Vorbereitet von Prof. Peter Bernard Ladkin Ph.D. und Dr.-Ing Bernd Sieker
anhand von Beiträgen von Mitarbeitern in DKE-Normungsgremien

Gefährdungsanalyse (HazAn) des Ladesystems

Version 8 vom 13. September 2012

Inhalt

Seite

1 Einführung

Das übliche Anfangsverfahren in einer System-Safety-Analyse besteht aus den folgenden Schritten:

1.1 Das System und die Systemgrenze festlegen

* Was für Objekte interagieren?
* Was für Zustande haben sie /können sie haben?
* Was für Relationen mit anderen Objekten haben sie?
* Was für Verhalten (Zustandsänderungen), allein oder zusammen mit anderen Objekten?

1.2 Die Umgebung beschreiben

Die „Umgebung“ ist der Teil der Außenwelt, der mit dem System teilweise interagiert

1.3 Die Schnittstelle zwischen System und Umgebung festlegen

Interagierende Objekte in System und Umgebung und die Interaktionen beschreiben

1.2 Eine PHA (vorläufige Gefährdungsanalyse) durchführen

Preliminary Hazard Analysis (PHA, vorläufige Gefährdungsanalyse) ist eine Hazardanalyse (HazAn), die auf Basis der groben Beschreibung in Schritt 1 gemacht werden kann. Es wird üblicherweise erwartet, dass detailliertere HazAns im Lauf der genaueren Systembeschreibung während der Entwicklung des Systems immer wieder durchgeführt werden.

2 Funktionale Sicherheit und Nichtfunktionale Sicherheit

2.1 Begriffe

Der Begriff der funktionalen Sicherheit behandelt die Sicherheit (hier im Sinn vom englischen „Safety“ und französischen „sûreté“) eines Systems in der Ausführung seiner vorgesehenen Funktionen und nicht die Sicherheit bzgl. Nebeneffekten. Z.B., dass ein Feuerwehrfahrzeug rot lackiert ist gehört zu den Eigenschaften des Fahrzeugs, in denen es im Betrieb einfacher zu sehen und zu bemerken ist und deshalb zur funktionalen Sicherheit dessen. Das der Lack keine Schadstoffe enthält und deshalb die Umwelt nicht belastet gehört nicht zur vorgesehenen Funktion des Fahrzeuges und deshalb zu dessen nichtfunktionaler Sicherheit.

Der Begriff der funktionalen Sicherheit umfasst z.B. elektrische Sicherheit in so weit, als dies im laufenden Betrieb gewährleistet bzw. nicht gewährleistet ist. Wenn aber ein elektrisches Gerät durch Vandalismus beschädigt wird und dabei der Täter einen elektrischen Schlag erhält, gehört dieser Gedanke zur nichtfunktionalen Sicherheit des Gerätes.

Zur Vereinfachung der Darstellungen werden im folgenden teilweise vereinfachende Formulierungen gebraucht. „Ladung“ bezeichnet hier den elektrischen Anschluss eines Fahrzeugs an das Energieversorgungsnetz zum Zweck der Energieversorgung durch hierzu vorgesehene Installationen. „Ladestation“ hier im Sinne des Lademodus 3 bezeichnet den ortsfesten Teil der Installation zur Energieversorgung von Elektrostraßenfahrzeugen; „Ladesäule“ bezeichnet eine solche Installation zur öffentlichen Nutzung. „Ladekabel“ oder „Ladeleitung“ wird hier verkürzend verwendet für die Ladekabelgarnitur bzw. Ladeleitungsgarnitur. Zum Vergleich mit dem Betrieb von Fahrzeugen mit Verbrennungsmotoren und zur Veranschaulichung der Situation taucht gelegentlich der Begriff der „Tankstellen-Situation“ auf. Dies beschreibt den Anschluss eines Elektrostraßenfahrzeugs an eine öffentliche Installation zum Zwecke der Energieversorgung, und soll keinesfalls eine Analogie herstellen zum Befüllen eines Kraftstofftanks mit fossilen Brennstoffen.

2.2 Zuordnen der Ereignismöglichkeiten zur funktionalen bzw. nichtfunktionalen Sicherheit

Betrachtet wird ein Elektrofahrzeug samt Ladesystem (Ladestation + Kabel + Zubehör) während des Ladens. Folgende bemerkenswerte Ereignisse werden diskutiert.

1. Das gesamte Ensemble würde von Vandalen mit Gewalt angegriffen. Bei der ersten Sitzung in Mai 2011 wurde beschlossen, dass Vandalismus nicht zu den Szenarien der funktionalen Sicherheit gehört. Nach Einsicht in den britischen RAEng-Bericht Electric Vehicles, in dem die Möglichkeiten der Störung durch Vandalismus diskutiert und als hoch eingeschätzt wird, kam es in der Sitzung September 2011 zu Überlegungen, ob dieser Ausschluss eine passende Vorgehensweise sei. Z. B. kann, was ein Vandale an Ladesäule, Ladekabelstecker oder Ladekabel stören kann, in vielen Fällen auch durch Kollisionen oder andere unabsichtliche Ereignissen passieren. Überlegungen darüber, wie Vandalen einen Ladevorgang stören können ist deshalb auch hilfreich, um vorzustellen, was möglicherweise passieren könnte und dadurch die Ereignisse vom HAZOP möglicherweise zu erweitern.
2. Angriffe gegen eine öffentlich stehende Ladestation, die nicht in Betrieb ist, gehört nicht zum Systemverhalten, das hier betrachtet wird. Hier wird nur das gesamte System Fahrzeug + Ladekabel + Ladestation + Stromnetz während eines Ladevorgangs (inklusive Herstellen und Trennen der elektrischen Verbindung) betrachtet. Das gleiche gilt für einen Angriff auf die Ladebuchse am Elektrofahrzeug, wenn es nicht zur Aufladung an die Ladestation angeschlossen ist.
3. Das gesamte Ensemble wird von einem nahen Blitzschlag heftig beeinflusst. Da ein Blitzschlag während des Betriebs eines elektrischen Gerätes praktisch zum Alltag gehört, wird dieses Szenario zu denen der funktionalen Sicherheit gehören.
4. Eine ähnliche externe Wirkung, aber möglicherweise viel stärker, könnte durch ein Sonnenfleckenereignis (Solarsturm, ein elektromagnetischer Sturm) erreicht werden. Das Carrington-Ereignis von 1859 ist bekannt als das stärkste seit dem Anfang der meteo-wissenschaftlichen Beobachtung und könnte zu allgemeinen Störungen im Stromnetz führen, sowie lokale Wirkung durch elektromagnetischen Feldern in der Umgebung der Ladestation haben.
5. Das Elektrofahrzeug wird während des Ladens von einem anderen Fahrzeug angefahren und mehrere Meter mitgenommen. Ladekabel mit Fahrzeugstecker sowie Ladestationsstecker und Ladestation werden schweren mechanischen Kräften ausgesetzt und möglicherweise beschädigt. Da Ladestationen auf Strassen vorgesehen sind und Kollisionen zwischen geparkten Autos und fahrenden Autos keine Seltenheit sind, wird dieses Szenario auch denen der funktionalen Sicherheit zugeordnet.

