Hochverfügbarkeit für die Datenbank

Was ist zu beachten?

Spitzenleistung heißt, sich auf seine Stärken zu konzentrieren.

merlin.zwo

Wir machen Oracle - nur Oracle.

Aus gutem Grund.

Jochen Kutscheruk

Oracle Certified Master

merlin.zwo InfoDesign GmbH & Co. KG

76228 Karlsruhe

ORACLE Platinum Partner

Wir kümmern uns!

Hochverfügbarkeit und Datensicherheit

Hochverfügbarkeit und Datensicherheit

RAC schützt unterbrechungsfrei vor physischen Fehlern der Server, die Datenbank bleibt erreichbar.

RAC schützt nicht vor logischen Fehlern.

Über 85% der Fehler sind jedoch logische Fehler!

Eine physisch erreichbare, jedoch logisch korrupte Datenbank, ist nicht verfügbar!

Hochverfügbarkeit und Datensicherheit

DataGuard schützt vor Datenverlust, jedoch nicht unterbrechungsfrei.

Physische Fehler bedingen eine kurze Unterbrechung.

DataGuard schützt auch vor logischen Fehlern.

DataGuard gibt es nur in der Enterprise Edition.

Hochverfügbarkeit und Datensicherheit

Hochverfügbarkeit und Datensicherheit werden gerne verwechselt!

Real Application Cluster (RAC)	DataGuard
Hochverfügbarkeit	Datensicherheit
Beispiel: Tourismus-Webseite	Beispiel: Hochregallager

Warum schützt DataGuard vor Datenverlust?

Primärdatenbank

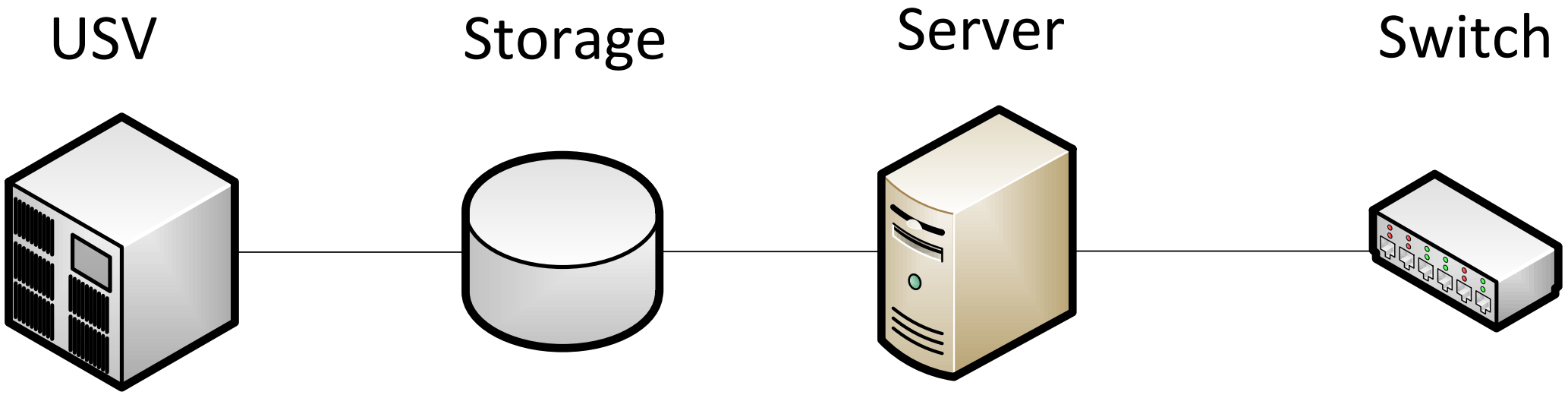
Standby

Alternativ: Manuelle Standby-Datenbank

Datenverlust garantiert!

