei sind oft nicht nur die Betreiber, sondern auch Wartungspersonal oder Unbeteiligte direkt oder indirekt gefährdet. Dabei hängt die Gefährdung sowohl von der Art und Funktionsweise der Maschine oder Anlage als auch von dem Verhalten der betreffenden Person ab.

In der Regel werden Maschinen oder Anlagen mit elektrischen oder elektronischen Systemen gesteuert. Diese Systeme sind letztlich dafür verantwortlich, dass der Mensch keine Gefahr eingeht. An die Systeme werden daher gewisse Anforderungen gestellt, die sich aus dem Risiko ergeben, das für die involvierte Person besteht. Um die Gefahren einer Maschine oder Anlage einstufen zu können, wird eine Gefahrenanalyse durchgeführt. Besonders bei elektrischen Systemen, bei denen gefährliche Spannungen anliegen können, sind besondere Vorkehrungen zu treffen, um diese Systeme sicher zu machen. Für die Risikobetrachtung wird im Folgenden die induktive Analyse angesetzt, indem der

Ausfall von kritischen Komponenten angenommen wird und der Effekt auf die Umgebung oder den Nutzer bestimmt wird.

Systemdefinition und Systemgrenzen

Abbildung 2 Plasmasystem, bestehend aus 19Zoll Hochspannungsquelle, Hochspannungskabel und Erzeugerdüse.

Die Stromversorgung PS2000 ist Teil eines Atmosphärendruck-Plasmagenerators, der zur atmosphärischen Plasmabehandlung bzw. -vorbehandlung von verschiedensten Materialoberflächen eingesetzt wird.

Er ist für industrielle Anwendungen bestimmt, in denen beispielsweise Oberflächen vor dem Bedrucken, Verkleben oder Lackieren mit Plasma aktiviert und gereinigt werden. Das Gehäuse ist für den Schaltschrankeinbau vorgesehen. Die Stromversorgung PS2000 ist ausschließlich für den Betrieb eines Plasmaerzeugers der Firma relyon plasma GmbH vorgesehen und daher wird in der Risikoanalyse das Gesamtsystem, bestehend aus Hochspannungsquelle und Plasmaerzeuger, betrachtet.

Die PS2000 ist nach Maschinenrichtlinie mit einem Notauskreis ausgerüstet, der hier als zusätzliche Sicherheitsmaßnahme bewertet werden soll.

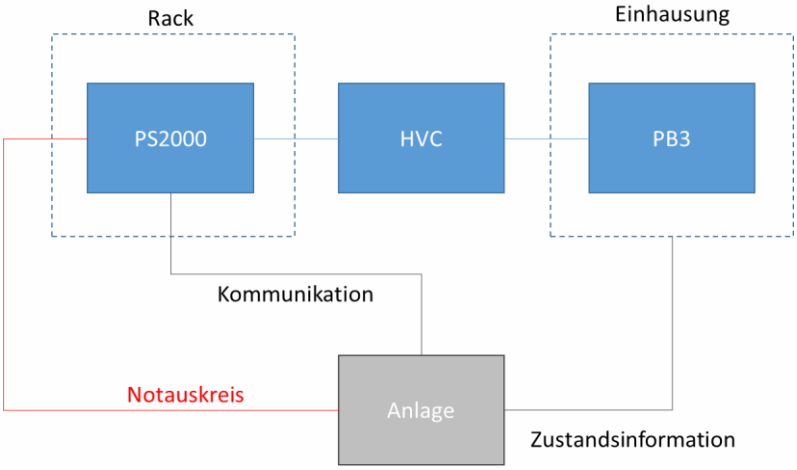

Abbildung 3 Blockdiagramm der Hochspannungsquelle (PS2000), die über ein Hochspannungskabel (HVC) an einen Plasmaerzeuger (PB3) angeschlossen ist. Dabei ist die PS2000 in ein Rack eingebaut und der Plasmaerzeuger in einer

sicheren Einhausung mit Schutzvorrichtung (Tür oder Lichtschranke) gegen unbeabsichtigte Berührung geschützt. Alle Informationen der Schutzvorrichtung werden mit der übergeordneten Anlage ausgetauscht. Der Notauskreis ist über einen gesonderten Kanal verknüpft.

