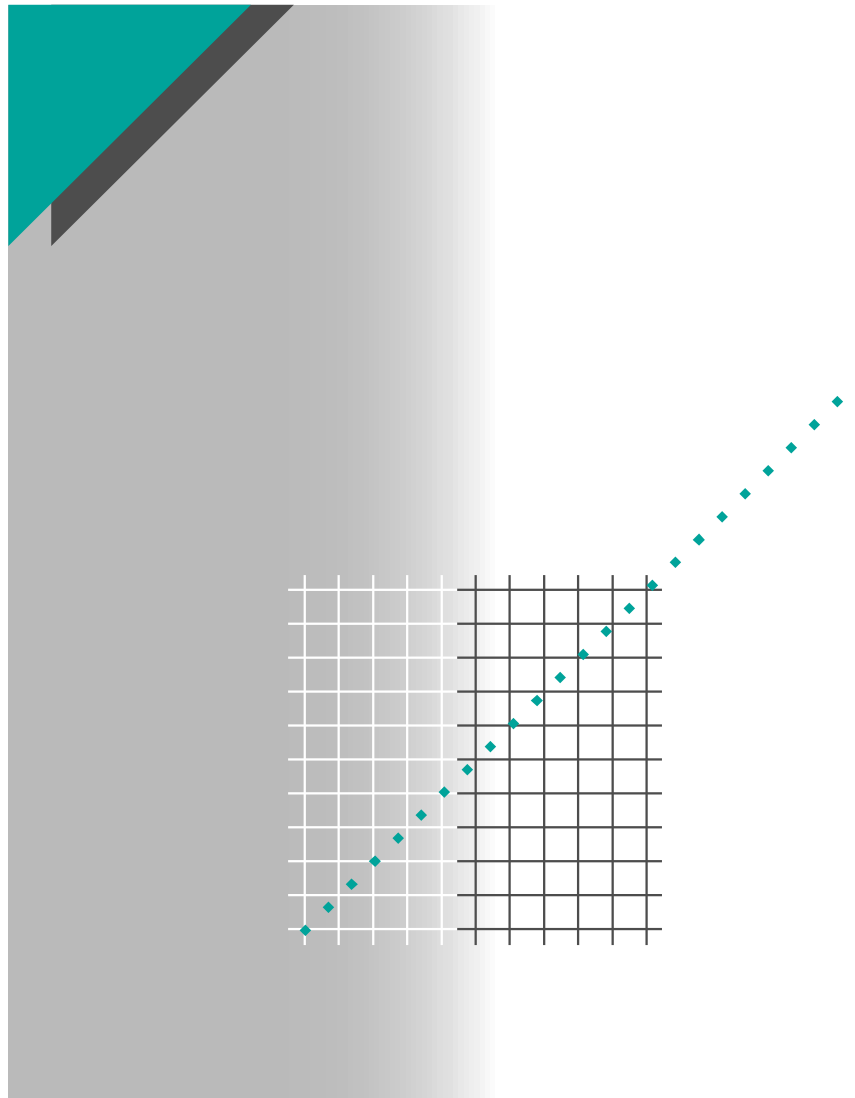


Technisches Heft Nr. 184

Sicherheitsstudien für elektrische Anlagen



Merlin Gerin

Modicon

Square D

Telemecanique

Die Technischen Hefte sind eine Sammlung von Dokumenten, die für jene bestimmt sind, die weitergehende Informationen suchen, als sie in den Leitfäden, Katalogen und Datenblättern enthalten sind.

Für Spezialisten und Techniker sowie für Lehrer und Studenten bilden diese Hefte ein Hilfsmittel für die Schulung in den neuen Techniken und Technologien auf den Gebieten der Elektrotechnik und Elektronik.

Hier finden Sie insbesondere die Grundlagen, welche zum besseren Verständnis für die in den Anlagen, Systemen, Komponenten und Einrichtungen für den Transport, die Verteilung und/oder die Bewirtschaftung der elektrischen Energie auftretenden Erscheinungen beitragen.

Eine Liste der verfügbaren Technischen Hefte erhalten Sie auf Verlangen.



Nr. 184

Sicherheitsstudien für elektrische Anlagen

Autorin: Sylvie LOGIACO

Als Ingenieurin ISTG (Institut Scientifique et Technique de Grenoble) mit Abschluss 1987 befasste sie sich zuerst mit Risikostudien in der chemischen Industrie bei P echiney und hierauf bei Atochem. Seit 1991 ist sie bei Schneider t atig. Sie geh ort zum Kompetenzzentrum Betriebssicherheit und hat in dieser Eigenschaft zahlreiche Studien zur Betriebssicherheit von elektrischen Anlagen und Leittechnik-Systemen durchgef uhrt.

Lexikon

Störungsanalyse

Aufgrund der Funktionsanalyse, die Analyse der Funktionsstörungen eines Systems (in der Praxis gleichbedeutend mit «Sicherheitsstudie»).

Erfahrungswerte

Bei Ausfällen im Betrieb gesammelte Zuverlässigkeitsdaten.

Betriebssicherheit

Generischer Begriff, er die unabhängigen Grössen Zuverlässigkeit, Verfügbarkeit, Wartbarkeit und Sicherheit in sich vereint.

Verfügbarkeit

Prozentualer Anteil der Zeit, während der das System normal funktioniert.

Zuverlässigkeit

Befähigung eines Systems, möglichst lange richtig zu funktionieren.

Wartbarkeit

Befähigung eines Systems, rasch repariert zu werden.

Sicherheit

Befähigung eines Systems, keine Personen zu gefährden.

Sicherheitsstudien für elektrische Anlagen

Inhaltsverzeichnis

1. Einleitung	Allgemeines	S. 4
	Sicherheitsstudien	S. 6
2. Ablauf der Studien	Chronologische Phasen	S. 9
	Angabe und Analyse der Bedürfnisse	S. 9
	Funktionsanalyse des Systems	S. 10
	Analyse der Ausfallarten	S. 11
	Zuverlässigkeitsdaten	S. 11
	Modellierung	S. 12
	Rechnerische Auswertung der Sicherheitskriterien	S. 14
3. Beispiele von Studien	Vergleich der Architektur von zwei Stromversorgungsnetzen für eine Aufbereitungsanlage	S. 15
	Vorteil einer abgesetzten Leittechnik-Station für eine Höchstspannungsanlage	S. 17
4. Die Hilfsmittel auf dem Gebiet der Betriebssicherheit	Tools für die Störungsanalyse	S. 20
	Modellierungs-Tools	S. 20
5. Schlussfolgerung		S. 21
6. Literaturverzeichnis		S. 22

In der Industrie wie im Dienstleistungssektor nimmt die Bedeutung der Qualität der Stromversorgung ständig zu. Die Qualität des Produktes Strom ist abgesehen von Mängeln wie Spannungsschwankungen oder Oberwellenverzerrungen vor allem durch die Verfügbarkeit der elektrischen Energie gekennzeichnet.

Ein Ausfall der Stromversorgung ist immer unangenehm, kann jedoch zum Beispiel für Informationsverarbeitungssysteme (Informatik, Leittechnik usw.) sehr nachteilig sein. Für bestimmte Prozessindustrien kann er sogar katastrophal sein, und in gewissen Fällen kann er Menschenleben in Gefahr bringen.

Mit Hilfe von Betriebssicherheitsstudien kann die Übereinstimmung zwischen den Anforderungen an die Verfügbarkeit der elektrischen Energie und dem zu errichtenden Netz hergestellt werden. Solche Studien bieten ferner die Möglichkeit, zwei Anlagenarchitekturen miteinander zu vergleichen usw., denn die teuerste Lösung ist nicht immer die beste Lösung...

Der Zweck des vorliegenden Technischen Heftes besteht darin, zu zeigen, wie eine Sicherheitsstudie gemacht wird und welche Methoden und Hilfsmittel angewendet werden. Es werden zwei Beispiele von praktischen Studien vorgestellt: für ein Stromversorgungsnetz für eine Aufbereitungsanlage und für ein Leittechnik-System für eine Hochspannungsanlage.

Solche Studien werden in zunehmendem Masse durch Informatik-«Tools» erleichtert.

1. Einleitung

Allgemeines

Die Spannung an den Klemmen eines Verbrauchers wird durch Erscheinungen beeinflusst, die vom Netz des Elektrizitätsversorgungsunternehmens, der elektrischen Anlage eines anderen Abonnenten oder von der eigenen elektrischen Installation herrühren können.

Störungen des Produktes Strom

■ Die wichtigsten Eigenschaften der von einem öffentlichen MS- oder NS-Verteilnetz gelieferten Spannung sind in der Europäischen Norm EN 50160 festgelegt. Sie gibt die Toleranzen an, die für die Spannung und die Frequenz gewährleistet sein müssen, sowie die Pegel der normalerweise angetroffenen Störssignale, wie zum Beispiel Oberwellenverzerrungen.

Die Tabelle der Abbildung 1 zeigt die von der Norm festgelegten Werte. Somit kann die Qualität der den Verbrauchern einer Anlage gelieferten Energie jederzeit durch verschiedene Störungen beeinträchtigt werden, die entweder vom externen Versorgungsnetz stammen oder von der internen Verteilnetz selbst erzeugt werden. Das Funktionieren der unabhängigen oder zu Systemen zusammengefassten Verbraucher wird durch diese Störungen negativ beeinflusst.

■ Die Funktionsstörungen sowie die Art und die Kosten der dadurch verursachten Schäden hängen sowohl von der Art der Verbraucher als auch vom Reaktionsniveau der Anlage ab. So kann die vorübergehende Abschaltung eines kritischen Verbrauchers schwerwiegende Auswirkungen auf das Verhalten der Anlage haben, ohne dass dieser Verbraucher selber betroffen ist.

■ In allen Fällen muss eine eingehende Studie der Auswirkungen der befürchteten Störungen durchgeführt werden.

Es müssen Massnahmen getroffen werden, um deren Folgen zu begrenzen.

■ In der Tabelle der Abbildung 2 sind die gewöhnlich in elektrischen Netzen angetroffenen Störungen zusammen mit ihren Ursachen und den möglichen Lösungen zur Verringerung ihrer Auswirkungen zusammengefasst.

Norm EN 50160	Niederspannungsstromversorgung
Frequenz	50 Hz \pm 1% während 95% einer Woche 50 Hz + 4% während 100% einer Woche
Spannungsamplitude	Für jede Periode von einer Woche müssen 96% des mittleren Effektivwertes im Bereich von $U_n \pm 10\%$ liegen
Schnelle Spannungsänderungen	5% bis 10% von U_n (4% bis 6% in der Mittelspannung)
Spannungseinbrüche	Richtwerte: ■ Tiefe: Zwischen 10% und 99% von U_n Mehrzahl der Spannungseinbrüche < 60% von U_n ■ Dauer: Zwischen 10 ms und 1 Minute Mehrzahl der Spannungseinbrüche < 1 s ■ Anzahl: Einige 10 bis 1000 im Jahr
Kurze Unterbrechungen	Richtwerte: ■ Tiefe: 100% von U_n ■ Dauer: Bis zu 3 Minuten, 70% der kurzen Unterbrechungen sind kürzer als 1 s ■ Anzahl: Einige 10 bis mehrere 100 im Jahr
Lange Unterbrechungen	Richtwerte: ■ Tiefe: 100% von U_n ■ Dauer: Mehr als 3 Minuten ■ Anzahl: Zwischen 10 und 50 im Jahr

Abb. 1: Störungen in den Netzen und von der Norm festgelegte Werte.

■ Die Verringerung der Auswirkungen von Oberwellen, schnellen Spannungsschwankungen, Spannungungleichgewichten, Frequenzschwankungen und Überspannungen wird mit Hilfe von an den entsprechenden Fall angepassten Betriebsmitteln bewerkstelligt. Deren Dimensionierung und die Wahl ihres Anschlusspunktes bilden den Gegenstand von eingehenden Studien, die den Rahmen des vorliegenden Dokumentes sprengen (siehe Literaturverzeichnis).

Ausfälle der Stromversorgung

Diese sind für industrielle Prozesse und Schwachstromsysteme immer weniger tolerierbar, da sie hohe Kosten verursachen.

■ Die Unempfindlichkeit gegen Ausfälle der Versorgungsspannung erfordert spezielle Einrichtungen, wie zum Beispiel unterbrechungsfreie Stromversorgungen oder Notstromaggregate. Diese Einrichtungen genügen in der Regel nicht, um alle Probleme zu lösen. Die Netzarchitektur, die Wiedereinspeisungsmechanismen, das Zuverlässigkeitsniveau der Betriebsmittel, die

Selektivität der Schutzeinrichtungen sowie die Wartungspolitik spielen bei der Reduktion und Beseitigung der Unterbrechungszeiten eine wichtige Rolle. Das Minimieren der Stromausfälle erfordert Zuverlässigkeits- bzw. Verfügbarkeitsstudien, die alle diese Faktoren sowie die von der Anlage zugelassene Unterbrechungsdauer berücksichtigen.