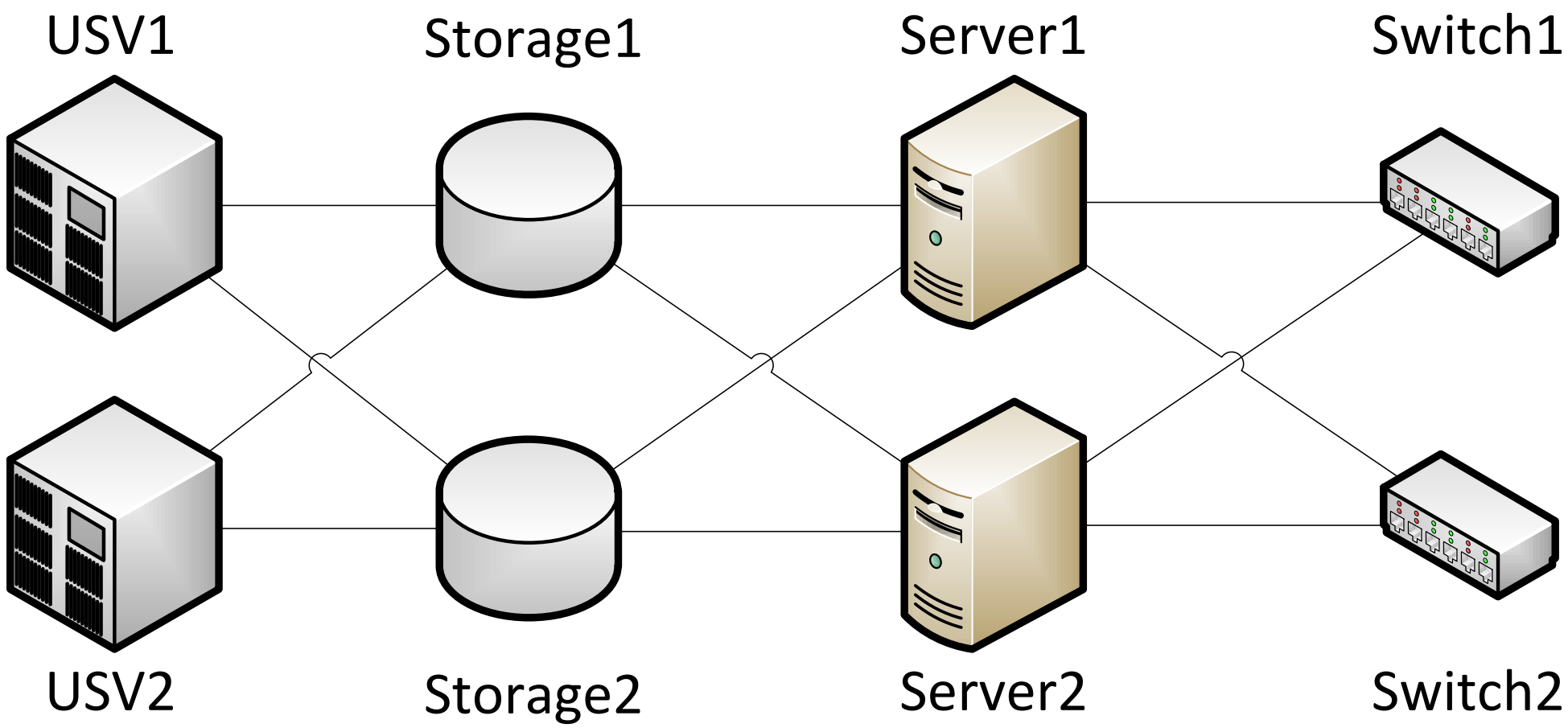
Unwahrscheinlich wahrscheinlich

Ein kleines Beispiel



Ausfall einer Komponente = Ausfall des Gesamtsystems

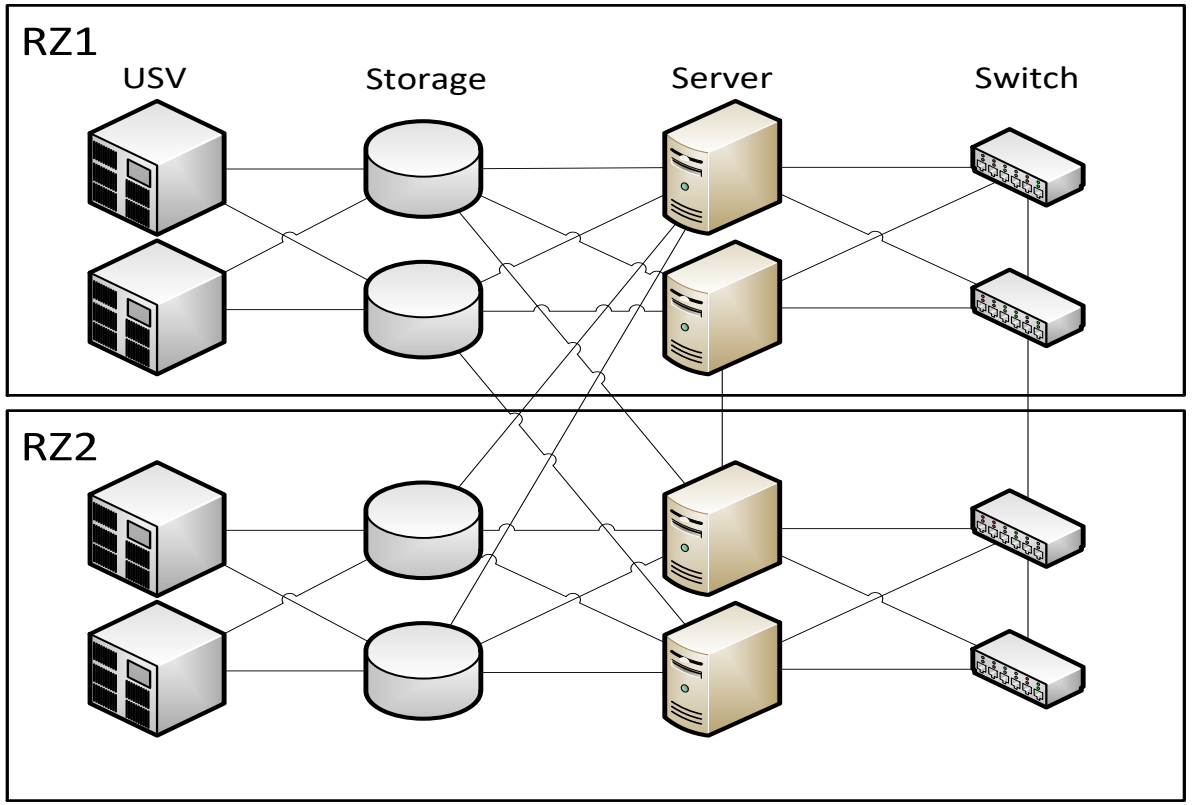
Ein kleines Beispiel



Alle Komponenten redundant, Ausfall jeweils einer Komponente tolerierbar

Ein kleines Beispiel

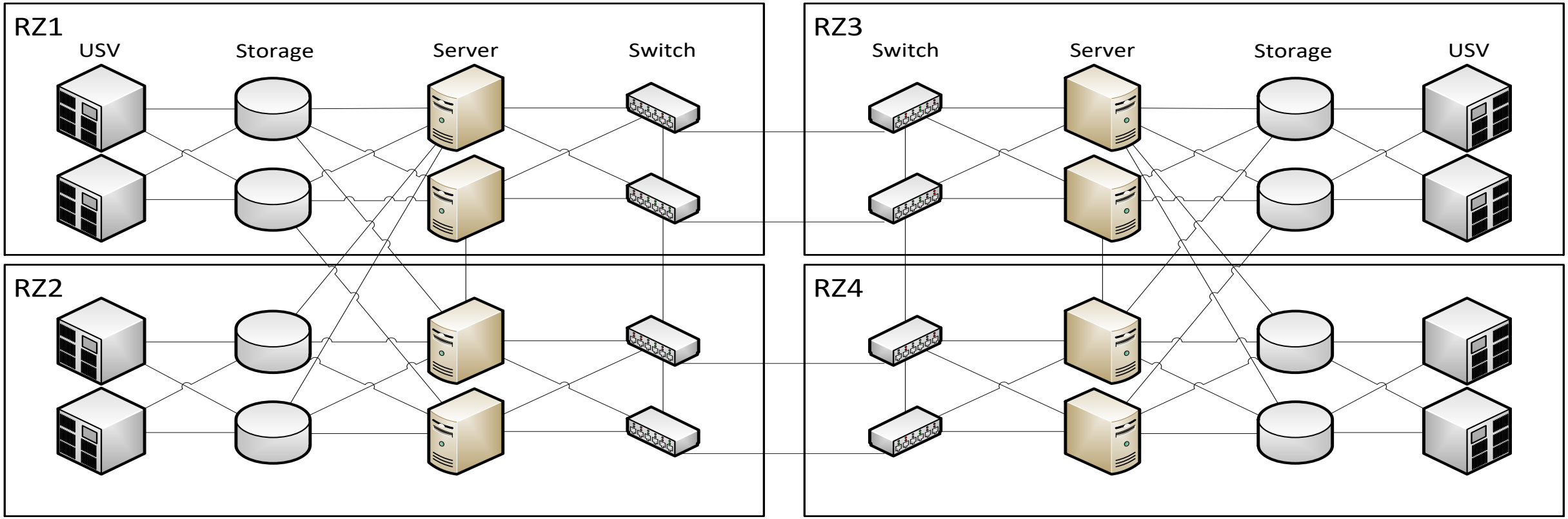
Hochverfügbarkeit durch RAC



Ein kleines Beispiel

Hochverfügbarkeit durch RAC

Datensicherheit durch Dataguard

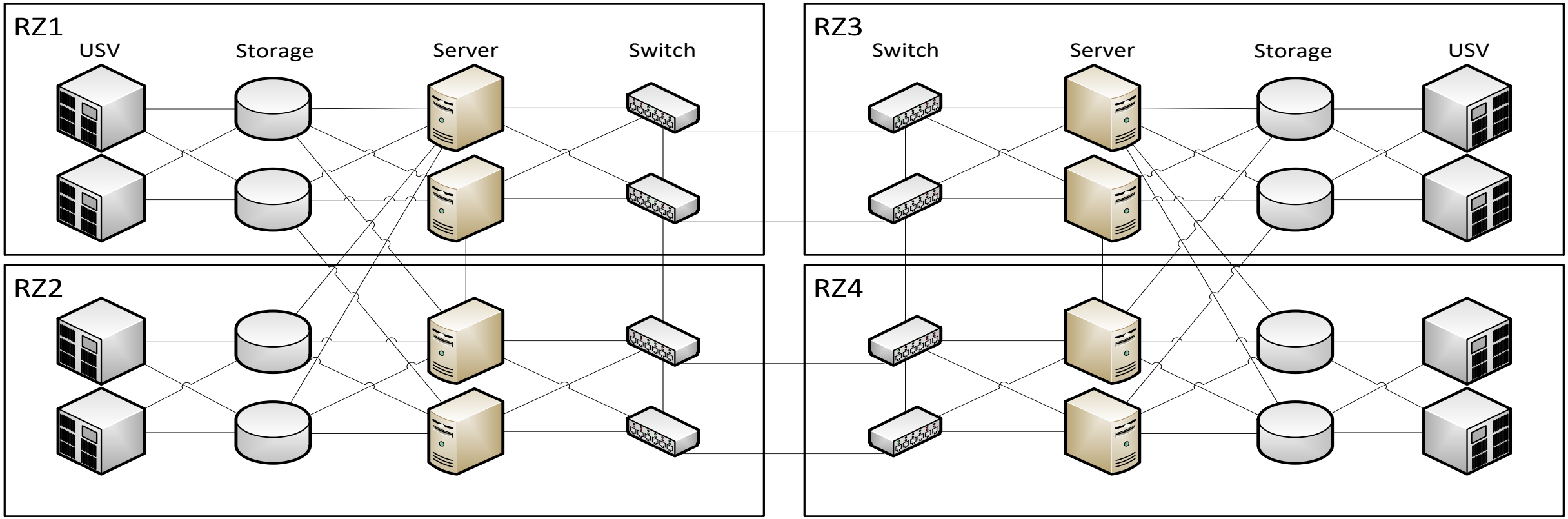


Wahrscheinlichkeit eines Totalausfalls ???

Ein kleines Beispiel

Hochverfügbarkeit durch RAC

Datensicherheit durch Dataguard

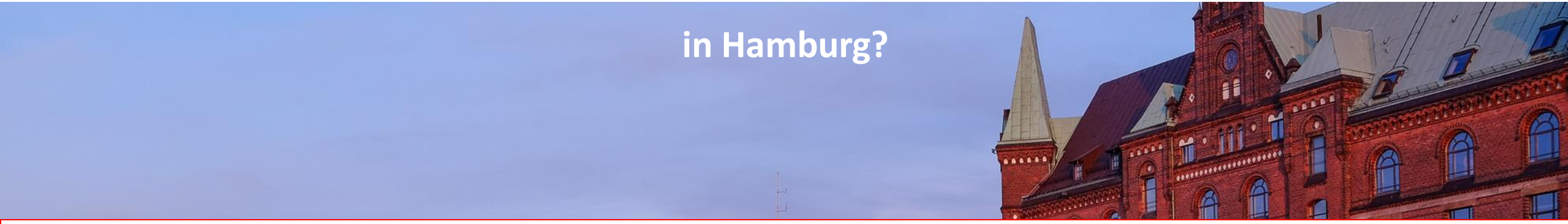


Wahrscheinlichkeit eines Totalausfalls: 100%

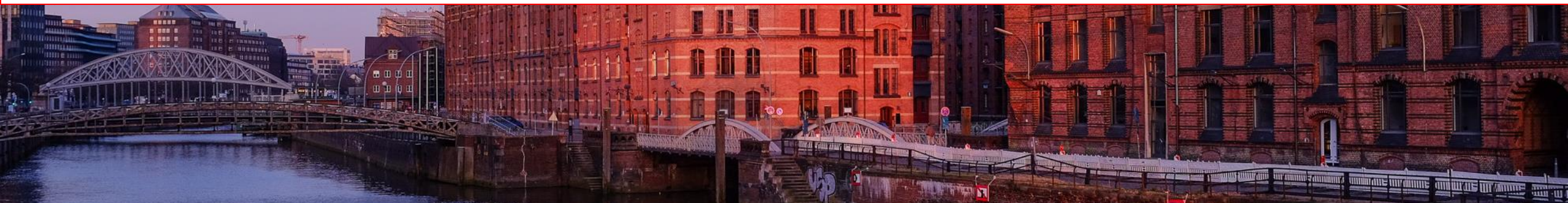
Schätzfrage zu Wahrscheinlichkeiten

Wie wahrscheinlich ist denn eigentlich

ein Erdbeben der Stärke 9



100 %



Der Teufel steckt in der Zeitachse

Wann passiert es?

Deshalb kamen uns die 30.000 Jahre zwischen Tschernobyl und Fukushima so kurz vor!

Definition der Verfügbarkeit

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 wichtig:

MTBF: Mean Time Between Failure

MTTR: Mean Time To Recover

Arten der Verfügbarkeit

Die Definition „Hochverfügbarkeit“ ist abhängig von den Anforderungen!

Verfügbarkeit der Daten	Verfügbarkeit der Anwendung
• Ein Datenverlust ist nicht akzeptabel • Ein kurzzeitiger Ausfall der Anwendung ist akzeptabel	• 24 x 7 x 365 notwendig • Ein (kleiner) Datenverlust ist akzeptabel
Beispiel: Hochregallager	Beispiel: Tourismus-Webseite

Wunsch und Wirklichkeit

Der Wunsch (des Managements?)