2.3 Beschränkung der HazAn

Viele mögliche Gefährdungen werden mit den existierenden anzuwendenden Normen und dem Stand der Praxis ausgeschlossen bzw. gemindert, z.B.,

- die Möglichkeit eines Stromschlages während des Einstöpseln bzw. Ausziehen eines Steckers in/aus der Steckdose
- die Berührung eines Steckers bzw. einer Steckdose unter Spannung.
- Art und Umfang (Ausmaß) der Isolierung, die üblicherweise notwendig ist, um elektrische Leitungen bestimmter Größenordnung gegen Fehlerströme in den zu erwartenden Wettersituation zu schützen

Die Gefährdungen, die allein durch elektrische Sicherheit ausgeschlossen bzw. gemindert werden, werden in dieser Analyse nicht weiter betrachtet.

Ereignisse, die die elektrische Sicherheit möglicherweise in einer Weise beeinflussen , dass sie nicht mehr gewährleistet werden kann, und zwar kausal durch die besondere Situation des Ladevorgangs, werden betrachtet.

2.4 Glossar

Folgende Termini technici werden in diesem Bericht verwendet. Die Bedeutung der Termini findet man bei www.electropedia.org mit zwei Ausnahmen: Berührungsfestigkeit und Mechanische Festigkeit, deren Bedeutung hier näher festzulegen ist.

- Ableitstrom

- Berührungsfestigkeit
- Drehstrom (3-phasig)
- Fehlerstrom
- Frequenz
- Isolationswiderstand
- Mechanische Festigkeit
- Neutralleiter
- Nullleiter
- Phase
- Serienresonanz (Reihenresonanz)
- Rückspeisung
- Strom
- Spannung
- Überspannung
- Überstrom
- Unterspannung
- Wechselstrom (1-phasig)

3 Festlegung des Systems: die Objekte

Ein System besteht aus Objekten, ihren Eigenschaften, Relationen zueinander und gemeinsamem Verhalten (zeitliche Änderung des momentanen Zustandes). Folgende Objekte wurden als Teile des Systems festgestellt:

1. Schnittstelle Netz-Ladestation
2. Ladestation
3. Schnittstelle Ladestation-Ladekabel
4. Ladekabel
5. Schnittstelle Ladekabel-Fahrzeug
6. Fahrzeug

Über die obengenannten Objekte findet ein elektrischer Energiefluss statt. Dieser Energiefluss hat die Eigenschaften: Spannung, Strom, Frequenz, Phase. Also wird unter funktionaler Sicherheit hauptsächlich die Interaktion des „Objekts“ elektrische Energie mit den anderen Objekten bezüglich ihres Gefährdungspotentials betrachtet.

Hier werden auch die unterschiedlichen Lademodi benannt und diskutiert. Die wesentlichen Unterscheidungen sind:

1. Wechselstromladung (vom allgemeinen Stromnetz gespeist) gegen Gleichstromladung (von einem dedizierten lokalen Stromnetz: die „Tankstelle“-Situation). Hier wird nur die Wechselstromladung durch das allgemeine Stromnetz betrachtet.
2. Der „Profi“-Lademodus durch eine dedizierte Ladestation mit getrenntem Ladekabel gegen z.B. den „zu-Hause“-Lademodus, in dem das Fahrzeug in das Hausnetz mit den üblichen Eigenschaften zur „Übernachtladung“ direkt eingesteckt wird.

Hier wurde entschieden, zunächst nur die Wechselstromladung und nur den „Profi“-Lademodus (weiter hier als Modus 3 bezeichnet) zu betrachten, da die „weicheren“ Lademodi mehr Gefährdungspotential hervorrufen. Es wurde als sinnvoll erachtet, die „einfachste“ Variante (also mit mehr ingenieurswissenschaftlicher Kontrolle) zuerst zu betrachten, weil hier die wenigsten Randbedingungen vorliegen. Alle vier Modi müssen aber irgendwann analysiert werden.

Das Stromnetz wurde nicht als Eigenobjekt in das Ladesystem aufgenommen. Soweit die Eigenschaften des Stromnetzes das Verhalten des Ladesystems beeinflussen, wird dies über Objekt 1, die Schnittstelle Netz-Ladestation, behandelt.

Als Sonderfall wird ein lokales Netz betrachtet, das aus irgendeinem Grund vom allgemeinen Stromnetz abgetrennt ist, z.B. durch das Auslösen eines Schutzorgans. Wenn ein Elektrofahrzeug mit Teilladung an ein solches „leeres“ lokales Netz angeschlossen wird, könnte die dabei erzeugte Rückspeisung in das Netz hoch und gefährlich sein.

Ähnlich zu dieser Ausnahme könnte der „Tankstellen“-fall sein, aber nach Stand der Technik wird bei einer Ansammlung von Ladestationen jede Ladestation als Einzelobjekt in der Risikoanalyse betrachtet.

Das Objekt 1 (Fahrzeug) wird in der Wirklichkeit nur ein Teil des aktuellen Fahrzeuges sein müssen. Der hier ausgeführte Auftrag umfasst deutlich nicht die Teile des Fahrzeuges, die unter der Regelung von ISO 26262 zur funktionalen Sicherheit des Automobiles sowie anderen Regelungen liegen. Hier werden nur allgemein die Gefährdungsmöglichkeiten abstrakt benannt. Der Begriff „Fahrzeug“ ist hier nur als die zu betrachtenden Eigenschaften zu verstehen, die durch die Fahrzeugbuchse das Ladesystem beeinflussen können.

4 Festlegung des Systems: die Eigenschaften und Relationen (kurz: Parameter)

Da es hier hauptsächlich um fließenden elektrische Energie geht werden folgende Parameter betrachtet:

- *Strom*
- *Spannung*
- *Phase*
- *Frequenz*

Für bestimmte Teile (1-6) des Systems, aber nicht für alle, spielen folgende Parameter auch eine Wichtige Rolle in Gefährdungserzeugung:

- *Isolationswiderstand. Betrifft 1,2,3,4,5*
- *Ableitstrom . Betrifft alle*
- *Neutralleiterstrom (anwesend/abwesend) Betrifft 2, 3, 5.*
- *Mechanische Festigkeit inkl. Verriegelung. Betrifft 2,4.*
- *Eigenschaften bzgl. Berührung insb. Berührungswiderstand. Betrifft 2,3,4.*
- *Eigenschaften bzgl. Unterbrechung, insb. Durchgängigkeit (ja/nein). Betrifft 2,3,4.*

5 HAZOP und Guidewords

Die Art von HazAn, die hier angewendet wird basiert sich auf Hazard and Operability Studies, Abkürzung HAZOP. HAZOP ist eine Methode, die in der Prozessindustrie, vor allem der chemischen Industrie, entwickelt worden ist, um den Einfluss der Störung des normalen Betriebs durch nicht gewünschte Änderungen der Messgrößen der wichtigsten Parameter (Stoff- oder Flüssigkeitsmenge oder -strom, Temperaturen, Druck, Viskosität, usw.) abzuschätzen. HAZOP ist in IEC 61882 für die Anwendung in der Prozessindustrie genormt.

Ein normaler Betrieb wird zuerst abgebildet und die wichtigen Parameter festgelegt. Danach werden die möglichen Änderungen der Messgrößen der Parameter betrachtet durch Anwendung von sogenannten „Guidewords“ (Leitwörter) auf die Parameter.

