**Angewandte Sicherheitsprinzipien und Risikobewertung zum ultraleichten, elektrischen Antriebssystem für Luftsportgeräte**

Bearbeiter: Joachim Geiger
Version: 1.4
Datum: 08.03.2019



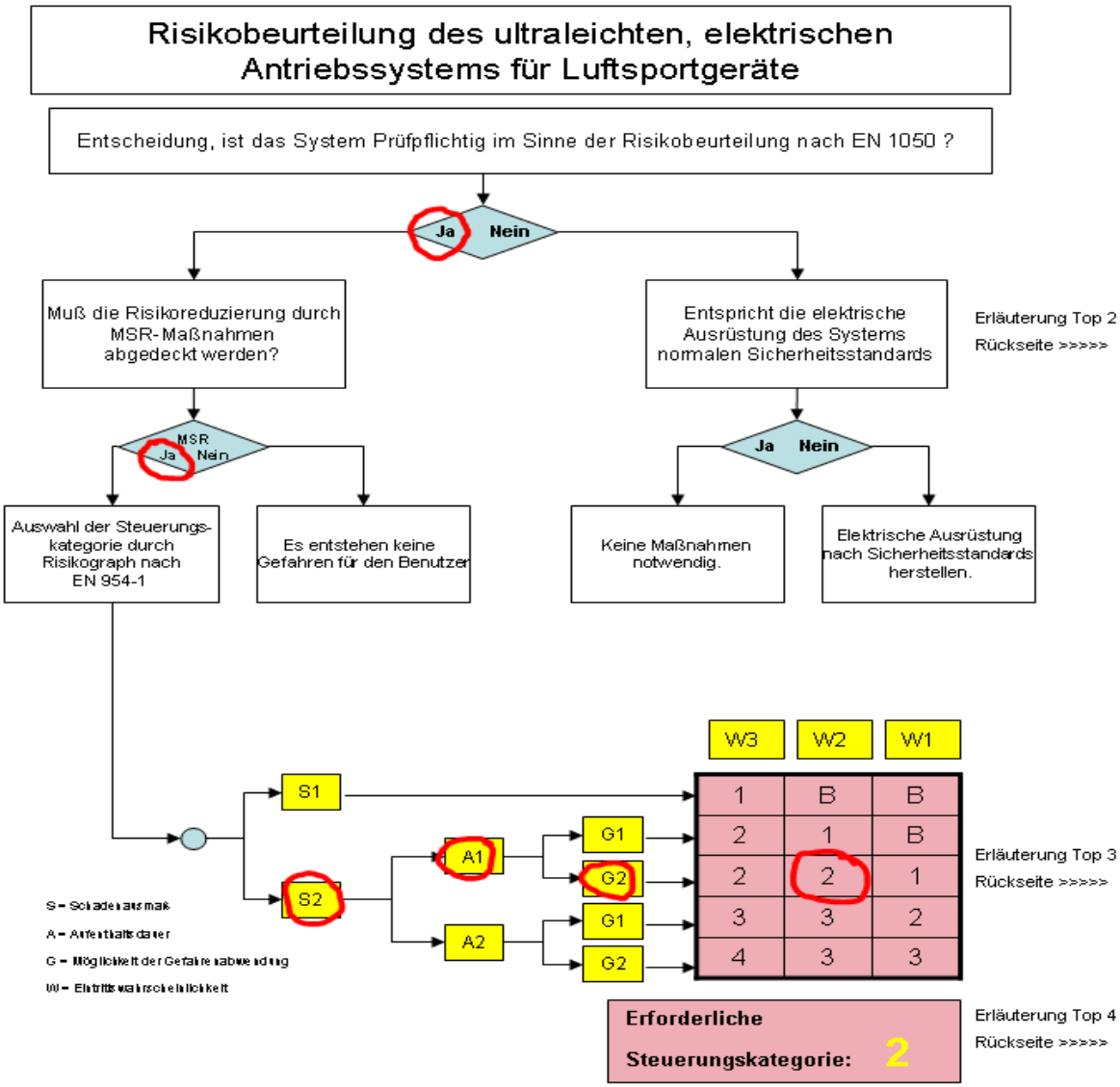

GEIGER ENGINEERING GMBH
Große Wiese 4
96114 Hirschaid

T 09545 4 41 54 80
F 09545 4 41 54 78
M 0170 5 66 77 99

jgeiger@geigerengineering.de
www.geigerengineering.de

## 1. Risikobewertung nach DIN-EN:

Um das vom Antriebssystem ausgehende Gefahrenpotenzial zu bewerten, wurde folgende Risikobewertung nach industriellen und europäischen Sicherheitsrichtlinien und Normen durchgeführt, welche sich auf die nachfolgende Steuerungsauslegung auswirkt:




### Sonstige Maßnahmen:

Darüber hinaus wird das Prinzip der Redundanz angewandt.

Die Betriebsspannung liegt unterhalb des PELV - Niveaus.

Bei manchen Anwendungen ist auch ein Schutzkäfig um den Propellerkreis unabdingbar.

Bamberg, den 05.10.2007 Joachim Steiger

**Top 2:** Folgenden Normen sind anzuwenden:

- EU – Maschinenrichtline 98/37 EWG (MSRL). (entspricht 9. Verordnung des Gerätesicherheitsgesetzes)
- EU – Niederspannungsrichtlinie 73/23 EWG
- EU – EMV-Richtlinie 89/336 EWG

**Top3:** Beschreibung der Risikofaktoren:

- Schadenausmaß S
  - S1 : Leichte Verletzung
  - S2 : Schwere irreversible Verletzung von einer oder mehreren Personen, Tod einer Person
  - S3 : Tod mehrerer Personen
  - S4 : Katastrophale Auswirkung, sehr viele Tote
- Aufenthaltsdauer A
