Das Thema im Überblick

Von Telekommunikationsnetzen wird eine nahezu uneingeschränkte Verfügbarkeit erwartet. Um die dafür nötige Netzqualität sicherzustellen, müssen Netzbetreiber ein breites Spektrum von Maßnahmen ergreifen, die jeweils aufeinander abgestimmt und koordiniert werden müssen. Dies erfordert über alle Phasen, von der Konzeption bis zum täglichen Betrieb, eine lückenlose Qualitätssicherung. Mit einem durchgängigen betrieblichen Netzmanagement muss der Netzbetreiber auf alle möglichen Störfälle vorbereitet sein, um schnell und angemessen reagieren zu können.

Ausfallsicherheit von Telekommunikationsnetzen

Immer mehr geschäftskritische Anwendungen setzen eine hoch verfügbare Datenverbindung voraus. Für den Privatkunden ist es selbstverständlich, dass der Zugang zum Internet oder der Telefonanschluss rund um die Uhr an 365 Tagen im Jahr zur Verfügung steht. Der Einsatz von Datendiensten und besonders der Zugriff auf das Internet sind aus unserem täglichen Leben nicht mehr wegzudenken und haben mittlerweile das Telefon als wichtigstes Telekommunikationsmittel ersetzt. Dementsprechend hoch sind die Qualitätsanforderungen.

Die Autoren

Dipl.-Ing. Stefanus Römer ist als Projektleiter in der zentralen Netzplanung bei T-Mobile Deutschland tätig.

Dipl.-Ing. (FH) Matthias Peitzsch ist in der zentralen Netzplanung bei T-Mobile Deutschland tätig.

1 Einführung

Die meisten Internetnutzer setzen inzwischen eine quasi-permanente und unterbrechungsfreie Internetverbindung voraus, obwohl dies in der Anfangszeit der kommerziellen Nutzung des Internets keinesfalls immer so war. Noch vor wenigen Jahren wurde die Eignung des Internets für geschäftskritische Anwendungen oder für die Übertragung von Sprache oder Video von den Fachleuten infrage gestellt. Heute ist es eine Selbstverständlichkeit, dass das Internet zunehmend alle anderen klassischen Übertragungsnetze verdrängt und auch für kritische Applikationen genutzt wird. Die Internet-Technologie ist inzwischen die bedeutendste Übertragungstechnik in der Telekommunikationsindustrie. Internet-Access-Provider investieren daher erhebliche Mittel in die Ausfallsicherheit (Redundanz) ihrer Netze.

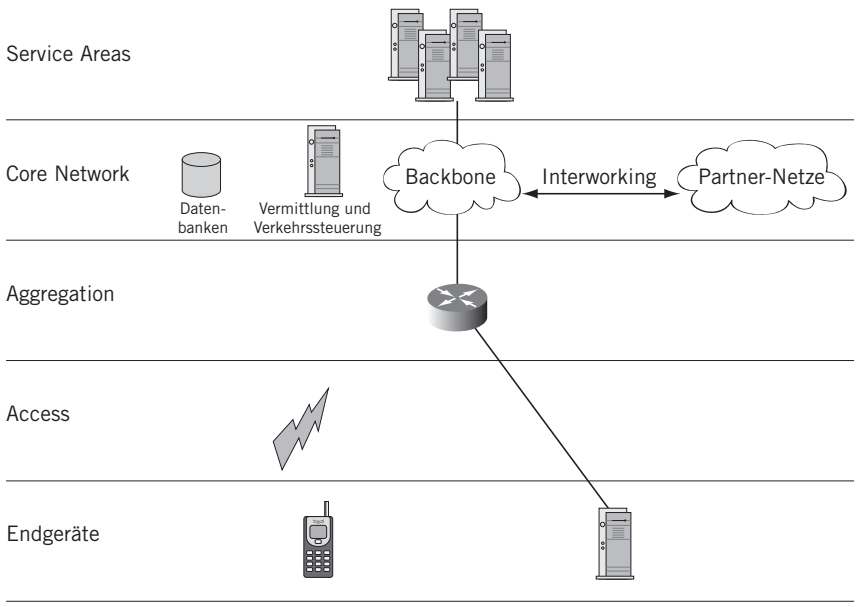
2 Elemente und schematischer Aufbau von Telekommunikationsnetzen

Ein Internetzugangsnetz besteht im Allgemeinen aus einer Teilnehmerzugangsleitung (last mile) und aus einer zentralen Vermittlungsplattform mit verschiedenen geografisch verteilten Vermittlungsrechnern (Routern). Die Teilnehmerzugangsleitung ist in der Regel nur einfach, d. h. ohne zusätzliche Ausfallsicherheit (z. B. über eine Zusatzleitung mit getrennter Wegeführung oder über einen separaten Mobilfunkanschluss), ausgeführt. Die zentralen Vermittlungsrechner hingegen sind höchst kritisch für die Gesamtverfügbarkeit der unterschiedlichen Dienste, weil über sie der Zugangsdienst für alle Nutzer erbracht wird. Sie werden daher mit einer Vielzahl von Redundanz-Maßnahmen gegen einen möglichen Ausfall gesichert.