Diese Studien ermöglichen die Bestimmung der am besten auf die Bedürfnisse des Betreibers abgestimmten Architektur und Betriebsmittel. Dabei müssen in der Regel die Verbraucher oder Systeme nach ihrem Empfindlichkeitsniveau klassifiziert werden, wobei unterschieden werden muss zwischen

- Verbraucher, die längere Unterbrechungen von 1 Stunde oder mehr zulassen (ohne Priorität),
- Verbraucher, die längere Unterbrechungen von einigen Minuten zulassen (mit Priorität),
- Verbraucher, die nach einigen Sekunden wieder gespeist werden müssen (wichtige),

Störung	Mögliche Ursachen	Wichtigste Auswirkungen	Mögliche Lösungen
Frequenzschwankungen	<ul style="list-style-type: none"> ■ Versorgungsnetz ■ Inselbetrieb an unabhängigen Notstromaggregaten 	<ul style="list-style-type: none"> ■ Drehzahlschwankungen von Motoren ■ Funktionsstörungen elektronischer Geräte 	<ul style="list-style-type: none"> ■ Unterbrechungsfreie Stromversorgung
Schnelle Spannungsänderungen	<ul style="list-style-type: none"> ■ Versorgungsnetz ■ Lichtbogenofen ■ Schweißmaschine ■ Belastungstöße 	<ul style="list-style-type: none"> ■ Flackern der Beleuchtung (Flicker) ■ Drehzahlschwankungen von Motoren 	<ul style="list-style-type: none"> ■ Erhöhung der Kurzschlussleistung ■ Änderung der Anlagenarchitektur
Spannungseinbrüche	<ul style="list-style-type: none"> ■ Versorgungsnetz ■ Einschalten von bedeutenden Lasten ■ Externe oder interne Fehler 	<ul style="list-style-type: none"> ■ Verlöschen von Entladungslampen ■ Funktionsstörungen von Reglern oder Antrieben ■ Drehzahlschwankungen oder Stillstand von Motoren ■ Abfallen von Schützen ■ Störungen der Digitalelektronik ■ Funktionsstörungen der Leistungselektronik 	<ul style="list-style-type: none"> ■ Unterbrechungsfreie Stromversorgung ■ Erhöhung der Kurzschlussleistung ■ Änderung der Anlagenarchitektur
Kurze oder lange Unterbrechungen	<ul style="list-style-type: none"> ■ Versorgungsnetz ■ Wiedereinschaltungen ■ Interne Fehler ■ Speisungsumschaltungen 	<ul style="list-style-type: none"> ■ Stillstand von Betriebsmitteln ■ Stillstand der Anlage ■ Produktionsausfall ■ Abfallen von Schützen ■ Diverse Funktionsstörungen 	<ul style="list-style-type: none"> ■ Unterbrechungsfreie Stromversorgung ■ Unabhängige Notstromaggregate ■ Änderung der Netzarchitektur ■ Einführung einer Wartungspolitik
Spannungsunsymmetrie	<ul style="list-style-type: none"> ■ Versorgungsnetz ■ Zahlreiche Einphasenlasten 	<ul style="list-style-type: none"> ■ Erwärmung der Motoren und Generatoren 	<ul style="list-style-type: none"> ■ Erhöhung der Kurzschlussleistung ■ Änderung der Netzarchitektur ■ Ausgleich der Einphasenlasten ■ Ausgleichseinrichtungen
Überspannungen	<ul style="list-style-type: none"> ■ Blitzschlag ■ Schaltvorgänge ■ Isolationsfehler 	<ul style="list-style-type: none"> ■ Durchschlag von Betriebsmitteln 	<ul style="list-style-type: none"> ■ Überspannungsableiter ■ Wahl des Isolationspegels ■ Beherrschung der Erdungswiderstände
Oberwellen	<ul style="list-style-type: none"> ■ Versorgungsnetz ■ Zahlreiche nichtlineare Verbraucher 	<ul style="list-style-type: none"> ■ Erwärmung oder Beschädigung von Betriebsmitteln, vor allem von Motoren oder Kondensatoren ■ Funktionsstörungen der Leistungselektronik 	<ul style="list-style-type: none"> ■ Erhöhung der Kurzschlussleistung ■ Änderung der Anlagenarchitektur ■ Filterung

Abb. 2: Störungen in den Netzen, Ursachen, Auswirkungen und Lösungen.

- Verbraucher, die keine Unterbrechung zulassen (lebenswichtige). Die Abbildung 3 zeigt als Beispiel das vereinfachte Schema eines Netzes, für das diese Unterscheidung gemacht wurde.
- Die **lebenswichtigen** Verbraucher, die absolut keine Unterbrechung zulassen, werden durch eine unterbrechungsfreie Stromversorgung gespeist.
- Die **wichtigen** Verbraucher werden wenige Sekunden nach dem Netzausfall wieder gespeist, sobald die Spannung und die Frequenz des Notstromaggregates stabilisiert sind.
- Die Verbraucher **mit Priorität** werden wieder eingeschaltet, sobald die wichtigen Verbraucher wieder in Betrieb sind.
- Die Verbraucher **ohne Priorität**, die eine längere Unterbrechungsdauer zulassen, werden erst wieder eingeschaltet, wenn die Spannung des externen Versorgungsnetzes wieder vorhanden ist.

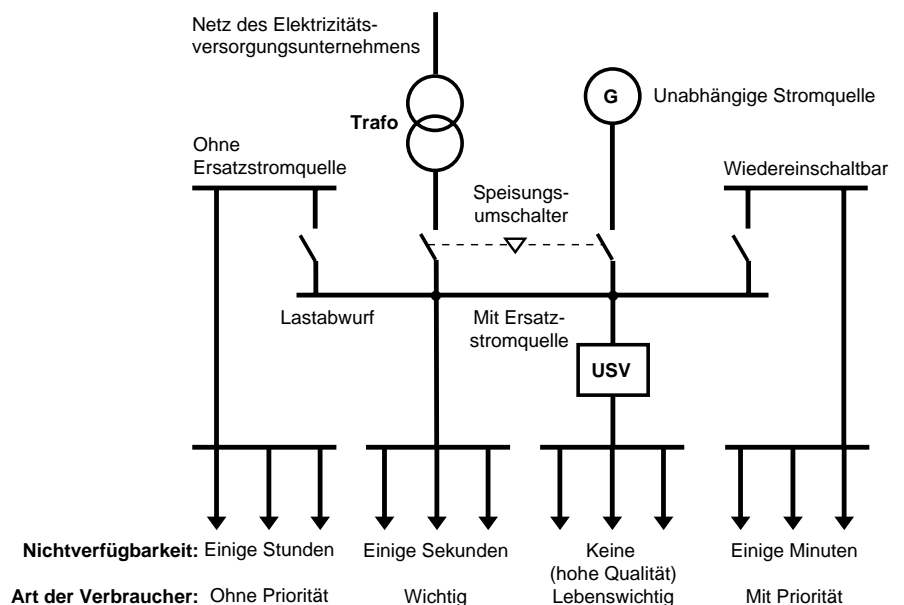


Abb. 3: Zuverlässig gemachte Stromversorgung. Vereinfachtes Schema eines Netzes.

Durch die Wahl einer geeigneten Architektur und von entsprechenden Speisungs-Umschaltautomatiken (siehe Technisches Heft Nr. 161) kann die Positionierung und Dimensionierung der Hilfs- und Ersatzstromquellen optimiert werden, um die betrieblichen Randbedingungen einzuhalten. Es muss daran erinnert werden, dass die Wahl der Erdungsschemas ein wichtiger Faktor ist, denn es hat sich eindeutig gezeigt, dass für Verbraucher, die ein erhöhtes Verfügbarkeitsniveau verlangen, ein isolierter Stern-

punkt dringend zu empfehlen ist, da dieses Schema die Kontinuität der Versorgung beim ersten Isolationsfehler zulässt (siehe Technische Hefte Nr. 172 und 173).

Sicherheitsstudien

Bevor wir auf Sicherheitsstudien für elektrische Anlagen eingehen, ist es angebracht, die Definitionen einiger der von den Zuverlässigkeitsspezialisten verwendeten Begriffe in Erinnerung zu

rufen, auch wenn jedermann weiss, was die Ausdrücke zuverlässig, verfügbar, Wartung, Sicherheit usw. bedeuten (siehe Abb. 4 und 5). Ferner müssen der Anwendungsbereich und die generellen Eigenschaften der Studien genannt werden.

Anwendungsbereiche und charakteristische Eigenschaften der Studien

■ Anwendungsbereiche: Die Studien werden für alle Arten von elektrischen Netzen durchgeführt, von der Niederspannung bis zur Hochspannung und für Ihre Schutz- und Leittechnik-Systemen.

Betriebssicherheit:

Die Betriebssicherheit ist ein generischer Begriff, der die von einem System gebotene Versorgungsqualität misst, so dass der Anwender in dieses System ein begründetes Vertrauen hat. Das begründete Vertrauen kann durch qualitative und quantitative Analysen der einzelnen Eigenschaften der vom System gebotenen Versorgung erhalten werden. Diese Eigenschaften beruhen auf den nachstehend definierten probabilistischen Werten.

Zuverlässigkeit:

Wahrscheinlichkeit, dass eine Betrachtungseinheit unter bestimmten Bedingungen während einer bestimmten Zeit $[t_1, t_2]$ eine geforderte Funktion erfüllen kann. Bezeichnung $R(t_1, t_2)$.

Verfügbarkeit:

Wahrscheinlichkeit, dass eine Betrachtungseinheit in der Lage ist, unter bestimmten Bedingungen zu einem bestimmten Zeitpunkt t eine geforderte Funktion zu erfüllen. Bezeichnung $D(t)$.

Wartbarkeit:

Wahrscheinlichkeit, dass eine bestimmte Wartungsoperation während einer bestimmten Zeit $[t_1, t_2]$ durchgeführt werden kann.

Sicherheit:

Wahrscheinlichkeit der Vermeidung eines Ereignisses, dessen Folgen gefährlich sind.

Ausfallrate:

Wahrscheinlichkeit, dass eine Betrachtungseinheit ihre Befähigung verliert, eine Funktion im Intervall $[t, t+dt]$ zu erfüllen, wobei sie während der Zeit $[0, t]$ nicht ausgefallen war. Bezeichnung λ .

Äquivalente Ausfallrate:

Wahrscheinlichkeit, dass ein System seine Befähigung verliert, eine Funktion im Intervall $[t, t+dt]$ zu erfüllen, wobei es während der Zeit $[0, t]$ nicht ausgefallen war. Bezeichnung $\lambda_{\text{äq}}$.

MTTF (Mean Time To Failure):

Mittlere störungsfreie Zeit bis zum ersten Ausfall.

MTBF (Mean Time Between Failure):

Mittlere Zeit zwischen zwei Ausfällen eines reparierbaren Systems.

MUT (Mean Up Time):

Mittlere störungsfreie Zeit zwischen zwei Ausfällen eines reparierbaren Systems.

MTTR (Mean Time To Repair):

Mittlere Reparaturzeit.

MDT (Mean Down Time):

Mittlere Zeit, während der das System nicht verfügbar ist. Diese umfasst die Zeit für die Feststellung der Störung, die Zeit für die Mobilisierung des Wartungsdienstes, die Zeit für die Beschaffung des defekten Materials und die Reparaturzeit.

Reparaturrate:

Kehrwert der mittleren Reparaturzeit. FMEA (Fehlermöglichkeits- und einflussanalyse): Ermöglicht das Studium der Auswirkungen der Ausfälle von Komponenten aus das System.

Modell:

Grafische Darstellung der Kombination der bei der FMEA gefundenen Ausfälle und ihrer Wartungsprozesse.

Befürchtetes Ereignis:

Systemausfall, der analysiert werden muss, um nachzuweisen, dass der Anwender ein begründetes Vertrauen in das System haben kann. Dieser Systemausfall ist ein Mass für die Versorgungsqualität.

Abb. 4: Definitionen.

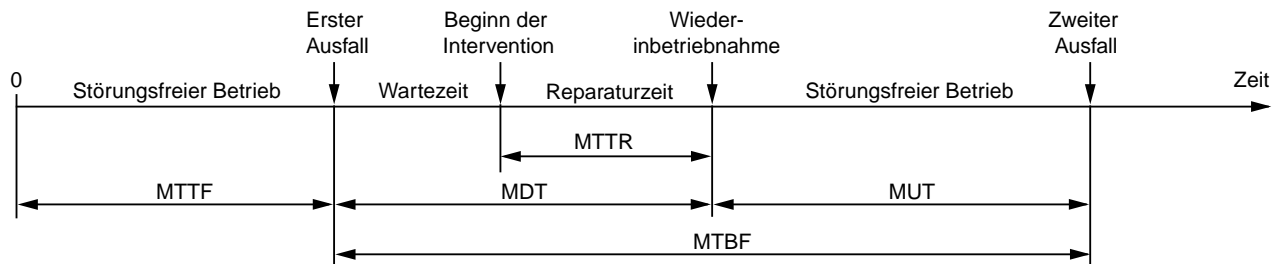


Abb. 5: Beziehungen zwischen der verschiedenen Grössen, welche die Zuverlässigkeit, Wartbarkeit und Verfügbarkeit einer Maschine kennzeichnen.

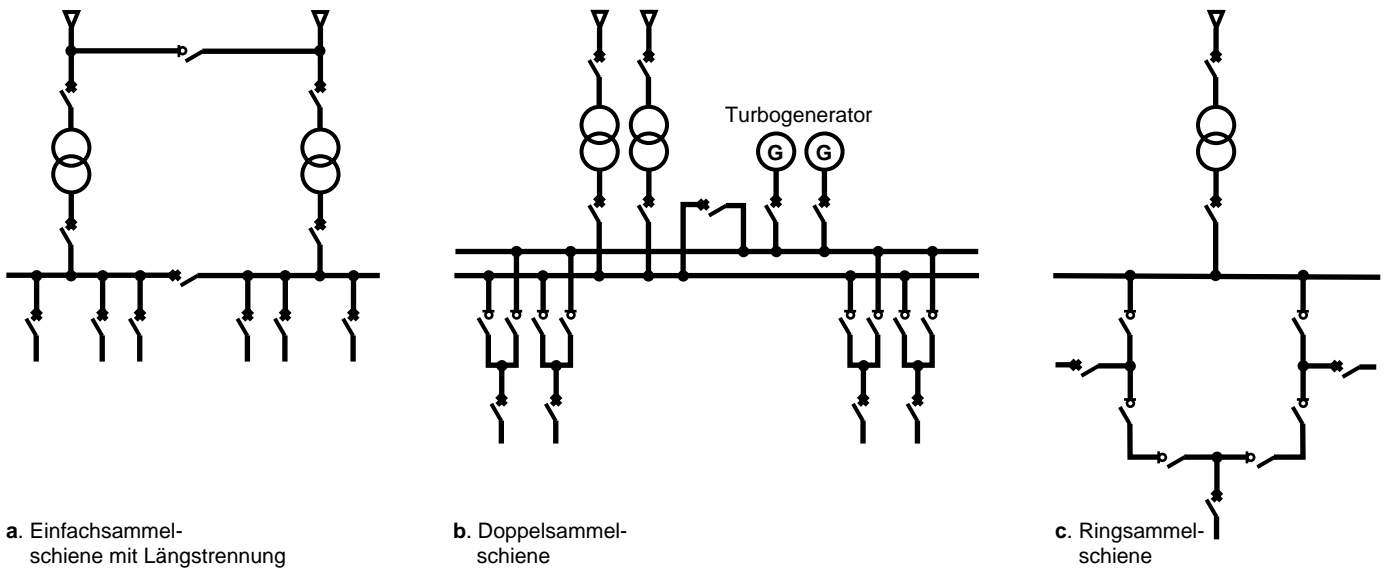


Abb. 6: Netzarchitekturen.

