DuEPublico
Duisburg-Essen Publications online

Der folgende Text wird über DuEPublico, den Dokumenten- und Publikationsserver der Universität Duisburg-Essen, zur Verfügung gestellt.

Diese auf DuEPublico veröffentlichte Version der E-Publikation kann von einer eventuell ebenfalls veröffentlichten Verlagsversion abweichen.

Kochs, Hans-Dieter:

Ermittlung der Zuverlässigkeit/Verfügbarkeit industrieller Systeme

DOI: http://dx.doi.org/10.17185/duepublico/44357

URN: urn:nbn:de:hbz:464-20170825-133830-0

Link: http://duepublico.uni-duisburg-essen.de/servlets/DocumentServlet?id=44357

Fortschritt-Berichte VDI

VDI

Reihe 21

Elektrotechnik

Univ.-Prof. Dr.-Ing. Hans-Dieter Kochs,
Düsseldorf

Nr. 403

Ermittlung der Zuverlässigkeit/Verfügbarkeit industrieller Systeme

Anwendung auf ein Prozessleitsystem

Univ.-Prof. Dr.-Ing. Hans-Dieter Kochs
Fakultät für Ingenieurwissenschaften
Technische Informatik (*Ti*), Informationslogistik *(iL*)
Universität Duisburg-Essen

Ermittlung der Zuverlässigkeit/Verfügbarkeit industrieller Systeme

Anwendung auf ein Prozessleitsystem

Zuverlässigkeit - Verfügbarkeit - Zuverlässigkeitsmodelle - Zuverlässigkeitsanalyse - Minimalschnittverfahren - Markov Prozesse - Markov Minimalschnittverfahren - Leitsystem - Automatisierungssystem

2. korrigierte Auflage 2017 (Open Access Publikation)

Kochs, Hans-Dieter

Ermittlung der Zuverlässigkeit/Verfügbarkeit industrieller Systeme Anwendung auf ein Prozessleitsystem

Fortschr.-Ber. VDI Reihe 21 Nr. 403. Düsseldorf: VDI Verlag 2012.
100 Seiten, 49 Bilder, 16 Tabellen.
ISBN 978-3-18-340321-9, ISSN 0178-9481,
€ 37,00 / VDI-Mitgliederpreis € 33,30.

Bibliographische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet abrufbar unter http://dnb.ddb.de.

Bibliographic information published by the Deutsche Bibliothek

(German National Library)
The Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie (German National Bibliography); detailed bibliographic data is available via Internet at http://dnb.ddb.de.

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe (Fotokopie, Mikrokopie, der Speicherung in Datenverarbeitungsanlagen, im Internet und das der Übersetzung) vorbehalten.

Als Manuskript gedruckt. Printed in Germany.

ISSN 0178-9481

ISBN 978-3-18-340321-9

2. korrigierte Auflage 2017

Kurzfassung

Dieser Bericht beschreibt das Ergebnis einer umfassenden Studie zum Nachweis der Zuverlässigkeit bzw. Verfügbarkeit eines industriellen Leitsystems zur Überwachung, Steuerung und Regelung eines verfahrenstechnischen Prozesses. Ziel der Studie ist es, beispielhaft aufzuzeigen, welche Schritte notwendig sind, um z.B. in den Phasen der Entwicklung frühzeitig Zuverlässigkeitsaussagen zu ermitteln und um vertrags- und rechtsrelevante Zuverlässigkeitsaussagen eines Produktes zu erhalten. Neu ist der Einsatz der Modellierungstechnik und der theoretischen Verfahren sowie deren Kombination auf Basis der Booleschen Logik an einem aktuellen industriellen System. Möglichkeiten und Grenzen der Aussagefähigkeit werden aufgezeigt. Sämtliche Schritte der Zuverlässigkeitsanalyse von den Eingangsgrößen bis zu den Ausgangsgrößen werden an dem konkreten Leitsystem nachvollziehbar beschrieben. Die Vorgehensweise lässt sich sinngemäß auf andere komplexe Systemstrukturen übertragen.

Ausgehend von der umfassenden Systemanalyse (Abbildung 1, Schritt 1) werden in den Schritten 2 bis 5 die Definitionen und Festlegungen beschrieben, dazu gehören die Definition der zuverlässigkeitstheoretisch zu bewertenden Systemfunktionen (Systemzustände), die Festlegung der Voraussetzungen, die Festlegung von Komponenten und System, die Definition der Eingangskenngrößen und die Festlegung der Eingangsdaten. Für die Zuverlässigkeitsanalyse standen umfangreiche aktuelle Zuverlässigkeitsdaten, Komponenten- und Systemspezifikationen sowie Experten-Know-How zur Verfügung. Zur Zuverlässigkeits-/Verfügbarkeitsmodellierung und -berechnung in den Schritten 6 und 7 werden leistungsfähige Methoden und Verfahren eingesetzt wie z.B. das *Minimalschnittverfahren* mit *eingebetteten Markov Modellen (Markov Minimalschnittverfahren)* und *Fehlerbäumen*, die durch Erfahrungswissen ergänzt werden. Zur Transparenz und Nachvollziehbarkeit werden analytische Verfahren bevorzugt. Ein wichtiger Aspekt bei einer Zuverlässigkeitsanalyse ist nicht nur die Ermittlung von Systemkenngrößen, sondern ebenso die Ermittlung von Kenngrößen einzelner Subsysteme, um Schwachstellen aufzudecken (Sensitivitätsanalyse).

Eine 10-seitige englische Kurzfassung des Reports mit allen Ergebnissen ist unter ***Executive Summary*** ab Seite 76 zu finden.

Danksagung

Der Autor dankt besonders

- ABB für die Bereitstellung und Erläuterung von Komponenten- und Systemspezifikationen für ein spezielles System, Dokumenten und Daten sowie

- Herrn Frank Baldauf, Beratung Industrial IT (www.industrial-it.biz), Eschborn und Berlin, für die fachkundige Beratung und Diskussion der technischen Spezifikationen, besonders zu den Kapiteln 1 bis 5.

Inhaltsverzeichnis

Formelzeichen und Abkürzungen

A	Ausfallzustand
A_S	Systemausfallzustand
ANP	Anlagen Netzwerk (primary)
ANS	Anlagen Netzwerk (secondary)
B	Betriebszustand (ausfallfreier Zustand)
B_S	Systembetriebszustand
BS	Bediensystem
CCF	Common Cause Failure, der einen Common Cause Ausfall verursacht
ES	Engineering System
H, H(.)	mittlere Häufigkeit (eines Zustands)
MS	Minimalschnitt
MTTF	Mean Time to Failure
MTTSF	Mean Time to System Failure
MTTR	Mean Time to Repair
MTTSR	Mean Time to System Repair
MZ	Markov Zustand
P, P(.)	Wahrscheinlichkeit (eines Zustands)
PNP	Prozess Netzwerk (primary)
PNS	Prozess Netzwerk (sekundary)
R	Reservezustand
roon	r-out-of-n
SPoF	Single Point of Failure
T, T(.)	mittlere Dauer (eines Zustands)

λ	Ausfallrate
μ	Instandsetzungsrate
p_c	Wahrscheinlichkeit eines CCF

Firmenspezifische und allgemein bekannte Abkürzungen, z.B. TCP/IP, sind hier nicht aufgeführt. Sie sind für die Nachvollziehbarkeit der Zuverlässigkeitsanalyse entweder nicht notwendig oder ergeben sich aus dem Kontext der Beschreibung.

Expertise

Einführung und Definitionen

Zur Berechnung der Zuverlässigkeit/Verfügbarkeit des Prozessleitsystems im **Übersichtsschema Leittechnik** (Anhang A) wird eine Zuverlässigkeitsanalyse nach **Abbildung 1** durchgeführt. Es werden technisch und wissenschaftlich etablierte und in der industriellen Praxis bewährte Methoden und Verfahren eingesetzt, z.B. [Endrenyi 1979, Kochs 1984, Billinton et al.1992, Kochs SFB 2001] und auf Basis der Booleschen Logik kombiniert. Weiterhin fließen Erfahrungswissen und aktuelle Daten in die Anlayse ein. Die Schritte 1 bis 9 werden in den folgenden (gleichnummerierten) Kapiteln auf das Prozessleitsystem angewandt und beschrieben.

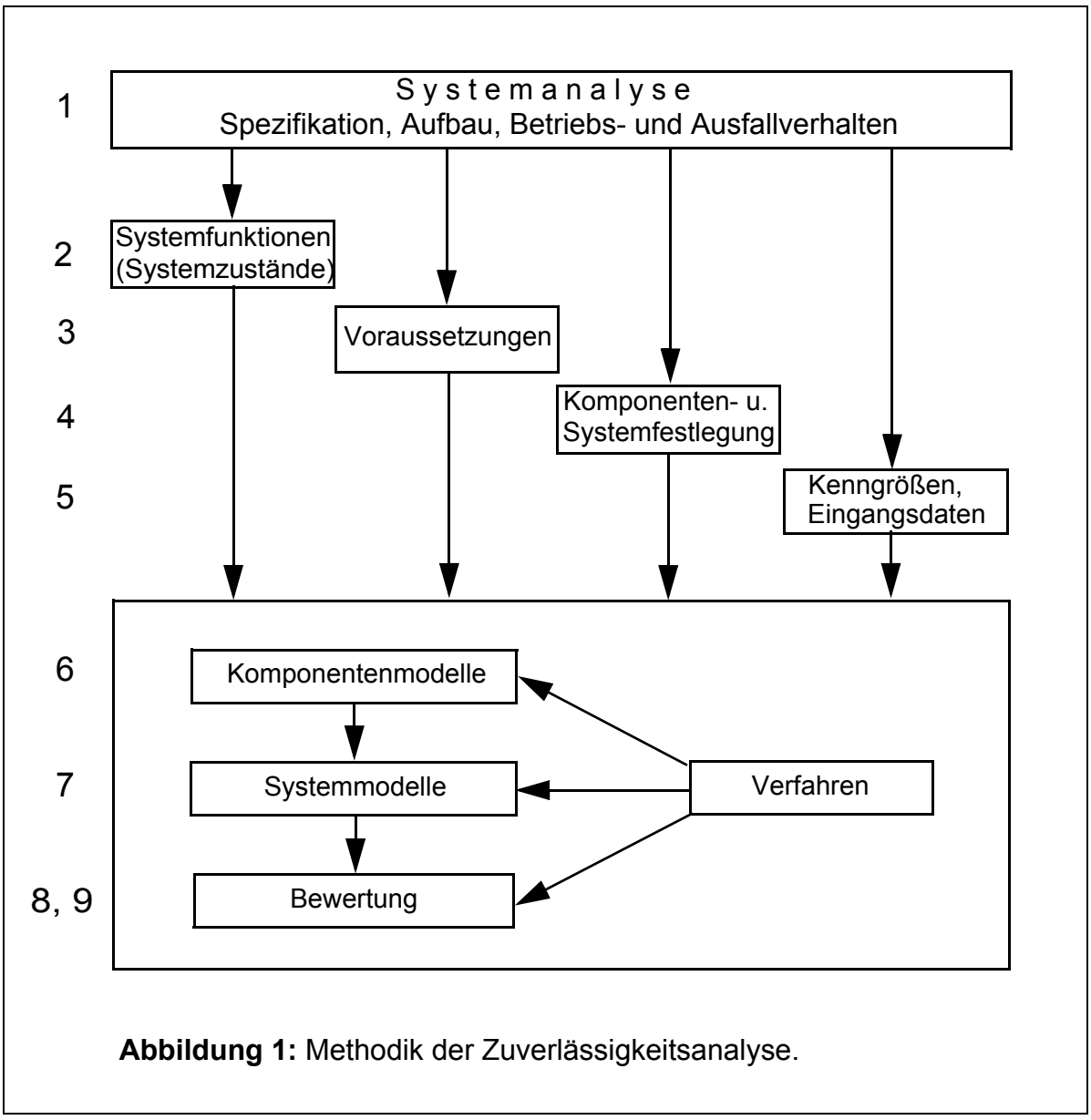


Abbildung 1: Methodik der Zuverlässigkeitsanalyse.

In [DKE-IEV 191-02-03 2012] ist die Zuverlässigkeit allgemein wie folgt definiert.

> **Zuverlässigkeit ist ein zusammenfassender Ausdruck** zur Beschreibung der Verfügbarkeit und ihrer Einflussfaktoren Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft.

Anmerkung 1: Instandhaltung umfasst Instandsetzung oder Austausch, Wartung und Inspektion.

Anmerkung 2: Zuverlässigkeit wird nach dieser Definition entsprechend den Anmerkungen in DKE-IEV 191-02-03 nur für allgemeine Beschreibungen in nichtquantitativem Sinne benutzt.

In [IEEE 90 1990] (sinngemäß) und in [DKE-IEV 603-05-01 2012] ist der Begriff Zuverlässigkeit präzisiert.

> **Zuverlässigkeit** ist die Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion unter vorgegebenen Bedingungen während eines festgelegten Zeitintervalls zu erfüllen.

Anmerkung 1: Eine Betrachtungseinheit kann entweder eine Komponente oder ein System sein (Schritt 4 in Abbildung 1, Kapitel 4).

Anmerkung 2: Die Fähigkeit einer Betrachtungseinheit wird durch Zuverlässigkeitskenngrößen ausgedrückt.

Andere Definitionen in Normen (VDI->DIN->EN->ISO->IEC->IEV) sind weitgehend inhaltsgleich. Beispielsweise ist in der älteren Definition [DIN 40041 1990] die Zuverlässigkeit wie folgt definiert.

> Die **Zuverlässigkeit** ist die Fähigkeit einer Betrachtungseinheit, innerhalb der vorgegebenen Grenzen denjenigen durch den Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten ihrer Eigenschaften während einer gegebenen Zeitdauer gestellt sind.

Der allgemeine Begriff Zuverlässigkeit wird nach [DKE-IEV 191-02-03 2012] als Oberbegriff aufgefasst, der ebenfalls den Begriff Verfügbarkeit umfasst. Die Konkretisierung des Begriffs Verfügbarkeit kommt u.a. in der Norm [DKE-IEV 191-02-05 2012] zum Ausdruck.

> Die **Verfügbarkeit** ist die Fähigkeit einer Einheit, zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls eine geforderte Funktion un-

> ter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die erforderlichen äußeren Hilfsmittel bereitgestellt sind.

Nach dieser Definition umfasst der Begriff Verfügbarkeit Zuverlässigkeitanforderungen (siehe DKE-IEV 191-02-05, “NOTE 1: This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance“). In dieser Studie werden ausschließlich reparierbare Komponenten mit stochastisch (außerplanmäßigen) auftretenden Ausfällen und Instandsetzungen betrachtet, weshalb die Definitionen und ebenfalls die Modellierungs- und Berechnungsgrundlagen für Zuverlässigkeit *und* Verfügbarkeit gleich sind. Wartungsleistungen sind nicht Gegenstand dieser Zuverlässigkeitsanalyse. Sie werden zu den äußeren Hilfsmitteln gezählt. Es gelten die bei der präzisierten Zuverlässigkeit (siehe vorherige Seite) gemachten Anmerkungen 1 und 2.

Unter äußere Hilfsmittel werden solche verstanden, die außerhalb der Grenzen der definierten Betrachtungseinheiten Komponente und System liegen (Schritt 4 in Abbildung 1), aber trotzdem für die Funktionsfähigkeit notwendig sind. Diese können z.B. Stromversorgung, Filter- und Lüftungsanlagen, Ersatzteillager, Wartungsleistungen, usw. sein (die z.B. von Zulieferfirmen stammen).

Es soll noch der in [DKE-IEV 603-05-04 2012] allgemeiner gefasste Begriff Verfügbarkeit erwähnt werden.

> Mit **Verfügbarkeit** wird der Zustand einer Betrachtungseinheit bezeichnet, in welchem diese die geforderte Funktion erfüllen kann.

Im englischsprachigen Raum hat sich für den Oberbegriff Zuverlässigkeit, der auch Verfügbarkeit umfasst, der Begriff **Dependability** [Laprie 1991, Laprie 1995, Avizienis et al. 2000, Kochs et al. 2004, DKE-IEV 191-02-03 2012] durchgesetzt.

Angemerkt sei, dass für aussagefähige Zuverlässigkeits-/Verfügbarkeitsangaben nicht nur die Wahrscheinlichkeit, sondern weitere Kenngrößen wie mittlere Häufigkeit und mittlere Dauer von Zuständen wichtig sein können. Anstelle des Begriffs Wahrscheinlichkeit wäre der Begriff wahrscheinlichkeitstheoretische Kenngrößen passgenauer.

Fazit: Diesen Definitionen sind folgende wesentliche Punkte gemeinsam.

- Die **Zuverlässigkeit und die Verfügbarkeit** einer Einheit (Betrachtungseinheit) bezieht sich immer auf deren geforderte Funktionen. Diese werden entweder erfüllt oder nicht erfüllt (binäre Aussage). Für jede zuverlässigkeitstheoretisch zu bewertende geforderte Funktion wird ein Systemzustandspaar definiert (Schritt 2 in Abbildung 1, beschrieben in Kapitel 2).

- Für die Zuverlässigkeit müssen immer die Voraussetzungen (Annahmen, Bedingungen, Grenzen) vorgegeben werden (Schritt 3 in Abbildung 1, Kapitel 3).
- Die Einheit bzw. Betrachtungseinheit kann sowohl eine Komponente als auch ein System darstellen (Schritt 4 in Abbildung 1, Kapitel 4), für die Zuverlässigkeitskenngrößen definiert werden (Schritt 5 in Abbildung 1, Kapitel 5).
- Die gegebene Zeitdauer (Zeitintervall) ist in der Regel der Bereich des stationären Zustands (keine Kinderkrankheiten und keine Verschleißausfälle, konstante Ausfallraten).

Die zu berücksichtigenden Funktionen sind in dieser Anwendung Überwachungs-, Steuerungs- und Regelungsfunktionen des Prozessleitsystems, in anderen Systemen, z.B. [Kochs SFB 2001], sind es entsprechend andere Funktionen. Es gibt keine von Funktionen unabhängige Zuverlässigkeit/Verfügbarkeit des physikalischen bzw. technischen Systems selbst (also des Übersichtsschemas Leittechnik), wenn man von einer reinen Part-Count-Berechnung, wie bei elektronischen Baugruppen üblich, absieht. Deshalb wird nach der Systemanalyse im Kapitel 2 zuerst die zu berechnende Systemfunktion definiert.

1 Systemanalyse

Das Prozessleitsystem (**Übersichtsschema Leittechnik, Anhang A**) zur Überwachung, Steuerung und Regelung der verfahrenstechnischen Prozesse besteht aus einem Anlagennetzwerk (mit redundantem Bussystem ANP/ANS, Seite 20 bis 24) und einem Prozessnetzwerk (mit redundantem Bussystem PNP/PNS, Seite 20 bis 31). Neun Server sind am Anlagennetzwerk und teilweise am Prozessnetzwerk angeschlossen (Seite 22). Am Prozessnetzwerk sind 28 AC800M Controller zur Überwachung, Steuerung und Regelung der verfahrenstechnischen Anlagen angeschlossen (Seite 25 bis 30). Die technischen Anlagen (Seite 23) sind bis auf die Ankopplungskomponenten nicht Gegenstand der Zuverlässigkeitsanalyse. Die Überwachung und Steuerung erfolgt im Wesentlichen über die Bedienstationen (Seite 20) und im Notfall eingeschränkt über die Engineering Station 1 und 2 (Seite 21).

Von ABB wurden folgende Systemkonfiguration, Systemspezifikationen, Dokumente und Daten zur Verfügung gestellt.

- Übersichtsschema Leittechnik - Systemkonfiguration (Seite 20 bis 30) und Systemspezifikation der Controller (Seite 31) und Profibus (Seite 32).
- Systemspezifikation 800xA mit MNSiS und Kopplung MCC MNSiS mit AC800 und OPC Server.
- Ausführungsbeschreibung Automatisierungskonzept und Liste der S800 E/A Module.

- Zusammenstellung aller Controller mit Angabe der Anzahl von: IO-Cluster, CI854, OZD, MLink.
- Automation System Reliability and Availability Documents.
- Preventive Maintenance and its Influence on an Automation System Life Cycle Cost.
- Aspects on Automation System Spare Parts.

Die komplette Beschreibung des Prozessleitsystems und seiner Module würde den Rahmen dieses Berichts sprengen, sie ist zum Verständnis der Zuverlässigkeitsanalyse auch nicht notwendig. Die notwendigen Anforderungen, Definitionen, Kenngrößen, usw., sind in den folgenden Kapiteln eingearbeitet und, soweit für das Verständnis erforderlich, beschrieben. Besonders ist im Kapitel 2 festgelegt, welche Komponenten zur Erfüllung der geforderten Systemfunktion notwendig sind.

2 Definition der Systemzustände

Es wird folgende Systemfunktion (binäre Größe) definiert, deren Zuverlässigkeit/Verfügbarkeit berechnet wird (In dieser Studie wird nur eine geforderte Systemfunktion untersucht).

Systemfunktion (Systembetriebszustand) B_S: Prozessüberwachung und Prozesssteuerung und Prozessregelung dürfen nicht ausfallen.

Der **Systemausfallzustand A_S ist der Komplementärzustand zum Systembetriebszustand B_S ($A_S = \neg B_S$).**

Für den **Systembetrieb** müssen **alle 28 Controller AC800M** (Übersichtsschema Leittechnik, Anhang A, Seite 25 bis 30) funktionsfähig sein. Diese müssen **hauptsächlich über die Bedienstationen** (A0CRU10, 20, 30, 40, Seite 20) überwacht und gesteuert werden können (siehe Präzisierung in Punkt 1 und 7, Seite 6 und 7). Das bedeutet, dass der (stochastische) Ausfall mindestens eines Controllers als Systemausfall gewertet wird. Alle angeschlossenen IO-Cluster und IO-Module können dann ihre Funktion nicht mehr erfüllen. Die planmäßige Abschaltung eines Controllers für Wartungen, z.B. Aufspielen neuer Software, zählt nicht dazu.

Zur Berechnung der Zuverlässigkeit der Systemfunktion werden folgende Festlegungen getroffen.

1) Im **Bediensystem (BS)**, das aus den **Bedienstationen** (A0CRU10, 20, 30, 40) besteht, darf nicht mehr als ein Arbeitsplatz ausfallen, was einer 3-out-of 4 (3oo4) Struktur entspricht (Übersichtsschema Leittechnik, Seite 20). Dies

ist eine konservative (d.h. auf der sicheren Seite liegende) Annahme, da im Notfall der Systembetrieb auch mit 2 Bedienstationen weitergeführt werden könnte, eventuell mit Einschränkungen. (Selbst bei dieser konservativen Annahme 3oo4 ist das Bediensystem sehr zuverlässig, siehe Excel-Tabelle, Anhang V, Zeile BS, Spalte 5.) Zur Berücksichtigung der Engineering Station 1 und 2 (Seite 21) sowie des Beamers siehe Punkt 6 und 7.

2) Alle **7 Server** vom Domain-Server (A0CRQ10/20) bis zum PGIM-Archiv Server (A0CRX10/20) und der Asset-Monitor Server (A0CRP70/80) müssen voll funktionsfähig sein (Seite 22 und 23).

3) Nicht alle Komponenten im Prozessleitsystem haben die gleichen schwerwiegenden Auswirkungen wie der Ausfall eines Controllers. Dies wird im folgenden begründet.

   3.1 Der Ausfall des **NAS** (A0CRV50, Speicherung bzw. Archivierung von Prozessinformationen) hat keinen Einfluss auf die definierte Systemfunktion. Er wird nicht berücksichtigt.

   3.2 Der Ausfall des **PGIM-Anwendungs-Servers** (A0CRX30) hat im ungünstigen Fall nur Einfluss wegen fehlender Berichte, Berechnungen usw. auf die Systemfunktion. Er wird deshalb mit dem **Wichtungsfaktor 1/2** gewichtet (Wichtungsfaktoren siehe Spalte 2 der Excel-Tabelle).

   3.3 Ein Ausfall der vier **MNSiS OPC Server** (A0CRP51, 52, 53, 54, Seite 23) hat keinen Einfluss auf die Systemfunktion, da diese dann weiterhin über die Controller gewährleistet wird. Allenfalls können einige Meldungen für Trends, Statistik usw. verlorengehen, falls sie nicht nachgeführt werden können. Der Ausfall eines MNSiS OPC Servers wird deshalb mit dem **Wichtungsfaktor 1/4** konservativ gewichtet.

   Eine Alternative wäre, einen Ausfall eines MNSiS OPC Servers nicht zu berücksichtigen.

   Zur Interpretation der Wichtungsfaktoren: Ein Wichtungsfaktor von 1/4 bedeutet, dass der 4-malige Ausfall der Betrachtungseinheit das Gewicht bzw. die Schwere wie der Ausfall eines Controllers hat.

   3.4 Komponenten, die zum Systembetrieb nicht unbedingt erforderlich sind, d.h. keinen Einfluss auf die Systemfunktion haben, werden nicht berücksichtigt, siehe Liste im Anhang B.

4) Ein **IO-Cluster** kann infolge eines Common Cause Failure (CCF) oder eines Single-Point-of-Failure (SPoF) eines IO-Moduls, ausfallen. Beispiel: Der Controller A0CRC30 (Seite 26) hat 7 IO-Cluster mit im Mittel angenommenen 8 IO-Modulen pro IO-Cluster (S800). Der Ausfall eines IO-Clusters hat nicht das gleiche Gewicht wie der Ausfall eines Controllers (mit allen ange-

schlossenen IO-Cluster). Wenn ein IO-Cluster ausfällt (unterstellt, dass der AC800M weiterhin in Funktion ist), dann sind maximal die zugehörigen 8 IO-Module außer Funktion. Wenn der Controller ausfällt, wären es 7 x 8 = 56 IO-Module. Es wird deshalb der Ausfall eines IO-Clusters in diesem Beispiel mit dem Faktor 1/7 gewichtet (entspricht dem Ausfall eines IO-Clusters an jedem Controller).

Der Ausfall eines IO-Clusters, der durch andere Fehler als durch Fehler in IO-Modulen verursacht wird, ist bereits in der Ausfallrate des AC800M mit berücksichtigt.

Im Folgenden wird zwischen den Begriffen CCF und SPoF nicht unterschieden. Sie haben die gleichen Auswirkungen.

5) Der unabhängige Ausfall **einzelner IO-Module** (ohne CCF des angeschlossenen IO-Clusters) wird nicht berücksichtigt.

6) Der Ausfall der **Beamer** (Seite 20) wird nicht berücksichtigt, da deren Ausfall keinen Systemausfall verursacht. Der kritische Punkt bei Beamern dürfte die begrenzte Lampenlebensdauer von z.B. 2.000 Stunden sein. Selbst damit ist das Beamersystem bei der konservativen Annahme (2oo3) sehr zuverlässig (Berechnungsergebnis, siehe im Anhang B).

7) Für die Kombination von **Bediensystem (BS) und Engineering Station System (ES)** soll folgende Annahme gelten: Der Ausfall von BS (3oo4) führt in jedem Fall zum Systemausfall, auch wenn ein eventuell eingeschränkter Systembetrieb über ES weitergeführt werden könnte (konservative Annahme). Der Ausfall von ES (1oo2) führt nicht zum Systemausfall, wenn BS weiterhin in Betrieb ist. Dies wird durch ein spezielles Systemmodell im Anhang I berücksichtigt. Die Kombination von Bediensystem und Engineering Station System wird als **Überwachungs- und Steuerungssystem bezeichnet** (Anhang B).

8) Es wird nicht berücksichtigt, dass beim Ausfall des Bediensystems (BS) ein Weiterbetrieb mit eventuell eingeschränkter Funktion über die beiden Bedienstationen im Betriebsmeisterbüro (A0CRU80 und A0CRU90, Seite 24) möglich ist (konservative Annahme).

In der Systemfunktion ist auch implizit ein Totalausfall der Bussysteme: PNP und PNS oder ANP und ANS berücksichtigt.

Die Definition weiterer Systemzustandspaare wäre denkbar, ist aber hier nicht gefordert worden. (Hinweis: Für jedes weitere Systemzustandspaar müsste ein neues oder abgeändertes Systemmodell entwickelt werden, Kapitel 7).

In der Zuverlässigkeitsanalyse werden die Systemkenngrößen

Wahrscheinlichkeit P

Mittlere Häufigkeit H

der **Systemzustände** B_S und A_S berechnet. **P** und **H** bilden die **Basiskenngrößen** der Zuverlässigkeits-/Verfügbarkeitsrechnung. Weitere Systemkenngrößen, z.B. **mittlere Dauer T** oder **akkumulierte Ausfalldauer** über einen festgelegten Zeitraum können aus diesen Basiskenngrößen abgeleitet werden.

Neben absoluten Zuverlässigkeitszahlen des Gesamtsystems liefert die Zuverlässigkeitsanalyse auch die Sensitivität einzelner Teilsysteme oder Komponenten auf **P** und **H** des Gesamtsystems, siehe Kapitel 9.

3 Festlegung der Voraussetzungen

Der Zuverlässigkeitsermittlung liegen folgende Voraussetzungen zu Grunde.

