TECHNISCHE UNIVERSITÄT MÜNCHEN
Institut für Informatik

Diplomarbeit

Entwurf eines Modells für die Erstellung einer Verfügbarkeitsdokumentation und deren effektive Nutzung im Bereich des integrierten Netzmanagements

Bearbeiter: Rudolf Egerer
Aufgabensteller: Prof. Dr. Heinz-Gerd Hegering
Betreuer: Dr. Sebastian Abeck
Abgabedatum: 15. November 1994

Ehrenwörtliche Erklärung

Hiermit versichere ich, daß ich diese Diplomarbeit selbständig verfaßt und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. November 1994 .....

Entwurf eines Modells für die Erstellung einer Verfügbarkeitsdokumentation und deren effektive Nutzung im Bereich des integrierten Netzmanagements

Rudolf Egerer

Rudolf Egerer: Erstellung einer Verfügbarkeitsdokumentation

Rudolf Egerer: Erstellung einer Verfügbarkeitsdokumentation

Rudolf Egerer: Erstellung einer Verfügbarkeitsdokumentation

Rudolf Egerer: Erstellung einer Verfügbarkeitsdokumentation

Rudolf Egerer: Erstellung einer Verfügbarkeitsdokumentation

Inhaltsverzeichnis

1 Einleitung, Motivation, Überblick 1

1.1 Motivation, Ziel des Projektes, Szenario 2

1.2 Definition „Verfügbarkeit“ 3

1.2.1 Definition „physikalische Verfügbarkeit“ 4

1.2.2 Definition „logische Verfügbarkeit“ 5

1.3 Überblick 5

2 Verfügbarkeitsdokumentation in einem Rahmenbetriebskonzept 7

2.1 Das instantiierte Dienstleistungskonzept 8

2.2 Das instantiierte Lokale Betriebskonzept 9

2.2.1 Regulierung, Ziele und Träger der Aufgabe 9

2.2.1.1 Aufgabenregulierung 9

2.2.1.2 Ziele der Aufgabe 10

2.2.1.3 Aufgabenträger 11

2.2.2 Qualitätssicherungssysteme 12

2.2.2.1 Qualitätssicherung nach der DIN-ISO-Normenreihe 9000 13

2.2.2.2 Qualitätsaudit nach DIN ISO 10 011 16

2.2.2.3 Umfassendes Qualitätsmanagement (TQM) 17

2.2.3 Vom Lokalen Betriebs- zum Verfahrenskonzept 19

2.3 Das instantiierte Verfahrenskonzept 19

2.3.1 Verfahrensregulierung 19

2.3.2 Definition der benutzten Verfahren 20

2.3.2.1 Verfahren „Zugriff auf die Verfügbarkeitsdaten(quellen)“ 20

2.3.2.2 Verfahren „Aufbereiten der Verfügbarkeitsdaten“ 21

2.3.2.3 Verfahren „Interaktive Verfügbarkeitsdaten(nach)bearbeitung“ 21
2.3.2.4 Verfahren „Erstellen anforderungsgemäßer Analysen / Präsentation“ 22
2.3.3 Vom Verfahrens- zum Werkzeugkonzept 22
2.4 Das instantiierte Werkzeugkonzept 23
2.4.1 Werkzeugregulierung 23
2.4.2 CLI-Ansatz versus API-Ansatz 23
2.4.2.1 Der CLI-Ansatz 24
2.4.2.2 Der API-Ansatz 25
2.4.2.3 Folgerung und Empfehlung 25
2.4.3 Definition der eingesetzten Werkzeuge 26
2.4.3.1 Werkzeug „Datenquellen“ 26
2.4.3.2 Werkzeug „Datensenken und Präsentation“ 27
2.4.3.3 Werkzeug „Programmiersprachen“ 27

3 Anforderungen an eine Verfügbarkeitsdokumentation 28

3.1 Anforderungen der Empfänger 28
3.1.1 Empfänger-Zielgruppen 29
3.1.2 Allgemeine Anforderungen an Auswertungen 29
3.1.3 Anforderungen des „Managements“ an Auswertungen 31
3.1.4 Anforderungen der „Technik“ an Auswertungen 31
3.2 Anforderung: benötigte Verfügbarkeitsdaten 32
3.2.1 Daten der physikalischen Verfügbarkeit 32
3.2.2 Daten der logischen Verfügbarkeit 33
3.2.3 Daten über aufgetretene Fehler (Ausfallursachen) 33
3.2.3.1 Alarm-Basiskategorien nach ISO/IEC 10 164-4 34
3.2.3.2 Anforderungen an die Alarm-Behandlung nach ISO/IEC 10 164-5 36
3.3 Anforderung: benötigte Datenquellen 37
3.3.1 Netzmanagementsysteme 37
3.3.2 Netzdokumentationssysteme 38
3.3.3 Manuelle Eingaben 38
3.4 Anforderung: Präsentation und Layout der Dokumentation 39

