Fachtagung Risikoanalyse Informationssicherheit

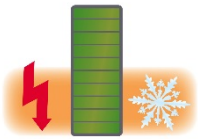
13.-14.07.2015 BERLIN

Dipl.-Ing. Uwe Müller
ibmu.de GmbH

Risikoanalyse von Rechenzentren I

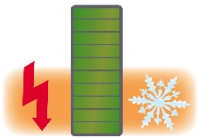
Normen, Kennwerte, Verlässlichkeitsanalyse

Risikoanalyse von Rechenzentren I
Normen, Kennwerte, Verlässlichkeitsanalyse



1. **Einführung**
   - Begriffe und Hintergründe
   - Notwendigkeit der Risikoanalyse
2. **Bestandteile und Dienste**
   - Standort und Gebäude
   - Versorgungs-Infrastruktur
   - Sicherheit, Überwachung, Betrieb
3. **Versorgung-Infrastruktur**
   - Richtlinien und Normen
   - Zertifizierungen
4. **Kennwerte und Metriken**
   - Verfügbarkeit, Zuverlässigkeit, Fehlertoleranz
   - Methodik der Verlässlichkeitsanalyse

1.1 Risikoanalyse von Rechenzentren I
Was ist ein Rechenzentrum?

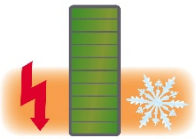


Bundesamt für Sicherheit in der Informationstechnik (**BSI**):

Als **Rechenzentrum** werden bezeichnet …

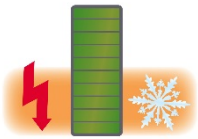
- … die für den Betrieb von komplexen **IT-Infrastrukturen**
  - Server- und Speichersysteme, Systeme zur Datensicherung, aktive Netzkomponenten, TK-Systeme, zentrale Drucksysteme usw.
- … **erforderlichen Einrichtungen**
  - **Elektroenergieversorgung** und **Klimatechnik**
  - überwachende und alarmierende Technik
- … und **Räumlichkeiten:**
  - Rechnersaal, Räume für die aktiven Netzkomponenten,
  - Technikräume, Archiv, Lager, Aufenthaltsraum usw.
- Abgrenzung zum **Serverraum** besteht in der
  - räumlichen Trennung zwischen IT-Systemen und Versorgungs-Infrastruktur

1.2 Risikoanalyse von Rechenzentren I
Das RZ als notwendige Grundlage der IT



- **Informationstechnologie** (IT) des Unternehmens
  - Geschäftszweck und Prozesse
  - Anwendungen, Rollen bzw. Funktionen
- **IT Infrastructure Library** (**ITIL**) ISO/IEC 20000
  - Internationaler De-facto-Standard für IT-Geschäftsprozesse
  - Servicestrategie, Serviceentwicklung, Serviceinbetriebnahme, Servicebetrieb, Serviceverbesserung
  - Aktuell Zertifizierungsmodell ITIL v3
- **Informationssicherheits-Managementsystem** (ISMS) gemäß DIN ISO/IEC 27001
- **Bundesamt für Sicherheit in der in der Informationstechnik**
  - Zuordnungstabelle zur ISO 27001 sowie ISO 27002

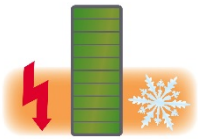
1.3 Risikoanalyse von Rechenzentren I
Bedeutung der Verfügbarkeit des RZ



- **Geschäftsausfall**
  - Nichtverfügbarkeit von Leistung
  - Imageverlust
  - Penalties ggf.
- **Betriebsausfall** für Mitarbeiter
  - Zwangspausen
  - Terminprobleme
  - Stress und Frustration
- Gefahr des **Datenverlust**
  - Abgebrochene Transaktionen
  - Verlorene Daten
  - Folgekosten zur Widerherstellung

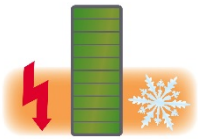
Was geschieht bei einem (großflächigen) **Blackout** ?