1) Alle Komponenten werden fehlerfrei bezüglich Hardware und Software entworfen, gefertigt, getestet, eingebaut, instandgehalten (instandgesetzt und gewartet) und betrieben. Diese Annahme ist realistisch bei einer großen Stückzahl von Komponenten, die sich seit Jahren im Betrieb bewährt haben, wie z.B. der Controller AC800M. (Allenfalls geänderte Software kann vorübergehend zu Ausfällen führen (Kinderkrankheiten).)

2) Ausfälle der Komponenten werden fehlerfrei erkannt und gemeldet und sind somit sofort erkennbar.

3) Ausgefallene Komponenten werden in der Regel durch gleichwertige ersetzt. Es muss eine ausreichende Anzahl an Ersatzkomponenten vorrätig sein oder innerhalb kurzer Zeit beschafft werden können, um die festgelegte Instandsetzungsdauer (siehe Kapitel 5) einhalten zu können.

4) Die Umgebungsbedingungen wie klimatische Bedingungen (z.B. Temperatur, Feuchtigkeit), mechanische Bedingungen (z.B. Stöße, Vibrationen), elektromagnetische Bedingungen (bzw. Abschirmungen), Energieversorgung, usw., müssen dauerhaft der Spezifikation entsprechen. Besonders steigt die Ausfallrate elektronischer Bauteile mit steigender Temperatur stark an.

5) Bedienungsfehler werden nicht berücksichtigt. Bedien- und Instandsetzungspersonal müssen gut geschult und mit dem System vertraut sein.

4 Festlegung von Komponenten und System

Für die Zuverlässigkeitsermittlung werden die beiden Betrachtungseinheiten Komponente und System definiert.

- Eine **Komponente** ist definiert als die kleinste statistische Betrachtungseinheit in einem System, die nicht weiter systemtheoretisch untergliedert wird.
- Unter einem **System** wird der funktionale Zusammenhang derjenigen Komponenten verstanden, die laut Spezifikation berücksichtigt werden müssen.

In dieser Studie sind die Komponenten durch das funktionale Übersichtsschema Leittechnik (Seite 20 bis 32) weitgehend vorgegeben oder können entsprechend den zu Grunde liegenden Spezifikationen modelliert werden, z.B. die Controller AC800M (Anhang M bis P).

Das Zuverlässigkeitsblockdiagramm des Systems hängt von der im Kapitel 2 definierten Systemfunktion ab unter Berücksichtigung der in den Kapiteln 2 und 3 gemachten Annahmen bzw. Voraussetzungen. Bei mehreren Systemfunktionen muss für jede Systemfunktion ein eigenes (oder modifiziertes) Systemmodell entwickelt werden.

Aus der funktionalen Struktur des Übersichtsschemas Leittechnik wird das noch näher beschriebene Systemmodell als Zuverlässigkeitsblockdiagramm im Anhang B bis E entwickelt. Jeder Block stellt den Funktions- oder Betriebszustand einer Komponente bzw. eines Subsystems dar ($\neg$MS , Kapitel 7), die logisch UND verkettet sind.

5 Festlegung der Kenngrößen

Grundsätzlich wird für jede Komponente das zweistufige Modell im Anhang F zu Grunde gelegt, das applikationsbezogen weiterentwickelt wird, z.B. im Anhang J. Zur Ermittlung der Zuverlässigkeitskennwerte, z.B. Ausfallraten λ und Instandsetzungsraten μ, wurden von ABB umfangreiche Zuverlässigkeitsdaten und Informationen zur Verfügung gestellt. Die Zuverlässigkeitsdaten sind in der Excel Tabelle (Anhang V) zur Zuverlässigkeits-/Verfügbarkeitsberechnung aufgeführt.

In der Zuverlässigkeitsanalyse werden „Failure type 2.1“ (z.B. Einfachfehler der Komponente) und „Failure type 2.2“ (umfasst CCF und somit Systemauswirkungen) berücksichtigt (ABB Dokumente). Die Berechnung der Ausfallraten erfolgte für industrielle Umgebungsbedingungen, z.B. 20 Grad Celsius.

Die Ausfallraten der Komponenten sind nach dem Standard [MIL-HDBK-217F 1991] berechnet worden. Darin gehen z.B. alle Bauelemente einer Baugruppe ein, auch wenn diese für die spezielle Anwendung nicht benötigt werden (und somit ein Ausfall des Bauelements nicht zum Ausfall der Baugruppe im System führt). Die Berech-

nungsmethode nach MIL-HDBK-217F ist deshalb als konservativ zu betrachten. In der Praxis wird häufig beobachtet, dass die Ausfallraten oft um einen Faktor 2 bis 5 kleiner sind als die nach MIL-HDBK-217F berechneten Werte.

Speziell für den hier eingesetzten Controller AC800M (nicht redundante Ausführung) sind beispielsweise die Werte

- Predicted Failure Rate: $7{,}9 * 10^{-6}\ h^{-1}$
- Observed Failure rate: $2{,}3 * 10^{-6}\ h^{-1}$
- Faktor: **3,4 (niedrigere Ausfallrate)**

Niedrigere „Observed Failure Rate“ wurden in der Zuverlässigkeitsanalyse nicht berücksichtigt. Es wurden die höheren „Predicted Failure Rate“ bei den ABB-Daten zu Grunde gelegt (konservative Berücksichtigung).

Teilweise sind die Ausfallraten von den Firmen auf der Basis von 40 ^{o}C berechnet worden, z.B. für MLink oder MMI Control Unit. Eine Umrechnung auf die Temperaturbasis 20 ^{o}C (die niedrigere Ausfallraten ergeben würde) wurde nicht vorgenommen (konservative Berücksichtigung).

Folgende Fehler werden nicht berücksichtigt.

- Fehler in der Konstruktion (wozu auch Software gezählt wird), Fertigung, beim Einbau, bei der Instandhaltung, im Betrieb.
- Intermittierende Fehler.
- Fehlerhafte Meldung von ausgefallenen Komponenten (Über- und Unterfunktion).
- Fehler in reinen Verdrahtungseinheiten wie Patchbox (Übersichtsschema Leittechnik, Seite 32).
- Fehler in Blackbox-Komponenten (Seite 32).
- Bruch von Kabel oder Leitungen inklusive Bus.
- Fehler infolge von Umgebungsbedingungen (z.B. bezüglich Temperatur, Vibration, Schmutz), die außerhalb der Spezifikation liegen oder nicht erfasst sind.

Für die mittlere Instandsetzungs-/Ersatzdauer werden einheitlich **8 Stunden (MTTR**) angenommen. Es handelt sich um einen Referenzwert, der in Zuverlässigkeitsanalysen üblicherweise angesetzt wird, wenn keine anderen Vorgaben gemacht werden und der Wert plausibel erscheint. MTTR umfasst auch die Anreisezeit an den Ausfallort.

Für Instandsetzungs- und Hochfahrdauer der PNP/PNS- oder ANP/ANS-Bussysteme werden ebenfalls **8 Stunden** zu Grunde gelegt. (Mit dem Modell im Anhang K lassen sich auch kürzere oder längere Hochfahrdauern berücksichtigen.)

Für Instandsetzung/Austausch eines IO-Moduls werden im Mittel **2 Stunden** festgelegt (Anfahrtzeit mit berücksichtigt). In vielen Fällen kann ein defektes IO-Modul auch einfach aus dem IO-Cluster herausgezogen werden, um eine Blockade des IO-Modulbusses (infolge eines CCF des IO-Moduls) aufzuheben. Ein IO-Modul kann typischerweise in **0,5 Stunden** online ausgewechselt werden.

Eine mittlere Instandsetzungs-/Ersatzdauer bedeutet, dass die individuelle Instandsetzungs-/Ersatzdauer sowohl länger als auch kürzer sein kann. Eine mittlere Instandsetzungs-/Ersatzdauer von 8 Stunden bedeutet beispielsweise, dass in 47 % aller Fälle die Instandsetzung zwischen 4 und 16 Stunden liegt, in 13 % aller Fälle diese sogar länger als 16 Stunden ist (was z.B. am Wochenende auftreten kann). Hierbei werden exponentialverteile Instandsetzungs-/Ersatzdauern angenommen (μ = 1/MTTR), wie dies in Zuverlässigkeitsanwendungen meistens - stillschweigend - vorausgesetzt wird.

Es sei darauf hingewiesen, dass die Zuverlässigkeitskenngrößen der Komponenten nur für die zu Grunde gelegten Spezifikationen in der eingesetzten Systemumgebung gelten. Sobald Einsatzort, Aufbau und Bestückung der Komponenten, z.B. AC800M mit IO-Cluster und IO-Modulen, variieren, können die Zuverlässigkeitskenngrößen abweichen. Das gilt prinzipiell für alle eingesetzten Komponenten.

6 Komponentenmodelle und Komponentenberechnung

Die Komponenten- und Subsystemmodelle werden im Hinblick auf die Systemfunktion entwickelt und sind im Anhang F bis P mit ihren Kenngrößen beschrieben. Dabei sind Komponenten zu Makrokomponenten zusammengefasst worden.

Beispiel: Um die Komponente Controller AC800M (Seite 25 bis 30 und 31) zuverlässigkeitstheoretisch zu berechnen, wird dieser mit seinen Anschlusskomponenten als Subsystem betrachtet. Dabei ist zu beachten, dass die Zusammenfassung der Komponenten des Subsystems in der Art und Weise erfolgt, dass die daraus resultierende Zuverlässigkeit der Komponente AC800M auf der sicheren Seite liegt (konservative Modellierung und Berechnung). Besonders bei komplexen Betriebs- und Ausfallkonstellationen wird damit eine Modellierung und Berechnung überhaupt erst ermöglicht, wie im Anhang U am redundanten Controllersystem AC800M demonstriert wird. Zum Verständnis sind einige komplexe Betriebs-/Ausfallkonstellationen analysiert worden. Die daraus resultierende Zerlegung in einfache und konservative Modellstrukturen (Ziel: Serien- und Parallelstrukturen) ist im Anhang M dargestellt und im Anhang N bis P berechnet worden.

In der Komponente AC800M bestimmen die CCF (SPoF) maßgeblich die Zuverlässigkeit, siehe Anhang M bis O. Gegenüber CCF sind die unabhängigen Ausfälle redundanter Komponenten vernachlässigbar, wie die Beispielrechnung im Anhang P zeigt.

7 Systemmodelle und Systemberechnung

Die Systemmodellierung und Systemberechnung werden mit dem Verfahren der Minimalschnitte mit eingebetteten Markov Modellen (Markov(sche) Minimalschnitte) und eingebetteten Fehlerbäumen durchgeführt. Die Markov Modelle werden mit dem Verfahren der Wahrscheinlichen Markov Wege [Kochs 1984, Kochs et al. 1999, Kochs SFB 2001, Kochs et al. 2004] analytisch berechnet. Der Ursprung dieses leistungsfähigen Verfahrens geht auf die Arbeiten [Dib 1978, Nachtkamp 1979] zurück. Besonders applikationsbezogene bzw. realistische Abhängigkeiten zwischen Komponenten (z.B. CCF) können mit dem Verfahren der Markov Minimalschnitte modelliert und berechnet werden (Beispiele: Subsystemmodelle im Anhang G bis L und T).

Ausgangspunkt der Zuverlässigkeitsanalyse bildet die Ermittlung der Minimalschnitte aus der funktionalen Struktur des Prozessleitsystems im Hinblick auf die Systemfunktion.

Unter einem Minimalschnitt (MS) wird eine Kombination notwendiger und hinreichender Komponentenausfallzustände (minimale Anzahl) verstanden, die einen Systemausfall entsprechend der Definition im Kapitel 2 verursacht. In einem Minimalschnitt führt die Wiederinbetriebnahme jeder ausgefallenen Komponente zur Aufhebung des Minimalschnitts und somit wieder zum definierten Systembetrieb (Monotoniebedingungen werden als erfüllt vorausgesetzt) [Singh et al. 1977]. Die Kenntnis aller Minimalschnitte eines Systems und deren logische ODER-Verknüpfung (Gleichung 1) beschreibt vollständig das Ausfallverhalten des Systems (immer bezogen auf den definierten Systemzustand).

In einem System können Minimalschnitte 1. Ordnung (Ausfall einer Komponente), 2. Ordnung (Ausfall zweier Komponenten) und beliebig hoher Ordnung auftreten. Die Ermittlung aller Minimalschnitte ist bei großen Systemen oft sehr aufwändig und meistens nicht vollständig möglich. Bei technischen Systemen ohne Sicherheitsverantwortung bestimmen jedoch fast ausschließlich die Minimalschnitte 1. und gegebenenfalls 2. Ordnung (bei redundanten Strukturen und (n-1)-aus-n-Strukturen) den Systemausfall. Minimalschnitte höherer Ordnung können meistens vernachlässigt werden, was jedoch einige Erfahrung in der Erkennung von und im Umgang mit Minimalschnitten erfordert, besonders bei einer sehr hohen Anzahl an Minimalschnitten höherer Ordnung. Beispielsweise sind Ausfallkombinationen im Anhang Q, R und S analysiert worden, die, wie die Berechnungen zeigen, vernachlässigbar sind, was jedoch nicht offensichtlich ist und im Einzelfall analysiert werden muss.

Die Analyse liefert insgesamt **46 maßgebende Minimalschnitte**, die praktisch den Systemausfall (Kapitel 2) verursachen. Theoretisch gibt es eine sehr viel größere Anzahl an Minimalschnitten höherer Ordnung, die jedoch bei dieser Leitsystemstruktur vernachlässigt werden können, siehe Anhang Q, R und S. Die berücksichtigten 46 Minimalschnitte sind im Anhang B bis E benannt.

Der **Systemausfall bzw. Systemausfallzustand** ist eine logische ODER-Verknüpfung der Minimalschnitte (MS19-MS46 sind Zusammenfassungen von Minimalschnitten).

$$A_S \approx MS_1 \vee MS_2 \vee \ \ldots \ \vee MS_{46} \tag{1}$$

Die **Systemfunktion bzw. der Systembetriebszustand** ist

$$B_S = \neg A_S \tag{2}$$

Im Prinzip stellt das Zuverlässigkeits-/Verfügbarkeitsmodell des Prozessleitsystems (Anhang B bis E) eine logische Serienstruktur aller negierten 46 Minimalschnitte ($\neg MS$) dar, also eine logische UND-Verknüpfung von Betriebszuständen der Komponenten bzw. Subsysteme. Somit steht bei Kenntnis der Minimalschnitte auch das maßgebende Zuverlässigkeitsblockdiagramm fest. Minimalschnitte können aus funktionalen Systemstrukturen ermittelt werden, sie benötigen nicht die Kenntnis von Zuverlässigkeitsblockdiagrammen, was von Vorteil sein kann. Die Ermittlung und Auswahl der relevanten Minimalschnitte aus der funktionalen Struktur erfolgt manuell, nicht automatisch durch einen Algorithmus.

Durch die Konzentration auf die maßgebenden Minimalschnitte wird die komplexe Struktur des Betriebs- aus Ausfallverhaltens auf eine einfache Zuverlässigkeits-/Verfügbarkeitsstruktur reduziert. Die Basiskenngrößen **Wahrscheinlichkeit $P(A_S)$** und **mittlere Häufigkeit $H(A_S)$** des Systemausfalls sowie **weitere Systemkenngrößen** lassen sich dann näherungsweise berechnen [Kochs 1984, Kochs 1995/1996, Kochs SFB 2001].

$$P(A_S) \approx \sum_{\forall i} P(MS_i) \qquad \text{(Nichtverfügbarkeit)} \tag{3}$$

$$H(A_S) \approx \sum_{\forall i} H(MS_i) \tag{4}$$

$$P(B_S) = 1 - P(A_S) \qquad \text{(Verfügbarkeit)} \tag{5}$$

$$H(B_S) = H(A_S) \tag{6}$$

$$T(B_S) = \frac{P(B_S)}{H(B_S)} \qquad \text{(MTTSF)} \tag{7}$$

$$T(A_S) = \frac{P(A_S)}{H(A_S)} \qquad \text{(MTTSR)} \tag{8}$$

Die Kenngrößen $P(MS_i)$ und $H(MS_i)$ spiegeln den Einfluss der Minimalschnitte und somit einzelner Komponenten oder Subsysteme auf das System ($P(A_S)$ und $H(A_S)$) wider (Sensitivitätsanalyse). Damit können Schwachstellen aufgedeckt werden.

Eine vollständige Berechnung der Minimalschnitte und der Systemkenngrößen $P(A_S)$ (= Nichtverfügbarkeit) und $P(B_S)$ (= Verfügbarkeit) sowie $H(A_S)$ ist in der Excel-Tabelle (Anhang V) im Detail durchgeführt worden. Die dazu notwendigen Komponenten-, Subsystem- und Systemmodelle sind im Anhang F bis T aufgeführt.

8 Bewertung der Systemergebnisse

Die Zuverlässigkeitsanalyse des Prozessleitsystems liefert folgende Ergebnisse (Excel Tabelle, Anhang V).

Mittlere Häufigkeit des Systemausfalls:	**$H(A_S) = 1{,}25 * 10^{-4}\ h^{-1}$**
Wahrscheinlichkeit des Systemausfalls (≡ Nichtverfügbarkeit):	**$P(A_S) = 9{,}08 * 10^{-4}$**
Wahrscheinlichkeit der Systemfunktion (≡ Verfügbarkeit):	**$P(B_S) = 0{,}999\ 092$**

Die Systemberechnung basiert auf den beschriebenen Voraussetzungen und Annahmen sowie den teilweise konservativen Festlegungen, besonders auf den konservativen Annahmen zu den Ausfallraten im Kapitel 5 und der konservativen Modellierung der Controller AC800M.

Bei Redundanzumschaltung redundanter Komponenten wird für CCF (SPoF) ein typischer Wert von 2% (CCF-Faktor, Beta-Faktor) angenommen. Höhere Werte würden auf unzuverlässige Komponenten bzw. Subsysteme hinweisen.

Im folgenden wird die Sensitivität der Subsysteme auf die Zuverlässigkeit/Verfügbarkeit des Systems diskutiert.

9 Sensitivitätsanalyse

Das **Ausfalldiagramm** (Excel-Diagramm, Anhang W) zeigt die Verteilung der Ausfallwahrscheinlichkeiten der Teilsysteme (das sind die Wahrscheinlichkeiten der Minimalschnitte, siehe Excel-Tabelle, Spalte 24). Hier ist deutlich sichtbar, dass die beiden nicht redundanten Server **MS10** PGIM Anwendungs-Server (A0CRX30) und **MS18** EMI Rechner Emission Monitoring (A0CRV40) die Zuverlässigkeit/Verfügbarkeit des Prozessleitsystems maßgeblich beeinflussen. Ohne diese Rechner wäre die Verfügbarkeit des Prozessleitsystems **0,999 247!**

Alle redundanten Komponenten (bis auf die o.g. nichtredundanten Rechner im MS10 und MS18), besonders die 28 Controller, zeigen im Ausfalldiagramm (Anhang W) eine **relativ gleichmäßig niedrige Verteilung der Ausfallwahrscheinlichkeit**, was

darauf hinweist, dass aus zuverlässigkeitstheoretischer Sicht keine Schwachstelle erkennbar ist.

Ausfall der zentralen Server

Die zentralen redundanten Server, ausgedrückt durch MS3 bis MS9, haben eine niedrige Ausfallwahrscheinlichkeit von jeweils **$2{,}07 * 10^{-6}$**.

Ausfall des Überwachungs- und Steuerungssystems

Das Überwachungs- und Steuerungssystem (BS+ES, MS1 im Anhang B) hat eine Ausfallwahrscheinlichkeit von **$2{,}53 * 10^{-6}$**, d.h. die Verfügbarkeit von BS+ES ist **0,999 997 47** (Excel-Tabelle für MS1, Spalte 24). (Modellierung und Berechnung erfolgen nach Anhang B und I.)

Ausfall der Systemuhrzeit

Nach dem Ausfall der Systemuhr (MS2, Syst.Uhr) übernimmt ein dafür vorgesehener Master die Führung der Systemuhrzeit bis zur Wiederinbetriebnahme der Systemuhr. Wenn dieser Master ausfällt, übernimmt der nächste dafür vorgesehene Master die Systemuhrzeit. Es stehen **zwei Master** zur Übernahme der Systemuhrzeit zur Verfügung. Deshalb ist dieses Teilsystem zweifach redundant und somit grundsätzlich hoch zuverlässig ausgelegt. Die Ausfallwahrscheinlichkeit (Nichtverfügbarkeit) der Systemuhrzeit ist unter den gemachten konservativen Annahmen in Spalte 4, Excel-Tabelle **$3{,}25 * 10^{-8}$**, die Verfügbarkeit ist **0,999 999 967**. (Modellierung und Berechnung erfolgen im Anhang T.)

Ausfall der Bussysteme

Beim PNP/PNS- und ANP/ANS-Bussystem bilden 2 x 6 und 2 x 3 Switche in Parallelschaltung das Rückgrad der Kommunikationssysteme (MS11 und MS12, Anhang D). Bei Ausfall eines Switches am Primärbus wird auf die Parallelswitche am Sekundärbus des jeweiligen Bussystems umgeschaltet. Da ein Totalausfall einer der beiden Bussysteme einen „Black-out“ des Prozessleitsystems und somit einen Stillstand der Prozesse bedeuten würde, muss den Bussystemen besondere Aufmerksamkeit gewidmet werden. Zuverlässigkeitsmodellierung und Berechnung sind im Anhang J und K beschrieben.

Die Berechnung liefert folgende Werte (Excel-Tabelle für MS11 und MS12, Spalte 23, 24).

	$H(MS11_{ANP/ANS}) = 4{,}04 * 10^{-9}\ h^{-1}$	$P(MS11_{ANP/ANS}) = 3{,}24 * 10^{-8}$
	$H(MS12_{PNP/PNS}) = 1{,}62 * 10^{-8}\ h^{-1}$	$P(MS12_{PNP/PNS}) = 1{,}29 * 10^{-7}$
Summe:	$\mathbf{H(A_{Bussysteme}) = 2{,}02 * 10^{-8}\ h^{-1}}$	$\mathbf{P(A_{Bussysteme}) = 1{,}61 * 10^{-7}}$

Die Bussysteme ANP/ANS und PNP/PNS zusammen haben eine rechnerische Verfügbarkeit (bezüglich des Totalausfalls) von **0,999 999 839**. Ein Ausfall der Bussysteme ist somit äußerst unwahrscheinlich (unter Einhaltung der Spezifikationen).

Ausfälle der IO-Cluster

Ausfälle der 131 IO-Cluster infolge von CCF (SPoF) der IO-Module (Annahme: 131 x 8 = 1.048 IO-Module) treten mit einer Wahrscheinlichkeit von **$5{,}72 * 10^{-5}$** auf (Excel-Tabelle, Spalte 22, Zeile Summe). Alle anderen Ausfälle des Prozessleitsystems treten mit einer Wahrscheinlichkeit von **$8{,}51 * 10^{-4}$** auf (Excel-Tabelle, Spalte 17, Zeile Summe). Die Summe dieser beiden Werte ergibt die Nichtverfügbarkeit des Prozessleitsystems von **$9{,}08 * 10^{-4}$** (Excel-Tabelle, Spalte 24, Zeile Summe).

Einfluss der mittleren Instandsetzungs-/Ersatz-/Reparaturdauer (MTTR)

Diese hat großen Einfluss auf die Zuverlässigkeit/Verfügbarkeit des Prozessleitsystems. Würde die mittlere Instandsetzungsdauer (MTTR) der Komponenten von **8 auf 6 Stunden** reduziert werden, so würde die Verfügbareit des Prozessleitsystems auf **0,999 305** (anstelle von 0,999 092 für 8 Stunden) ansteigen.

Mehrfachausfälle

Unabhängige **Mehrfachausfälle** von AC800M und/oder IO-Cluster (infolge von CCF von IO-Modulen) können **vernachlässigt** werden, siehe Anhang Q bis S.

Fazit: Für die definierte Systemfunktion (Systembetrieb, Systemausfall) wird eine Zuverlässigkeit/Verfügbarkeit von > 0,999 errechnet.

10 Hinweise für Garantieerklärungen

Auf einige Punkte im Hinblick auf Garantieerklärungen soll hingewiesen werden. Weil theoretisch berechnete Zuverlässigkeitsangaben auf der **Theorie der Wahrscheinlichkeit** und der **stochastischen Prozesse** beruhen, sollten Zuverlässigkeitsangaben - alleine aus diesem Grund - **nicht determinativ garantiert** werden, selbst wenn die Zuverlässigkeitsanalyse 100 % exakt wäre.

Hinzu kommt, dass oft die Eingangsdaten, wie Ausfallraten und Instandsetzungsraten, geschätzte **Mittelwerte** sind, die mehr oder weniger große statistische Unsicherheiten aufweisen. Darüber hinaus liegen die zugehörigen **Wahrscheinlichkeits-Dichtefunktionen** (oder **Wahrscheinlichkeits-Verteilungsfunktionen**), die Voraussetzung zur Bestimmung von **Konfidenzintervallen** sind, in der Praxis meistens nicht vor. Es werden deshalb, wenn überhaupt, diese Funktionen als Exponential- oder Weibullverteilungen angenommen (**aleatorische Unsicherheiten**).

Beim Einsatz technologisch neuer Produkte liegen meistens keine gesicherten (quantitativen) Kenntnisse über **Einflussfaktoren** vor, sondern qualitatives Expertenwissen, was zudem häufig unter Experten variiert. Auch hier sind meistens Annahmen notwendig, die zu Unsicherheiten führen (**epistemische Unsicherheiten**).

Weiterhin beschreiben Modelle nur näherungsweise die Realität. Für komplizierte Berechnungsformeln werden ebenfalls häufig Näherungformeln verwendet (**Verfahrens-Ungenauigkeiten**) [Limbourg 2008, Limbourg et al. 2007 a und b].

In der Regel wird deshalb versucht, **konservative** (auf der sicheren Seite liegende) Annahmen zu treffen.

Bei Zuverlässigkeitszusicherungen sollten folgende Punkte berücksichtigt und dokumentiert werden.