Fehlerhäufigkeit (Risikobewertung)

Bei der vorliegenden Sicherheitsbetrachtung wird ausdrücklich nur die Sicherheit der funktional verknüpften Komponenten PS2000, HVC und PB3 bewertet. Es wird davon ausgegangen, dass diese Komponenten nach Vorgabe der Bedienungshinweise in eine nach Maschinenrichtlinie aufgebaute Anlage eingebettet sind. Die Funktion der Gesamtanlage wird hier nicht bewertet. Insbesondere wird davon ausgegangen, dass die übergeordnete Anlage fehlerfrei funktioniert und zu den Risiken nicht beiträgt. Beispielsweise wird also nicht bewertet, ob das Notaussignal der Anlage korrekt abgesetzt wird oder die Einhausung des Plasmaerzeugers sicher umgesetzt wurde. Auch eine je nach Prozess erforderliche Absaugung wird hier nicht betrachtet.

Mögliche Fehler (Identifizierung der Gefährdung)

1. Berührung des geöffneten PB3 Erzeugers bei geöffneter Anlage
2. Berührung des Lichtbogens bei laufender Anlage
3. Schaden am Hochspannungskabel
4. Trennung des Hochspannungskabels vom Plasmaerzeuger im Betrieb
5. Trennung des Hochspannungskabels von der Hochspannungsquelle im Betrieb

Alle Fehler, die mit hochspannungsführenden Bauteilen in Verbindung stehen, werden als schwerwiegende Fehler mit hohem Risiko für Gesundheit und Leben eingestuft und müssen daher in einem entsprechenden Sicherheitskonzept vermieden oder abgefangen werden.

Fehler 1 (Berührung des geöffneten PB3 Erzeugers bei geöffneter Anlage) und Fehler 2 (Berührung des Lichtbogens bei laufender Anlage) können täglich auftreten, beispielsweise im Rahmen einer Wartung bzw. eines Öffnens der Anlage oder aufgrund eines manuellen Eingriffs in den Produktionsprozess.

Zwar kann eine erhebliche Schädigung der gefährdeten Person die Folge sein, jedoch werden beide Fehler über den Notauskreis sicher abgefangen, wenn dieser entsprechend der Richtlinien in das übergeordnete Anlagenkonzept eingebunden ist.

Fehler 3 (Schaden am Hochspannungskabel) tritt nur selten auf. Im Fehlerfall wird typischerweise ein Hochspannungsdurchschlag zu einem Kabelkurzschluss führen und die Spannungsquelle schaltet ab (Fehler: Strom zu hoch). Bei den im Feld befindlichen Anlagen ist dieser Fehler durch falsche Handhabung, Verschleiß oder sonstige Gründe auf geschätzte 1.000.000 Betriebsstunden bislang weniger als zehn Mal aufgetreten und hat in jedem Fall zum Abschalten der PS2000 geführt. Der Fehler ist persistent und ein erneutes Hochfahren der Anlage führt unmittelbar zum identischen Fehler. Das Kabel und die Steckverbindung sind brandgehemmt und selbstlöschende Ausführungen. Um das Risiko der Brandgefahr und die Sicherheit der Fehlererkennung beim Kabelschaden genauer einzugrenzen, ist eine systematische und praktische Fehlersimulation durchgeführt worden.

Fehler 4 (Trennung des Hochspannungskabels vom Plasmaerzeuger im Betrieb) tritt nur dann auf, wenn bei Wartungsarbeiten die Hochspannungsverbindung getrennt und anschließend die Anlage wieder hochgefahren wird; die Sicherheitsvorkehrungen hierfür sind dieselben wie für Fehler 5 (Trennung des Hochspannungskabels von der Hochspannungsquelle im Betrieb). Für beide Fälle wird die Fehlerhäufigkeit aus der Praxis mit 1/Jahr abgeschätzt. Alle Verbindungen sind mit Stecker/Buchse-Systemen (Typ HSB30 GES Electronic) ausgeführt, so dass die spannungsführende Seite stets berührungssicher ist und ein Durchschlag via Lichtbogen nicht erfolgen kann. Die

Trennung von Stecker und Buchse kann nur durch bewusstes Lösen des Schraubverschlusses erreicht werden. Die Hochspannungsversorgung wird daraufhin einen Zustand ohne Last detektieren und nach 1s wegen Erreichen der maximalen Zündspannung mit einer Fehlermeldung den Hochspannungsteil abstellen. Die Kommunikation läuft weiter.