Moderne Telekommunikationsnetze, so genannte NGNs (Next Generation Network), sind hochkomplexe, weltumspannende Multivendor-Systeme[1], die nur mit einem hohen Aufwand an Überwachungs- und Steuerungstechnik sowie entsprechend geschultem Personal zu betreiben sind. Eine Betriebsüberwachung und -steuerung – nachfolgend Betrieb oder Netzmanagement genannt – solcher Netze ist stark automatisiert und steht an 365 Tagen rund um die Uhr zur Verfügung. Ein Next Generation Network zeichnet sich im Gegensatz zu früheren monolithisch aufgebauten Telekommunikationsnetzen dadurch aus, dass über ein gemeinsames zentrales Transportnetz (Backbone) verschiedene IP-basierte Dienste (Service Areas) über unterschiedliche Zugangsnetze (Access Networks) bereitgestellt werden können. Ein NGN besteht im Allgemeinen aus folgenden Bereichen (Bild 1):

- den Endgeräten, die die verschiedenen Dienste anfordern und in Anspruch nehmen
- dem Bereich der Zugangsnetze (Access), bestehend aus dem Teilnehmerzugangsbereich (z. B. eine drahtgebundene Anschlussleitung oder eine Funkschnittstelle wie beispielsweise UMTS [Universal Mobile Telecommunications Systems]) und dem Bereich der regionalen Verkehrskonzentratoren (Aggregation)
- dem zentralen Kernnetz (Core Network), bestehend aus einer dienst- und zugangsunabhängigen Transportplattform (Backbone), Vermittlungs- und Verkehrssteuerungselementen und den Netzübergängen (Gateways) zu anderen Netzen
- den zentralen Datenbanken zur Teilnehmerverwaltung und Identitätsmanagement (z. B. Authentisierung und/oder Autorisierung)
- dem Bereich der Diensterbringung (Service Areas)
- der Netzsteuerung, bestehend aus herstellerabhängigen Elementmanagement und einem zentralen Netzmanagementsystem, die eine Gesamtsicht über verschiedene Komponenten oder sogar das Gesamtnetz ermöglicht.

Bild 1 **Schematisches Modell eines NGN**



NGN Next Generation Network

Tabelle **Übersicht der Verfügbarkeit**

Prozentsatz	durchschnittliche nicht verfügbare Zeit
90,000000%	876 Std. = 36 Tage, 12 Std.
98,500000%	131,5 Std. = 5 Tage, 11 Std., 30 Min.
99,000000%	87,6 Std. = 3 Tage, 15 Std., 36 Min.
99,900000%	8,76 Std. = 8 Std., 45 Min., 36 Sek.
99,970000%	2,628 Std. = 2.Std.,37 Min., 41 Sek.
99,990000%	0,876 Std. = 52 Min., 33,6 Sek.
99,999000%	0,0876 Std. = 5 Min., 15,36 Sek.
99,999900%	0,00876 Std. = 31,54 Sek.
99,999990%	0,000876 Std. = 3,15 Sek.
99,999999%	0,0000876 Std. = 0,32 Sek.

Jeder dieser Teilbereiche besteht aus einer Vielzahl verschiedener Technologien, die von verschiedenen Herstellern bereitgestellt werden können. Beispielsweise werden in der Regel verschiedene drahtgebundene oder drahtlose Zugangstechniken sowie verschiedene Dienste (z. B. Sprachübertragung, Messaging oder Internetzugang) in einem NGN integriert.

