

Informationssicherheit im Unternehmen – ISO/IEC/DIN 27001



Bing!



Prof. Dr. Thomas Horn
IBH IT-Service GmbH
Gostritzer Str. 61-63
01217 Dresden
<http://www.ibh.de>
info@ibh.de

I B H Übersicht

1. Vorwort
2. Ziele eines ISMS
3. Operationelle Risiken
4. Risikomanagement
5. Verfügbarkeit
6. Zentrales Rechenzentrum vs. verteilte Serverdienste
7. Redundantes Rechenzentrum
8. IT-Grundschutz: Rechenzentrum
9. Ausfall der Stromversorgung
10. Klimatisierung
11. USV-Anlagen
12. Überwachung der Infrastruktur

Zur Historie der ISO/IEC/DIN 27001

- ◆ Ausgangspunkt ist der britische Standard BS 7799-2:2002
- ◆ Die ISO/IEC 27001:2005 wurde als internationale Norm aus dem britischen Standard entwickelt und 2005 veröffentlicht.
- ◆ Seit September 2008 ist diese Norm auch als DIN-Norm ISO/IEC/DIN 27001 unter dem Titel "*Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme – Anforderungen*" in deutscher Sprache verfügbar.
- ◆ Der Standard spezifiziert die Anforderungen für Erstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten **Informationssicherheits-Managementsystems** (ISMS) unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
- ◆ Unter *Organisation* versteht der Standard jede Form von Unternehmen, Einrichtungen, Behörden, Verbänden ...

IBH Vorwort (2)

IT-Grundschutz des BSI

- ◆ Das IT-Grundschutzhandbuch vom BSI gibt es seit 2002 (55 Bausteine, 600 Maßnahmen, 2194 Seiten)
- ◆ Es gab keine klare Regelung, ob der IT-Grundschutz für Firmen etc. überhaupt eine Bedeutung hat
- ◆ Mit der 10. Ergänzungslieferung vom Oktober 2008 gab es beim BSI einen Paradigmenwechsel von "*IT-Sicherheit*" zu "*Informationssicherheit*", der mehr als ein reiner Begriffswechsel ist
- ◆ Außerdem wurde als wesentliche Erkenntnis verankert, dass die Ziele und Geschäftsprozesse einer Organisation der Ausgangspunkt aller Sicherheitsüberlegungen sind
- ◆ Die Fortschreibungen der ISO-Standards der ISO 2700x-Reihe wurden eingearbeitet
- ◆ Aktuell gibt es seit November die 11. Ergänzungslieferung mit einem Umfang von 4.101 Seiten (78 Bausteine, 553 Gefährdungen, 1.157 Maßnahmen)



ISO/IEC/DIN 27001 vs. IT-Grundschutz

- ◆ Der Standard ISO/IEC/DIN 27001 ist sehr abstrakt gefasst und lässt relativ große Spielräume zu
- ◆ Da der Standard ISO/IEC 27001 seit September 2008 eine verbindliche DIN-Norm ist, braucht man nicht mehr darüber zu diskutieren, ob das IT-Grundschutzhandbuch des BSI verbindlich ist oder nicht
- ◆ Durch die Erhebung des ISO/IEC 27001 in den Rang einer nationalen deutschen Norm, kann man sich in der praktischen Tätigkeit auch an dem IT-Grundschutzhandbuch des BSI orientieren, denn das IT-Grundschutzhandbuch ist ein guter Ratgeber auf den Weg zu einer Zertifizierung nach ISO/IEC 27001
- ◆ Mit seiner einfachen, strukturierten Vorgehensweise stellt das IT-Grundschutzhandbuch des BSI ein "Kochbuch" zum Handeln dar und ist wesentlich strenger gefasst ist.

Begriffsbestimmung

In der Vergangenheit wurden sowohl die Begriffe *Privacy* als auch *Security* mit *Datenschutz* übersetzt.

- ◆ Privacy Schutz der Privatsphäre
Datenschutz (jur.)
- ◆ Security Schutz gegen unbefugte Benutzung
Datenschutz (techn.)
(read, write, modify)
- ◆ Safety technische Datensicherheit
(Schutz vor technischen Defekten,
physikalischen Einflüssen und Ausfällen)
→ Erhöhung der Verfügbarkeit
→ Disaster-Toleranz

Datenschutz

**Informations-
sicherheit
gemäß
ISI/IEC/DIN 27001**

I B H Ziele eines ISMS (1)

Minderung der operationellen Risiken durch Schutz vor

- ◆ menschliches Versagen
- ◆ kriminelle Handlungen (gekündigte Mitarbeiter, bewusste Schädigung durch Konkurrenz, Hacker)
- ◆ Katastrophen (Feuer, Wasser, Erdbeben etc.)
- ◆ Softwarefehler

Oberste Ziele

- ◆ **Erhöhung der Verfügbarkeit → Unternehmen muß arbeitsfähig bleiben**
- ◆ **Schutz der Daten gegen Verlust und Verfälschung**
- ◆ **keinen Mißbrauch der Daten zulassen**

I B H Ziele eines ISMS (2)

Unternehmensstabilität, Geschäftserfolge und Image hängen im entscheidenden Maße von qualifizierten Management-Prozessen in der Organisation ab, die

- ◆ vom Gesetzgeber gefordert werden
- ◆ von den Vertragspartnern erwartet werden
- ◆ in Ausschreibungen gefordert werden
- ◆ von Kunden bei der Auftragserteilung berücksichtigt werden
- ◆ von Banken und Versicherungen bewertet werden.

In der ISO/IEC/DIN 27001 werden für das Management der Informationssicherheit keine standardisierten Management-Systeme festgelegt, sondern nur Mindestanforderungen formuliert.

ISO/IEC/DIN 27001 spezifiziert, welche Anforderungen an das Management der Informationssicherheit zu stellen sind und welche Komponenten ein ISMS enthalten muss!

I B H Operationelle Risiken 1

Was sind operationelle Risiken?

- ◆ Operationelle Risiken sind alle Risiken,
 - die weder durch den Unternehmer
 - noch durch den Markt verursacht werden.
- ◆ Sie können in vier Kategorien eingeordnet werden:
 - Verursachung durch den Menschen
 - Verursachung durch die verwendeten Systeme
 - Verursachung durch die implementierten Prozesse
 - Verursachung durch externe Ereignisse
- ◆ Einen besonderen Stellenwert erhalten diese Ursachen durch die allumfassende elektronische Datenverarbeitung und globale Vernetzung

Die Herstellung einer hohen Informationssicherheit im Unternehmen ist ein ständiger Prozess.

**Daher fordert ISO/IEC/DIN 27001 ein Informationssicherheits-
Managementsystem im Unternehmen!**

IBH Operationelle Risiken 2

Die vier Kategorien operationeller Risiken

Mensch

- Betrug
- Fehler
- menschliches Versagen
- ungenügend qualifiziertes Personal

Systeme

- Datensicherheit
- Datenintegrität
- Systemabstürze
- Softwarefehler
- Hardwareausfälle

Prozesse

- fehlerhafte Arbeitsrichtlinien
- unvollständige Berichterstattung
- mangelhafte interne Kontrollen

Externe Ereignisse

- Naturkatastrophen
- Terroranschläge
- rechtliche Risiken

Der Schutz gegen die systembedingten operationellen Risiken ist in erster Linie ein Problem der Gestaltung der elektronischen Datenverarbeitung!
Die Bedeutung einer vernünftigen Gestaltung der elektronischen Datenverarbeitung geht aber weit über die systembedingten operationellen Risiken hinaus!!!