1.4 Risikoanalyse von Rechenzentren I
Richtlinien und Normen für Errichtung und Betrieb



- **BSI** Hochverfügbarkeitskompendium
  - Band G: Einführung und methodische Grundlagen
  - Band B: Bausteine
  - Band M: Maßnahmen
  - Band AH: Anleitungen und Hilfsmittel
- **BITKOM** „Leitfäden“
  - Leitfaden Betriebssicheres Rechenzentrum
  - Leitfaden Energieeffizienz im Rechenzentrum
- **DIN EN 50600 ff.** Einrichtungen und Infrastrukturen von Rechenzentren
  - **DIN EN 50600-2-1** Gebäude
  - **DIN EN 50600-2-2** Stromversorgung
  - **DIN EN 50600-2-3** Überwachung der Umgebung
  - **DIN EN 50600-2-4** Infrastruktur der Telekommunikationsverkabelung
  - **DIN EN 50600-2-5** Sicherungssysteme
  - **DIN EN 50600-2-6** Informationen für das Management und den Betrieb

1.5 Risikoanalyse von Rechenzentren I
Verfügbarkeit des Rechenzentrums

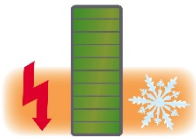


- Welche **Verfügbarkeit** muss das RZ erreichen?
  - Auswirkung auf das **Rechenzentrums-Design**
  - Auswirkung auf die **Lebenszykluskosten** (LCC)

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 %)**

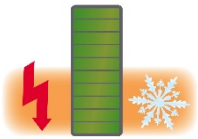
- Je **höher** die **Verfügbarkeit** desto **höher** die **Lebenszykluskosten**
  - **Investitionskosten** (Baukosten, Planungskosten, Nebenkosten)
  - Energieverbrauchskosten
  - Kosten für **Wartung** und **Service**
  - Kosten für **Reinvestitionsmaßnahmen**

2.1 Risikoanalyse von Rechenzentren I
Notwendige Bestandteile und Dienste, Übersicht



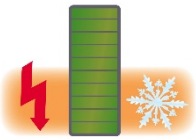
- **Standort**
- **Gebäude**
- **Raumanforderungen**
- **Elektroenergieversorgung**
- **Klimatisierung** (Steuerung der Umgebungsbedingungen)
- **Kommunikationsanbindung**
- **Sicherheitskonzeption**
- **Brandschutz**
- **Wartung und Pflege**
- **Betriebsoptimierung**
- **Anpassungen, Umbauten, Erweiterungen**

2.2 Risikoanalyse von Rechenzentren I
Bewertung der Standortsituation (BSI)



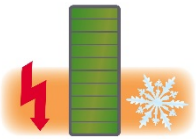
- **Standortprüfung**
  - Umsetzbarkeit von **Sicherheitsanforderungen**
  - Eine vs. mehrere **Mietparteien**
  - **Umfeld** und **Zugänglichkeit**
  - Vermeidung von Lagehinweisen
- **Versorgungtechnische Anforderungen**
  - **Elektroenergie:** verfügbare Mittelspannung bzw. Hochspannungssetze
  - **Carrier:** Redundanz, Kapazität
- **Gefährdung** durch höhere Gewalt, Elementarereignisse, Unfälle
  - Hochwasser, Erdbeben, Feuer, Blitzschutz, ...
  - Flughäfen, Bahnlinien, Autobahnen, Kraftwerke, Industrie ...
- **Verbrauchskosten**
  - Elektroenergie, Wasser, Kraftstoff
  - Wartung und Service

2.3 Risikoanalyse von Rechenzentren I
Gebäude- und Raumanforderungen



- **Gelände**
  - Zufahrtmöglichkeit mit LKW
  - Bei Dachaufbringung: Kran (Netzersatzanlagen, Kälteerzeugung)
- **Datacenter-Bereich** (Serverraum)
  - Ggf. mehrere Serverräume mit verschiedenen Anforderungen
  - Zentrale Druckerräume, Datensicherung
- **Aktive und passive Vernetzung**
  - Meetme-Room
  - Übergaberaum für Carrier
- **Operating**
  - Leitwarte
  - Vorbereitungsräume
  - Nebenräume (Lager, Toilette)
  - Ggf. Lastenaufzüge

