

Verfügbarkeit, Zuverlässigkeit & Fehlertoleranz von Rechenzentren

Dipl.-Ing. Uwe Müller

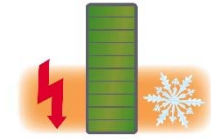
ibmu.de[®] Ingenieurgesellschaft für technische
Beratung, Medien und Systeme mbH



InfraOpt[®]

PowerBuilding und DataCenter Convention

Wien, am 24. September 2015



1. Verlässlichkeitsanalyse

- Motivation zur numerischen Analyse
- Richtlinien und Normen

2. Praxisbeispiel

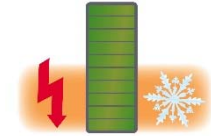
- Aufgabenstellung Variantenvergleich N+1, 2N
- Methodik der Verlässlichkeitsanalyse mittels InfraOpt

3. Designvergleich

- Gegenüberstellung verschiedener Redundanzkonzepte
- Berechnete Zuverlässigkeit, Verfügbarkeit und Fehlertoleranz

1.1 Verlässlichkeitsanalyse im Rechenzentrum

Motivation zur numerischen Analyse

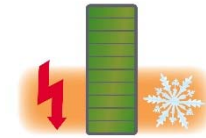


- Welche **Verfügbarkeit** und welche **Zuverlässigkeit** wird erwartet?
- Was müssen **Wartungs-** und **Servicepläne** (SLA) fordern?
- In welche **technischen Lösungen** ist es ratsam zu investieren?
- Wie sind **Mehrinvestitionen** zu begründen?
- Welche **Effizienzziele** sind zu erreichen?
- Ist die Infrastruktur während der **Umbaumaßnahme** verlässlich?
- Sind **vorgefertigte Lösungen** die bessere Wahl?
- Wie ist fortlaufende **Zuverlässigkeitsbewertung** (bspw. für ein ISMS nach DIN ISO 27001) zu realisieren?
- Was leistet das RZ, verglichen mit **Richtlinien** und **Normen**?

... denn „eigentlich“ **darf** das Rechenzentrum **niemals ausfallen!**

1.2 Richtlinien und Normen

Uptime Institute - Tier Klassifikation

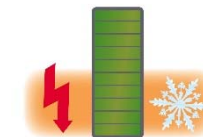


Uptime Institute	Tier I	Tier II	Tier III	Tier IV
Single Points-of Failure	Many+ Human Error	Many+ Human Error	Some+ Human Error	Fire, EPO+Some Human Error
Representative Planned Maintenance Shut Downs	2 Annual Events at 12 Hours Each	2 Events Over 2 Years at 12 Hours Each	None Required	None Required
Representative Site Failures	6 failures Over 5 Years	1 Failure Every Year	1 Failure Every 2.5 Years	1 Failure Every 5 Years
Annual Site-Caused End-User Downtime (based on field data)	28.8 hours	22.0 hours	1.6 hours	0.8 hours (0.4 hours)
Resulting End-User Availability on Site-Caused Downtime	99.67 %	99.75 %	99.98 %	99.99 % (99.995 %)
First Deployed	1965	1970	1985	1995

Quelle (Auszug): Uptime Institute, 2008, White Paper, „Tier Classifications Define Site Infrastructure Performance“, Page 14

1.3 Richtlinien und Normen

BSI Verfügbarkeitsklassen und BITKOM Kategorien



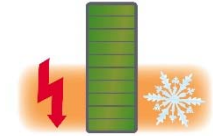
BSI	VK 0	VK 1	VK 2	VK 3	VK 4	VK 5
Ausfallzeit /Jahr	ca. 2-3 Wo.	< 90 Std.	< 9 Std.	< 1 Std.	ca. 5 min.	-
Anforderung an Verfügbarkeit	Keine	normal	hoch	sehr hoch	höchste	Desaster-tolerant
Verfügbarkeit	ca. 95 %	> 98,97 %	> 99,90 %	> 99,99 %	> 99,999 %	(100 %)

BITKOM	Kategorie A	Kategorie B	Kategorie C	Kategorie D
Zul. Ausfallzeit /Jahr	12 h	1 h	10 min.	< 1 min
Verteilung	USV/Normal empfohlen	Redundanz A und B	Redundanz A und B	Redundanz A und B
USV	mind. 10 min	mind. 10 min N+1	mind. 10 min 2 N	mind. 10 min 2 (N+1)
Notstrom	optional	Anlauf 15 s 24 h Brennstoff	Anlauf 15 s 72 h Brennstoff	Anlauf 15 s 72 h Betankung
Klimatisierung	Redundanz opt. bzw. notwendig	Redundanz notwendig	Redundanz notwendig	Komplette Redundanz
➔ Verfügbarkeit	99,86 %	99,99 %	99,998 %	99,9998 %

Quelle (Auszug): BITKOM e. V., Betriebssicheres RZ, Leitfaden 2013

1.4 Richtlinien und Normen

DIN EN 50600 ff.



Verfügbarkeits-Klasse	VK 1	VK 2	VK 3	VK 4	VK 4 erweitert
Verfügbarkeit	niedrig	mittel	hoch	sehr hoch	
DIN EN 50600-2-2 Stromversorgung	keine Redundanz	Komponenten Redundanz	Instandsetzung im lfd. Betrieb	Fehlertoleranz	
Versorgung	Einzelpfad	Einzelpfad	Mehrfad	Mehrfad	
Redundanz	N	N+1	N+1 bzw. 2N	2N	
Transferschalter	k. A.	(Ja)	Ja	Ja, mehrere	
Bei Ausfall der Stromversorgung	USV, kontroll. Abschalten	USV, kontroll. Abschalten	USV, alternative Versorgung	USV, alternative Versorgung	
DIN EN 50600-2-3 Regelung d. Umgebungsbedingungen	-	keine Ausfallsicherheit	Komponenten Redundanz	Instandsetzung im laufenden Betrieb	
				weitgehend	vollständig
Versorgung	-	Einzelpfad	Einzelpfad	Mehrfad passiv	Mehrfad aktiv
Redundanz		N	N+1	N+1	2N