3.5 Anforderung: Datenintegration 39

3.6 Anforderung: Datenarchivierung 41

4 Die Ablauforganisation **43**

4.1 Modelle für das Eventmanagement 43

4.1.1 Modell nach ISO/IEC 10 164-5 43

4.1.2 Erweitertes Modell 44

4.2 Die Ablauforganisation 46

4.2.1 Identifikation und Korrelation von Netzkomponenten 47

4.2.2 Datenvorverarbeitung 47

4.2.2.1 Steuerung und Konfiguration über eine Textdatei 48

4.2.2.2 Steuerung und Konfiguration über ein Netzdokumentationssystem 49

4.2.2.3 Folgerung und Bewertung: empfohlenes Vorgehen 50

4.2.3 Spiegelung des Netzdokumentationssystems 51

4.2.4 Datenbanksystem und interaktive Daten(nach)bearbeitung 52

4.3 Sonderfälle 53

4.3.1 Probleme im FDDI-Ring 53

4.3.1.1 Kabelunterbrechungen 54

4.3.1.2 Brouter-Probleme 55

4.3.2 Verlorengegangene Traps 56

4.3.3 Zugang des Netzmanagementsystems zum Netz unterbrochen 57

4.4 Dokumentation: Präsentation und mathematische Analyse 58

4.4.1 Grundsätzliches über Diagramme 58

4.4.1.1 Achsen 59

4.4.1.2 Grunddiagrammarten 59

4.4.2 Mathematische Verfahren zur Verfügbarkeitsanalyse 61

5 Technische Erstellung einer Verfügbarkeitsdokumentation **65**

5.1 Realisierung: Identifikation der Netzkomponenten 67

5.2 Datenquelle: Netzmanagementsystem 68

5.3 Realisierung: die Datenvorverarbeitung 69

5.3.1 Anbindung zum Netzmanagementsystem 69
5.3.2 Steuerung und Konfiguration 70
5.3.2.1 Steuerung und Konfiguration durch eine Textdatei 70
5.3.2.2 Steuerung und Konfiguration durch CINEMA 71
5.3.3 Anbindung des lokalen (Oracle-)Datenbanksystems 72
5.3.3.1 Aktualisieren der temporären Eingangstabellen 72
5.3.3.2 Empfehlung zum Realisieren der Realzeit-Verdichtung 73
5.3.3.3 Empfohlene Behandlung von Contact-lost-Meldungen 73
5.3.4 Berechnen der Ausfalldauer am Beispiel von Cisco-Brouters 74
5.4 Datenbanksystem und Anbindungen 77
5.4.1 Kopplung mit dem Netzdokumentationssystem 77
5.4.2 Anbindung an das BMW-Problemmanagement 78
5.5 Realisierung: die interaktive Daten(nach)bearbeitung 78
5.5.1 Fehlerklassifizierung 78
5.5.2 Die temporären Eingangstabellen 81
5.5.2.1 Die Übersichts-Bildschirmmaske 81
5.5.2.2 Die temporäre Eingangstabelle für den LAN-Bereich 83
5.5.2.3 Die temporäre Eingangstabelle für den WAN-Bereich 86
5.5.3 Die Archivtabellen 87
5.5.3.1 Zeilenkopf 88
5.5.3.2 Zeilenrest 88
5.5.4 Zusammenfassung: die nötigen Tabellen 89
5.6 Realisierung: Statistiken und Diagramme 89
5.6.1 Dokumentation der physikalischen Verfügbarkeit 90
5.6.1.1 Definitionen zur Berechnung der physikalischen Verfügbarkeit 90
5.6.1.2 Folgerungen 92
5.6.1.3 Beispiel zur Berechnung der physikalischen Verfügbarkeit 93
5.6.1.4 Beispiel-Auswertungen für das „Management“ 94
5.6.1.5 Beispiel-Auswertungen für die „Technik“ 95
5.6.2 Dokumentation der logischen Verfügbarkeit 99
5.6.2.1 Definition der zu erstellenden Auswertungen 99
5.6.2.2 Beispiele für Auswertungen 100