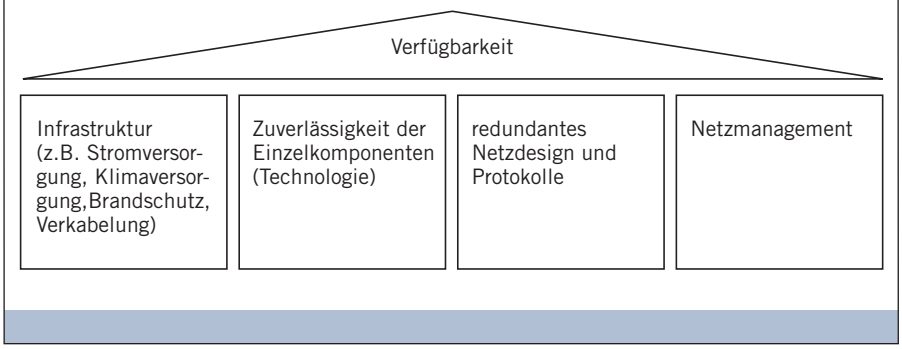
3 Grundlagen der Ausfallsicherheit

Die Verfügbarkeit eines Telekommunikationsdienstes ist definiert als Verhältnis der tatsächlichen Betriebszeit zur planmäßigen Betriebszeit innerhalb eines Betrachtungszeitraums. Die planmäßige Betriebszeit ist gleich der Gesamtzeit des Betrachtungszeitraums verringert um die geplanten Wartungsarbeiten innerhalb eines vereinbarten Wartungsfensters, die eine Unterbrechung der Diensterbringung notwendig machen. Die tatsächliche Betriebszeit ergibt sich als Differenz der planmäßigen Betriebszeit und der summierten Ausfallzeit auf Grund unvorhergesehener Störungen.

$$V = \frac{\text{tatsächliche Betriebszeit}}{\text{Betrachtungszeitraum} - \text{geplante Wartungszeiten mit Unterbrechungen}}$$

[1] **Multivendor-System:** Verbindung von Hardware und Software verschiedener Hersteller in einem Netzwerk.

Bild 2 **Säulen der Verfügbarkeit**



Üblicherweise wird als Betrachtungszeitraum eine Dauer von einem Jahr zugrunde gelegt. Je seltener eine Störung auftritt und je kürzer die Ausfallzeit auf Grund einer Störung ist, desto höher ist die Verfügbarkeit. So ergibt sich beispielsweise bei einer geforderten Verfügbarkeit von 99,9 Prozent für den Betrachtungszeitraum von einem Jahr eine maximale Ausfallzeit von nur 8,76 Stunden (Tabelle).

Eine Erhöhung der Ausfallsicherheit geht stets mit dem Bereithalten ungenutzter Systemressourcen (Redundanzen) einher. Ein Beispiel hierfür sind Ersatzteile in einem Lager, aber auch Netzkomponenten, die bereits voll installiert und betriebsbereit sind und im Falle einer Störung lediglich aktiviert oder stärker ausgelastet werden. Im ersten Fall spricht man von Cold-Stand-by- und im letzteren von Hot-Stand-by-Komponenten. Wie viele Systemressourcen an welcher Stelle des Gesamtsystems mehrfach vorgehalten werden müssen, ergeben sich aus den Anforderungen an die Verfügbarkeit, der Zuverlässigkeit der Einzelkomponenten und aus den gewählten Redundanzverfahren.

Sofern nur sehr kleine Ausfallzeiten toleriert werden können, kommen in der Regel nur Verfahren in Frage, die einen Störfall automatisch erkennen und durch automatische Umschaltung auf entsprechende redundante Systemkomponenten mit minimaler Unterbrechungszeit beheben. Während der Dienst nach einer automatischen Umschaltung ungestört über die redundanten Systemkomponenten weiterläuft, kann die gestörte primäre Systemkomponente ohne weitere Service-Beeinträchtigungen im Rahmen des Problemmanagements repariert werden.

Ausgangspunkt für ein hoch verfügbares Telekommunikationsnetz ist eine sorgfältige Netzplanung, die die einzelnen Verfügbarkeitsanforderungen berücksichtigt und die notwendigen Redundanzverfahren im Netzdesign von Beginn an vorsieht. Ein Telekommunikationsnetz ist jedoch kein starres System, das einmalig geplant und aufgebaut wird, sondern es unterliegt ständigen Anpassungen. Einerseits ändert sich dauernd das Nutzerverhalten, andererseits werden fortwährend neue Dienste eingeführt. Diese Einflüsse führen zu wesentlichen Veränderungen der Verkehrsbeziehungen und der Auslastung der verfügbaren Systemressourcen (z. B. Übertragungswege, CPU-Last [Central Processing Unit] oder Speicher). Um dauerhaft eine hohe Verfügbarkeit gewährleisten zu können, müssen kritische Systemressourcen regelmäßig überprüft und potenzielle Kapazitätsengpässe durch einen bedarfsgerechten und rechtzeitigen Kapazitätsausbau vermieden werden.

Die Verfügbarkeit eines Telekommunikationsnetzes hängt von einer Vielzahl verschiedener Einflussgrößen ab. Bild 2 zeigt einen Überblick über die verschiedenen Einflussgrößen:

- Infrastruktur,
- Zuverlässigkeit der Einzelkomponenten
- redundantes Netzdesign und
- Netzmanagement.

Zum Bereich der Infrastruktur zählen alle Komponenten, die unabhängig von der jeweiligen Systemtechnik für den Betrieb von Telekommunikationsanlagen benötigt werden. Hierzu gehören unter anderem Gebäude, Stromversorgung, Klimatechnik oder Verkabelung. Die Zuverlässigkeit der Infrastruktur ist die Grundlage für den Betrieb hoch verfügbarer Telekommunikationsnetze.

