Neue Metriken zur Ausfallsicherheit von Rechenzentren

***S**ingle **P**oints **o**f **R**educed **A**vailability*

***D**ouble **P**oints **o**f **R**educed **A**vailability*

Dipl.-Ing. Uwe Müller · InfraOpt GmbH · 13. Juni 2017 · Frankfurt/Main

Neue Metriken zur Ausfallsicherheit von Rechenzentren

Agenda · 13. Juni 2017 · Frankfurt/Main

Herleitung zur Notwendigkeit analytischer Verfahren

- Die Rechenzentrumsnorm DIN EN 50600
- Qualitative Bewertung vs. Kennzahlen im Kontext RZ

Etablierte und neue Kennzahlen der Ausfallsicherheit

- Zuverlässigkeit, Verfügbarkeit, 1- und 2-Fehlertoleranz
- Einführung der neuen Kennzahlen: ***SPoRA*** und ***DPoRA***

InfraOpt

- Prozess der Modellierung und Analyse
- Beweis der Aussagekraft ***SPoRA*** und ***DPoRA***
- Timeline zur Forschung, Entwicklung, Zertifizierung

InfraOpt®

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: BITKOM e. V., Betriebssicheres Rechenzentrum, Leitfaden 2013

Verfügbarkeitsklasse EN 50600	VK 1	VK 2	VK 3	VK 4	VK 4 erweitert
Verfügbarkeit	**niedrig**	**mittel**	**hoch**	**sehr hoch**	
EN 50600-2-2 Stromversorgung	keine Redundanz	Komponenten Redundanz	Instandsetzung im lfd. Betrieb	**Fehlertoleranz** (Transferschalter)	
Versorgungspfade	**Einer, *N***	**Einer, *N*+1**	**Mehrere, 2*N***	**Mehrere, 2*N***	
Herabgesetzte **Ausfallsicherheit**	nicht erwähnt	nicht erwähnt	nicht erwähnt	**relevant**	
EN 50600-2-3 Regelung der Umgebungsb.	-	keine Aus-fallsicherheit	Komponenten Redundanz	Instandsetzung im laufenden Betrieb	
Versorgungspfade	-	**Einer, *N***	**Einer, *N*+1**	**Einer, *N*+1**	**Mehrere, 2*N***
Herabgesetzte **Ausfallsicherheit**	nicht erwähnt	nicht erwähnt	nicht erwähnt	**relevant** (da abh. von Stromversorgung)	

Quellen: DIN EN 50600-1 2013, DIN EN 50600-2-2 2014, DIN EN 50600-2-3 2015

VK 1…4 assoziieren **keine quantitativen Verfügbarkeitsangaben**.
Anforderungen zur **Ausfallsicherheit** (resilience) **werden** referenziert!

Ausfallsicherheit (resilience) des Rechenzentrums

Qualitäten im Kontext **EN 50600**

- MTBF/MTTR stehen in Zusammenhang mit der Verfügbarkeitsklasse
- Verfügbarkeitsklassen (niedrig, mittel, hoch, sehr hoch)
- Redundanz, Versorgungspfade 2*N* bzw. *N*+1 (Fehlertoleranz)
- Ausfallsicherheitsgrad (herabgesetzt)

Kennzahlen der **Ausfallsicherheit** mittels **InfraOpt**

- Zuverlässigkeit (reliability) *R(t)*
- Inhärente Verfügbarkeit (inherent availability) A_i
- Operationale Verfügbarkeit (operational availability) A_o
- 1-Fehler-Toleranz (Single Point of Failure) *SPoF*
- 2-Fehler-Toleranz (Double Point of Failure) *DPoF*
- Neu: **Single Point** of **Reduced Availability** *SPoRA*
- Neu: **Double Point** of **Reduced Availability** *DPoRA*

