

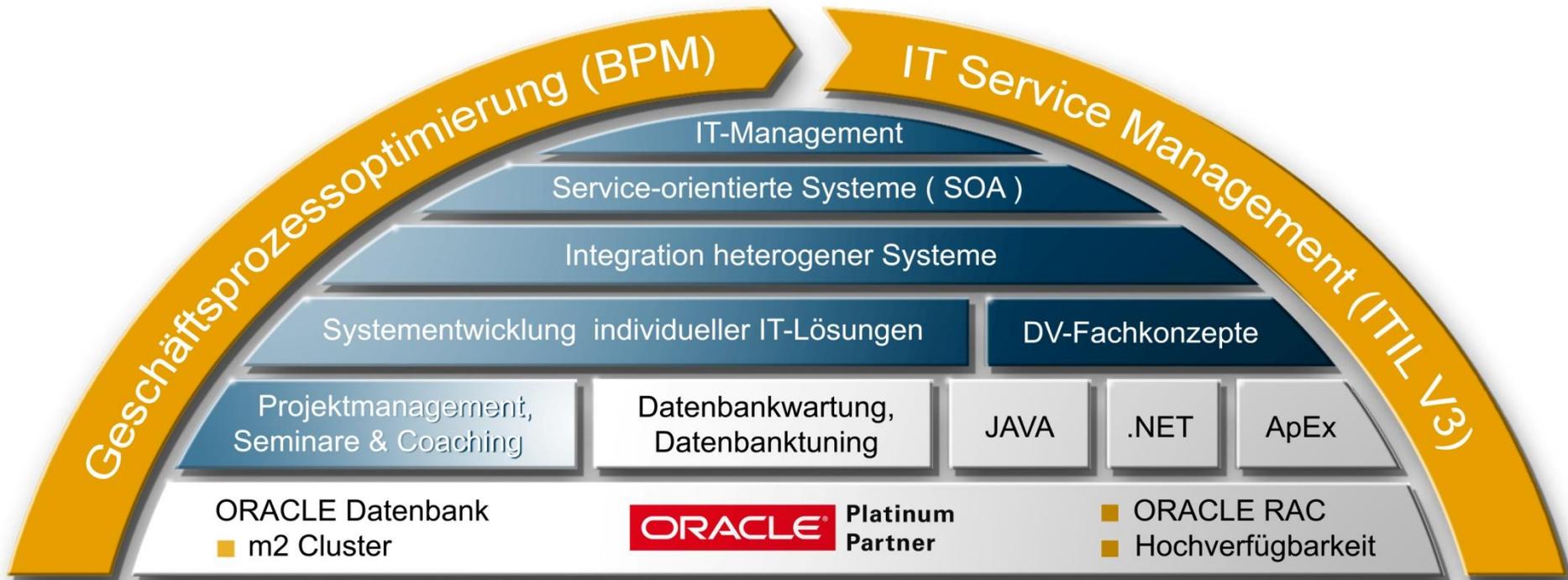
# Hochverfügbarkeit für die Datenbank

Was ist zu beachten?

