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

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 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 geboten um diese Systeme sicher zu machen. Für die Risikobetrachtung wird im nachfolgenden die induktive Analyse angesetzt indem der Ausfall von kritischen Komponenten angenommen wird und der Effekt auf die Umgebung oder den Nutzer bestimmt wird.

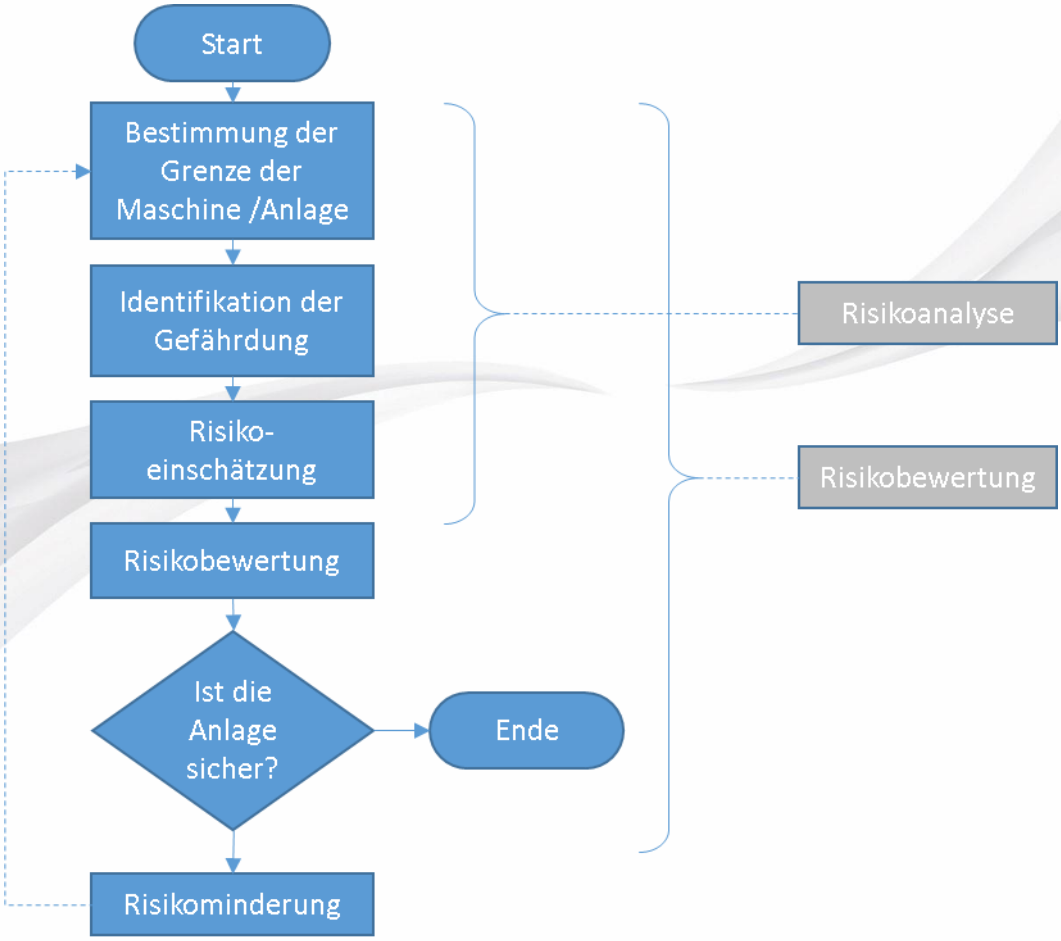

Abbildung 1 Flussdiagramm zur Risikoabschätzung

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.

Es 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 Fa. relyon plasma GmbH vorgesehen und daher wird als Gesamtsystembestehend aus Hochspannungsquelle und Plasmaerzeuger in der Risikoanalyse betrachtet.