Änderungen der gesetzlichen Rahmenbedingungen

- ◆ Sicherung der europäischen Kreditinstitute durch die Baseler Beschlüsse
 - 1988: Basel I
 - 2007: Basel II (EU-Richtlinien 2006/48/EG und 2006/49/EG)
- ◆ Änderung des § 147 AO vom 27.10.2000
- ◆ Haftung von Vorstand und Geschäftsleitung bei mangelnder Vorsorge bzw. Frühwarnung im Rahmen des betrieblichen Risikomanagements
KonTraG vom 27.4.1998
- ◆ Änderung des HGB, siehe §289 (1)
Damit gelten die Änderungen des KonTraG auch für beliebige Kapital- und Personengesellschaften
- ◆ Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) → Regeln zur Aufbewahrung digitaler Unterlagen und zur Mitwirkungspflicht der Steuerpflichtigen bei Betriebsprüfungen
→ Verwaltungsanweisung des Bundesfinanzministeriums vom 16. Juli 2001 (BGBl. I S. 1542), modifiziert 2002
- ◆ Weitere: BDSG, SOX, TDG, UrhG, SüG, etc.

IBH Verfügbarkeit (1)

Verfügbarkeit und Zuverlässigkeit nach ITIL (ISO 20000)

- ◆ **Verfügbarkeit** = (Betriebszeit – Ausfallzeit) / Betriebszeit
- ◆ was bedeutet eine solche Angabe in der Praxis?

Verfügbarkeit	Ausfallzeit pro Jahr		
	Tage	Stunden	Minuten
95%	18,25	438,00	26.280
98%	7,30	175,20	10.512
99%	3,65	87,60	5.256
99,5%	1,83	43,80	2.628
99,9%	0,37	8,76	526
99,99%	0,04	0,88	53
99,999%	0,00	0,09	5

- ◆ **Zuverlässigkeit [MTBF]** = (Betriebszeit – Ausfallzeit) / Ausfälle
- ◆ Verfügbarkeit 98%, 4 Ausfälle/Jahr → MTBF = 2.146h

I B H Verfügbarkeit (2)

- ◆ Für jede Applikation bzw. für jeden Dienst, muss durch die Informationsverantwortlichen der Abteilungen in Abstimmung mit der Leitung der Organisation eine Verfügbarkeitsschutzklasse festgelegt werden:
 - Schutzklasse 0 = keine besondere Verfügbarkeit (95-98%)
(Wiederherstellung/Reparatur in angemessener Zeit)
 - Schutzklasse 1 = mittlere Verfügbarkeit (98,5-99,2%)
(Wiederherstellung/Reparatur spätestens am nächsten Geschäftstag)
 - Schutzklasse 2 = hohe Verfügbarkeit (99,5-99,9%)
(Wiederherstellung/Reparatur binnen 8 Stunden)
 - Schutzklasse 3 = sehr hohe Verfügbarkeit (>99,99%)
(Wiederherstellung der Funktionsfähigkeit unter 1 Stunde)

I B H Zentrales Rechenzentrum vs. verteilte Serverdienste

Warum alle Dienste in *einem* Rechenzentrum konzentrieren?

- ◆ Es geht um maximale Informationssicherheit:
 - Weniger Sicherheitsbereiche
 - Schutz der Daten vor dem Zugriff Unbefugter einfacher realisierbar
 - Verfügbarkeit einfacher zu realisieren
 - einfacheres Management
 - Reduzierung der Anzahl der Server und Speichersysteme
- ◆ Zugriff auf die zentralen Ressourcen über ein "eigenes" Netzwerk
- ◆ Gemeinsame Nutzung der Daten und Dienste

**Kosten für ein RZ
steigen weiter**

Arbeitslohn, Betriebsmittel
und Investitionen werden
nicht billiger



**Kosten für ein Netzwerk
fallen weiter**

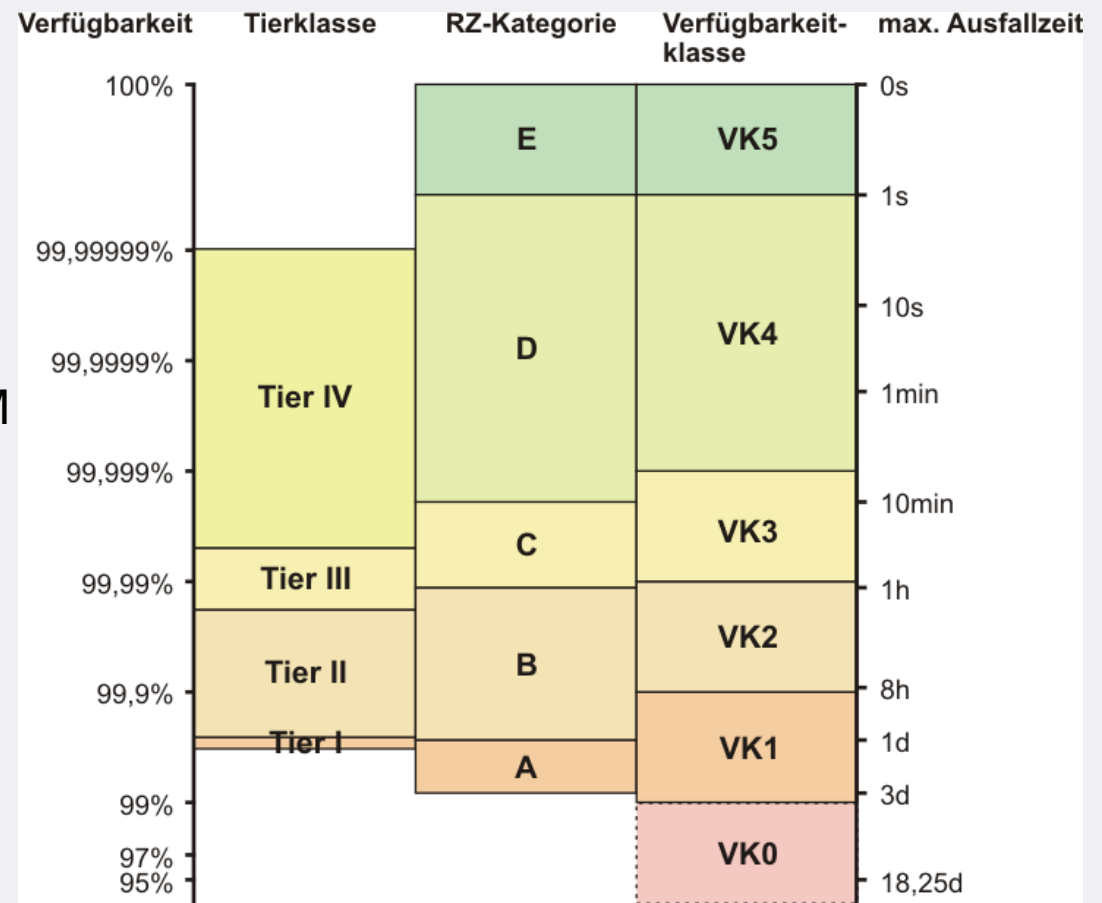
Bandbreiten und Leitungen
haben auch zukünftig einen
weiteren Preisverfall

Ein Rechenzentrum ist aber ein globaler Single Point of Failure (SPOF)!