Eine weitere Voraussetzung ist die Verfügbarkeit der einzelnen Netzkomponenten und die Zuverlässigkeit der Übertragungswege zwischen den Einzelkomponenten. Ein Netzbetreiber muss zum einen darauf achten, dass nur qualitativ hochwertige Anlagen mit einer hohen Komponentenzuverlässigkeit in seinem Netz installiert werden und diese Komponenten über redundante Verkehrswege miteinander verbunden werden (präventive Maßnahmen). Hierzu zählt beispielsweise, dass er nach Möglichkeit nur Netzelemente integriert, die sich bereits im Betrieb bewährt haben und die vor Inbetriebnahme im Testlabor ausgiebig getestet wurden. Zum anderen muss ein Netzbetreiber durch Vorhalten entsprechender Ersatzanlagen (Redundanzen) und durch ein redundantes Netzdesign im Falle einer Störung möglichst automatisch auf entsprechende Ersatzanlagen und/oder Ersatzwege umschalten können, um die Ausfallzeit aus Sicht der Nutzer zu minimieren.

Darüber hinausgehende Störungen, für die keine automatischen Redundanzlösungen vorhanden sind, müssen manuell durch das Betriebspersonal beseitigt werden (reaktive Maßnahmen). Hierzu wird über alle Betriebsbereiche hinweg eine effiziente und kohärente[2] Betriebsorganisation benötigt (Netzmanagement).

Nachfolgend werden die wichtigsten Voraussetzungen und Konzepte beschrieben, die notwendig sind, um einen hoch verfügbaren Netzbetrieb zu ermöglichen.

3.1 Infrastruktur

Die Gewährleistung eines störungsfreien Betriebs von Telekommunikationsnetzen be-

[2] **kohärent:** zusammenhängend.

ginnt mit den lokalen Sicherungs- und Qualitätsmaßnahmen vor Ort in der jeweiligen Betriebsstätte (Infrastruktur). Die Betriebsstätte muss vor allem dauerhaft und stabil die notwendigen Anforderungen bezüglich Stromversorgung und Klimabedingungen erfüllen. Zu den Sicherungsmaßnahmen der Infrastruktur gehören im Einzelnen:

- doppelte Stromversorgung über getrennte Energieversorgungssysteme
- Notstromaggregate, Über-/Unterspannungsschutz und Schutz vor Frequenzschwankungen
- doppelte Klimaanlage, um die Betriebstemperatur der Anlagen im zulässigen Bereich zu halten
- thermische Brandfrüherkennungssysteme mit zentraler Alarmierung
- getrennte Brandabschnitte für jeweils wechselseitig redundante Netzkomponenten
- Zugangskontrolle und Objektschutz

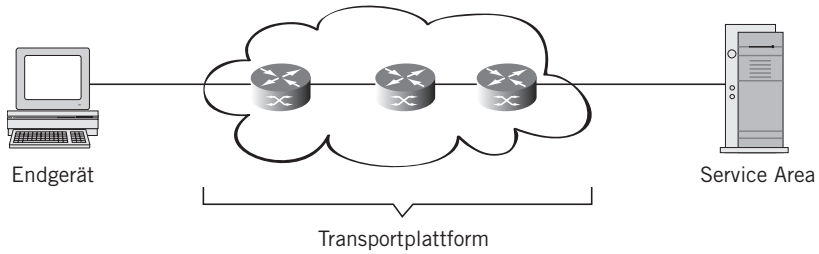
3.2 Zuverlässigkeit der Einzelkomponenten

Eine weitere Säule der Verfügbarkeit ist die Zuverlässigkeit der Einzelkomponenten. Ein zuverlässiger Betrieb der Einzelkomponenten setzt einerseits eine hochwertige und ausfallsichere Infrastruktur voraus, andererseits wird die Verfügbarkeit der Einzelkomponenten durch ihre interne Beschaffenheit bestimmt. In den Datenblättern der Hersteller findet man häufig den Wert MTBF (Mean Time Between Failure), der als durchschnittliche Zeit zwischen zwei Ausfällen unter idealen Betriebsbedingungen (Infrastruktur) definiert ist. Zusammen mit dem Parameter MTTR (Mean Time To Repair), der im Rahmen eines Servicevertrages mit dem jeweiligen Hersteller zu vereinbaren ist, ergibt sich die Komponentenverfügbarkeit wie folgt:

$$V_{Einzelkomponenten} = \frac{MTBF}{MTBF + MTTR}$$

Bild 3 zeigt ein einfaches Modell eines Telekommunikationssystems, bestehend aus einer Kette von hintereinander geschalteten Einzelkomponenten zwischen Service Area und Endgerät. Der Dienst steht in diesem Modell nur zur Verfügung, wenn alle Einzelkomponenten und alle Übertragungswege funktionsbereit sind. Die Dienstverfügbarkeit des Gesamtsystems ergibt sich demnach als Produkt der Einzelverfügbarkeiten und ist in diesem Modell wesentlich geringer als die Verfügbarkeit jeder Einzelkomponente.