  - A1 : seltener bis öfterer Aufenthalt im Gefahrenbereich
  - A2 : häufiger bis dauernder Aufenthalt im Gefahrenbereich
- Gefahrenabwendung G (Ausweichmöglichkeit im Gefahrenbereich, Dynamik der Antriebe beachten)
  - G1 : möglich unter bestimmten Bedingungen
  - G2 : kaum möglich
- Eintrittswahrscheinlichkeit W
  - W1 : Sehr geringe Wahrscheinlichkeit des unerwünschten Ereignisses
  - W2 : Geringe Wahrscheinlichkeit des unerwünschten Ereignisses
  - W3 : relativ hohe Wahrscheinlichkeit des unerwünschten Ereignisses

Bsp: Weitertakten einer Packmaschine = W3, Anlauf durch einen defekten Umrichter = W1.

**Top 4:** Beschreibung der Steuerungskategorien nach EN 954-1:

- B = Steuerung gemäß dem Stand der Technik
- 1 = Sicherheitstechnisch bewährte Komponenten und Prinzipien
- 2 = Testung
  - Kategorie B muss erfüllt sein
  - sicherheitstechnisch bewährte Prinzipien
  - Prüfung der Sicherheitsfunktionen in angemesenen Intervallen durch die Maschinensteuerung
  - z. B.: Prüfung beim Anlaufen der Maschine oder periodisch während des Betriebes – abhängig vom Risiko
- 3 = Redundanz (mit partieller Fehlererkennung)
  - Kategorie B muss erfüllt sein
  - sicherheitstechnisch bewährte Prinzipien
  - ein Fehler führt nicht zum Verlust der Sicherheitsfunktionen
  - der einzelne Fehler soll bei oder vor der nächsten Nutzung der Sicherheitsfunktion erkannt werden
  - z. B.: zwangsgeführte Relaiskontakte; Überwachung von redundanten elektrischen Ausgängen
- 4 = Selbstüberwachung