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

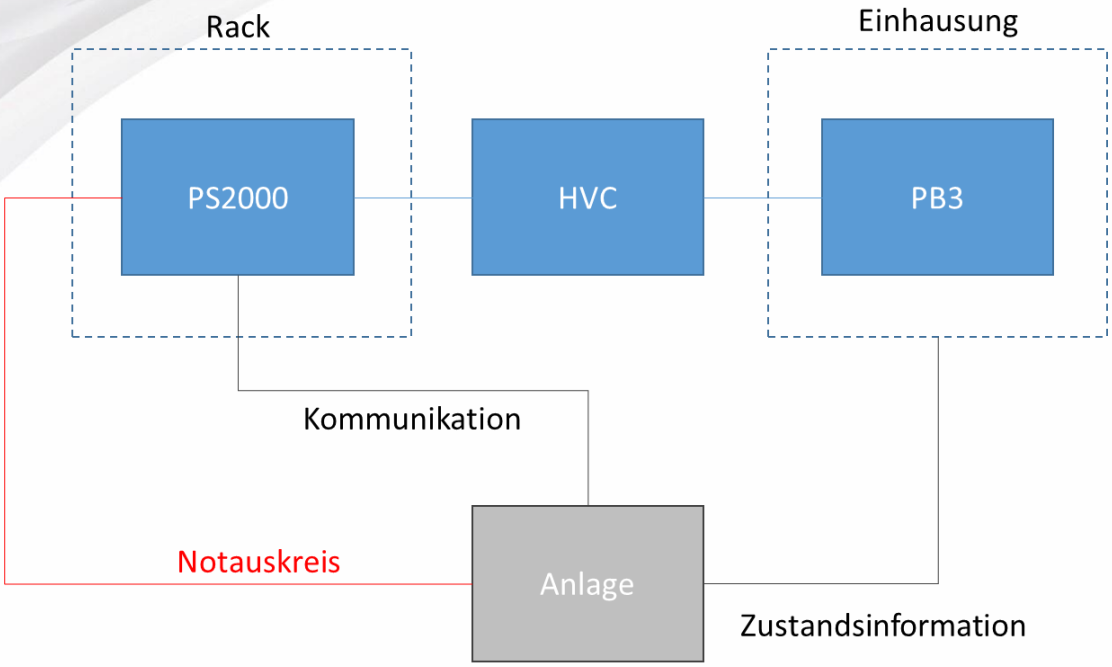

Abbildung 3 Blockdiagramm der Hochspannungsquelle (PS2000) die über ein Hochspannungskabel (HVC) an einen Plasmaerzeuger (PB3) angeschlossen ist. Dabei ist die PS2000 in ein Rack eingebaut und der Plasmaerzeuger in einer sicheren Einhausung mit Schutzvorrichtung gegen unbeabsichtigte Berührung (Tür, oder Lichtschranke). Alle Informationen der Schutzvorrichtungen (Tür oder Lichtschranke) werden mit der übergeordneten Anlage ausgetauscht. Der Notauskreis ist über einen gesonderten Kanal verknüpft.

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 und eingebettet in eine nach Maschinenrichtlinie aufgebauten Anlage eingebettet sind. Die Funktion der Gesamtanlage wird hier **nich**t bewertet. Insbesondere wird davon ausgegangen, dass die übergeordnete Anlage fehlerfrei funktioniert und zu den Risiken nicht beiträgt. Z.B. wird nicht bewertet ob das Notaussignal der Anlage korrekt abgesetzt wird, oder die Einhausung des Plasmaerzeugers sicher umgesetzt wurde.

Mögliche Fehler (Identifizierung der Gefährdung)

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

Fehlerhäufigkeit (Risikobewertung)

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 und 2 können täglich auftreten (Wartung oder öffnen der Anlage, Manueller Eingriff in den Produktionsprozess) und können zu einer erheblichen Schädigung der gefährdeten Person führen.

Fehler 1 und Fehler 2 werden über den Notauskreis sicher abgefangen wenn dieser entsprechend der Richtlinien in das übergeordnete Anlagenkonzept eingebunden ist.