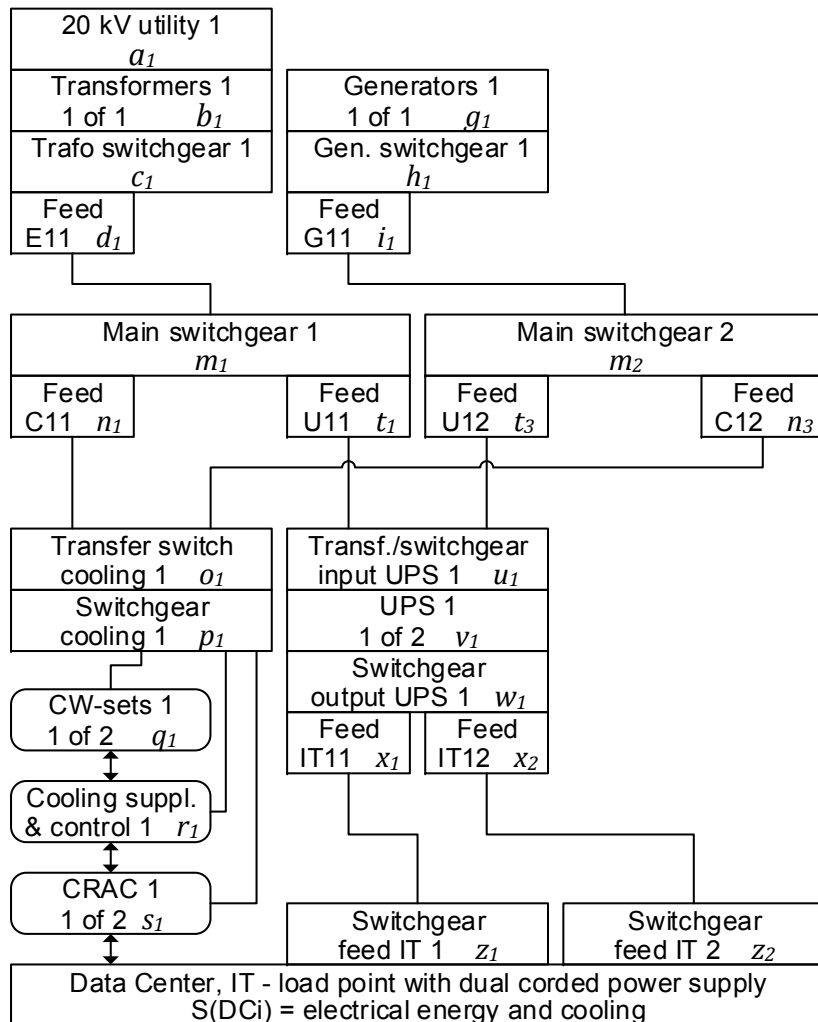
Quelle (Auszug): DIN EN 50600-1 2013, DIN EN 50600-2-2 2014, DIN EN 50600-2-3 2015

2.1 Praxisbeispiel

Aufgabenstellung: Vergleich von Designs mittels Metriken



Design 1: N_{E+1}, N_{C+1}



Vergleiche 4 Designs der Elektroenergie- & Kälteversorgung:

- 1) N_{E+1} & N_{C+1}
- 2) $2N_E$ & N_{C+1}
- 3) N_{E+1} & $2N_C$
- 4) $2N_E$ & $2N_C$

Verlässlichkeitsanalyse:

- Zuverlässigkeit $R(t)$
- Inhärente Verfügbarkeit A_i
- Operationale Verfügbarkeit A_o
- 1- und 2-Fehlertoleranz

2.2 Verlässlichkeitsanalyse mittels InfraOpt[®]

Praktische Interpretation der Metriken



- **Zuverlässigkeit** (Reliability): $R(t) = e^{-1/MTBF * t}$ als Wahrscheinlichkeitsmaß
 - Strukturdesign (Tier, Kategorie), Redundanzen ($x*N$, $y*M$)
 - Komponenten (MTBF), Betriebsdauer etc.

➤ Alterung: **Wann** und in **welche Teilsysteme** ist zu **investieren**?
- **Inhärente Verfügbarkeit**: $A_i = MTBF / (MTBF + MTTR)$
 - MTBF: Mittlere Zeit zwischen Fehlern
 - MTTR: Mittlere Zeit bis zur Reparatur

➤ Welche **Servicelevel** sind notwendig, **was** ist zu **bevorraten**?
- **Operationale Verfügbarkeit**: $A_o = MTBM / (MTBM + MDT)$
 - MTBM: Mittlere Zeit zwischen notwendigen oder geplanten Instandsetzungen
 - MDT: Mittlere Zeit der tatsächlichen Nichtverfügbarkeit

➤ **Funktionieren** die **Managementsysteme** (Qualität, Sicherheit)?
- Simulation aller **1- und 2-Fehlerkombinationen**, Bewertung der Single Points of Failure **SPoF** und Double Points of Failure **DPoF**

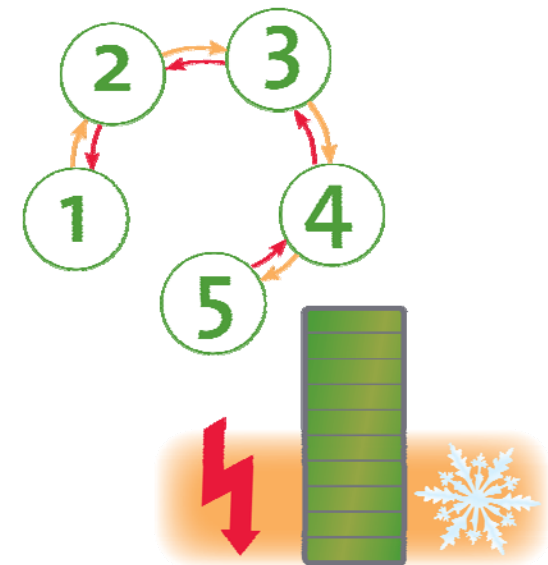
➤ **Vorhersage** der **Reaktion** auf **geplante** bzw. **nicht geplante Ereignisse**!

2.3 Verlässlichkeitsanalyse mittels InfraOpt®

Praxisbewährter Dienstleistungsprozess

Fünf Schritte zur Optimierungsvariante:

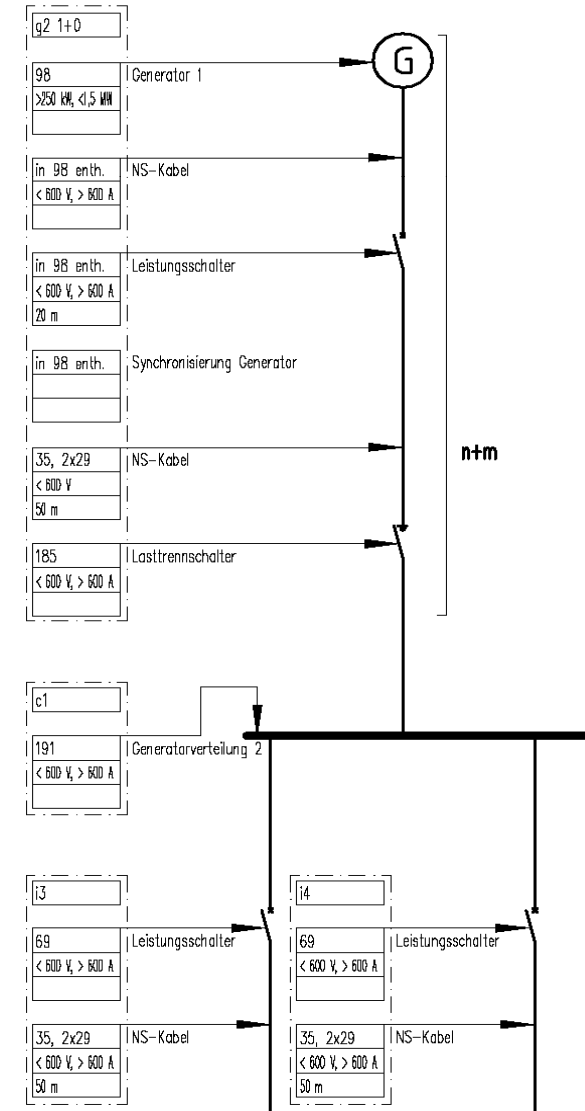
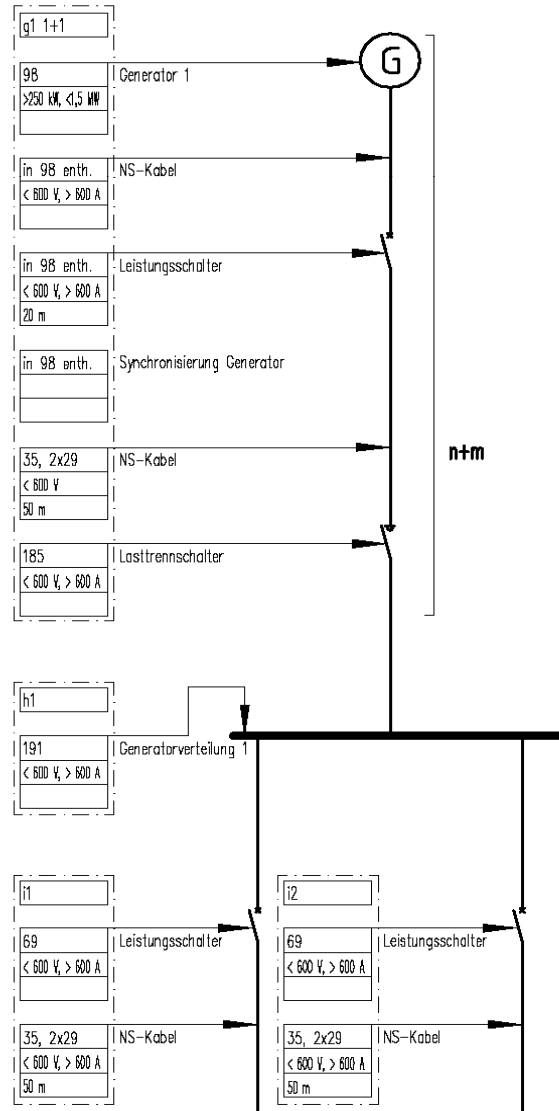
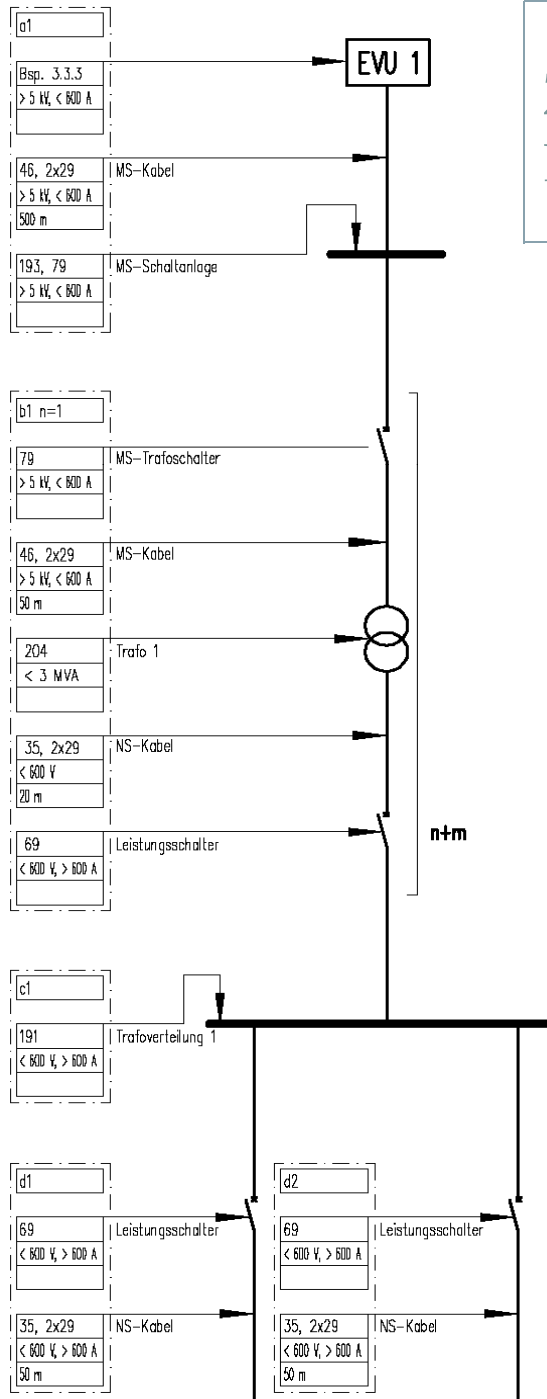
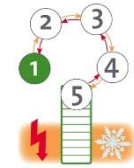
1. **Überführung** des Designs in das integrale Verlässlichkeitsschema
2. Boolesche **Modellierung** in InfraOpt®
3. **Aufbereitung** der Komponentendaten
4. **Berechnung** Zuverlässigkeit und Verfügbarkeiten
5. **1- und 2-Fehlersimulation** über alle Teilsysteme