InfraOpt®

	Rechenzentrumszertifizierung	Analytik der Ausfallsicherheit
Bewertungsprinzip der **Infrastruktur**	**Qualitativ**: Checklisten bzw. Kriterienkataloge	**Quantitativ**: Berechnung von **Kennzahlen**
Anbieter	Uptime Institut, TÜV Nord/Süd/ Rheinland/Hessen, BSI, eco, ...	InfraOpt GmbH …
Ergebnis	Tier I … IV oder Level I … IV (+) oder Kategorie I … IV oder 1 … 5 Stars oder Verfügbarkeitsklasse 1 … 4	**Zuverlässigkeit,** inhärente und operationale **Verfügbarkeit**, **1** – und **2** – **Fehlertoleranz**, SPoF, DPoF, SPoRA, DPoRA Verfügbarkeitsklasse 1 … 4
Kennzahlen	☒ nein	☑ **Ja**
Optimierung	☒ nein	☑ **Ja**
Investitionsplanung	☒ nein	☑ **Ja**
SLA-Validierung	☒ nein	☑ **Ja**
BIM-Integration	☒ nein	Perspektivisch **möglich**

InfraOpt®

Kennzahlen: **Verlässlichkeit** (dependability)

Zuverlässigkeit $R(t) = e^{-t/MTBF}$

- Merkmal für die Wahrscheinlichkeit, dass das RZ die Funktion erfüllt
- Berücksichtigt die Ausfallrate von Komponenten im Verlauf der Zeit

Inhärente Verfügbarkeit $A_i = MTBF / (MTBF + MTTR)$

- Berechnete Verfügbarkeit auf Grundlage der eingesetzten Komponenten und Systeme

Operationale Verfügbarkeit $A_o = MTBM / (MTBM + MDT)$

- Berechnete Verfügbarkeit, berücksichtigt Wartungen, Umbauten, Elementarereignisse, Fehlhandlungen, tatsächliche Liefer- und Reparaturzeiten usw.

Kennzahlen: **Fehlertoleranz**

Single Point of Failure: $|\boldsymbol{SPoF}| = \boldsymbol{N}$

- Anzahl der 1-Fehlerpunkte, durch welche die DCI ausfallen kann
- Analytische Bestimmung der Verfügbarkeitsklassen nach EN 50600-2-2 „Stromversorgung“ und EN 50600-2-3 „Regelung der Umgebungsbedingungen“

Double Point of Failure: $|\boldsymbol{DPoF}| = \binom{\boldsymbol{N}}{\boldsymbol{k}}; \boldsymbol{k} = \mathbf{2}$

- Anzahl der 2-Fehlerkombinationen, durch welche die DCI ausfallen kann
- Vorhersage, wie die DCI im Fall von geplanten oder ungeplanten Fehlerereignissen reagiert
- Bestimmung des „herabgesetzten Ausfallsicherungsgrades“ gemäß EN 50600-2-2

Weshalb zwei **neue Kennzahlen** zur **Ausfallsicherheit**?

Nachteile der **Verfügbarkeitsanalyse**

- Berücksichtigt das tatsächliche Rechenzentrumsdesign ungenügend
- Ungeeignet für Optimierungsverfahren auf Grund relativ geringer „Auflösung“
- Bestimmung des „herabgesetzten Ausfallsicherungsgrades“ gemäß EN 50600-2-2 nicht möglich

Nachteile der **Designspezifikation** nach ***2N*** bzw. ***N+1***

- Ungenügend definiert, bspw. für: $N = 1$ gilt: $N + 1 = 2\,N$
- Ungenügende Berücksichtigung der integralen Betrachtung, die EN 50600-2-2 und EN 50600-2-3 als notwendige Dienste umschließt
- Bestimmung des „herabgesetzten Ausfallsicherungsgrades“ gemäß EN 50600-2-2 nicht möglich

Neue Kennzahlen: Betrachtung der **Verfügbarkeit** im **Fehlerfall**

Single Point of **Reduced Availability**: $|SPoRA|$

- Anzahl der Punkte, bei deren Ausfall die minimal akzeptable operationale Verfügbarkeit der DCI unterschritten ist.
- Bestimmt den „**herabgesetzten Ausfallsicherungsgrad**“ gemäß EN 50600-2-2
- Operationale **Verfügbarkeit** des RZ **während geplanter** oder **ungeplanter 1-Fehlerereignisse**

Double Point of **Reduced Availability**: $|DPoRA|$

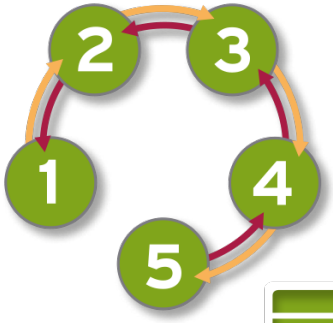
- Anzahl der 2-Fehlerkombinationen, bei deren Ausfall die minimal akzeptable operationale Verfügbarkeit der DCI unterschritten ist.
- Operationale **Verfügbarkeit** des RZ, sofern während geplanter oder ungeplanter 1-Fehlerereignisse das **2. Fehlerereignis** eintritt

$SPoRA$ und $DPoRA$ sind **aussagekräftig** für **Optimierungsverfahren**!