Jochen Kutscheruk

merlin.zwo InfoDesign GmbH & Co. KG

# Die merlin.zwo-Gruppe

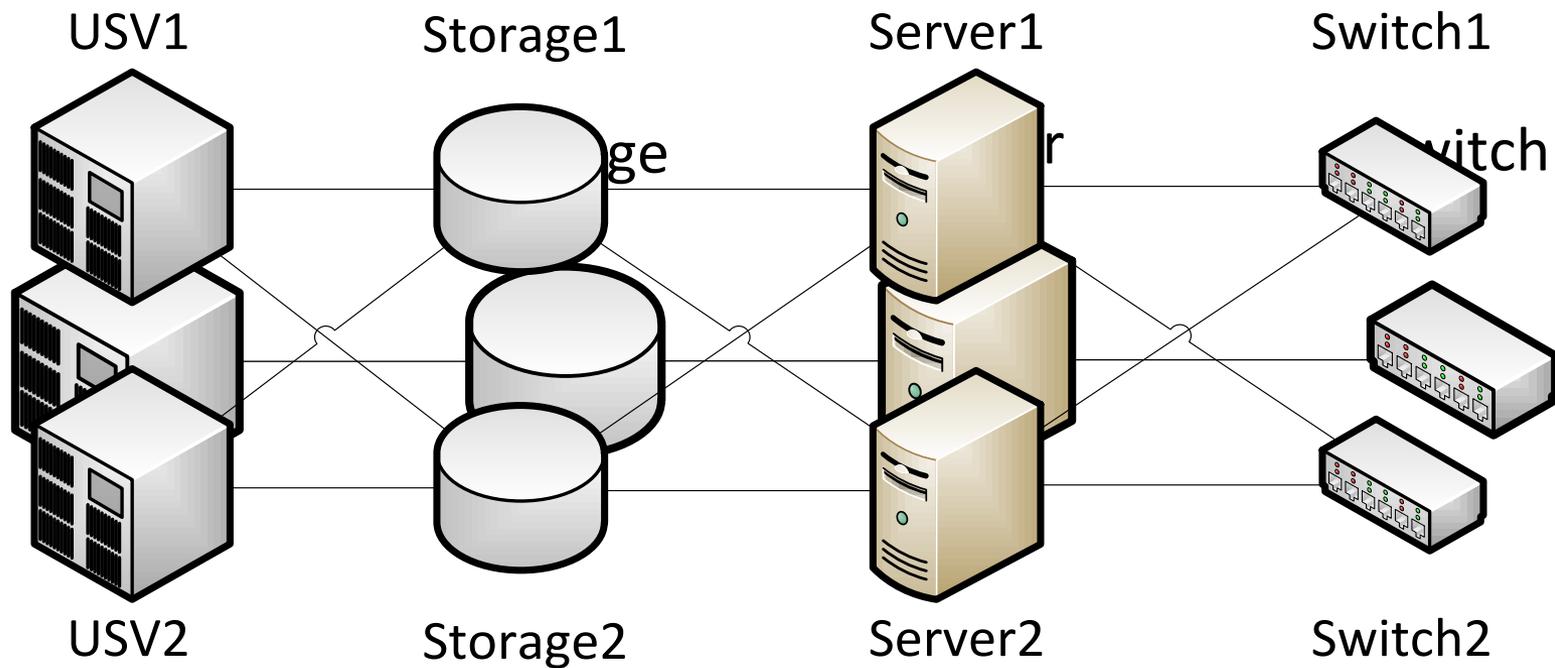


Bad Liebenzell • Karlsruhe • Neustadt / W. • Eningen

# Warum Hochverfügbarkeit für die Datenbank?

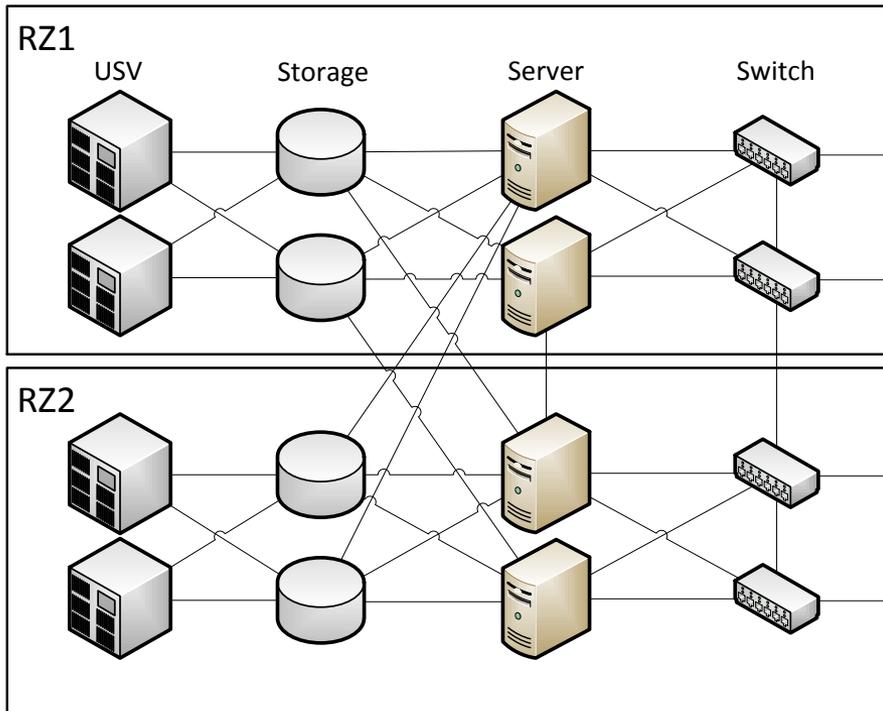
# Überlegungen zur Wahrscheinlichkeit

# Ein kleines Beispiel

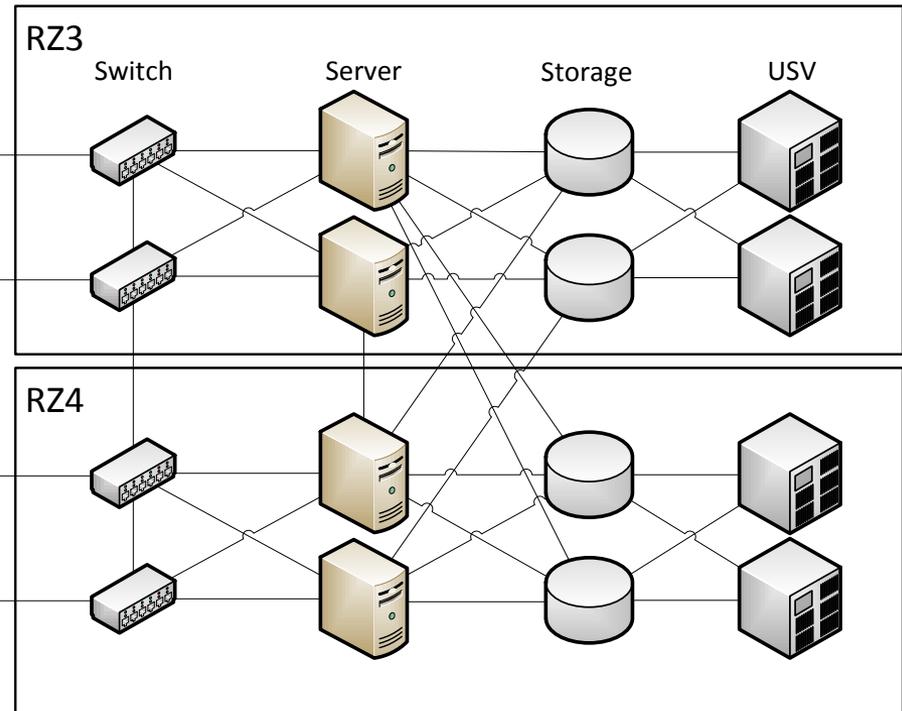


# Ein kleines Beispiel

## RAC



## Dataguard RAC



Wahrscheinlichkeit eines Totalausfalls: **100% !!**

Wie wahrscheinlich ist denn eigentlich

ein Erdbeben der Stärke 9

!!! 100% !!!  
!!! in Nürnberg ?

## Nur wann?



**(Deshalb kamen uns die 30.000 Jahre zwischen  
Tschernobyl und Fukushima so kurz vor)**

# Definition der Verfügbarkeit

„Ein System wird als verfügbar bezeichnet, wenn es in der Lage ist, die Aufgaben zu erfüllen, für die es vorgesehen ist.

Als Verfügbarkeit wird die Wahrscheinlichkeit bezeichnet, dass ein System innerhalb eines spezifizierten Zeitraums funktionstüchtig (verfügbar) ist.

Die Verfügbarkeit wird als Verhältnis aus fehlerbedingter Stillstandszeit (= Ausfallzeit) und Gesamtzeit eines Systems bemessen.“