	Vorstudie	Detaillierte Studie
Detaillierungsgrad der Hypothesen	1 einzige Ausfallart (1 Häufigkeit, 1 mittlere Dauer)	In Familien aufgeteilte Ausfälle in Funktion ihrer Auswirkungen auf das System
Detaillierungsgrad der Modellierung	Die Auswirkungen der Ausfälle werden grossen Familien zugeordnet	Die Auswirkungen der Ausfälle werden detailliert analysiert

Abb. 7: Unterschiede zwischen einer Vorstudie und einer detaillierten Studie.

Dabei können die Netze wie folgt ausgeführt sein:

- Einfachsammelschiene,
- Einfachsammelschiene mit Längstrennung (siehe Abb. 6a),
- Doppelsammelschiene (siehe Abb. 6b),
- Ringsammelschiene (siehe Abb. 6c) und

□ mit oder ohne Umkonfigurierung oder Lastabwurf.

■ Charakteristische Eigenschaften der Studien:

Die Studien werden an die angegebenen Bedürfnisse angepasst. Dies zeigt sich an

- dem Detaillierungsgrad der Studie,
- der Art der Analyse,
- der Art der Betriebssicherheitskriterien.

□ Detaillierungsgrad der Studie (siehe Abb. 7)

– Kurz- oder Vorstudie:

Dabei handelt es sich um eine pessimistische Studie, die im allgemeinen gebraucht wird, um rasch eine technische Wahl zu treffen.

– Sehr detaillierte Studie, die möglichst viele Faktoren berücksichtigt: Berücksichtigung aller Betriebsarten, detaillierte Analyse der möglichen Ausfälle und ihrer Auswirkungen, möglichst wirklichkeitsnahe Modellierung des Störungsverhaltens des Systems.

□ Arten der Analyse

– Auslegungshilfe durch Bewertung der Betriebssicherheitskriterien (siehe Abb. 8),

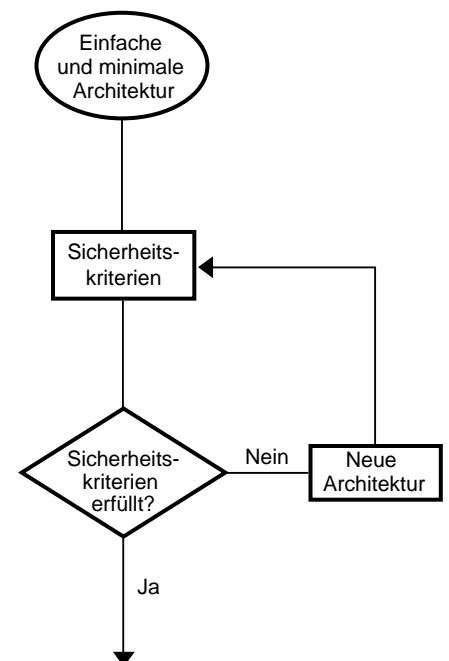


Abb. 8: Auslegungshilfe.

– Vergleich verschiedener Architekturen (siehe Abb. 9)

□ Arten der zu quantifizierenden Kriterien (siehe Abb. 10)

– Mittlere Zeit, während der das System störungsfrei arbeitet (MUT),

– Mittlere Zeit, während der das System arbeitet, bis es bestimmte Verbraucher erstmals nicht mehr speist (MTTF),

– Wahrscheinlichkeit, bestimmte Verbraucher nicht mehr zu speisen (Verfügbarkeit),

– Mittlere Anzahl Ausfälle im Jahr (λ_{aq}),

– Mittlere Reparaturzeit ($1/\mu_{\text{aq}}$),

– optimale Häufigkeit einer vorbeugenden Wartung,

– Berechnung von Ersatzteilsätzen.

Diese Kriterien ermöglichen eine Bewertung des Verhaltens des Systems und somit eine Bestimmung einer Architektur, welche die Sicherheitserwartungen erfüllt, ohne dass die wirtschaftlichen Randbedingungen vergessen werden.

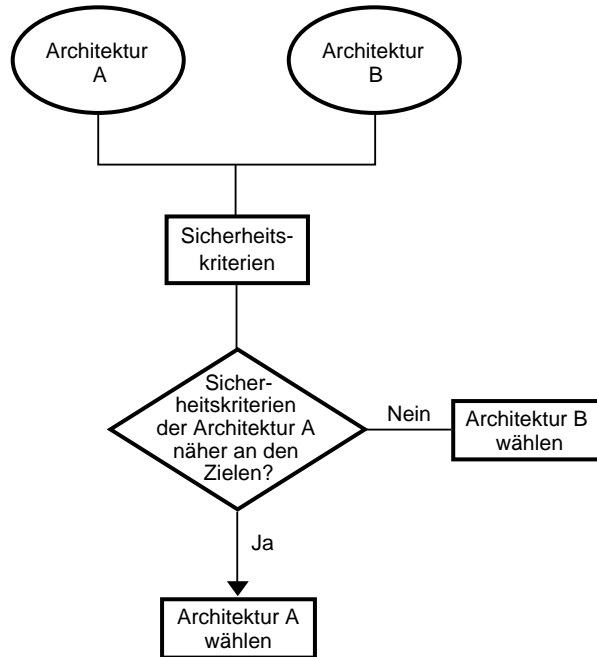
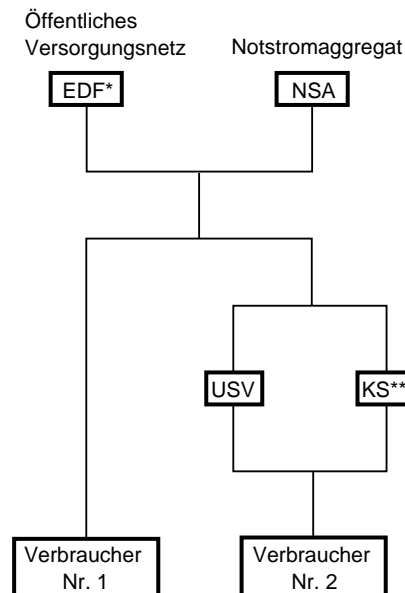


Abb. 9: Vergleich verschiedener Architekturen.



Berechnet werden kann:

– die Wahrscheinlichkeit, dass das NSA bei einem Ausfall des EDF-Netzes nicht anläuft,

– die optimale Häufigkeit der vorbeugenden Wartung des NSA,

– die Anzahl Minuten im Jahr, während denen der Verbraucher Nr. 1 ohne Spannung ist,

– die Anzahl Minuten im Jahr, während denen der Verbraucher Nr. 2 ohne Spannung ist,

* EDF: Electricité de France

** KS: Kontaktloses Schütz

Abb. 10: Darstellung der Kriterien für die Bewertung der Betriebssicherheit.

2. Ablauf der Studien

Chronologische Phasen

Unabhängig von den vom Projektanten oder Betreiber einer elektrischen Anlage angegebenen Bedürfnissen umfasst der Ablauf der Sicherheitsstudie die folgenden Phasen (siehe Abb. 11):

- Angabe und Analyse der Bedürfnisse
- Funktionsanalyse des Systems
- Analyse der Ausfallarten
- Modellierung
- Rechnerische Auswertung der Sicherheitskriterien

In den meisten Fällen müssen diese Phasen mehrmals durchlaufen werden:

- Zweimal, wenn zwei Schemas miteinander verglichen werden müssen,
- n-mal, wenn es sich um Iterationen handelt, um die Architektur zu bestimmen, welche die Bedürfnisse unter Berücksichtigung der technisch-wirtschaftlichen Gegebenheiten am besten erfüllt.

Angabe und Analyse der Bedürfnisse

Wie am Schluss des vorhergehenden Kapitels erwähnt, muss der Auftraggeber genau angeben (siehe Abb. 12):

- auf was sich die Studie bezieht, zum Beispiel Leittechnik-System für eine Schaltanlage, und die verfügbaren Auslegungsdaten liefern,
- Art des Auftrags (Art der Analyse), zum Beispiel:
 - Nachweis des Vertrauensniveaus, das man der elektrischen Speisung eines kritischen Prozesses zuordnen kann (auf eine Studienart und Arten von zu bewertenden Kriterien ausgerichtet),
 - Suche nach objektiven Kriterien, die eine technisch-wirtschaftliche Analyse gestatten,
 - Ermittlung der am besten an die Bedürfnisse angepassten Architektur (auf eine Studienart ausgerichtet),
 - Unterstützung der Auslegung eines Betriebsmittels.

Diese Punkte lassen sich kombinieren. So kann ein Unternehmen die Architektur suchen, die seine Bedürfnisse in Bezug auf die Speisung eines

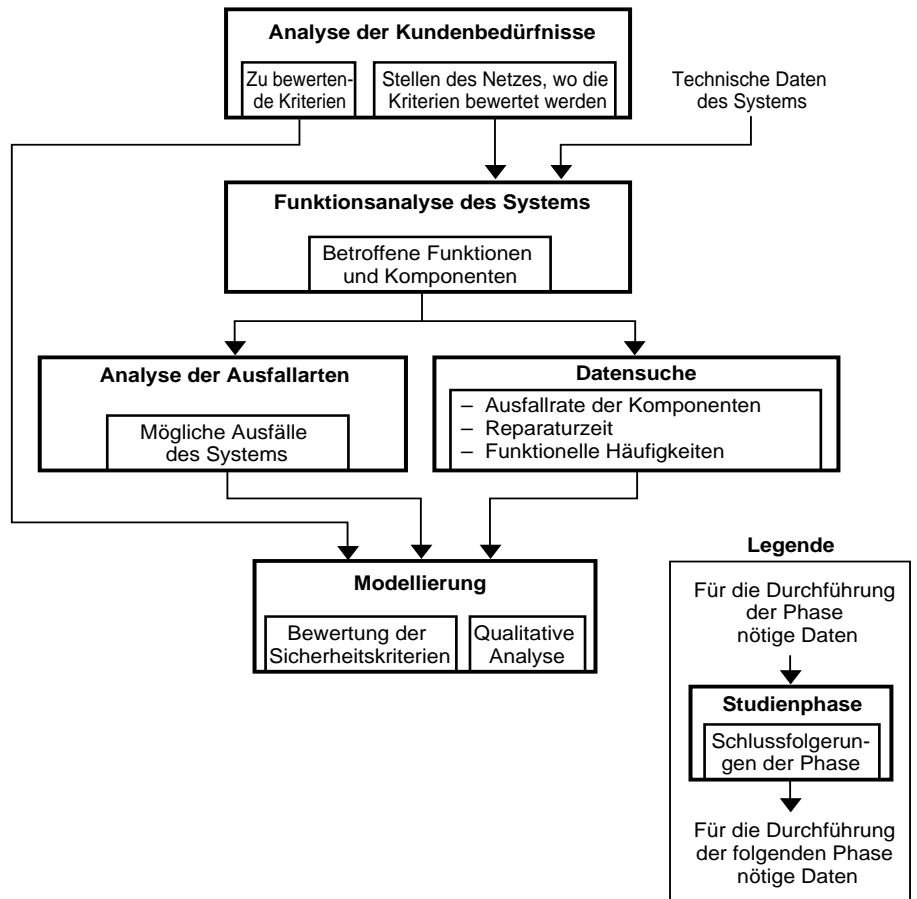


Abb. 11: Die chronologischen Phasen der Durchführung einer Betriebssicherheitsanalyse.

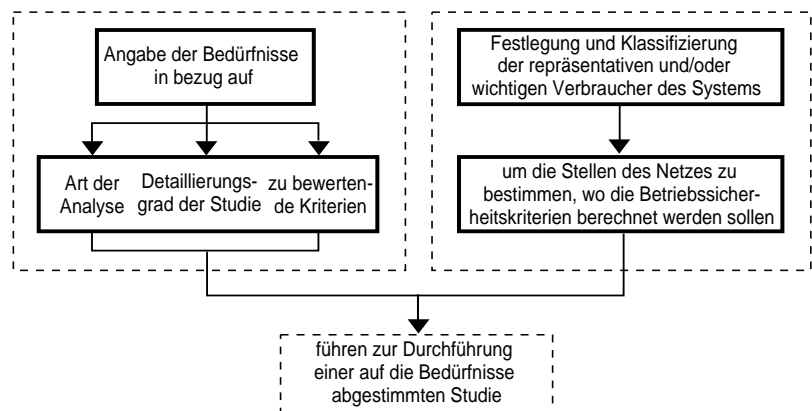


Abb. 12: Für die Studie erforderliche Informationen.