Die genormten Guidewords sind:

- *Kein* (englisch: no)
- *Mehr* (englisch: more)
- *Weniger* (englisch: less)
- *Zusätzlich* (englisch: as well as)
- *Teil von* (englisch: part of)
- *Rückwarts* (english: reverse)
- *Etwas anderes* (englisch: other than)

Andere hilfreiche Guidewords könnten sein:

- *Woanders* (englisch: where else)
- *Vor/nach* (englisch: before/after)
- *Vorgezogen/verzögert* (englisch: early/late)
- *Schneller/langsamer* (englisch: faster/slower)

(Siehe, z. B., System Safety: HAZOP and Software HAZOP, Felix Redmill, Morris Chudleigh und James Catmur, Wiley, 1999, S. 73; sowie HAZOP: Guide to Best Practices, Frank Crawley, Malcolm Preston, Brian Tyler, Institution of Chemical Engineers, London, 2000, S. 13-14.)

Da es in dieser Analyse ausschließlich um elektrischen Strom und funktionale Sicherheit geht, haben die folgende Guidewords keine vorauszusehende Anwendung:

- *Kein*: da ohne Strom oder Spannung in dieser Ladesituation keine Gefahr besteht
- *Zusätzlich*: dies wird interpretiert als Fehlerstrom und Fehlerstrom wird explizit als Gefährdung betrachtet
- *Woanders*: wird als Fehlerstrom interpretiert
- *Vor/nach*: die Stelle, wo Strom fliesst oder nicht wird allgemein als Fehlerstrom betrachtet
- *Schneller/langsamer*: Geschwindigkeit ist kein sinnvolles Merkmal für elektrischen Strom

Also werden die folgende Guidewords in dieser Analyse verwendet:

- *Mehr* (englisch: more)
- *Weniger* (englisch: less)
- *Rückwärts* (english: reverse)
- *Etwas anderes* (englisch: other than)
- *Vorgezogen/verzögert* (englisch: early/late)
- *Teil von* (englisch: part of)

6 Anwendung der Guidewords auf die gegebenen Parameter

HAZOP verlangt, dass man die Guidewords mit den Parameter zusammenstellt und eine passende Interpretation für jede Kombination findet. Folgende Interpretationen wurden als sinnvoll identifiziert:

- Mehr/weniger passt zu
  - Strom (hier: Überstrom/zu wenig Strom)
  - Spannung (hier: zu hohe, bzw. zu niedrige Spannung)
  - Isolationswiderstand (hier: zu hohe, bzw. zu niedrige Isolationswiderstand)
  - Mechanische Festigkeit (hier: zu hohe, bzw. zu wenig Festigkeit, s. z. B. DIN VDE 0100-510 Anhang A für unterschiedliche Wertigkeiten mechanischer Festigkeit)
  - Berührungswiderstand (hier: zu hohe, bzw. zu niedrige Widerstand)

- Teil von passt zu
  - Phase: wenn aus z.B. Drehstrom wenige Phasen vorhanden sind als vorgesehen (durch Aderbruch oder Fehlfunktion oder .. wie auch immer)

- Rückwärts passt zu
  - Strom (hier: insb. Rückspeisung)

- Anders passt zu
  - Spannung (aber gleiche Interpretation als mit mehr/weniger)
  - Phase (in Relation: zwei ungleiche Phasen)
  - Frequenz (in Relation: zwei ungleiche Frequenzen)
  - Isolationswiderstand (aber gleiche Interpretation als mit mehr/weniger)
  - Berührungswiderstand
  - Mechanische Festigkeit (aber gleiche Interpretation wie mehr/weniger)
  - Stromwege (hier: Fehlerstrom)

- Vorgezogen/verzögert passt zu
  - Schutzmechanismen, insbesondere Sicherung und die Reaktionszeit
  - Mechanische Festigkeit (eine Sollbruchstelle bricht zu schnell/zu langsam)
  - Wirkung des Ladevorgangs auf das spätere Verhalten des Fahrzeuges während einer Fahrt, da ein Teil des Fahrzeugsystems auf Digitalelektronik basiert

    - Wirkung des Ladevorgangs auf das spätere Verhalten der Ladesäule, da ein Teil des Ladesäulesystems auf Digitalelektronik basiert

Also wurden die folgenden abstrakten Wirkungen in den unterschiedlichen Teilen des Systems explizit betrachtet und das Gefahrenpotential (mögliche Gefährdungen) bestätigt bzw. verneint:

- Überstrom (zu wenig Strom wurde nicht als sicherheitskritisch betrachtet)
- Überspannung bzw. Unterspannung
- Zu wenig Isolationswiderstand (zu hohe Isolationswiderstand wurde nicht als sicherheitskritisch betrachtet, es sei denn, es führt zu Fehlerstrom, aber dies schon in der Liste
- Zu viel/zu wenig Festigkeit gegen Berührung bei den Schnittstellen. (Es ist vorgesehen, dass die Schnittstellen 2 und 4 sowie das Kabel 3 über die übliche oder erhöhte Schutzmassnahmen gegen Berührung verfügen.)
- Rückspeisung in Richtung Fahrzeug ➞ Stromnetz
- Fehlerstrom (anwesend/abwesend, Höhe wird hier nicht betrachtet)
- Die Wirkung von ungleiche Phasen bzw. Frequenzen über eine Schnittstelle

7 Objekte haben folgende Eigenschaften

Oben sind abstrakt die Objekte und ihre Eigenschaften aufgelistet. Die Liste enstand durch Diskussion der realen Situation und die Bemerkungen in der Diskussion lauteten wie folgt. Die Objekte wurden in umgekehrter Reihenfolge betrachtet.

Objekt 1 – die Schnittstelle Netz-Ladestation ist wahrscheinlich hinreichend abgedeckt durch Vorschriften zur Selektivität der Überstromschutzeinrichtungen (TAB, VDE 0100). Dies muss aber überprüft werden. Jedoch müssen insbesondere die Möglichkeit von erhöhten Neutralleiterströmen in Folge von Oberschwingungen und/oder unsymmetrischer Beanspruchungen beachtet werden.

Objekt 2 – die Ladestation hat Isolationswiderstand, verfügt auch über Schutzfunktionen gegen Fehlerstrom und Überströme.

Die Ladestation hat Schutzleiter sowie auch Control-Pilot (zusätzliche Kommunikationsleitung im das Ladekabel zum Fahrzeug, welches ebenfalls über ein Control-Pilot verfügen muss.)

Die Bedeutung von Überstrom wurde diskutiert. Eine Interpretation: der Strom ist höher als Bemessungsstrom von Ladestation, Leitung, Fahrzeug. Eine zweite Interpretation: der Strom ist höher als der vorgegebene Strom („Stromsollwert“). Wenn nachfolgend von Überstrom gesprochen wird ist die erste Interpretation gemeint.

Nota bene: Rückwirkungen auf das Netz, die nur die Versorgungszuverlässigkeit und nicht die Sicherheit betreffen, z.B. Überschreiten des Stromsollwertes werden hier nicht betrachtet.

Objekt 3 – die Schnittstelle Ladestation-Ladekabel hat eine Verriegelung (damit während des Stromflusses der Stecker nicht abgezogen werden kann), sowie auch Berührungsschutz. Eine Sollbruchstelle gegen extreme mechanische Belastung wäre denkbar. Schutz gegen Umwelteinflüsse ist in gewisser Weise notwendig, ebenso wie eine gewisse mechanische Festigkeit.

