Datacenter Symposium

LANline Events

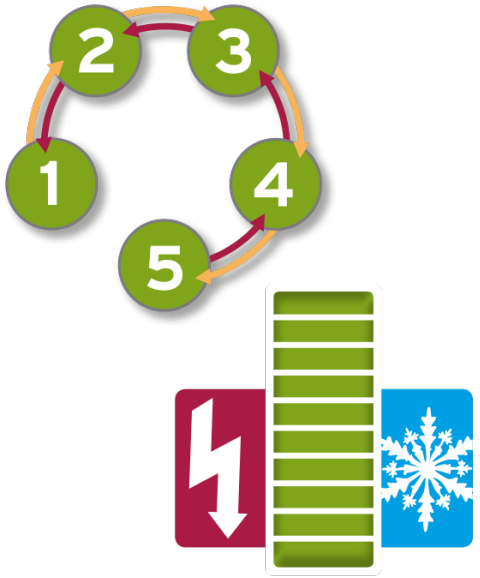
PRÄSENTIERT

Resilienz?

Zuverlässigkeit, Verfügbarkeit und Fehlertoleranz von Rechenzentren!

Ein Beitrag von

Dipl.-Ing. Uwe Müller
Geschäftsführender Gesellschafter
InfraOpt® GmbH



www.infraopt.eu

DIN EN 50600	VK 1	VK 2	VK 3	VK 4	VK 4 erw.
Verfügbarkeit	**niedrig**	**mittel**	**hoch**	**sehr hoch**	
DIN EN 50600-2-2 Stromversorgung	keine Redundanz	Komponenten Redundanz	Instandsetzung im lfd. Betrieb	**Fehlertoleranz** (Transferschalter)	
Ausfallsicherheit (resiliency) durch Versorgungspfade	**Einer, *N***	**Einer, *N*+1**	**Mehrere, 2*N***	**Mehrere, 2*N***	
Herabgesetzte Ausfallsicherheit	-	-	-	**relevant**	
DIN EN 50600-2-3 Regelung d. Umgebungsbed.	-	keine Aus-fallsicherheit	Komponenten Redundanz	Instandsetzung im laufenden Betrieb	
Ausfallsicherheit (resiliency) durch Versorgungspfade	-	**Einer, *N***	**Einer, *N*+1**	**Einer, *N*+1**	**Mehrere, 2*N***
Herabgesetzte Ausfallsicherheit	-	-	-	**relevant** (abh. von Stromversorgung)	

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

Verfügbarkeit

Verfügbarkeit (Availability):

$$\boldsymbol{A = \frac{(Betrachtungszeit - Ausfallzeit)}{Betrachtungszeit}}$$

Verfügbarkeit in %:

$$A = \frac{(Betrachtungszeit - Ausfallzeit)}{Betrachtungszeit} * 100\ \%$$

Die Zeitspannen können nur **für Data Center** ermittelt werden, die sich bereits **im Betrieb** befinden!

Resilienz (resiliency)

Synonym für:

- Belastbarkeit
- Widerstandsfähigkeit
- Stabilität
- Elastizität
- **Ausfallsicherheit** (DIN EN 50600)

„… **Fähigkeit** von technischen Systemen, bei Störungen bzw. Teil-Ausfällen **nicht** vollständig **zu versagen** …“ (Wikipedia)

SLA: **Dienst soll zu 99,99 % verfügbar sein**

Dieser Dienst erfordert folgende **fünf Anlagengruppen**:

- Externes Netzwerk (aktive und passive Komponenten)
- Internes Netzwerk (aktive und passive Komponenten)
- Server (einschließlich Storage)
- Software (Betriebssysteme, Applikationen)
- Data Center Infrastruktur (Elektroenergie, Klimatisierung)

SLA: **Dienst soll zu 99,99 % verfügbar sein**

Angenommene Verfügbarkeit der fünf Anlagengruppen:

- Netzwerk extern: $A_{Ne} = 0,99998$
- Netzwerk intern: $A_{Ni} = 0,99998$
- Server: $A_{Sv} = 0,99998$
- Software: $A_{Sw} = 0,99998$
- **Data Center Infrastruktur**: $A_{DCI} = ?$

$$A_{NS} = A_{Ne} * A_{Ne} * A_{Ne} * A_{Ne} = 0,99998^4 = 0,99992$$

$$A_{DCI} = \frac{A_{SLA}}{A_{NS}} = \frac{0,9999}{0,99992} = 0,99998$$

Erfüllt mein Data Center diese Anforderung?

1. Mein Data Center war im letzten Jahr 100 % verfügbar, bedeutet das, es ist „**höchst**“ verfügbar?
2. Wegen Wartung bzw. Umbau, muss ich mein Data Center **geplant abschalten**. Für welche Zeit darf ich das, um dennoch „hoch“ oder „sehr hoch“ verfügbar zu sein?
3. Bedeutet $A_{DCI} = 0,99998$ (bzw. 99,998 %) „**mittel**“, „**hoch**“ oder „**sehr hoch**“ verfügbar?

DIN EN 50600	VK 1	VK 2	VK 3	VK 4	VK 4 erweit.
Verfügbarkeit	niedrig	mittel	hoch	sehr hoch	

BITKOM	Kategorie A	Kategorie B	Kategorie C	Kategorie D
Zul. Ausfallzeit /Jahr	12 h	1 h	**10 min.**	**< 1 min**
➔ **Verfügbarkeit**	99,86 %	99,99 %	**99,998 %**	**99,9998 %**

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

Uptime Institut	Tier I	Tier II	Tier III	Tier IV
Representative Site Failures	6 failures / 5 year	1 failure / 1 year	1 failure / 2.5 years	1 failure / 5 years
Annual Site … Downtime	28.8 h	22.0 h	1.6 h	**0.8 h**
… End-User **Availability** …	99.67 %	99.75 %	99.98 %	**99.99 %**

Quelle: Uptime Institut, 2008, White Paper, „Tier Classifications Define Site Infrastructure Performance“, Page 14

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 %)**

Zwischenfazit

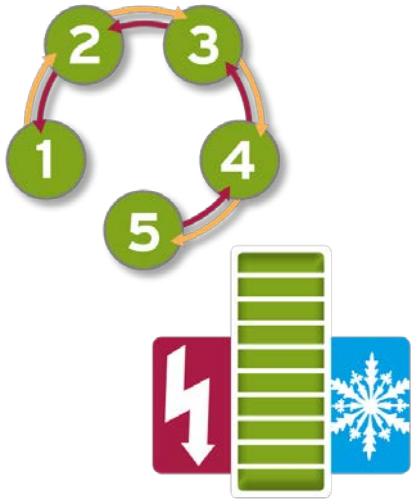
1. **Verfügbarkeit** und **Ausfallsicherheit** (resiliency) sind nicht unabhängig voneinander.
2. **Die Zuverlässigkeit** eines Data Center verringert sich mit der Zeit, denn es unterliegt der **Alterung**.
3. **Zuverlässigkeit**, **Verfügbarkeit** und **Fehlertoleranz** können berechnet werden!

„Was man nicht messen kann, kann man nicht lenken.“

Peter F. Drucker (Ökonom, *1909 Wien; †2005 Claremont)

InfraOpt Analyseprozess in fünf Schritten

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



www.infraopt.eu

Praxiserprobt: Automotive, Colocation, Industrie, Telekommunikation …

Kennzahlen der **Verlässlichkeit**

Zuverlässigkeit $R(t) = e^{-t/MTBF}$

- Merkmal für die Wahrscheinlichkeit, dass das RZ die Funktion erfüllt
- Berücksichtigt eine konstante Ausfallrate bei exponentieller Verteilungsfunktion 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, Elementar-ereignisse, Fehlhandlungen, tatsächliche Liefer- und Reparaturzeiten usw.