Fehler 4 und 5 können auch auftreten, wenn die Steckverbindungen nur lose verbunden wurden und sich während des Betriebs lockern. Hierdurch kann ein Betriebszustand entstehen, bei dem ein Lichtbogen zwischen Buchse und Stecker brennt. Da jedoch die Stecker einen Eingriff mit mehreren mm Hub besitzen und durch eine Überwurfverschraubung gegen Lösen gesichert sind, ist dieser Fall selten und wird ohne gesonderte Betrachtung unter 4 und 5 summiert.

Fehler 1 und 2 werden durch ein geeignetes Notaus-Konzept komplett abgefangen. Das Error Handling für Fehler 3-5 erfolgt durch die Notabschaltung der PS2000 innerhalb einer zu bewertenden Latenzzeit und einer zu bewertenden Zuverlässigkeit.

Performance Bewertung des internen Notaus-Konzeptes

Die einzige nach außen geführte gefährliche Spannung bei der PS 2000 ist die Hochspannung, die über ein Schaltnetzteil im Gerät aktiv erzeugt wird. Entfällt die Taktung des Schaltnetzteiles, kann am Ausgang keine Spannung mehr anliegen, da der Hochspannungsausgang von allen anderen Spannungsversorgungen streng galvanisch getrennt ist.

Das externe Ausschalten der Hochspannung kann entweder durch einen Hochspannung-Aus-Befehl über die CAN-Kommunikationsschnittstelle erfolgen oder durch Auslösen des Notaus.

Notaus (Geräterückseite PS2000)

Die PS2000 besitzt auf der Geräterückseite einen Notausstecker. Bei geöffnetem Notauskontakt (externe Komponente, hier nicht bewertet) wird über ein konventionelles Relais die Netzspannung vom PFC Modul und damit vom Zwischenkreis getrennt. Ebenso wird bei geöffnetem Notaus die Ansteuerung des Schaltnetzteils zur Hochspannungserzeugung gestoppt.

Das interne Trennrelais (Finder 45.91) ist einstufig ausgeführt und besitzt eine mittlere Lebensdauer von $>3*10^4$ Zyklen. Im Fehlerfall könnte beispielsweise das Relais klemmen oder festbacken und nicht mehr sauber trennen. Fällt das Relais aus, bewirkt der geöffnete Notaus ebenso auf einem davon getrennten Kanal eine unmittelbare Unterbrechung der Taktung des Schaltnetzteiles und die Spannung geht in weniger als fünf Millisekunden auf ein unkritisches Niveau zurück.

Beim simulierten Relaisausfall (Brücke) wurde unter allen möglichen Betriebszuständen der PS2000 die Reproduzierbarkeit der softwaregestützten Abschaltung der Hochspannung getestet. Bei einer Zyklenzahl von 10^4 wurde hier kein Fall erzeugt, bei dem eine unzulässige Spannung an der Ausgangsbuchse anlag. Sollte ein fataler Fehler der internen Firmware oder ein Ausfall der Hilfsspannungsversorgung eintreten, stoppt auch die Taktung des Schaltnetzteiles und es wird keine Hochspannung mehr erzeugt.

Damit kann das PL des Not-Aus bewertet werden mit:

Ausfallwahrscheinlichkeit des Relais pro Stunde bei angenommener Häufigkeit des Fehlers von 1/Tag:

$$P_{Rel} < 1/24*1/30.000 = 1.38 \times 10^{-6}$$

$$P_{Soft} < 10^{-4}$$

$$\underline{P_{Notaus} < 1.38e^{-6}*10^{-4} = 1.38*10^{-10}}$$

Risikobewertung der Beschädigung der Hochspannungsleitung (Fehler 3)

Wird die Hochspannungsleitung beschädigt oder tritt durch Materialermüdung ein Schaden auf, der die Isolation soweit schwächt, dass ein Überschlag auftritt, kann eine gefährliche Situation auftreten.