**Im Folgenden werden die einzelnen Baugruppen des Antriebes auf Restrisiken untersucht und bewertet:**

## 2. Die Luftschraube:

**Vor jedem Betrieb der Luftschraube sind die Blätter und die Nabe auf Beschädigung hin zu kontrollieren. Bei einem Verdacht auf Beschädigung senden Sie den Propeller umgehend an den Hersteller zur Inspektion bzw. Reparatur.**

**Es ist bei jedem Betrieb der Luftschraube auszuschließen, dass Gefahr für Leib und Leben von Menschen und Tiere entstehen kann.**

**Die Grenzdrehzahl der Luftschraube liegt bei 2500 1/min. Stellen sie sicher, dass diese Drehzahl niemals überschritten wird.**

Dieses Risiko muss beim Einbau und Betrieb des Antriebssystems mit konstruktiven Maßnahmen (Schutzkäfig / Beabstandung) angemessen abgesichert oder durch elektronische Schutzmaßnahmen abgesichert werden.

*Siehe auch das Datenblatt zur Luftschraube*

## 3. Der Motor:

Beim Motor HPD10 handelt es sich um einen permanentmagneterregten Synchronmotor. Der Motor besitzt eine sehr hohe Leistungsdichte und ist somit in der Lage große und langsam drehende Luftschrauben anzutreiben. Dabei gehen vom Motor zwei grundsätzliche Risiken aus:

- Die rotierende Luftschraube (siehe Luftschraube)
- Die Oberflächentemperatur <100°C

Es sollte vor einer direkten Berührung des Motors gewarnt werden. Leichte Verletzungsgefahr!
In der Nähe befindliche Bauteile sollten einen Mindestabstand zu diesem Bauteil aufweisen.

*Siehe auch die Bedienungsanleitung des Motors HPDxx*

## 4. Die Steuerung:

### Die elektrische Auslegung:

Die Auslegung der Spannungshöhe der Steuerung wurde bewusst auf max. 58,8V Gleichspannung ausgelegt, das entspricht der Ladeschlussspannung von 14 Zellen LiIo Akku's, in Reihe geschaltet. Mit dieser Auslegung ist die Obergrenze von 60V Gleichspannung, so wie sie nach DIN EN 61140 als SELV (Safety Extra Low Voltage) definiert ist, eingehalten.

> *SELV (früher „Schutzkleinspannung") ist eine kleine elektrische Spannung, die aufgrund ihrer geringen Höhe und der Isolierung im Vergleich zu Stromkreisen höherer Spannung besonderen Schutz gegen einen elektrischen Schlag bietet.*
>
> *Mit SELV betriebene Geräte, die selbst keine höheren Spannungen erzeugen, werden gemäß DIN EN 61140 (VDE 0140-1) mit der Schutzklasse III bezeichnet.*
>
> *Die Spannung ist so klein, dass elektrische Körperströme im Normalfall ohne Folgen bleiben. Die Spannungsquelle kann entweder ein Generator sein, zum Beispiel ein Fahrraddynamo, oder eine Batterie.*

Da es sich bei dem Motor um einen permanentmagneterregten Synchronmotor handelt, ist zum Betrieb ein Frequenzumrichter mit digitalen Eigenschaften und hoher Leistungsdichte unbedingt erforderlich. Dieser Frequenzumrichter im weiteren kurz mit MC(Motorcontroller) bezeichnet, erzeugt ein magnetisches Drehfeld, dem der Rotor des Motors folgt. Naturgemäß ergibt sich bei einer Störung am MC immer der sichere Zustand eines nicht mehr drehenden Motors.