- Verfügbarkeitsklasse 6 (Ausfall max. 32s / Jahr)
- Minimale Anschaffungskosten
- Minimale laufende Kosten

Die Wirklichkeit

XOR

- Verfügbarkeitsklasse 6
- Maximale Anschaffungskosten
- Maximale laufende Kosten

- Minimale Anschaffungskosten
- Minimale laufende Kosten
- Verfügbarkeitsklasse 2

Die Wirklichkeit

Begrenztes Budget

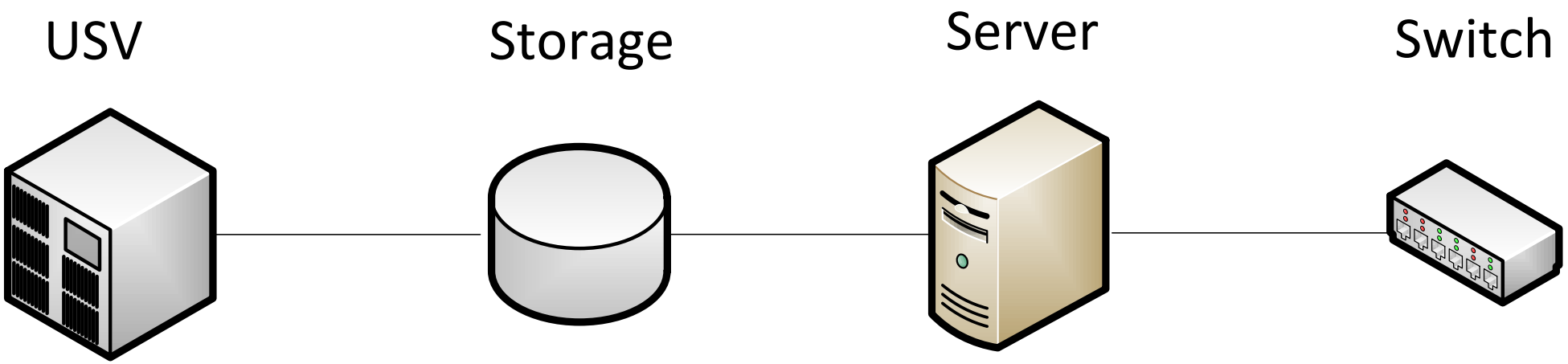
Begrenzte Zeit

Unbedingt klar kommunizieren, was mit dem gegebenen Budget in der gegebenen Zeit erreicht werden KANN!

Berechnung der Verfügbarkeit

Serienschaltung abhängiger Komponenten

Berechnet als Produkt der Verfügbarkeit



Der Einfachheit halber: Verfügbarkeitsklasse 3 (99,9%) für jede Komponente

Verfügbarkeit: 0,999 x 0,999 x 0,999 x 0,999 = 0,996 = 99,6% Gesamt!

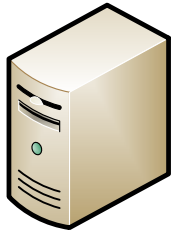
Jährliche Ausfallzeit: 34,99 Stunden statt 8,76 Stunden!

Parallelschaltung von Komponenten

Berechnet als Produkt der Ausfallzeiten

0,001% = 8,76 Stunden / Jahr

RAC-Server



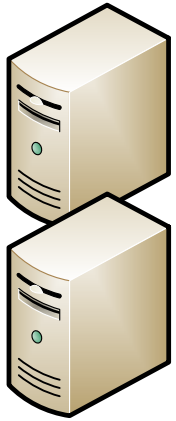
Parallelschaltung von Komponenten

Berechnet als Produkt der Ausfallzeiten

0,001% = 8,76 Stunden / Jahr

0,001 x 0,001 = 0,000001 = 31,5 Sekunden / Jahr

RAC-Server



Parallelschaltung von Komponenten

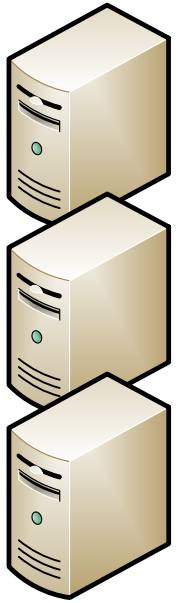
Berechnet als Produkt der Ausfallzeiten

0,001% = 8,76 Stunden / Jahr

0,001 x 0,001 = 0,000001 = 31,5 Sekunden / Jahr

0,001 x 0,001 x 0,001 = 0,000000001 = 0,03 Sekunden / Jahr

RAC-Server



Parallelschaltung von Komponenten

Berechnet als Produkt der Ausfallzeiten

0,001% = 8,76 Stunden / Jahr

0,001 x 0,001 = 0,000001 = 31,5 Sekunden / Jahr

0,001 x 0,001 x 0,001 = 0,000000001 = 0,03 Sekunden / Jahr

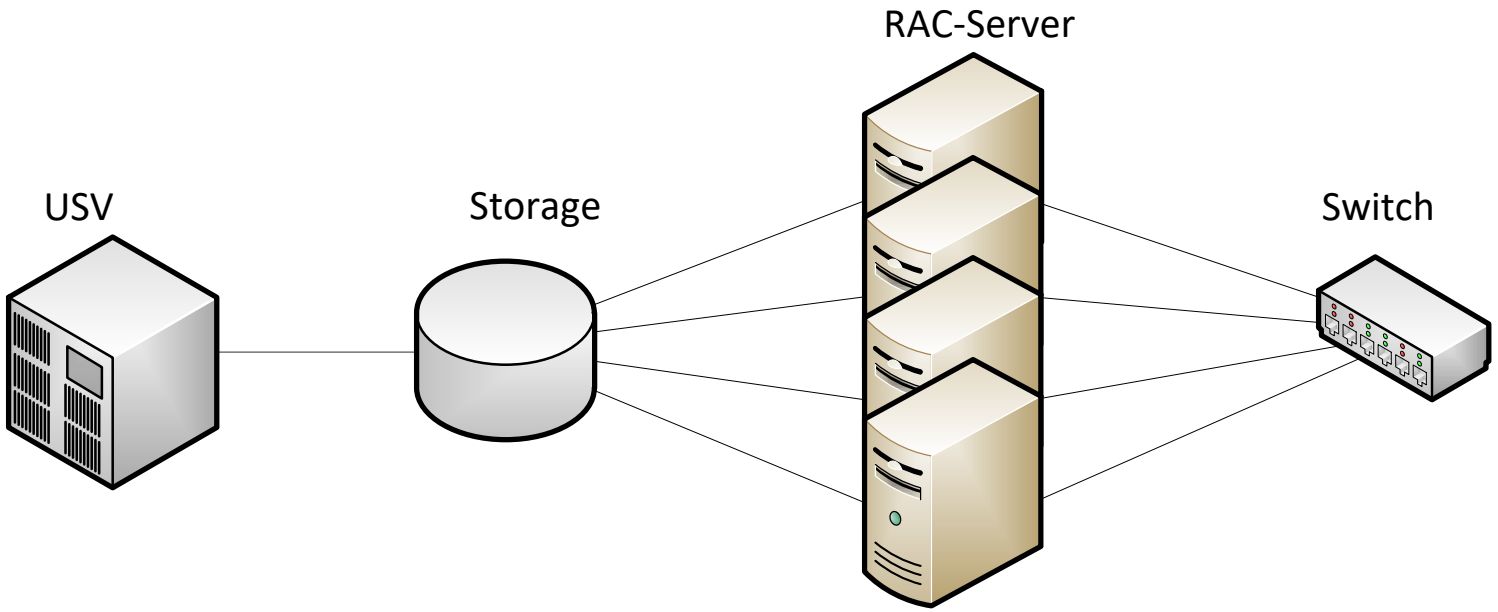
$0{,}001^4 = 1 \times 10^{-12} = 0{,}00003$ Sekunden / Jahr