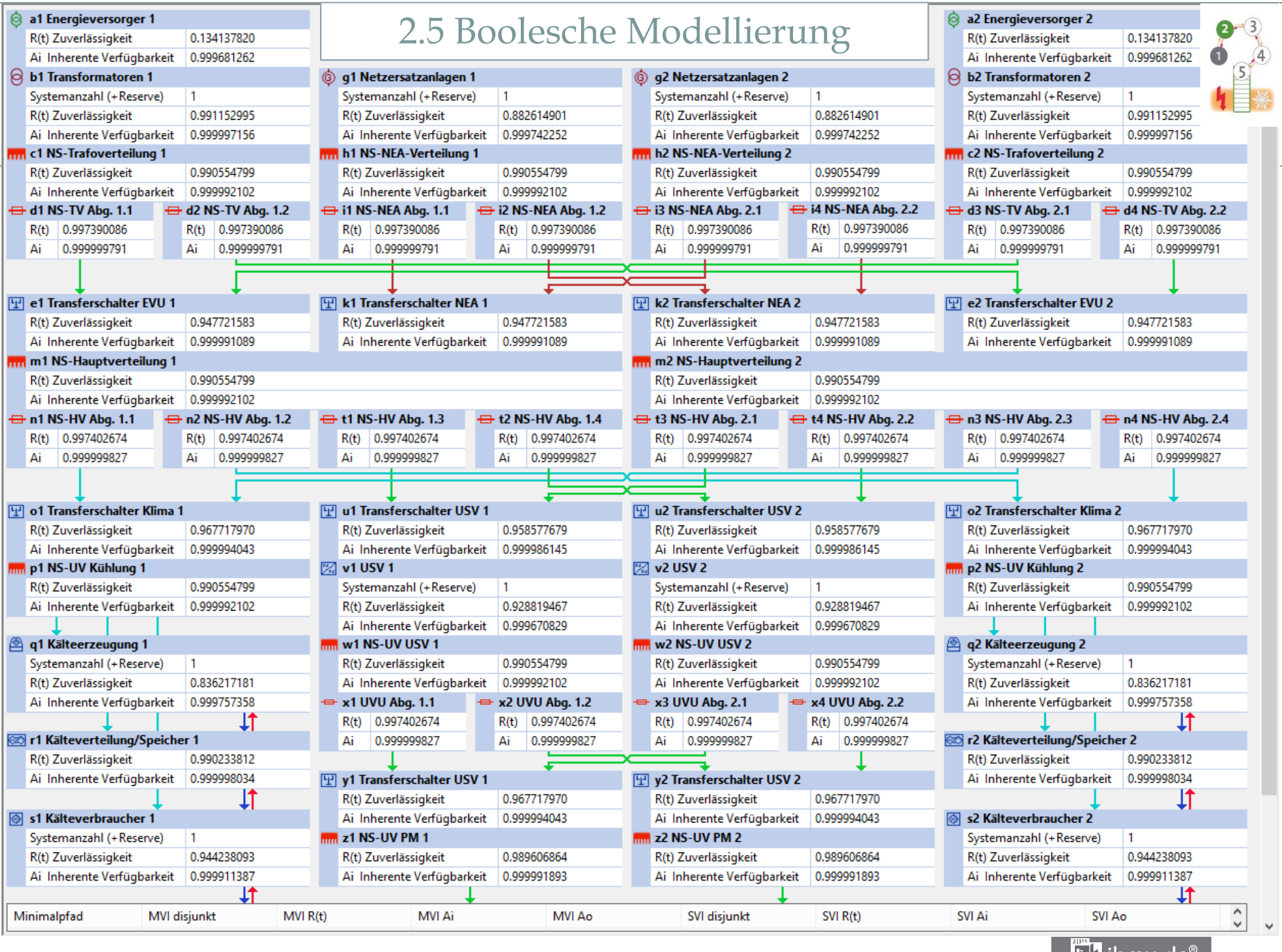
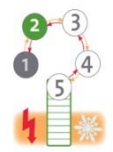
Ziel des Optimierungsprozesses:

Maximierung Verlässlichkeit ↔ **Minimierung Lebenszykluskosten**

2.4 Integrales Verlässlichkeitsschema Elektroenergie- und Kälteversorgung

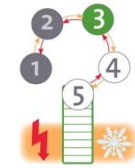


2.5 Boolesche Modellierung



Minimalpfad MVI disjunkt MVI R(t) MVI Ai MVI Ao SVI disjunkt SVI R(t) SVI Ai SVI Ao

2.6 Aufbereitung der Komponentendaten Datenquellen



- **Aufbereiten** aller **Teilsysteme** des Zuverlässigkeitsmodells in InfraOpt[®]
 - Ein Teilsystem kann **beliebig** viele **Komponenten** enthalten
 - Je Komponente kann das **Alter** festgelegt werden
 - **Redundante Komponenten** sind möglich
 - **Komponentenattribute** werden unterstützt (z. B. Kabellänge)
 - Beliebige **redundante Teilsysteme** sind möglich
- **Verwendung** von **Zuverlässigkeitsdaten** aus folgenden Quellen:
 - Statistische Erhebungen des **Rechenzentrums-Betreibers**
 - Reaktionszeiten bzw. Statistiken von **Lieferanten** oder **Dienstleistern**
 - Zuverlässigkeitsdaten von **Herstellern**
 - Zuverlässigkeitsdaten aus **IEEE Std. 493-2007**

2.7 Komponentendaten

Verlässlichkeit des System - q1 Kälteerzeugung 1



q1 Kälteerzeugung 1												
Typ	Quelle	R(t)	Ai	Ao	MTBF	MTTR	MTBM	MDT	Länge /m	Betrieb /h	Anz. n(+m)	
Leistungsschalter; 600 V; Einschub...	IEEE Std 493-2007 gold Book (69)	0.994461784	0.999999894	0.999954308	4732057.80...	0.500000	32411.0000	1.481000		26280	1	
Kabel; überirdisch; kein Rohr; ≤ 60...	IEEE Std 493-2007 gold Book (20)	0.999940860	0.999999994	0.999999984	72896904.0...	2.500000	816772.0000	0.078000	50.0	26280	1	
Kabelverbindung	IEEE Std 493-2007 gold Book (29)	0.997777624	0.999999937	0.999999937	23624073.0...	0.750000	23624073.0...	0.750000		26280	2	
Kühler; Kolbenverdichter; geschlos...	IEEE Std 493-2007 gold Book (56)	0.681336910	0.999809501	0.998736758	68491.3000	13.050000	1314.0000	1.662000		26280	1	
Steuereinheit; für Kompressoren, K...	IEEE Std 493-2007 gold Book (129)	0.999546428	1.000000000	0.999982208	57926964.7...	0.000000	58733.0000	1.045000		26280	1	
Schaltanlage; isolierte Sammelschi...	IEEE Std 493-2007 gold Book (195)	0.988716986	0.999996546	0.999696325	2316000.00...	8.000000	2548.0000	0.774000		26280	1	
Filtersieb; Kühlmittel	IEEE Std 493-2007 gold Book (177)	0.996588939	1.000000000	0.999333914	7691200.00...	0.000000	2444.0000	1.629000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Überdruckventil	IEEE Std 493-2007 gold Book (235)	0.996018730	0.999999696	0.999994751	6587760.00...	2.000000	36196.0000	0.190000		26280	1	
Tank; Wasser	IEEE Std 493-2007 gold Book (199)	0.989171120	0.999999793	0.999989526	2413680.00...	0.500000	12221.0000	0.128000		26280	1	
Pumpe; zentrifugal; integrierter An...	IEEE Std 493-2007 gold Book (163)	0.977713987	0.999993654	0.999897372	1166025.60...	7.400000	5836.0000	0.599000		26280	1	
Ventil; 3-Wege; Mischungsregelung	IEEE Std 493-2007 gold Book (237)	0.998713181	1.000000000	0.999980695	20409317.6...	0.000000	52836.0000	1.020000		26280	1	
Ventilantrieb; elektrisch	IEEE Std 493-2007 gold Book (229)	0.970767486	0.999979206	0.999934106	885794.0000	18.420000	21245.0000	1.400000		26280	1	
Wärmetauscher; Wasser zu Wasser	IEEE Std 493-2007 gold Book (124)	0.988434959	1.000000000	0.999862264	2259200.00...	0.000000	392.0000	0.054000		26280	1	
Ventil; 3-Wege; Mischungsregelung	IEEE Std 493-2007 gold Book (237)	0.998713181	1.000000000	0.999980695	20409317.6...	0.000000	52836.0000	1.020000		26280	1	
Ventilantrieb; elektrisch	IEEE Std 493-2007 gold Book (229)	0.970767486	0.999979206	0.999934106	885794.0000	18.420000	21245.0000	1.400000		26280	1	
Pumpe; zentrifugal; integrierter An...	IEEE Std 493-2007 gold Book (163)	0.977713987	0.999993654	0.999897372	1166025.60...	7.400000	5836.0000	0.599000		26280	1	
Verrohrung; Wasser; > 10,16 ≤ 20,3...	IEEE Std 493-2007 gold Book (156)	0.994321376	1.000000000	1.000000000	4614729.40...	0.000000	0.0000	0.000000		26280	1	
Filtersieb; Wasser; > 10,16 cm	IEEE Std 493-2007 gold Book (176)	0.997245736	1.000000000	0.999506093	9528423.50...	0.000000	6411.0000	3.168000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	
Ventil; Geradsitzventil, normal geö...	IEEE Std 493-2007 gold Book (228)	0.999711392	1.000000000	0.999999612	91044470.6...	0.000000	1031837.00...	0.400000		26280	1	