Kennzahlen der **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: $|\boldsymbol{DPoF}| = \binom{\boldsymbol{N}}{\boldsymbol{k}}; \boldsymbol{k} = \boldsymbol{2}$

- 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

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):

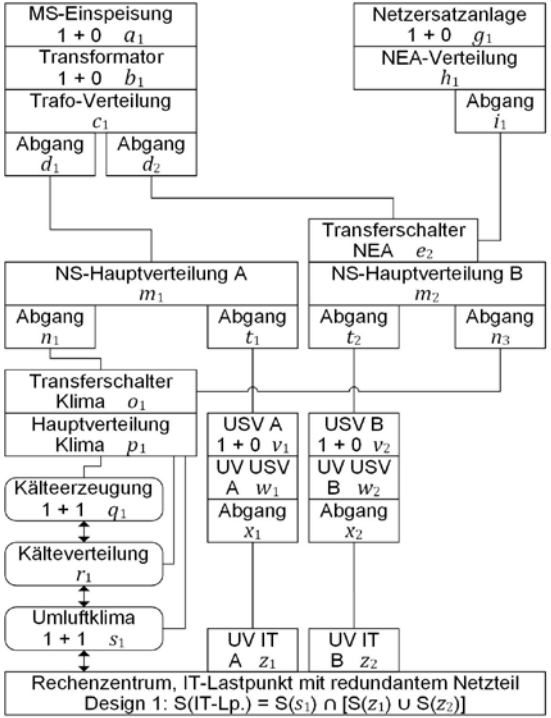
- $S(Loadpoint) = S(Power) \wedge S(Environmental\ Control)$
- Ein Erfolgspfad beschreibt genau eine notwendige, minimale, ununterbrochene Funktionskette zum Lastpunkt
- Redundanzen bzw. Transferschalter dienen zur Vermehrung Erfolgspfade

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

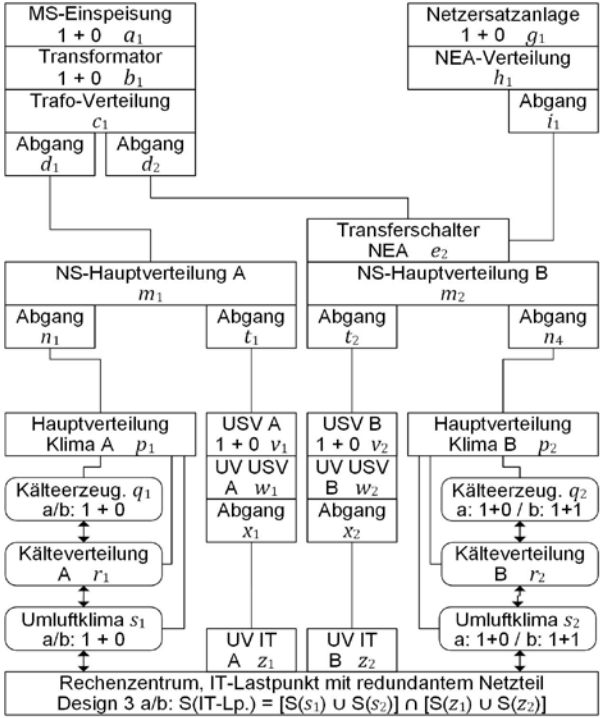
- Boolesche Algebra mit Disjunktstellung der Erfolgspfade gemäß EN 61078:2006
- Berechnung der Kennzahlen *R(t)*, A_i, A_o; vollständige Simulation *SPoF*, *DPoF*