Quelle: Wikipedia

# Verfügbarkeitsklassen

Klasse	Verfügbarkeit	Ausfall pro Jahr
2	99%	3T 15:39:36 h
3	99,9%	0T 08:45:58 h
4	99,99%	0T 00:52:36 h
5	99,999%	0T 00:05:16 h
6	99,9999%	0T 00:00:32 h

## Dabei unbedingt zusätzlich zu beachten:

MTBF: Mean Time Between Failure

MTTR: Mean Time To Recover

## Availability Environment Classification (AEC)

(Harvard Research Group)

Klasse	Typ	Beschreibung
<b>AEC-0</b>	Conventional	Funktion kann unterbrochen werden, Datenintegrität ist nicht essentiell
<b>AEC-1</b>	Highly Reliable	Funktion kann unterbrochen werden, Datenintegrität gewährleistet
<b>AEC-2</b>	High Availability	Funktion darf nur innerhalb festgelegter Zeiten oder zur Hauptbetriebszeit minimal unterbrochen werden
<b>AEC-3</b>	Fault Resilient	Funktion muss innerhalb festgelegter Zeiten oder während der Hauptbetriebszeit ununterbrochen aufrecht erhalten werden
<b>AEC-4</b>	Fault Tolerant	Funktion muss ununterbrochen aufrechterhalten werden, 24/7 Betrieb muss gewährleistet sein
<b>AEC-5</b>	Disaster Tolerant	Funktion muss unter allen Umständen verfügbar sein