InfraOpt®

InfraOpt: **Dienstleistungsprozess** in fünf Schritten

1. **Rezeption des Designs**
2. **Boolesche Modellierung**
3. **Datenaufbereitung**
4. **Numerische Analyse**
5. **Optimierungen**



www.infraopt.eu

Praxiserprobt: Automotive, Colocation, Industrie, Telekommunikation

InfraOpt®

Rechenzentrums-Versorgungs-Infrastruktur

Data Center Infrastructure (**DCI**)

Notwendige Teilsysteme der **DCI**:

- Power Distribution – Stromversorgung EN 50600-2-2
- Environmental Control – Regelung der Umgebungsbedingungen EN 50600-2-3

Systemerfolg S eines **Lastpunktes** (z.B. Servers):

- $S(Loadpoint) = S(Power) \wedge S(Environmental\ Control)$
- Ein Erfolgspfad beschreibt genau eine notwendige, minimale, ununterbrochene Funktionskette zum Lastpunkt
- Redundanzen bzw. Transferschalter dienen zur Vermehrung Erfolgspfade

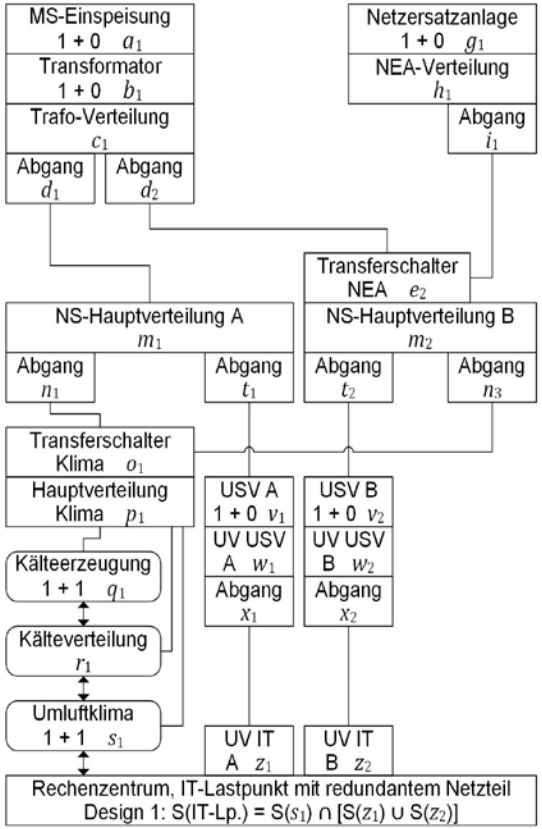
Prinzip der **Modellierung** mittels **InfraOpt**:

- Boolesche Algebra mit Disjunktstellung der Erfolgspfade gemäß EN 61078:2006
- Berechnung der Kennzahlen *R(t)*, A_i, A_o; vollständige Simulation *SPoF*, *DPoF*