IBH Redundantes Rechenzentrum (1)

Warum redundante Rechenzentren?

- ◆ Es geht um Verfügbarkeiten und maximale Ausfallzeiten
- ◆ es gibt verschiedene RZ-Einstufungen:
 - US-Norm TIA-942
 - RZ-Kategorie nach BITKOM
 - Verfügbarkeitsklasse nach BSI



IBH Redundantes Rechenzentrum (2)

Warum redundante Rechenzentren?

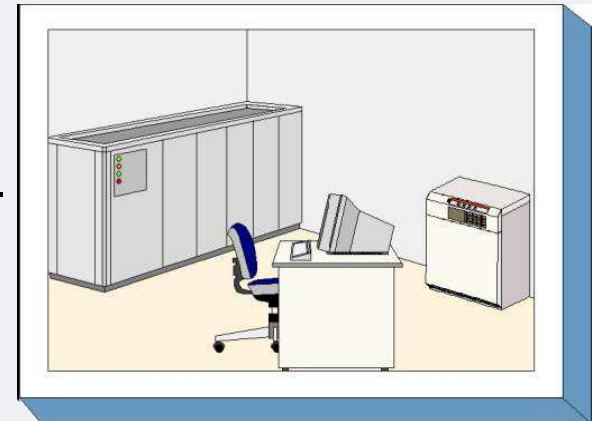
- ◆ Was kosten Ausfälle einer Organisation?
- ◆ Welche Kosten verursacht ein zuverlässiges Rechenzentrum: TIA-942 sagt Tier II kostet etwas das 1,5fache Tier IV kostet etwa das 2,5fache wobei aber durch ein Rechenzentrum nicht alle Risiken abgesichert werden können
- ◆ Daher sind zwei RZ der Klasse Tier I günstig:
 - moderate Kosten
 - Absicherung aller Risiken, wie Komplettausfall eines Standortes

Standort 1 \ Standort 2	Tier I	Tier II	Tier III	Tier IV
Tier I	Tier III	Tier III	Tier III	Tier IV
Tier II	Tier III	Tier IV	Tier IV	Tier IV
Tier III	Tier III	Tier IV	Tier IV	Tier IV
Tier IV	Tier IV	Tier IV	Tier IV	Tier IV

IBH IT-Grundschutz 1

Neuer Baustein: B 2.9 Rechenzentrum

- ◆ Gegenstand dieses Bausteins ist ein Rechenzentrum mittlerer Art und Güte. Die Sicherheitsanforderungen liegen zwischen denen eines Serverraums oder "Serverparks" und denen von Hochsicherheitsrechenzentren.
- ◆ Für Rechenzentren ist im Unterschied zum Serverraum eine räumliche Trennung der IT-Systeme und der unterstützenden Infrastruktur (Elektroversorgung, Klimatechnik usw.) obligatorisch.
- ◆ Ein Rechenzentrum sollte insgesamt einen Sicherheitsbereich bilden.
- ◆ 27 Gefährdungen vom *Ausfall der Stromversorgung* bis hin zu *Sabotage*
- ◆ 33 Maßnahmevorschläge von der *Netzersatzanlage* bis zum *Notfallarchiv*
- ◆ Neue Maßnahme M 1.49 "*Technische und organisatorische Vorgaben für das Rechenzentrum*":
 - lichte Raumhöhe von 3,00m
 - getrennter Raum für Patchfelder u. v.a.m.



Gefährdungskataloge

enthalten die ausführlichen Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden. In der 11. ergänzten Ausgabe gibt es insgesamt 553 Gefährdungen, die in fünf Kataloge unterteilt worden:

- ◆ G1: Höhere Gewalt
- ◆ G2: Organisatorische Mängel
- ◆ G3: Menschliche Fehlhandlungen
- ◆ G4: Technisches Versagen
- ◆ G5: Vorsätzliche Handlungen

Maßnahmenkataloge

beschreiben die in den Bausteinen des Handbuchs zitierten IT-Sicherheitsmaßnahmen ausführlich. In der 11. ergänzten Ausgabe gibt es insgesamt 1.157 Maßnahmen die in sechs Kataloge eingruppiert wurden:

- ◆ M 1: Infrastrukturelle Maßnahmen
- ◆ M 2: Organisatorische Maßnahmen
- ◆ M 3: Personelle Maßnahmen
- ◆ M 4: Maßnahmen im Bereich Hard- und Software
- ◆ M 5: Maßnahmen im Kommunikationsbereich
- ◆ M 6: Notfallvorsorge-Maßnahmen

Maßnahmenkataloge

Mit der 10. ergänzten Ausgabe wurden alle vom BSI empfohlenen Maßnahmen erstmals wie folgt klassifiziert:

- ◆ A-Maßnahmen sind essentiell für die Sicherheit und daher vorrangig umzusetzen. Ihre Umsetzung ist eine Voraussetzung für Erteilung eines Zertifikats nach BSI und ISO 27001.
- ◆ B-Maßnahmen müssen für das BSI-Zertifikat "IT-Grundschatz Aufbaustufe" und für das ISO 27001-Zertifikat auf Basis von IT-Grundschatz umgesetzt sein.
- ◆ C-Maßnahmen müssen zusätzlich für das ISO 27001-Zertifikat auf Basis von IT-Grundschatz umgesetzt sein.
- ◆ Z-Maßnahmen sind zusätzliche Maßnahmen, deren Umsetzung bei höheren Sicherheitsanforderungen empfohlen wird.
- ◆ W-Maßnahmen dienen im wesentlichen zur Wissensvermittlung, die u. U. zum besseren Verständnis von A-, B- und C-Maßnahmen dienen.

IBH G 4.1 Ausfall der Stromversorgung

Wichtigste Gefährdung (direkt benannt in 16 Bausteinen)

- ◆ Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als ~~20~~ ms sind geeignet, den IT- **10** Betrieb zu stören. Bei einer Messung mit ca. 60 Messstellen wurden 1983 in Deutschland rund 100 solcher Netzeinbrüche registriert.
- ◆ Von der Stromversorgung sind nicht nur die offensichtlichen Stromverbraucher (PC, Beleuchtung usw.) abhängig. Alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig.
- ◆ Die Liberalisierung des Strommarktes führte in einigen Industrieländern zu einer Verschlechterung des Versorgungsniveaus. Auch in Deutschland könnte daher die Gefahr wachsen, dass Probleme durch Ausfälle der Stromversorgung oder durch Schaltvorgänge an nationalen Versorgungsübergängen entstehen.
- ◆ Beispiele: 2001: Kalifornien, 2005: Niedersachsen/NRW, etc.