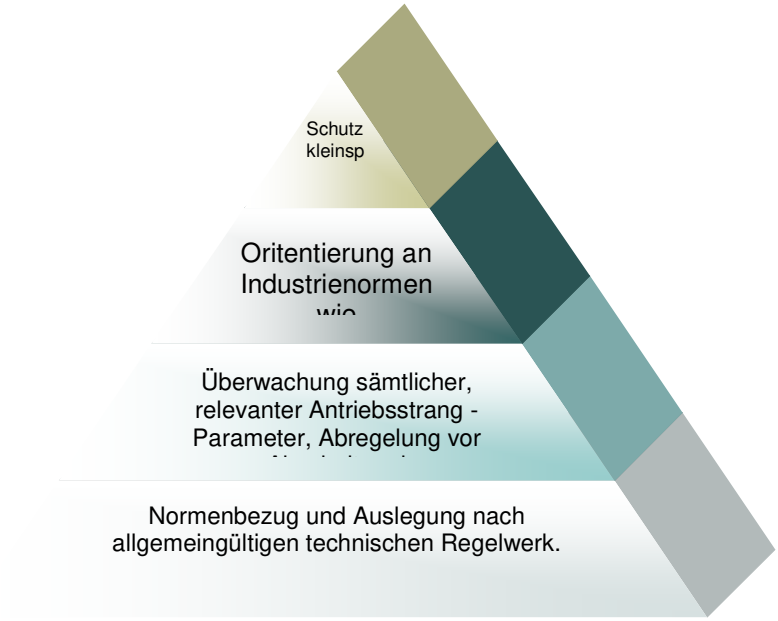
Die im Motorcontroller integrierten Steuerungsalgorithmen übernehmen dabei die Sollwertvorgabe und die permanente Überwachung von relevanten Betriebsgrößen. Der MC ermöglicht somit den sicheren und komfortablen Betrieb des Motors und die Schnittstelle zum Bediener/Piloten.
Die Steuerungskategorie ergibt sich aus der oben resultierende Risikobwertung und der Sicherheitspyramide im Folgenden.

Von der Steuerung geht prinzipiell folgendes Restrisiko aus:

☝ Bei einem Bauteilversagen kann der Motor in den sicheren „Aus-Zustand" kommen, was bei einem Fluggerät einer Notlandesituation gleichkommt.

**Das grundlegende Sicherheitskonzept der Steuerung für das elektrische Antriebssystem.**

Die Sicherheitspyramide:




*Siehe auch die Bedienungsanleitung der Steuerung*

EU – Niederspannungsrichtlinie 2014/35/EG
DIN IEC61140 SELV (Safety Extra Low Voltage)
UN38.3 Akku Transport und Prüfvorschrift

**Maßnahmen zur Erreichung der erforderlichen Sicherheits-, und Verfügbarkeitsintegrität**

**Normenbezug und Auslegung:**

EU – Niederspannungsrichtlinie 2014/35/EG
DIN IEC61140 SELV (Safety Extra Low Voltage)
UN38.3 Akku Transport und Prüfvorschrift

**Weiterführende Maßnahmen**

- Konsequente Anwendung des Ruhestromprinzips
- Einsatz eines mit dem Antriebskommunizierenden Batteriemangagementsystems mit elektronischem Überlast- und Kurzschlussschutz

- Überwachung sämtlicher, relevanter Antriebsstrang – Parameter wie Temperaturen, Ströme und Spannungen, um im Grenzfall oder bei Drahbruch Abregelung vor Abschaltung zu realiseren! → Hochverfügbarkeit

- Maximale Spannungslevel 60V DC → (Safety Extra Low Voltage)

**CE - Konformität**

Diese Geräte genügen den einschlägigen und zwingenden EU-Richtlinien.
Diese sind im Folgenden:

- EN 1050 – Leitsätze zur Risikobeurteilung und Gefahrenanalyse
- EN 954-1 - Maschinenrichtlinie
- EU – Maschinenrichtline 98/37 EWG (MSRL) (entspricht 9. Verordnung des Gerätesicherheitsgesetzes)
- EU – Niederspannungsrichtlinie *2014/35/EG*
- EN61000-6-1 bis 4 EMV Emission/Immission
- EN 62311 - Begrenzung der Exposition der Bevölkerung gegenüber elektromagnetischen Feldern
- **UN Transportvorschriften** (nach **UN Prüfhandbuch Teil III, Abschnitt 38.3 Lithiumbatterien** / Part III: Classification Procedures, Test Methods and Criteria relating to Class 3, Class 4, Division 5.1 and Class 9 – Section 38.3).