Bild 3 Transportplattform mit hintereinander geschalteten Einzelkomponenten



Von entscheidender Bedeutung bei der Beschaffung und der Integration neuer Netzelemente ist daher die sorgfältige Auswahl des jeweiligen Herstellers. Bevor eine neue Netzkomponente in einem Telekommunikationsnetz integriert werden kann, muss sie zuvor umfassend getestet werden. Testen gehört zu den präventiven Maßnahmen, um Störereignisse von vornherein zu vermeiden.

Zunächst wird die Komponente mit Hilfe von Schnittstellensimulatoren isoliert auf korrekte Funktionsweise getestet. Dabei wird, vereinfacht ausgedrückt, das „Klemmenverhalten“ als Blackbox anhand der funktionalen Spezifikation überprüft. Die Komponente muss auf bestimmte Protokollnachrichten an den Eingangsschnittstellen auf eine protokollkonforme Weise mit entsprechenden Nachrichten an den Ausgangsschnittstellen reagieren. Danach folgen Lasttests, bei denen überprüft wird, wie die Komponente auf eine Vielzahl von Protokollbeziehungen reagiert und ob die angegebenen Lastgrenzen (beispielsweise Durchsatz oder Anzahl gleichzeitiger paralleler Verbindungen) eingehalten werden. Ein weiterer Schritt ist der Verbundtest mit anderen Netzelementen, mit denen die Komponente direkt über bestimmte Protokolle zusammenarbeiten muss. Im Redundanztest wird in einem zusätzlichen Schritt das redundante Netzdesign überprüft. Dabei kommt es darauf an, dass bei einer Unterbrechung von Verbindungsleitungen oder einer Deaktivierung von Ports auf einen alternativen Übertragungsweg umgeschaltet wird.

Bevor die Komponenten uneingeschränkt im „Live“-Netz genutzt werden können, werden sie zunächst in einem Pilottest für eine eingeschränkte Nutzerzahl unter einer höheren Last und über einen längeren Zeitraum erprobt. In allen diesen genannten Testphasen können kritische Fehler auftreten, die analysiert und behoben werden müssen, bevor die nächste Phase beginnen kann.

3.3 Redundantes Netzdesign und Protokoll

Die Verfügbarkeit eines Telekommunikationsnetzes lässt sich nur durch die Einbeziehung zusätzlicher ungenutzter Systemressourcen (Redundanzen) erhöhen.

In Bild 3 ist ein einfaches Modell eines Telekommunikationsnetzes mit hintereinandergeschalteten Einzelkomponenten dargestellt. Die Dienstverfügbarkeit des Gesamtsystems ist in diesem Beispiel, wie bereits erwähnt, wesentlich geringer als die Verfügbarkeit jeder Einzelkomponente. In der Praxis ist ein derartiges Netzdesign nicht akzeptabel, weil es die hohen Verfügbarkeitsanforderungen, die an ein Telekommunikationsnetz gestellt werden, nicht erfüllen kann. Jede einzelne Komponente bildet hier einen so genannten SPOF (Single Point of Failure). Der Ausfall einer Komponente oder deren Anbindung würde den Gesamtausfall des kompletten Netzes (und damit des Dienstes) herbeifüh-

Bild 4 Transportplattform mit zusätzlichen Redundanzen

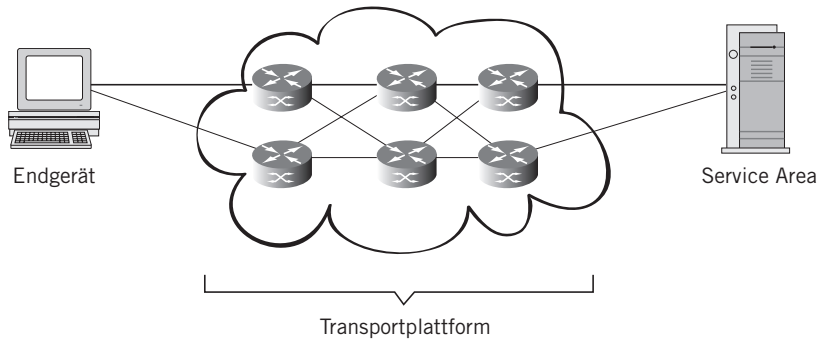
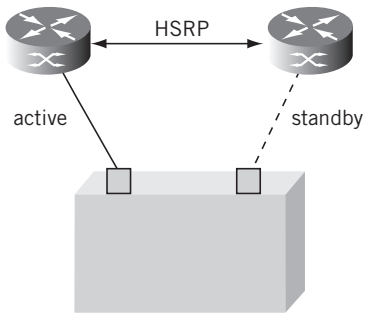
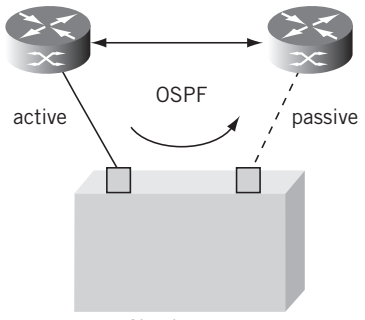