Wenn mit undefinierten Kräften am Kabel gezogen wird, ist dieser Fall nicht vollständig geklärt. Es gibt zu viele sich widersprechende Forderungen, wie z.B. Diebstahlsschutz.

Obwohl ein selbstständiges Wegfahren nach ISO unterbunden sein muss, können bei einem stehenden Fahrzeug, das geladen wird, z. B. durch Kollision eines LKW mit dem stehenden Fahrzeug sehr hohe Abreißkräfte auftreten.

Objekt 4 – das Ladekabel hat Isolationswiderstand + Durchgangswiderstand (mehrere, für die Einzeladern). Die Durchgängigkeit ist eine sehr wichtige Eigenschaft, deren Minderung unterschiedliche kausalen Quellen haben kann. Diese muss detailliert betrachtet werden: dieses Treffen bestätigte nur das Gefahrpotential.

Einige mechanische Fehler können nur durch eine Sichtprüfung erkannt werden. Eine Sichtprüfung ist die Regel in ähnlichen aber nicht identischen Fällen. Eine Sichtprüfung reicht hier, um Beschädigungen des Mantels auszuschließen. Zur Ermittlung von Fehlern innerhalb der Ladeleitung müssten elektrische Messungen durchgeführt werden.

Objekt 5 – die Schnittstelle Ladekabel-Fahrzeug wird unter Modus 3 als gleich zu Objekt 3 angesehen.

Objekt 6 – das Fahrzeug hat Strom, Spannung, Phase, Frequenz, Isolationswiderstand (rein ohmsch), sowie Ableitstrom (Hochvoltnetz ist isoliert)

8 Gefährdungspotential

Das Ergebnis der HazAn sind die folgenden Phänomene, die durch Anwendung der Guidewords auf die Parameter identifiziert wurden, lautete wie folgt.

Als mögliche Gefährdungen (Hazards) werden angesehen:

Objekt 1 – Schnittstelle Netz-Ladestation: Gefährdung wenn

1. mehr Strom oder mehr Strom rückwärts fließt
2. unterschiedliche Frequenzkombinationen auftreten (Oberschwingungen)
3. Stromeigenschaften anders sind (AC und DC)
4. Spannung anders ist (Rückspeisung in ein abgeschaltetes Netz)
5. Neutralleiterbelastung auftritt durch 3. und weitere Oberschwingungen

Objekt 2 – Ladestation: Gefährdung wenn

1. Isolationsfehler
2. Stromeigenschaften anders sind (AC und DC)
3. Überspannung durch Blitz, die die Elektronik insb. Kontrollelektronik ändern kann
4. Überstrom durch Blitz
5. leicht entzündbare Gemische anwesend sind
6. Spannung angeboten wird, wenn dies vom Ablauf her nicht erwartet wird
7. ein Ladevorgang eine spätere Wirkung auf das Verhalten der Ladestation nach dem Ladevorgang hat

Objekt 3 – Schnittstelle Ladestation-Ladekabel: Gefährdung wenn

1. zu hohe mechanische Kräfte eingesetzt werden
2. zu geringe strukturelle Kräfte vorhanden sind (z.B., der Stecker sitzt locker)
3. mechanische Überlast anderer Art
4. höherer Übergangswiderstand durch Verschmutzung der Kontakte und durch Verschleiß

Objekt 4 – Ladekabel: Gefährdung wenn

1. mehr Strom (Kabel hat zu geringer Querschnitt für die angeforderten Strom, der das Fahrzeug verlangt und die Ladestation versorgt)
2. zuwenig Isolationswiderstand
3. zu großer Durchgangswiderstand
4. Fehlerstrom (AC und DC)
5. es besteht eine erhöhte Gefährdung durch äußere Einflüsse (z.B. Kabel wird überrollt)
6. Abriss bei zu starker Belastung: zwischen Kabel und Stecker, an einer In-Cable-Box, im Kabel selbst oder an einer vorgesehenen Sollbruchstelle
7. außergewöhnliche Umweltparameter z.B. Wärmequellen (Auspuff/Katalysator)

Objekt 5 – Schnittstelle Ladekabel-Fahrzeug: wird als gleich wie Objekt 3 angesehen, mit einer Ausnahme:

5. Gleichfehlerstrom, verursacht durch einen Isolationsfehler in einem bestimmten Bereich der Elektronik des Ladegerätes. Diese Situation zeigt Definitionsprobleme in der Normung. Eine weitergehende Betrachtung ist daher an dieser Stelle nicht möglich.

Objekt 6 – Fahrzeug: Gefährdung wenn

1. Strom anders ist (z.B. DC statt AC inkl. Gleichfehlerströme),
2. die Frequenz anders ist
3. eine andere Phasenfolge entsteht bei dreiphasiger Rückspeisung
4. die Spannung anders ist
5. mehr Strom fließt
6. erhöhte Spannung entsteht
7. mehr Ableitstrom fließt

8. weniger Isolationswiderstand entsteht (mit der Folge der Berührungsspannung an Chassis und Karosserie)
9. der Strom rückwärts fließt (ungewollte Rückspeisung)
10. die Frequenz anders ist (Fehlerstrom ist Gleichstrom oder hochfrequent)
11. Der Ladevorgang spätere Wirkung auf das Fahrzeugverhalten in der Fahrt hat

9 Ereignisbaum für jede Gefährdung

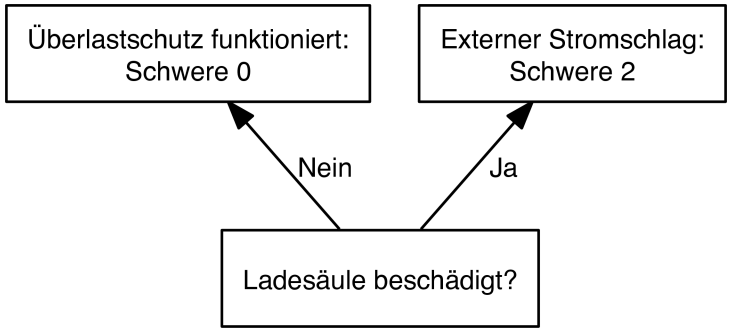
Laut Ergebnisbericht der Sitzung vom 16.12.2011 wird als Metrik für die Gefährdungsmöglichkeiten vereinbart: Als Metrik wird Schwere 0 (keine Auswirkung), Schwere 1 (Brandgefahr) und Schwere 2 (Stromschlag oder nicht vorhersehbare Wirkung) vereinbart.

Als Häufigkeit werden die drei Stufen „unvorstellbar“, „theoretisch möglich“ und „plausibel“ festgelegt. Dabei wird davon ausgegangen dass Schutzmassnahmen nach Norm vorhanden sind.