## Die Definition „Hochverfügbarkeit“ ist abhängig von den Anforderungen!

### ■ Verfügbarkeit der Daten

- Ein Datenverlust ist nicht akzeptabel
- Ein kurzzeitiger Ausfall der Anwendung ist akzeptabel
- Beispiel: Hochregallager

### ■ Verfügbarkeit der Anwendung

- 24 x 7 x 365 notwendig
- Ein (kleiner) Datenverlust ist akzeptabel
- Beispiel: Tourismus-Webseite

## ■ Der Wunsch (des Managements?):

- Verfügbarkeitsklasse 6 bzw. AEC-5
- Minimale Anschaffungskosten
- Minimale laufende Kosten

## ■ Die Wirklichkeit:

- Entweder
  - Verfügbarkeitsklasse 6
  - Aber: Maximale Anschaffungs- und laufende Kosten
- Oder
  - Minimale Anschaffungs- und laufende Kosten
  - Aber: Verfügbarkeitsklasse 2

- **Begrenzttes Budget**
- **Begrenzte Zeit**

Daher muss gegenüber dem Management klar kommuniziert werden, was mit dem gegebenen Budget in der gegebenen Zeit erreicht werden KANN!

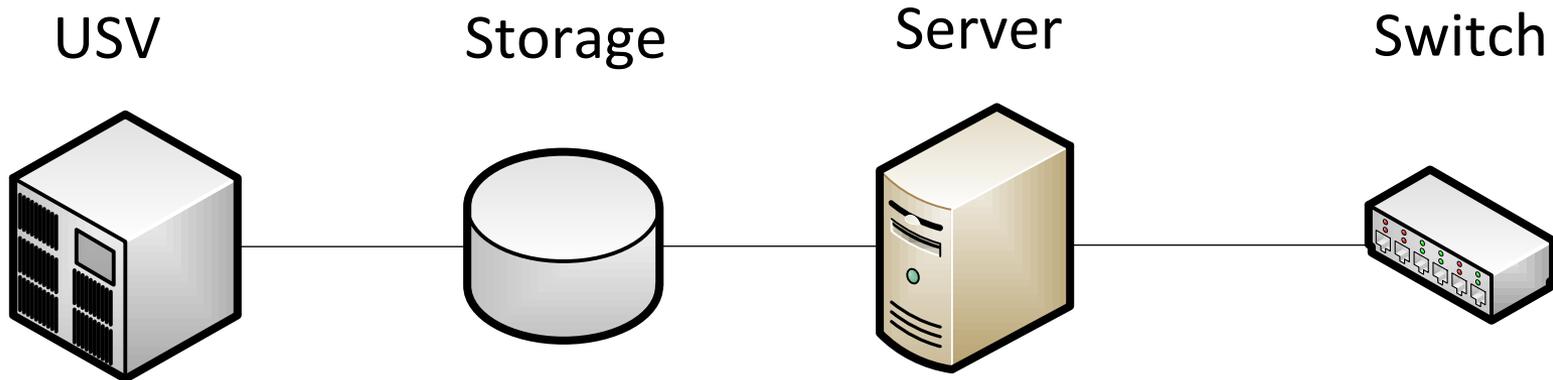
Aber: was kann denn erreicht werden?

# Berechnung der Verfügbarkeit

## Serienschaltung abhängiger Komponenten

Der Einfachheit halber:

Verfügbarkeitsklasse 3 (99,9%) für jede Komponente

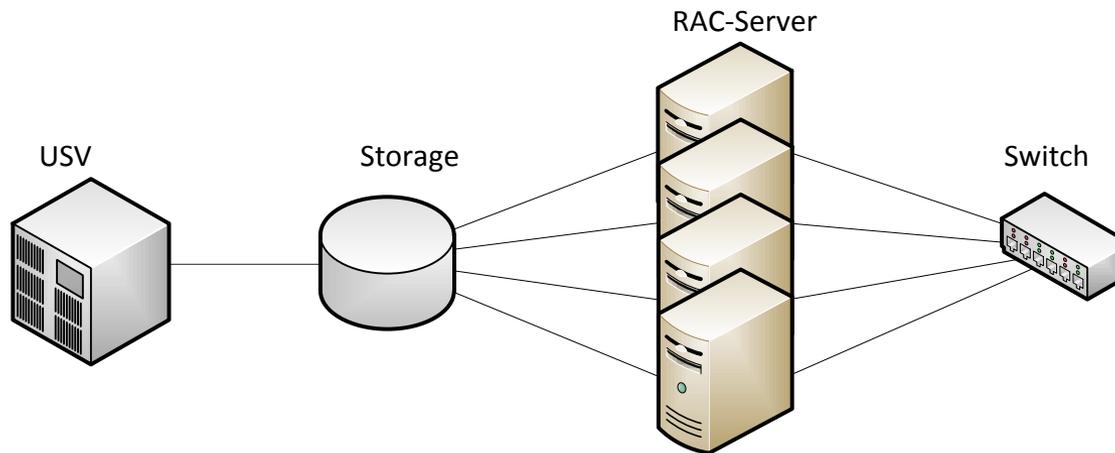


$$0,999 \times 0,999 \times 0,999 \times 0,999 = 0,996 \text{ Gesamt!}$$

Jährliche Ausfallzeit: **34,99 Stunden** statt 8,76 Stunden!



## Parallelschaltung von Komponentengruppen

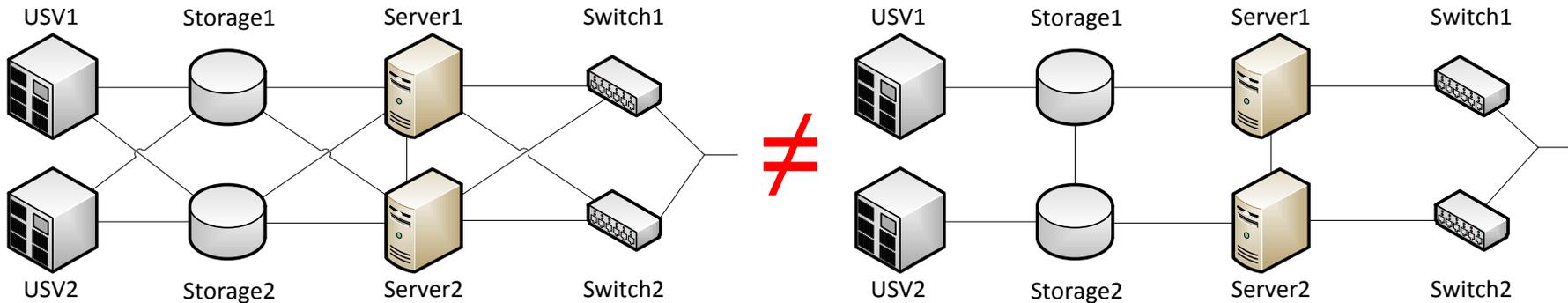


Berechnet als Produkt der Verfügbarkeiten:

$$0,999 \times 0,999 \times 0,999999999999999 \times 0,999 = 0,997$$

Jährliche Ausfallzeit: **26,3 Stunden** statt 30  $\mu$ s!

## Serienschaltung abhängiger redundanter Komponenten



$$(1 - (1 - 0,999)^2)^4$$
$$= 0,9999999999984$$
$$= 0,5 \text{ ms / Jahr}$$

≠

$$1 - (1 - 0,999^4) \times (1 - 0,999^4)$$
$$= 0,99998405$$
$$= 8,4 \text{ Minuten / Jahr}$$

- Die Eliminierung des SPOF (Single Point Of Failure) wäre notwendig, um die Verfügbarkeit wirklich steigern zu können.
- Der SPOF lässt sich jedoch nur verschieben, niemals eliminieren!
- Je weiter der SPOF verschoben wird, desto teurer wird das Gesamtsystem – die Kosten steigen dabei nicht linear, sondern exponentiell.

- **Zusätzliche Ausfallzeiten durch die gestiegene Komplexität des Gesamtsystems.**
- Höhere Anforderungen an das Personal
- Höhere laufende Kosten!

## Kleines Beispiel:

- redundante Internetleitung im zweiten Brandabschnitt vorhanden?
- Wie lange wird benötigt, um das alternative Routing Intern/Extern korrekt lauffähig zu haben?