Fehler 3 tritt nur selten auf. Im Fehlerfall wird typischerweise ein Hochspanungsdurchschlag 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 oder Verschleiß oder sonstige Gründe auf abgeschätzte 10^5 Betriebsstunden bislang < 10x 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 notwendig.

Fehler 4 tritt nur dann auf, wenn bei Wartungsarbeiten die Hochspannungsverbindung getrennt wird, und anschließend die Anlage wieder hochgefahren wird. Die Fehlerhäufigkeit wird 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. Diese Trennung kann nur durch bewusstes lösen der Stecker/Buchse Verbindung (Schraubverschluss) erreicht werden. Die Hochspannungsversorgung wird bei ausgestecktem Plasmaerzeuger einen Zustand ohne Last detektieren und nach 1s wegen erreichen der maximalen Zündspannung mit einer Fehlermeldung den Hochspannungsteil abstellen. Die Kommunikation läuft weiter.

Fehler 5 kann auftreten, wenn z.B. im Betrieb das Hochspannungskabel von der Hochspannungsquelle getrennt wird. . Die Fehlerhäufigkeit wird aus der Praxis mit 1/Jahr abgeschätzt. Diese Trennung kann nur durch bewusstes lösen der Stecker/Buchse Verbindung (Schraubverschluss) erreicht werden. Auch in diesem Fall wird die Hochspannungsversorgung einen Zustand ohne Last detektieren und nach 1s wegen erreichen der maximalen Zündspannung mit einer Fehlermeldung den Hochspannungsteil abstellen. Die Kommunikation läuft weiter.

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

Performance Bewertung des internen Notaus Konzeptes

Einzige nach außen geführte gefährliche Spannung ist die Hochspannung, die über ein Schaltnetzteil in der PS2000 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. Z.B. könnte das Relais klemmen oder festbacken und nicht mehr sauber trennen. Fällt das Relais aus, bewirkt der geöffnete Notaus ebenso auf einem davon getrennten Kanal ein unmittelbaren Stopp der Taktung des Schaltnetzteiles und die Spannung geht in <5ms auf ein unkritisches Niveau zurück.

Bei 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. Bei einem fatalen Fehler der internen Firmware oder einem Ausfall der Hilfsspannungsversorgung 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:

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

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

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

Risiko Bewertung der Beschädigung der Hochspannungsleitung (Fehler 3)

Wird die Hochspannungsleitung beschädigt oder durch Materialermüdung tritt 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 100 Versuchen jedes Mal die PS2000 nach <1s in den spannungslosen Zustand übergeht ohne dass dabei ein Brandherd entsteht. Bei der entsprechenden Fehlerwahrscheinlichkeit von

$P_{Kabelschaden} < 10/300/4000 = 8{,}33*10^{-6}$

$P_{Nichterkennung} < 1/200 = 10^{-2}$

Durchgeführt durch Prüfung des Abschaltens bei Fehlen an 200 induzierten Kabelschäden.

$\underline{P_{HV} < 4{,}16*10^{-8}}$

Risiko Bewertung 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:

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

$P_{Nichterkennung} < 1/10.000$

$\underline{P_{HVC} < 2{,}3*10^{-8}}$

Durchgeführt durch Prüfung des Abschaltens bei Fehlen der Last an 5 zufällig gewählten Geräten jeweils 2000 Zyklen.

Zusammenfassung der Gesamtrisiken

Durch Summierung der verschiedene Risiken (zu Fehlertypus 1-5) mit Wichtung der zugeordneten Sicherheitsmaßnahmen ergibt sich für die Gesamtwahrscheinlichkeit das ein **gefährlichen Fehler pro Stunde auftritt ein Wert von <10^{-7}**.

Damit kann für die betrachteten Fehler dem Plasmasystem PB3 (Erzeuger) mit dem vorgeschriebene 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)