Komponente

Hinzufügen Ändern aufwärts

Entfernen Duplizieren abwärts

Leeren Vorhandenes System kopieren

Verlässlichkeit Einzelsystem

Zuverlässigkeit R(t):

Verfügbarkeit inhärent Ai:

Verfügbarkeit operativ Ao:

Redundanzkonfiguration

Teilsystemzahl n(+m):

Ersatzsystem vorhanden:

Identische Systeme gesamt:

Verlässlichkeit des Systems

Zuverlässigkeit R(t):

Verfügbarkeit inhärent Ai:

Verfügbarkeit operativ Ao:

Manuelle Dateneingabe:

Systemfunktion

Normalbetrieb

abgeschaltet und inaktiv

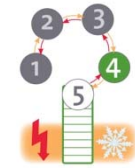
entfernt und überbrückt

Übernehmen Abbrechen

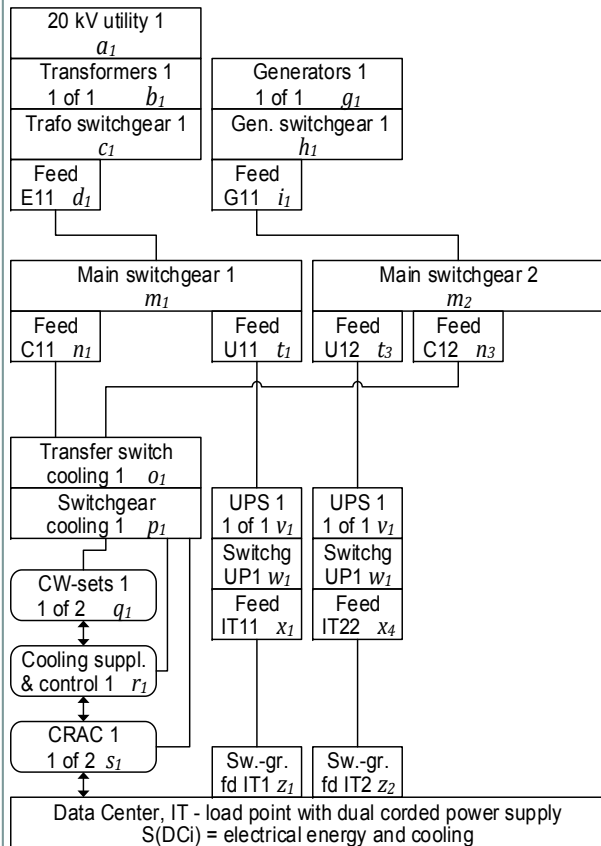
Boolesches Modell
 $2 (P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16 P17 P18 P19 P20 P21 P22 P23 P24 P25 P26)^{\wedge} 1 - 1 (P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16 P17 P18 P19 P20 P21 P22 P23 P24 P25 P26)^{\wedge} 1 - 1$

3.1 Verlässlichkeitsanalyse mittels InfraOpt[®]

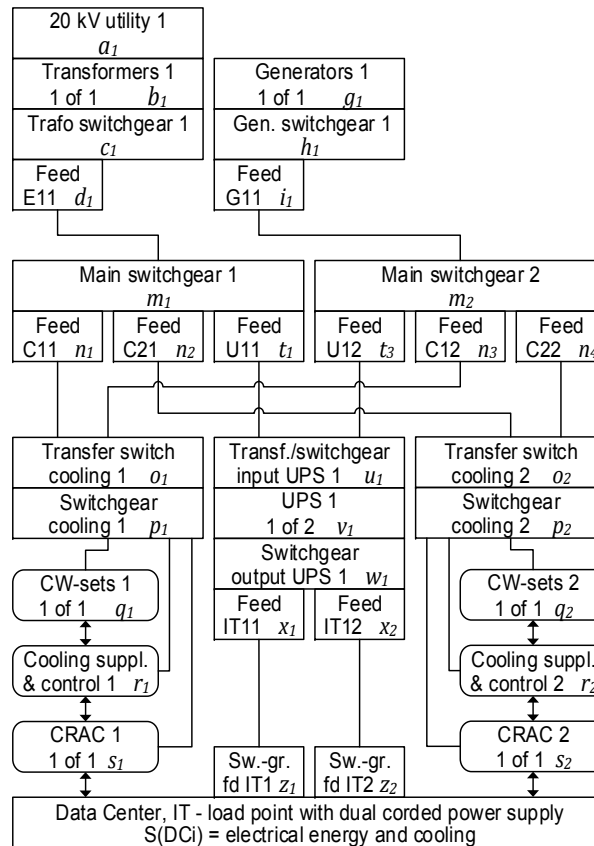
Variantenvergleich verschiedener Redundanzkonzepte