- ◆ Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT
- ◆ Verantwortlich für Umsetzung: Haustechnik, Administrator
- ◆ Mit einer USV kann ein kurzzeitiger Stromausfall überbrückt werden oder die Stromversorgung solange aufrechterhalten werden, dass ein geordnetes Herunterfahren angeschlossener Rechner möglich ist. Dies ist insbesondere dann sinnvoll,
 - wenn im Rechner umfangreiche Daten zwischengespeichert werden (z. B. Cache-Speicher im Netz-Server), bevor sie auf nichtflüchtige Speicher ausgelagert werden,
 - beim Stromausfall ein großes Datenvolumen verloren gehen würde und nachträglich nochmals erfasst werden müsste,
 - wenn die Stabilität der Stromversorgung nicht ausreichend gewährleistet ist.
- ◆ Zwei Arten der USV sind zu unterscheiden:
 - offline-USV: Hierbei werden die angeschlossenen Verbraucher im Normalfall direkt aus dem Stromversorgungsnetz gespeist. Erst wenn dieses ausfällt, schaltet sich die USV selbsttätig zu und übernimmt die Versorgung.
 - online-USV: Hier ist die USV ständig zwischen Netz und Verbraucher geschaltet. Die gesamte Stromversorgung läuft immer über die USV.

I B H M 1.28 Lokale unterbrechungsfreie Stromversorgung 2

- ◆ Beide USV-Arten können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch dazu dienen, Überspannungen zu glätten.
- ◆ Werden IT-Geräte in einem Gebäude mit TN-S-Netz mit einer lokalen USV versorgt, ist zu beachten: Um die Schutzwirkung des TN-S-Netzes gegen Ausgleichsströme auf Schirmen von Datenleitungen aufrecht zu erhalten, ist darauf zu achten, dass USV-ausgangsseitig keine Verbindung zwischen N- und PE-Leiter (Nullung) besteht. Ggf. sind solche oft serienmäßig eingebauten Verbindungen vor Einbau in das TN-S-Netz zu entfernen.
- ◆ Bei der Dimensionierung einer USV kann man in der Regel von einer üblichen Überbrückungszeit von ca. 10 bis 15 Minuten ausgehen. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, so dass nach Abwarten dieser Zeitspanne noch 5 Minuten übrig bleiben, um die angeschlossene IT geordnet herunterfahren zu können, sollte der Stromausfall länger andauern.



M 1.70 Zentrale unterbrechungsfreie Stromversorgung 1 (neu)

- ◆ Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT
- ◆ Verantwortlich für Umsetzung: Haustechnik, Administrator
- ◆ Begründung der Notwendigkeit einer USV-Anlage
- ◆ Drei Arten der USV sind zu unterscheiden:
 - VFD-USV (Voltage and Frequency Dependent)
Verbraucher im Normalbetrieb direkt aus dem Stromversorgungsnetz gespeist. Eine VFD-USV hat Umschaltlücke von bis zu 10 ms (Umschaltlücke) → früher: Offline-USV
 - - VI-USV (Voltage Independent)
Versorgungsspannung wird bei kleineren Schwankungen nachgeregelt (VI steht für Voltage Independent), Frequenz am Ausgang einer VI-USV ist aber wie bei einer vom Versorgungsnetz abhängig. Auch bei VI-USV kann es Umschaltlücken geben.
 - VFI-USV (Voltage and Frequency Independent)
Im Normalfall keine direkte Verbindung mehr zwischen USV-Eingang und –Ausgang → Doppelwandler-USV bzw. früher auch Online-USV
VFI-USV ist wirklich unterbrechungsfrei
Gemäß DIN IEC 62040-3: VFI-SS-111

◆ Wertvolle Hinweise zu:

- Bei der Festlegung der Ausgangsleistung sollte man also ausreichende Reserven einplanen.
- Typische Werte für die Stützzeit liegen bei 30 bis 60 Minuten. Der doppelte Ansatz der Shutdown-Zeit bewirkt ein Sicherheitspolster.
- Empfindlichster Teil einer USV ist die Batterie. Nur wenn diese bei der vom Hersteller genannten optimalen Temperatur (typischerweise um 20°C) untergebracht wird, kann sie ihre maximale Leistung und Lebensdauer erreichen. Pro 10 Kelvin, um die diese Solltemperatur überschritten wird, vermindern sich Leistung und Lebensdauer um circa 50 %.
- **Redundante USV-Anlagen kennt das GSHB noch nicht, aber es gibt einen Hinweis:**
Außerdem ist bei einer USV besonders auf den Schutz vor dem Zugriff Unbefugter, Brand und Wasser zu achten. Ein sinnvoller Schutz gegen Brand macht es nahezu unverzichtbar, einander Redundanz bietende USV-Einheiten in getrennten Brandabschnitten unterzubringen.

I B H Klimatisierung 1

Klimatechnik

Für die Erreichung der maximalen Zuverlässigkeit der Computertechnik sollten strengste klimatische Kriterien eingehalten werden:

- ◆ Temperatur **20-30°C** (optimal <25°C)
Oberhalb 30°C nimmt die Zuverlässigkeit schnell ab!
- ◆ rel. Luftfeuchtigkeit **40-60%**
Zu niedrige Luftfeuchte führt zum Austrocknen der Bauelemente!
Oberhalb 90% ist mit Kondenswasserbildung zu rechnen!

Geräte im Winter erst 1-2h akklimatisieren lassen!

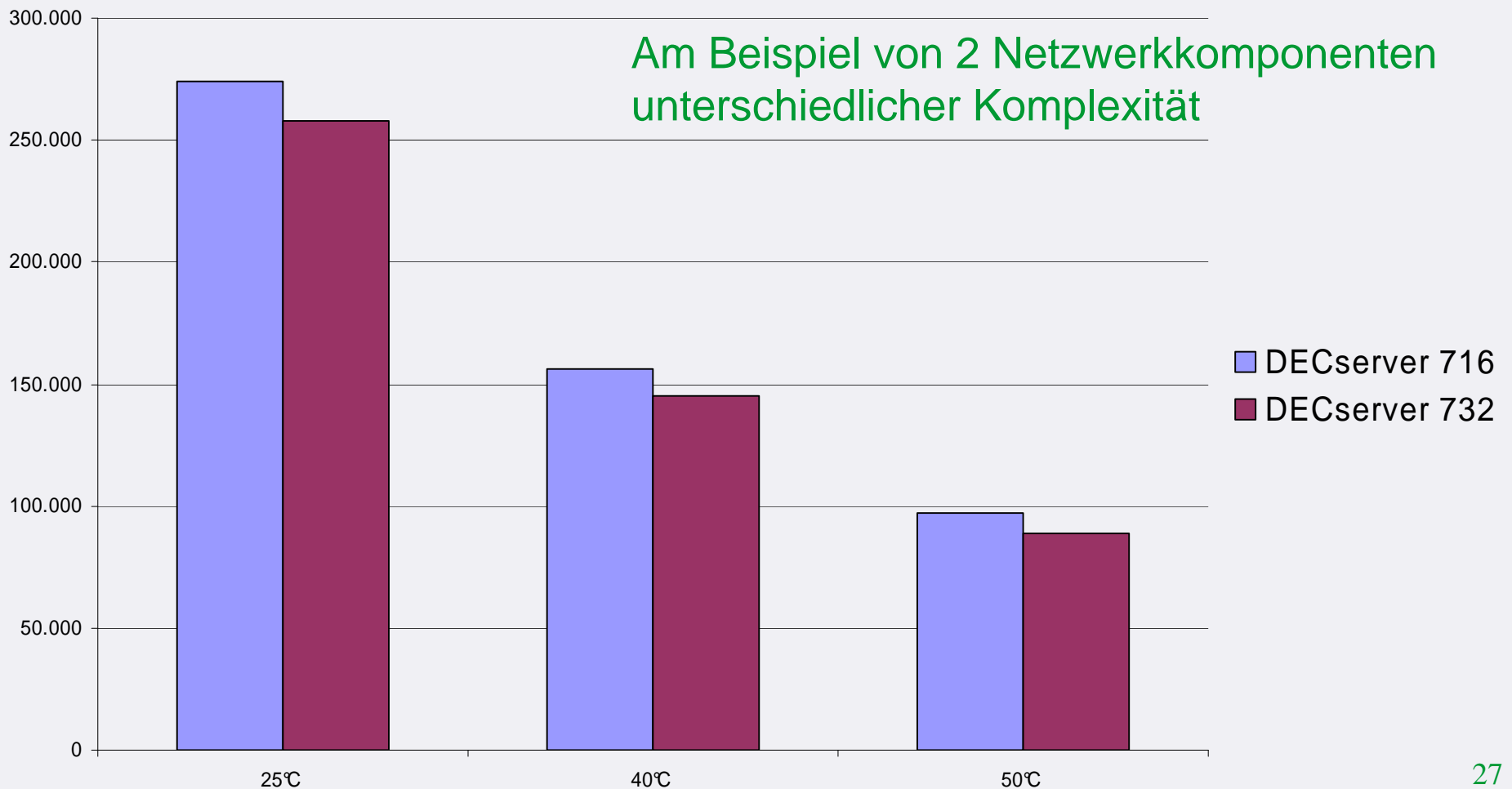
Nie kalt einschalten!