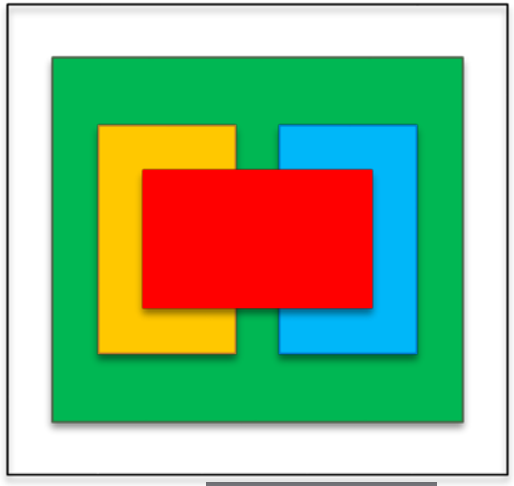
2.4 Risikoanalyse von Rechenzentren I
Gebäudekonstruktion



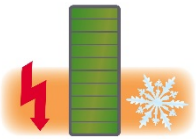
- **Gründung und Tragwerk**
  - Traglasten im Gebäude, ggf. auf dem Dach
  - Schutz vor Wasser
  - Schutz vor Elementarereignissen und Havarien
- **Decken, Fenster, Türen, Gänge, Doppelböden, Aufzüge**
  - Traglasten, Flächenbedarf, Raumhöhen
  - Einbringgrößen, Durchbruchsgrößen
  - Bauliche Sicherheit (Widerstandklassen)
  - Baulicher Brandschutz
- **Qualitativ**
  - Dampfdichte, Rauchschutz, Oberflächenqualität
  - EMV-Schutz, Äußerer und innerer Blitzschutz
  - Überspannungsschutz
  - Erweiterungsmöglichkeit, Modularität, Ökologie

2.5 Risikoanalyse von Rechenzentren I
Sicherheit

- **Sicherheitskonzeption**
  - Festlegung von Schutzbedarf und Schutzzielen
  - Bauliche Maßnahmen (Türen und Fenster)
  - Einbruchmeldeanlage nach VdS Klassifizierung
  - Schließsystem, Zutrittskontrolle, Vereinzelung
  - Videoüberwachung
  - Einbruchschutz
  - Gefahrenmeldeanlagen (Brand-, Feuchte-, Gasdetektion)
- Bildung von **Sicherheitszonen**
  - Grundstück
  - Halböffentlicher Bereich, angrenzende Flächen
  - Operating, Nebenräume der IT
  - Technische Anlagen zum Betrieb
  - IT- und Kommunikations-Infrastrukturbereich



2.6 Risikoanalyse von Rechenzentren I
Anbindung und Betrieb



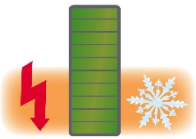
Weitere **notwendigen Dienste:**

- **Kommunikationsanbindung** (teilw. DIN EN 50600-2-4)
  - Inneres aktives und passives Netzwerk
  - Connects zum Internet
  - Interconnects zu redundanten bzw. abhängigen RZ‘s
- **Wartung, Pflege und Erweiterung** (teilw. DIN EN 50600-2-6)
  - Zyklische Instandhaltungen und Wartung
  - Zyklische **Funktionstests**
  - Modularität, **Erweiterungsmöglichkeit**
  - Optimierung der **Effizienz**

Planung und Betrieb des Rechenzentrums als **Optimierungsaufgabe:**

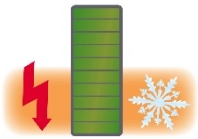
Maximum(Verlässlichkeit) bei **Minimum**(Lebenszykluskosten)

2.7 Risikoanalyse von Rechenzentren I
Brandschutz



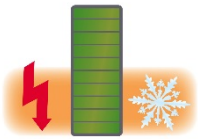
- **Baulicher Brandschutz**
  - Brandschutzkonzept, Brandmeldekonzept
  - Ausbildung von Brandabschnitte
  - Ausbildung von Decken, Wänden, Türen, Rettungswegen, Trassen
- **Anlagentechnischer Brandschutz** (Branderkennung)
  - Automatische Rauchmelder, Handmelder
  - Rauch-Ansaugsysteme mit Vorwarnmöglichkeit
  - Brandmeldeanlage mit Aufschaltung zur ständig besetzten Stelle
  - Alarmierung (akustisch, optisch)
- **Löschvorrichtungen** (humanverträglich)
  - Handfeuerlöscher
  - Gaslöschanlagen (Sauerstoffverdrängung)
  - Permanente Inertisierung (Sauerstoffreduktion)