6 Nutzung des Konzeptes im integrierten Netzmanagement **102**

6.1 Einsatz eines Performancemanagement-Systems 103

6.1.1 Einführung 103

6.1.2 Eignung des SAS/CPE-Systems zur Verfügbarkeitsdokumentation 105

6.2 Einsatz eines Trouble-Ticket-Systems 105

6.2.1 Einführung in Trouble-Ticket-Systeme 105

6.2.2 Nutzung des Konzeptes bei Trouble-Ticket-Systemen 108

6.2.3 Bewertung, Folgerung 110

7 Ausblick **111**

7.1 Vision „Global-Verfügbarkeitsdokumentation“ 111

7.2 Gesetzliche Grenzen der Verfügbarkeitsdaten-Erfassung 112

7.3 Weitere Arbeiten 114

8 Literaturverzeichnis **115**

Abbildungsverzeichnis

1.1 Definition des Begriffes Verfügbarkeit 4

2.1 Instantiiertes Rahmenbetriebskonzept 7
2.2 Gewichtung der TQM-Kriterien 18
2.3 Beziehungen — Lokales Betriebs- und Verfahrenskonzept 19
2.4 Beziehungen — Verfahrens- und Werkzeugkonzept 22

3.1 Repräsentation der Verfügbarkeitsinformation 37
3.2 Kooperation zwischen Problem-, LAN- und WAN-Management 40

4.1 „Event Report Management Model“ nach ISO/IEC 10 164-5 44
4.2 Erweitertes Eventmanagement-Modell 45
4.3 Ablauforganisation 46
4.4 FDDI-Ring mit einer Kabelunterbrechung — keine Teilringbildung 54
4.5 FDDI-Ring mit zwei Kabelunterbrechungen — Teilringbildung 55
4.6 Problem mit dem Brouter 6 — keine Teilringbildung 55
4.7 Probleme mit den Brouters 6 und 11 — Teilringbildung 56
4.8 Die Objekte eines Diagramms 58

5.1 Datenflußplan 66
5.2 Daten-Export- und Zugriffsalternativen von SPECTRUM 69
5.3 Kennbuchstaben für die Wahl des Netzinfrastrukturtyps 71
5.4 Kennbuchstaben für die Wahl des Auswertungstyps 72
5.5 Korrespondierende Events zur Berechnung der Ausfalldauer 75

5.6 Untergliederung der Basiskategorie „Communications Alarm Type“ 79
5.7 Untergliederung der Basiskategorie „Quality of Service Alarm Type“ 79
5.8 Untergliederung der Basiskategorie „Processing Error Alarm Type“ 80
5.9 Untergliederung der Basiskategorie „Equipment Alarm Type“ 80
5.10 Untergliederung der Basiskategorie „Environmental Alarm Type“ 81
5.11 Felder der Übersichts-Bildschirmmaske 82
5.12 Temporäre Eingangstabelle für den LAN-Bereich 83
5.13 Syntax und Semantik des Backup-Ausfall-Codes 85
5.14 Temporäre Eingangstabelle für den WAN-Bereich 87
5.15 Archivtabelle für den LAN-Bereich 87
5.16 Beispiel für die Berechnung der physikalischen Verfügbarkeit 93
5.17 Physikalische Verfügbarkeit ohne und mit Gewichtung 94
5.18 Physikalische Verfügbarkeit und Ausfallstunden 95
5.19 Physikalische Verfügbarkeit des Local- und Remote-Bereiches 95
5.20 Örtliche Verteilung der physikalischen Ausfälle im Local-Bereich 96
5.21 Örtliche Verteilung der physikalischen Ausfälle im Remote-Bereich 96
5.22 Ausfallursachen im Local-Bereich 96
5.23 FDDI-Backbone: Verfügbarkeit und Anzahl der Ausfälle 97
5.24 Anzahl und durchschnittliche Dauer aller aufgetretenen Ausfälle 97
5.25 Tages-Verfügbarkeit mit gleitendem Durchschnitt zur Trendanalyse 98
5.26 Einige charakteristische Werte zu Abbildung 5.25 98
5.27 Monats-Spitzenauslastung 100
5.28 Tages-Spitzenauslastung 101

6.1 Überblick über das SAS/CPE-System 103
6.2 Aufbau eines Trouble-Ticket-Systems 106
6.3 Vererbungshierarchie zum Trouble Management 107
6.4 Verfügbarkeitsdokumentation mit einem Trouble-Ticket-System 109

1 Einleitung, Motivation, Überblick

Im Bereich der *Rechnernetzintegration* waren auf der Messe *Systems '93*, die vom 18. bis 22. Oktober auf dem Münchener Messegelände stattfand ([SYSTEMS]), das kräftige Wachstum und die permanente Produktinnovation wieder besonders auffällig; die Netzintegration bleibt neben der Vereinheitlichung bestehender Netzperipherie das zweitwichtigste Umsatzfeld. Marktforscher der International Data Corporation (IDC) rechnen mit einem Anstieg der weltweiten Ausgaben für die Netzintegration von knapp drei Milliarden US-Dollar ($) im Jahr 1989 auf fast sieben Milliarden $ bis zum Jahr 1994.