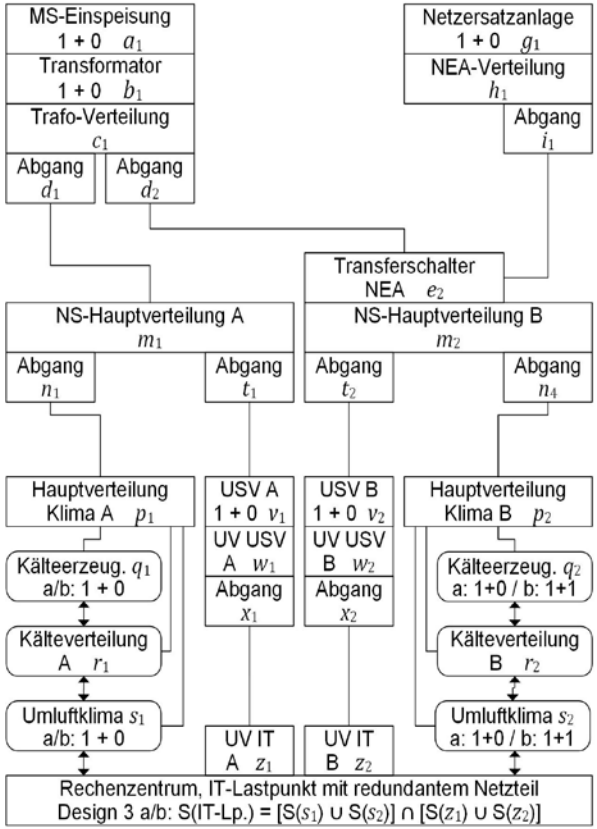
InfraOpt®

Analyse der **Ausfallsicherheit** von **Designvarianten**

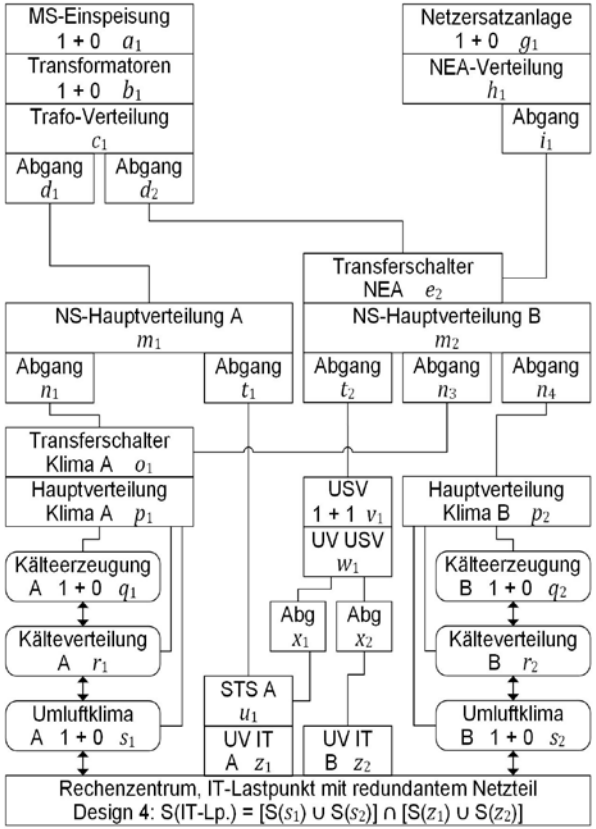
Design 1: $2N_E$ & N_C+1



Design 3 a/b: $2N_E$ & $2N_C$



Design 4: $2N_E$ & $2N_C$



InfraOpt®

Analyse der **Ausfallsicherheit** von **Designvarianten**

Metrik	Design 1 $2N_E$ & N_C+1	Design 3 a $2N_E$ & $2N_C$	Design 3 b $2N_E$ & $2N_C$	Design 4 $2N_E$ & $2N_C$
$N_{k=1}$	28	31	31	32
$N_{k=2}$	378	465	465	496
$R(t=1\ a)$	0,8304	**0,8006**	**0,8749**	**0,8660**
A_i	**0,9999**	**0,9999**	**0,9999**	**0,9999**
A_o	**0,9938**	0,9998	**0,9999**	**0,9999**
SPoF	**3**	**0**	**0**	**0**
DPoF	**165**	139	**119**	**82**
SPoRA	**28**	27	25	**20**
DPoRA	**378 (100 %)**	462	453	**442**