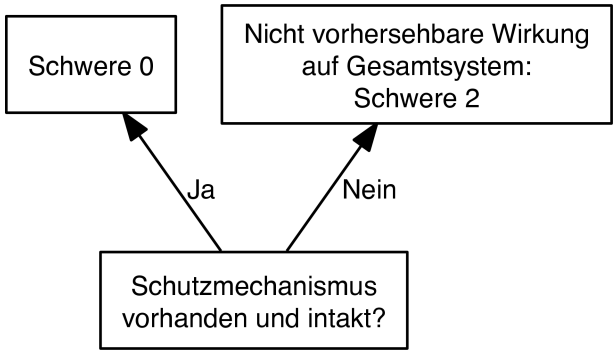
Ereignisbäume

Objekt 1: Schnittstelle Netz-Ladestation

Gefährdungen 1: Mehr Strom, Fehlerstrom

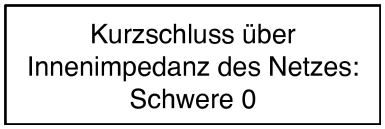


Gefährdung 2: Frequenzkombination
Häufigkeit: plausibel

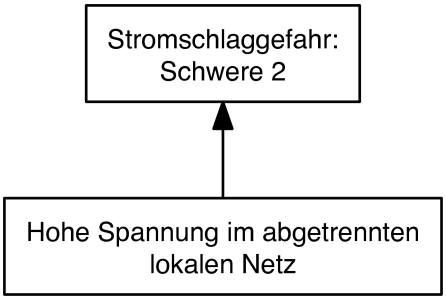


(s. auch Bender-Analyse, DKE-353.0.4_2011-0031, S. 5)

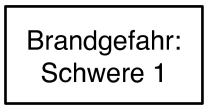
Gefährdung 3: Stromeigenschaften anders
Häufigkeit: plausibel



Gefährdung 4: Rückspeisung in abgetrenntes Netz
Häufigkeit: theoretisch möglich



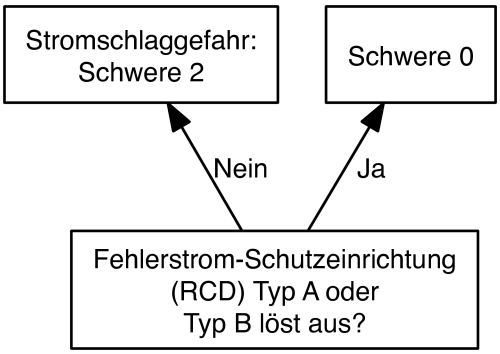
Gefährdung 5: Neutralleiterbelastung
Häufigkeit: theoretisch möglich



Durch Erdung der Ladestation kann es nicht zu einer gefährlichen Spannung auf dem Schutzleiter kommen. (Annahme: PEN-Leiter vom Transformator bis zur Ladestation ausreichend dimensioniert.)

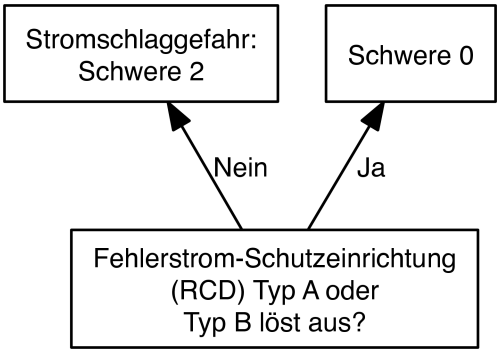
Objekt 2: Ladestation

Gefährdung 1: Isolationsfehler
Häufigkeit: plausibel



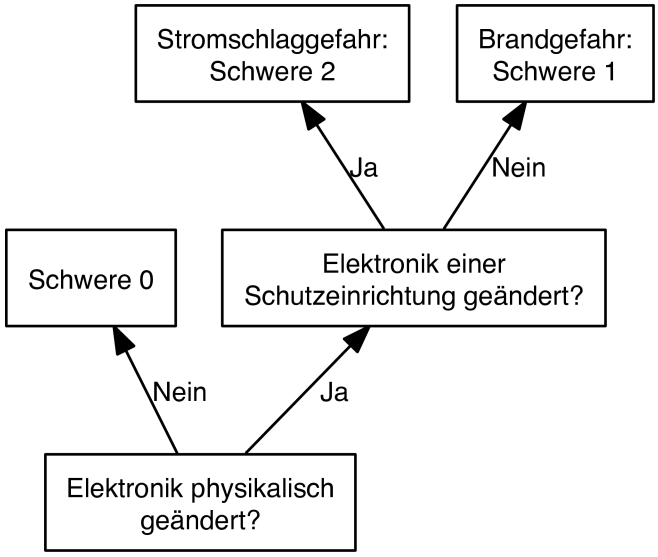
Gefährdung 2: Stromeigenschaften anders

Häufigkeit: plausibel

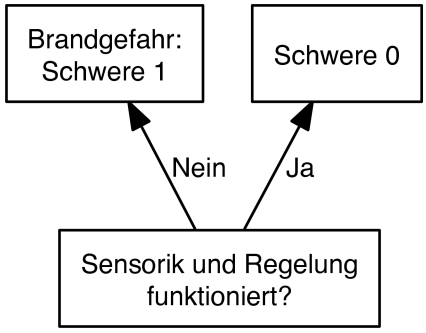


Anmerkung: Auslösung eines Fehlerstrom-Schutzeinrichtung (RCD) Typ A kann durch Gleichfehlerströme > 6 mA blockiert werden. Dazu sind diese Gleichfehlerströme sicher zu vermeiden. Dies kann auf Fahrzeugseite erfolgen, oder durch ein entsprechendes zusätzliches Schutzelement in der Ladestation.

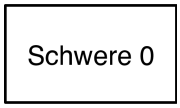
Gefährdungen 3 und 4: Überspannung (Blitz oder interne) oder Überstrom
Häufigkeit: plausibel



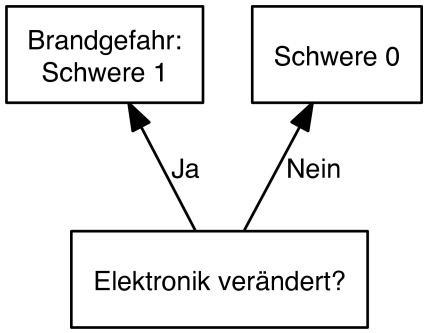
Gefährdung 5: leicht entzündliche Gemische vorhanden
Häufigkeit: plausibel



Gefährdung 6: Spannung liegt unerwartet an
Häufigkeit: plausibel

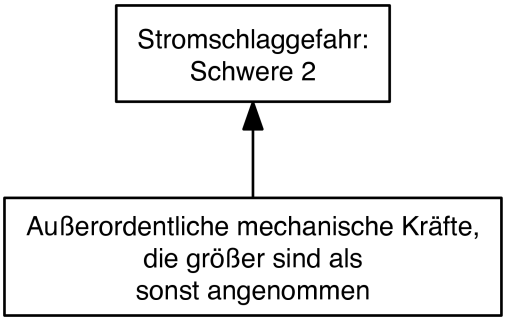


Gefährdung 7: Ladevorgang hat Einfluss auf späteres Verhalten
Häufigkeit: theoretisch möglich

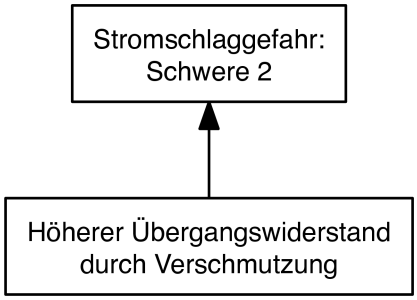


Objekt 3: Schnittstelle Ladekabel-Ladestation

Gefährdungen 1, 2 und 3: Können zusammengefasst werden als außerordentliche mechanische Kräfte
Häufigkeit: plausibel