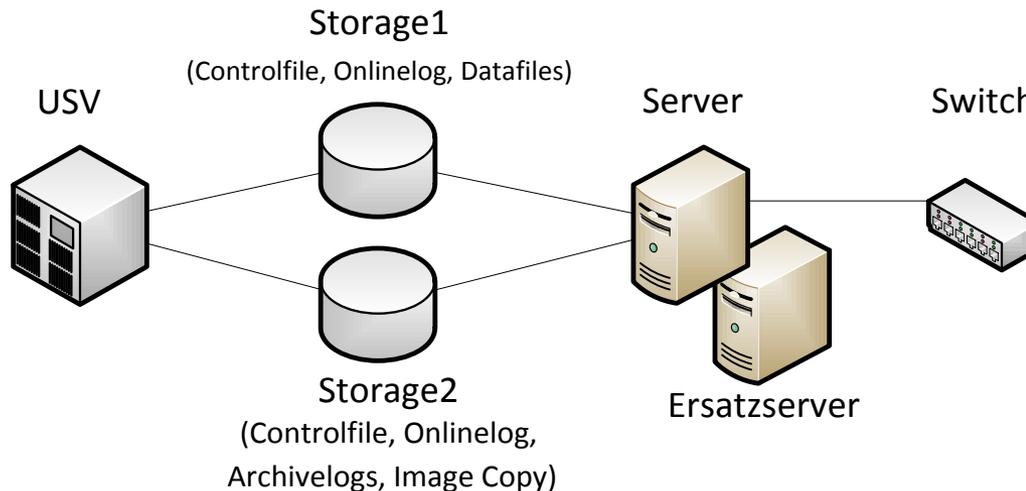
# Alternative / Ergänzende Ansätze

## Können einfache Lösungen auch funktionieren?

- Abhängig von den konkreten Anforderungen
  - Wird „nur“ Verfügbarkeit gefordert?
  - Wird „nur“ Datensicherheit gefordert?
  - Welche Ausfallzeiten werden toleriert?
  
- Die Kombination **Real Application Cluster / DataGuard** auf entsprechender Hardware ist
  - Unschlagbar im Bereich Ausfallsicherheit  
**(Muss jedoch korrekt aufgesetzt worden sein!)**
  - Unschlagbar im Bereich Kosten

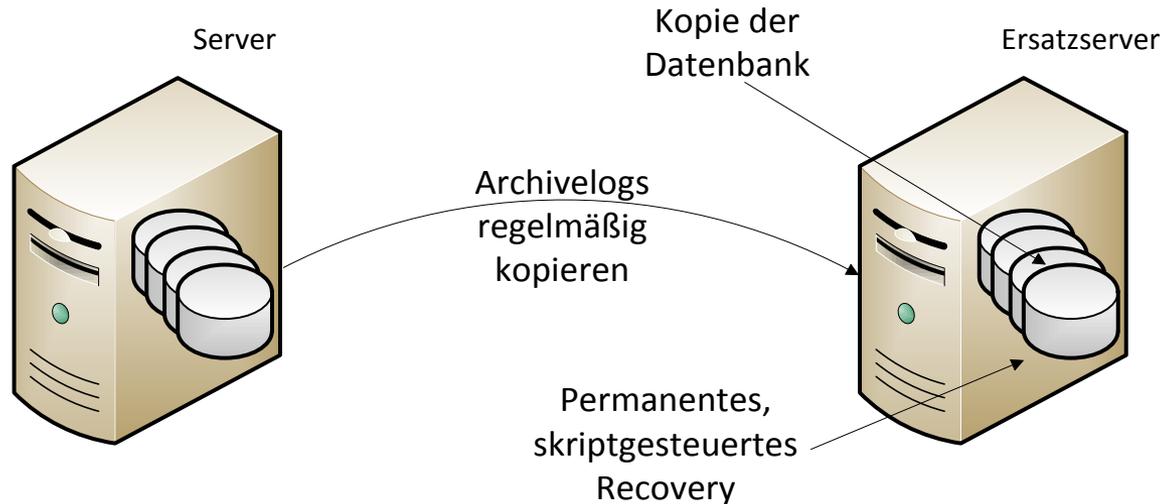
- Ab wann ist ein System denn nicht mehr verfügbar?
  - Hardwareausfall
  - Dienste werden nicht gestartet (nach reboot)
  - Antwortzeit: z.B. 30 Minuten statt 30ms
  - Logisch (inhaltlich) korrupte Daten
  - Physisch korrupte Datenblöcke
  - ...