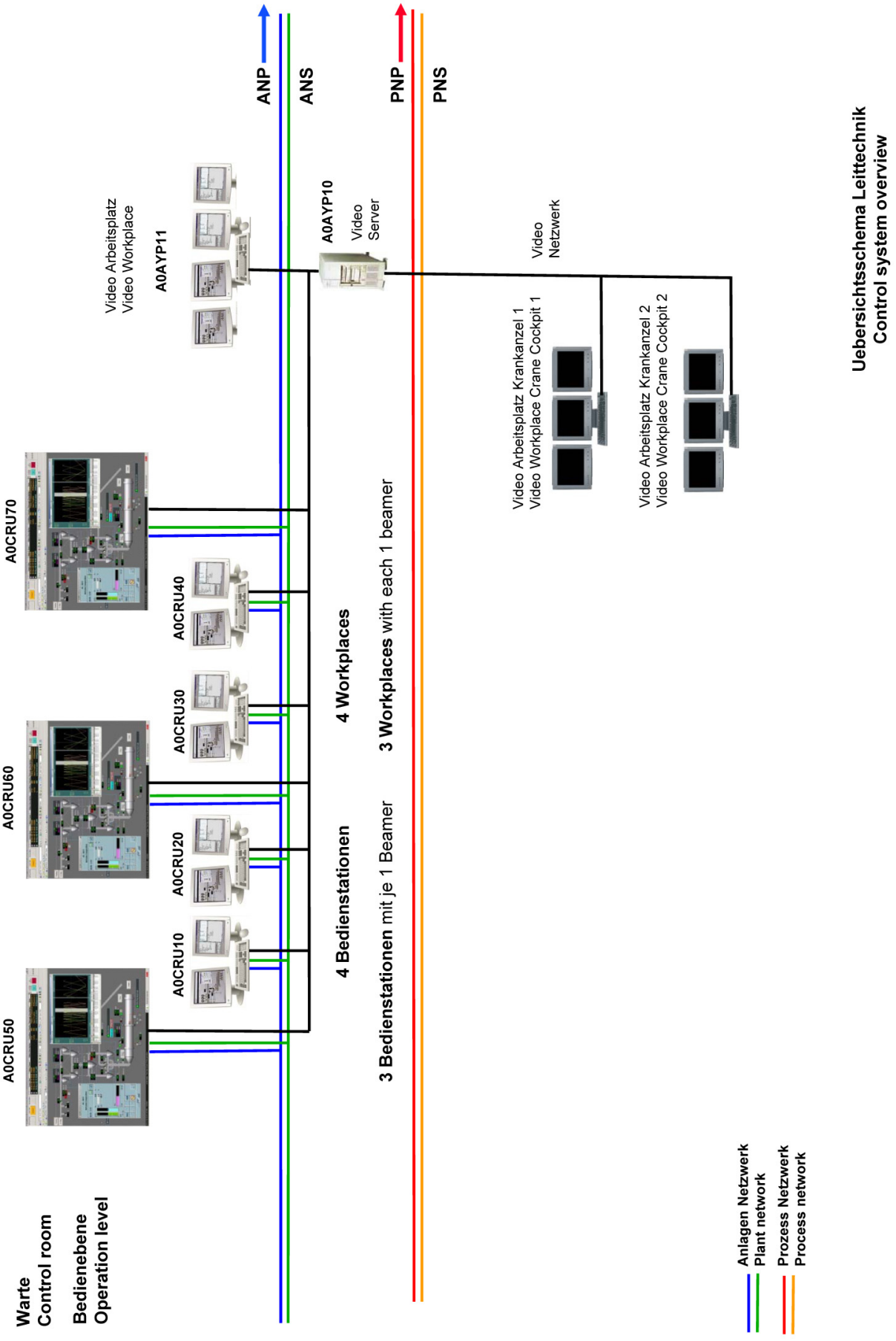
1. Basis sind definierte Systemfunktionen (auf Normen und Richtlinien bezüglich der Begriffe Zuverlässigkeit bzw. Verfügbarkeit sollte Bezug genommen werden).
2. Festlegung der Annahmen bzw. Voraussetzungen zur Zuverlässigkeitanalyse.
3. Hinweis, dass es sich um wahrscheinlichkeitstheoretische Angaben (z.B. arithmetische Mittelwerte) handelt, die als solche zu interpretieren sind (also keine festen Garantiewerte im determinativen Sinne).
4. Hinweis auf Unsicherheiten, wie oben beschrieben.
5. Zuverlässigkeitsaussagen beziehen sich auf den stationären Zustand des Systems („eingeschwungener“ Zustand, keine Kinderkrankheiten, keine

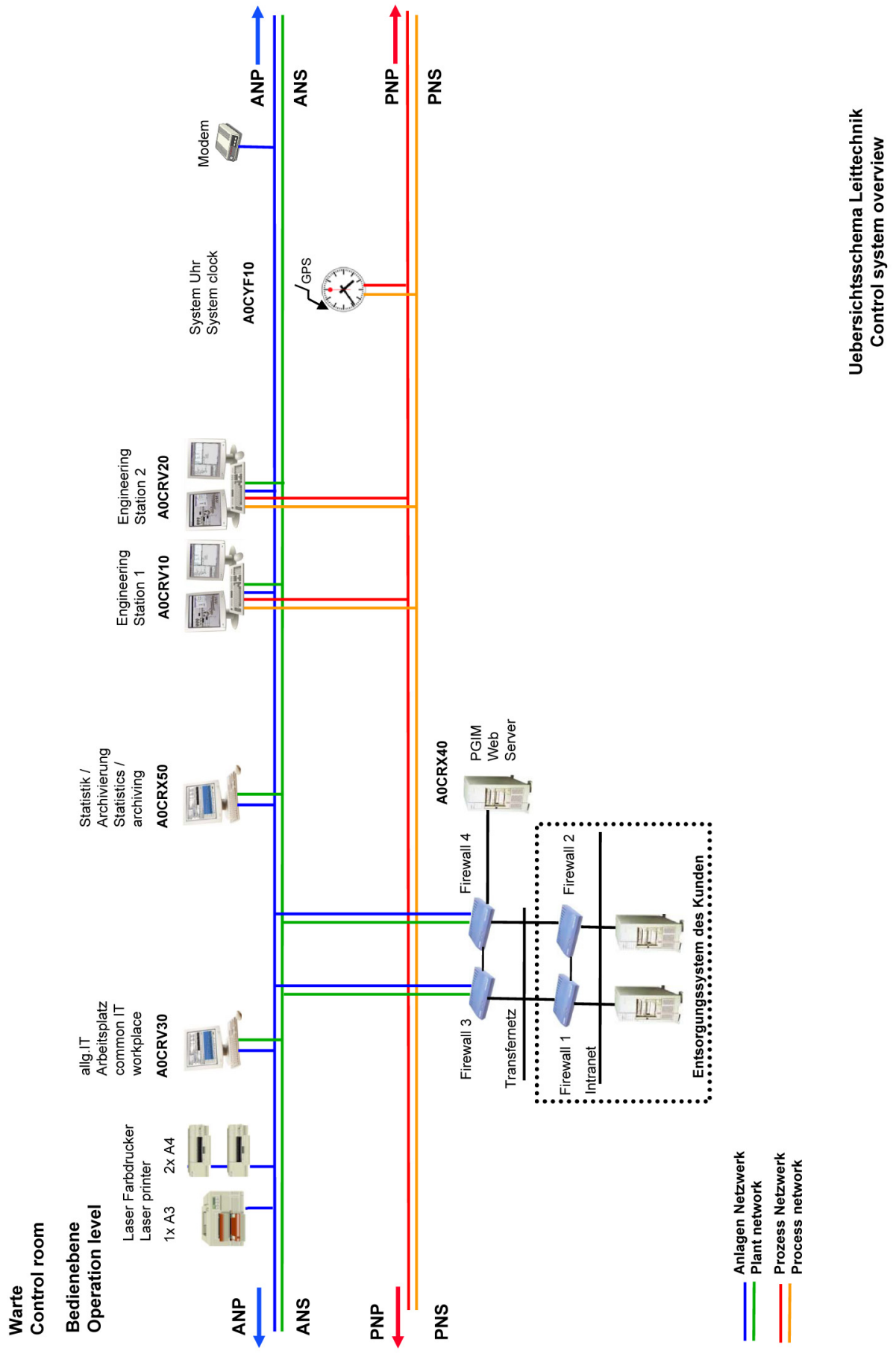
Verschleißausfälle, Exponentialverteilung, konstante Übergangsraten) oder auf ein vorgegebenes Zeitintervall, z.B. wenn Weibullverteilungen zugrunde gelegt werden (nicht konstante Übergangsraten).

6. Ein Nachweis der berechneten Zuverlässigkeitskenngrößen kann nicht auf der Basis einer Betriebs-/Ausfallstatistik eines relativ kurzen Betriebszeitraumes erfolgen, was besonders beim Nachweis von hohen Verfügbarkeitswerten zu beachten ist. Beispielsweise wäre eine halbjährige Probephase für den Nachweis von vereinbarten Zuverlässigkeitskenngrößen (wegen Punkt 3) zu kurz. Hier könnten auch Kinderkrankheiten (Punkt 5) eine Rolle spielen.

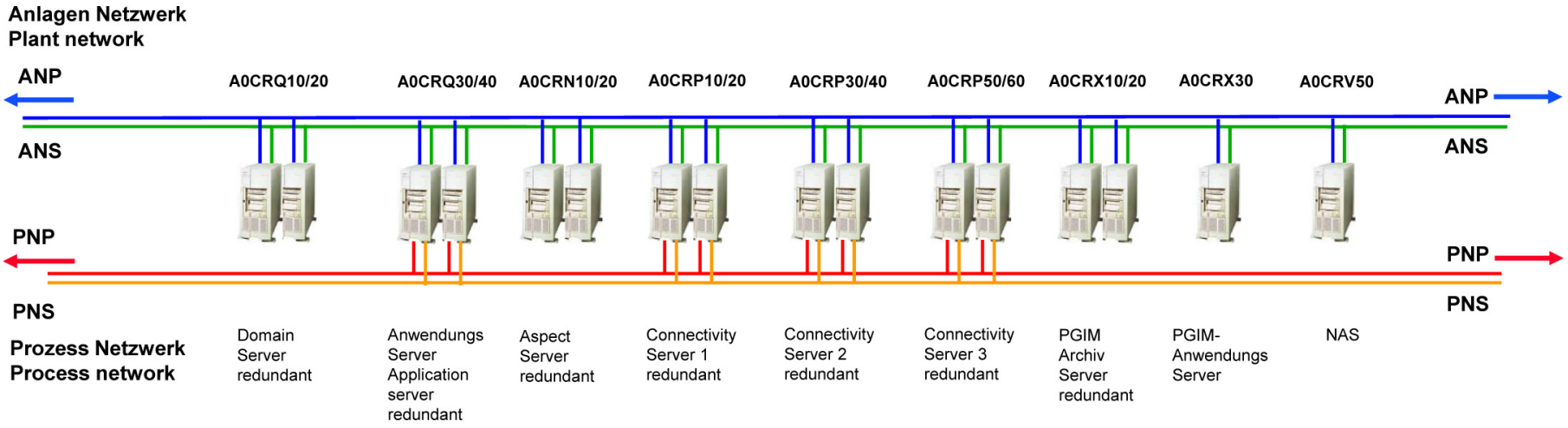
Trotz aller Unsicherheiten liegt der unbestreitbare **Nutzen von Zuverlässigkeitsanalysen** darin, dass Systeme mit berechneten Zuverlässigkeitskennwerten, die vorgegebene Zuverlässigkeitsanforderungen theoretisch erfüllen, in der Regel auch im Betrieb zuverlässig arbeiten, zumindest alle Voraussetzungen dafür mitbringen. Beim **Vergleich** verschiedener Systemvarianten besitzen die Daten, Modelle und Verfahren Unsicherheiten, die die gleiche Tendenz in allen Systemen haben (entweder zur zuverlässigen oder unzuverlässigen Seite) und somit einen Systemvergleich praktisch zulassen, vorausgesetzt, die Daten-, Modellierungs- und Berechnungsbasis ist gleich, z.B. [Kochs et al. 2011 und 2012]. Ein weiterer Vorteil von Zuverlässigkeitsanalysen ist die Aufdeckung von **Schwachstellen** im System.

Anhang A: Übersichtsschema Leittechnik

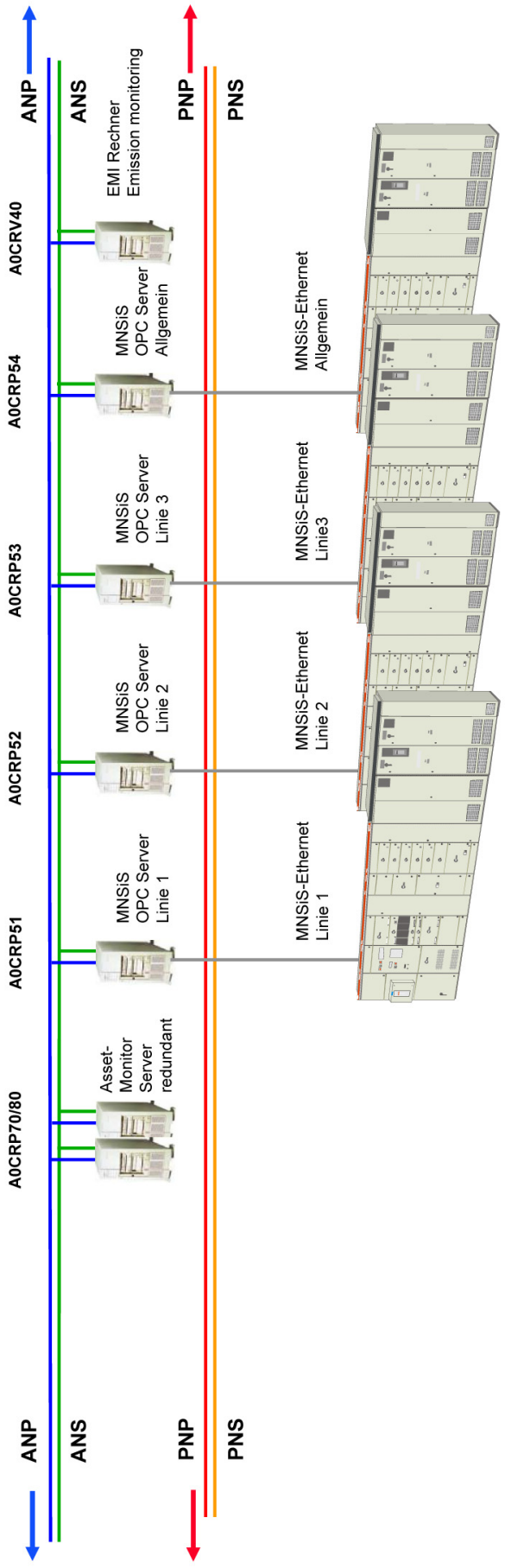

Uebersichtsschema Leittechnik
Control system overview
Warte
Control room
Bedienebene
Operation level
A0CRU50
A0CRU60
A0CRU70
A0CRU10
A0CRU20
A0CRU30
A0CRU40
4 Bedienstationen
4 Workplaces
3 Bedienstationen mit je 1 Beamer
3 Workplaces with each 1 beamer
ANP
ANS
PNP
PNS
A0AYP10
Video Server
A0AYP11
Video Arbeitsplatz
Video Workplace
Video Netzwerk
Video Arbeitsplatz Krankanzel 1
Video Workplace Crane Cockpit 1
Video Arbeitsplatz Krankanzel 2
Video Workplace Crane Cockpit 2
Anlagen Netzwerk
Plant network
Prozess Netzwerk
Process network



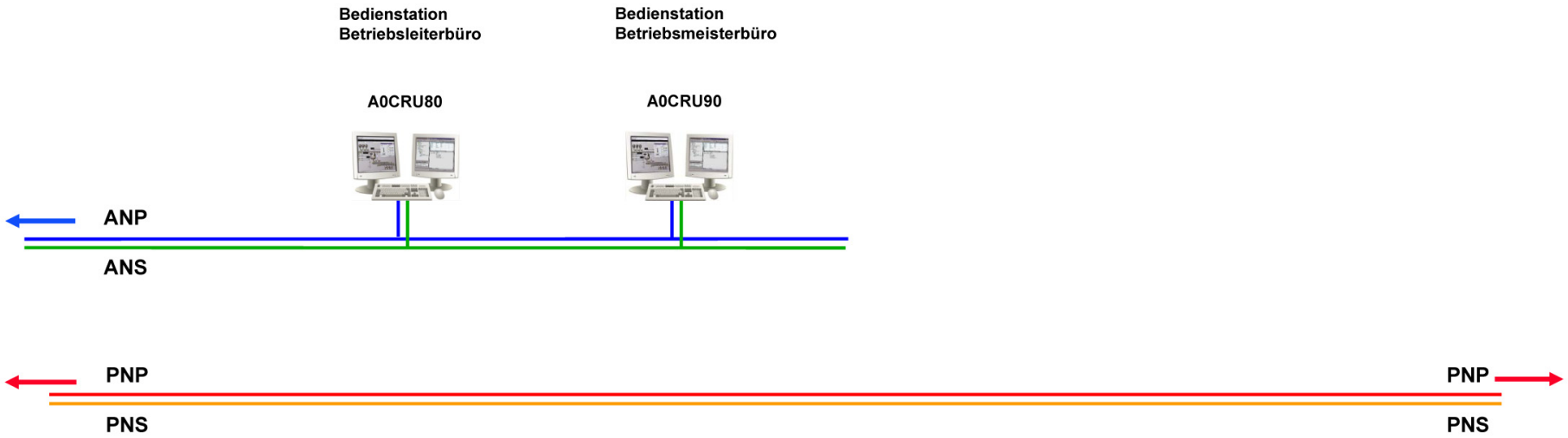
Uebersichtsschema Leittechnik
Control system overview



Uebersichtsschema Leittechnik
Control system overview

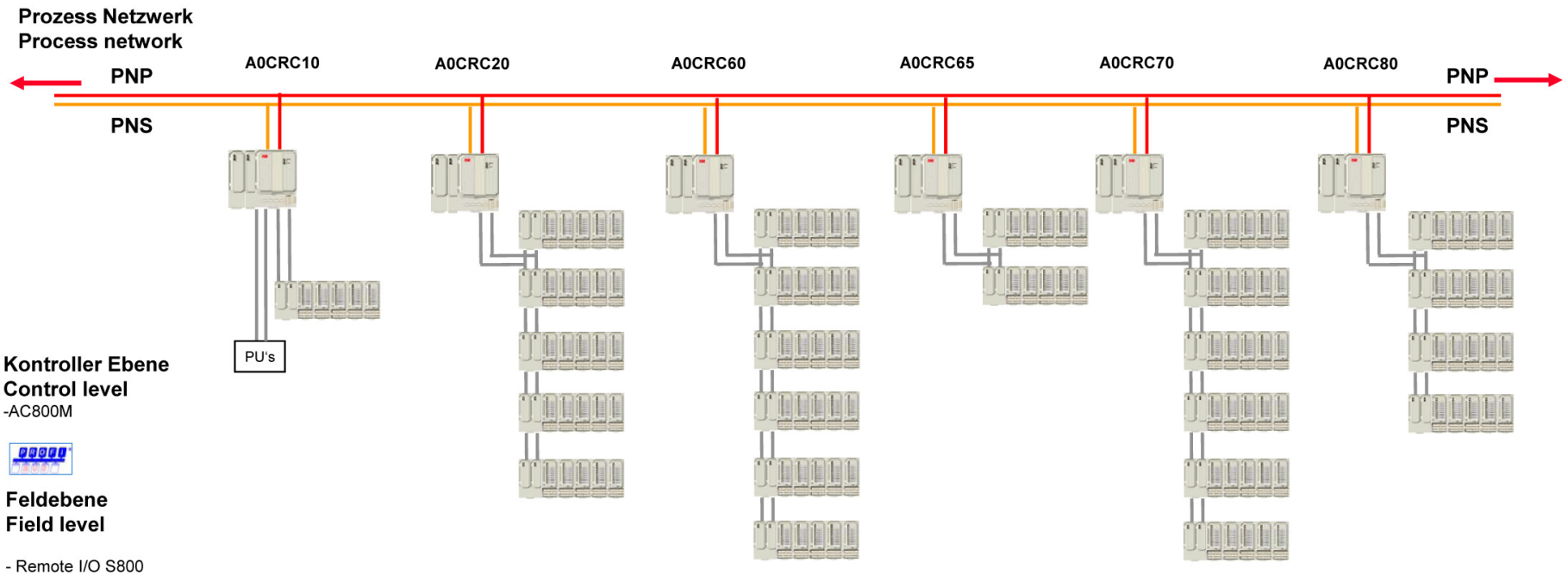


Uebersichtsschema Leittechnik
Control system overview



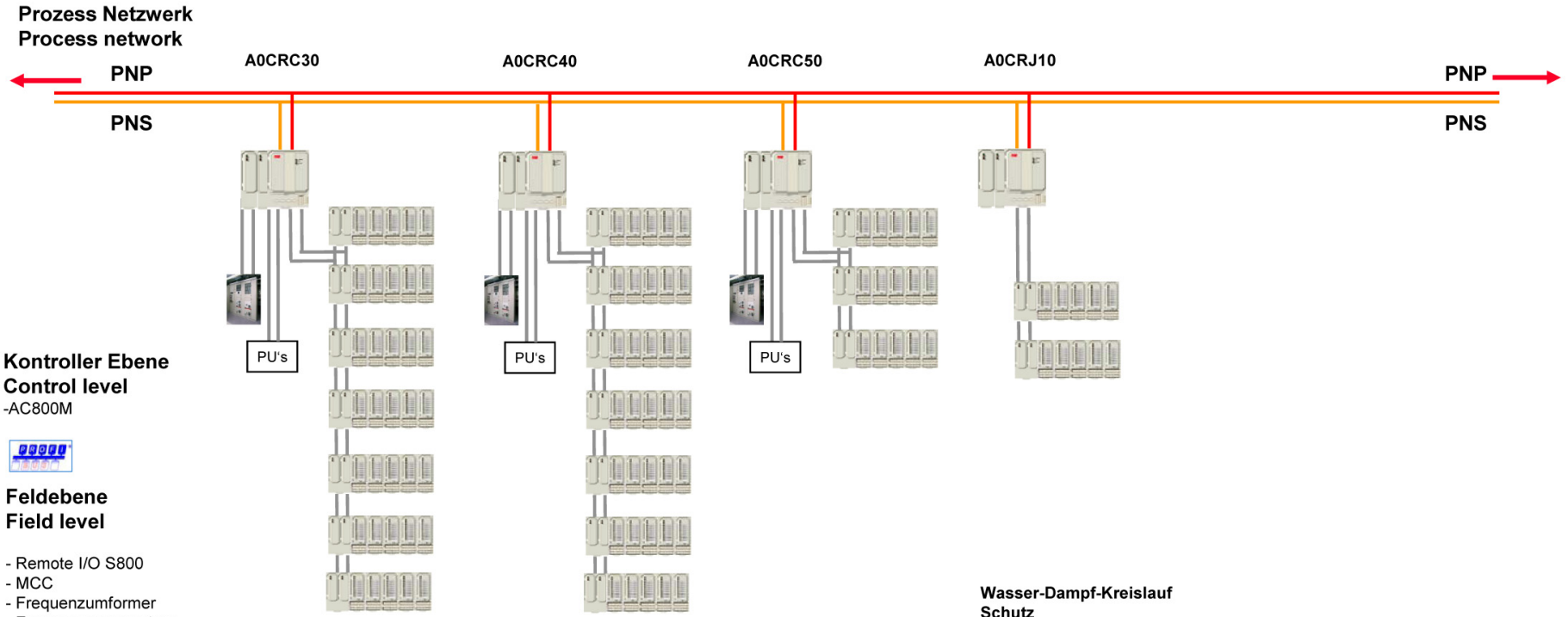
Uebersichtsschema Leittechnik
Control system overview

Prozess allgemeine Systeme
Process common systems



Uebersichtsschema Leittechnik
Control system overview

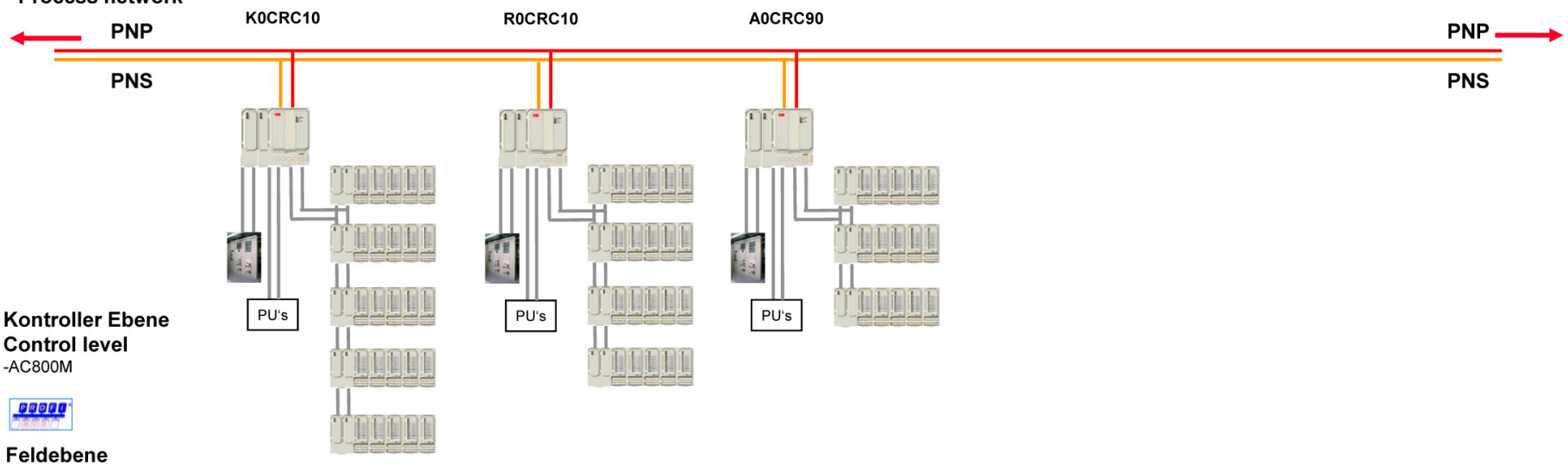
Prozess allgemeine Systeme
Process common systems



Uebersichtsschema Leittechnik
Control system overview

Prozess allgemeine Systeme
Process common systems

Prozess Netzwerk
Process network



Kontroller Ebene
Control level
-AC800M

Feldebene
Field level

- Remote I/O S800
- MCC
- Frequenzumformer
- Frequnecy converters
- Package Units

Kessel allgemein
Boiler common

red. Kontroller
red. controller

Rauchgasreinigung allgemein
FGC common

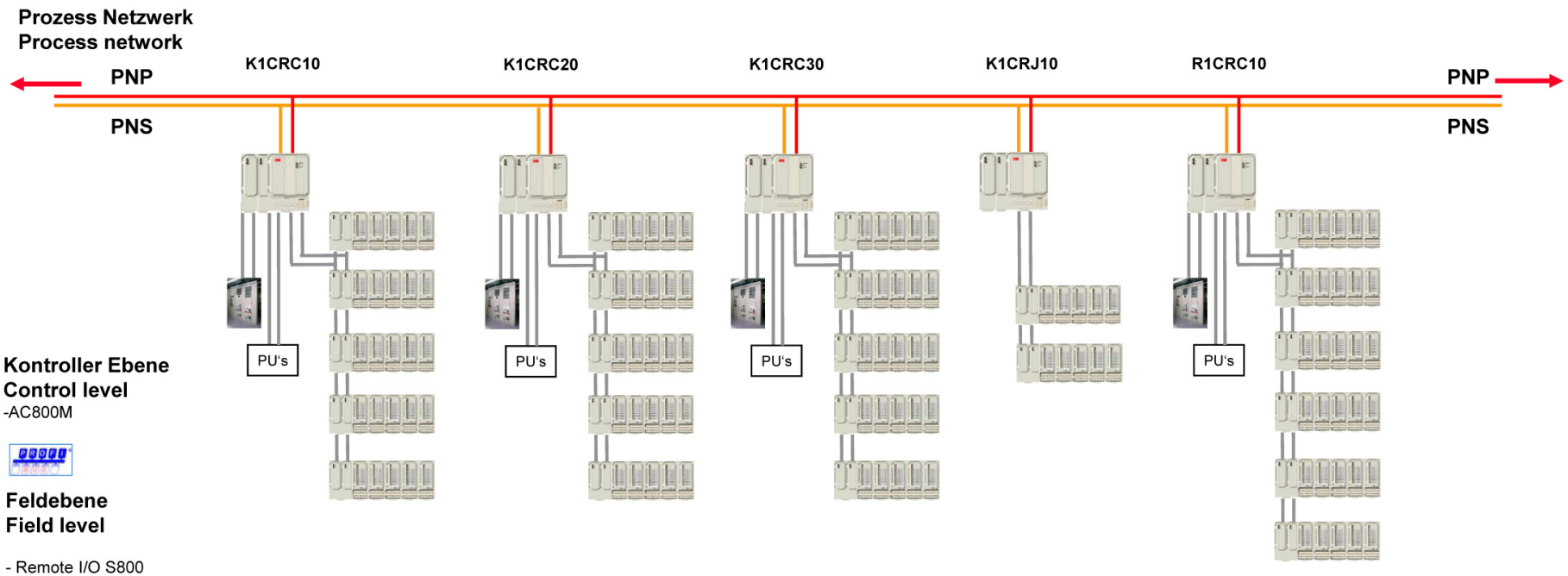
red. Kontroller
red. controller

Verkehrsleitung
Traffic control

red. Kontroller
red. controller

Uebersichtsschema Leittechnik
Control system overview

Prozess Linie 1
Process Line 1



Kontroller Ebene
Control level
-AC800M

Feldebene
Field level

- Remote I/O S800
- MCC
- Frequenzumformer
- Frequnecy converters
- Package Units

Kessel Linie 1
Boiler line 1

red. Kontroller
red. controller

Kessel Linie 1
Boiler line 1

red. Kontroller
red. controller

Kessel Linie 1
Boiler line 1

red. Kontroller
red. controller

Kessel Linie 1
Schutz
Boiler protection
line 1

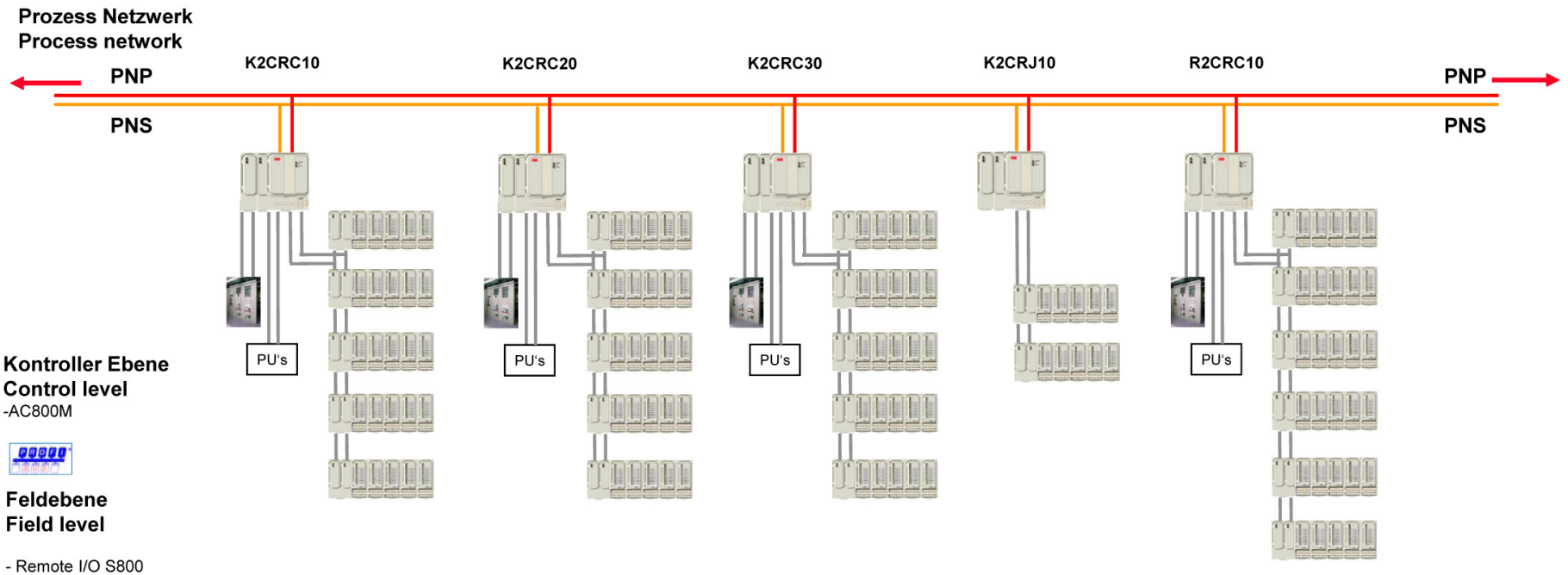
red. Kontroller
hochverfügbar
red. high integrity
controller