Das Ziel der Netzintegration ist das sogenannte *Internetworking*, welches aufgrund des zunehmenden Zusammenwachsens von einzelnen proprietären Netz-Insel-Lösungen und der eskalierenden Anforderungen an die Leistungsfähigkeit und Qualität von Netzen immer mehr in den Blickpunkt des Interesses der Anwender rückt.

Konsequenterweise setzen zukunftsorientierte Unternehmen (wie der Netzbetreiber Bayerische Motoren Werke Aktiengesellschaft[1]) im Rahmen von Ersatz-, Rationalisierungs- oder Erweiterungsinvestitionen schon seit einiger Zeit und in zunehmendem Maße *Lichtwellenleiternetze* ein. Ein Beispiel für ein solches Glasfasernetz ist das *Fibre Distributed Data Interface (FDDI)*, dessen Spezifikation bei einer Übertragungsrate von 100 Mbps weniger als einen Fehler je $2{,}5 \cdot 10^{10}$ Bits verlangt. Aufgrund der innerhalb von drei Jahren auf ein Zehntel gefallenen Preise der 100-Mbps-FDDI-Komponenten und ihrer hohen Qualität (Durchsatz, Zuverlässigkeit) werden diese heute bereits in *lokalen Netzen* (Local Area Networks, LANs) verwendet, in denen bisher das als *Ethernet* (= wichtigster Vertreter der Norm IEEE[2] 802.3) bekannte *Diffusionsnetz* starke Verbreitung gefunden hat.

Bei der gesamten Entwicklung wurde auf der Systems ein Trend deutlich sichtbar:

- Früher ging es zunächst einmal darum, überhaupt in der Lage zu sein, proprietäre, isolierte Systeme und Netze zu verbinden.
- Heute und auch in Zukunft bemüht man sich dagegen verstärkt darum, bei den vorhandenen bzw. geplanten Netzen, deren Heterogenität (allen Standardisierungsbemühungen zum Trotz) eher noch anzuwachsen scheint, insbesondere die *Qualität* zu verbessern.

Der wichtigste Bestandteil dieser Qualität ist — neben der ständigen Forderung nach einem immer höheren Durchsatz — vor allem eine *zugesicherte hohe Zuverlässigkeit* der eingesetzten Netze und ihrer Komponenten, also eine *garantierte permanente Verfügbarkeit* (zur Be-

---

[1] Im folgenden wird die Abkürzung „BMW“ verwendet.

[2] Institute of Electrical and Electronics Engineers.

griffsdefinition siehe Abschnitt 1.2 auf Seite 3), die für unsere schnellebige Welt immer wichtiger wird.

Beispiele:

1. **Medizin:** Für die Verwaltung der Daten der für eine Transplantation bereitstehenden Organe einerseits und der auf eine möglicherweise lebensrettende Organspende wartenden Patienten andererseits existiert seit einiger Zeit eine in mehreren Ländern verfügbare Datenbank, die permanent ausgebaut wird. Besonders bei Herztransplantationen spielt die Zeit — und damit natürlich die Verfügbarkeit aller zur Ermittlung eines für die Transplantation geeigneten Patienten benutzten Netze und Systeme — zwischen Organentnahme und der Einpflanzung eine entscheidende Rolle.
2. **Wirtschaft:** [BUDDEN] beschreibt ein interessantes Beispiel des technischen Aufwandes, für die Deutsche Terminbörse GmbH (DTB) mit Hilfe von ausgeklügelten und ständig weiterentwickelten Backup-Systemen nach den Prinzipien Redundanz und Modularität eine möglichst 100prozentige Gesamt-Systemverfügbarkeit zu erreichen. Die DTB stellt als vollelektronische Börse höchste Ansprüche an die Zuverlässigkeit und Verfügbarkeit des Systems, um auf dem sehr umkämpften Markt Erfolg zu haben, da bei der Größe der bewegten Geldmenge und des damit verbundenen Risikos die beteiligten Händler und die sogenannten Marketmaker jederzeit und uneingeschränkt in der Lage sein müssen, in den Handel einzugreifen.