RAC-Server

Jährliche Ausfallzeit: 30 µSekunden statt 8,76 Stunden!

Parallel/Seriell-Schaltung von Komponentengruppen

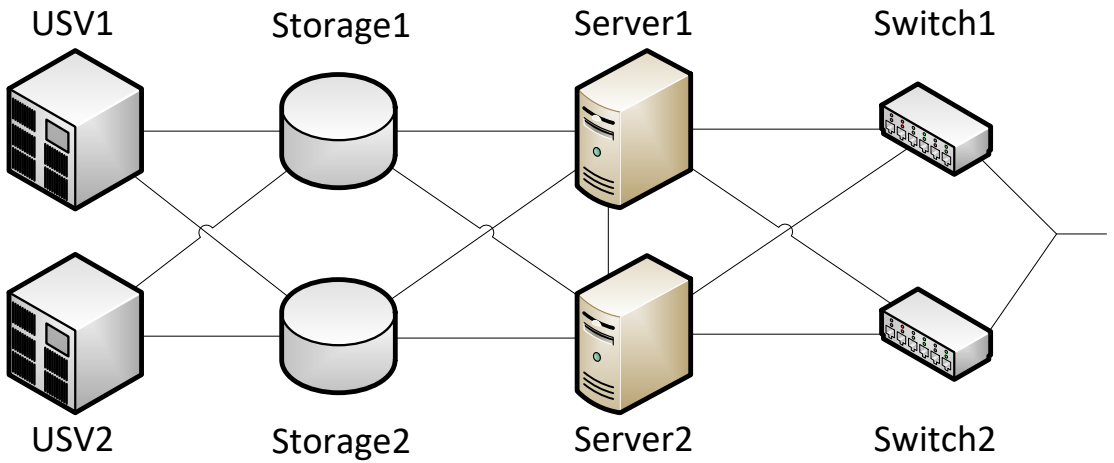
Berechnet als Produkt der Verfügbarkeiten



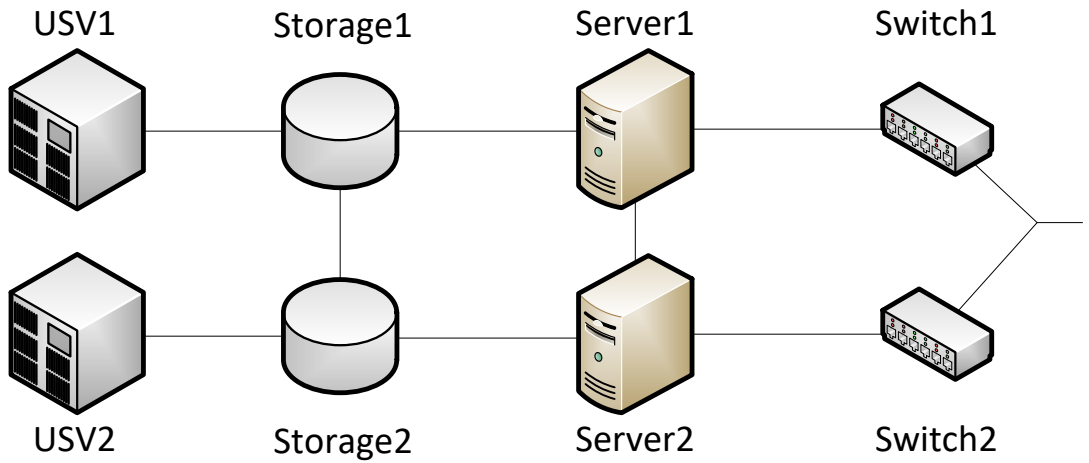
Verfügbarkeit: 0,999 x 0,999 x 0,999999999999 x 0,999 = 0,997 = 99,7% Gesamt!

Jährliche Ausfallzeit: 26,3 Stunden statt 30 µSekunden!

Serienschaltung abhängiger redundanter Komponenten



≠



$(1-(1-0{,}999)^2)^4 = 0{,}999999999984$ **= 0,5 ms / Jahr**

≠

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

Der Single Point of Failure

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 exponentiell, nicht linear.