Analyse der **Ausfallsicherheit** (resiliency) von **Designvarianten**

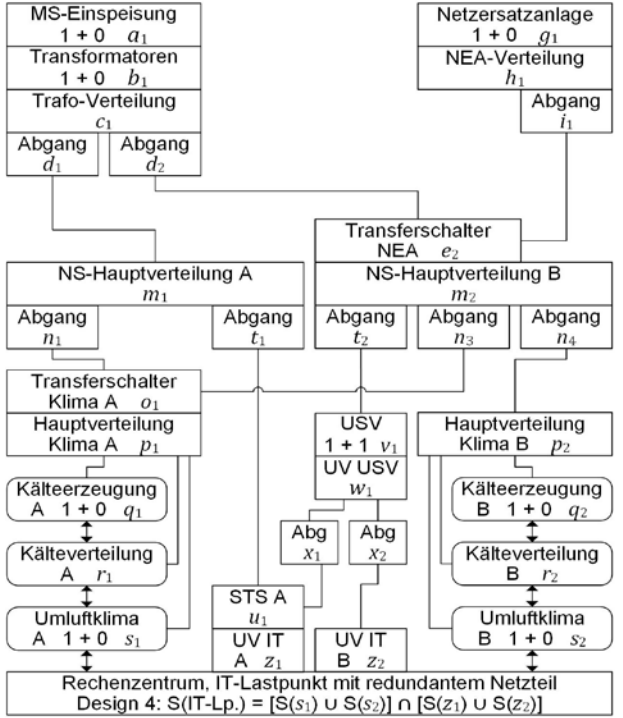
Design 1: $2N_E$ & N_C+1



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



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

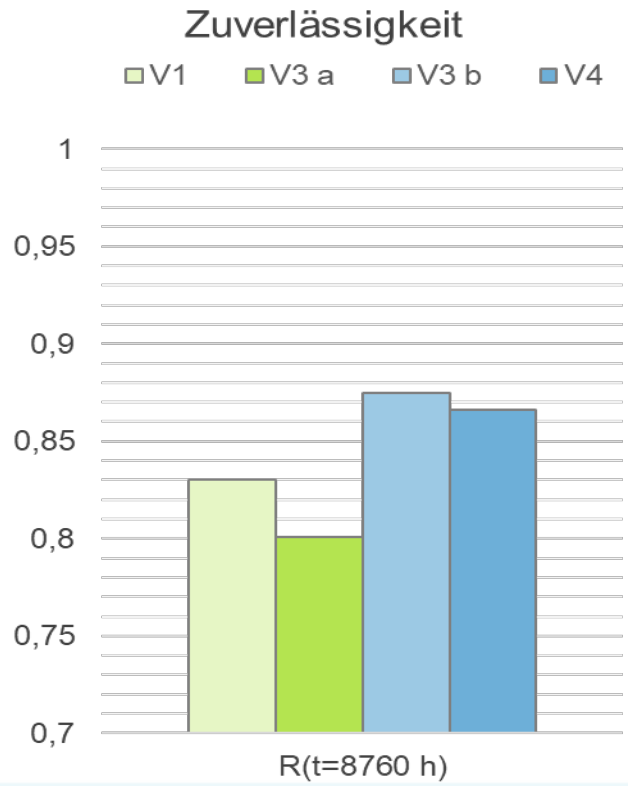


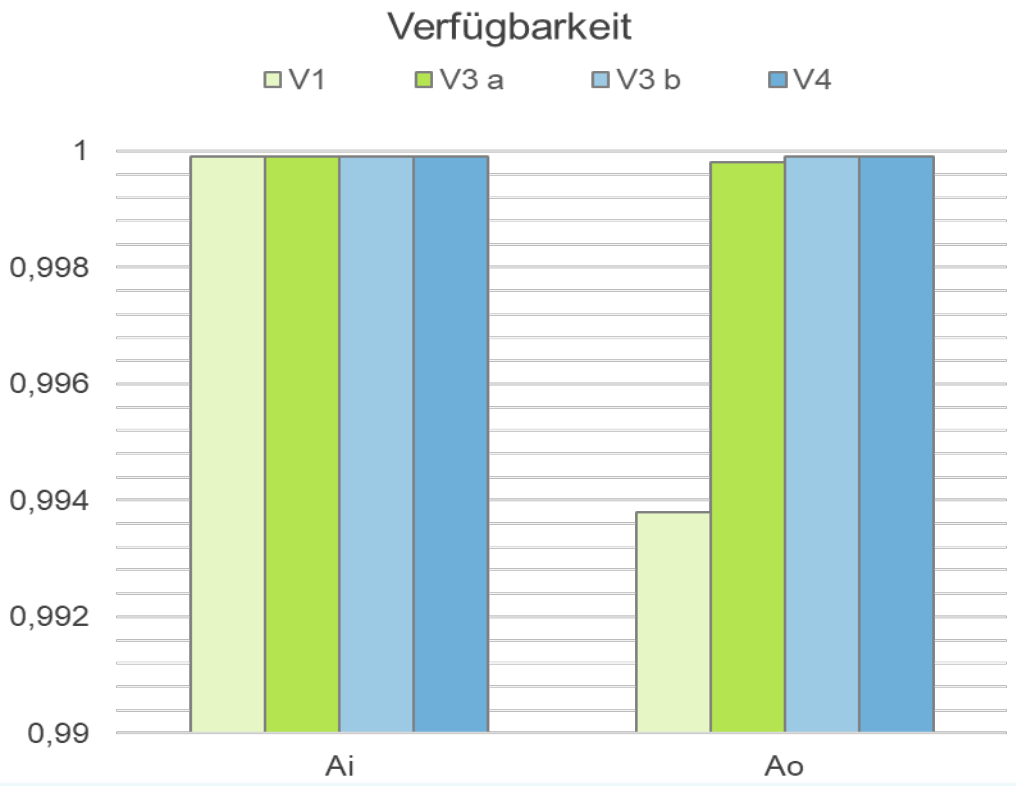
Analyse der **Ausfallsicherheit** (resiliency) von **Designvarianten**

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
$R(t=1\ a)$	0,83043	**0,80064**	**0,87492**	**0,86605**
A_i	**0,99998**	**0,99999**	**0,99999**	**0,99999**
A_o	**0,99384**	**0,99982**	**0,99987**	**0,99986**
SPoF	**3**	**0**	**0**	**0**
DPoF	**165**	139	**119**	**82**