Systeme und Komponenten konsistent; *SPoRA*, *DPoRA* bezogen auf A_o = 0,9967

InfraOpt®

Ergebnisdiskussion der Variantenanalyse

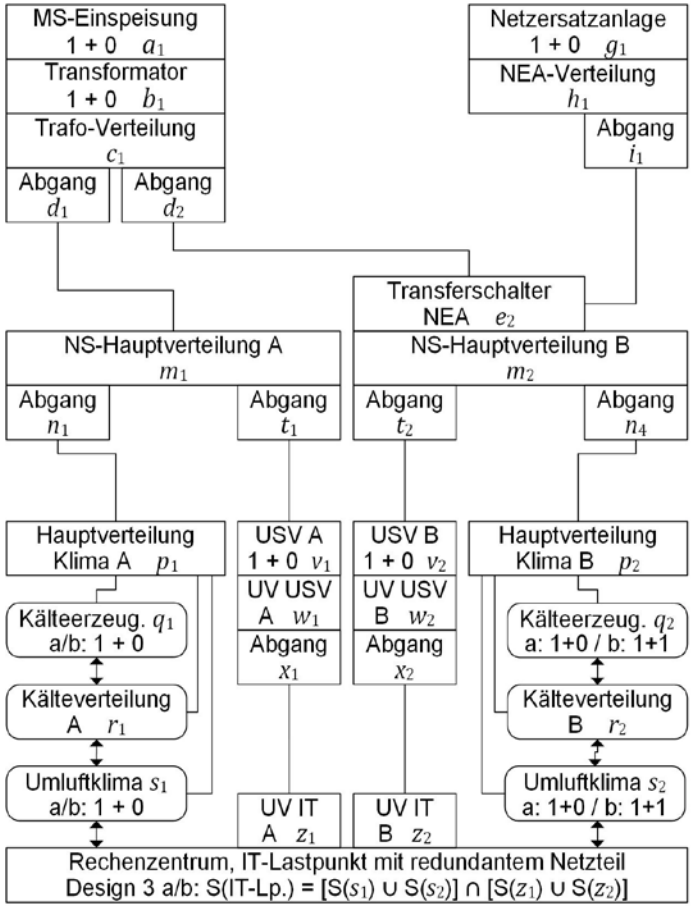
Design 3 a: $2N_E$ & $2N_C$

- ☺ Keine *SPoF*
- ☹ Schlechteste Zuverlässigkeit aller Beispiele!

Design 3 b: $2N_E$ & $2N_C$

- ☺ Keine *SPoF*, weniger *DPoF* als Design 3 a, beste Zuverlässigkeit der Beispiele
- ☹ Aufwändige Klimatisierung, resultierend in höheren CAPEX und OPEX

Frage: Sind ***A*$_i$**, ***A*$_o$**, ***SPoF*** zum **Variantenvergleich hinreichend geeignet**?



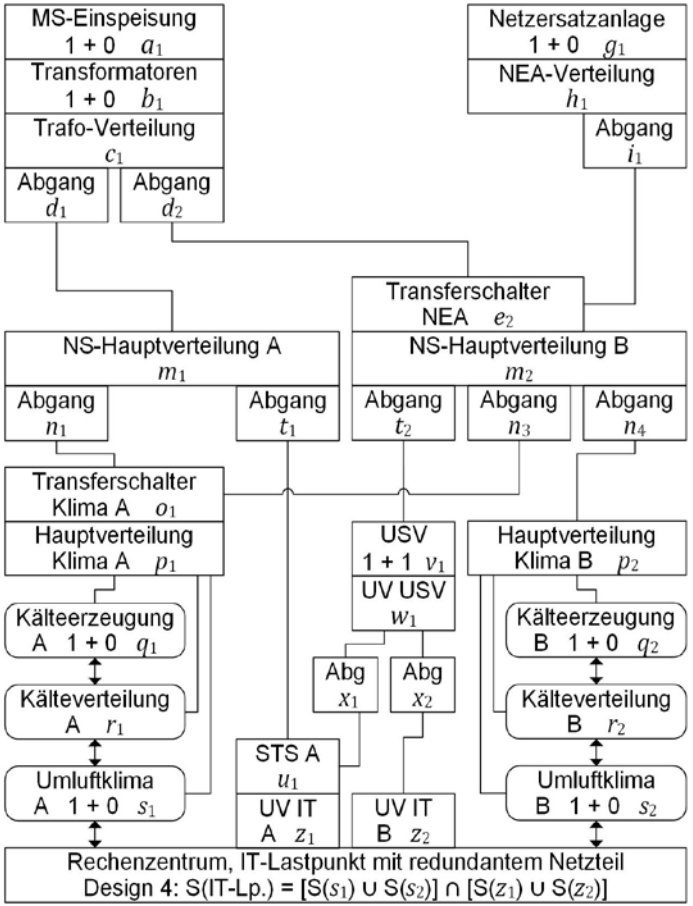
Ergebnisdiskussion der **Variantenanalyse**

Design 4: $2N_E$ & $2N_C$

- ☺ Keine *SPoF*, geringste Anzahl *DPoF*
- ☺ Beste inhärente und operationale Verfügbarkeit, zweitbeste Zuverlässigkeit
- ☺ ***SPoRA*** und ***DPoRA*** belegen die **höchste Ausfallsicherheit** der beispielhaften Variantenanalyse