Möglichst keine häufigen größeren Temperatur- und/oder Feuchtezyklen!!!

IBH Klimatisierung 2

Klimatisierung und MTBF

MTBF in h



IBH Klimatisierung 3

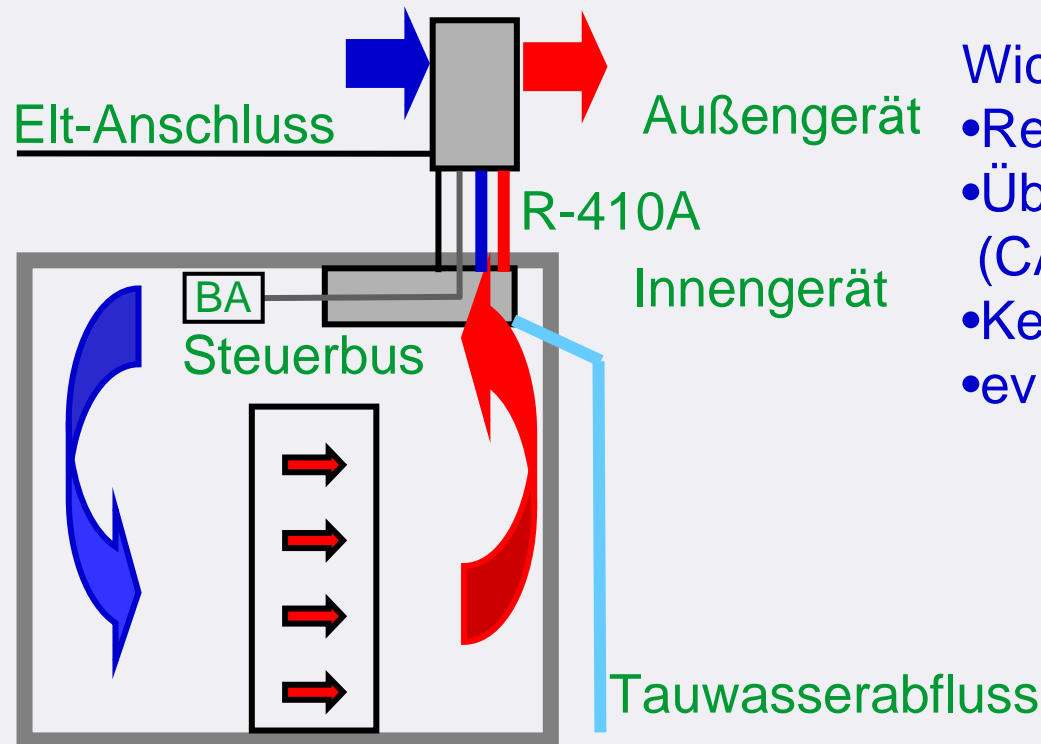
Klimatisierung und Kosten

- ◆ Jedes elektrische Gerät gibt eine bestimmte Wärmemenge ab, die in der Elektronik der aufgenommenen Energie entspricht
- ◆ BTU – British Thermal Unit, Einheit der Wärmeenergie:
1 BTU = 0,293 Wh
(Eine BTU ist definiert als die Energie, die man benötigt, ein Pfund Wasser um ein Grad Fahrenheit zu erwärmen.)
- ◆ Jede Klimaanlage benötigt Energie, um die Wärme zu "entsorgen"
- ◆ Entscheidend ist der EER (Energy Efficiency Ratio):
$$\text{EER} = E_w / E_c$$
- ◆ Je höher der EER, um so günstiger die Klimaanlage
- ◆ Üblich ist ein EER=2,5-3,5

IBH Klimatisierung 4

Klimaanlagen

- ◆ Split-Geräte haben den günstigsten EER
- ◆ Das Kältemittel R-410A ist umweltfreundlicher und kann mehr Wärme entsorgen als ältere (R-22, R-407)



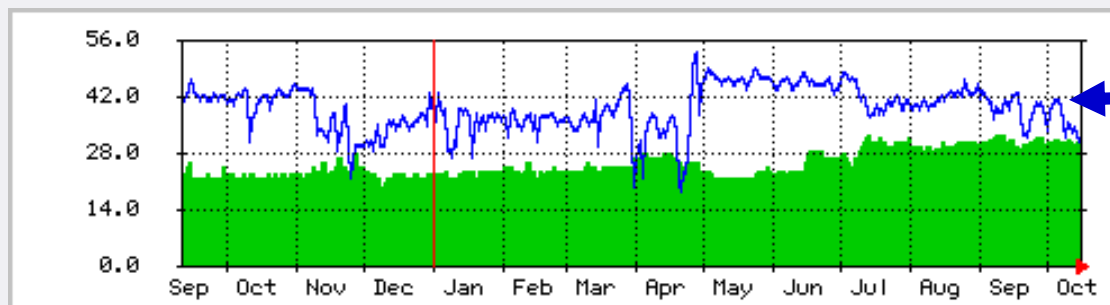
Wichtig:

- Redundante Klimaanlagen
- Überwachung der Klimaanlagen (CAN-Bus)
- Kein Anschluß an USV
- ev. Anschluß an Dieselaggregat