Rauchgasreinigung
Linie 1
FGC line 1

red. Kontroller
red. controller

Uebersichtsschema Leittechnik
Control system overview

Prozess Linie 2
Process Line 2



Kontroller Ebene
Control level
-AC800M

Feldebene
Field level

- Remote I/O S800
- MCC
- Frequenzumformer
- Frequnecy converters
- Package Units

Kessel Linie 2
Boiler line 2

red. Kontroller
red. controller

Kessel Linie 2
Boiler line 2

red. Kontroller
red. controller

Kessel Linie 2
Boiler line 2

red. Kontroller
red. controller

Kessel Linie 2
Schutz
Boiler protection
line 2

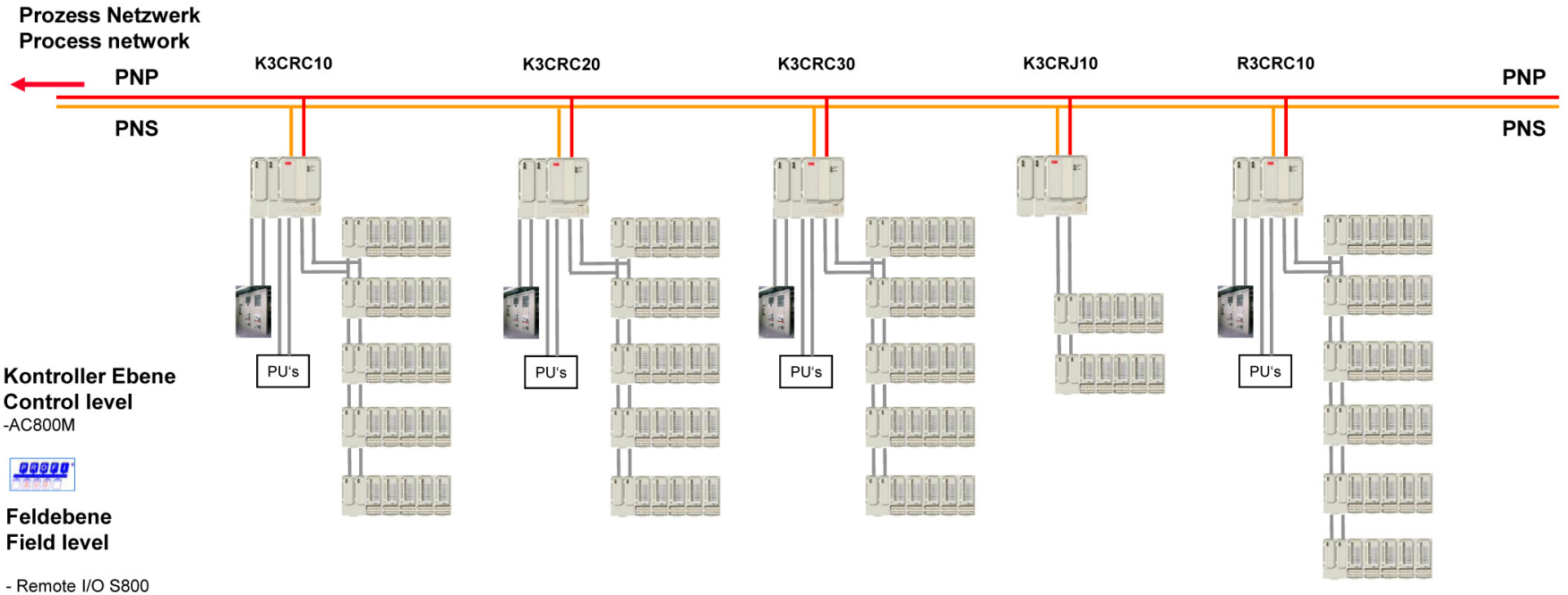
red. Kontroller
hochverfügbar
red. high integrity
controller

Rauchgasreinigung
Linie 2
FGC line 2

red. Kontroller
red. controller

Uebersichtsschema Leittechnik
Control system overview

Prozess Linie 3
Process Line 3



Kontroller Ebene
Control level
-AC800M

Feldebene
Field level

- Remote I/O S800
- MCC
- Frequenzumformer
- Frequnecy converters
- Package Units

Kessel Linie 3
Boiler line 3

red. Kontroller
red. controller

Kessel Linie 3
Boiler line 3

red. Kontroller
red. controller

Kessel Linie 3
Boiler line 3

red. Kontroller
red. controller

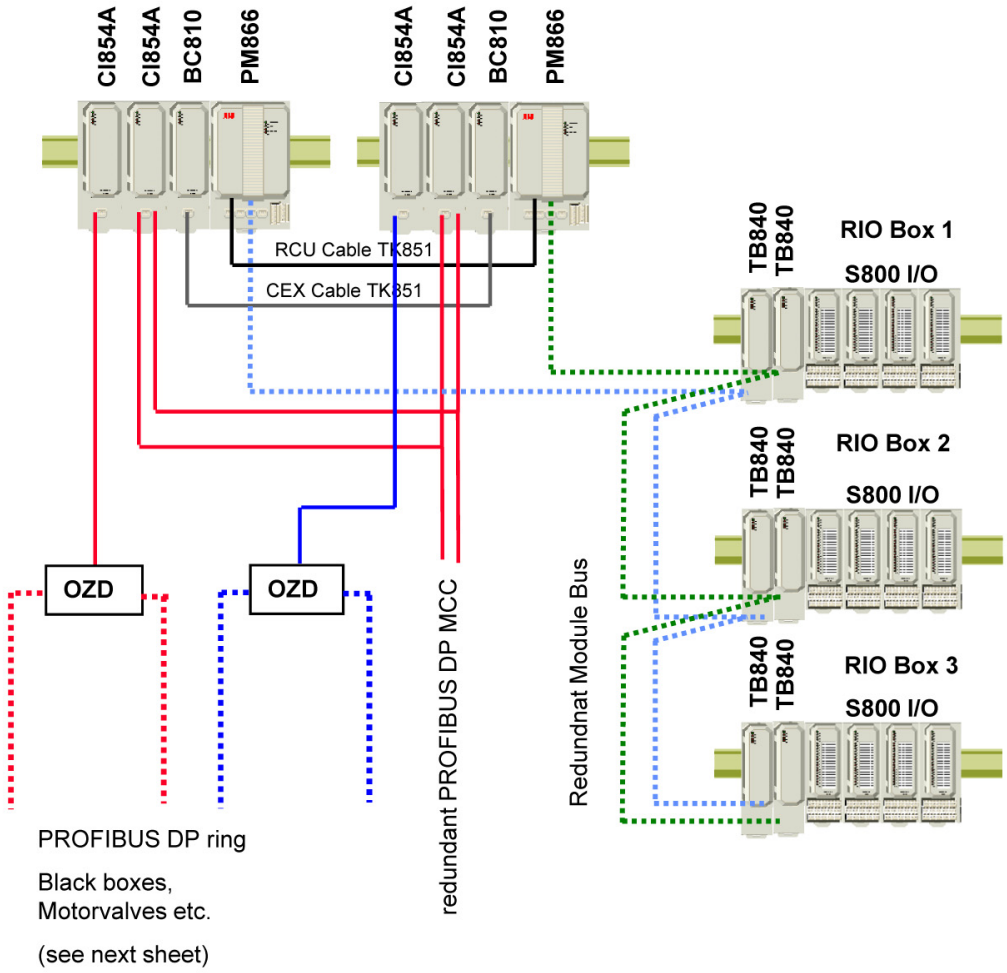
Kessel Linie 3
Schutz
Boiler protection
line 3

red. Kontroller
hochverfügbar
red. high integrity
controller

Rauchgasreinigung
Linie 3
FGC line 3

red. Kontroller
red. controller

Uebersichtsschema Leittechnik
Control system overview



BC810: CEX Bus Verbindugsmodul
CEX Bus interconnection unit

CI854A: Profibus DP Schnittstelle
Profibus DP Interface

PM864: Kontroller CPU
Controller CPU

TB840: Modulbus Gruppen Modem
Modulebus Cluster Modem

RCU cable TK851: Redundanz Verbindung
Redundancy link

CEX cable TK851: Verbindungskabel
interconnection link

PROFIBUS DP ring : LWL Kabel
FO Cable

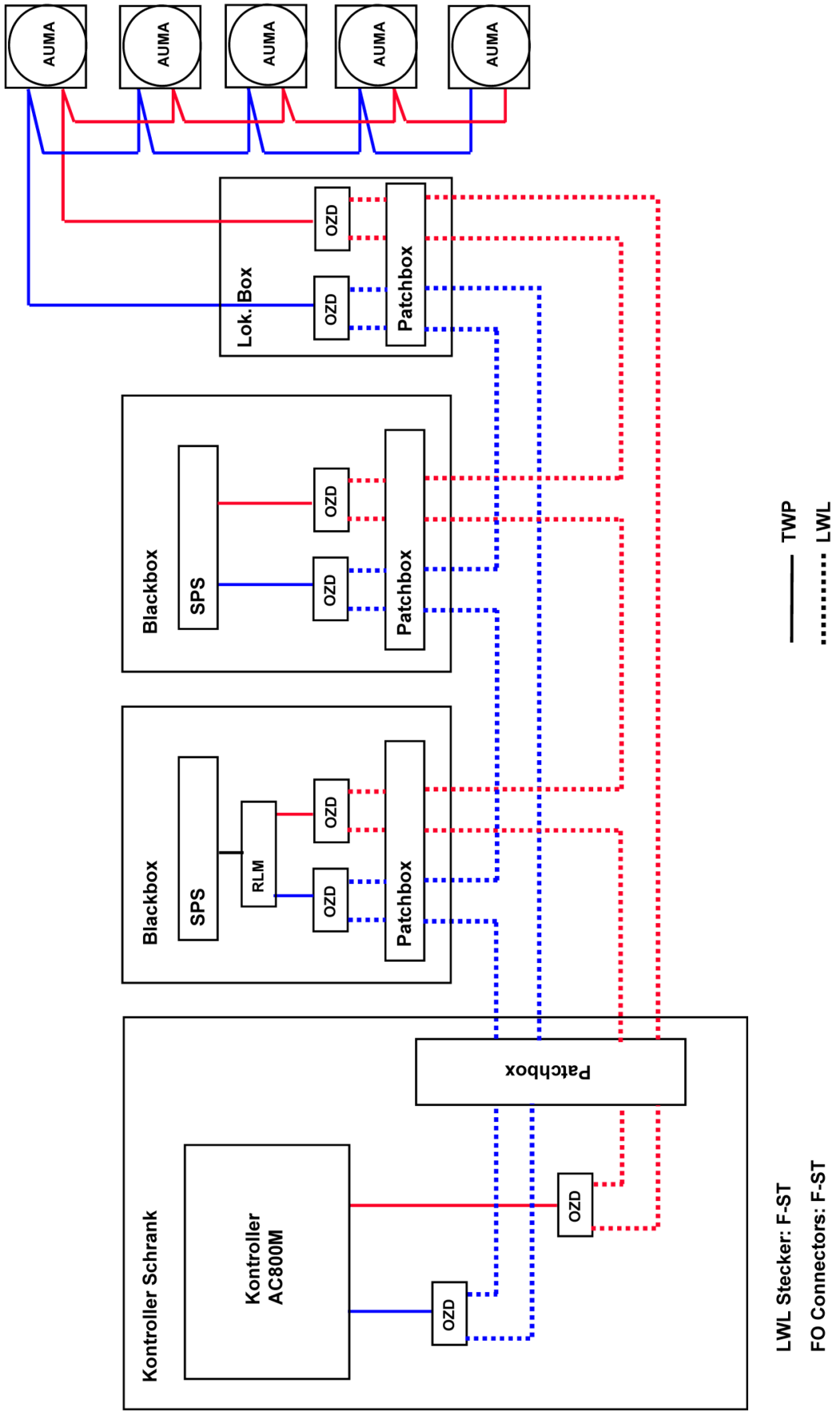
PROFIBUS DP MCC: geschirmtes TWP Kabel
shielded TWP Cable

PROFIBUS DP Auma: geschirmtes TWP Kabel
shielded TWP Cable

Module bus : LWL Kabel
FO Cable

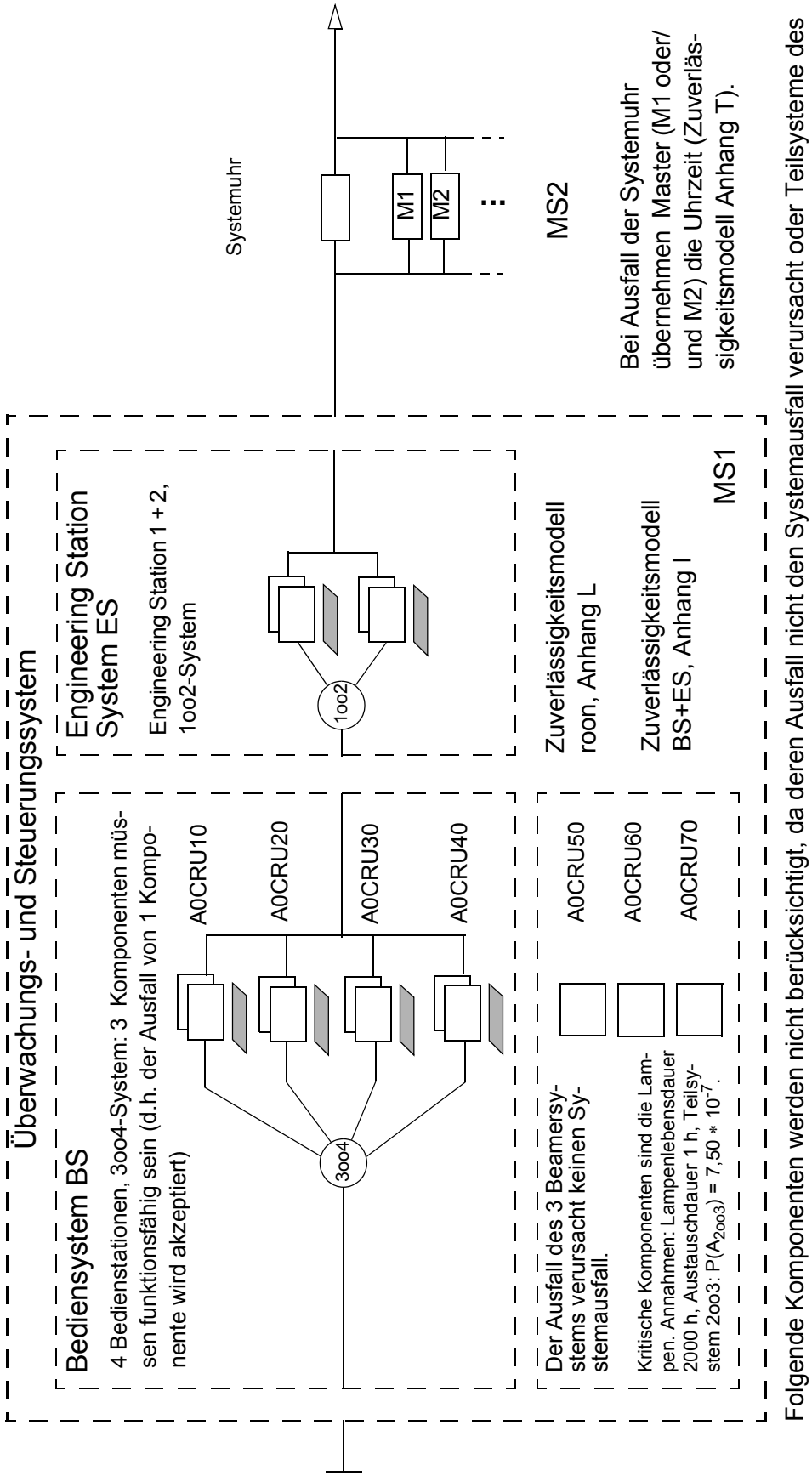
OZD Elektro-Optischer Umsetzer
Electro-optical converter

Kontroller Typical
Controller typical


AUMA
AUMA
AUMA
AUMA
AUMA
Lok. Box
OZD
OZD
Patchbox
Blackbox
SPS
OZD
OZD
Patchbox
Blackbox
SPS
RLM
OZD
OZD
Patchbox
Patchbox
Kontroller Schrank
Kontroller AC800M
OZD
OZD
TWP
LWL
LWL Stecker: F-ST
FO Connectors: F-ST
Profibus DP Ring Typical
Profibus DP ring typical

Anhang B - U: Zuverlässigkeits-/Verfügbarkeits-Modellierung

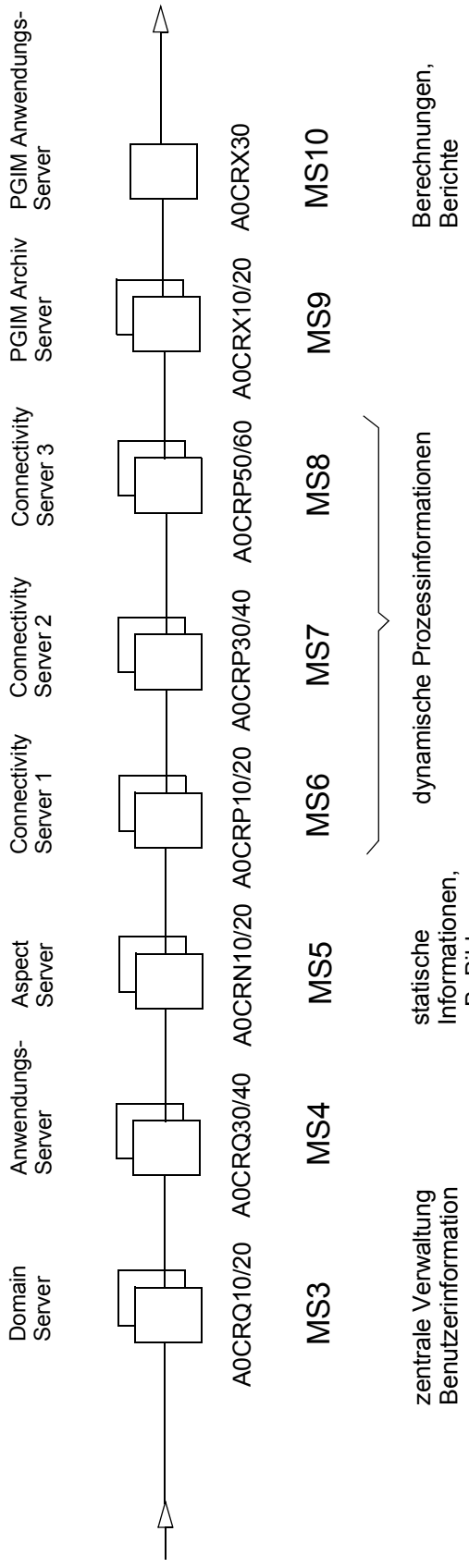
Anhang B: Zuverlässigkeits-/Verfügbarkeitsmodell der Systemkonfiguration des Übersichtsschemas Leittechnik, Anhang A, Seite 20 und 21.



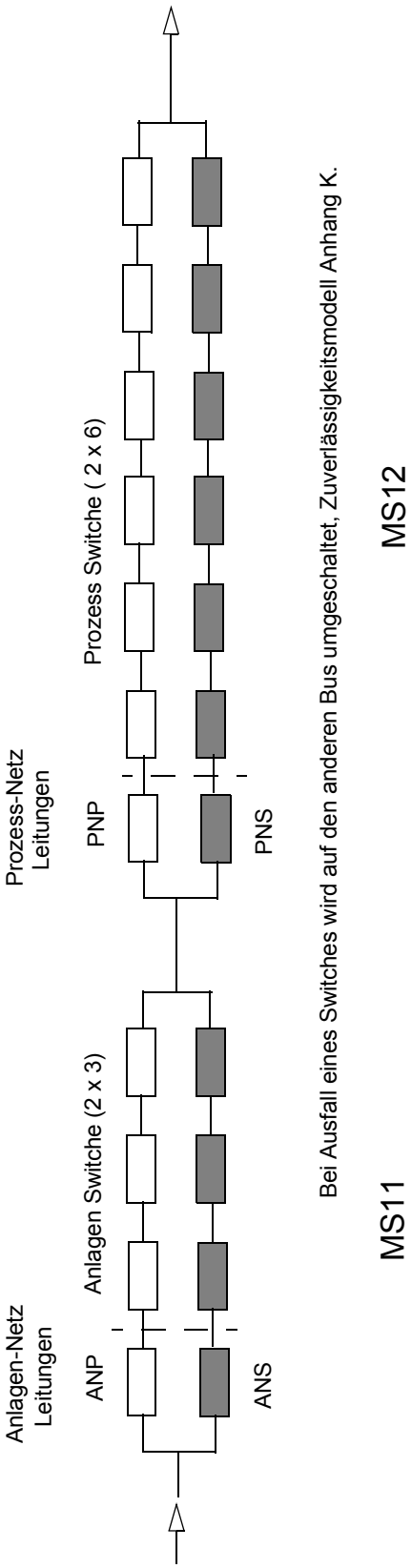
Folgende Komponenten werden nicht berücksichtigt, da deren Ausfall nicht den Systemausfall verursacht oder Teilsysteme des Kunden sind:

- Video Arbeitsplatz (A0AYP11),
- Video Server (A0AYP10) und Video Arbeitsplatz Krankanzel 1 und 2,
- Firewall 1 bis 4, PGIM Web Server (A0CRX40), Transfernetz, Intranet ISH und Entsorgungssystem des Kunden,
- allg. IT Arbeitsplatz (A0CRV30),
- Statistik/Archivierung (A0CRX50),
- Laser Farbdrucker 1xA3 und 2xA4,
- Modem.

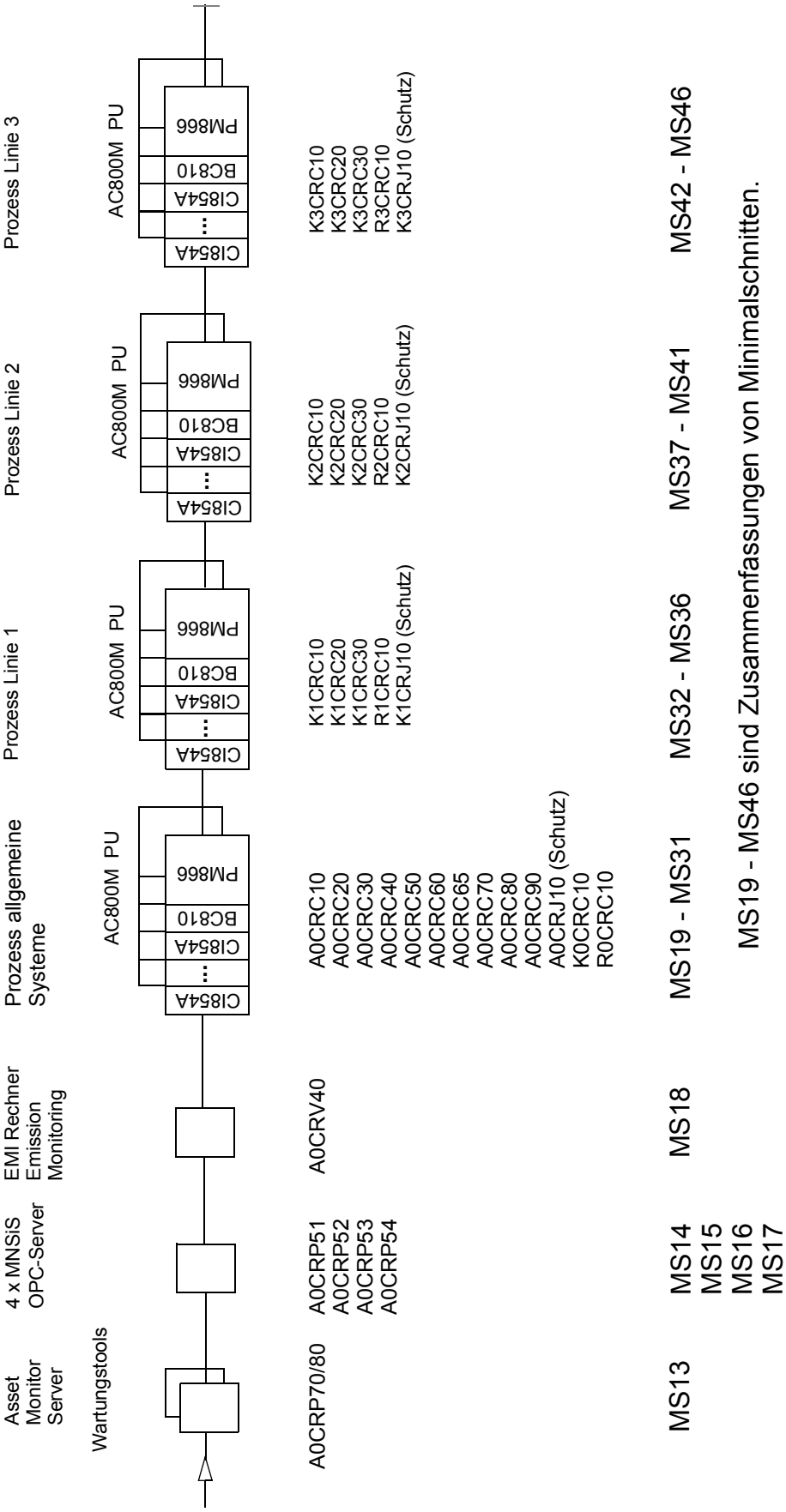
Anhang C: Zuverlässigkeits-/Verfügbarkeitsmodell der Systemkonfiguration des Übersichtsschemas Leittechnik, Anhang A, Seite 22.



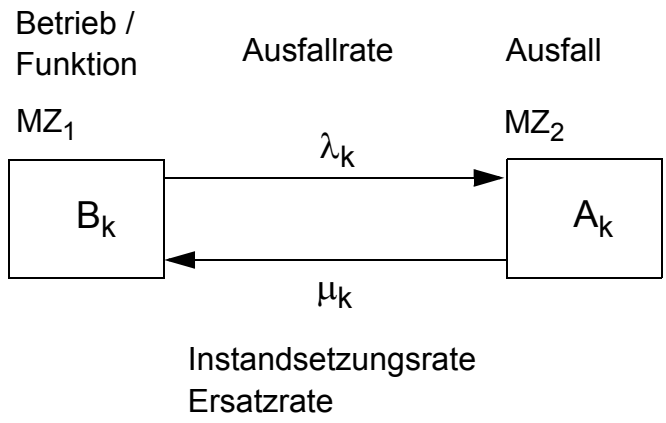
Anhang D: Zuverlässigkeits-/Verfügbarkeitsmodell der Bussysteme des Übersichtsschemas Leittechnik, Anhang A, Seite 20 - 30.



Anhang E: Zuverlässigkeits-/Verfügbarkeitsmodell der Systemkonfiguration des Übersichtsschemas Leittechnik, Anhang A, Seite 23 - 30.



Anhang F: Allgemeines Markov Modell einer Komponente.



MZ_i Markov Zustand i, B_k Betriebszustand und A_k Ausfallzustand der Komponente k, λ_k Ausfallrate und μ_k Instandsetzungsrate (Reparatur oder gleichwertiger Ersatz) der Komponente k.

$$MTTF = \frac{1}{\lambda_k} \qquad MTTR = \frac{1}{\mu_k} \qquad MTBF = MTTF + MTTR$$

Mittlere Häufigkeit $H(MZ_2)$, Wahrscheinlichkeit $P(MZ_2)$ eines Ausfalls der Komponente k:

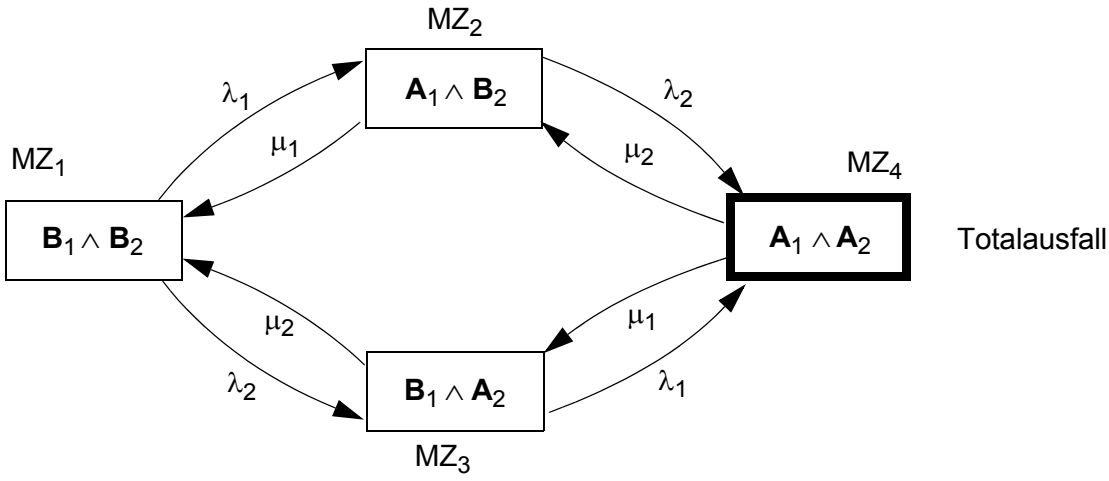
$$H(MZ_2) = P(MZ_1)\lambda_k \approx \lambda_k$$

$$P(MZ_2) = \frac{\lambda_k}{\lambda_k + \mu_k} \approx \frac{\lambda_k}{\mu_k} \quad \text{mit} \quad \mu_k \gg \lambda_k$$

Nichtverfügbarkeit: $P(MZ_2)$

Verfügbarkeit: $P(MZ_1) = 1 - P(MZ_2)$

Anhang G: Markov Modell parallel redundanter Komponenten (Anhang F) ohne stochastische Abhängigkeiten.