Bild 5 Active-Stand-by-Redundanz mit HSRP



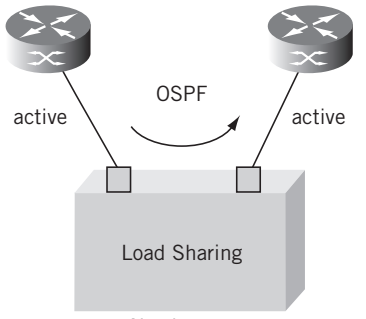
HSRP Hot Stand-by Routing Protocol

Bild 6 Active-Passive-Redundanz mit dynamischen Routing



OSPF Open Shortest Path First

Bild 7 Active-Active-Redundanz mit dynamischen Routing (Load Sharing)



OSPF Open Shortest Path First

ren. Durch zusätzliche Redundanzen (Bild 4) kann erreicht werden, dass die Dienstverfügbarkeit höher ist als die Verfügbarkeit jeder Einzelkomponente. Dabei wird jede Einzelkomponente jeweils über einen Primärweg und einen Ersatzweg an das übrige Netz angeschlossen. Um die Umschaltung zwischen Primär- und Ersatzweg vorzunehmen, ist der Einsatz bestimmter Protokolle nötig. Hierzu gibt es folgende Konzepte:

- active/stand-by (Bild 5): Die aktive Verbindung trägt 100 Prozent der Last. Sofern die aktive Verbindung ausfällt, wird die andere Verbindung aktiv und übernimmt die gesamte Last. Das Umschalten wird mit Hilfe eines Redundanzprotokolls vorgenommen, wie beispielsweise HSRP (Hot Stand-by Routing Protocol) oder VRRP (Virtual Router Redundancy Protocol).
- active/passive (Bild 6): Zwei getrennte Wege mit unterschiedlicher Routing-Gewichtung. Die aktive Verbindung trägt 100 Prozent der Last. Sofern die aktive Verbindung ausfällt, wird die andere Verbindung aktiv und übernimmt 100 Prozent der Last. Das „Umschalten“ wird mit Hilfe eines dynamischen Routing-Protokolls vorgenommen, wie beispielsweise OSPF (Open Shortest Path First).
- active/active (Bild 7): Load Sharing (Lastverteilung) über zwei gleichzeitig aktive Verbindungen, die jeweils maximal bis zu 50 Prozent ausgelastet werden sollten. Sofern eine Verbindung ausfällt, übernimmt die andere Verbindung die gesamte Last. Das Umschalten wird mit Hilfe eines dynamischen Routing-Protokolls (z. B. OSPF) vorgenommen.

Weitere Konzepte zur Erhöhung der Verfügbarkeit sind

- Baugruppen-Redundanz: Hierbei sind Baugruppen (z. B. Prozessorkarten) in Netzkomponenten doppelt (als aktiv und/oder Stand-by) vorhanden und über einen internen Systembus miteinander verbunden. Sollte die aktive Baugruppe ausfallen, übernimmt die Stand-by-Baugruppe die gleiche Funktion (Switch over).
- Knoten-Redundanz (als Cold-Stand-by-Komponente oder Hot-Stand-by-Komponente) an getrennten Standorten oder am selben Standort in getrennten Brandabschnitten: Sollte eine aktive Netzkomponente vollständig ausfallen, so übernimmt eine Redundanz-Komponente deren Funktion.

3.4 Netzmanagement

Das Ziel eines effizienten Netzmanagements ist es, durch reaktive Maßnahmen die Ausfallzeit jedes einzelnen Störereignisses zu minimieren. Um dies zu ermöglichen, ist es notwendig, alle denkbaren Störereignisse von vornherein zu erfassen, zu kategorisieren und zu priorisieren. Störereignisse müssen möglichst schnell (d. h. automatisch) erkannt und einer Bearbeitung zugeführt werden. Jedes Störereignis löst abhängig von seiner Priorität in jeder einzelnen Phase vordefinierte Teilprozesse aus, die genau festlegen, wer welche Maßnahmen zu ergreifen hat und wer nach welcher Zeit zu informieren ist. Störungskategorien werden im Allgemeinen anhand der Störungswirkbreite definiert. Die Störungswirkbreite einer Störung gibt beispielsweise an, wie viele Kunden von einer Störung betroffen sind oder wie

viel Umsatz pro Zeiteinheit durch eine Störung verloren geht oder wie viele Kosten durch eine Störung entstehen. Je höher die Störungswirkbreite einer Störung, desto höher ihre Priorität. Je höher die Priorität eines Störereignisses, desto höher der notwendige Automatisierungsgrad zur Störungsbehebung.