Der Single Point of Failure

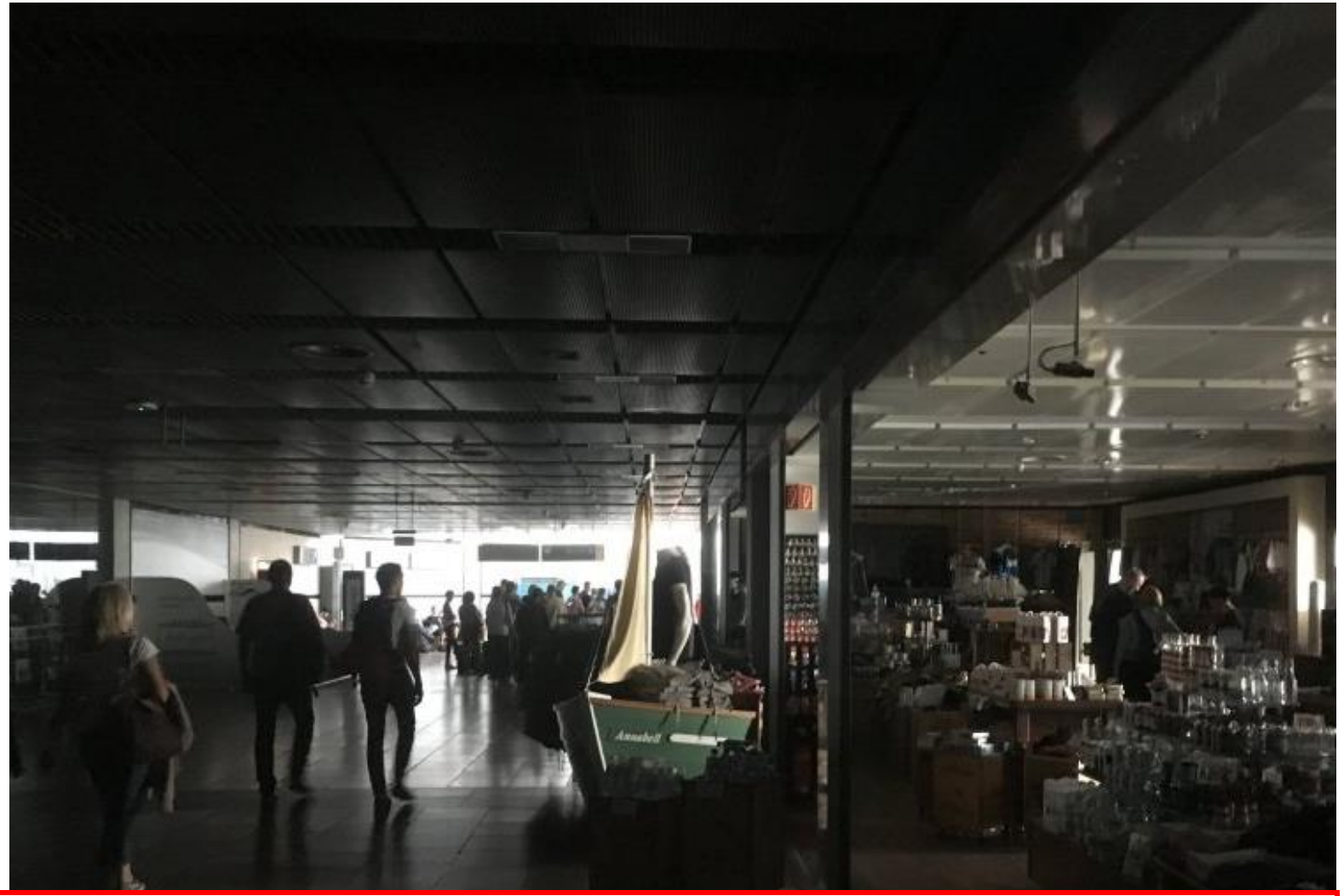
03.06.2018

10 Uhr morgens

Die Frisur sitzt

Flughafen Hamburg

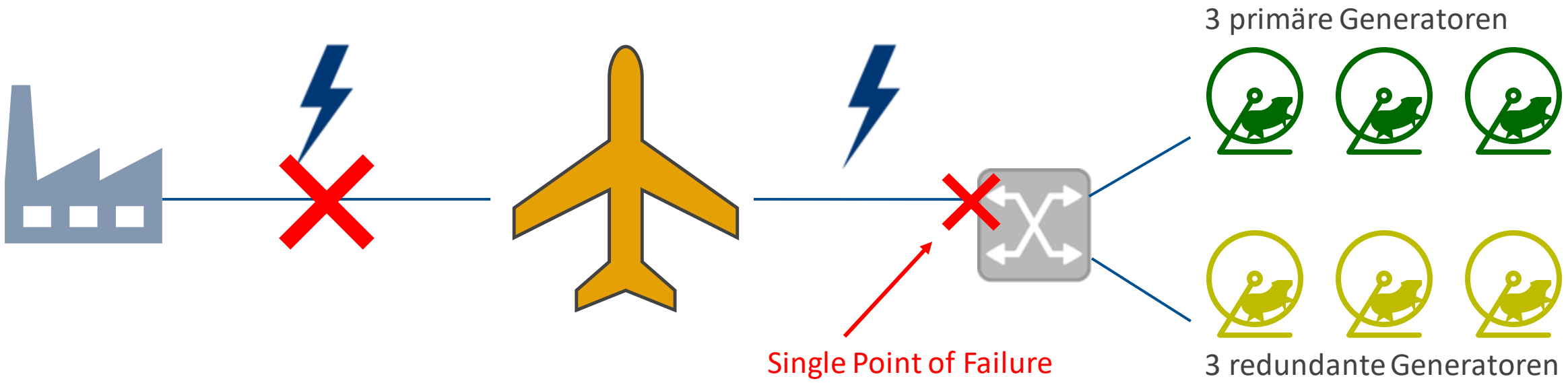
Das Unmögliche geschieht...



Über 20 Stunden Totalausfall!