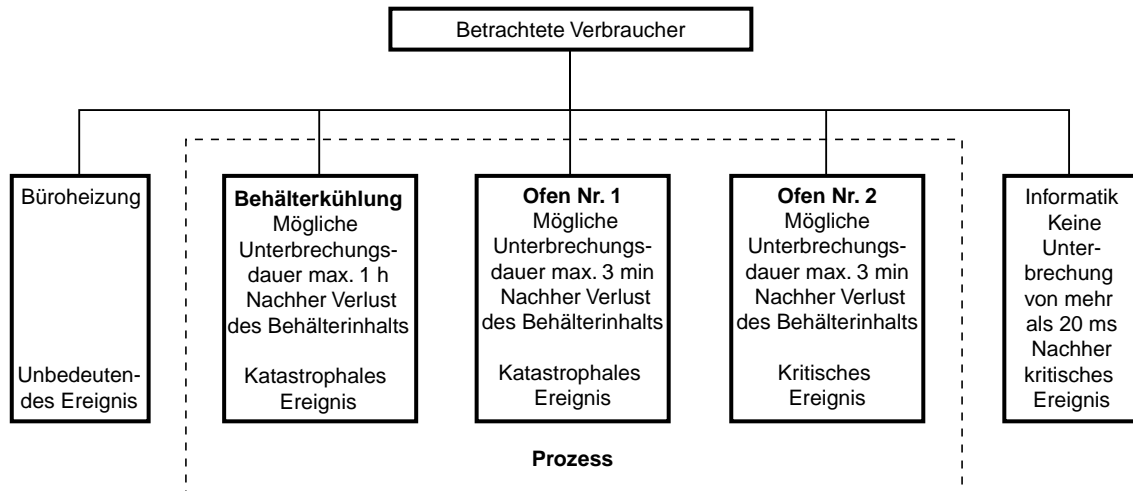


Abb. 13: Die Spezifizierung der Verfügbarkeit ist Sache des Kunden.

kritischen Prozesses im Rahmen einer technisch-wirtschaftlichen Analyse am besten erfüllt.

Welches die Reaktion und die zulässige Dauer eines Ausfalls der Versorgung ist, um wo was zu speisen, muss sich der Kunde zum Beispiel in bezug auf die Sicherheit, den Produktionsausfall oder den Informationsverlust überlegen.

■ Risiko:

Für eine Versicherungsgesellschaft entspricht der Begriff des Risikos dem (moralischen, sozialen und wirtschaftlichen) Gewicht der befürchteten Ereignisse. In bezug auf einen Produktionsausfall ist die Abschätzung des Risikos ziemlich einfach: das Produkt aus der Eintretenswahrscheinlichkeit und den Kosten des befürchteten Ereignisses ergibt eine ziemlich genaue Idee.

Die Bewertung des Risikos ermöglicht die Kenntnis des zu bezahlenden Preises für den entgangenen Gewinn oder die Versicherung oder eine optimierte elektrische Anlage.

■ Formalisierung der Bedürfnisse (siehe Abb. 13):

Eine Möglichkeit, die Bedürfnisse auszudrücken, besteht darin, die verschiedenen Verbraucher je nach der Unterbrechungsdauer, die sie aushalten können (keine, einige Sekunden, einige Minuten, einige Stunden) zu klassifizieren.

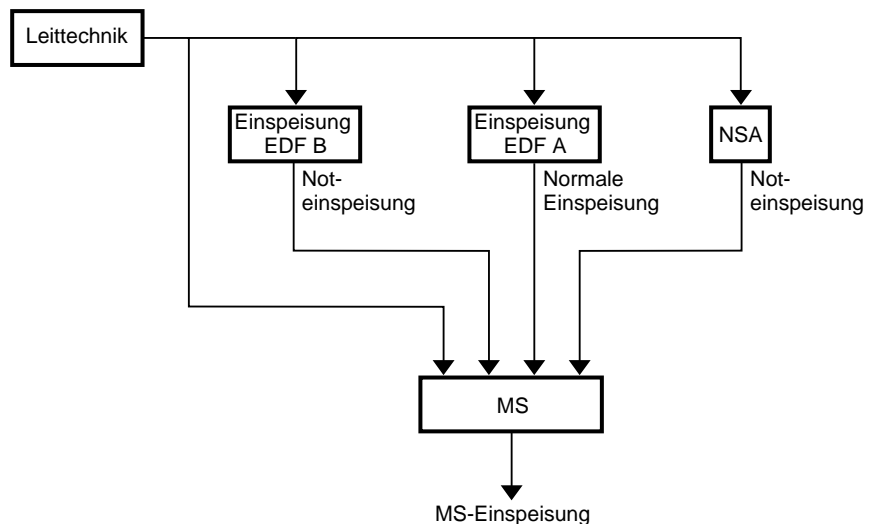


Abb. 14: Funktionelles Blockschema.

Funktionsanalyse des Systems

Die Funktionsanalyse beschreibt in visueller oder textlicher Form die Rolle des Netzes und/oder von Bestandteilen desselben.

Diese Analyse führt zu zwei sich ergänzenden Beschreibungen des Netzes:

■ Eine formelle Beschreibung mit funktionellen Blockschemas (siehe

Abb. 14), deren Zweck darin besteht, die Architektur des Systems und die funktionellen Verbindungen zwischen den einzelnen Teilen des Systems darzustellen.

■ Eine Verhaltensbeschreibung (siehe Abb. 15), deren Zweck darin besteht, die Verkettung der einzelnen möglichen Zustände zu beschreiben. Das Schwergewicht liegt auf der Identifikation der Ereignisse, die Veränderungen des Systems bewirken. Das bei dieser

Analyse entwickelte Modell legt das Schwergewicht auf die verschiedenen Umkonfigurationenpunkte der Architektur. Diese zweite Analyse bietet die Möglichkeit, den funktionellen Aspekt zu berücksichtigen, wenn er mit dem Störungsaspekt in Wechselwirkung steht.

Analyse der Ausfallarten

Diese Analyse hat den Zweck, folgendes zu ermitteln:

- Liste der möglichen Ausfallarten für jeden der in der Funktionsanalyse identifizierten Teile.
- Deren Ursachen (eine einzige Ursache genügt).
- Die Auswirkungen dieser Ausfälle auf das System (auch «einfache Ereignisse» genannt).
- Die mit jeder Ausfallart im Rahmen einer quantitativen Studie verbundenen Ausfallarten.

Die Resultate werden als Tabellen dargestellt (siehe Abb. 16).

Diese Analyse kann als die erste Modellierungsstufe betrachtet werden.

Zuverlässigkeitsdaten

Im Rahmen der quantitativen Bewertung müssen probabilistische Ausfalldaten der Betriebsmittel des Systems zur Verfügung stehen. Die probabilistischen Eigenschaften müssen mit den Ausfallarten verbunden werden.

Diese sind:

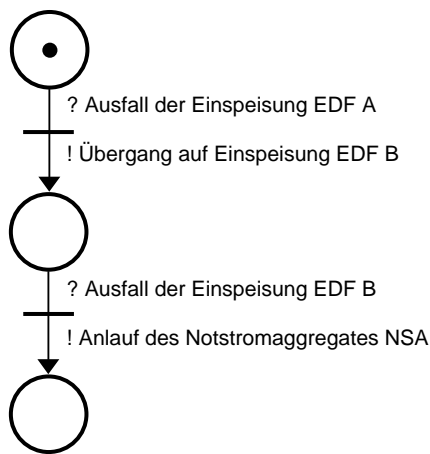
- Die Ausfallrate und ihre Aufteilung in Funktion der Ausfallarten.
- Die damit verbundene mittlere Reparaturzeit und die Häufigkeit der vorbeugenden Wartung (siehe Abb. 17).

Die Ausfallraten

Es sei daran erinnert, dass es sich darum handelt, die Wahrscheinlichkeit zu quantifizieren, dass im Intervall $[t, t+dt]$ ein Ausfall eintritt, wobei vor t kein Ausfall vorhanden war.

Schneider Electric verfügt über eine von verschiedenen Quellen gespeiste Datenbank:

- Interne Studien und Analyse der bei einem Ausfall zurückerhaltenen Betriebsmittel.
- Statistiken der von den Elektrizitätsversorgungsunternehmen und anderen Herstellern beobachteten Ausfälle.
- Vorwiegend amerikanische Sammlungen von Zuverlässigkeitsdaten:



Dieses Petri-Netz drückt die Tatsache aus, dass beim Ausfall von EDF A auf EDF B übergegangen wird. Wenn EDF B ausgefallen ist, startet das Notstromaggregat NSA

Abb. 15: Verhaltensbeschreibung in der Form eines Petri-Netzes.

Funktion	Ausfallart	Ursachen	Auswirkungen auf das System
Einspeisung EDF	Verlust des normalen Modus	<ul style="list-style-type: none"> ■ Störung bei der EDF ■ Ausfall des Transformators ■ Leistungsschalter unbeabsichtigt offen 	Umschaltung auf die Noteinspeisung
Not-einspeisung	Verlust des Not-Modus im Betrieb	<ul style="list-style-type: none"> ■ Funktionsstörung des NSA ■ Leistungsschalter unbeabsichtigt offen ■ Ausfall des Transformators 	Ausfall der Stromversorgung
	Störung des Normal-Modus und Not-Modus nicht verfügbar	<ul style="list-style-type: none"> ■ Nichtanlauf des NSA ■ Leistungsschalter offen blockiert 	

Abb. 16: Analyse der Ausfallarten.

Betriebsmittel	Ausfallarten	Ausfallraten	Reparaturzeit, Häufigkeit der vorbeugenden Wartung
Leistungsschalter	■ geschlossen blockiert	λ_1	μ_1 , —
	■ unbeabsichtigt offen	λ_2	
Notstromaggregat	■ Ausfall im Betrieb	λ_4	μ_2 , 6 Monate
	■ Ausfall beim Anlaufen	λ_5	
Transformator	■ Ausfall im Betrieb	λ_6	μ_3 , X Monate

Abb. 17: Fiktiver Auszug aus den für eine Studie notwendigen Zuverlässigkeitsdaten.

□ Für nichtelektronische Komponenten:
– IEEE 500 (Erfahrungswerte von US-Kernkraftwerken)

– NPRD 91 (Erfahrungswerte von militärischen und nichtmilitärischen Systemen der USA)

□ Für elektronische Komponenten werden die Daten normalerweise durch Berechnung aufgrund des Military Handbook 217 (F) oder der Zuverlässigkeitsdatensammlung des Centre National d'Etudes des Télécommunications erhalten.

Gewisse Komponenten haben während einer Periode ihrer Lebensdauer eine Ausfallrate (λ), die in Funktion der Zeit konstant ist. Das heisst, dass ihre Ausfallfähigkeit zeitunabhängig ist. Dies ist der Fall bei den elektronischen Komponenten (Exponentialgesetz). Elektrische Komponenten altern, was bedeutet, dass ihre Ausfallrate in Funktion der Zeit nicht konstant ist. Meistens beruhen die verfügbaren Daten auf der Annahme von konstanten Ausfallraten.

Die Verwendung von für das untersuchte System nichtspezifischen Daten sowie von konstanten Ausfallraten, obschon bestimmte Bestandteile altern, ist trotzdem von grossem Interesse, da dadurch gültige Vergleiche zwischen verschiedenen Systemen angestellt werden können.

Eine Architektur zu finden, die 10mal zuverlässiger oder 10mal verfügbarer ist als eine andere usw. bedeutet, dass diese Architektur für das betrachtete Kriterium 10mal besser ist. Der relative Wert ist oft wichtiger als der absolute Wert.

Die Zuverlässigkeits-Datenbank von Schneider Electric bezweckt, möglichst viele Daten zusammenzufassen. Es sind Validitätskriterien eingeführt worden, um die Qualität der enthaltenen Daten sicherzustellen.

Überprüft wird

- die Art und Weise, wie die Erfahrungswerte gesammelt worden sind, und auf welchen Daten sie beruhen,
- das angewendete Berechnungsverfahren für die voraussichtlichen Anwendungsbedingungen, Temperaturen, Umgebungsbedingungen usw.

Mit der Zeit stehen aufgrund dieser Arbeit Zuverlässigkeitsdaten für das Studium irgendeiner Anlage zur Verfügung, oder diese können extrapoliert werden.

Die mittleren Reparaturzeiten

hängen direkt von der Wartungspolitik des Unternehmens ab. Die wichtigsten Entscheidungen betreffen insbesondere die Ersatzteillager, die Präsenzzeiten der Wartungsteams, die Häufigkeit der vorbeugenden Wartungsarbeiten und die Art der mit den Lieferanten abgeschlossenen Wartungsverträge usw. Die Auswirkungen von Änderungen der Parameter der Wartungspolitik auf das Verhalten der Systeme können den Gegenstand einer spezifischen Analyse sein.

Die betrieblichen Umkonfigurierungen

Bei betrieblichen Umkonfigurierungen, wenn der funktionelle Aspekt mit dem Störungsaspekt in Wechselwirkung steht (zum Beispiel bei einem Lastabwurf aus Tarifgründen), haben diese Umkonfigurierungen einen Einfluss auf die Modellierung.

Modellierung

Die Störungen des Netzes werden durch ein Modell dargestellt. Das Modell ist eine grafische Darstellung der Kombinationen der von der Analyse der Ausfallarten festgestellten Ereignisse, die zum Beispiel zum Ausfall der Stromversorgung bestimm-

ter Verbraucher und zu ihrem Reparaturprozess beitragen. Dieses Modell bietet die folgenden Möglichkeiten:

- Mit dem Kunden ist Gespräch zu treten, um unser Verständnis der Störungen des Netzes zu validieren.

- Die Leistungsdaten des Netzes durch die Suche nach systematischen Ausfällen und den einfachsten Kombinationen, die zum befürchteten Ereignis beitragen, qualitativ zu analysieren.

- Bewertung der Leistungsdaten des Netzes durch die Berechnung der Betriebssicherheitskriterien. Je nach der Architektur des untersuchten Systems, den unerwünschten Ereignissen, den zu bewertenden Kriterien und den in den Modellen berücksichtigten Hypothesen stehen verschiedene Verfahren zu Verfügung.

Die wichtigsten Modellierungsverfahren

- Kombinatorisch:

Kombination von einfachen Ereignissen. Dies ist bei einem Fehlerbaum der Fall (siehe Abb. 18).

Ein Fehlerbaum ist eine Zerlegung von Ereignissen in einfache Ereignisse.