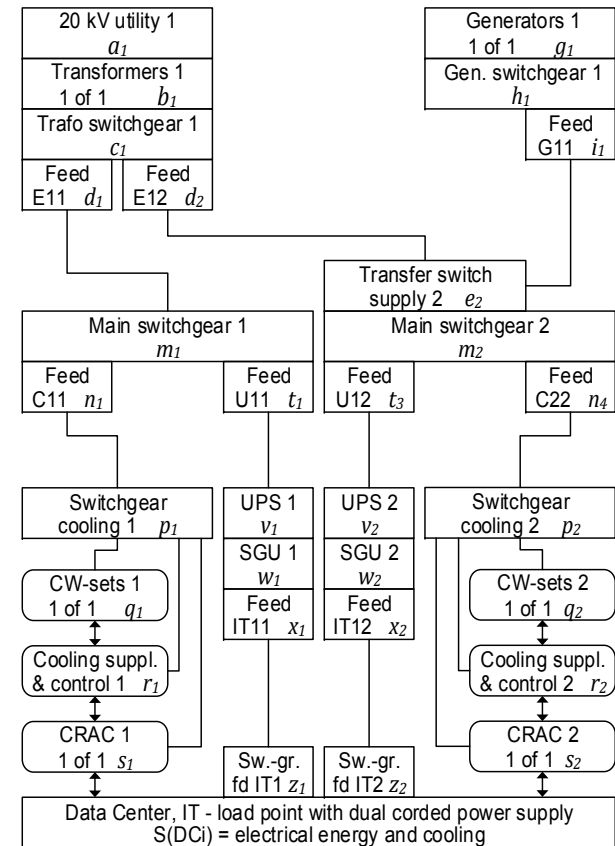
Design 2: $2N_E, N_C+1$



Design 3: $N_E+1, 2N_C$



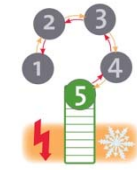
Design 4: $2N_E, 2N_C$



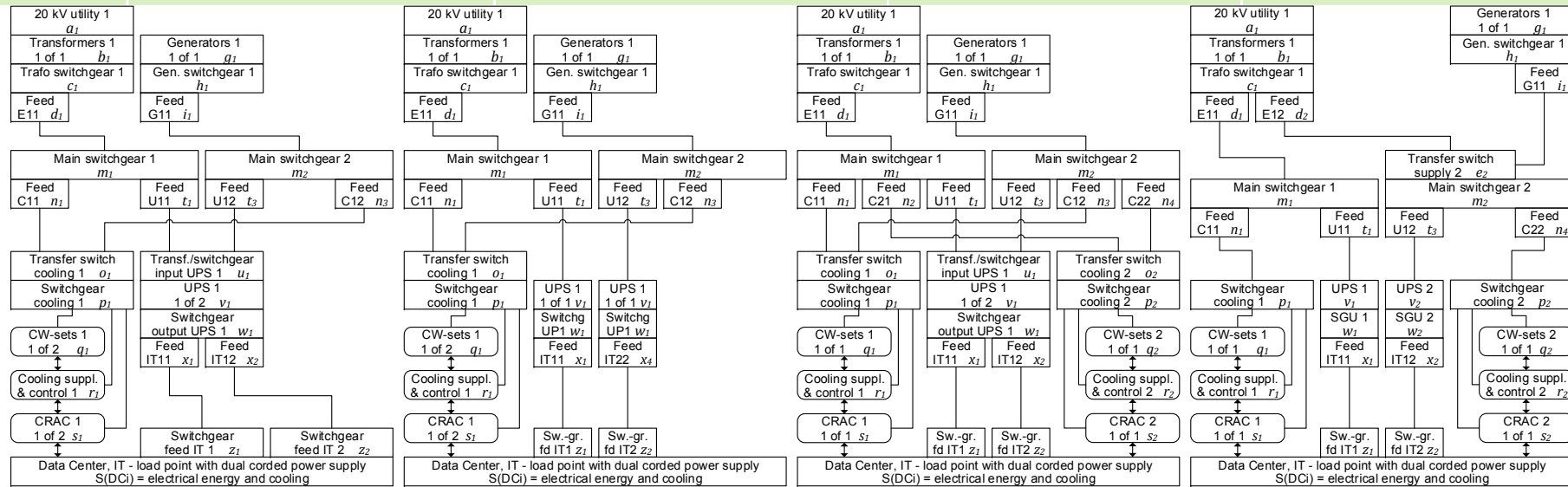
Identische Komponentendaten für die Designs 1 bis 4
Datenquelle: IEEE Std. 493-2007, Annex Q

3.2 Verlässlichkeitsanalyse mittels InfraOpt[®]

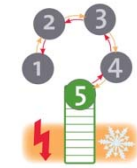
Metriken zum Bewerten von Infrastrukturen



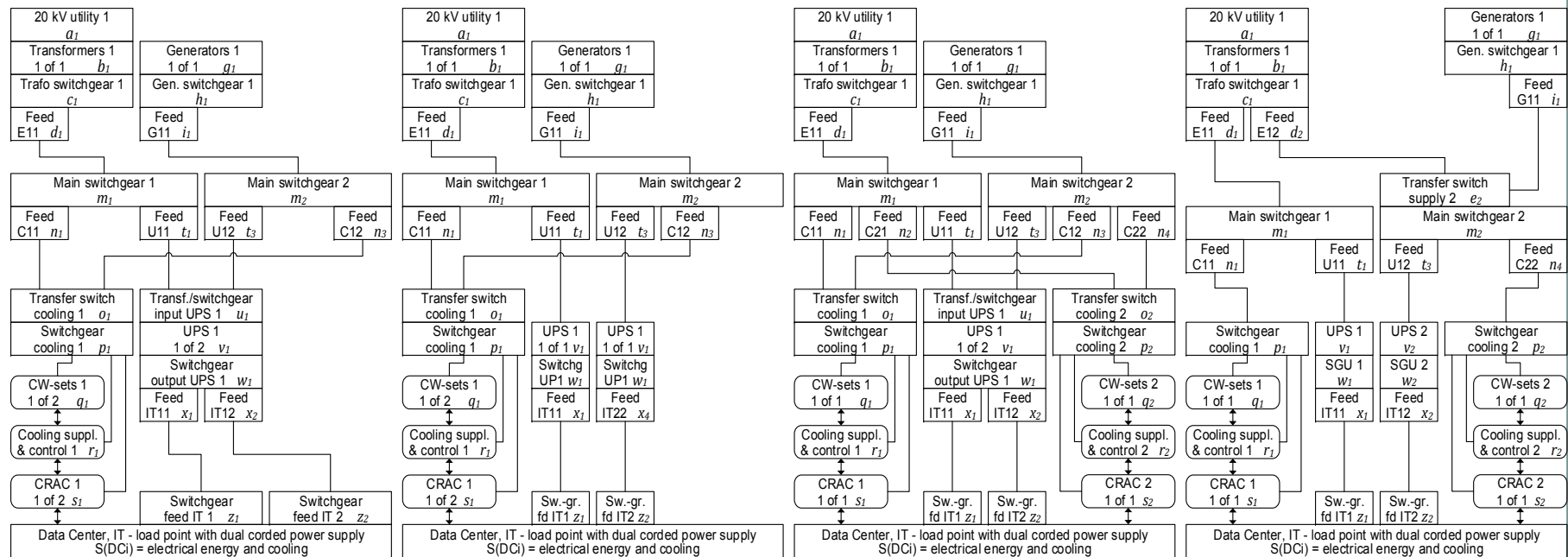
Design	N_{E+1}, N_{C+1}	$2N_E, N_{C+1}$	$N_{E+1}, 2N_C$	$2N_E, 2N_C$
N	25	26	32	31
R(t=1J)	0,82629	0,83885	0,83733	0,80050
A_i	0,99996	0,99998	0,99998	0,99999
A_o	0,99261	0,99392	0,99854	0,99982
SPoF	5 von 25	3 von 26	2 von 32	0 von 31
DPoF	146 von 300	156 von 325	120 von 496	139 von 465