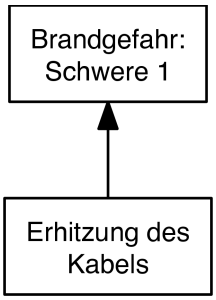


Gefährdung 4: Höherer Übergangswiderstand durch Verschmutzung
Häufigkeit: plausibel



Objekt 4: Ladeleitung

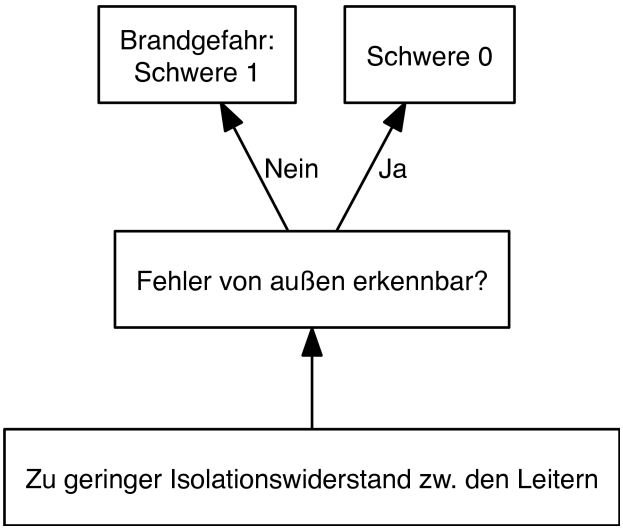
Gefährdung 1: Mehr Strom für gegebenen Querschnitt
Häufigkeit: plausibel



Anmerkung: Mehr Strom für den gegebenen Querschnitt werden in der DIN VDE 0298 Teil 4 geregelt. Diese Norm regelt durch das Zusammenwirken mit DIN VDE 0100 Teil 520 die jeweiligen Fälle. Der Schutz der Leitung wird durch den Leitungsschutzschalter gewährleistet.

Anmerkung: Überhitzung der Leitung kann auch zu einer Überhitzung des Stecksystems und entsprechenden Schäden führen.

Gefährdung 2: Zu geringer Isolationswiderstand
Häufigkeit: plausibel

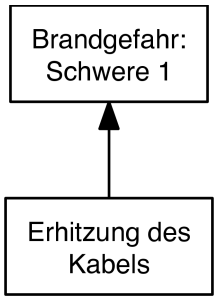


Anmerkung: Zu geringer Isolationswiderstand haben wir in zwei Fällen: Eine Mantelbeschädigung kann durch optische Beurteilung erkannt und der Berührungsschutz gesichert werden. Beschädigungen der Isolierhüllen innerhalb der Leitungen sollten ein Auslösen des Leitungsschutzschalters oder der Fehlerstrom-Schutzeinrichtung (RCD) Typ A hervorrufen.

Anmerkung: Ein zu geringer Isolationswiderstand kann durch Querdruck oder unzulässig kleine Biegeradien verursacht werden. Diese können z. B. beim Überrollen entstehen. Folgende Faktoren unterscheiden diese Situation von sonst üblichen:

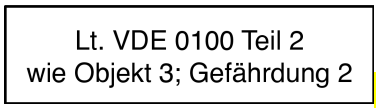
- Deutlich höhere Stromaufnahme
- Deutlich höheres Gewicht des Fahrzeugs im Vergleich z. B. zum Rasenmäher
- Nutzung auch im öffentlichen Bereich
- Vandalismus
- Unbeabsichtigtes Überfahren
- Dauer der Benutzung deutlich höher (mehrere Stunden mehrmals pro Woche)
- Nutzung durch Nicht-Elektrofachkraft

Gefährdung 3: Zu großer Durchgangswiderstand
Häufigkeit: theoretisch möglich



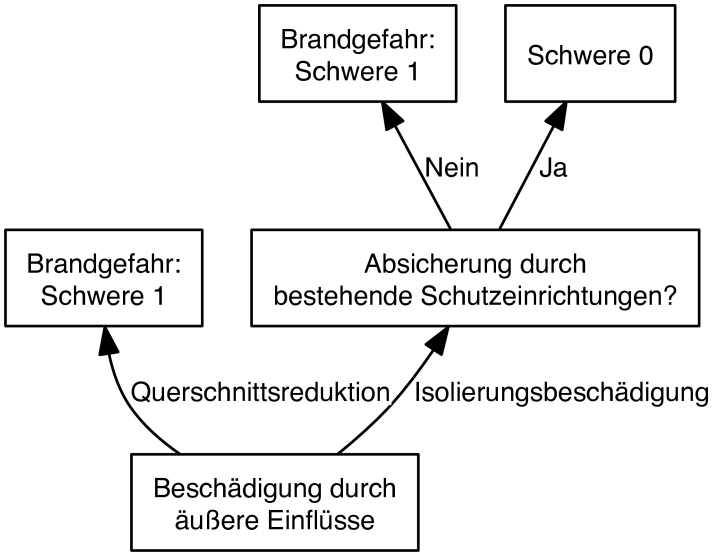
Anmerkung: Zu großer Durchgangswiderstand ist durch die Norm DIN VDE 0100 Teil 430 Schutz von Kabel und Leitungen gegen zu hohe Erwärmung geregelt.

Gefährdung 4: Stromeigenschaften anders (AC und DC)
Häufigkeit: plausibel



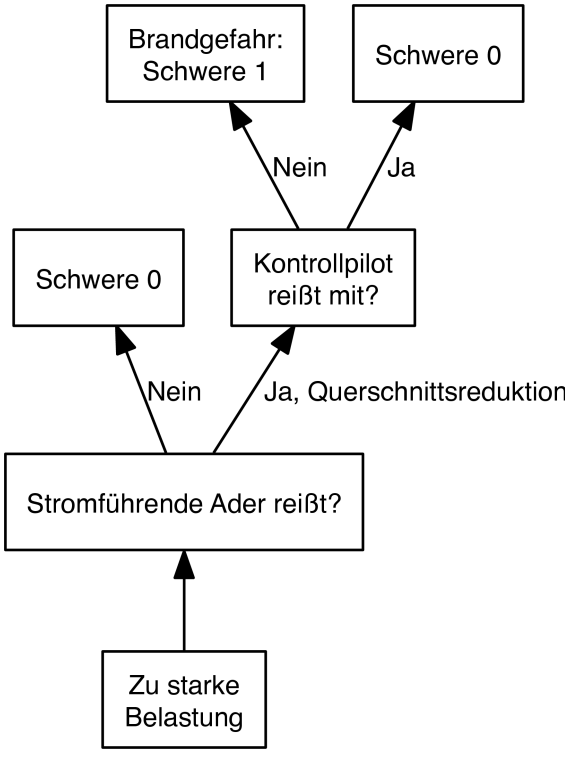
Anmerkung: Siehe auch DIN VDE 0298 Teil 4 Verwendung von Kabeln und isolierten Leitungen für Starkstromanlagen.

Gefährdung 5: Erhöhte Gefährdung durch äußere Einflüsse
Häufigkeit: plausibel



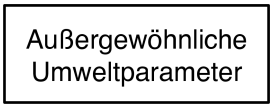
Anmerkung: Mindestrobustheiten für verschiedene Beanspruchungen regelt die DIN VDE 0298 Teil 300 Leitfaden zur Verwendung.

Gefährdung 6: Abriss bei zu starker Belastung
Häufigkeit: plausibel



Anmerkung: Mindestrobustheiten für verschiedene Beanspruchungen regelt die DIN VDE 0298 Teil 300 Leitfaden zur Verwendung.