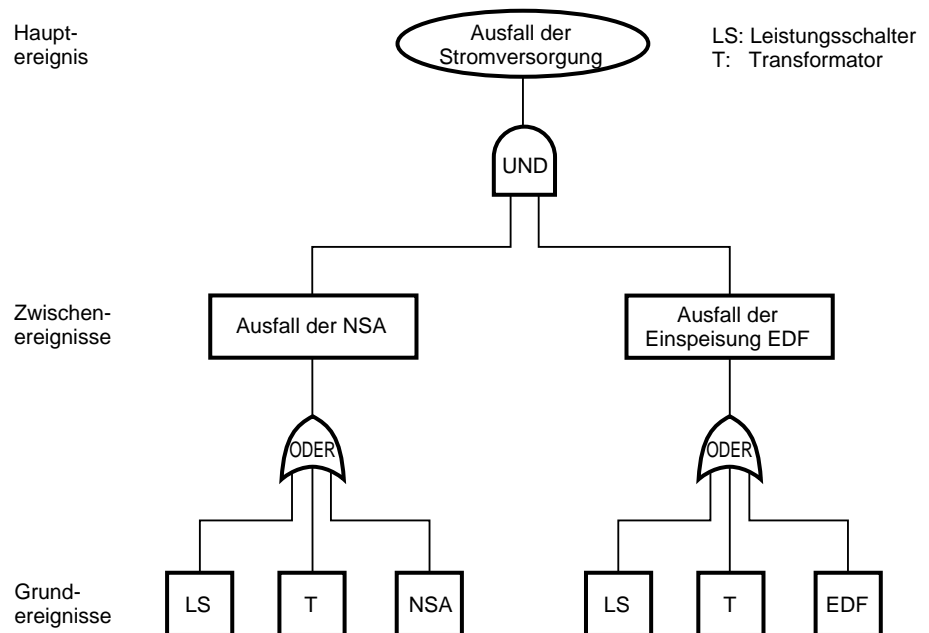


Abb. 18: Modellierung durch Fehlerbaum. Die Tatsache, dass der Ausfall der NSA nur einen Sinn hat, wenn zuerst die EDF ausgefallen ist, erscheint nicht.

Auf diese Weise werden die unmittelbaren Ursachen des Ausfalls der Stromversorgung gesucht. Das sind die Zwischenereignisse. Die Ursachen dieser Zwischenereignisse werden ihrerseits gesucht. Die Zerlegung geht weiter, bis sie nicht mehr möglich ist oder nichts mehr bringt. Die Endereignisse werden Basisereignisse genannt. Die Zerlegung eines Ereignisses in verursachende Ereignisse erfolgt durch logische Operationen, die Gatter genannt werden (UND-Gatter, ODER-Gatter).

Der Fehlerbaum der Abbildung 18 besagt, dass im als Beispiel genommenen Netz ein totaler Ausfall der Stromversorgung eintritt, wenn die «Einspeisung EDF» und die «Notstromaggregate» ausfallen. Bei einer Modellierung dieser Art wird nicht berücksichtigt, dass der Ausfall der Notstromaggregate nur einen Sinn hat, wenn zuerst die «Einspeisung EDF» ausfällt.

Netze mit Umkonfigurierung und Wartungsstrategien, die komplex sind, sind mit einem Fehlerbaum schwer zu modellieren.

■ **Kombinatorisch und sequentiell:** Kombination von einfachen Ereignissen unter Berücksichtigung des Momentes, wo die Ereignisse auftreten.

□ Vom Markov-Typ (siehe Abb. 19). Zum Formalisieren dieses Modells ist es üblich, einen Graph zu verwenden, der die verschiedenen möglichen Zustände des Systems darstellt. Die Bögen, mit denen die Systemzustände miteinander verbunden werden können, sind durch Raten charakterisiert, die Ausfallraten, Reparaturraten und Häufigkeiten sein können, die für die Betriebsweise repräsentativ sind. Diese Raten stellen die Wahrscheinlichkeit dar, dass das System zwischen t und $t+dt$ seinen Zustand ändert.

Der Graph der Abbildung 19 sagt aus, dass das System 4 Betriebszustände haben kann:

- Der Zustand Nr. 1 ist der Zustand des richtigen Funktionierens.
- Der Zustand Nr. 2 ist der Zustand, in dem die «Einspeisung EDF» ausgefallen ist und die Notstromaggregate angelaufen sind.
- Der Zustand Nr. 3 ist der Zustand, in dem die «Einspeisung EDF» ausgefallen ist und die Notstromaggregate nicht angelaufen sind.

λ_a : Häufigkeit des Ausfalls der Einspeisung EDF
 λ_b : Häufigkeit des Ausfalls der NSA
 μ : Reparaturhäufigkeit

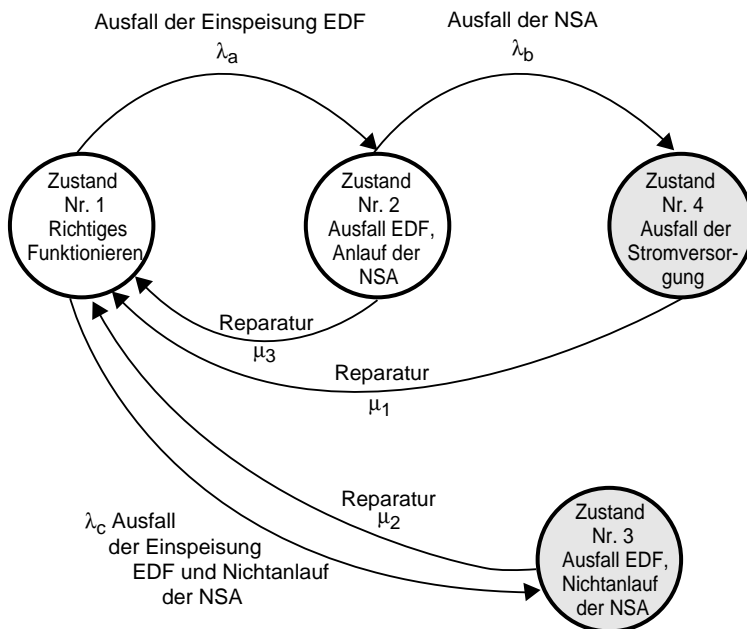


Abb. 19: Störungs-Modellierung in der Form eines Markov-Graph. $\lambda_a, \lambda_b, \mu$ sind aus Prinzip konstant.

– Der Zustand Nr. 4 ist der Zustand, in dem die Notstromaggregate im Betrieb einen Ausfall hatten, während die «Einspeisung EDF» ausgefallen ist. Eine Markov-Modellierung geht davon aus, dass die Häufigkeiten (oder Raten), die den Übergang von einem Zustand des Systems zu einem anderen zulassen, konstant sind. Die mit diesem Modellierverfahren verbundenen Berechnungs-algorithmen können nur unter diesen Bedingungen angewendet werden. Diese Beschränkung führt dazu, Schätzungen vorzunehmen, die mehr oder weniger der Wirklichkeit entsprechen.

□ Von irgendeinem Typ. Der angewendete Formalismus ist in der Regel jener der Petri-Netze. Das Netz wird durch Plätze, Transitionen und Marken dargestellt. Wenn eine Marke eine Transition durchläuft, entspricht dies einem möglichen Betriebs- oder Störungsereignis des

Systems. Diese Transitionen können mit einem probabilistischen Gesetz irgendeiner Art verbunden werden. Solche Kalküle können nur durch Simulation gelöst werden.

- [Seite 14:] Das Petri-Netz der Abbildung 20 stellt die verschiedene Ausfälle dar, die das System erleiden kann:
- Der Transition Nr. 1 ist die Wahrscheinlichkeit des Ausfalls der «Einspeisung EDF» zugeordnet.
 - Der Transition Nr. 2 sind die Wahrscheinlichkeiten des Anlaufs und des Nichtanlaufs der Notstromaggregate zugeordnet.
 - Der Transition Nr. 3 ist die Wahrscheinlichkeit des Ausfalls der Notstromaggregate im Betrieb zugeordnet.

Kriterien für die Wahl einer Modellierungsart: Die Abbildung 21 stellt diese Kriterien tabellarisch dar.

Rechnerische Auswertung der Sicherheitskriterien

Dazu können zwei Verfahren angewendet werden:

- Analytische Auflösung:
 - für Zustands-Graphen,
 - für Fehlerbäume.

Wenn ein System gross oder komplex ist, kann eine analytische Auflösung unmöglich sein.

- Simulation des Verhaltens der Komponenten (Funktionieren oder Ausfall) eines Systems:
 - für Petri-Netze,
 - für Fehlerbäume.

Um eine gewisse Genauigkeit zu erreichen, muss eine grosse Anzahl von Simulationen durchgeführt werden und kann die Berechnungszeit prohibitiv werden, wenn die Abschätzung der Massnahmen mit seltenen Ereignissen verbunden ist.

Die Modellierung eines Systems mit Hilfe eines Petri-Netzes ist die Modellierung, die der effektiven Funktionieren des betrachteten Systems am nächsten liegt. Angesichts der mit der Simulation verbundenen Grenzen wird dieses Verfahren jedoch nicht systematisch angewendet.

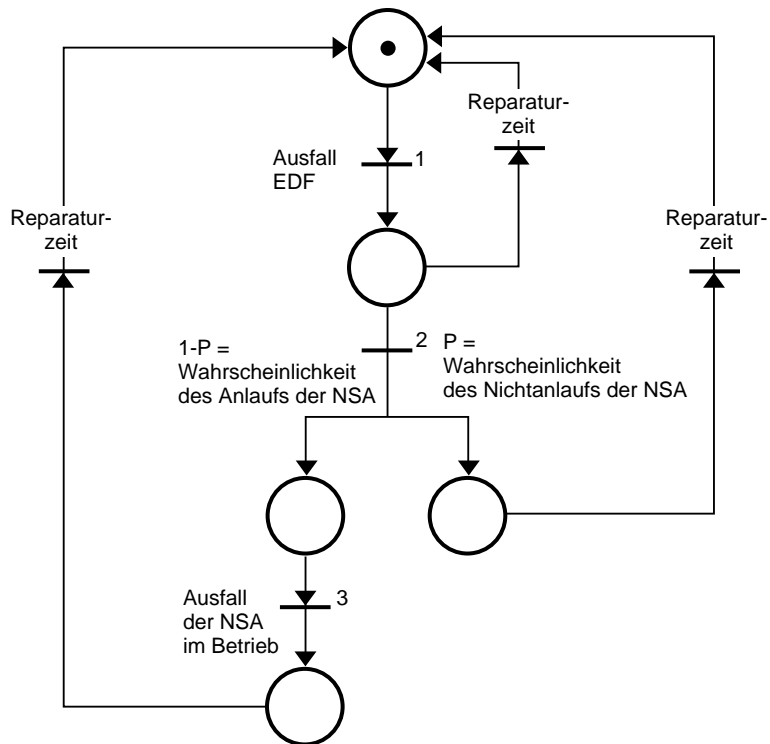


Abb. 20: Modellierung in der Form eines Petri-Netzes.

Auswahlkriterien	Fehlerbaum	Markov-Graph	Petri-Netz
Interaktion der Betriebsart bei der Modellierung	Auflösung unmöglich oder je nach den Algorithmen falsch	Unter bestimmten Bedingungen kann die Auflösung unmöglich oder je nach den verwendeten Algorithmen falsch sein	Geeignet
Numerische Streuung der Daten (Faktor 1000)	Auflösung unmöglich oder je nach den verwendeten Algorithmen falsch; problemlos, wenn Simulation	Unter bestimmten Bedingungen kann die Auflösung unmöglich oder je nach den verwendeten Algorithmen falsch sein	Geeignet
Der zeitliche Aspekt der Ausfälle ist wichtig	Nein	Geeignet	Geeignet
Abschätzung mit seltenen Ereignissen verbunden	Die Simulationsdauer kann prohibitiv sein; bei analytischer Auflösung kein Problem	Geeignet	Die Simulationsdauer kann prohibitiv sein
Abschätzung von:			
■ MUT	–	Geeignet	Geeignet
■ MTTF	Geeignet	Geeignet	Geeignet
■ D(t)	–	Geeignet	–
■ D(∞)	Geeignet (analytische Berechnung)	Geeignet	Geeignet
■ D Mittelwert bei t	Geeignet (Simulation)	–	Geeignet
■ MTTR	–	Geeignet	Geeignet
■ $\lambda_{\text{äq}}$	–	Geeignet	Geeignet

Abb. 21: Kriterien für die Auswahl einer Modellierungsart.

3. Beispiele von Studien

Vergleich der Architektur von zwei Stromversorgungsnetzen für eine Aufbereitungsanlage

■ Vorstellung der Aufbereitungsanlage
Eine Trinkwasseraufbereitungsanlage liefert während 300 Tagen/Jahr bei niedriger Leistung 100 000 m³/Tag und während 65 Tagen/Jahr bei hoher Leistung 200 000 m³/Tag. Die Wasseraufbereitung erfolgt durch 4 Blöcke, von denen jeder 100 000 m³/Tag liefern kann. Mit jedem Block sind 6 Verbrauchertypen R₁, R₂, R₃, R₄, R₅ und R₆ (Pumpen, Desinfektionsanlagen usw.) verbunden, die gleichzeitig funktionieren müssen, damit die Aufbereitung funktioniert (siehe Abb. 22). Der Verbraucher, die das Funktionieren der einzelnen Blöcke sicherstellen, können wie folgt bezeichnet werden:

R_{1a}, ..., R_{6a} Block Nr. 1
R_{1b}, ..., R_{6b} Block Nr. 2
R_{1c}, ..., R_{6c} Block Nr. 3
R_{1d}, ..., R_{6d} Block Nr. 4

Um das Funktionieren bei niedriger Leistung sicherzustellen, wird nur ein einziger Block benötigt. Bei hoher Leistung sind zwei Blöcke erforderlich.

- Bedarfs- und Bedürfnisanalyse
Nach zwei Gesprächen mit dem Kunden haben die Spezialisten folgendes bestimmt:
- Es muss:
 - eine neue Architektur des elektrischen NS-Netzes vorgeschlagen werden, während auf der MS-Ebene (5,5 kV) nicht viel zu ändern ist,
 - nachgewiesen werden, dass das vorgeschlagene Schema mindestens für bestimmte Betriebssicherheitskriterien ebenso gut ist wie das alte.
 - Die zu bewertenden Betriebssicherheitskriterien sind folgende:

- die Wahrscheinlichkeit, gleichzeitig die Stromversorgung der Verbraucher Nr. 1 und der Verbraucher Nr. 6 zu verlieren,
- die Wahrscheinlichkeit, die Stromversorgung der Verbraucher Nr. 3 zu verlieren.