3.3 Verlässlichkeitsanalyse mittels InfraOpt[®] Klassifizierung zum Bewerten von Infrastrukturen

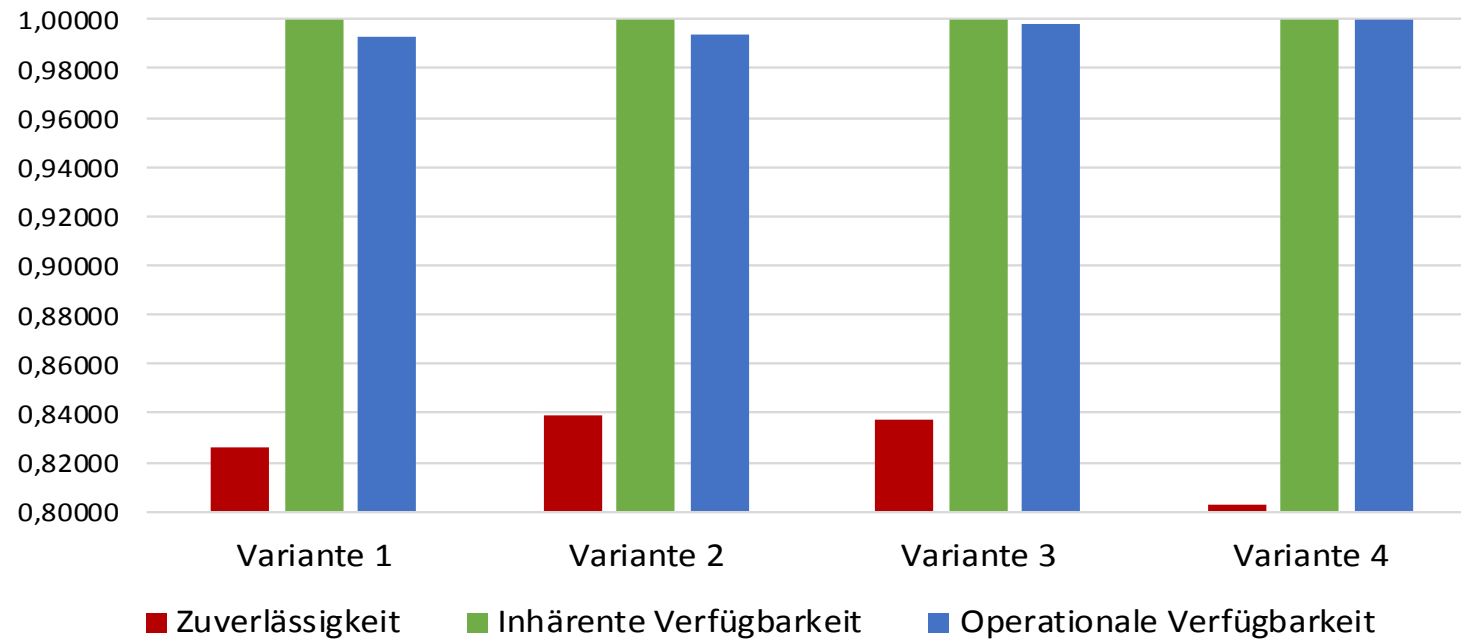


Einteilung nach A_o	99,261 %	99,392 %	99,854 %	99,982 %
Uptime Institute	< Tier 1	< Tier 1	Tier 3	Tier 3
BSI Verfüg.-klasse	< VK 0	< VK 0	~ VK 2	~ VK 3
BITKOM Kategorie	< Kat. A	< Kat. A	Kategorie A	~ Kategorie B
Redundanz nach DIN EN 50600 ff.	VK 2	VK 3	VK 2	VK 4 erweitert

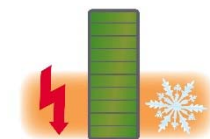
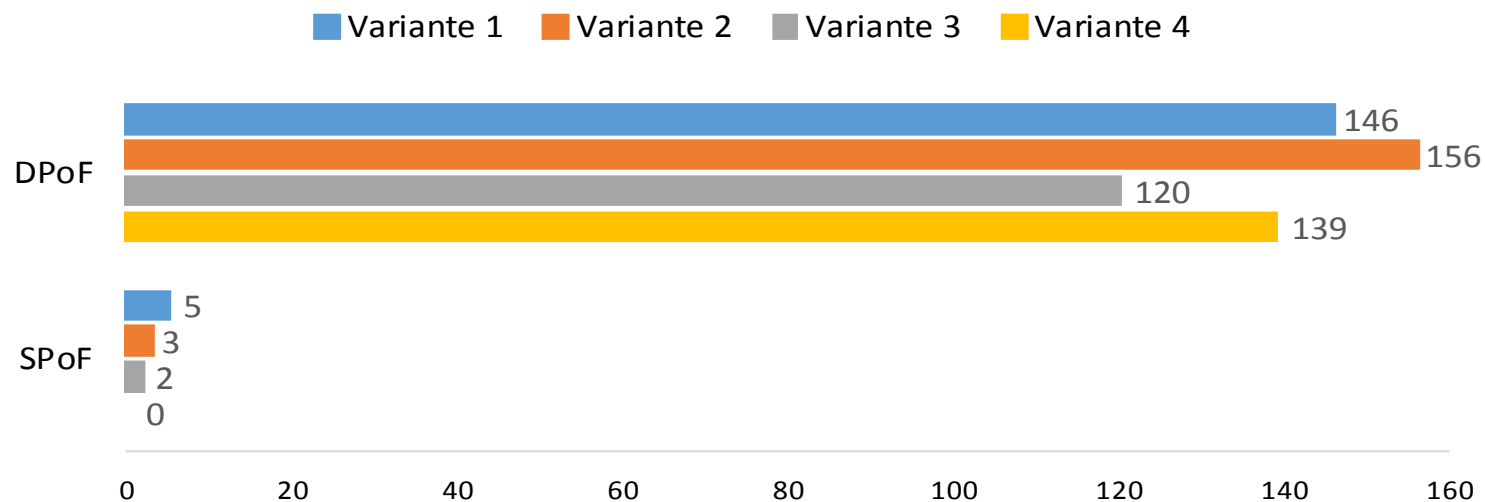