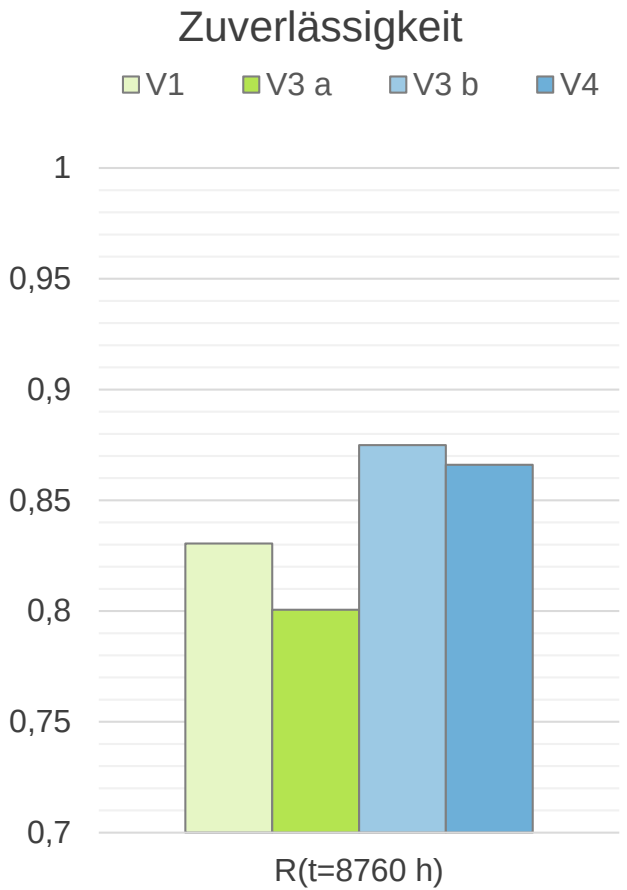
A_i, ***A_o***, ***SPoF*** sind zum **Variantenvergleich nicht hinreichend geeignet**!

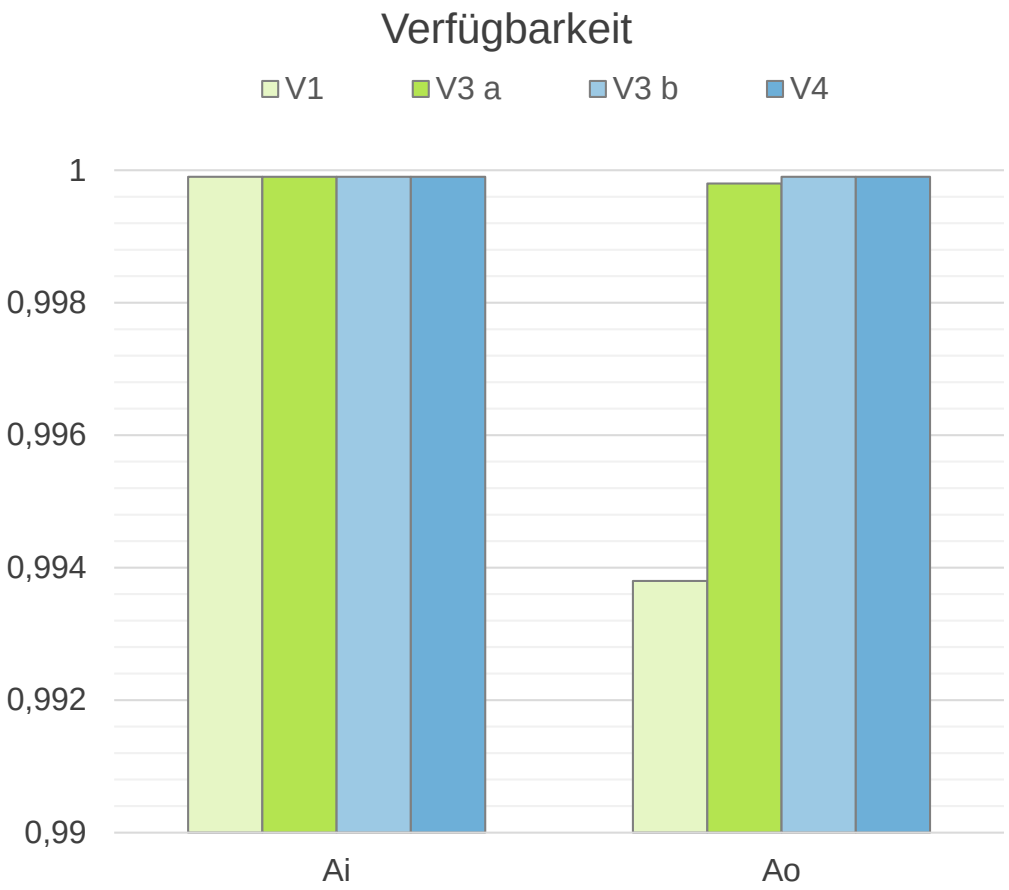
SPoRA und ***DPoRA*** beweisen **Aussagekraft**, auch für **Optimierungsverfahren.**