- Funktionsanalyse
Allgemeine Überlegungen zum Funktionieren des Netzes:
- Die Anlage wird durch zwei unabhängige EDF-Einspeisungen versorgt. Es sind zwei Notstromgeneratoren vorhanden, um Ausfällen der EDF-Einspeisungen entgegenzuwirken..
 - Im Normalbetrieb wird die Anlage durch die Einspeisung EDF A versorgt. Wenn diese Einspeisung ausfällt, übernimmt die Einspeisung EDF B die Versorgung. Wenn beide EDF-Einspeisungen ausgefallen sind, laufen die Notstromaggregate an.
 - Es sind zwei Leistungsstufen vorgesehen, niedrige Leistung und

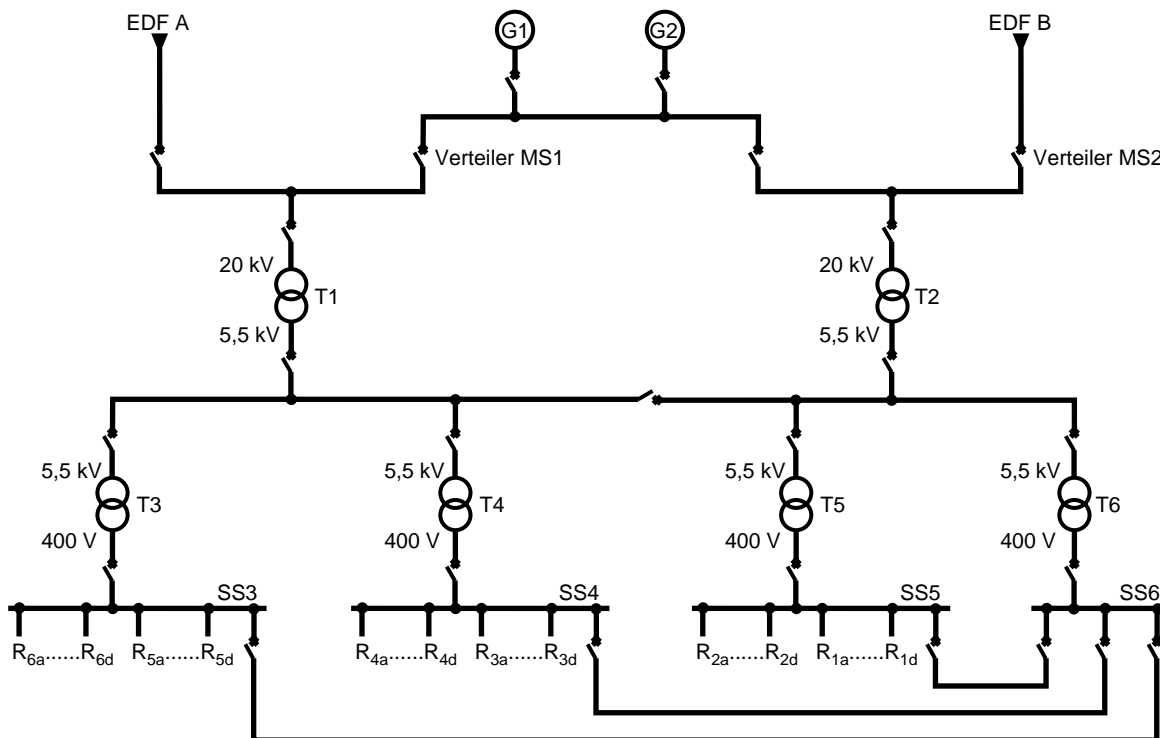


Abb. 22: Vereinfachtes Prinzipschema der ursprünglichen elektrischen Anlage. Einige nachteilige systematische Ausfallmöglichkeiten sind nicht gezeigt.

hohe Leistung. Für den Betrieb mit hoher Leistung genügt die Leistung der Notstromaggregate nicht.

□ Die Aufteilung der Stromversorgung der Verbraucher ist so, dass die Verfügbarkeit nicht sehr hoch ist. So legt zum Beispiel ein Fehler an der Sammelschiene SS3 alle Verbraucher vom Typ R_5 und R_6 still. Die ganze Anlage steht still, da kein Block mehr in Betrieb stehen kann.

□ Das bestehende elektrische Netz wies Sammelschienen mit systematischem Ausfall auf. Ein Kurzschluss an diesen Sammelschienen hätte die Umkonfigurationen betriebsunfähig gemacht.

Die Wahrscheinlichkeit des Kurzschlusses einer Sammelschiene ist klein. Da jedoch das System stark umkonfigurierbar ist, wird dieser Fehler ausschlaggebend. Die systematischen Ausfälle lagen auf der Ebene der Kupplung bei den Umkonfigurationen, die den Transformator T4 betreffen.

□ Für das neue Netz wurden die Verbraucher so voneinander getrennt, dass es möglich ist, den Betrieb mit niedriger Leistung mit den damit verbundenen Verbrauchern an einem einzigen Transformator sicherzustellen, und den Betrieb mit hoher Leistung mit den damit verbundenen Verbrauchern an zwei Transformatoren. Die Abbildung 23 zeigt das Schema des vorgeschlagenen Netzes und die Abbildung 24 seine Funktionsanalyse.

■ Analyse der Resultate

Die Verbesserung der Resultate durch das vorgeschlagene Netz wird durch Verbesserungsverhältnisse in Bezug auf das bestehende Netz dargestellt.

Ausser der Wahrscheinlichkeit des gleichzeitigen Ausfalls der Verbraucher Nr. 1 und Nr. 6 und der Wahrscheinlichkeit des Ausfalls der Verbraucher Nr. 3 haben wir ihre Ausfallhäufigkeit bewertet. Ferner wurden die optimale Wartungshäufigkeit für die Notstromaggregate und der Beitrag an die befürchteten Ereignisse des MS- und NS-Netzes berechnet.

Nachstehend die erzielten Verbesserungen:

□ In Bezug auf die relative Wahrscheinlichkeit des gleichzeitigen Ausfalls der Stromversorgung der Verbraucher Nr. 1 und Nr. 6:

- Niedrige Leistung 110
- Hohe Leistung 55
- Insgesamt 105

□ In Bezug auf die relative Wahrscheinlichkeit des Ausfalls der Verbraucher Nr. 3:

- Niedrige Leistung 99
- Hohe Leistung 54
- Insgesamt 97

Insgesamt ist es mit dem alten Netz 100mal wahrscheinlicher, dass die Stromversorgung der Verbraucher Nr. 1 und Nr. 6 ausfällt, als mit dem vorgeschlagenen Netz. Im alten Netz gibt es effektiv Ausfälle, die direkt zum Ausfall der Lieferung der elektrischen Energie führen.

Wenn das System ausschliesslich mit niedriger Leistung betrieben würde, wäre dieses Verhältnis praktisch dasselbe, da das System vorwiegend mit niedriger Leistung betrieben wird, deshalb auch sein überwiegender Einfluss auf das Gesamtergebnis.

Wenn das System ausschliesslich mit hoher Leistung betrieben wird, ist es mit dem alten Netz rund 50mal wahrscheinlicher, dass die Stromversorgung der Verbraucher Nr. 1 und Nr. 6 ausfällt. Im Fall des Betriebs mit hoher Leistung sind die mit der MS verbundenen Ausfälle ausschlaggebend, wobei dieser Teil des Netzes nur wenig abänderungsfähig ist.

□ In Bezug auf die Ausfallhäufigkeit der Stromversorgung der Verbraucher Nr. 1 und der Verbraucher Nr. 6:

- Niedrige Leistung 22
- Hohe Leistung 21
- Insgesamt 21

□ In Bezug auf die Ausfallhäufigkeit der Stromversorgung der Verbraucher Nr. 3:

- Niedrige Leistung 18
- Hohe Leistung 21
- Insgesamt 20

Die Leistungsdaten des neuen Netzes sind weniger klar, was die Ausfallhäufigkeiten anbetrifft.

Die Berechnungsparameter einer Nichtverfügbarkeitswahrscheinlichkeit sind die Ausfallhäufigkeiten und die Reparaturzeiten. Die Ausfälle, die direkt zu einem Ausfall der Lieferung der elektrischen Energie führen, haben einen desto grösseren Einfluss auf die Nichtverfügbarkeitswahrscheinlichkeit, je länger die Reparaturzeit ist. Das neue Netz ermöglicht eine simultane vorbeugende Wartung, d.h. ohne Unterbrechung des Betriebs der Aufbereitungsanlage.

■ Zusätzliche Auswertungen

Es schien von Interesse zu sein, zusätzliche Vergleichskriterien

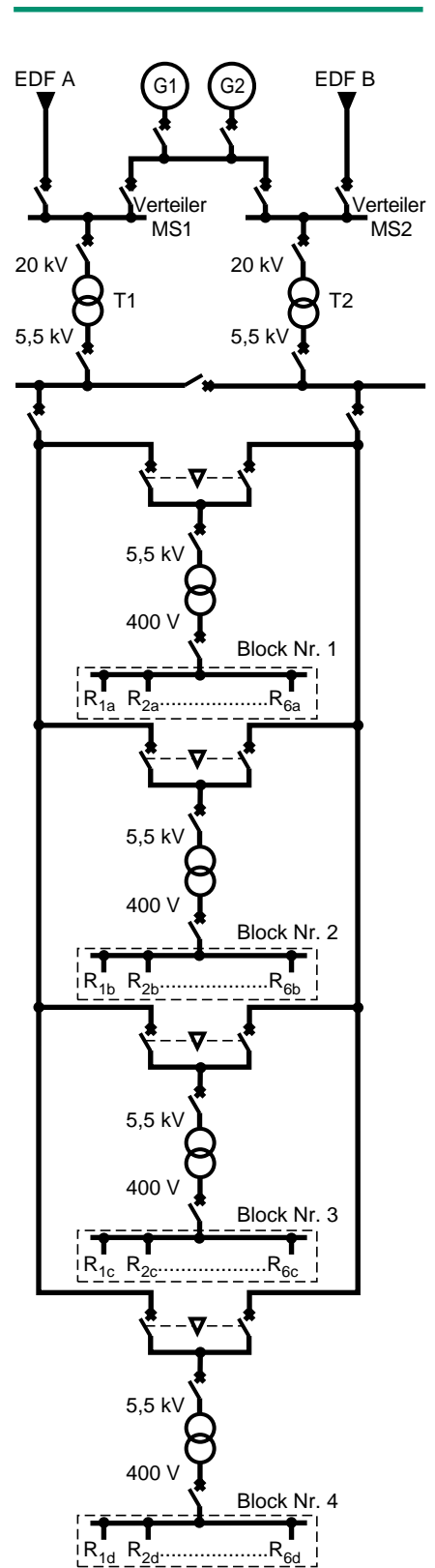


Abb. 23: Prinzipschema der neuen Architektur.

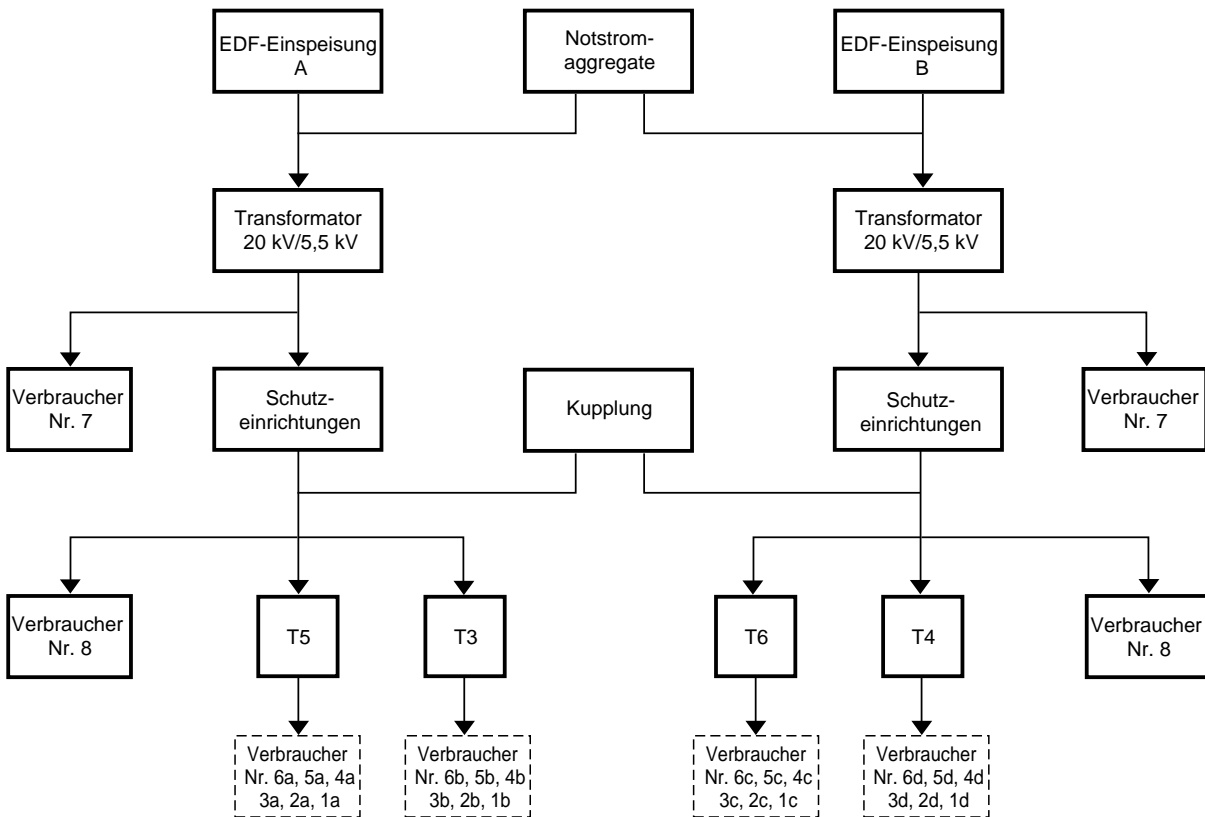


Abb. 24: Funktionsanalyse der neuen Architektur.

zwischen den beiden Architekturen auszuwerten.
 □ Relative Wahrscheinlichkeit des Ausfalls des Betriebs mit hoher Leistung
 Beim Betrieb mit hoher Leistung steht die Wirtschaftlichkeit in hohem Masse auf dem Spiel. Die berechneten Kriterien massen dieses Risiko nicht. Es ist absolut möglich, dass der Betrieb mit hoher Leistung ausfällt, obschon die Verbraucher Nr. 1, 6 und 3 mit Strom versorgt werden.