3.4 InfraOpt® Analysen

Verfügbarkeitsanalyse



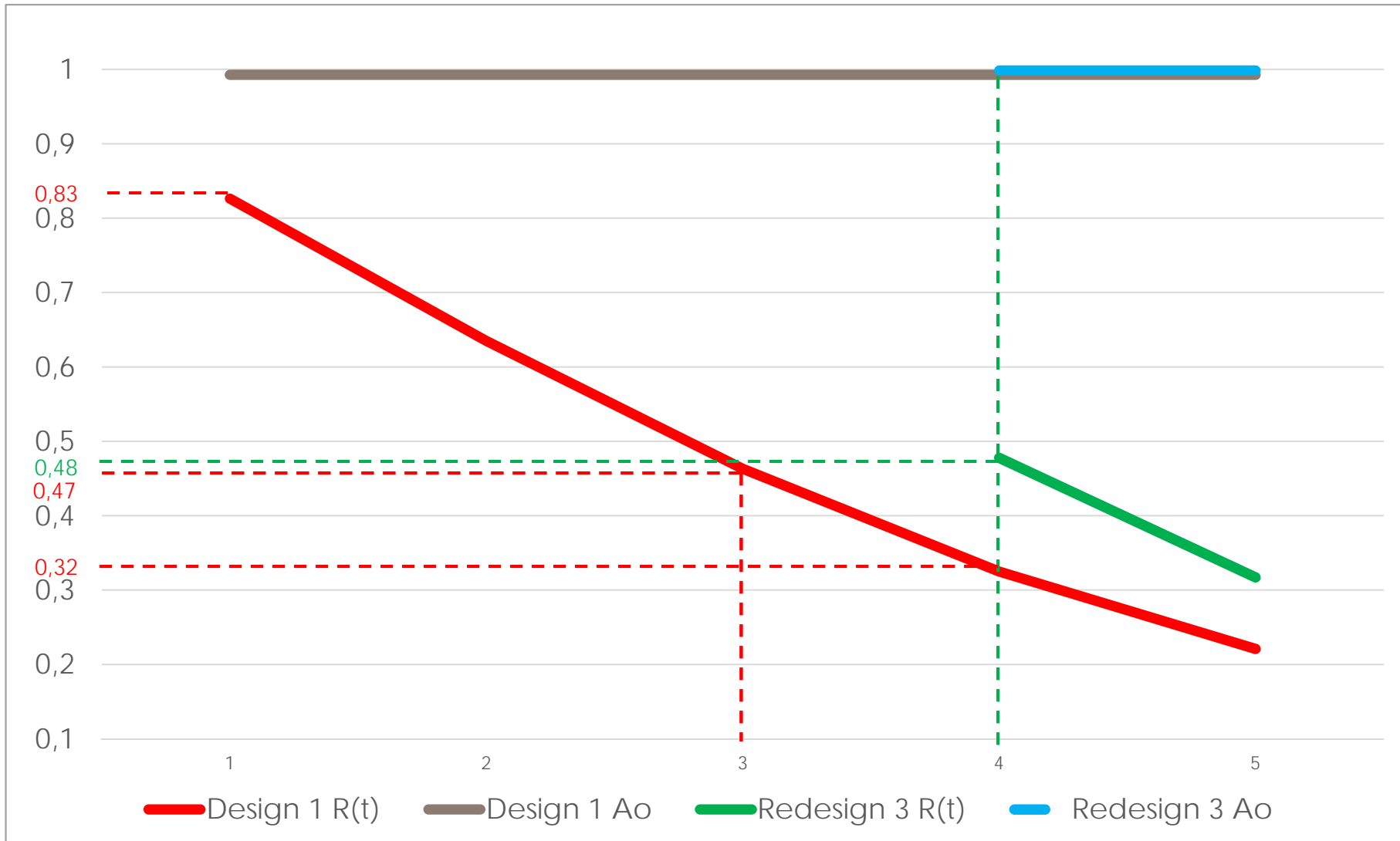
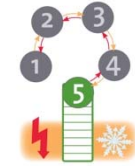
Fehleranalyse



3.5 Zuverlässigkeit und Operationale Verfügbarkeit

Design 1: $R(t = 1 \dots 5 \text{ Jahre})$

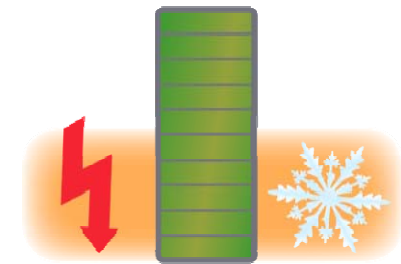
Design 3: $R(t = 4 \dots 5 \text{ Jahre})$



4.1 InfraOpt[®] – für Entscheider, Planer, Betreiber, Co-Locator Methodik zur Optimierung von RZ-Infrastrukturen

Vorhersage der Reaktion der Rechenzentrums-Infrastruktur auf **geplante** bzw. **ungeplante Ereignisse** - auf der Grundlage numerischer **Metriken**.

- Bewertung beliebiger **Designs / Kategorien / Verfügbarkeitsklassen**
- Bewertung beliebiger **Redundanzanordnungen**
- Bewertung von Komponenten hinsichtlich **MTBF** bzw. **MTTR**
- **Variantsimulation** beim Design und Redesign:
 - **Identifizieren** von **Schwachstellen**
 - **Investitionsbegründung** auf der Grundlage von Metriken
 - Bestimmung des „herabgesetzten **Ausfallsicherungsgrades**“ in Schalt- oder Wartungssituationen gemäß **DIN EN 50600-2-2**
 - Validierung von **Service-Level-Agreements**
 - Optimieren von **Wartungs-** und **Serviceplänen**
- **Zuverlässigkeitsbewertung** für Informationssicherheits-Managementssysteme gemäß **DIN ISO 27001**

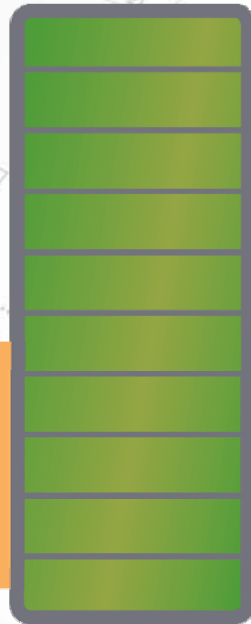


Der Analyse und Optimierung
Ihrer RZ-Infrastruktur sehe ich
mit Interesse entgegen.

Dipl.-Ing. Uwe Müller

Geschäftsführender Gesellschafter

ibmu.de[®] Ingenieurgesellschaft für
technische Beratung, Medien
und Systeme mbH



InfraOpt[®]

A.1 InfraOpt[®]

Forschungs- und Entwicklungsvorhaben



- August 2009 – Dezember 2011: FuE-Vorhaben **InfraOpt[®]**
 - FuE-Vorhaben für KMU, **Investitionsbank des Landes Brandenburg**
 - Externe Partner: **Technische Universität Berlin, Prof. Strunz**; Universität Potsdam, Prof. Schaub; Associate Prof. C. M. Welzig (USA)
 - Ergebnis: **Dienstleistungsprozess** basierend auf **Simulationssoftware InfraOpt64**
- Wissenschaftliche Veröffentlichungen
 - 2012 **IEEE PES ISG**, "Integrated Reliability Modeling for Data Center Infrastructures: A Case Study"
 - 2015 ...
- Juni 2014 – Mai 2016: FuE-Vorhaben **InfraOpt[®] REALTIME** 
 - FuE-Vorhaben für KMU, **Investitionsbank des Landes Brandenburg**
 - Externe Partner: **Technische Universität Berlin, Prof. Strunz**; Associate Prof. C. M. Welzig (USA)