2.8 Risikoanalyse von Rechenzentren I
Infrastruktur und Ausstattung



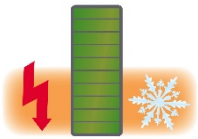
- **Notwendige** Anlagen und Systeme
  - Elektroenergieversorgung
  - Kälteversorgung, Regelung der Luftfeuchte
  - Humanlüftung
  - Aktive und passive Datenversetzung, Telekommunikation
  - Brandmeldeanlage, Brandfrüherkennung
  - Einbruchmeldeanlage, Zutrittskontrollanlage
  - Energiemessung, Fehlerstromüberwachung, Monitoring
  - Fluchtweganzeige
- **Optionale** Anlagen und Systeme
  - Redundanzen (Elektroenergie- und Kälteversorgung)
  - Gaslöschanlage
  - Videoüberwachungsanlage
  - Feuchteerkennung
  - Personen-Vereinzelung

2.9 Risikoanalyse von Rechenzentren I
Sicherung des fortlaufenden Betriebs



- **Servicedienstleister**
  - Reaktionszeiten und Service Level Agreements (SLA)
  - Reaktionszeit vs. Wiederherstellungszeit
- **Monitoring**
  - Störmeldungen, Zutrittsüberwachung
  - Energiemessung, Fehlerstromüberwachung
- **Betriebsoptimierung**
  - Energieeffizienz, Prozessoptimierung
- **Notfälle**, **Havarien**, Funktionsproben
  - Notfallübungen , Notfallmanagement
  - Zyklische Test der Teilsysteme, Mitarbeiterschulung
- Gewährleistung der **Zuverlässigkeit** des Gesamtsystems
  - Wartung, Reinigung, Ersatz, Vorhaltung
  - Austausch, Kraftstoffalterung

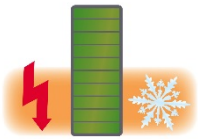
3.1 Risikoanalyse von Rechenzentren I
Eingehende analytische Fragestellungen



- 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 bergründen?
- Welche **Effizienzziele** sind zu erreicht?
- Ist die Infrastruktur während der **Umbaumaßnahme** verlässlich?
- Sind **vorgefertigte Lösung** 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**!

3.2 Risikoanalyse von Rechenzentren I
Versorgungs-Infrastruktur



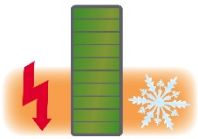
Die Rechenzentrums-Infrastruktur umfasst alle zur Aufrechterhaltung des Rechenzentrumsbetriebes **notwendigen Hilfsdienste:**

- **Elektroenergieversorgung** (DIN EN 50600-2-2)
  - Erzeugung, Übertragung, Verteilung, Überbrückung
  - Verbrauchsmessung, Schutzmaßnahen, Monitoring
  - Je **Teilsystem** ein **separater Brandabschnitt**
- **Steuerung der Umgebungsbedingungen** (DIN EN 50600-2-3)
  - **Kälteversorgung**, Luftfeuchteregelung
  - Erzeugung, Übertragung und Verteilung

Die ununterbrochene **Elektroenergieversorgung** und kontinuierliche **Kälteversorgung** des Rechenzentrums sind unabdingbar.

Die Kälteversorgung benötigt **ebenfalls** Elektroenergie zum Betrieb.