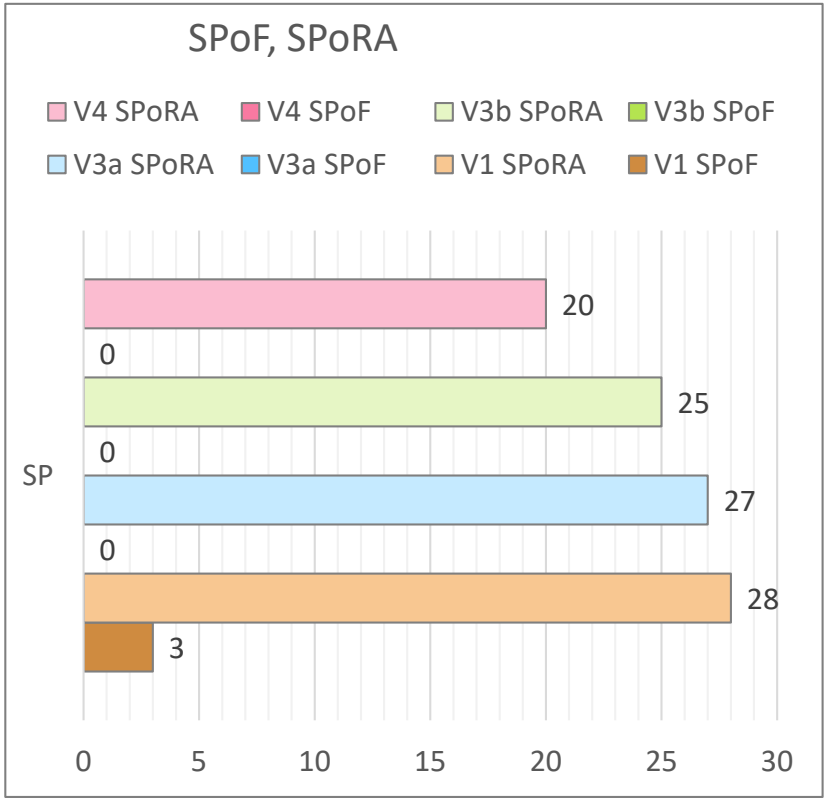
InfraOpt®

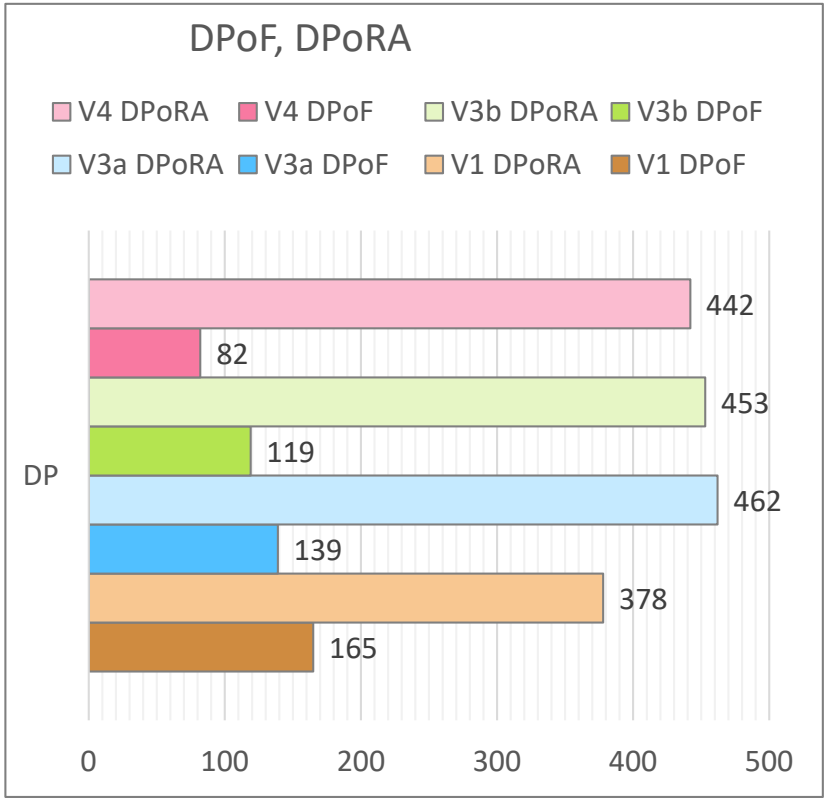
Variantenanalyse: Optimierung Zuverlässigkeit und Verfügbarkeit