MZ_i Markov Zustand i, B_k Betriebszustand, A_k Ausfallzustand der Komponente k, λ_k Ausfallrate, μ_k Instandsetzungsrate (Ersatzrate) der Komponente k.

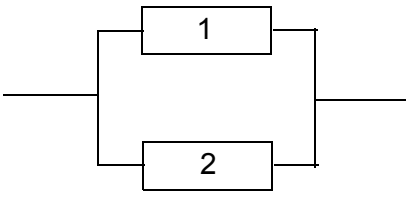
Mittlere Häufigkeit $H(MZ_4)$, Wahrscheinlichkeit $P(MZ_4)$ eines Totalausfalls MZ_4 (berechnet mit dem Verfahren der Wahrscheinlichen Markov Wege)

$$H(MZ_4) = P(MZ_2)\lambda_2 + P(MZ_3)\lambda_1$$

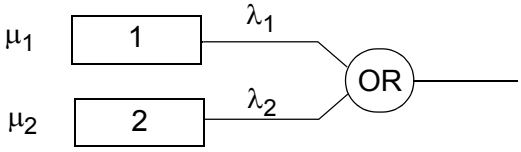
$$\approx \frac{\lambda_1\lambda_2}{\mu_1} + \frac{\lambda_1\lambda_2}{\mu_2}$$

$$P(MZ_4) = \frac{H(MZ_4)}{\mu_1 + \mu_2} \approx \frac{\lambda_1\lambda_2}{\mu_1\mu_2}$$

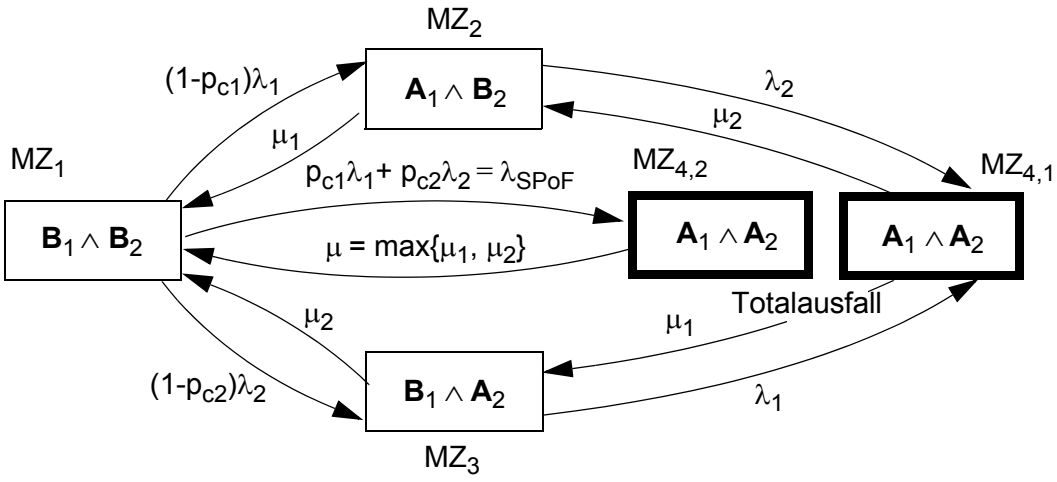
Zuverlässigkeitsblockdiagramm



Fehlerbaummodell



Anhang H: Markov Modell parallel redundanter Komponenten (Anhang F) mit Common Cause Fehler (CCF).



MZ_i Markov Zustand i, B_k Betriebszustand, A_k Ausfallzustand der Komponente k, SPoF Single-Point-of-Failure (CCF), λ_k Ausfallrate, μ_k Instandsetzungsrate (Reparatur oder Ersatz) der Komponente k, p_{ck} Wahrscheinlichkeit eines CCF, ausgelöst durch Komponente k, der zu einem Common Cause Ausfalls führt (in DIN EN 61508 als Beta(β)-Faktor bezeichnet).

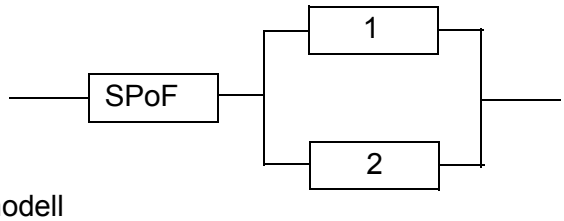
Mittlere Häufigkeit $H(MZ_4)$, Wahrscheinlichkeit $P(MZ_4)$ eines Totalausfalls
$MZ_4 = MZ_{4,1} \vee MZ_{4,2}$ (berechnet mit dem Verfahren der Wahrscheinlichen Markov Wege

$$H(MZ_4) = H(MZ_{4,1}) + H(MZ_{4,2}) = P(MZ_2)\lambda_2 + P(MZ_3)\lambda_1 + P(MZ_1)\lambda_{SPoF}$$

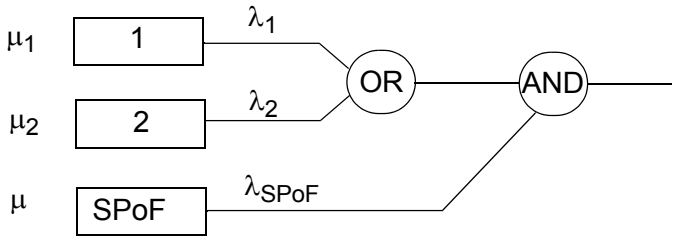
$$\approx \frac{\lambda_1\lambda_2}{\mu_1} + \frac{\lambda_1\lambda_2}{\mu_2} + \lambda_{SPoF}$$

$$P(MZ_4) = \frac{H(MZ_{4,1})}{\mu_1 + \mu_2} + \frac{H(MZ_{4,2})}{\mu} \approx \frac{\lambda_1\lambda_2}{\mu_1\mu_2} + \frac{\lambda_{SPoF}}{\mu}$$

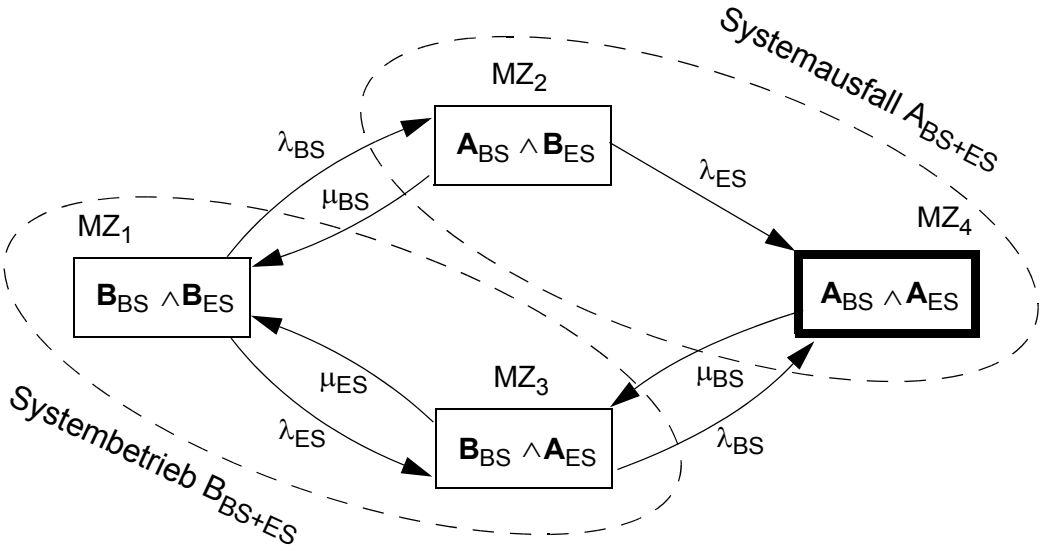
Zuverlässigkeitsblockdiagramm



Fehlerbaummodell



Anhang I: Markov Modell des Überwachungs- und Steuerungssystems, das aus Bediensystem (BS) und Engineering Station System (ES) (Anhang B) besteht.



Mittlere Häufigkeit $H(A_{BS+ES})$, Wahrscheinlichkeit $P(A_{BS+ES})$ eines Systemausfalls, verursacht durch Ausfall der Systeme BS und ES (berechnet mit dem Verfahren der Wahrscheinlichen Markov Wege)

$$A_{BS+ES} = MZ_2 \vee MZ_4$$

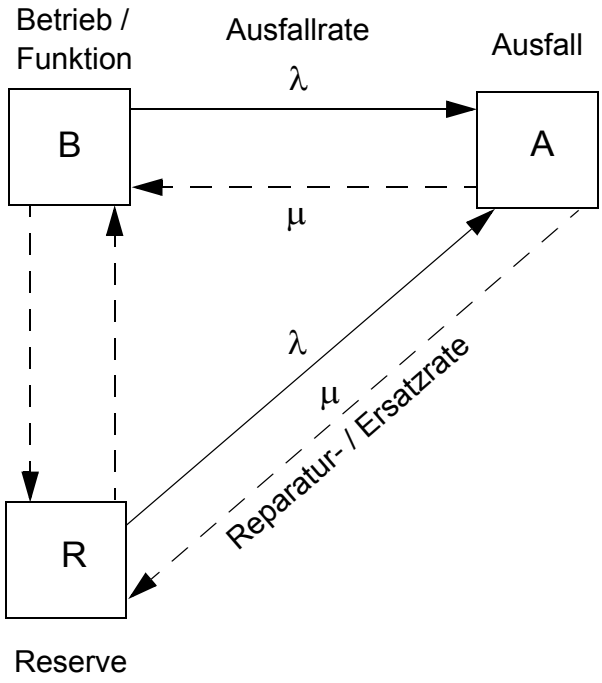
$$B_{BS+ES} = MZ_1 \vee MZ_3$$

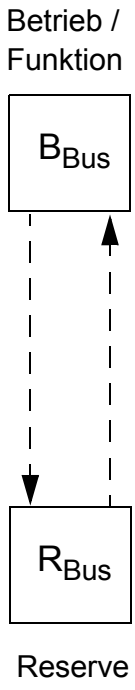
$$H(A_{BS+ES}) \approx \lambda_{BS} + P(MZ_3)\lambda_{BS}$$

$$\approx \lambda_{BS} + \frac{\lambda_{ES}\,\lambda_{BS}}{\mu_{ES}}$$

$$P(A_{BS+ES}) \approx \frac{\lambda_{BS}}{\mu_{BS}} + \frac{\lambda_{ES}\,\lambda_{BS}}{\mu_{ES}\,\mu_{BS}}$$

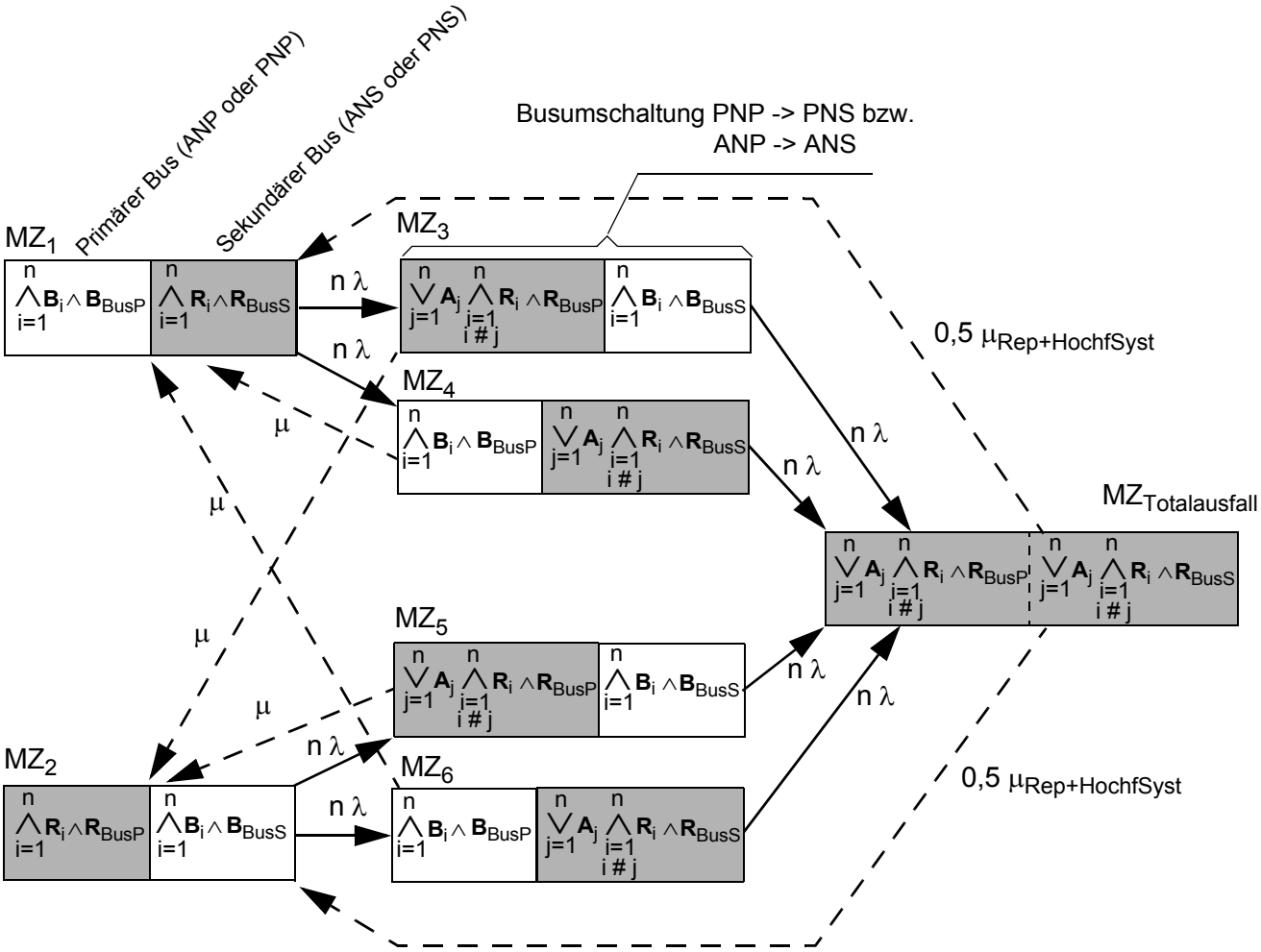
Anhang J: Markov Modell eines Switches (oben) und eines Busses (unten).





vom Systemzustand abhängige Übergänge

Anhang K: Markov Modell für das Teilsystem: 2 x n Switche an den redundanten Bussen (ANP/ANS: n = 3 und PNP/PNS: n = 6).



MZ_x Markov Zustand x, B_k Betriebszustand, A_k Ausfallzustand, R_k Reserve (stand-by) der Komponente Switch k (Modell Anhang J oberes Bild).

Der Ausfall der Buskabel wird hier nicht berücksichtigt, da deren Ausfall als unwahrscheinlich angenommen wird (Modell Anhang J unteres Bild).

A_k wird sofort erkannt, sowohl im Betriebszustand (weißer Bereich) als auch im Reservezustand (grauer Bereich) des Busses. Bei Ausfall eines Switches am primären Bus wird auf **alle** Switche am sekundären Bus umgeschaltet.

Die Instandsetzung bzw. der Ersatz eines ausgefallenen Switches wird mit μ (= 1/MTTR) durchgeführt.

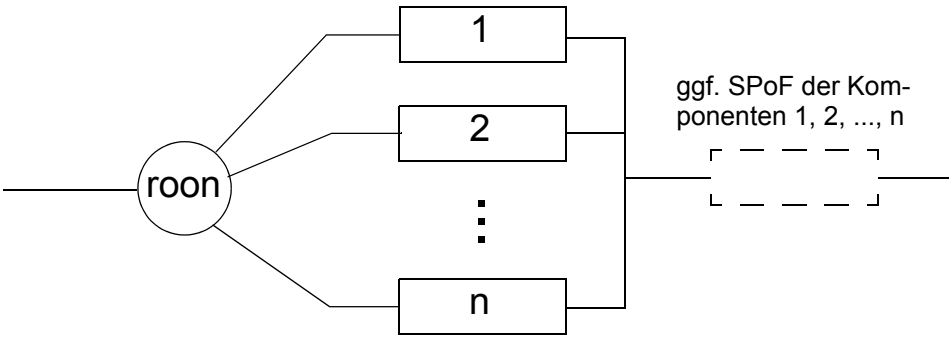
Die Reparatur und das Hochfahren des gesamten Systems nach einem Totalausfall des Bussystems wird mit $\mu_{Rep+HochfSyst}$ (= $1/T_{Rep+HochfSyst}$) berücksichtigt.

Mittlere Häufigkeit $H(MZ_{Totalausfall})$, Wahrscheinlichkeit $P(MZ_{Totalausfall})$, mit der der Primärbus und der Sekundärbus ausfallen (berechnet mit dem Verfahren der Wahrscheinlichen Markov Wege)

$$H(MZ_{Totalausfall}) \approx 2 \cdot (n\lambda/\mu)^2 \mu$$

$$P(MZ_{Totalausfall}) \approx 2 \cdot (n\lambda/\mu)^2 (\mu/\mu_{Rep+HochfSys})$$

Anhang L: Zuverlässigkeitsblockdiagramm für ein r-out-of-n System (roon System), Beispiel für BS und ES (MS1), Anhang B, Anhang I, Excel Tabelle (Anhang V), Zeile 1 bis 3.



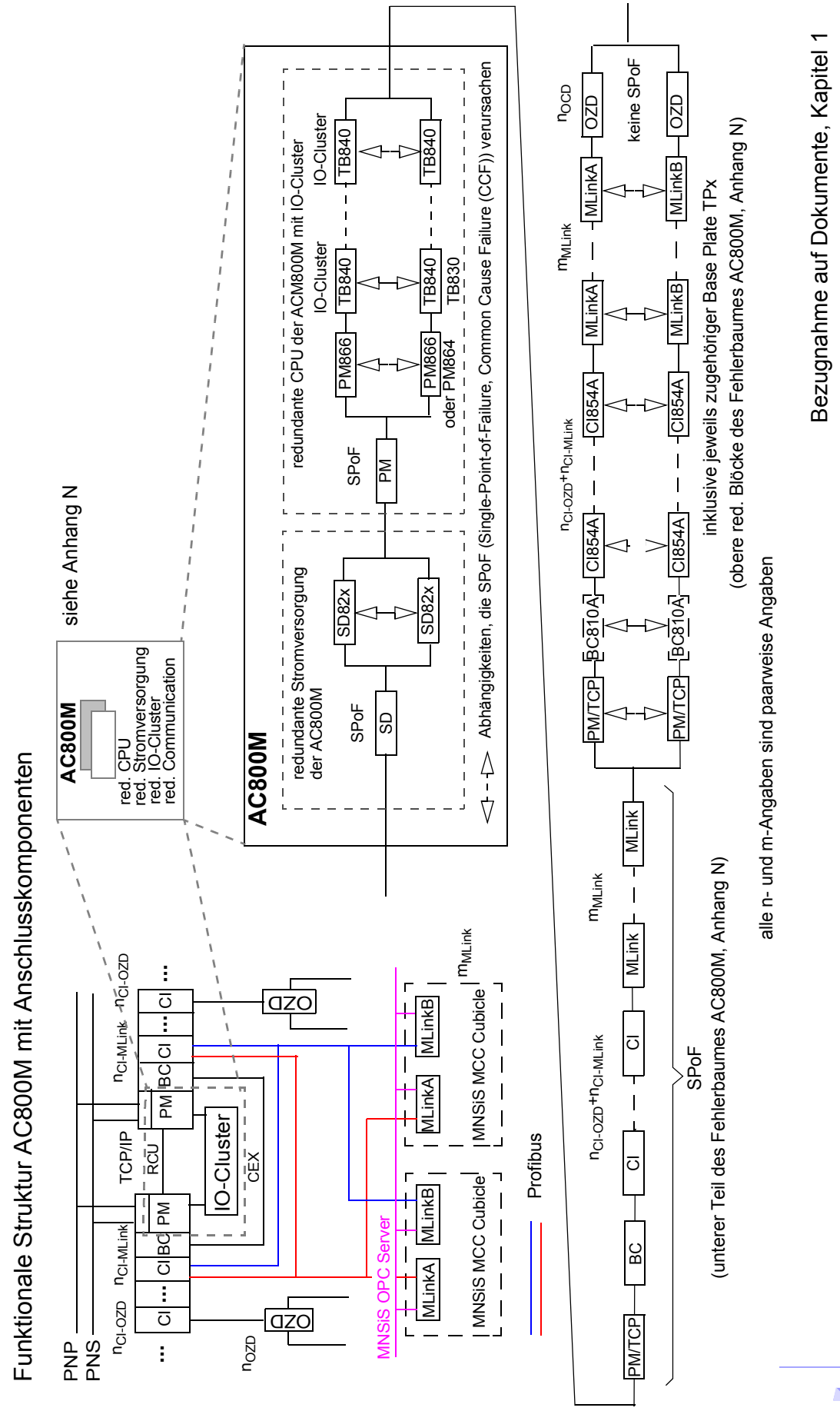
roon: Mindestens r von n (r-out-of-n) Komponenten müssen im Systembetriebszustand sein, d.h. der Ausfall von maximal n - r Komponenten wird akzeptiert.

Mittlere Häufigkeit $H(A_{roon})$, Wahrscheinlichkeit $P(A_{roon})$ eines Ausfalls des roon Systems (mit r = n - 1 (3oo4, 1oo2, Anhang B), berechnet mit dem Verfahren der Minimalschnitte, Modell im Anhang G):

$$H(A_{roon}) \approx \frac{n * (n-1)}{1 * 2} (\frac{\lambda}{\mu})^2 * 2 * \mu$$

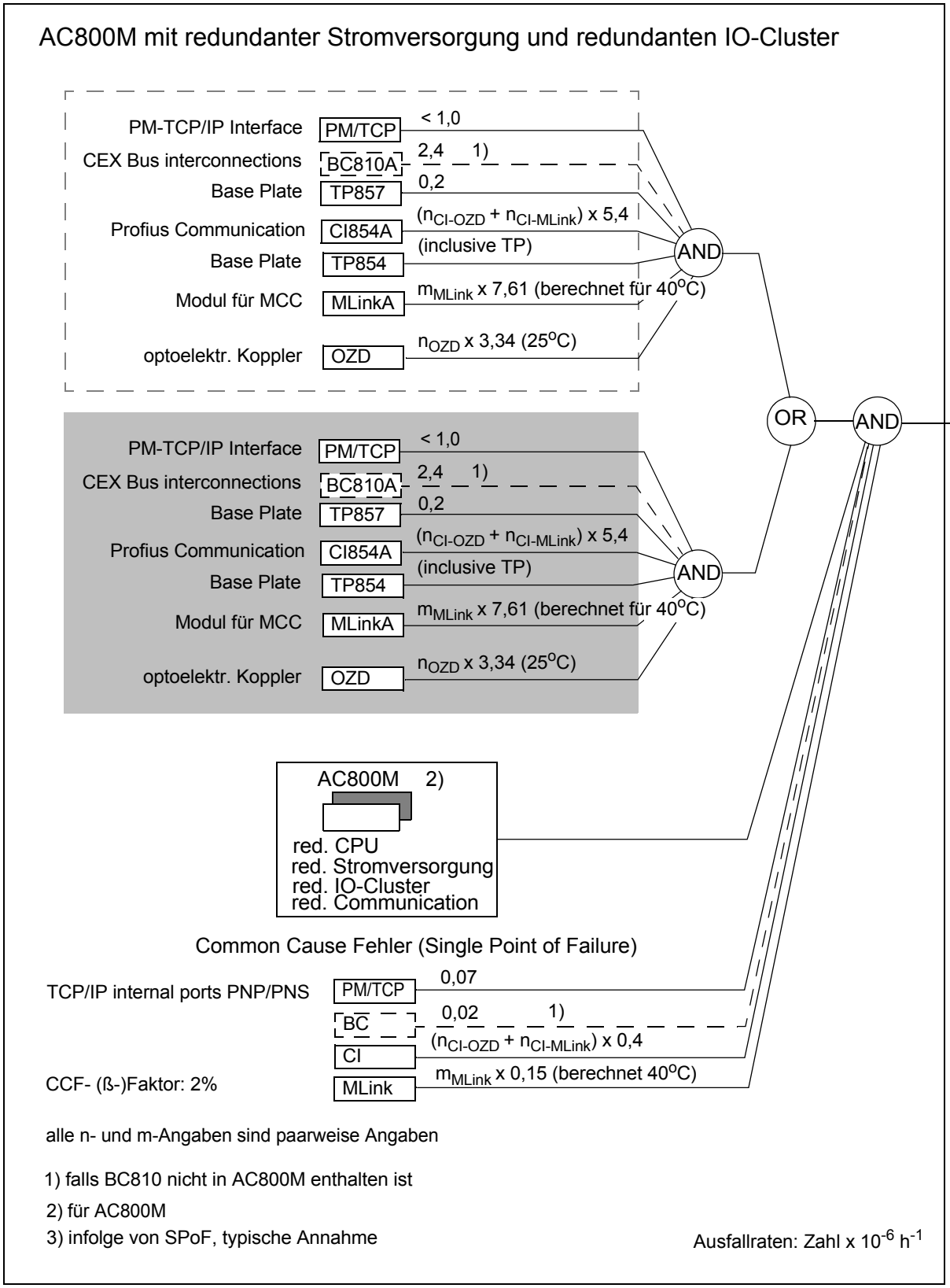
$$P(A_{roon}) \approx \frac{n * (n-1)}{1 * 2} (\frac{\lambda}{\mu})^2$$

Anhang M: Funktionale Struktur eines Controllers AC800M im PNP/PNS-Netzwerk mit angeschlossenen OZD und MLink sowie IO-Cluster (Beispielbestückung) und dazu entwickeltes Zuverlässigkeitsblockdiagramm.



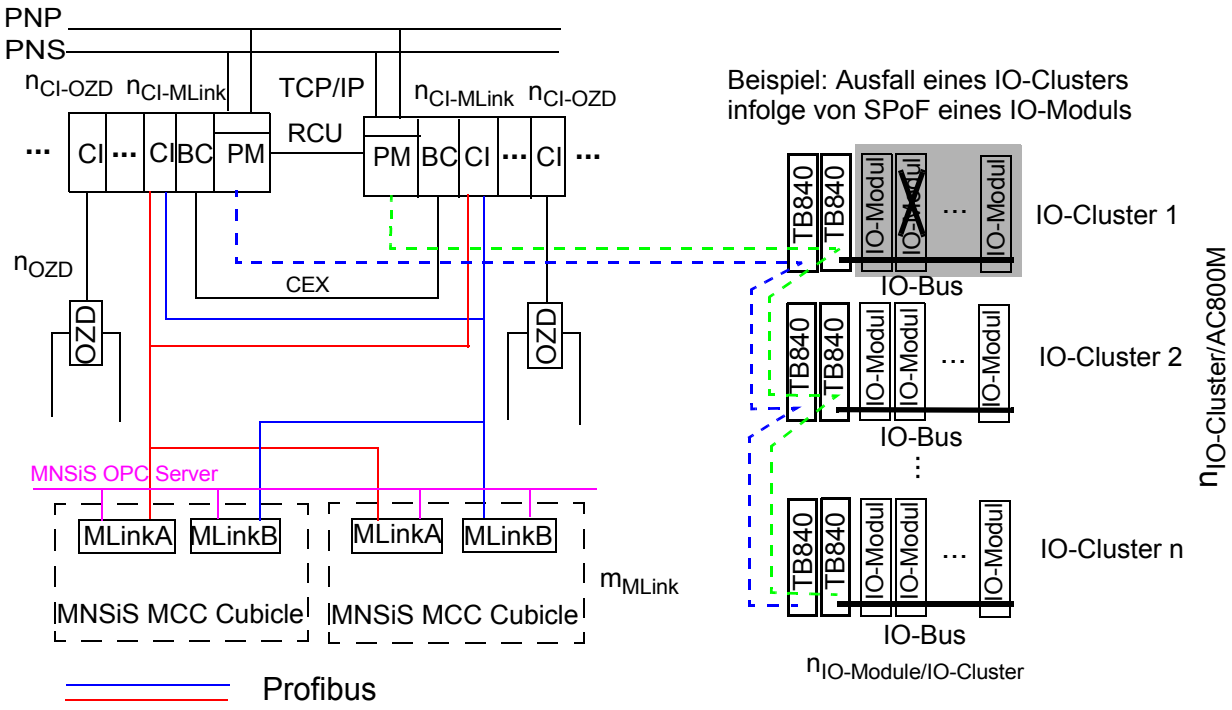
Zuverlässigkeitsblockdiagramm AC800M mit Anschlusskomponenten: Vereinfachte konservative Modellbildung, siehe Anhang U. Für die redundanten Teilsysteme werden die Modelle im Anhang G und H zu Grunde gelegt.