Durch simulierten Schadensfall am Kabel konnte nachgewiesen werden, dass bei 200 Versuchen jedes Mal die PS2000 nach weniger als einer Sekunde in den spannungslosen Zustand übergeht, ohne dass dabei ein Brandherd entsteht. Die Fehlerwahrscheinlichkeit setzt sich aus mehreren Komponenten zusammen, die im Folgenden abgeschätzt werden:

$P_{Kabelschaden} < 10/300/4000 = 8{,}33*10^{-6}$ (weniger als 10 Schäden bei 300 Anlagen, die im Mittel 4000 Stunden pro Jahr in Betrieb sind)

$P_{Nichterkennung} < 1/200 = 5*10^{-3}$ (200 Kabelschäden wurden induziert und ausgewertet)

Hieraus errechnet sich ein oberer Grenzwert für einen kritischen Fehler auf der Hochspannungsstrecke:

$P_{HVC1} = P_{Kabelschaden} * P_{Nichterkennung} < 4{,}16*10^{-8}$

Risikobewertung des unsachgemäßen Trennens der Hochspannungsverbindung (Fehler 4-5)

Unter der Annahme, dass die Verbindung von Hochspannungsquelle und Plasmaerzeuger zweimal im Jahr unsachgemäß und im Betrieb getrennt wird oder bei getrenntem Zustand die Anlage in Betrieb geschaltet wird, gilt folgende Fehlerwahrscheinlichkeit pro Stunde:

$P_{Trennung} < 2/365*24 = 2{,}28*10^{-4}$

$P_{Nichterkennung}<1/10.000$ (Erkennung und Lastabwurf durch 5x2000 Prüfungen)

$P_{HVC2}= P_{Trennung}* P_{Nichterkennung} <2{,}3*10^{-8}$

Die Durchführung erfolgte durch Prüfung des Abschaltens bei Fehlen der Last an fünf zufällig gewählten Geräten über jeweils 2000 Zyklen.

Zusammenfassung der Gesamtrisiken

Durch Summierung der verschiedenen Risiken (zu Fehlertypus 1-5) mit Wichtung der zugeordneten Sicherheitsmaßnahmen ergibt sich für die Gesamtwahrscheinlichkeit, dass ein gefährlicher Fehler auftritt, pro Stunde ein Wert von $<10^{-7}$.

$P_{gesamt}= P_{UVC1}+P_{HVC2+}P_{Notaus} < 4{,}16*10^{-8}+2{,}3*10^{-8}+8{,}33*10^{-6} < 10^{-7}$

Damit kann für die betrachteten Fehler dem Plasmasystem PB3 (Erzeuger) mit dem vorgeschriebenen Hochspannungskabel und der vorgesehenen Hochspannungsquelle PS2000 bei Einbau in einer geeigneten Anlage ein PL=D zugeordnet werden.

Performance Level (PL) nach EN ISO 13849-1	Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde	Sicherheits-Integritätslevel (SIL) nach IEC 61508
A	$10^{-4} – 10^{-5}$	-
B	$10^{-5} – 3\ 10^{-}6$	1
C	$3\ 10^{-6} – 10^{-7}$	1
D	$10^{-7} – 10^{-8}$	2
E	$10^{-7} – 10^{-8}$	3

Abbildung 4 Übersicht über Ausfallwahrscheinlichkeiten und abgeleiteten PL. Die Einstufung des PL-Werts geht von A (niedriger Beitrag zur Risikoreduzierung) bis zu E (hoher Beitrag zur Risikoreduzierung)

Fazit

Durch eine empirische Risikobewertung und die Betrachtung der redundanten Sicherheitskreise in der Hochspannungsversorgung kann das in einer Anlage integrierte Plasmasystem besonders sicher ausgeführt werden. Moderne Technik liefert so einen Beitrag zur Arbeitssicherheit und zur Vermeidung von Störungen.