Mit dem neuen Netz ist es 4mal weniger wahrscheinlich, dass der Betrieb mit hoher Leistung ausfällt. Die Verbesserung ist weniger ausgeprägt als für die übrigen berechneten Kriterien, da sich die diesbezüglich wichtigsten Ausfälle auf der MS-Ebene ereignen, die nicht geändert wurde.

□ Optimale Häufigkeit der vorbeugenden Wartung
 Die sich aus den Kalkülen ergebende Kurve (siehe Abb. 25) zeigt die Auswirkungen der Häufigkeit der

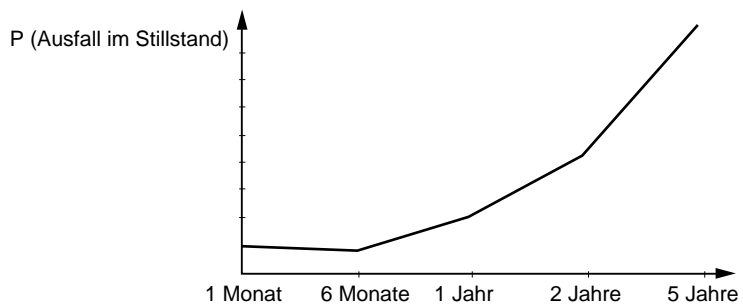


Abb. 25: Nichtverfügbarkeit im Stillstand eines Notstromaggregates in Funktion der Wartungshäufigkeit.

vorbeugenden Wartung der Notstromaggregate auf die Wahrscheinlichkeit, dass sie bei einem Bedarf verfügbar sind. Für eine Wartungshäufigkeit von 6 Monaten hat die Kurve für die Wahrscheinlichkeit der Nichtverfügbarkeit im Stillstand ein Minimum.
 □ Beitrag des MS-Teils und des NS-Teils zu den befürchteten Ereignissen beim vorgeschlagenen Netz

Der MS-Teil leistet einen wesentlich grösseren Beitrag als der NS-Teil (etwa 99,9% gegenüber 0,1%). Da das MS-Netz nicht geändert wurde, muss seine vorbeugende Wartung optimiert werden. Zudem ist es äusserst wünschenswert, für das MS-Netz über eine gute Leittechnik zu verfügen.

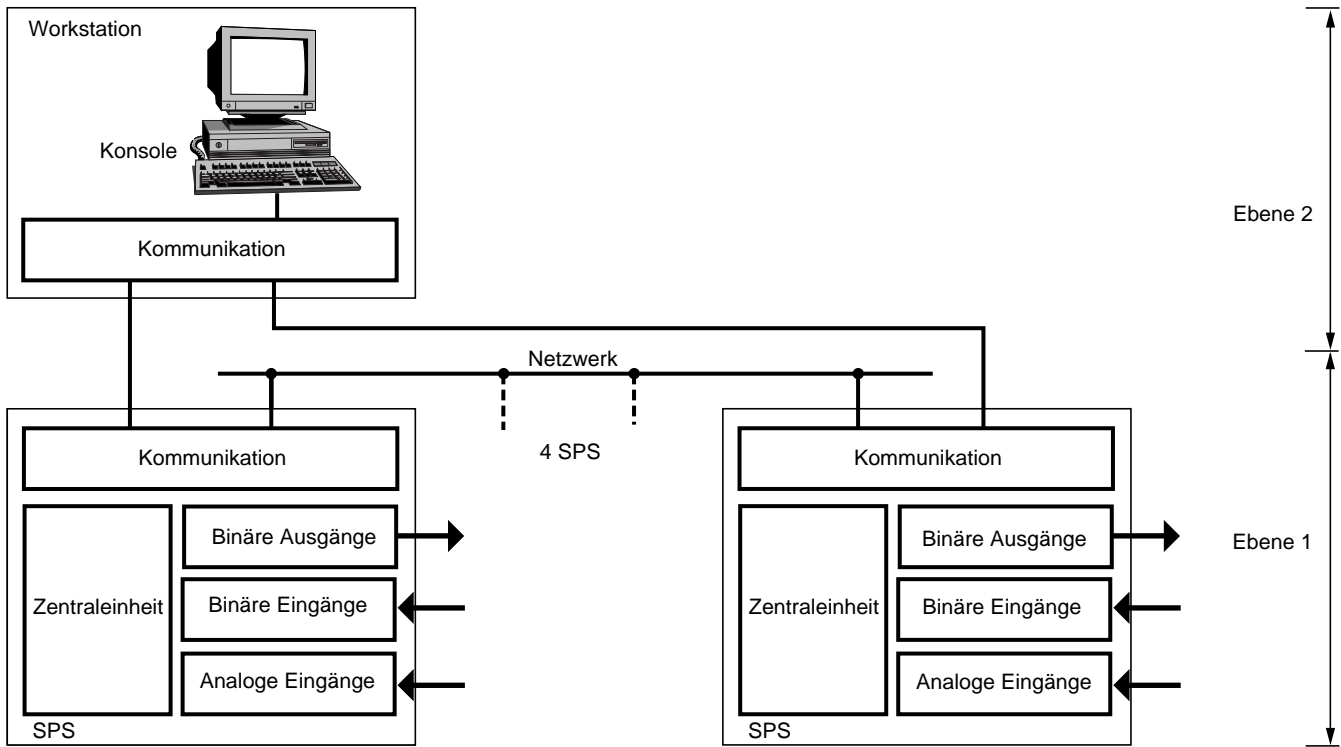


Abb. 26: Basis-Architektur der Leittechnik einer Höchstspannungsanlage.

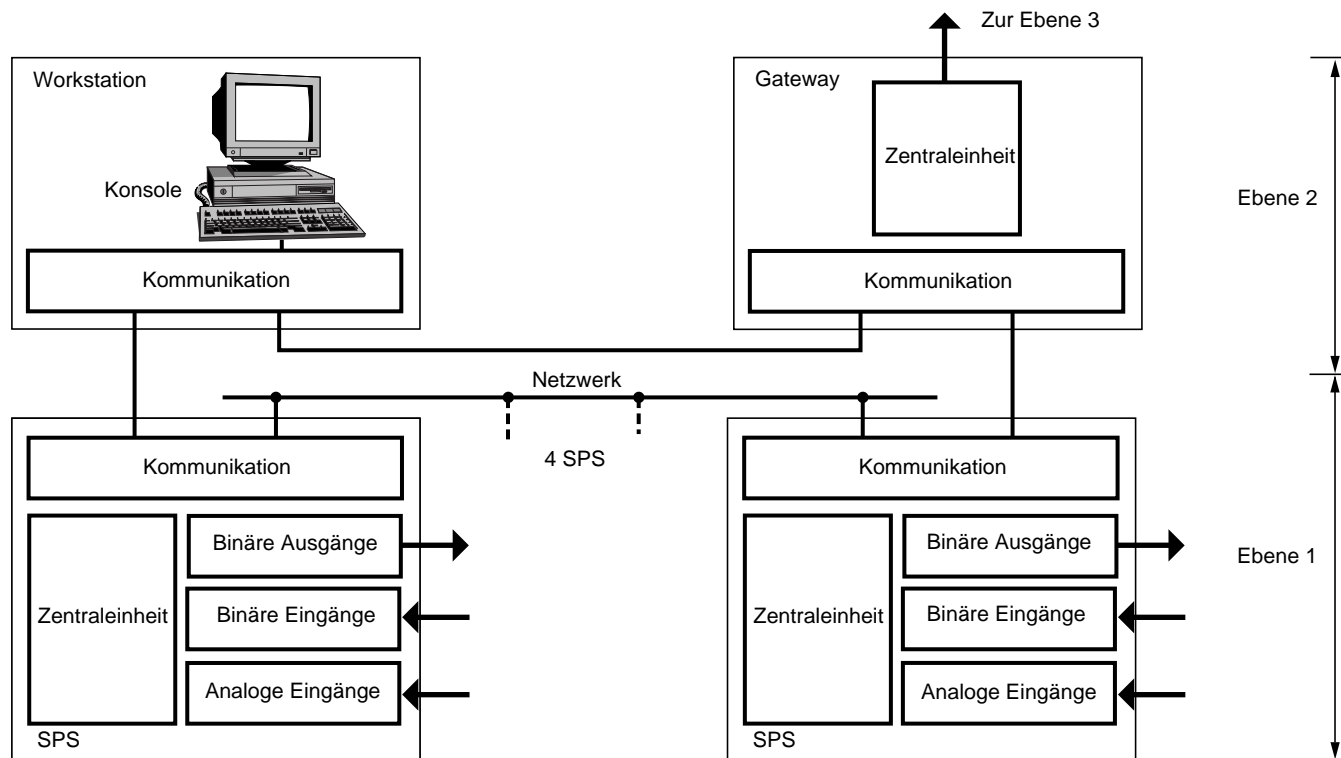


Abb. 27: Architektur der Leittechnik der Höchstspannungsanlage mit Gateway und Workstation.

Vorteil einer abgesetzten Leittechnik-Station für eine Höchstspannungsanlage

■ Bedarfs- und Bedürfnisanalyse

Im Rahmen der Offerten für die Leittechnik für eine Höchstspannungsanlage im Ausland führte Schneider Sicherheits-Vorstudien durch. Die folgende Vorstudie sollte ermitteln, welche Architektur es ermöglichte, die vom Kunden festgelegten Betriebssicherheitsziele in bezug auf den Verlust der Leittechnik zu erreichen. Es musste festgestellt werden, ob es notwendig sei, eine redundante abgesetzte Workstation zu vorzusehen.

■ Funktionsanalyse

Die Leittechnik dieser Höchstspannungsanlage umfasst:

- Vier speicherprogrammierbare Steuerungen (SPS), welche die Erfassung der Zustände der elektrischen Betriebsmittel der Schaltanlage und die Restitution der Befehle durchführen (Ebene 1).
 - Eine Workstation, an welcher der Zustand der Schaltanlage visualisiert werden kann und mit der Befehle übermittelt werden können (Ebene 2).
 - Eventuell eine abgesetzte Workstation. Die abgesetzte Workstation ist somit im Verhältnis zur Workstation der Schaltanlage redundant.
- Die Abbildung 26 zeigt die Basis-Lösung, die einer einzigen Workstation auf der Ebene 2 entspricht. Die Abbildung 27 zeigt die Lösung mit Gateway zu einer abgesetzten Workstation.

■ Analyse der Resultate

Die gewählte Leittechnik muss eine Nichtverfügbarkeitswahrscheinlichkeit von weniger als 10^{-4} bei $t = 1200$ Stunden haben. Dies entspricht einer Nichtverfügbarkeitsdauer des Systems von weniger als 7 Minuten nach 1200 Betriebsstunden (50 Tagen). Das befürchtete Ereignis – Ausfall der Leittechnik – wurde in drei befürchtete Ereignisse aufgeteilt, die

- der Wahrscheinlichkeit des vollständigen Ausfalls der Leittechnik (systematischer Ausfall),
- der Wahrscheinlichkeit des Verlustes mindestens einer binären Information,
- der Wahrscheinlichkeit des Verlustes mindestens einer analogen Information entsprechen, was drei Kalküle pro Architektur bedeutet.

	MDT der Betriebsmittel vom Typ n	MDT der Betriebsmittel vom Typ s
Hypothese 1	1 Stunde	3 Stunden
Hypothese 2	4 Stunden	12 Stunden

Abb. 28: Zwei Hypothesen für die mittleren Reparaturzeiten.

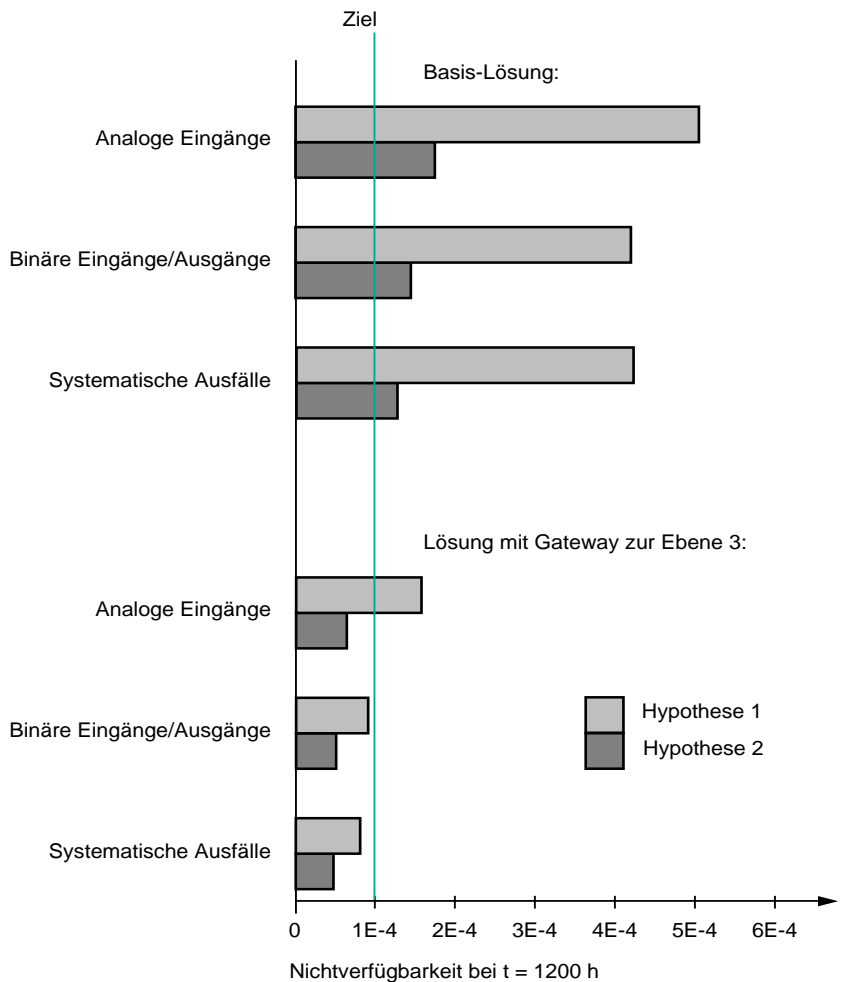


Abb. 29: Balkendiagramm der Nichtverfügbarkeiten für die beiden Lösungen (die orangefarbene Linie entspricht dem zu erreichenden Ziel, das erreicht wird, wenn der Balken links von der Linie bleibt).