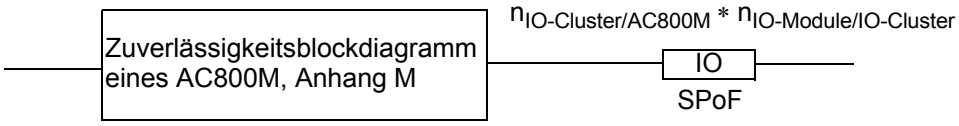
Anhang N: Fehlerbaum für die Controller AC800M mit Anschlusskomponenten (Zuverlässigkeitsblockdiagramm, Anhang M).



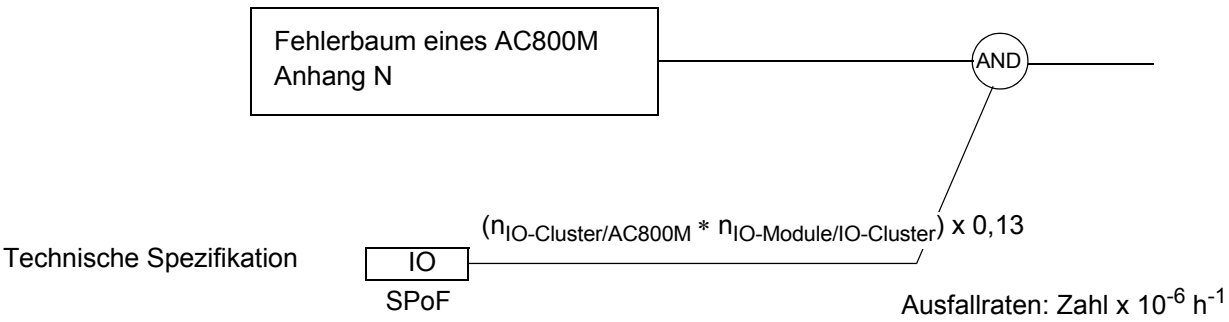
Bezugnahme auf Dokumente, Kapitel 1

Anhang O: Ergänzung der Modelle zur Berücksichtigung des Ausfalls eines IO-Clusters infolge von SPoF von IO-Modulen.





Zuverlässigkeitsblockdiagramm AC800M mit S800 I/O zur Berechnung des Betriebs- und Ausfallverhaltens eines IO-Clusters.



Bezugnahme auf Dokumente, Kapitel 1

Fehlerbaum AC800M mit S800 I/O zur Berechnung des Betriebs- und Ausfallverhaltens eines IO-Clusters.

Anhang P: Beispielrechnung MS21 (A0CRC30): AC800M mit 7 IO-Cluster.

Berechnung nach Anhang N, Fehlerbaum, alle Zahlen x 10^{-6} h^{-1}:

λ_1 = 1,0 + 2,4 + 0,2 + (n_{CI} = 3) ∗ 5,4 + (m_{MLink} = 2) ∗ 7,61 + (n_{OZD} = 1) ∗ 3,34
= 38,36 (oberer gestrichelt eingerahmter weißer Block, Anhang N)

$\lambda_2 = \lambda_1$ (redundanter Teil des Fehlerbaumes, grau)

$\lambda_{AC800M\ (red)}$ = 2,15 (aus Firmenunterlagen ermittelt, 7 Cluster, SV)

$\lambda_{SPoF/AC800M}$ = 0,07 + 0,02 + (n_{CI} = 3) ∗ 0,4 + (m_{MLink} = 2) ∗ 0,15 = 1,59 (Anhang N)

Anhang O, Ergänzung des Fehlerbaumes, siehe auch Excel-Tabelle:

$\lambda_{SPoF/IO}$ = ($n_{IO\text{-}Cluster}$ = 7) ∗ ($n_{IO\text{-}Module}$ = 8) ∗ 0,13 ∗ (Wichtungsfaktor: $1/n_{IO\text{-}Cluster}$ = 1/7) = 1,04

Anhang H, Modellberechnung:

$$H(MZ_4) \approx \frac{\lambda_1\lambda_2}{\mu_1} + \frac{\lambda_1\lambda_2}{\mu_2} + \lambda_{SPoF}$$

$H(MZ_4) \approx 2 * \lambda^2 * MTTR + \lambda_{AC800M\ (red)} + \lambda_{SPoF/AC800M} + \lambda_{SPoF/IO} =$

$2 * (38{,}36 * 10^{-6}\ h^{-1})^2 * 8\ h$ +	(redundante Komponenten) [1]
$2{,}15 * 10^{-6}\ h^{-1}$ +	(AC800M red. [2])
$1{,}59 * 10^{-6}\ h^{-1}$ +	(SPoF/AC800M)
$1{,}04 * 10^{-6}\ h^{-1}$ =	(SPoF/IO)
$2{,}35 * 10^{-8}\ h^{-1}$ +	(redundante Komponenten) [1]
$2{,}15 * 10^{-6}\ h^{-1}$ +	(AC800M red. [2])
$2{,}63 * 10^{-6}\ h^{-1}$ =	(SPoF/AC800M + SPoF/IO)
$4{,}80 * 10^{-6}\ h^{-1}$	(siehe Excel-Tabelle, MS21)

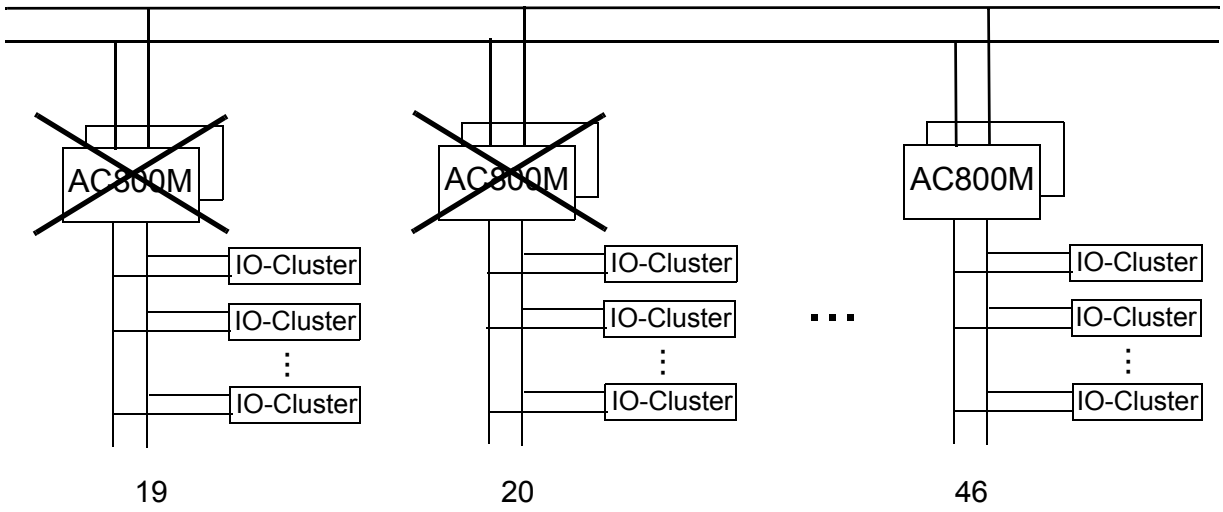
$$P(MZ_4) \approx \frac{\lambda_1\lambda_2}{\mu_1\mu_2} + \frac{\lambda_{SPoF}}{\mu}$$

$P(MZ_4) \approx (\lambda * MTTR)^2 + \lambda_{AC800M+SV+7Cluster} * MTTR +$
$+ \lambda_{SPoF/AC800M} * MTTR + \lambda_{SPoF/IO} * MTTR_{IO} =$

$(38{,}36 * 10^{-6}\ h^{-1} * 8\ h)^2$ +	(redundante Komponenten) [1]
$2{,}15 * 10^{-6}\ h^{-1} * 8\ h$ +	(AC800M red. [2])
$1{,}59 * 10^{-6}\ h^{-1} * 8\ h$ +	(SPoF/AC800M)
$1{,}04 * 10^{-6}\ h^{-1} * 2\ h$ =	(SPoF/IO)
$9{,}42 * 10^{-8}$ +	(redundante Komponenten) [1]
$1{,}72 * 10^{-5}$ +	(AC800M red. [2])
$1{,}27 * 10^{-5}$ +	(SPoF/AC800M)
$2{,}08 * 10^{-6}$ =	(SPoF/IO)
$3{,}21 * 10^{-5}$	(siehe Excel-Tabelle, MS21)

1) Der unabhängige Ausfall der redundanten Komponenten (mit $2{,}35 * 10^{-8}\ h^{-1}$ und $9{,}42 * 10^{-8}$) der AC800M (Anhang N, oberer gestrichelt eingerahmter weißer Bereich und grauer Bereich) ist vernachlässigbar.
2) ohne Ausfälle von IO-Modulen

Anhang Q: Minimalschnitte 2. Ordnung aus Kombinationen von AC800M Ausfällen.



Minimalschnitte 2. Ordnung

$$A_{2xAC800M} = \bigvee_{\substack{\text{für alle } i, j = 19 \ldots 46 \\ \text{und } j > i}} A_{AC800M\ i} \wedge A_{ACM800M\ j}$$

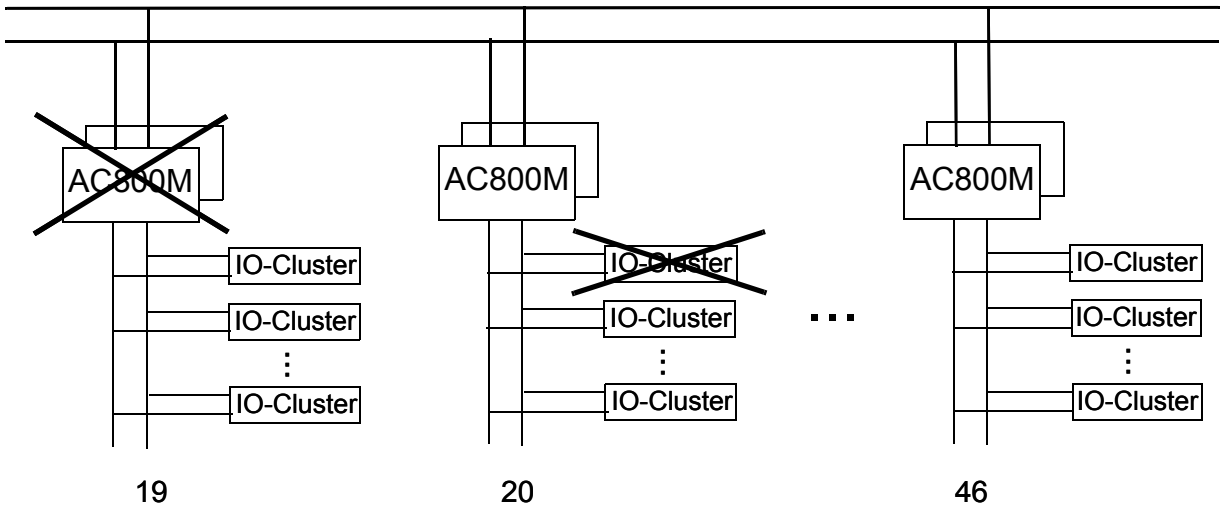
$$P(A_{2xAC800M}) = \frac{M * (M - 1)}{1 * 2} * P(A_{AC800M\text{-}Anhang\ P})^2$$

mit M = 28 und $P(A_{AC800M\text{-}Anhang\ P}) < 3{,}3 * 10^{-5}$ folgt

$$\mathbf{P(A_{alle\ 2xAC800M}) < 4{,}12 * 10^{-7}}$$

Alle Minimalschnitte 2. Ordnung sind somit vernachlässigbar.

Anhang R: Minimalschnitte 2. Ordnung aus Kombinationen von AC800M Ausfall und IO-Clusterausfall.



Minimalschnitte 2. Ordnung

$$A_{AC800M+IO\text{-}Cluster} = \bigvee_{i=19}^{46} A_{AC800M\ i} \wedge \bigvee_{\substack{\text{für alle } k,j \\ k = 19, \ldots, 46 \text{ und } k \neq i \\ j = 1, \ldots, n_{IO\text{-}Cluster/AC800M}}} A_{IO\text{-}Cluster\ k,j}$$

$$P(A_{AC800M+IO\text{-}Cluster}) = M * P(A_{AC800M\text{-}Anhang\ P}) * (M - 1) * * n_{IO\text{-}Cluster/AC800M} * P(A_{IO\text{-}Cluster})$$

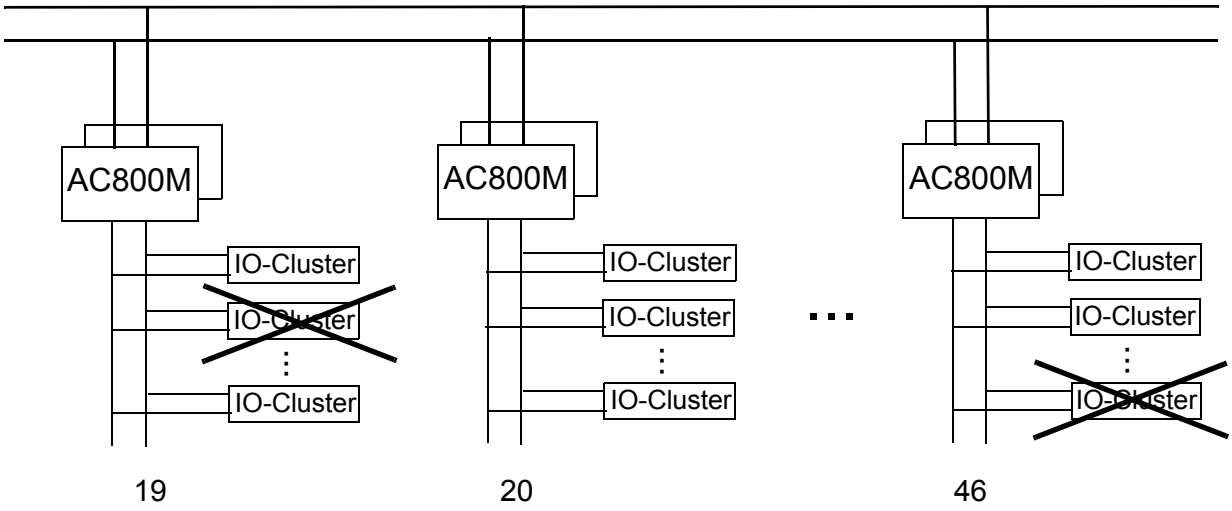
mit $M = 28$, $P(A_{AC800M\text{-}Anhang\ P}) < 3{,}3 * 10^{-5}$, $n_{IO\text{-}Cluster/AC800M} =$ 5 (Mittelwert: 131/28),

$P(A_{IO\text{-}Cluster}) = n_{IO\text{-}Module/IO\text{-}Cluster} * 0{,}13 * 10^{-6}\ h^{-1} * MTTR_{IO\text{-}Modul}$
und $n_{IO\text{-}Module/IO\text{-}Cluster} = 8$ (Annahme), $MTTR_{IO\text{-}Modul} = 2$ Stunden, folgt:

$P(A_{alle\ AC800M+IO\text{-}Cluster}) < 2{,}59 * 10^{-7}$

Alle Minimalschnitte 2. Ordnung sind somit vernachlässigbar.

Anhang S: Minimalschnitte 2. Ordnung aus Kombinationen von IO-Clusterausfällen.



Minimalschnitte 2. Ordnung

$$A_{2xIO\text{-}Cluster} = \bigvee_{\substack{\text{alle } i \\ i,j = 1,\ldots,n_{IO\text{-}Cluster\text{-}gesamt} \\ \text{und } j > i}} A_{IO\text{-}Cluster\ i} \wedge \bigvee_{\text{alle } j} A_{IO\text{-}Cluster\ j}$$

$$P(A_{2xIO\text{-}Cluster}) = \frac{n_{IO\text{-}Cluster\text{-}gesamt} * (n_{IO\text{-}Cluster\text{-}gesamt} - 1)}{1 * 2} * P(A_{IO\text{-}Cluster})^2$$

mit $n_{IO\text{-}Cluster\text{-}gesamt} = 131$, $P(A_{IO\text{-}Cluster}) = n_{IO\text{-}Module/IO\text{-}Cluster} * 0{,}13 * 10^{-6}\ h^{-1} * * MTTR_{IO\text{-}Modul}$,

$n_{IO\text{-}Module/IO\text{-}Cluster} = 8$ (Mittelwert), $MTTR_{IO\text{-}Modul} = 2$ Stunden, folgt:

$P(A_{alle\ 2xIO\text{-}Cluster}) = 3{,}68 * 10^{-8}$

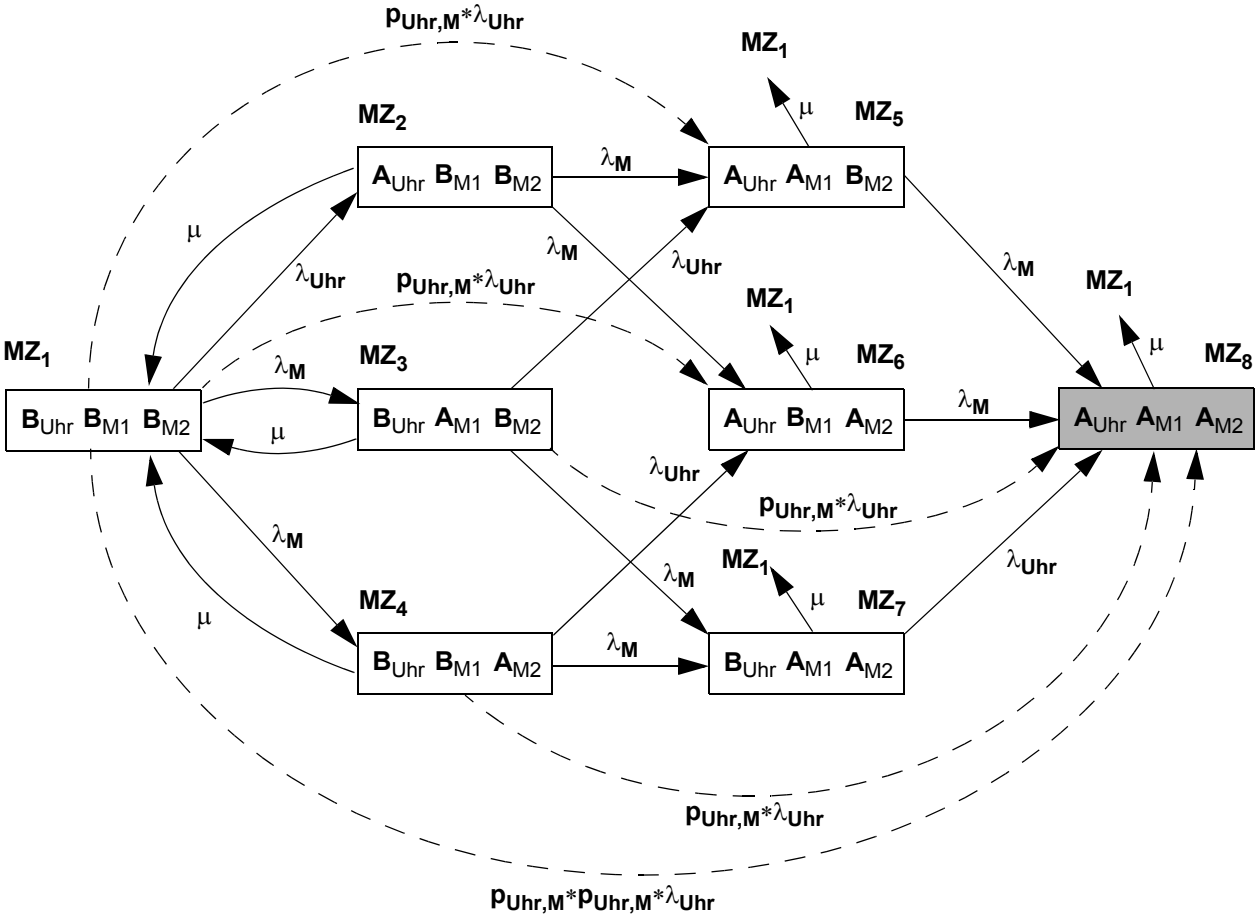
Alle Minimalschnitte 2. Ordnung sind auch hier vernachlässigbar.

Fazit:

Alle Minimalschnitte 1. Ordnung (mit eingebetteter Redundanz) sind im Anhang B bis E angegeben. Dies sind die relevanten Minimalschnitte.

Alle Minimalschnitte höherer als 1. Ordnung aus Ausfallkombinationen von AC800M und/oder IO-Cluster sind in Summe vernachlässigbar.

Anhang T: Markov Modell des Systemuhrzeit-Systems.



Innerhalb der MZ sind die Zustände logische UND verknüpft.

$p_{Uhr,M}$ bezeichnet den CCF (ß-Faktor), das ist die Wahrscheinlichkeit eines gemeinsamen Ausfalls von Uhr und Master M für den Fall, dass die Uhr ausfällt und M die Systemuhrzeit übernehmen soll und dabei gleichzeitig ausfällt.

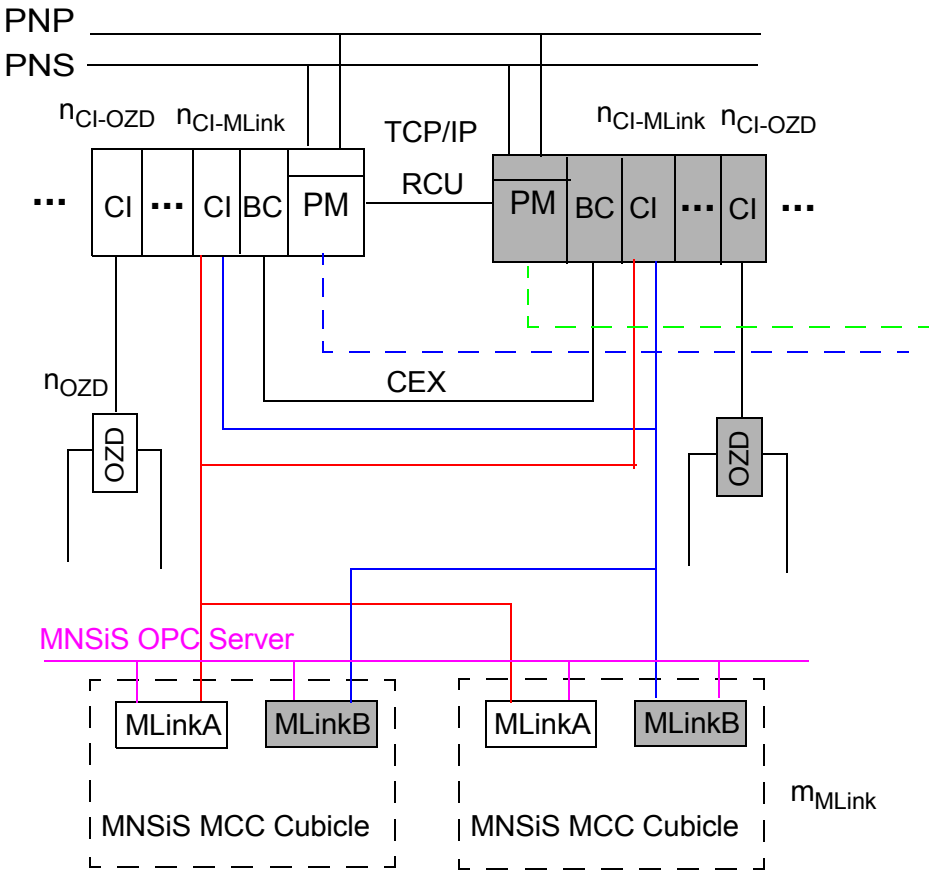
Mittlere Häufigkeit $H(MZ_8)$ und Wahrscheinlichkeit $P(MZ_8)$ eines Totalausfalls der Uhrzeit (berechnet mit dem Verfahren der Wahrscheinlichen Markov Wege)

$$H(MZ_8) \approx 6*\frac{\lambda_{Uhr}}{\mu}\frac{\lambda_M}{\mu}\lambda_M + 4*p_{Uhr,M}\frac{\lambda_{Uhr}}{\mu}\lambda_M + p_{Uhr,M}*p_{Uhr,M}\lambda_{Uhr}$$

$$P(MZ_8) \approx \underbrace{6*\frac{\lambda_{Uhr}}{\mu}\frac{\lambda_M}{\mu}\frac{\lambda_M}{\mu}}_{\text{unabhängige Ausfälle}} + \underbrace{4*p_{Uhr,M}\frac{\lambda_{Uhr}}{\mu}\frac{\lambda_M}{\mu}}_{\text{einfach CCF (Common Cause Fehler -> Common Cause Ausfall)}} + \underbrace{p_{Uhr,M}*p_{Uhr,M}\frac{\lambda_{Uhr}}{\mu}}_{\text{zweifach CCF (Common Cause Fehler -> Common Cause Ausfall)}}$$

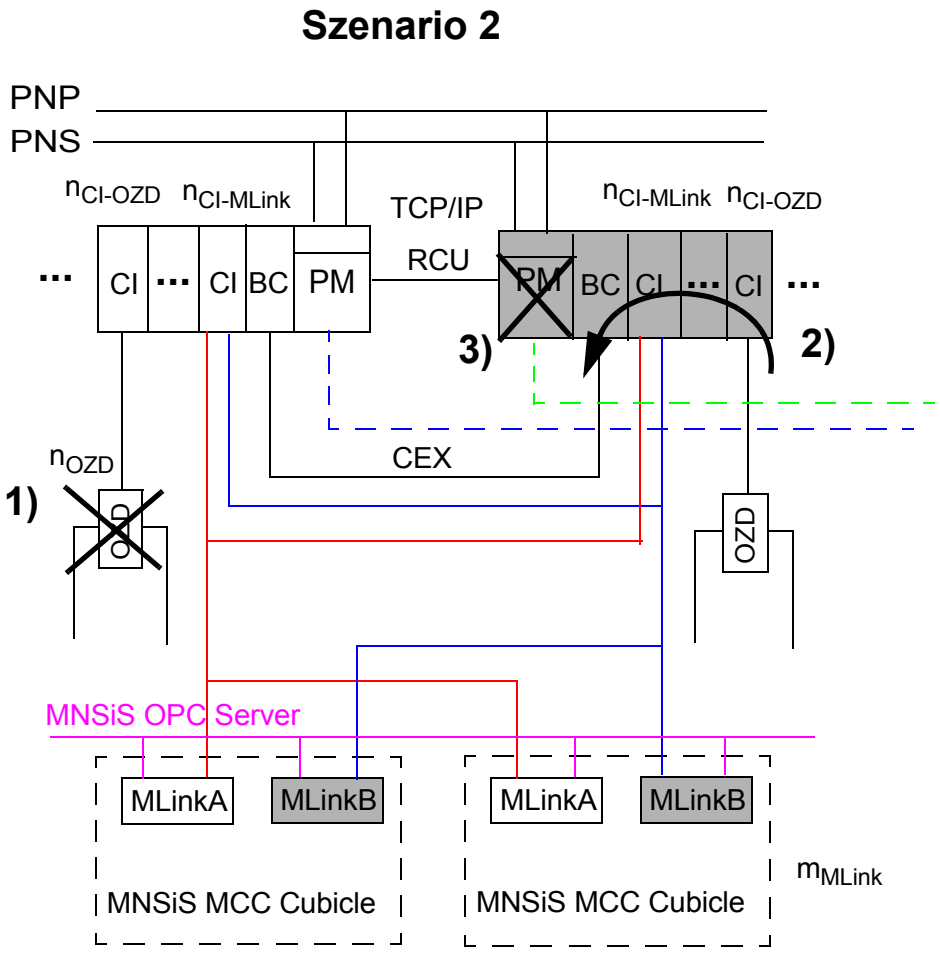
Anhang U: Beispiele für konservative Zuverlässigkeitsmodellierung einer komplexen Subsystemstruktur für Anhang M, N, O.