Ein Störereignis lässt sich in folgende Phasen unterteilen (Bild 8):

- Alarmierungszeit T_1: Die Zeit bis zur Alarmierung des Netmanagements.
- Reaktionszeit T_2: Die Zeit, die das Betriebspersonal benötigt, um auf eine Alarmierung zu reagieren.
- Analysezeit T_3: Die Zeit, die das Betriebspersonal benötigt, um die Störung zu analysieren und Entstörmaßnahmen zu beschließen.
- Entstörzeit T_4: Die Zeit bis zur Beseitigung der Störung (z. B. mit Hilfe einer Zwischenlösung).
- Reparaturzeit T_5: Die Zeit bis zur endgültigen Reparatur.

Die Ausfallzeit T_A errechnet sich demnach aus der Gleichung

$$T_A = T_1 + T_2 + T_3 + \min(T_4, T_5).$$

Um die Ausfallzeit T_A zu minimieren, ist es notwendig, jede einzelne Teilzeit zu minimieren. Dies erfordert ein effizientes und umfassendes Netzmanagement. Ein Netzmanagement unterteilt sich im Allgemeinen in sechs Funktionsbereiche (Bild 9):

- Alarm-Management: Jede Funktionsstörung oder ein Überschreiten vordefinierter Schwellwerte wird automatisch dem Betriebspersonal gemeldet, das Tag und Nacht bereitsteht, um schnellstmöglich einzugreifen und eine Störung zu beseitigen. Störereignisse sind klassifiziert und je nach Störungswirkbreite priorisiert. Das Betriebspersonal bearbeitet die Störereignisse entsprechend ihrer Priorität nach vordefinierten Entstörprozessen, die genau festlegen, wer in welcher Reihenfolge bei welchem Störereignis wie zu informieren ist und welche vordefinierten kurzfristigen Entstörmaßnahmen zu ergreifen sind. Fehlerreports ermöglichen eine genaue Fehleranalyse im Problem-Management.
- Problem-Management: Das Problem-Management beginnt nach Abschluss des Entstörprozesses. Aufgabe des Problem-Managements ist es, aufgetretene Probleme zu analysieren und eine dauerhafte Lösung zu finden. Häufig werden die unmittelbaren Auswirkungen einer Störung im Netz durch kurzfristige Umschaltmaßnahmen (workaround) auf redundante Systemkomponenten vorübergehend beseitigt, ohne die eigentliche Ursache zu beheben. Die eigentliche Störungsursache ist jedoch damit nicht beseitigt und muss im Rahmen des Problem-Managements analysiert und behoben werden. Beispielsweise kann die Fehleranalyse ergeben, dass ein Softwareproblem vorliegt, das erst mit einem speziellen Software-Patch[3] vom Hersteller zu beheben ist.
- Change-Management: Störereignisse treten häufig auf, wenn Änderungen in das Telekommunikationsnetz eingebracht werden. Aufgabe des Change-Managements ist es, die Prozedur zur Einbringung von Netzänderungen genau festzulegen und ein Monitoring der korrekten Funktionsweise nach erfolgter Einbringung zu gewährleisten. Störereignisse, die mit einer Netzänderung in Verbindung stehen, müssen unmittelbar erkannt werden. Sollten sich diese Störungen nicht innerhalb einer vordefinierten Zeit beheben lassen, so muss über eine vordefinierte Rückfallprozedur der ursprüngliche Zustand wieder hergestellt werden.
- Konfigurations-Management: Große Telekommunikationsnetze sind hochkomplexe Systeme mit vielen Parametereinstellungen auf verschiedenen Komponenten unterschiedlicher Hersteller, die aufeinander abgestimmt sein müssen. Die Aufgabe des Konfigurations-Managements ist es, jederzeit den aktuellen Konfigurationsstand im gesamten Netz