Die Betriebsmittel wurden in zwei Klassen aufgeteilt:

- Betriebsmittel, für die Ersatzteilsätze vorhanden sind (n).
 - Betriebsmittel, für die keine Ersatzteilsätze vorhanden sind (s).
- Pro befürchtetes Ereignis wurden zwei Kalküle durchgeführt, um die Auswirkungen der Wahl der mittleren Reparaturzeiten auf das Endresultat zu zeigen (siehe Abb. 28).

Die Hypothese 2 ist die realistischere. Diese Zeiten wurden für die Wahl

zwischen den beiden Lösungen verwendet.

Die Abbildung 29 zeigt folgendes:

- Die Lösung ohne abgesetzte Workstation ermöglicht es nicht, die gewünschte Verfügbarkeit zu erhalten.
- Die Lösung mit abgesetzter Leittechnik ermöglicht es, das Ziel für die binären Eingänge und die systematischen Ausfälle zu erreichen. Die Wahrscheinlichkeit, mindestens ein analoges Eingangssignal zu verlieren, ist hingegen höher als gewünscht.

4. Die Hilfsmittel auf dem Gebiet der Betriebssicherheit

Tools für die Störungsanalyse

Gewisse Tools erzeugen aufgrund der Betriebsanalyse des Systems und den Ausfallarten der Komponenten automatisch eine Störungsanalyse. Dabei wird ein Modell erzeugt, das die Bewertung der Betriebssicherheitskriterien ermöglicht. Diese Tools sind für komplexe und/oder sich wiederholende Systeme nützlich. Sie gestatten die Erstellung einer Datenbank über die Ausfallarten der Komponenten und über die Auswirkungen dieser Ausfälle, wenn dies möglich ist (siehe Abb. 30).

Modellierungs-Tools

Es gibt zwei Arten von Tools (siehe Abb. 31):

- Simulations-Tools
- Tools für den analytischen Kalkül

Anmerkung: Ein Markov-Graph kann sehr einfach in ein Petri-Netz umgewandelt werden und den Gegenstand einer Simulation bilden. Umgekehrt kann mit jedem Petri-Netz ein Graph verbunden werden, man muss jedoch die Transitionen «markovisieren», denn in einem Markov-Graph sind die Durchlaufhäufigkeiten der Transitionen gezwungenermaßen konstant. Schneider verfügt gegenwärtig über eine grafische Benutzeroberfläche mit der Bezeichnung PCDM, die automatisch die Definitionsdatei des Markov-Graphs oder des gezeichneten Petri-Netzes erzeugt (siehe Abb. 32). Dies bewirkt einen Zeitgewinn und erhöhte die Zuverlässigkeit der Datenerfassung. Die Verwendung von Petri-Netzen ist heute das Modellierungsverfahren, das dem effektiven Verhalten eines Systems am nächsten kommt. Die Beschleunigung der Simulation von Petri-Netzen, insbesondere mit Hilfe der Software MOCA-RP, war das Thema einer Dissertation, deren erste Resultate an der ESREL '96 (European Safety and Reliability Conference) vorgestellt worden sind. In nächster Zukunft wird die Anwendung von Petri-Netzen nicht mehr durch die Simulationsdauer begrenzt sein.

Name des Tools	Modellierungsverfahren	Lösungsverfahren für den Kalkül	Haupteigenschaften
Adélia	Fehlerbaum	<ul style="list-style-type: none"> ■ analytisch ■ Simulation 	Von Schneider Electric entwickeltes Tool zum Modellieren der Störungen der Komponenten von elektrischen Netzen. Es enthält eine Datenbank über die Störungen der elektrischen Netze. Die Beschreibung des Netzes und des befürchteten Ereignisses bewirkt die automatische Erzeugung des entsprechenden Fehlerbaums.
Sofia	Fehlerbaum	<ul style="list-style-type: none"> ■ analytisch logisches Polynom 	Von SGTE Sofreten entwickelt. Automatische Erzeugung eines Fehlerbaums und der damit verbundenen FMEA durch die Funktionsbeschreibung des Systems und Erzeugung einer damit verbundenen Störungsdatenbank.

Abb. 30: Zwei normalerweise von Schneider verwendete Arten von Hilfsmitteln für die Störungsanalyse.

Modellierungsart	Simulations-Tool	Tool für den analytischen Kalkül
Markov-Graph		supercab entwickelt von ELF AQUITAINE
Petri-Netz	MOCA-RP entwickelt von Microcab	

Abb. 31: Modellierungs-Tools.

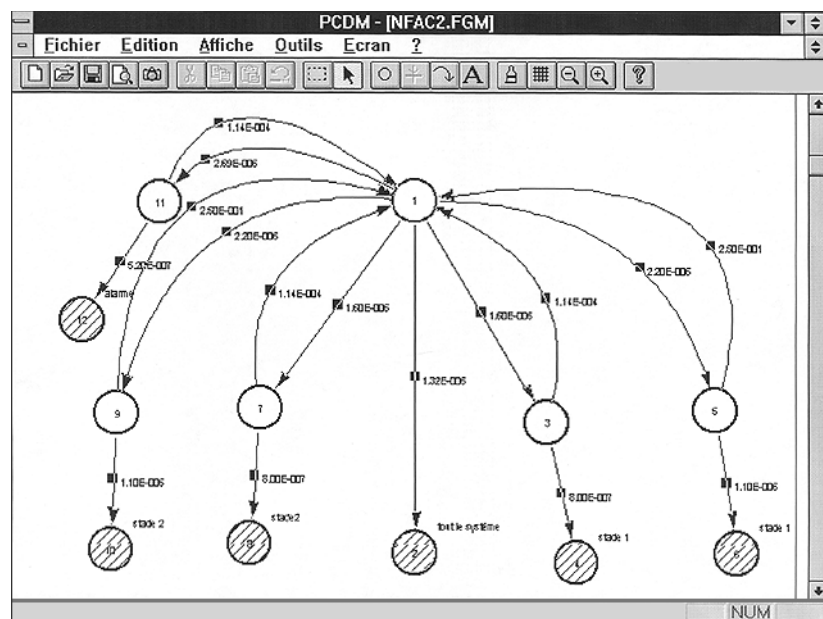


Abb. 32: Grafische Benutzeroberfläche PCDM mit Markov-Graph.

5. Schlussfolgerung

Der Begriff Betriebssicherheit zerfällt in:

- Sicherheit (von Personen),
- Zuverlässigkeit,
- Verfügbarkeit,
- Wartbarkeit.

Die Sicherheitsforderungen haben zuerst Betriebssicherheitsstudien für risikobehaftete Anwendungen verlangt: Bahn- und Lufttransporte, Kernkraftwerke usw. Wenn man die Forderungen der Zuverlässigkeit, Verfügbarkeit und Wartbarkeit hinzufügt, werden zahlreiche weitere Gebiete betroffen.

Die Anforderungen in bezug auf die Qualität der Stromversorgung sind gestiegen. In Anbetracht der bedeutenden Verbesserung der Methoden und Betriebsmittel, haben die Anwender heute das Recht, ein hohes Verfügbarkeitsniveau zu erwarten. Um dieses Ziel mit einem begründeten Vertrauen zu erreichen, sind Betriebssicherheitsstudien erforderlich.

Sie gestatten eine Optimierung

- der Architektur des elektrischen Netzes,

- des Leittechnik-Systems

- der Wartungspolitik.

Sie ermöglichen die Wahl der Lösungen, die geeignet sind, das gewünschte Verfügbarkeitsniveau mit minimalen Kosten zu erreichen. Die Studie kann sich oft auf einen Hauptfaktor der Anlage beschränken, auf dem den grössten Teil der Gesamt-Nichtverfügbarkeit beruht.

In zahlreichen Fällen ist es von Interesse, einen Spezialisten beizuziehen. Sein Rat kann ausschlaggebend sein.

Literaturverzeichnis

Normen

- IEC 50: Internationales Elektrotechnisches Wörterbuch, Kapitel 191: Betriebssicherheit und Versorgungsqualität.
- IEC 271/UTE C20310: Liste der Grundbegriffe, Definitionen und mathematischen Begriffe für die Zuverlässigkeit.
- IEC 300: Lenkung der Betriebssicherheit – 3. Teil: Anwendungsrichtlinien – Abschnitt 1: Analyseverfahren für die Betriebssicherheit - Methodologischer Leitfaden.
- IEC 395/UTE C20321 bis 20327: Prüfung der Zuverlässigkeit von Betriebsmitteln.
- IEC 362/UTE C20313: Richtlinien für die Erfassung von Zuverlässigkeits-, Verfügbarkeits- und Wartbarkeitsdaten aufgrund von Betriebsresultaten von elektronischen Einrichtungen.
- IEC 671: Periodische Kontrollen und Überwachung des Schutzsystems von Kernreaktoren.
- IEC 706/X 60310 und 60312: Richtlinien für die Wartbarkeit von Betriebsmitteln.
- IEC 812/X 60510: Analyseverfahren für die Zuverlässigkeit von Systemen. Verfahren der Fehlermöglichkeits- und einflussanalyse (FMEA).
- IEC 863/X 60520: Vorhersage der Zuverlässigkeits-, Wartbarkeits- und Verfügbarkeitseigenschaften.
- IEC 880: Software für die in Sicherheitssystemen von Kernkraftwerken verwendeten Rechner.
- IEC 987: Sicherheitsrelevante programmierte Rechner von Kernkraftwerken.
- IEC 1165: Anwendung der Markov-Verfahren.

- IEC 1226: Kernkraftwerk – Sicherheitsrelevantes Instrumentierungs- und Leittechnik-System – Klassifizierung.
- NF C 71-011: Betriebssicherheit von Software – Allgemeines.
- NF C 71-012: Betriebssicherheit von Software – Anforderungen an die Software.
- NF C 71-013: Betriebssicherheit von Software – Geeignete Sicherheitsanalyseverfahren.

Diverse Veröffentlichungen

[1] «Zuverlässigkeit von Systemen»

A. Pagès und M. Gondran
Eyrolles 1983

[2] «Betriebssicherheit industrieller Systeme»

A. Villemeur
Eyrolles 1988

[3] Sammlungen von Zuverlässigkeitsdaten:

- Military Handbook 217 F
Department of Defense (USA)

- Sammlung von Zuverlässigkeitsdaten des CNET (Centre National d'Etudes des Télécommunications). 1993

- IEEE 493 und 500 (Institute of Electrical and Electronics Engineers) 1980 und 1984

- IEEE Richtlinien für die Sammlung und Darstellung von Zuverlässigkeitsdaten von elektronischen Sensor-komponenten und mechanischen Ausrüstungen für Kernkraftwerke.

- Dokument NPRD91 (Nonelectronics Parts Reliability Data) des Reliability Analysis Center (Department of Defense, USA) 1991

[4] Empfehlungen

- MIL-STD 882 B
- MIL-STD 1623

Technische Hefte Merlin Gerin

- Entwicklungsmethode für eine Betriebssicherheits-Software, Technisches Heft Nr. 117 – A. Jourdil und R. Galera, 1982
- Einführung in das Sicherheitskonzept, Technisches Heft Nr. 144 – P. Bonnefoi
- Sicherheit und Elektrizitätsverteilung, Technisches Heft Nr. 148 – G. Gatine, 1989
- Betriebssicherheit von NS-Verteilern, Technisches Heft Nr. 156 – O. Bouju
- Automatische Umschaltung der Einspeisungen von MS- und NS-Netzen, Technisches Heft Nr. 161 – G. Thomasset
- Energieselektivität in Niederspannungsnetzen, Technisches Heft Nr. 167 – R. Morel, M. Serpinet
- Betriebssicherheit von MS- und HS-Schutzeinrichtungen, Technisches Heft Nr. 175 – M. Lemaire

Beteiligung von Schneider Electric an verschiedenen Arbeitsgruppen

- Statistik-Gruppe des Komitees 56 (Zuverlässigkeitsnormen) der IEC.
- Software-Sicherheit in der europäischen Gruppe des EWICS – TC7: Computer und kritische Anwendungen.
- Arbeitsgruppe der AFCET über die Betriebssicherheit von Informatik-Systemen.
- Beteiligung an der Aktualisierung der Sammlung von Zuverlässigkeitsdaten des CNET.
- IFIP-Arbeitsgruppe 10.4 – Zuverlässiges Computing.

Schneider Electric

Hauptverwaltung Deutschland:

Schneider Electric GmbH
Gothaer Strasse 29 • D-40880 Ratingen
Postfach 10 12 61 • D-40832 Ratingen
Telefon (0 21 02) 4 04-0
Telefax (0 21 02) 4 04 92 56

Hauptverwaltung Schweiz:

Schneider Electric (Schweiz) AG
Schermenwaldstrasse 11
Postfach • CH-3063 Ittigen
Telefon (031) 917 33 33
Telefax (031) 917 33 55