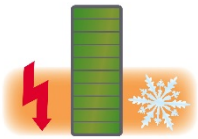
3.3 Risikoanalyse von Rechenzentren I
Uptime Institute - Tier Klassifikation



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

3.4 Risikoanalyse von Rechenzentren I
BSI Verfügbarkeitsklassen und BITKOM Kategorien

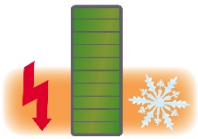


BSI	VK 0	VK 1	VK 2	VK 3	VK 4	VK 5
Ausfallzeit /Jahr	ca. 2-3 Wo.	< 90 Std.	< 9 Std.	< 1 Std.	ca. 5 min.	-
Anforderung an Verfügbarkeit	Keine	normal	hoch	sehr hoch	höchste	Desaster -tolerant
Verfügbarkeit	**ca. 95 %**	**> 98,97 %**	**> 99,90 %**	**> 99,99 %**	**> 99,999 %**	**(100 %)**

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

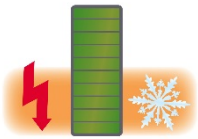
3.5 Risikoanalyse von Rechenzentren I
DIN EN 50600 ff. Einrichtungen und Infrastrukturen von RZ



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 (Transferschalter)	
Versorgungs-pfade	Einer **N**	Einer **N+1**	Mehrere **2N**	Mehrere **2N**	
Notstrom (NEA)	k. A.	k. A.	k. A.	k. A.	
DIN EN 50600-2-3 Überwachung der Umgebung	-	keine Aus-fallsicherheit	Komponenten Redundanz	Instandsetzung im laufenden Betrieb	
Versorgungs-pfade	-	Einer **N**	Einer **N+1**	Einer **N+1**	Mehrere **2N**

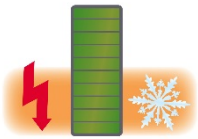
Quelle (Auszug): DIN EN 50600-1 2013, DIN EN 50600-2-2 2014, DIN EN 50600-2-3 2015

3.6 Risikoanalyse von Rechenzentren I
Zertifizierungen und numerische Analysen



- **Zertifizierungsinstanzen**
  - Uptime Unstitute, Tier I bis IV
  - TÜV IT (TÜV NORD), Zertifizierung von Rechenzentren, Ablauf
  - eco Verband e.V., Datacenter Star Audit
  - BSI Bundesamt für Sicherheit in der IT – Auditierung
  - TÜV Süd, TÜV Saarland, TÜV Rheinland
  - BITKOM, Leitfaden zur Zertifizierung (ISMS)
  - Einrichtungen und Infrastrukturen von Rechenzentren DIN EN 50600 ff.
- Vorgefertigte Lösungen
  - Standardisierung im RZ
- **Verlässlichkeitsanalyse** basierend auf **Metriken**
  - Qualitative Bewertung vs. Numerische Bewertungsverfahren
  - **Verfügbarkeit, Zuverlässigkeit, Fehlertoleranz**
  - Verlässlichkeitsanalyse mittels InfraOpt®

4.1 Risikoanalyse von Rechenzentren I
Metriken der Verlässlichkeitsanalyse



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

  ➥ **Wann** und in **welche Teilsysteme** ist zu **investieren** (Alterung)

- **Inhärente Verfügbarkeit:** **$A_i = MTBF / (MTBF + MTTR)$**
  - MTBF: Mittlere Zeit zwischen zwei Fehlern
  - MTTR: Mittlere Zeit zur Reparatur

  ➥ **Welche Servicelevel sind notwendig, was ist zu bevorraten**

- **Operationale Verfügbarkeit:** **$A_o = MTBM / (MTBM + MDT)$**
  - MTBM: Mittlere Zeit zwischen zwei Instandsetzungen
  - MDT: Mittlere Zeit der Nichtverfügbarkeit

  ➥ **Funktionieren** die **Managementsysteme** (Qualifikation, Sicherheit)

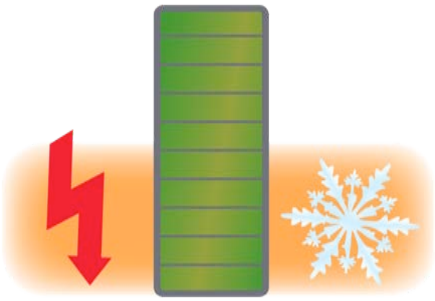
- Simulation **1-** und **2-Fehlerkombinationen** aller Teilsysteme, identifizieren der **S**ingle **P**oints **o**f **F**ailure (SPoF) und **D**ouble **P**oints **o**f **F**ailure (DPoF)