## RMAN Image Copy auf zweite, unabhängige Storage



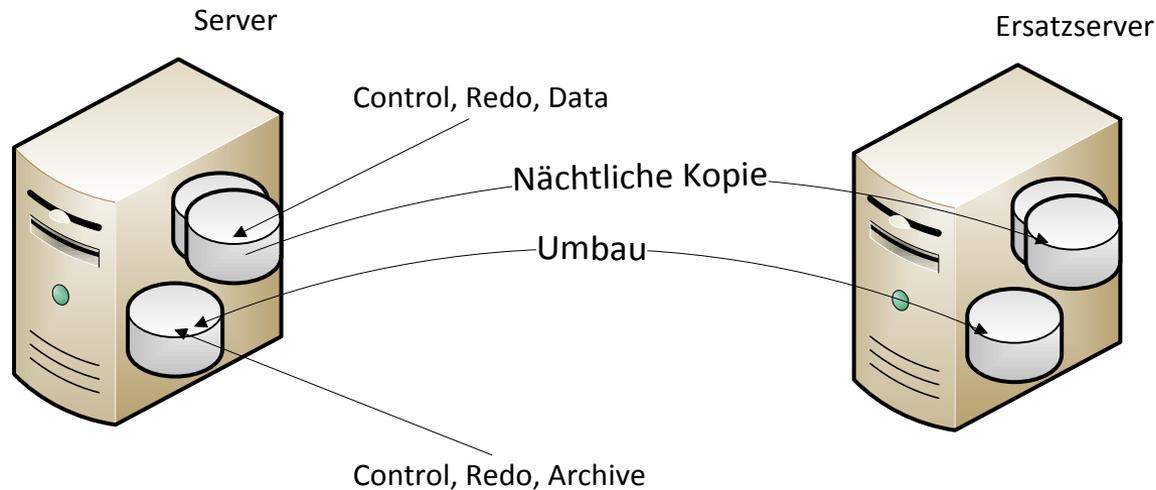
- Vorteil: Keinerlei Datenverlust bei Ausfall einer Storage
- Nachteil:
  - Zusätzliche, nicht unabhängige Storage-Komponente
  - Notwendiges KnowHow im Fehlerfall verfügbar ?
  - Doppelter Festplattenplatz benötigt

## Standby-Datenbank zu Fuß



- Vorteil: Günstig zu implementieren, wenig zusätzliches KnowHow notwendig
- Nachteil: Datenverlust garantiert

## Ungewöhnliche Variante: Transportable Disk



- Vorteil: Keinerlei Datenverlust
- Nachteil: Notwendiges KnowHow im Fehlerfall verfügbar?

- Flashback Database / Table
  - Flashback Query
  - RMAN Image Copy
  - ...
- 
- Allgemein: Strategien zur Vermeidung eines Datenbank Restores
  - Notfallkonzept unabhängig überprüfen lassen!
  - Ganz wichtig: Regelmäßige Notfallübungen!

Die tatsächliche Implementierung ist abhängig von vielerlei Faktoren:

- der geforderten Verfügbarkeit
- der benötigten Verfügbarkeit
- dem verfügbaren Budget
- der verfügbaren Zeit
- dem verfügbaren KnowHow des Fachpersonals

**Das in Abhängigkeit von diesen Faktoren**  
**erreichbare Ziel muss unbedingt**  
**klar kommuniziert werden!**



## Haben Sie noch Fragen?



**merlin.zwo InfoDesign GmbH & Co. KG**  
**Jochen Kutscheruk**

Telefon: 07052 – 50898 40

E-Mail: [jochen.kutscheruk@merlin-zwo.de](mailto:jochen.kutscheruk@merlin-zwo.de)



Web: <http://www.merlin-zwo.de>

## merlin.zwo

## Wir **kümmern** uns!

## Versprochen.

**merlin.zwo InfoDesign GmbH & Co. KG**

**Jochen Kutscheruk**

Taglöhnergärten 43

76228 Karlsruhe

Tel. 07052 – 508 98 40

[jochen.kutscheruk@merlin-zwo.de](mailto:jochen.kutscheruk@merlin-zwo.de)

<http://www.merlin-zwo.de>