Szenario 1: Fehlerfreier Systembetrieb



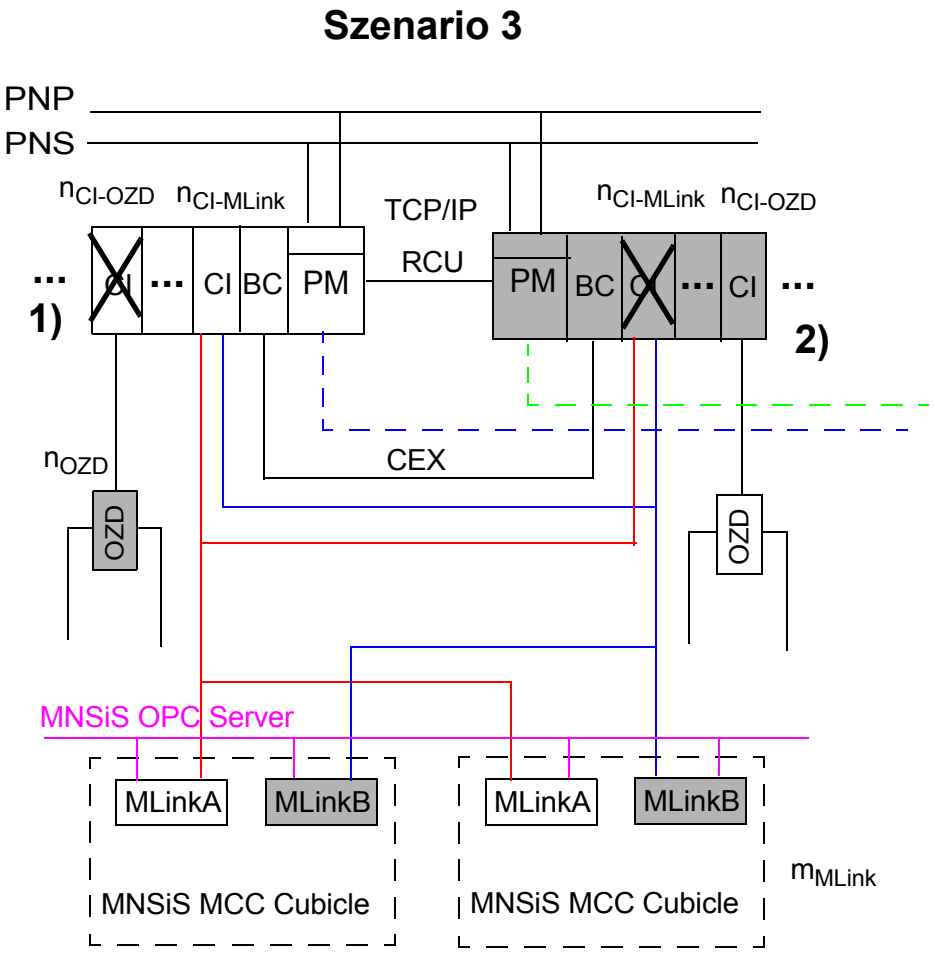
Szenario 1: Fehlerfreier Systembetrieb: Komponenten auf der linken Seite: in Betrieb, Komponenten auf der rechten Seite (grau): in Reserve (stand-by). Für die folgenden Szenarien ist Szenario 1 das Ausgangsszenario.

Anhang U: Beispiele für konservative Zuverlässigkeitsmodellierung einer komplexen Subsystemstruktur für Anhang M, N, O.



Szenario 2: Fehlerhafter Systembetrieb: Ausfall der Komponente 1) OZD. OZD auf der anderen Seite übernimmt die Funktion, Informationen werden über 2) BC810 über CEX an den linken Rechner PM geleitet (keine Redundanzumschaltung der Rechner PM866). Würde dann z.B. 3) PM866 ausfallen, bliebe das ohne Auswirkungen. Die linke Seite führt nach wie vor den Systembetrieb weiter. Das System fällt **nicht** aus.

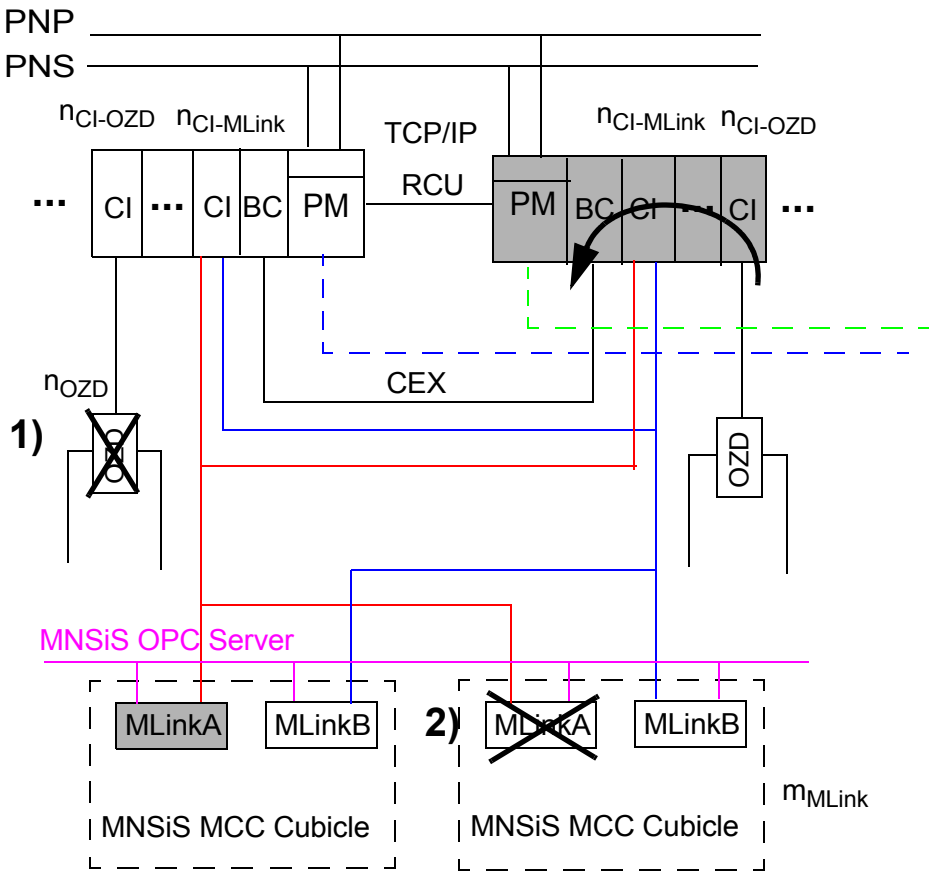
Anhang U: Beispiele für konservative Zuverlässigkeitsmodellierung einer komplexen Subsystemstruktur für Anhang M, N, O.



Szenario 3: Fehlerhafter Systembetrieb: Ausfall der Komponenten in der Reihenfolge 1), 2). Das System fällt **nicht** aus.

Anhang U: Beispiele für konservative Zuverlässigkeitsmodellierung einer komplexen Subsystemstruktur für Anhang M, N, O.

Szenario 4



Szenario 4: Fehlerhafter Systembetrieb: Ausfall der Komponenten in der Reihenfolge 1), 2). Alle m_{MLink} MLinkA am Controller werden auf MLinkB umgeschaltet. Das System fällt **nicht** aus.

Die Szenarien 2 bis 4 sind Beispiele von komplexen Ausfallkombinationen, in denen das System zwar fehlerhaft ist, jedoch der Systemausfall **nicht** eintritt.

In der **konservativen** Zuverlässigkeitsmodellierung (Anhang M, unteres Zuverlässigkeitsblockdiagramm) werden jedoch solche Ausfallkombinationen als Systemausfall gewertet. Damit liegt die Berechnung auf der sicheren Seite.

Anhang V: Zuverlässigkeits-/Verfügbarkeitsberechnung (Excel)

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
Berechnung von λ_{BS} für MS1	**BS** 4 Bedienstationen A0CRU10 A0CRU20 A0CRU30 A0CRU40 + 3 Bedienstationen mit je 1 Beamer A0CRU50 A0CRP60 A0CRP70	1		für jede der 4 red. Bedienstationen gilt: (red. MMI)1,2+ (Rechner)26,53+ (MMI Control U)29,65 = 57,38 = λ, damit folgt nach Anhang B und L: H(3oo4): λ_{BS} = $6*(\lambda/\mu)^2 * 2*\mu$ =	3,16E-07						8,00E+00	1,25E-01	Rechner: 37.700 h, **Teilsystem: 3oo4**, 3-out-of-4 sollen funktio-nieren. Anhang L
Berechnung von λ_{ES} für MS1	**ES** Engineering Station 1 + 2 A0CRV10 A0CRU20	1		für jede der 2 red. Bedienstationen gilt: (red. MMI)1,2+ (Rechner)26,53+ (MMI Control U)29,50 = 57,23 = λ, damit folgt nach Anhang B und L H(1oo2): λ_{ES} = $(\lambda/\mu)^2 * 2*\mu$	5,24E-08						8,00E+00	1,25E-01	Rechner: 37.700 h, **Teilsystem: 1oo2**, 1-out-of-2 sollen funktio-nieren. Anhang L
MS1 BS+ES	Bedien- und Engineeringsystem **BS+ES**	1									8,00E+00	1,25E-01	Modellierung und Berechnung erfolgen nach Anhang B und Anhang I mit den Ergebnissen der Ausfallraten der beiden vorherigen Zeilen **BS** und **ES** (Spalte 5)
MS2 Sys.Uhr	Systemuhr A0CYF10	1		Annahmen: $\lambda_{Syst.Uhr} < 1*10^{-5}h^{-1}$, $\lambda_{Master1} < 1*10^{-5}h^{-1}$, $\lambda_{Master2} < 1*10^{-5}h^{-1}$, CCF (ß-) Faktor 2%							8,00E+00	1,25E-01	Bei Ausfall der Systemuhr übernimmt ein Master die Systemuhrzeit, wenn dieser ausfällt der nächste Master. Es stehen 2 Master zur Übernahme der Systemuhrzeit zur Verfügung. Deshalb ist dieses Teilsystem zweifach redundant und grundsätzlich hoch zuverlässig. Modellierung und Berechnung erfolgen nach Anhang T.

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
Berechnung von λ_{BS} für MS1											
Berechnung von λ_{ES} für MS1											
MS1 BS+ES	$\lambda_{BS} + (\lambda_{ES}\lambda_{BS})/\mu_{ES}$	3,16E-07	$\lambda_{BS}/\mu_{BS} + (\lambda_{ES}\lambda_{BS})/(\mu_{ES}\mu_{BS})$	2,53E-06						3,16E-07	2,53E-06
MS2 Sys.Uhr	Formel Anhang T	4,06E-09	Formel Anhang T	3,25E-08						4,06E-09	3,25E-08

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS3 Domain	Domain Server (redundant) A0CRQ10/20	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).
MS4 Anwend	Anwendungs Server (redundant) A0CRQ30/40	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).
MS5 Aspect	Aspect Server (redundant) A0CRN10/20	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).
MS6 Connec1	Connectivity Server 1 (redundant) A0CRP10/20	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).
MS7 Connec2	Connectivity Server 2 (redundant) A0CRP30/40	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).
MS8 Connec3	Connectivity Server 3 (redundant) A0CRP50/60	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS3 Domain	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06
MS4 Anwend	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06
MS5 Aspect	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06
MS6 Connec1	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06
MS7 Connec2	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06
MS8 Connec3	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS9 PGIM Archiv	PGIM Archiv Server (redundant) A0CRX10/20	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h, Redundanzfehler geschätzt 2% (CCF-Faktor, Beta-Faktor 0,02).
MS10 PGIM Anw	PGIM Anwendungs Server (einfach) A0CRX30	0,5		(Rechner einfach)12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.
MS11 ANP/ANS	Anlagen Switch ANP/ANS	1		(24 Port Gigabit Switch)5,3	5,30E-06						Instand-setzungsdauer = 8 h Hochfahrdauer des Systems inkl.Rep. = 8 h	1,25E-01	2 x 3 Switche, 24 port Gigabit Switch: 187.805 h Bei Fehlern in einem Switch am ANP/PNP wird automatisch auf die Switche am ANS/PNS umgeschaltet. Alle Switche werden permanent überwacht und Fehler gemeldet (managed switch). Bei Totalausfall dauert das Hochfahren des gesamten Systems $T_{Rep+HochfSyst}$ (= 1/ $\mu_{Rep+HochfSyst}$). **Teilsystem Markov 1oo2**, Anhang J, K
MS12 PNP/PNS	Prozess Switch PNP/ANP	1		(24 Port Gigabit Switch)5,3	5,30E-06						Instand-setzungsdauer = 8 h Hochfahrdauer des Systems inkl.Rep = 8 h	1,25E-01	2 x 6 Switche. Spezifikation wie vorherige Zeile. **Teilsystem Markov 1oo2,** Anhang J, K
MS13 Asset	Asset Monitor (Wartung) (redundant) A0CRP70/80	1		(Rechner einfach)12,87, SPoF: Fehler Red.Umsch. geschätzt 0,02*12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS9 PGIM Archiv	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,60E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,60E-07	2,07E-06
MS10 PGIM Anw	Spalte 5 Ausfallrate zugrunde gelegt λ/h-1	6,44E-06	λ/μ	5,15E-05						6,44E-06	5,15E-05
MS11 ANP/ANS	Anhang J + K $18*(\lambda/\mu)^2*\mu$	4,04E-09	Anhang J + K $18*(\lambda/\mu)^2*(\mu/\mu_{Rep+HochfSyst})$	3,24E-08						4,04E-09	3,24E-08
MS12 PNP/PNS	Anhang J + K $72*(\lambda/\mu)^2*\mu$	1,62E-08	Anhang J + K $72*(\lambda/\mu)^2*(\mu/\mu_{Rep+HochfSyst})$	1,29E-07						1,62E-08	1,29E-07
MS13 Asset	Anhang H: $(\lambda/\mu)^2*2*\mu + \lambda_{SPoF}$	2,61E-07	Anhang H: $(\lambda/\mu)^2 + \lambda_{SPoF}/\mu$	2,07E-06						2,61E-07	2,07E-06

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS14 OPC1	MNSiS OPC Server A0CRP51	0,25		(Rechner einfach)12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.
MS15 OPC2	MNSiS OPC Server A0CRP52	0,25		(Rechner einfach)12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.
MS16 OPC3	MNSiS OPC Server A0CRP53	0,25		(Rechner einfach)12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.
MS17 OPC4	MNSiS OPC Server A0CRP54	0,25		(Rechner einfach)12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.
MS18 EMI	EMI Rechner Emission Monitoring (einfach) A0CRV40	1		(Rechner einfach)12,87	1,29E-05						8,00E+00	1,25E-01	Rechner: effective MTBF: 77.700 h.
MS19 GB LT	A0CRC10	0,5	0,4+ (PM/TCP)0,07+ (BC)0,02		4,90E-07	1	8	0	0	0	8,00E+00	1,25E-01	ACM800M red., 1 I/O-Cluster, Anhang M - S.
MS20 MS Schlt.Anl.	A0CRC20	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,79E-06	6	8	2	0	0	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.
MS21 WDK1	A0CRC30	1	2,15+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,74E-06	7	8	3	2	1	8,00E+00	1,25E-01	ACM800M red., 7 I/O-Cluster, Anhang M - S.
MS22 WDK2	A0CRC40	1	2,15+ (PM/TCP)0,07+ (BC) 0,02+ n-CIx0,4+ m-MLink*0,15		3,34E-06	7	8	2	2	0	8,00E+00	1,25E-01	ACM800M red., 7 I/O-Cluster, Anhang M - S.

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS14 OPC1	Spalte 5 Ausfallrate zugrunde gelegt λ/h-1	3,22E-06	λ/μ	2,57E-05						3,22E-06	2,57E-05
MS15 OPC2	Spalte 5 Ausfallrate zugrunde gelegt λ/h-1	3,22E-06	λ/μ	2,57E-05						3,22E-06	2,57E-05
MS16 OPC3	Spalte 5 Ausfallrate zugrunde gelegt λ/h-1	3,22E-06	λ/μ	2,57E-05						3,22E-06	2,57E-05
MS17 OPC4	Spalte 5 Ausfallrate zugrunde gelegt λ/h-1	3,22E-06	λ/μ	2,57E-05						3,22E-06	2,57E-05
MS18 EMI	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,22E-06	λ/μ	1,03E-04						3,22E-06	1,03E-04
MS19 GB LT	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,45E-07	λ/μ	1,96E-06	1,00	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	5,20E-07	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	1,04E-06	7,65E-07	3,00E-06
MS20 MS Schlt.Anl.	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,79E-06	λ/μ	2,23E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,83E-06	2,44E-05
MS21 WDK1	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,74E-06	λ/μ	2,99E-05	0,14	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,78E-06	3,20E-05
MS22 WDK2	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,34E-06	λ/μ	2,67E-05	0,14	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,38E-06	2,88E-05

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS23 WDK3	A0CRC50	1	1,15+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,04E-06	3	8	3	4	1	8,00E+00	1,25E-01	ACM800M red., 3 I/O-Cluster, Anhang M - S.
MS24 NS11	A0CRC60	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,39E-06	6	8	1	0	0	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.
MS25 NS12	A0CRC65	1	0,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		1,39E-06	2	8	1	0	2	8,00E+00	1,25E-01	ACM800M red., 2 I/O-Cluster, Anhang M - S.
MS26 NS21	A0CRC70	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,39E-06	6	8	1	0	0	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.
MS27 NS22	A0CRC80	1	1,65+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,14E-06	5	8	1	0	0	8,00E+00	1,25E-01	ACM800M red., 5 I/O-Cluster, Anhang M - S.
MS28 Anlieferung	A0CRC90	1	1,4+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		1,49E-06	4	8	0	0	0	8,00E+00	1,25E-01	ACM800M red., 4 I/O-Cluster, Anhang M - S.
MS29 SIS W/D	A0CRJ10 Schutz	1	0,9+ (PM/TCP)0,07+ (BC)0,02+	Für AC800M HI PU - Safety werden die konservativen Werte der AC800M PU eingesetzt	9,90E-07	2	8	0	0	0	8,00E+00	1,25E-01	ACM800M red., 2 I/O-Cluster, Anhang M - S. AC800M HI PU - Safety

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS23 WDK3	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,04E-06	λ/μ	2,43E-05	0,33	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,08E-06	2,64E-05
MS24 NS11	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,39E-06	λ/μ	1,91E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,43E-06	2,12E-05
MS25 NS12	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	1,39E-06	λ/μ	1,11E-05	0,50	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	2,43E-06	1,32E-05
MS26 NS21	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,39E-06	λ/μ	1,91E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,43E-06	2,12E-05
MS27 NS22	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,14E-06	λ/μ	1,71E-05	0,20	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,18E-06	1,92E-05
MS28 Anlieferung	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	1,49E-06	λ/μ	1,19E-05	0,25	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	2,53E-06	1,40E-05
MS29 SIS W/D	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	9,90E-07	λ/μ	7,92E-06	0,50	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	2,03E-06	1,00E-05

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS30 FKS Allg.	K0CRC10	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,49E-06	6	8	3	2	1	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.
MS31 RGR Allg.	Rauchgasreinigung allg. R0CRC10	1	1,4+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,89E-06	4	8	2	4	1	8,00E+00	1,25E-01	ACM800M red., 4 I/O-Cluster, Anhang M - S.
MS32 FKS1/1	K1CRC10	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,49E-06	6	8	3	2	1	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.
MS33 FKS1/2	K1CRC20	1	1,65+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,84E-06	5	8	2	2	0	8,00E+00	1,25E-01	ACM800M red., 5 I/O-Cluster, Anhang M - S.
MS34 FKS1/3	K1CRC30	1	1,4+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,84E-06	4	8	3	1	1	8,00E+00	1,25E-01	ACM800M red., 4 I/O-Cluster, Anhang M - S.
MS35 RGR1	R1CRC10	1	2,15+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,64E-06	7	8	2	4	2	8,00E+00	1,25E-01	ACM800M red., 7 I/O-Cluster, Anhang M - S.
MS36 SIS1	K1CRJ10 Schutz	1	0,9+ (PM/TCP)0,07+ (BC)0,02+	Für AC800M HI PU - Safety werden die konservativen Werte der AC800M PU eingesetzt	9,90E-07	2	8	0	0	0	8,00E+00	1,25E-01	ACM800M red., 2 I/O-Cluster, Anhang M - S. AC800M HI PU - Safety N35
MS37 FKS2/1	K2CRC10	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,49E-06	6	8	3	2	1	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS30 FKS Allg.	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,49E-06	λ/μ	2,79E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,53E-06	3,00E-05
MS31 RGR Allg.	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,89E-06	λ/μ	2,31E-05	0,25	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,93E-06	2,52E-05
MS32 FKS1/1	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,49E-06	λ/μ	2,79E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,53E-06	3,00E-05
MS33 FKS1/2	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,84E-06	λ/μ	2,27E-05	0,20	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,88E-06	2,48E-05
MS34 FKS1/3	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,84E-06	λ/μ	2,27E-05	0,25	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,88E-06	2,48E-05
MS35 RGR1	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,64E-06	λ/μ	2,91E-05	0,14	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,68E-06	3,12E-05
MS36 SIS1	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	9,90E-07	λ/μ	7,92E-06	0,50	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	2,03E-06	1,00E-05
MS37 FKS2/1	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,49E-06	λ/μ	2,79E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,53E-06	3,00E-05

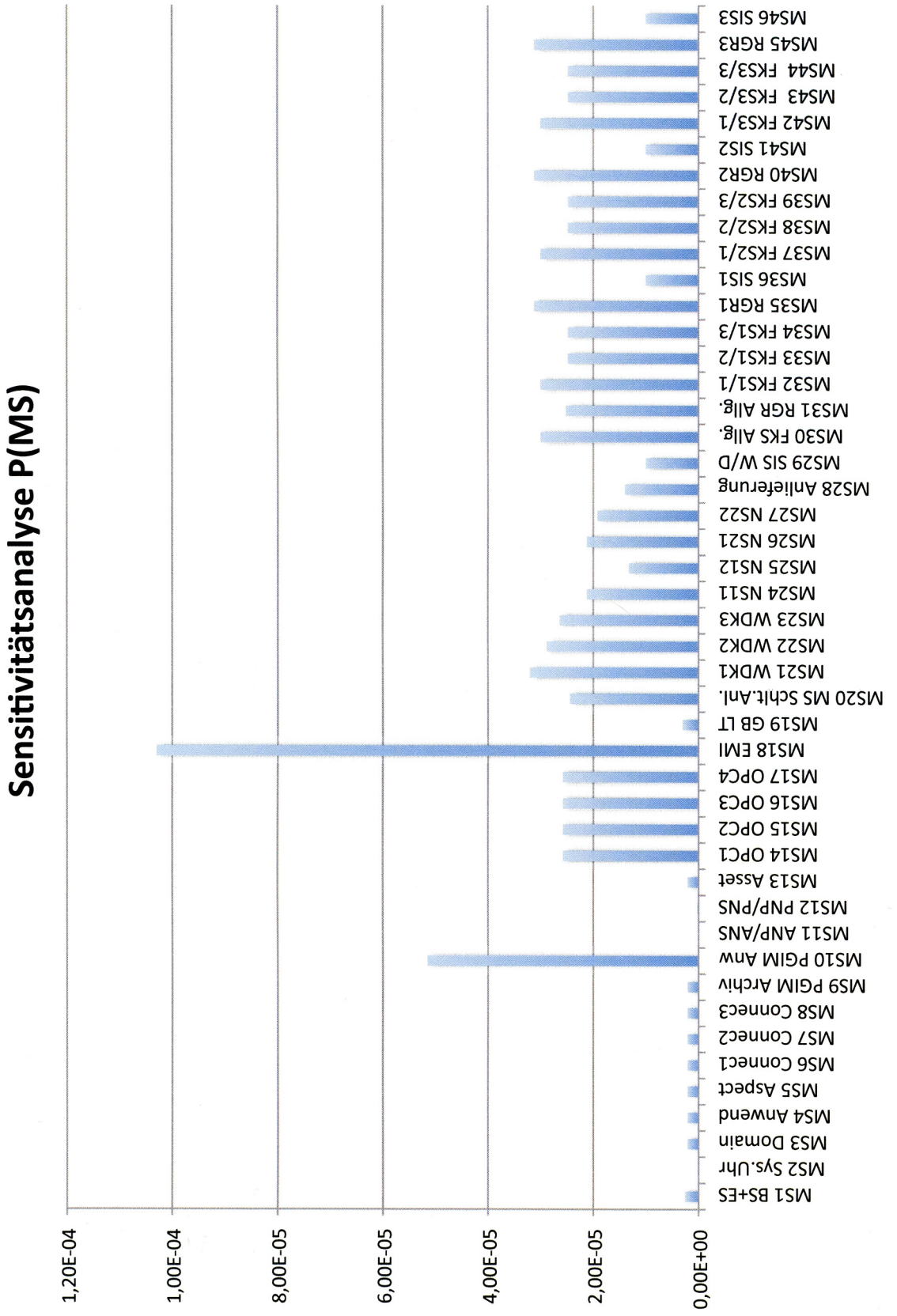
Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS38 FKS2/2	K2CRC20	1	1,65+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,84E-06	5	8	2	2	0	8,00E+00	1,25E-01	ACM800M red., 5 I/O-Cluster, Anhang M - S.
MS39 FKS2/3	K2CRC30	1	1,4+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,84E-06	4	8	3	1	1	8,00E+00	1,25E-01	ACM800M red., 4 I/O-Cluster, Anhang M - S.
MS40 RGR2	R2CRC10	1	2,15+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,64E-06	7	8	2	4	2	8,00E+00	1,25E-01	ACM800M red., 7 I/O-Cluster, Anhang M - S.
MS41 SIS2	K2CRJ10 Schutz	1	0,9+ (PM/TCP)0,07+ (BC)0,02	Für AC800M HI PU - Safety werden die konservativen Werte der AC800M PU eingesetzt	9,90E-07	2	8	0	0	0	8,00E+00	1,25E-01	ACM800M red., 2 I/O-Cluster, Anhang M - S. AC800M HI PU - Safety
MS42 FKS3/1	K3CRC10	1	1,9+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,49E-06	6	8	3	2	1	8,00E+00	1,25E-01	ACM800M red., 6 I/O-Cluster, Anhang M - S.
MS43 FKS3/2	K3CRC20	1	1,65+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,84E-06	5	8	2	2	0	8,00E+00	1,25E-01	ACM800M red., 5 I/O-Cluster, Anhang M - S.
MS44 FKS3/3	K3CRC30	1	1,4+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		2,84E-06	4	8	3	1	1	8,00E+00	1,25E-01	ACM800M red., 4 I/O-Cluster, Anhang M - S.
MS45 RGR3	R3CRC10	1	2,15+ (PM/TCP)0,07+ (BC)0,02+ n-CIx0,4+ m-MLink*0,15		3,64E-06	7	8	2	4	2	8,00E+00	1,25E-01	ACM800M red., 7 I/O-Cluster, Anhang M - S.

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS38 FKS2/2	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,84E-06	λ/μ	2,27E-05	0,20	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,88E-06	2,48E-05
MS39 FKS2/3	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,84E-06	λ/μ	2,27E-05	0,25	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,88E-06	2,48E-05
MS40 RGR2	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,64E-06	λ/μ	2,91E-05	0,14	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,68E-06	3,12E-05
MS41 SIS2	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	9,90E-07	λ/μ	7,92E-06	0,50	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	2,03E-06	1,00E-05
MS42 FKS3/1	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,49E-06	λ/μ	2,79E-05	0,17	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,53E-06	3,00E-05
MS43 FKS3/2	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,84E-06	λ/μ	2,27E-05	0,20	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,88E-06	2,48E-05
MS44 FKS3/3	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	2,84E-06	λ/μ	2,27E-05	0,25	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	3,88E-06	2,48E-05
MS45 RGR3	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	3,64E-06	λ/μ	2,91E-05	0,14	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	4,68E-06	3,12E-05

Spalte:	1	2	3	4	5	6	7	8	9	10	11	12	13
Minimal-schnitte	**Bezeichnung**	**Wichtungs-faktor**	**Ausfallrate (Firmenangabe) λredundant / E-6 h-1**	**Ausfallrate geschätzt / andere Quellen λ / E-6 h-1**	**Ausfallrate zugrunde-gelegt λ / h-1**	**n-IO-Cluster**	**n-IO-Module / IO-Cluster**	**n-CI-OZD + n-CI-MLink**	**m-MLink**	**n-OZD**	**Instand-setzungsdauer / Ersatzdauer / h**	**Instand-setzungsrate / Ersatzrate μ / h-1**	**Bemerkungen/Hinweise**
MS46 SIS3	K3CRJ10 Schutz	1	0,9+ (PM/TCP)0,07+ (BC)0,02	Für AC800M HI PU - Safety werden die konservativen Werte der AC800M PU eingesetzt	9,90E-07	2	8	0	0	0	8,00E+00	1,25E-01	ACM800M red., 2 I/O-Cluster, Anhang M - S. AC800M HI PU - Safety
Summe						131		49	41	18			

Spalte:	14	15	16	17	18	19	20	21	22	23	24
Minimal-schnitte	**Mittlere Häufigkeit H(MSi) / h-1**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster H(MSi) / h-1**	**Wahrscheinlich-keit P(MSi)**	**SYSTEM-FUNKTION ohne SPoF-IO-Cluster P(MSi)**	**Wichtungsf. IO-Cluster**		**Ergänzung SPoF-IO-Cluster H(MSi) / h-1**		**Ergänzung SPoF-IO-Cluster P(MSi)**	H(AS) Spalte 15+20	P(AS) Spalte 17+22
MS46 SIS3	Spalte 5 Ausfallrate zugrundegelegt λ/h-1	9,90E-07	λ/μ	7,92E-06	0,50	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1	1,04E-06	Anhang O: Spalte 2 * Spalte 6 * Spalte 7 * Spalte 18 * 0,13*10-6h-1*2 h	2,08E-06	2,03E-06	1,00E-05
Summe		9,67E-05		8,51E-04			2,86E-05		5,72E-05	1,25E-04	9,08E-04
										Verfügbarkeit 1-P(AS)	0,999092

Anlage W: Sensitivitätsanalyse (Excel Diagramm)


Sensitivitätsanalyse P(MS)
1,20E-04
1,00E-04
8,00E-05
6,00E-05
4,00E-05
2,00E-05
0,00E+00
MS1 BS+ES
MS2 Sys.Uhr
MS3 Domain
MS4 Anwend
MS5 Aspect
MS6 Connect1
MS7 Connec2
MS8 Connec3
MS9 PGIM Archiv
MS10 PGIM Anw
MS11 ANP/ANS
MS12 PNP/PNS
MS13 Asset
MS14 OPC1
MS15 OPC2
MS16 OPC3
MS17 OPC4
MS18 EMI
MS19 GB LT
MS20 MS Schlt.Anl.
MS21 WDK1
MS22 WDK2
MS23 WDK3
MS24 NS11
MS25 NS12
MS26 NS21
MS27 NS22
MS28 Anlieferung
MS29 SIS W/D
MS30 FKS Allg.
MS31 RGR Allg.
MS32 FKS1/1
MS33 FKS1/2
MS34 FKS1/3
MS35 RGR1
MS36 SIS1
MS37 FKS2/1
MS38 FKS2/2
MS39 FKS2/3
MS40 RGR2
MS41 SIS2
MS42 FKS3/1
MS43 FKS3/2
MS44 FKS3/3
MS45 RGR3
MS46 SIS3

Executive Summary

Reliability/Availability Evaluation of Industrial Systems - Application to a Process Control System

Abstract

This Executive Summary briefly describes the main steps and results of the detailed system reliability (and availability) evaluation of an industrial process control system. The initial steps 1 to 5 (Figure 1) of the system reliability evaluation include the comprehensive system analysis, the definitions of adequate system functions (system states) as basis for the reliability evaluation, further the definitions of the components and the system, the definition of the preconditions and assumptions, and last but not least the definition, collection, and preparation of reliability input data. For this study extensive reliability data sources as well as component and system specifications were provided by the participating industrial companies. The reliability modeling and calculation (steps 6 and 7) are based on a combination of well-established and further developed analytical approaches such as *Minimal cut approach* with embedded *Markov models (Markov minimal cut approach)*, combined with extensive expert knowledge. All evaluation steps of the reliability analysis are documented step-by-step. Besides the evaluation of overall system reliability indices, the detection of weak points is particularly important (sensitivity analysis).