IBH Klimatisierung 5

Luftfeuchte

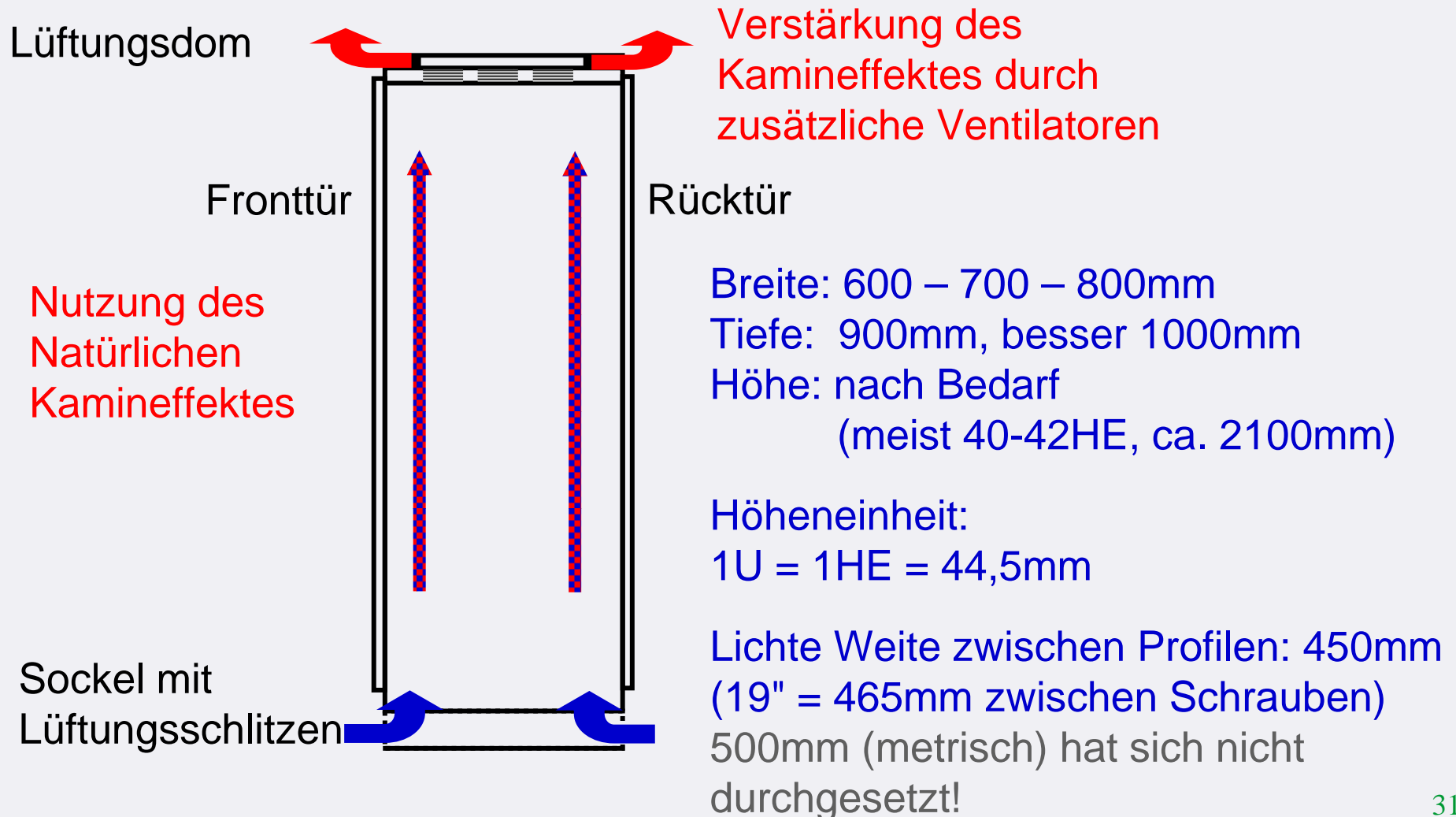
- ◆ Jede Klimaanlage (R-410A) entfeuchtet automatisch die Luft → 45-55%
→ **Befeuchtung nicht erforderlich**
- ◆ Der Sommer mit relativ hohen Luftfeuchten ist daher unproblematisch
- ◆ Im Winter, vor allem bei extremer Kälte (-25°C – -15 °C), herrscht eine trockene Luft vor, die nur wenig Feuchte binden kann. Bei Erwärmung reduziert sich die relative Luftfeuchte auf unter 10%
→ **folglich im Winter möglichst wenig lüften.**



Blaue Kurve:
relative Luftfeuchte
Einbrüche durch
starkes Lüften

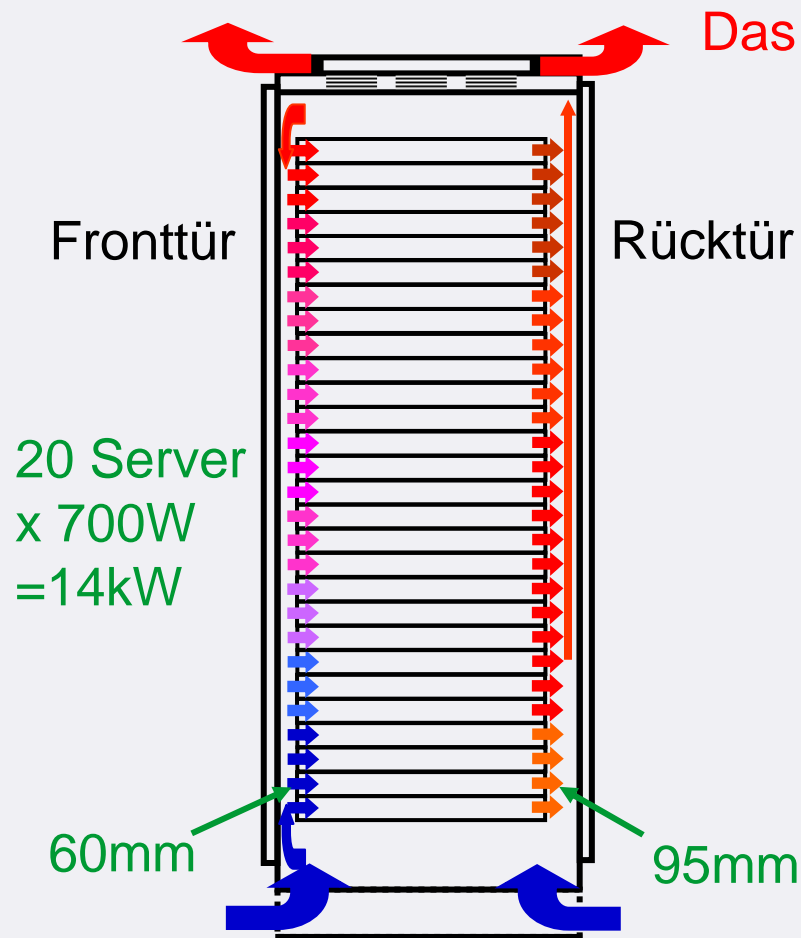
IBH Severräume/Serverschränke 1

Belüftung der Netzwerk-/Serverschränke



I B H Severräume/Serverschränke 2

Das Problem der Belüftung der Serverschränke



Das Schaffen keine Ventilatoren !!!

Lösungen:

1. Gestelzter Fußboden und Einblasen der kalten Luft von unten, zusätzlich Schränke mit einer Tiefe von 1000mm
2. Front- und Rücktüren entfernen, aufstellen der nackten Alu-Profile! Diesen Weg geht auch die Fa.Lampertz mit ihrer zertifizierten Rechnerraumzelle.
3. Kombination von 1. und 2.