Gefährdung 7: Außergewöhnliche Umweltparameter
Häufigkeit: plausibel



Anmerkung: Außergewöhnliche Umweltparameter regelt die DIN VDE 0100 Teil 420 Schutzmaßnahmen gegen thermische Auswirkungen.

Objekt 5: Schnittstelle Fahrzeug-Ladekabel

Bei der Gefährdungsanalyse kann dieses Objekt genauso behandelt werden wie Objekt 3, mit folgender Ausnahme:

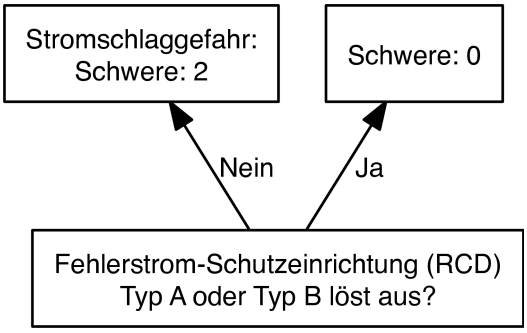
Gefährdung 5: Gleichfehlerstrom, verursacht durch einen Isolationsfehler in einem bestimmten Bereich der Elektronik des Ladegerätes. Diese Situation zeigt Definitionsprobleme in der Normung. Eine weitergehende Betrachtung ist daher an dieser Stelle nicht möglich.

Objekt 6: Fahrzeug

Die Betrachtung des Fahrzeuges selbst liegt in der Verantwortung des Fahrzeugherstellers. Dennoch halten wir es für sinnvoll, auf drei spezifische Gefährdungen aufmerksam zu machen:

Gefährdung 1: Strom ist anders (z.B. DC statt AC inkl. Gleichfehlerströme),

Höufigkeit: plausibel



Anmerkung: Wenn das Fahrzeug Gleichfehlerströme > 6 mA erzeugt, und es an eine Ladestation angeschlossen ist, die nur über eine Fehlerstrom-Schutzeinrichtung (RCD) Typ A verfügt, verliert dieser seine Schutzfunktion: Folge ist die Gefahr von Brand oder Stromschlag.

Gefährdung 4: Andere Spannung
Häufigkeit: plausibel

Gefährdung 10: Resonanzen

Häufigkeit: plausibel

Fahrzeug wird Teil eines Schwingkreises

10 Zusammenfassung

Durch die Anwendung von HAZOP wurden systematisch die Gefährdungsmöglichkeiten im Gesamtsystem eines ladenden Fahrzeuges untersucht. Der Vorteil von der Anwendung von HAZOP liegt in der systematischen Betrachtung der Phänomene, die auftreten können, die eine gewisse Vollständigkeit bietet, die über die Intuition der beteiligten Ingenieure hinausgeht und hoffentlich nicht so für den „Tunnelblick“ der gewöhnliche Denkweise anfällig ist.

In diesem verfahren werden mehrere Gefährdungsarten identifiziert. Besonders überlegungswert sind die mögliche Gefährdungen, deren Quellen in Eigenschaften des Fahrzeugs liegen (siehe gerade oben). Hier wird eine enge Zusammenarbeit zwischen Fahrzeughersteller und Stromnetz- bzw. Ladestation- und Kabelhersteller als notwendig gesehen.

Die Preliminary Hazard Analysis zeigt als erste Schritt die Gefährdungen auf. Es wird empfohlen ausgehend von dieser Analyse eine Risikoanalyse durchzuführen. Bei der Risikoanalyse sollen auch Sicherheitsfunktionen und Anforderungen an die Sicherheitsintegrität festgelegt werden.

Zu klären ist auch ob und wo die Risiken bestehen. Sind die aufgezeigten Gefährdungen aus der Preliminary Hazard Analysis auch tatsächlich vorhanden? Welche Normen sind davon betroffen und ggf. zu ändern. Ergebnisse sollten als Empfehlung an das jeweilige Normungsgremium weiter geleitet werden

10.1 Risikoanalyse: Allgemeine Punkte

Um eine Risikoanalyse auf Basis dieser Hazardanalyse zu machen, werden für jede Gefährdung folgende Parameter zugewiesen:

- Häufigkeit
- Schwere

Zu Häufigkeit:

Da der vorgesehene Vorgang noch nicht ein üblicher Vorgang ist, ist die Häufigkeit des Auftretens einer Gefährdung nicht aus Erfahrung bekannt. Man muss grobe Schätzungen zu den Häufigkeiten machen und dies nach der betrieblichen Erfahrung später korrigieren bzw. feiner spezifizieren. Die Norm ISO 26262 legt 5 qualitative Häufigkeitsstufen fest. Nach erster Überlegung scheinen hier auch 3-5 passend. Es ist auch vorgesehen, dass ISO 26262 für Elektrofahrzeuge in einer Version auch gilt, also müssen die hier ausgewählten Stufen konsistent mit denen in ISO 26262 sein, um Übersetzungsschwierigkeiten zu vermeiden.

Zu Schwere:

Für die Auswirkung eines Stromschlags auf Menschen und Tieren wird der Biegelmeier-Bericht verwendet.

Die ISO 26262 legt auch qualitative Stufen für Schwere fest. Diese nennen sich AIS. Die hier ausgewählte Skala für Schwere muss mit der AIS-Skala konsistent sein, um Übersetzungs-schwierigkeiten zu vermeiden.

10.2 Zusammenführen der Parameter zur Risikoabschätzung

Die Parameter Häufigkeit und Schwere könnten allein zu einer Risikoanalyse verwendet werden, in so weit man ein Risikomatrix einrichtet.

Eine Frage wäre, ob dies hier der Fall ist.

In der ISO 26262 gibt es mehr als diese zwei Eingabeparameter zu einer Risikoanalyse, nämlich severity, frequency (im Sinne von exposure) und controllability.

Der Parameter controllability wird im Fahrzeugbereich verwendet. Eine Frage wäre, ob controllability beim Ladevorgang eine Rolle spielt. Ein Beispiel wurde diskutiert: die Rückspeisung von einem Fahrzeug ins Stromnetz, während das lokale Teil des Stromnetzes wegen Wartungsarbeiten vom Gesamtstromnetz abgetrennt ist und ein Mensch am lokalen Teil des Netzes arbeitet. Solche Situationen sind durch Vorschriften kontrolliert und diese Vorschriften gelten für professionelle Elektriker und für Laien. Also könnte hier controllability auch bedeuten: Kontrollierbarkeit durch prozedurale Vorschriften. Also besteht offensichtlich eine Rolle für den Parameter controllability aber mit einer anderen Interpretation als beim Fahren.

Wenn controllability ein wichtiger Parameter für die Risikoanalyse sein soll, wird die Analyse nicht mit Hilfe von Risikomatrizen machbar sein. Man muss mehrdimensionale Verfahren wie Risikographen benutzen. Eine mögliche Schwierigkeit wäre, dass die Semantik von Risikographen nicht eindeutig ist. Eine Doktorarbeit wurde von Frau Dr. Birgit Milius an der T.U.Braunschweig in letzter Zeit über Risikographen, deren Bedeutung und Anwendung geschrieben.