Bild 8 **Zeitreihe Störereignis**

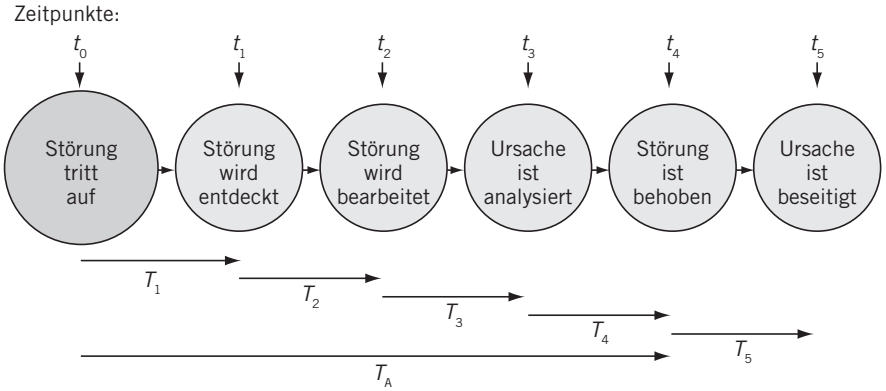
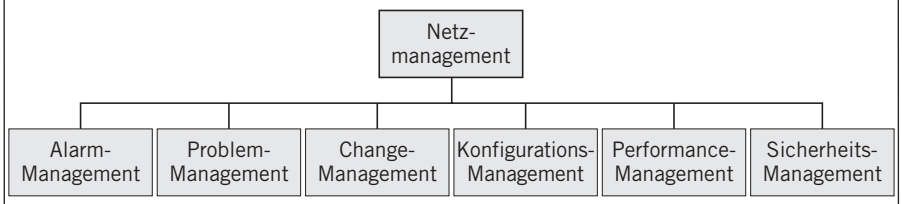


Bild 9 **Teilbereiche des Netzmanagements**



[3] Ein **Software-Patch** ist die Auslieferung einer Fehlerbehebung für ausführbare Programme und/oder Betriebssysteme und kann auch kleinere Funktionserweiterungen enthalten

Verwendete Abkürzungen

CPU	Central Processing Unit
HSRP	Hot Stand-by Routing Protocol
IP	Internet Protocol
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NGN	Next Generation Network
OSPF	Open Shortest Path First
SPOF	Single Point of Failure
UMTS	Universal Mobile Telecommunications System
VRRP	Virtual Router Redundancy Protocol

zu dokumentieren und frühere Konfigurationsstände jederzeit im Netz aktivieren zu können. Hierzu ist nicht nur die Kenntnis der einzelnen Parameter und deren Werte erforderlich, sondern es muss bekannt sein, welche Systembefehle, auf welcher Netzkomponente, in welcher Reihenfolge ausgeführt werden müssen. Eine weitere Aufgabe ist die Konfiguration von kurzfristigen Lösungen (workaround) im Falle einer Störung.

- Performance-Management: Die Aufgabe des Performance-Managements ist es, kurzfristig auftretende Kapazitätsengpässe einzelner Netzelemente zu erkennen. Kritische Systemparameter wie beispielsweise die CPU-Auslastung oder der Durchsatz auf den verschiedenen Verbindungen werden regelmäßig ausgewertet, um Engpässe oder Beeinträchtigungen zu erkennen.
- Sicherheits-Management: Der Zugang zu den Managementsystemen der Netzkomponenten muss durch Passwörter geschützt werden. Die Passwörter müssen den jeweils geltenden Richtlinien entsprechen und regelmäßig geändert werden. Eine weitere Aufgabe ist eine prozesskonforme Passwortvergabe, damit nur Berechtigte Zugriff erhalten. Weiterhin gehört der Zugangschutz zu den Gebäuden, an denen die Netzkomponenten installiert sind, zu diesem Bereich.

4 Zusammenfassung

Ein zuverlässiger Betrieb von Telekommunikationsnetzen und die Gewährleistung einer hohen Netzverfügbarkeit ist nur möglich, wenn folgende Voraussetzungen erfüllt sind:

- **Zuverlässigkeit der Einzelkomponenten:** Jedes einzelne Netzelement muss eine hohe Verfügbarkeit vorweisen. Weiterhin sollten alle Netzelemente sowohl isoliert als auch im Verbund mit anderen Netzelementen getestet werden, bevor sie im Wirknetz integriert werden.
- **Redundantes Netzdesign:** Für jede einzelne Netzkomponente entlang der gesamten Übertragungskette und deren Anbindungen sind die notwendigen Ersatzvorrichtungen (Redundanzen) vorhanden, die im Störungsfall entweder automatisch oder durch manuellen Eingriff durch das Betriebspersonal aktiviert werden.
- **Infrastruktur:** Redundante Netzkomponenten sollten an getrennten Brandabschnitten installiert werden. Für die einzelnen Standorte sind vor allem redundante Stromversorgungen und Klimaanlagen nötig.
- **Netzmanagement:** Es ist ein entsprechendes Netzmanagement mit ausreichend geschultem Personal sowie effiziente Betriebsprozesse und Werkzeuge vorhanden, um auf Störungen schnell und angemessen reagieren zu können. Ein integriertes Netzmanagement ermöglicht jederzeit sowohl eine umfassende Gesamtsicht auf das Telekommunikationsnetz als auch eine vollständige Kontrolle jeder einzelnen Komponente.

(Ar)