Beispiel: Optimierung der Fehlertoleranz





IntraOpt®

2009 2011 — **FuE-Vorhaben**: Investitionsbank des Landes Brandenburg; TU Berlin, Prof. Strunz; Uni Potsdam, Prof. Schaub; Ass. Prof. Welzig (USA)

2012 — **IEEE PES ISGT Europa**, Publikation: “Integrated Reliability Modeling for Data Center Infrastructures: A Case Study”

2013 — **Fünf-Stufen-Dienstleistungsprozess**
Simulationssoftware InfraOpt64

2014 2016 — **FuE-Vorhaben**: Investitionsbank des Landes Brandenburg; Technische Universität Berlin, Prof. Strunz

Juni 2017 — **InfraOpt GmbH**: Begutachtung, Analyse, Evaluation und Zertifizierung von technischen Infrastrukturen insbesondere Rechenzentren

Juni 2017 — Annahme des **ANTRAG** zur Prüfung der Akkreditierungsfähigkeit von Konformitätsbewertungsprogrammen durch die **DAkkS**.

Investition in **Ihre** Zukunft!
EUROPÄISCHE UNION
Europäischer Fonds für Regionale Entwicklung
www.efre.brandenburg.de

InfraOpt®

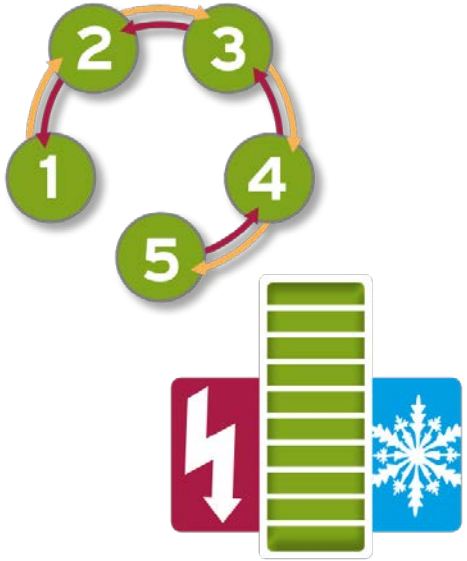
Akronyme

- A_i Inherent availability
- A_o Operational availability
- DAkkS Deutsche Akkreditierungsstelle GmbH
- DCI Data center infrastructure
- $DPoF$ Double point of failure
- $DPoRA$ Double point of reduced availability
- EN European standard
- IEEE Institute of Electrical and Electronics Engineers
- ibmu.de Ingenieurgesellschaft für technische Beratung, Medien und Systeme mbH
- MDT Mean downtime
- $MTBF$ Mean time between failure
- $MTBM$ Mean time between maintenance
- $MTTR$ Mean time to repair
- $R(t)$ Reliability
- $SPoF$ Single point of failure
- $SPoRA$ Single point of reduced availability

Dipl.-Ing. Uwe Müller
Inhaber und Geschäftsführer

InfraOpt GmbH
Puschkinstr. 23 · 14943 Luckenwalde · Germany
www.infraopt.eu · uwe.mueller@infraopt.eu
Tel: +49 3371 6433-55 · Mob: +49 172 8368 939
Amtsgericht Potsdam HRB 30023

InfraOpt®



Präventives Risikomanagement für
ausfallsichere Data Center Infrastrukturen.

Ich freue mich auf Ihre Fragen.