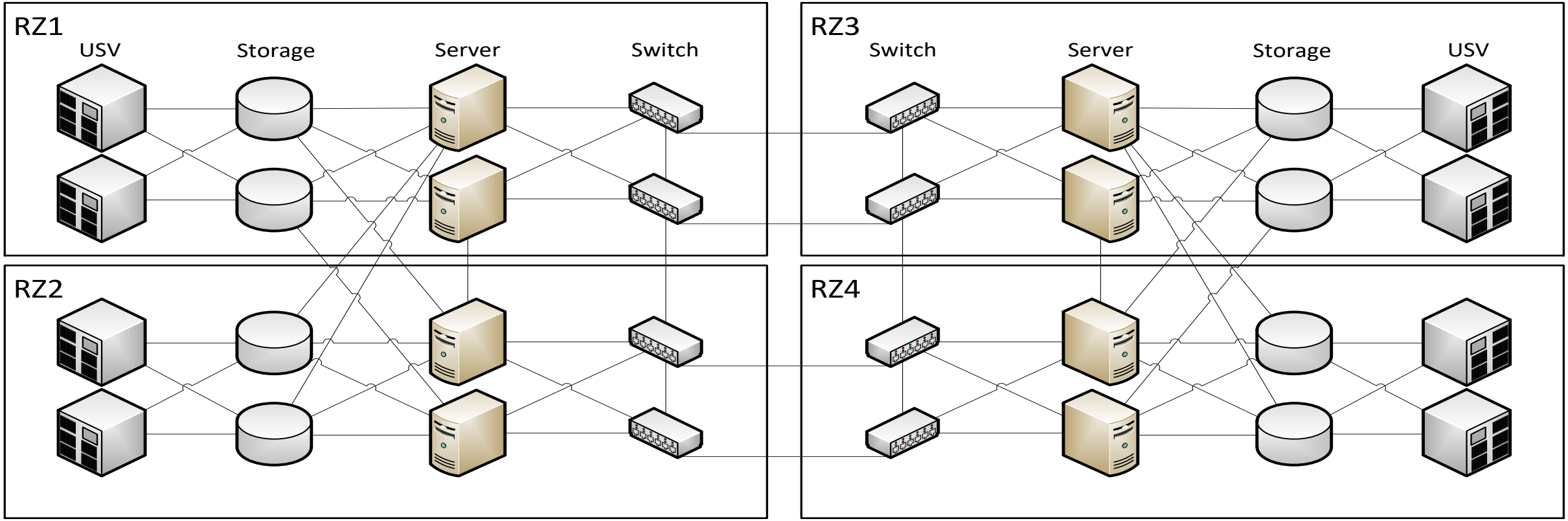
Der Single Point of Failure

Wo war das Problem?



Alternative / Ergänzende Ansätze

Alles bedacht?

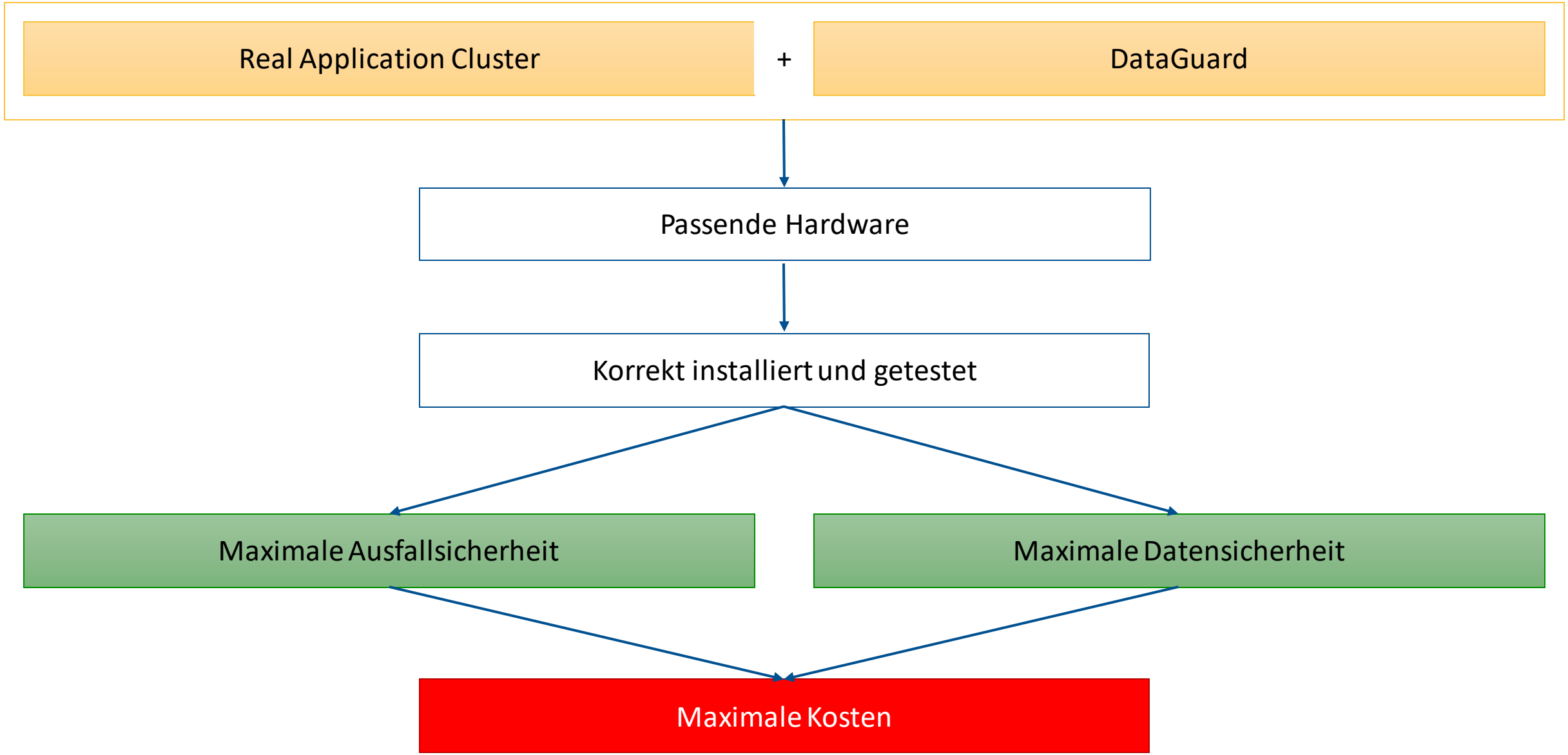


Höhere Anforderungen an das Personal!

Höhere laufende Kosten!

Zusätzliche Ausfallzeiten durch die gestiegene Komplexität des Gesamtsystems!

Weitere Überlegungen



Weitere Überlegungen

Können einfache Lösungen auch funktionieren?

Wie sind die Anforderungen?

„Nur“ Verfügbarkeit?

„Nur“ Datensicherheit?

Maximale Ausfallzeit? (MTTR)

Maximale Ausfallhäufigkeit? (MTBF)

Wann ist ein System nicht verfügbar?