Bautiefe der Server: 745mm (Industriestandard)

I B H USV-Anlagen 1

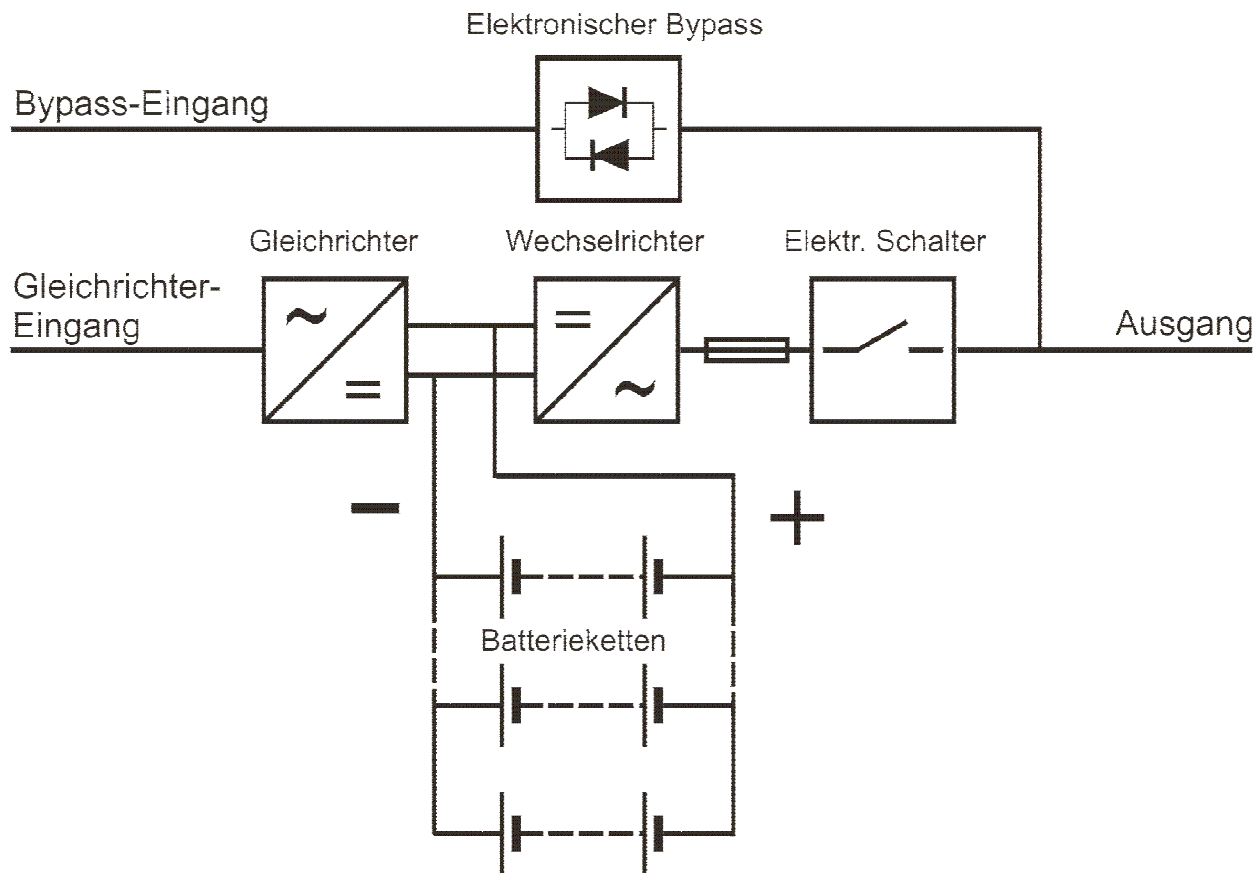
Wogegen schützen VFI-USV?

Der Spannungsschutz konzentriert sich auf folgende Spannungsprobleme:

- ◆ Stromausfall
- ◆ Spannungseinbrüche
- ◆ Überspannung
- ◆ Kurzschluß im öffentlichen Netz
- ◆ Störspannungen im Netz
- ◆ Hochspannungsspitzen
- ◆ Frequenzabweichungen
- ◆ Schaltspitzen
- ◆ harmonische Oberwellen

IBH USV-Anlagen 2

Aufbau einer VFI-USV



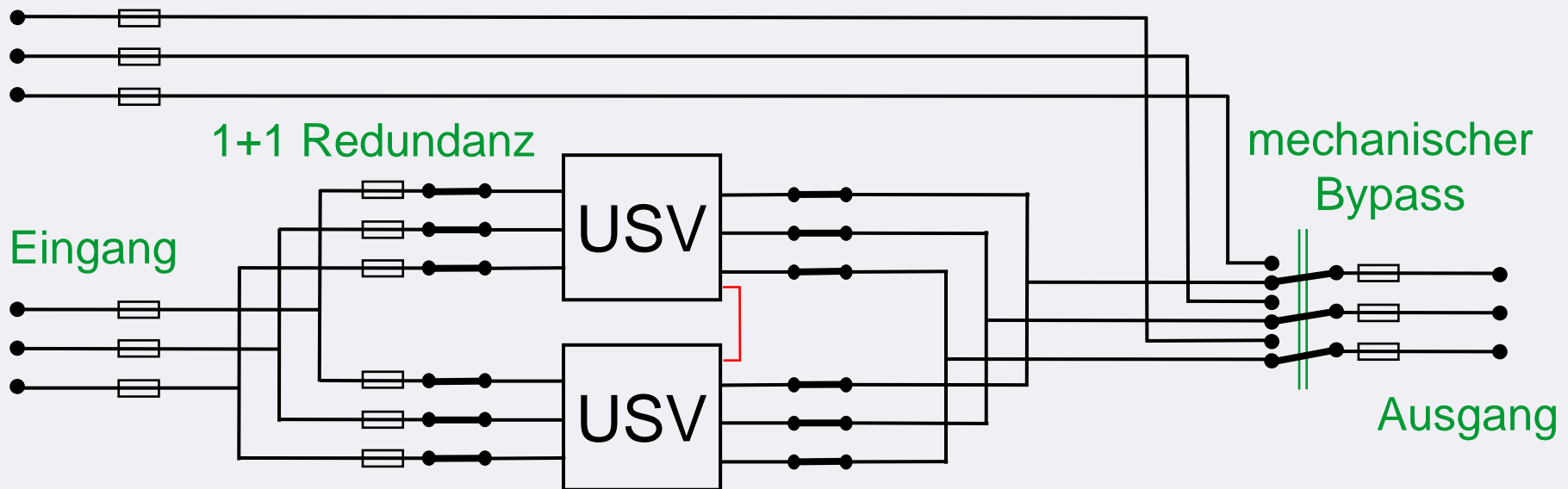
Wichtige Parameter:
Eingangs- und
Ausgangsleistungs-
faktor

Lebensdauer der
Batterien:
> 10 Jahre
nach EuroBAT
Nur bei optimaler
Temperatur 20°C
und ABM

Wirkungsgrad der
USV: 92%-94%
Wieviel
Elektroenergie
wird in Wärme
umgesetzt?