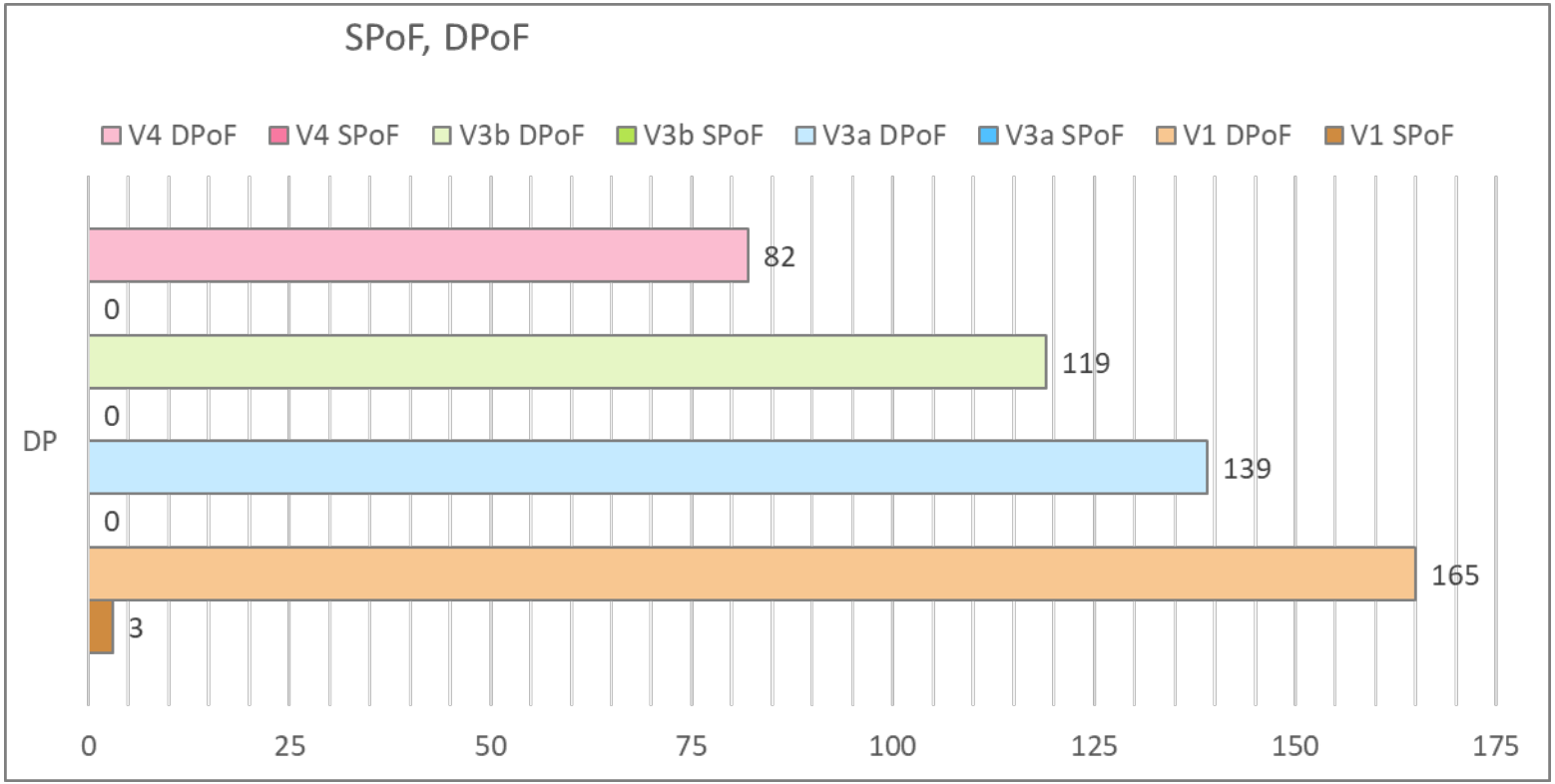
Systeme und Komponenten aller Varianten konsistent, sofern nicht anders bezeichnet.

Optimierung Zuverlässigkeit und Verfügbarkeit





Optimierung der Fehlertoleranz

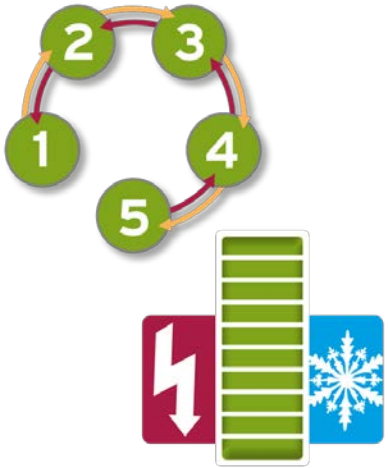


Präventives Risikomanagement für ausfallsichere Data Center

Ich freue mich auf Ihre Fragen.

InfraOpt® GmbH

Dipl.-Ing. Uwe Müller
Geschäftsführender Gesellschafter
Puschkinstr. 23 · D-14943 Luckenwalde
HRB 30023 P · St-Nr. 050/111/03563
www.infraopt.eu · uwe.mueller@infraopt.eu
fon +49 3371 6433-55 · mo +49 172 836 8939



Akronyme

- A_i Inherent availability
- A_o Operational availability
- DCI Data center infrastructure
- $DPoF$ Double point of failure
- EN European standard
- IEEE Institute of Electrical and Electronics Engineers
- 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