Hardwareausfall

Physisch korrupte Daten

Logisch korrupte Daten

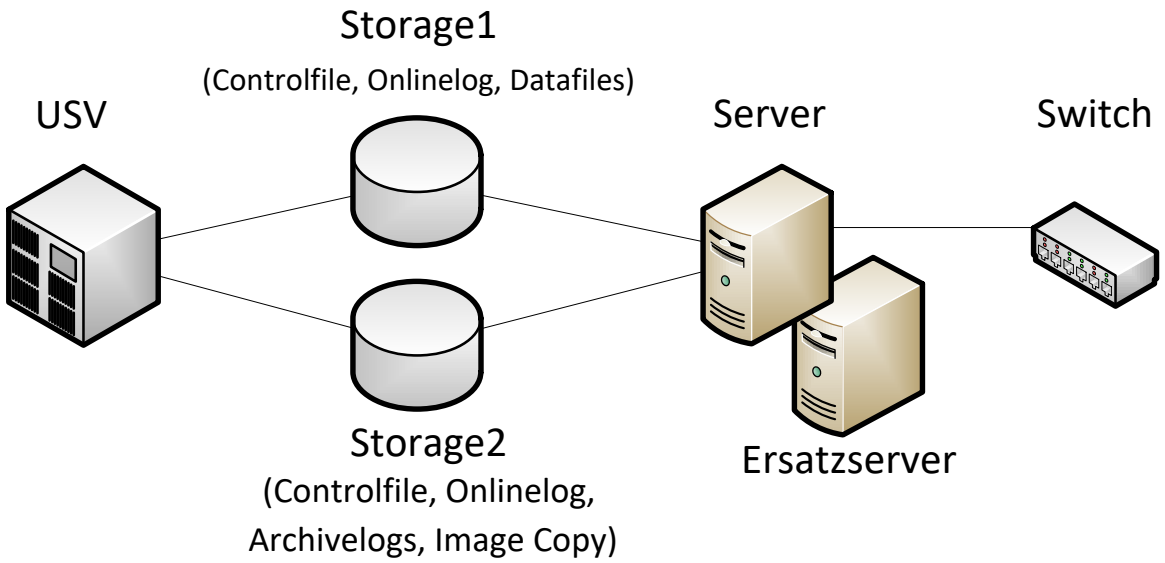
Dienste nicht gestartet (Reboot)

Antwortzeit 30 Minuten statt 30 ms

....

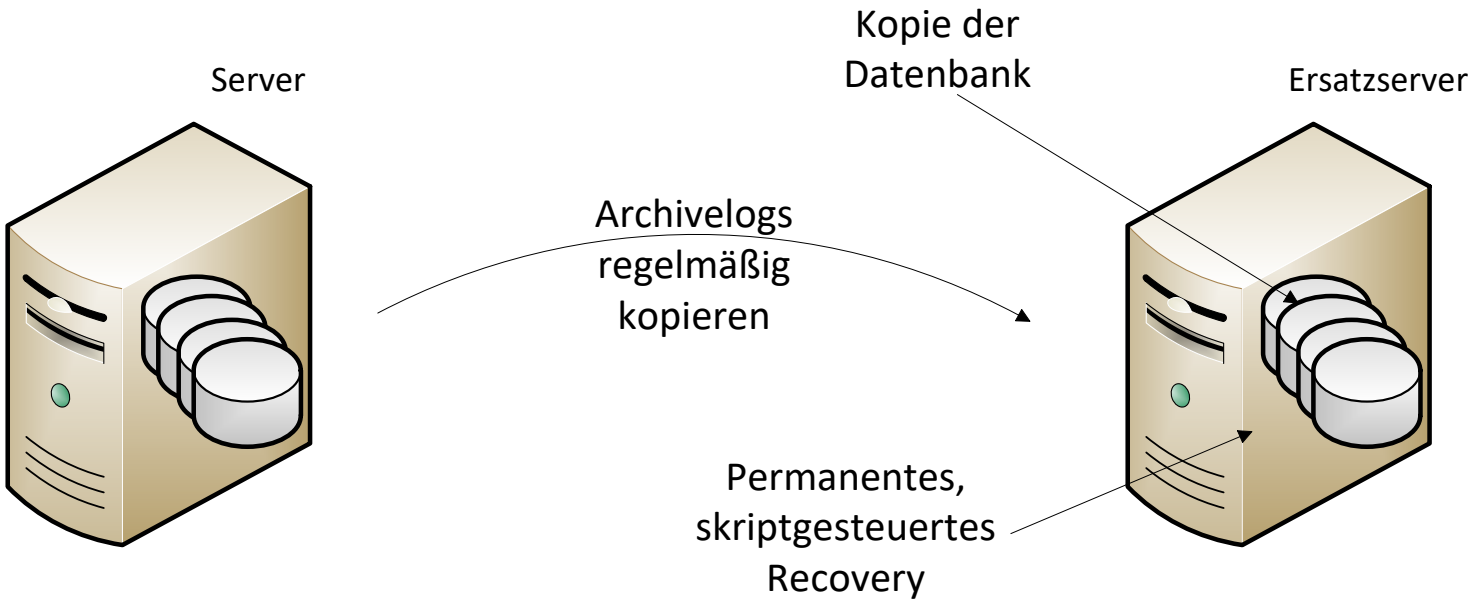
Alternative Datensicherheit

Imagecopy auf zweite, unabhängige Storage



Vorteile	Nachteile
Kein Datenverlust bei Ausfall einer Storage!	Nicht unterbrechungsfrei. Zusätzliche, nicht unabhängige Storage-Komponente. Notwendiges KnowHow im Fehlerfall verfügbar? Doppelter Festplattenplatz benötigt.

„Manuelle“ Standby-Datenbank



Vorteile

Günstig zu implementieren.

Wenig KnowHow notwendig.

Kommerzielle Produkte verfügbar.

Nachteile

Datenverlust garantiert.

Weitere Überlegungen

merlin2wo InfoDesign

Oftmals ungenutzte Möglichkeiten

Enterprise Edition	
Flashback Database	Flashback Table

Standard Edition	
Flashback Query	RMAN ImageCopy

Nutzen Sie die Cloud

Heute 14:30 Uhr:

Hochverfügbarkeit und Datensicherheit mit Hilfe der Cloud

Die Cloud als Backup-Rechenzentrum

Letzte Worte

Letzte Worte

Sie können den Single Point of Failure nicht eliminieren!

Versuchen Sie nicht um jeden Preis, das Unvermeidliche zu verhindern.

Je komplexer Ihr System ist, umso höher die Wahrscheinlichkeit, dass es ausfällt.

Was ist zu tun, damit Sie auch ohne Ihr Hauptsystem innerhalb kurzer Zeit wieder arbeiten können?

Investieren Sie Zeit in Ihren Notfallplan.

Üben Sie diesen Notfallplan regelmäßig.

Letzte Worte

RMAN Restore muss „Last Line of Defense“...	... und allerletzte Möglichkeit im Notfallplan sein!

Lassen Sie Ihr Notfallkonzept unabhängig überprüfen.

Führen Sie regelmäßige Notfallübungen durch.

Klare Kommunikation an das Management, was tatsächlich erreichbar ist!

Fragen?

merlin.zwo

Wir kümmern uns!

merlin.zwo InfoDesign GmbH & Co. KG

Jochen Kutscheruk

Elsa-Brändström-Straße 14
76228 Karlsruhe
Tel. 0721 – 132 096 21

jochen.kutscheruk@merlin-zwo.de
https://www.merlin-zwo.de