IBH USV-Anlagen 3

Ausfallsredundanz durch Hot-Sync



Verfügbarkeit einer USV:

$n = 99,5\% \rightarrow 43,8\text{h Ausfall/h}$

Parallelschaltung von 2 USV-Anlagen:

$n_a = 1 - (1 - n) \cdot (1 - n) = 99,9975\% \rightarrow 0,22\text{h Ausfall/h}$

Beispiel:

Eaton 9390, 60kVA

Ausgangsleistung:

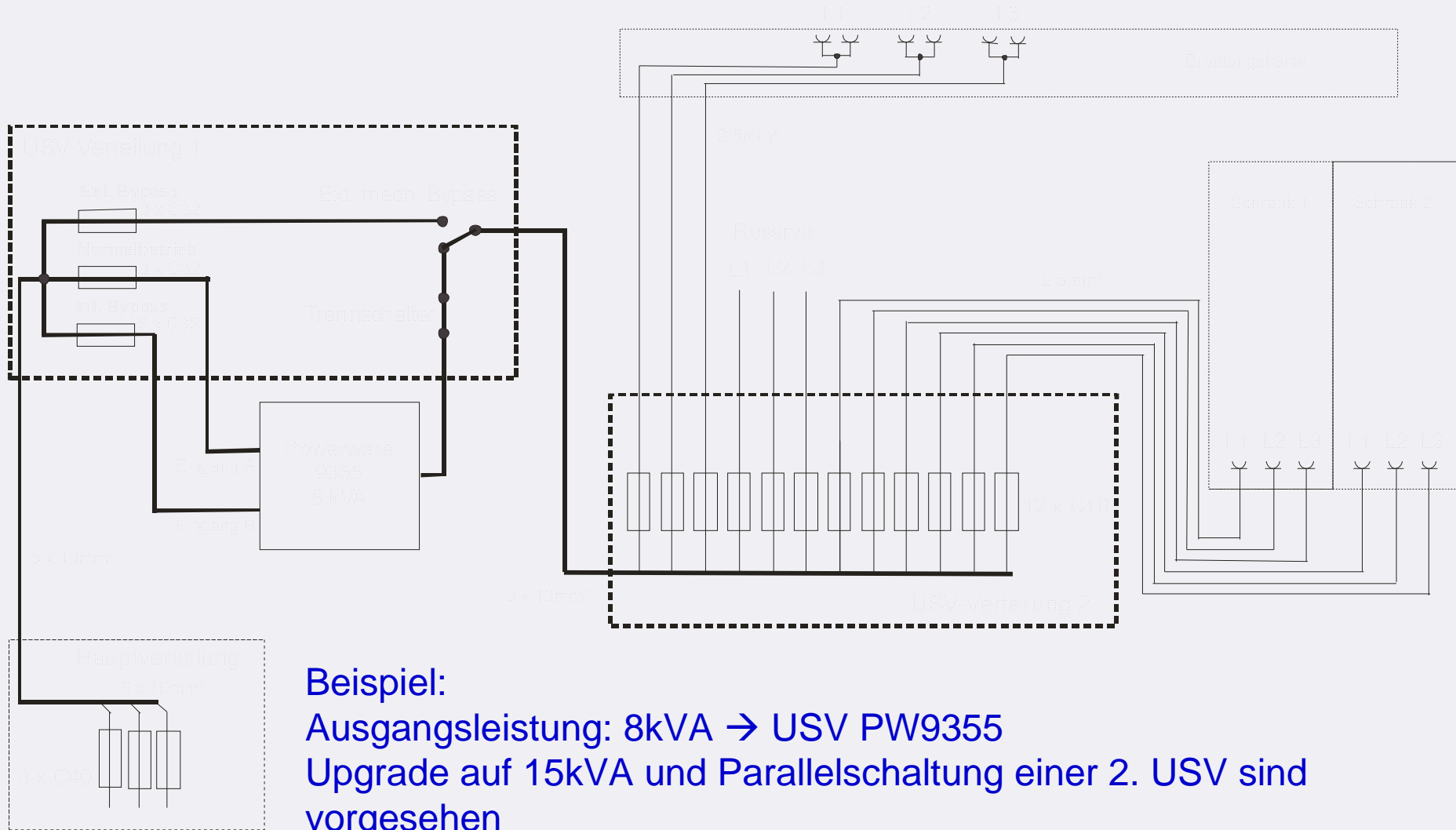
60kVA, 54kW

im Redundanzmodus

Sicherungen: 130A

IBH USV-Anlagen 4

Ortsfester USV-Anschluß



Beispiel:
Ausgangsleistung: 8kVA → USV PW9355
Upgrade auf 15kVA und Parallelschaltung einer 2. USV sind
vorgesehen

IBH USV-Anlagen 5

Überwachung der Elt-Verteilung im Rack mit Eaton ePDU



- ◆ messende ePDU
Ablezen der aktuellen Stromstärke



- ◆ überwachbare ePDU
Einlesen der aktuellen Stromstärke
per TCP/IP



- ◆ steuerbare ePDU
Einlesen von Stromstärke und Spannung je
Steckdose
Einzelschaltung je Steckdose
Messung von Temperatur und Luftfeuchte

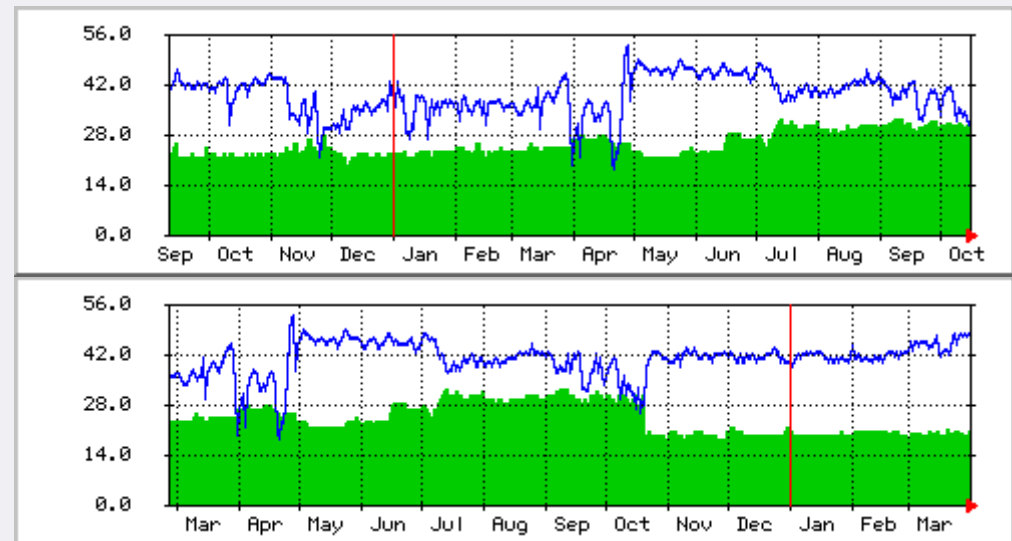


IBH Überwachung der Infrastruktur

Stromversorgung und Umwelt haben einen erheblichen Einfluß auf die Verfügbarkeit

◆ Überwachung der aller erforderlichen Parameter

- Zutrittskontrolle zu Server- und Netzwerkräumen
- Kontrolle der Primärphasen
- Kontrolle der USV
- Kontrolle der Klimatechnik
- Kontrolle von Temperatur und Luftfeuchte
- Kontrolle der Server- und Speichersysteme



◆ Bei Verletzung der eingestellten Grenzwerte:

- Verschicken von E-Mails
- Versenden von SMS in kritischen Fällen
- Alarmierung des Personals (akustisch/optisch) während der Arbeitszeit

Bing!

Vielen Dank!



**Fragen Sie!
Wir antworten.**