  ➥ **Vorhersage** der **Reaktion** auf **geplante** bzw. **nicht geplante Ereignissen**

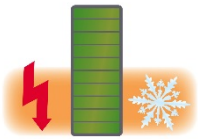
4.2 Infrastrukturdesign und Betrieb
InfraOpt® - Methodik zur Optimierung von Rechenzentren

Vorhersage der Reaktion der Rechenzentrums-Infrastruktur auf **geplante** bzw. **nicht geplante Ereignissen -** auf der Grundlage numerischer **Metriken**.

- Vergleich verschiedener **Tier-Designs** / **Kategorien** / **Verfügbarkeitsklassen**
- Vergleich **beliebiger Redundanzanordnungen** (2N, N+1, xN+yM)
- Vergleich von Komponenten mit **unterschiedlichen MTBF** bzw. **MTTR**
- Unterstützung beim Design / Redesign:
  - **Identifizieren** von **Schwachstellen** (strukturell, Komponenten)
  - **Investitionsbegründung** gegenüber dem Management auf der Grundlage von Metriken
  - Bestimmung des „herabgesetzten **Ausfallsicherungsgrades“** nach DIN EN 50600-2-2 in **Schalt-** bzw. **Wartungssituationen**
  - Validierung von **Service-Level-Agreements**
  - Optimieren von **Wartungs-** und **Serviceplänen**
- Fortlaufende **Zuverlässigkeitsbewertung** im Rahmen eines ISMS nach DIN ISO 27001 ff.



4.3 Risikoanalyse von Rechenzentren I
Fazit zur Verlässlichkeitsanalyse



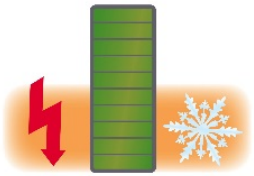
Zwei Fragen:

Wie reagiert das Rechenzentrum auf
geplante bzw. **nicht geplante Ereignissen**?

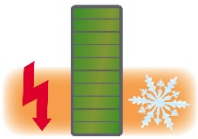
Welcher **Aufwand** ist dazu insgesamt notwendig?

Eine Antwort:

Die **Planung** und der **Betrieb** des Rechenzentrums
ist eine fortlaufende **Optimierungsaufgabe,**
es gilt das **Maximum** der **Verlässlichkeit**
bei einem **Minimum** der **Lebenszykluskosten**
zu erreichen.

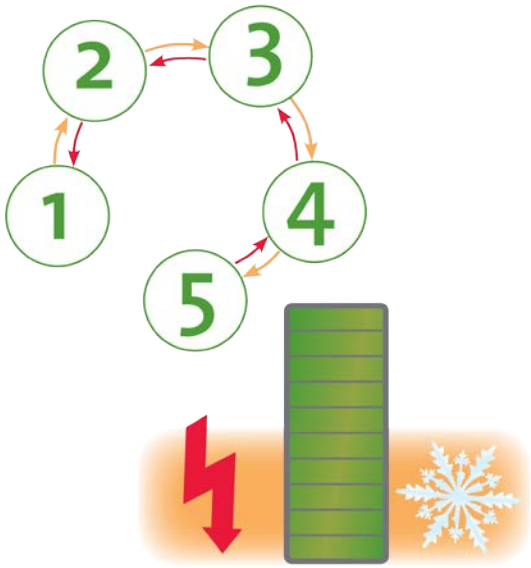


4.4 Risikoanalyse von Rechenzentren I
Methodik der Verlässlichkeitsanalyse mittels InfraOpt®



Fünf Schritte zur Optimierungsvariante:

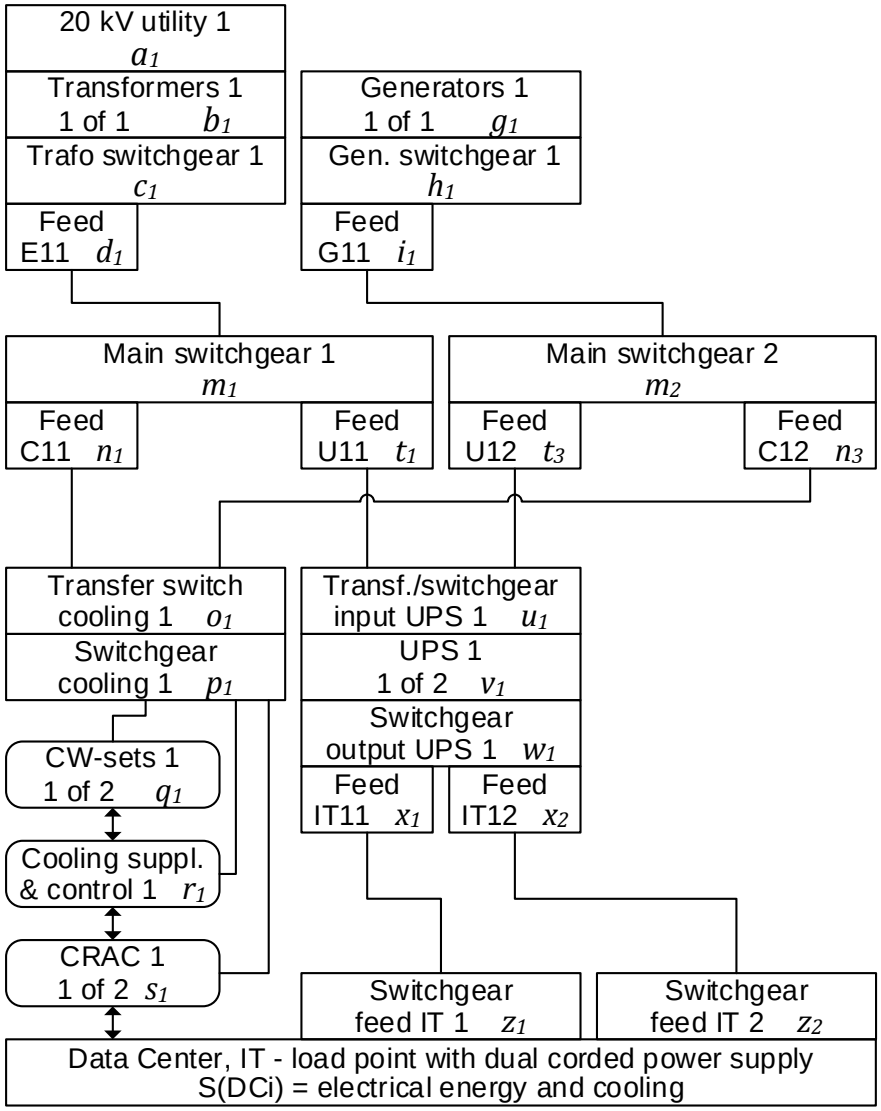
1. **Überführung** der Infrastruktur in ein integrales Zuverlässigkeitsschema
2. **Modellierung** der RZ-Infrastruktur in InfraOpt®
3. **Aufbereitung** der Zuverlässigkeitsdaten
4. **Berechnung** Zuverlässigkeit und Verfügbarkeiten
5. **1- und 2-Fehlersimulation** über alle Teilsysteme



Ziel des Optimierungsprozesses:

Maximierung Verlässlichkeit ⟺ Minimierung Lebenszykluskosten

4.5 Risikoanalyse von Rechenzentren I
Berechnungsbeispiel - Aufgabenstellung



Vergleiche Varianten **N+1 / 2N**:

1) N_E+1 Elektroenergieversorgung
   N_C+1 Kälteversorgung
2) $2N_E$ Elektroenergieversorgung
   N_C+1 Kälteversorgung
3) N_E+1 Elektroenergieversorgung
   $2N_C$ Kälteversorgung

Verlässlichkeitsanalyse:

- Zuverlässigkeit **R(t)**
- Inhärente Verfügbarkeit $\mathbf{A_i}$
- Operationale Verfügbarkeit $\mathbf{A_o}$
- **1-** und **2-Fehlertoleranz**

ibmu.de®

Vielen Dank für Ihre Aufmerksamkeit!

Dipl.-Ing. Uwe Müller

Geschäftsführender Gesellschafter

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