The described approaches can be applied analogously to many other system structures.

Introduction

The reliability/availability analysis is carried out with the following steps, based on state-of-the-art research and practice, as well as relevant standards.

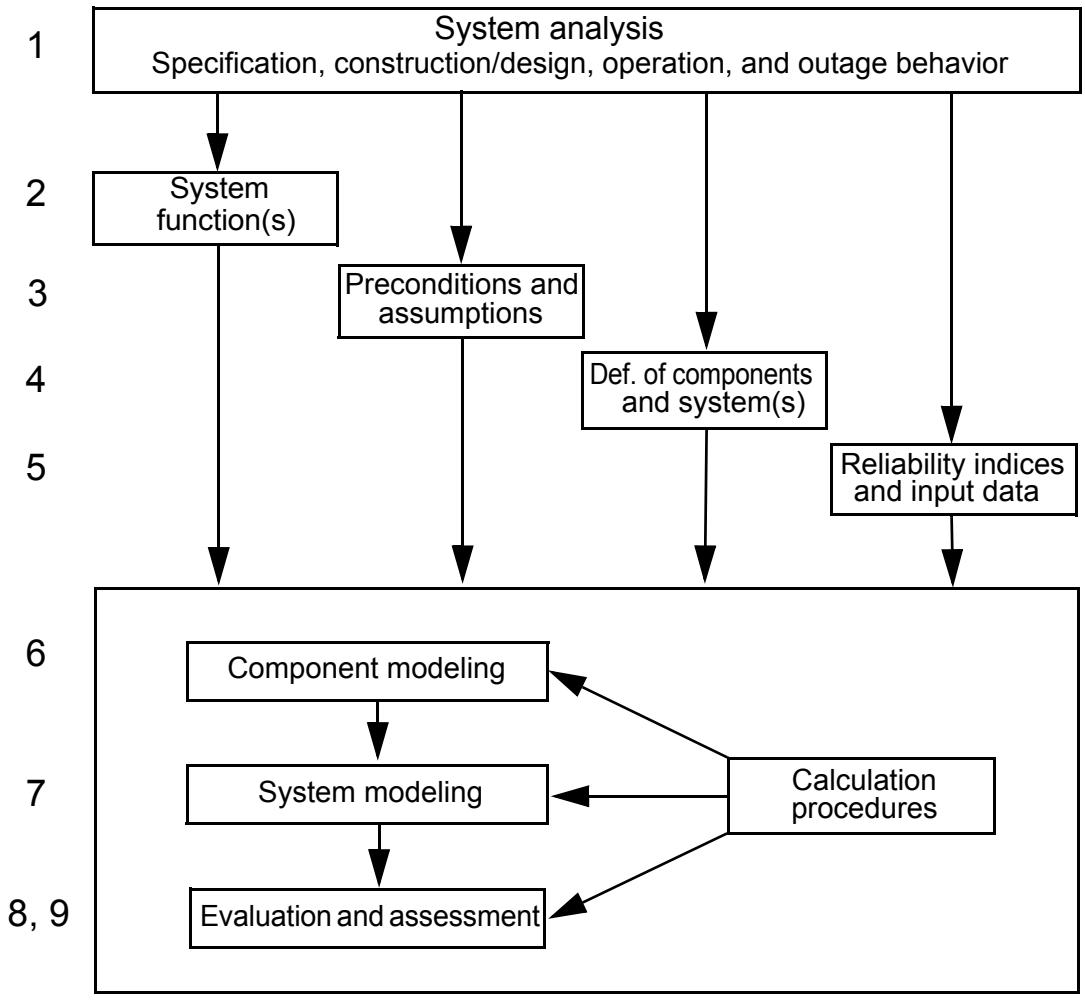


Figure 1: Framework of the system reliability/availability evaluation.

Definition of reliability according to [IEEE 90 1990] and [DKE-IEV 603-05-01 2012].

> **Reliability** is the ability of an item to perform a required function under stated conditions for a specified period of time.

Definition of availability according to [DKE-IEV 191-02-05 2012].

> **Availability** is the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

Note 1: This ability depends on the combined aspects of the reliability performance, the maintainability performance, and the maintenance support performance.

Note 2: Required external resources, others than maintenance resources, do not affect the availability performance of the item.

In this study, reliability performance is exclusively considered (maintenance performance is not part of this report). Thus, the terms reliability and availability are equivalently used. The term ability of an item to perform a required function depends on the definition of the system function (Chapter 2) under given conditions (Chapter 3), related to the defined item (consideration unit), which can be a component or a system (Chapter 4). Reliability can be assessed through appropriate indices (Chapter 5). External resources are those which are not part of the defined items (Chapter 4).

1 System analysis

For the Process control cystem, comprehensive data material is provided by ABB, by other companies, and by experts. The following system specifications and descriptions (documents) are the basis for the present system reliability evaluation.

- Control System Overview (Page 20 - 30) and System Specification of the Controller and the Profi Bus (Page 31 and 32).
- System Specification of 800xA with MNSiS, MCC MNSiS, AC800, and OPC Server.
- Construction Description of the Automation System with S800 E/A Modules.
- Assembly Description of all Controllers with Declaration and Number of IO-Cluster, CI854, OZD, MLink.
- Automation System Reliability and Availability Documents.

- Preventive Maintenance and its Influence on an Automation System Life Cycle Cost.
- Aspects on Automation System Spare Parts.

2 Definition of the system function(s) (system state(s))

The required function which has to be performed (related to [DKE-IEV 191-02-05 2012]) is defined as

> **System function (system state) B_S: Process monitoring and process control have to be completely fulfilled (without degradation).**
>
> **System outage (system state) A_S: = ¬ B_S** (complementary state of the system function B_S).

In agreement with the defined system function, **all** of the **28 Controller AC800M** (Page 25 - 30, Control System Overview) have to function **and** have to be monitored and controlled by the operator via the **Workplaces** (A0CRU10, 20, 30, and 40). That means that the outage of at least one Controller or the outage of the Workplace system causes a system outage.

Commitments

1. **Workplaces** (A0CRU10, 20, 30, and 40): 3oo4 structure (conservative assumption) and Engineering Station 1 + 2: 1oo2 structure.
2. **All 7 servers** (from Domain-Server A0CRQ10/20 to PGIM-Server A0CRX10/20 **and** the Asset-Monitor Server A0CRP70/80) have to function (100%).
3. Those components/subsystems which do **not** have the same **severe outage as a Controller** (e.g. MNSiS OPC Server A0CRP51, 52, 53, and 54) are weighted by a **factor < 1** (see detailed in-depth report and Excel Table, column 2).

   Failed components/subsystems (Appendix B) which do not cause the defined system outage are not considered.
4. **Common-Cause-Failure (CCF)** caused by Single-Point-of-Failure (SPoF) of an IO-Modul (on average about 8 for each IO-Cluster) which causes the outage of an IO-Cluster (total sum 131) are considered (Appendix O).
5. **Independent single failure** of IO-Modules which do not cause a CCF of the connected IO-Cluster are not considered.

The **aim of the reliability analysis** is the evaluation of the **system indices**

Probability	**P**
Mean Frequency	**H**

of the defined system states $\mathbf{B_S}$ and $\mathbf{A_S}$ (Chapter 2). For example: $P(B_S)$ means the availability, $P(A_S)$ the unavailability, and $1/H(A_S)$ the MTTSF (Mean Time to System Failure).

3 Definition of the preconditions and assumptions

1. All components are assumed to be **error-free** according to hardware and software (**concerning design, manufacture, maintenance and operation**). This is a realistic assumption, e.g. for mass products such as the Controller AC800M (although software changes/maintenance can cause failure, which is not considered).
2. Component outages are immediately detected and signaled.
3. Defect components are replaced by equivalent components, which are sufficiently available in stock.
4. The environmental conditions, e.g. climatic influences (e.g. temperature, humidity), mechanical impacts (e.g. physical shocks and vibration), electromagnetic impacts, and power supply etc., must agree with the specification.
5. Operating personal must be well-trained to perform their job free of error in the Process control cystem.

4 Definition of the components and system(s)

In reliability/availability evaluation, the term item (according to [DKE-IEV 191-02-05 2012] can mean a “component“ or a “system“, depending on the perspective.

- A **component** is defined as the smallest statistical item under consideration which needs no further subdivision from the reliability point of view.
- A **system** is the combination of those components that assure the defined system function. *External* resources (from outside the system boundary), although beeing necessary for the system to operate, are not considered.

In the present reliability analysis the items (components and system) are specified by the functional Control System Overview (Page 20 - 32). Some components have to be analyzed in detail (scrutinized as a system), e.g. the Controller AC800M (Appendix M to P).

5 Definition of the reliability indices

The two state model (renewal process, Appendix F) is the basic reliability model, which can be extended to application oriented models, e.g. Appendix J. Comprehensive data sources are provided by ABB and other companies. The reliability indices are listed in the Excel Table.

The **failure or outage rates** λ (reciprocal value of **MTTF** (Mean Time to Failure)) are calculated according to [MIL-HDBK-217F 1991]. The method is conservative (part-count-calculation), that means that the calculated (predicted) failure rates are approximately 2 to 5 times larger than the observed values (according to ABB). Aleatory (statistical) and epistemic (lack of knowledge) uncertainties are not considered in this report.

Following failure types are excluded in the reliability analysis.

- Failure in design and construction (also concerning software failure), production, assembly, maintenance, and operation.
- Hyperfunction and subfunction of components.
- Failure in Patchbox.
- Failure in Blackbox.
- Cable break.
- Physical shock and vibration impact (break) on connector and switches.

The **repair rate** μ is the reciprocal value of the **MTTR** (Mean Time To Repair). The MTTR, which includes e.g. times for initiation, diagnosis, and replacement of failed units, is assumed to be **8 hours**. This is a typical value (reference value) in most reliability analyses where no other specifications are given.

For repair and start up of the PNP/PNS- and ANP/ANS-bus systems, **8 hours** are also assumed (other start up times can also be modeled and calculated, Appendix K).

For the repair/replacement of an IO-Module, **2 hours** are assumed. In many cases shorter MTTR can be realized. A typical value for on-line replacement is 0.5 hours.

Emphasis is placed on to the preparation and definitions of the steps 1 to 5, before reliability/availability modeling and calculation can be performed in the steps 6 to 9 (Fig. 1) .

6 Component modeling and calculation

Realistic operation and outage behavior of components can be modeled by means of Markov process models. The basic component models are described in Appendix F and J.

In many reliability/availability analysis, complex functional component and subsystem structures cannot be exactly modeled without reasonable effort. Therefore, the goal is to simplify the reliability models with regard to **conservative reliability estimations**. Appendix M to P describe the conservative approach (modeling and calculation) on the Controller AC800M. Appendix U outlines a few operation and outage scenarios.

As a result, the CCF (SPoF) significantly determines the reliability of this system.

7 System modeling and calculation

The following methods/procedures are suitable for reliability evaluation (modeling and calculation) of the Process Control System.

- **Minimal cut approach** (suitable for large system structures).
- **Probable Markov path approach** (efficient and easy modeling and calculation approach for complex systems [Kochs 1984, Kochs et al. 1999, Kochs SFB 2001, Kochs et al. 2004]. The basis of this efficient approach has already been laid in the earlier research work of [Dib 1978, Nachtkamp 1979].
- **Reliability block diagram (RBD)** (combination of component states - logical network).
- **Fault tree method (FTM)**.

In this study, minimal cuts, RBD and Markov models are developed on the basis of Boolean logic in order to combine them easily. The approaches are based on the probability theory and the theory of stochastic processes. A combination of the approaches is applied in this reliability study. Especially, the consideration of CCF (SPoF) needs special attention in each reliability analysis due to its severe influence, see examples in Appendix H, M to P, and T.

Starting basis of the reliability analysis is the determination of the **minimal cuts (MS)** (always in view of the defined system function), which can be determined directly from the functional system structure (Page 20 - 30 of the Control System Overview).

Definition: A **minimal cut** is a set of system components which, if failing, causes outage of the system but when any one component of the set is repaired and put into

operation (again), then the system is in operation (again).
All minimal cuts of a system yield the system outage (and if negated the system function).

The determination of all minimal cuts (1st order, 2nd order, higher order, etc.) is a most difficult or even an impossible task, but mainly the minimal cuts of lower order influence the system outage. For example, Appendix Q to S illustrate that the minimal cuts of higher order in the Process Control System are negligible.

46 significant minimal cut (MS) of the Process Control System have been identified, which determine the system reliability. The logical OR-connection of these minimal cuts describes the **system outage**.

$$A_S \approx MS_1 \vee MS_2 \vee \ldots \vee MS_{46}$$

The **system function** is

$$B_S = \neg A_S$$

The **reliability block diagram** of the Process Control System is illustrated in Appendix B to E, where the $\neg MS$ (negated MS) are connected in series (logical AND-connection, up state mode). This logical network represents the reliability block diagram of the Process Control System.

The **probabilities $P(A_S)$, $P(B_S)$** and the **mean frequency $H(A_S)$** are approximately

$$P(A_S) \approx \sum_{\forall i} P(MS_i) \qquad \text{(unavailability)}$$

$$H(A_S) \approx \sum_{\forall i} H(MS_i)$$

$$P(B_S) = 1 - P(A_S) \qquad \text{(availability)}$$

Markov process approaches enable the calculation of the indices $P(MS_i)$ and $H(MS_i)$ of each minimal cut, and thus, the identification of those components and subsystems, which have major impact on the system outage (sensitivity analysis). The **minimal cuts are modeled by Markov process models** (and calculated with the probable Markov path approach) in the Appendices.

The detailed **reliability calculation** is outlined in the 16 page of the Excel Table.

Redundant component/subystem structures are significant to achieve **high system reliability** of the Process Control System.

8 System Results

The system reliability evaluation of the Process Control System yields the following overall system indices (Excel Table, line sum).

Mean freqency of the system outage:	**$H(A_S) = 1.25*10^{-4}\ h^{-1}$**
Probability of system outage (≡ unavailability):	**$P(A_S) = 9.08*10^{-4}$**
Probability of system function (≡ availability):	**$P(B_S) = 0.999\ 092$**

The system evaluation is based on the conservative modeling and calculation procedure, taking into consideration conservative failure/outage rates of the components (Chapter 5).

9 Sensitivity analysis

The **outage chart** in the Excel Table points out the distribution of the probabilities of the minimal cuts MS. **MS10** PGIM Application-Server (A0CRX30) and **MS18** EMI Computer Emission Monitoring (A0CRV40) stand out of the chart because they are not redundant. Without a consideration of these two computers, the availability of the Process Control System would increases to **0.999 247**!

All redundant components, especially the 28 Controllers, show a **nearly balanced probability distribution** in the Excel Chart, which indicates no reliability weakpoint.

Central Servers

The redundant central servers, expressed by MS3 - MS9 (Appendix C), have an **outage probability of $2.07*10^{-6}$** for each MS.

Workplace system (Operating Stations and Engineering Stations for process supervision and control)

The Workplaces (MS1, BS+ES, Appendix B) have an **outage probability** of **$2.53*10^{-6}$**, which means that the **availability** is **0.999 997 47** (Excel Table for MS1, column 24). Modeling and calculation see Appendix B and L.

System Clock Time

If the system clock (MS2 Syst.Clock, Appendix B) fails, a scheduled (first) master takes the time. If this master fails, another scheduled (second) master takes the time.

Therefore, the time is based on a very high redundant system (modeling see Appendix T, calculation see Excel Table). The **outage probability (unavailability)** is **3.25 *10^{-8}**, the **availability** is **0.999 999 967**.

Central Bus Systems

The bus systems PNP/PNS (with 2 x 6 switches) and ANP/ANS (with 2 x 3 switches) form the communication backbone of the Process Control System (MS11 and MS12, reliability block diagram see Appendix D, modeling and calculation see the Appendix J and K, results see Excel Table, line MS11 and MS12, column 23 and 24).

	$H(MS11_{ANP/ANS}) = 4{,}04 * 10^{-9}\ h^{-1}$	$P(MS11_{ANP/ANS}) = 3{,}24 * 10^{-8}$
	$H(MS12_{PNP/PNS}) = 1{,}62 * 10^{-8}\ h^{-1}$	$P(MS12_{PNP/PNS}) = 1{,}29 * 10^{-7}$
Sum:	$\mathbf{H(A_{bus\ systems}) = 2{,}02 * 10^{-8}\ h^{-1}}$	$\mathbf{P(A_{bus\ systems}) = 1{,}61 * 10^{-7}}$

Thus, the bus systems PNP/PNS and ANP/ANS altogether have a calculated availability of 0.999 999 839.

IO-Cluster

The **outage** of one (or multiple) of the 131 IO-Clusters due to **CCF (SPoF)** of the IO-Modules (Assumption: On average 131 x 8 = 1,048 IO-Modules) occur with a **probability of 5.72*10^{-5}** (Excel Table, column 22, line sum).

Impact of MTTR on reliability

The MTTR (Mean Time to Repair) has significant influence on the reliability/availability of the Process Control System. If **MTTR = 8 hours** decreases to **MTTR = 6 hours**, then the system availability would increases to **0.999 305** (instead of 0.999092 for MTTR = 8 hours).

Independent multiple outages

Independent **multiple outages** of the AC800M and/or the IO-Cluster (due to CCF of IO-Modules) are **not significant**, thus multiple outages are negligible, see the Appendix Q to S.

Conclusion: For the defined system function (system state) with the stated preconditions and assumptions, the system reliability evaluation yields the availability of the Process Control System of > 0.999.

Literaturverzeichnis

Bücher und Abschlussberichte

[Billinton et al. 1992]
Billinton, R., Allan, R. N. (1992). *Reliability Evaluation of Engineering Systems - Concepts and Techniques.* Plenum Press, New York (453 pages), ISBN 0-306-44063-6.

[Endrenyi 1979]
Endrenyi, J. (1979). *Reliability Modelling in Electric Power Systems*. Toronto/ Canada: J. Wiley & Sons (338 pages), ISBN 13: 978-0471996644.

[Kochs 1984]
Kochs, H.-D. (1984). *Zuverlässigkeit elektrotechnischer Anlagen - Einführung in die Methodik, die Verfahren und ihre Anwendung.* Springer Verlag Berlin Heidelberg New York Tokyo (400 Seiten), ISBN 3-540-13475-1 und ISBN 0-387-13475-1.

[Kochs SFB 2001]
Kochs, H.-D. (2001). *Sicherheits- und Zuverlässigkeitsanalyse komplexer Handhabungssysteme*. DFG-SFB Projekt C5 im Sonderforschungsbereich 291 „Elastische Handhabungssysteme für schwere Lasten in komplexen Operationsbereichen“, Abschlussbericht, S. 157 - 190.

[Laprie 1991]
Laprie, J. C. (1991). *Dependability: Basic Concepts and Associated Terminology*. Springer-Verlag, Berlin.

[Limbourg 2008]
Limbourg, Ph. (2008). *Dependability Modelling under Uncertaintiy - An Imprecise Probabilistic Approach.* Springer-Verlag Berlin Heidelberg (139 pages), ISBN 978-3-540-69286-7.

[O’Connor et al. 2002]
O'Connor, P. D. T., Newton, D., Bromley, R. (2002). *Practical Reliability Engineering.* 4 ed. Chichester, United Kingdom: Wiley, Websites.

[Pham 2003]
Pham, H. (Editor) (2003). *Handbook of Reliability Engineering*. Springer-Verlag London (663 pages), ISBN 1-85233-453-3.

[Singh et al. 1977]
Singh, C., Billinton, R. (1977). *System Reliability Modelling and Evaluation*. Hutchinson & Co. London (248 pages), ISBN 0091265002.

Publikationen

[Avizienis et al. 2000]
Avizienis, A., Laprie, J.-C., Randell, B. (2000). *Fundamental Concepts of Dependability.* LAAS-CNRS Toulouse, France.

[Dib 1978]
Rib, R. (1978). *Kombinierte Anwendung der Minimalschnitt-Methode und der Theorie Markoffscher Prozesse zur Zuverlässigkeitsberechnung von Kraftwerks-Eigenbedarfsanlagen und von Hochspannungsnetzen.* Diplom-Thesis am Institut für Elektrische Anlagen und Energiewirtschaft (IAEW) der RWTH Aachen, 1978.

[Kochs 1996]
Kochs, H.-D. (1995/1996). *Zuverlässigkeitsermittlung großer und komplexer Systeme mit effizienten Näherungsverfahren.* at - Automatisierungstechnik, Theorie für den Anwender, Teil 1: 11/1995, Teile 2 bis 7/1996. Oldenbourg-Verlag.

[Kochs et al. 1996]
Kochs, H.-D., Dieterle, W., Dittmar, E. (1996). *Reliability Evaluation of Highly Reliable Computer Control Systems for Energy Generation, Transmission and Distribution.* European Transactions on Electrical Power (ETEP), Vol. 6, No. 2, March/April 1996, Seite 111 - 118.

[Kochs et al. 1999]
Kochs, H.-D., Hilmer, H., und Nisbach, T. (1999). *Efficient Approximate Reliability Evaluation using the Markovian Minimal Cut Approach*. Journal of Universal Computer Science, Oktober 1999. Springer Verlag. Seite 644 - 667.

[Kochs 2001]
Kochs, H.-D. (2001). *Schwachstellenanalyse am Beispiel der Concorde.* Automatisierungstechnische Praxis atp, 10/2001, Seite 38 - 43.

[Kochs 2002]
Kochs, H.-D. (2002). *Mechatronic System Dependability Analysis - An Application Example. Architecture of Computing Systems*, ARCS 2002, Workshop Proceedings, Seite 55 - 65.

[Kochs et al. 2004]
Kochs, H.-D., Petersen, J. (2004). *A Framework for Dependability Evaluation of Mechatronic Units.* International Conference on Architecture of Computer Systems ARCS. Gesellschaft für Informatik (GI), Bonn, Proceedings, Seite 92 - 105, ISBN 3-8857-370-9, ISSN 1617-5468. Auch publiziert in GI/VDI/VDE-

GMA/ITG Mitteilungen Fachgruppe fehlertolerierende Rechensysteme. St. Augustin: FhG-AiS. 2005, ISSN 0724-5319).

[Kochs 2004]
Kochs, H.-D. (2004). *Key Factors of Dependability of Mechatronic Units: Mechatronic Dependability.* In: Panel Session on Risk Management and Dependability - What are the Key Factors? 28th Annual International Computer Software and Application Conference (COMPSAC 2004) page 584 - 586. IEEE Computer Society Press, Hong Kong 2004.

[Kochs et al. 2011]
Kochs, H.-D., Kongniratsaikul, P. (2011). *Comparing System Reliability of Various HVDC Substation Concepts.* Reliability Report, BMU (German Federal Ministry for the Environment, Nature Conservation, and Nuclear Safety), Project No. 0327648.

[Kochs et al. 2012]
Kochs, H.-D., Kongniratsaikul, P., Lutz, F. (2012). *Comparing System Reliability Considering Insufficient Knowledge: Application to HVDC Converter Stations.* IEEE-PES (Power & Energie Society), 22. - 26.07.2012, San Diego, CA, USA.

[Laprie 1995]
Laprie, J. C. (1995). *Dependability - its Attributes, Impairments and Measures in Predictably Dependable Computing-Systems.* B. Randell, J. C. Laprie, H. Kopetz and B. Littlewood, Ed. Springer-Verlag. 1995.

[Limbourg et al. 2007a]
Limbourg, Ph., Savic, R., Petersen, J., Kochs, H.-D. (2007). *Fault tree analysis in an early design stage using the Dempster-Shafer theory of evidence.* European Safety and Reliability Conference, ESREL 2007, Stavanger, Norway, 2007 Taylor & Francis Group, Seite 713 - 722, ISBN 978-0-415-44786-7.

[Limbourg et al. 2007b]
Limbourg, Ph., Kochs, H.-D., Echtle, K., Eusgeld, I. (2007). *Reliability Prediction in Systems with Correlated Component Failures - An Approach Using Copulas.* ARCS Workshop Dependability and Fault Tolerance, Seite 55 - 62, Zürich, Switzerland, 2007 VDE-Verlag.

[Nachtkamp 1979]
Nachtkamp, J. (1979). *Verfügbarkeitsorientierte Zuverlässigkeitsuntersuchung der Netzeinbindung und der Eigenbedarfsversorgung großer Wärmekraftwerksblöcke.* Dissertation am Institut für Elektrische Anlagen und Energiewirtschaft der RWTH Aachen, 1979.

Normen und Richtlinien

[VDI 4004 1986]
VDI 4004 Blatt 4 (1986-07). *Zuverlässigkeitskenngrößen, Verfügbarkeitskenngrößen*. VDI-Gesellschaft Produkt- und Prozessgestaltung.

[IEEE 90 1990]
IEEE 90 (1990). Institute of Electrical and Electronics Engineers, IEEE Standard Computer Dictionary: *A Compilation of IEEE Standard Computer Glossaries*. New York, 1990.

[DIN 40041 1990]
DIN 40041 (1990-12). *Zuverlässigkeit - Begriffe.* Beuth-Verlag, Berlin Heidelberg New York Tokyo.

[MIL-HDBK-217F 1991]
MIL-HDBK-217F (1991). *Reliability Prediction of Electronic Equipment.* Department of Defense, Washington. D.C.

[DIN EN 61709 1999]
DIN EN 61709 (1999) (= IEC 61709). *Electronic components - Reliability - Reference conditions for failure rates and stress models conversion*.

[DIN EN 61508 2000]
DIN EN 61508 (2000). *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES).* VDE-Verlag.

[VDI 2206 2003]
VDI 2206 2003. *Design methodology for mechatronic systems.* VDI, Beuth-Verlag, Berlin.

[CEI IEC 61165 2006]
CEI IEC 61165 ed. 2.0 (2006-05). *Application of Markov techniques*.

[CEI IEC 61078 2006]
CEI IEC 61078 ed. 2.0 (2006-01). *Analysis techniques for dependability - Reliability block diagram and boolean methods*.

[VDI 3423 2011]
VDI 3423 (2011-08). *Verfügbarkeit von Maschinen und Anlagen - Begriffe, Definitionen, Zeiterfassung und Berechnung*. VDI Richtlinie.

[DKE-IEV 191-02-03 2012]
DKE-IEV 191-02-03 (2012). *Definition Zuverlässigkeit allgemein*.

[DKE-IEV 191-02-05 2012]
DKE-IEV 191-02-05 (2012). *Definition Verfügbarkeit*.

[DKE-IEV 603-05-01 2012]
DKE-IEV 603-05-01 (2012). *Definition Zuverlässigkeit einer Betrachtungseinheit*.

[DKE-IEV 603-05-04 2012]
DKE-IEV 603-05-04 (2012). *Definition Verfügbarkeit*.