Ein weiteres Beispiel wurde diskutiert, nämlich die Häufigkeit und Schwere beim Überrollen eines Ladekabels. Dies hat nicht nur eine mögliche physikalische (mechanische) Wirkung sondern eine Wirkung auf den Strom sowie möglicherweise auf den Menschen. Sollte diese Wirkungen in einer einzigen Schwerekategorie zusammengefasst werden? Oder wären hier unterschiedliche Wirkungsstufen getrennt abzuschätzen und zu bearbeiten?

10.3 Gegenmaßnahmen

Eine Risikoanalyse beschäftigt sich rein formal gesehen nicht mit Gegenmaßnahmen. Die Gegenmaßnahmen zu hier identifizierten Gefährdungen sollten von Domänenexperten entwickelt werden. Aber die Möglichkeit und Offensichtlichkeit der Gegenmaßnahmen beeinflusst unvermeidlich die Klassifizierung, die Aufteilung der Gefährdungen. Z.B. Gefährdungen, die durch die üblichen Normen und Regelungen für elektrische Sicherheit abdeckt werden können (d.h., effektive Gegenmaßnahmen sind längst bekannt und angewendet) könnten zusammengefasst werden und dadurch wird die Risikoanalyse einfacher und übersichtlicher.

Also wären hier Überlegungen zu Gegenmaßnahmen als Kommentar passend.

Eine wichtige Frage wäre: wenn sind vorgeschlagene Gegenmaßnahmen ausreichend? Zwei Prinzipien werden in Europa meist angewendet:

- ALARP (Britisches Gesetz): „As Low As Reasonably Practicable“ - das Risiko wird so weit wie praktikabel gemindert. „Praktikabel“ hier bedeutet irgendeine Gleichgewichtsabschätzung von Kosten und Wirkung

- MGS (Deutsch, sowie GAMAB in Frankreich): „Mindestens Gleiche Sicherheit“ („Globalement Au Moins Aussi Bon“) - wenn man eine alte Technik oder ein altes Verfahren ersetzt, muss der Ersatz mindestens die Sicherheitsstufe erreichen, die die alte Technik bzw. das alte Verfahren erreicht hat. Man sollte sicherheitsmäßig den Zustand nicht verschlechtern.

In der Situation, dass hier ein neues System (Objekte 1-6) zusammen gesetzt wird und MGS eine Führungsprinzip für Deutschland gilt, wurde beschlossen, dass MGS als Prinzip zur Abschätzung der Suffizienz der Gegenmaßnahmen angewendet wird

Einige Gegenmaßnahmen werden vorgeschlagen:

- Die Normen und Prinzipien zur elektrischen Sicherheit, in so weit dies anwendbar sind
- Maßnahmen in der Form einiger Anforderungen an die Fahrzeughersteller, falls eine Gefährdung durch das Fahrzeug vorgestellt wird. Z. B., die spätere Wirkung einer Ladeaktion auf der Fahrt eines Fahrzeugs (durch z.B. einem Einfluss des Ladevorgangs auf die Digitalelektronik des Fahrzeugs) muss ausgeschlossen werden: dies würde durch einer Anforderung an das Fahrzeughersteller gesichert.
- Maßnahmen in der Form einiger Anforderungen an die Ladesäulehersteller, dass spätere Wirkung auf der Ladesäule eines Ladevorgangs ausgeschlossen wird

- Zur Gegenmaßnahme der Rückspeisungsgefährdung könnte als Anforderung an die Fahrzeughersteller sowie Ladekabel- und Ladesäulehersteller sein, dass Strom, Spannung und Frequenz einer Rückspeisung nicht höher sein können als bei der Ladung selbst.

11 Offene Fragen

- Die Anwendbarkeit des Begriffs *controllability* in einem Bereich außer der Fahrt
- Häufigkeitsstufen entwickeln und festlegen
- Schwerestufen entwickeln und festlegen
- Die Common-Cause-Wirkungen eines Carrington-Ereignisses festlegen und in der Gefährdungsliste einordnen
- Die Aufstellungsorten der Ladesäulen kann einen Einfluss auf Häufigkeit und Schwere eine Gefährdung haben. Wie wird der Aufstellungsort berücksichtigt?
- Ein Vergleich mit der Situation mit Fotovoltaikanlagen könnte hilfreich sein
- Bzgl. Rückspeisung als Fehlfunktion: Welche Szenarien gibt es?
- Bzgl. Wartungsarbeiten und die mögliche Folgen von einer Rückspeisung wurde die Fa. Bender an einer Erläuterung der möglichen Szenarien angefragt

Annex

Ladeleitung

Eine Ladeleitung für Mode 3 besteht im Wesentlichen aus drei passiven Bauelementen:

1. Infrastrukturseitiger Stecker nach IEC 62196-2 (nur Typen 2 und 3)
2. Fahrzeugseitige Kupplung nach IEC 62196-2 (alle Typen möglich)
3 Leitung nach VDE-AR-E 2283-5 (hieraus sollen EN und IEC – Normen entstehen)

Die IEC 61851-1 unterscheidet beim Anschluss des Fahrzeugs die Fälle Case A, B, C:

Case A: Die Ladeleitung ist fest am Fahrzeug angebracht, d. h. die Ladekupplung entfällt.

Case B: Die Ladeleitung ist an beiden Enden frei, d. h. sie besteht aus allen drei genannten Bauelementen.

Case C: Die Ladeleitung ist fest an der Ladestation angebracht, d. h. der Ladestecker entfällt.

Besonderheiten bei den verschiedenen Typen der Ladesteckvorrichtungen nach IEC 62196-2:

Typ 1: Für diesen Typ ist lediglich die Schnittstelle am Fahrzeug definiert. Der Case A (und infrastrukturseitig der Case B) sind nicht möglich. Die Kupplung besitzt keine Widerstandskodierung, so dass die Maximalstromstärke nicht redundant (PWM und Widerstand) übermittelt werden kann.

Typ 2: Für diesen Typ ist auf der Infrastrukturseite eine und sind auf der Fahrzeugseite zwei Ausprägungen definiert. Man unterscheidet auf der Fahrzeugseite bei den Kupplungen zwischen der Kupplung für Mode 1 und der Kupplung für die Mode 2 und 3. Durch diese Unterscheidung kann der Fahrzeughersteller festlegen, ob er es gestattet, dass das Fahrzeug von ihm ungewollt mit Spannung versorgt werden darf oder nicht. Für Typ 2 ist vorgeschrieben, dass durch eine Widerstandskodierung am PP-Kontakt die Maximal-stromstärke der Ladeleitung auf zwei getrennten Wegen (PWM und Widerstandkodierung) übermittelt wird (Redundanz).

Typ 3: Für diesen Typ sind sowohl auf der Infrastrukturseite als auch auf der Fahrzeugseite drei mechanisch zueinander inkompatible Ausgestaltungen vorgesehen. Es handelt sich um:

a. 16A 250V einphasig mit einem „Pilot“
b. 32A 250V einphasig mit CP- und PP-Kontakt
c. 63A 480V dreiphasig mit CP- und PP-Kontakt

Zur Nutzung des „Pilot“ wird keine Aussage gemacht. CP- und PP-Kontakt sind dafür vorgesehen so genutzt zu werden, wie es für gleichnamige Kontakte bei Typ 2 vorgeschrieben ist.

In den Kupplungen und Steckdosen ist bei allen Ausgestaltungen und bei den Steckern 32 A und 63 A ist ein Bauraum für Shutter vorgesehen.