## 5. Das Batteriemanagementsystem:

Das Batteriemanagementsystem kurz BMS ist integraler Bestandteil eines Akkumulators. Das BMS hat dabei die Aufgabe den Akkumulator in jeder Phase des Betriebszustandes zu Überwachen und dafür zu sorgen, dass der Akkumulator innerhalb seiner Spezifikation betrieben und nicht überlastet wird. Zudem wird durch die Integration des BMS der Akkumulator transportfähig im Sinne der UN-Transportvorschriften.
Zu den elementaren Aufgaben des BMS gehören: Zellschutz, Ladekontrolle, Lastmanagement, Bestimmung des Ladezustandes, Bestimmung der Zellgesundheit, Ausbalancieren der Zellen, Historie, Authentifizierung und Identifizierung, Kommunikation und Thermomanagement.
Über das Akkumanagement hinaus übernimmt das BMS eine wesentliche Sicherheitsfunktion für das Antriebssystem, den aktiven Leistungsschalter (Powerswitch). Der Leistungsschalter gibt immer genau soviel Strom an das Antriebssystem frei, wie dies vom Akku fordert. Wird aufgrund eines Überlastungsfalls des Antriebs mehr Strom abgefordert als der Antriebssollwert vorgibt, schaltet das BMS den Laststrompfad innerhalb einer Latenzzeit < 9µs ab. Das gleiche Überlastmanagement gilt für den Ladestrompfad. Beide Leistungsausgänge sind somit nicht nur kurzschlusssicher, sondern sichern den Anwender vor den praktisch auftretenden Gefahren beim Einsatz von Hochleistungsakkus (z.B.: Fehlkommutierung, Wechselrichter Querschluss, Motorwindungsschluss, Kurzschluss etc.)

Vom BMS geht prinzipiell ein Risiko aus:

☝ Bei einem Bauteilversagen kann der Motor in den sicheren „Aus-Zustand“ kommen, was bei einem Fluggerät einer Notlandesituation gleichkommt.

.
.

*Siehe auch die Bedienungsanleitung des BMS*

## 6. Der Akkumulator:

Der Akkumulator besteht aus mehreren in Serie und/oder parallel geschalteten Einzelzellen. Jede einzelne Zelle besitzt ein Sicherheitsventil, das bei einer Überlastung die Zelle vom Verband abtrennen wird.

**Vom Akku gehen zwei wesentliche Risiken aus:**

1. Brandgefahr bei mechanischer oder thermischer Einwirkung.

   *Bei mechanischer Beschädigung des Akkupacks, kann es zu Hitzeentwicklung oder einem Auslaufen des Elektrolytes kommen. Elektrolyt ist entflammbar. Im Falle eines Auslaufen des Elektrolytes, die Batterie sofort außer Reichweite des Feuers bringen. Toxizität: Dämpfe, verursacht durch brennende Batterien, können zu Reizungen der Augen, Haut und Atemwege führen.*

 Dieses Risiko kann minimiert werden, indem ausschließlich Zellen eingesetzt werden, die den UN-Test 38.3 bereits auf Zellenebene erfüllen und deren Gehäuse auf Zellenebene z.B.: aus Stahlbecher bestehen.

2. Hohe Kurzschlussleistung, Tiefenladung, Überladung, sowie der Betrieb außerhalb von Betriebsgrenzen.

 Die Handhabung, der Transport und der Betrieb muss durch ein im Akkupack integriertes BMS mit umfangreichen Kontrollmechanismen abgesichert werden.