1.1 Motivation, Ziel des Projektes, Szenario

Wie die obigen Beispiele zeigen, wird jeder Netzbetreiber darauf bedacht sein, die bestmögliche Zuverlässigkeit seines Netzes zu gewährleisten, die einen Grundbestandteil der *Dienstqualität (Quality of Service)* darstellt, die in einem Unternehmen von einem Dienst „Bereitstellung/Betrieb LAN (WAN)“ angeboten wird.

Um diesen Dienst zu leisten, sollten die beim Netzbetreiber vorhandenen Ressourcen, nämlich

- *technische Ressourcen:* Hardware und Software;
- *menschliche Ressourcen (auch als „Humankapital“ bezeichnet):* Arbeitskräfte (Mitarbeiter, internes bzw. externes Wartungs- und Instandsetzungspersonal, Kundendienst);
- *immaterielle Ressourcen:* z.B. Innovationsfähigkeit, Know-how

in technischer und ökonomischer Hinsicht optimal genutzt bzw. eingesetzt werden. Dazu kann eine aussagekräftige Netz-Verfügbarkeitsdokumentation beitragen,

- die dem Netzbetreiber einen Überblick über die Verfügbarkeit des von ihm betriebenen Netzes und seiner Komponenten ermöglicht — Informationen, die er zur Verifizierung der mit seinen
  - Lieferanten (z.B. Deutsche Telekom) und
  - Kunden

  abgeschlossenen (Service-)Verträge benötigt;
- aus welcher der Netzbetreiber die erforderlichen Maßnahmen zur Optimierung des Netzes und seiner Komponenten (z.B. effektive und effiziente Netzwartung, notwendige Infrastrukturänderungen) abzulesen vermag.

Dazu wird ein Modell für eine Verfügbarkeitsdokumentation auf Basis der unteren drei Ebenen eines am Lehrstuhl entwickelten Rahmenbetriebskonzeptes entworfen, wobei im Sinne eines Top-down-Vorgehens mit Rückkopplung (Bottom-up-Vorgehen, Feedback) anhand von Netzbetreiberanforderungen Aufgaben definiert sowie die zum Erbringen dieser Aufgaben zu verwendenden Verfahren erarbeitet und Anforderungen an die einzusetzenden Werkzeuge festgestellt werden:

- Erfassen der Netzbetreiberanforderungen an eine Verfügbarkeitsdokumentation.
- Einteilen von Aufgaben (Rollenverteilung) mit dem Ziel, im Bereich des Problemmanagements die Zusammenarbeit der Organisationseinheiten LAN-Gruppe, WAN-Gruppe und Störungsannahme durch weitestgehend gemeinsame Nutzung und Pflege der Netzdatenbestände (Datenintegration) unter Effektivitäts- und Effizienzgesichtspunkten zu verbessern.
- Entwickeln und Realisieren geeigneter Verfahren
  - zur Sammlung der von Netzmanagementsystemen bereitgestellten Verfügbarkeitsdaten in lokalen Datenbanken, die jederzeit einen externen Zugriff auf den aktuellen Netzzustand ermöglichen sollen;
  - zur Analyse und graphischen Aufbereitung (Diagramme), welche — abhängig vom jeweiligen Empfänger/Nutzer (Zielgruppe) der Auswertungen — unterschiedliche Detailliertheit und Komplexität aufweisen werden.
- Ermitteln von Anforderungen an Werkzeuge, die für die Datensammlung, Analyse und Präsentation geeignet sind (Netzmanagement-, Trouble-Ticket-, Performancemanagement-, Netzdokumentations- und Datenbanksysteme sowie Programmiersprachen).

Das im Hause BMW durchgeführte Projekt „Verfügbarkeitsdokumentation“ beinhaltet die (prototypische) Implementierung für die Umgebung des Netzbetreibers, an der seit September 1994 zwei weitere Studenten im Rahmen von Fortgeschrittenenpraktika nach dem vom Autor in enger Zusammenarbeit mit BMW erstellten vorliegenden Konzept (insbesondere Kapitel 4 und 5) engagiert arbeiten.

1.2 Definition „Verfügbarkeit“

Der Begriff „Verfügbarkeit“ ist bereits in unterschiedlicher Weise definiert; um Mißverständnisse von vornherein auszuschließen, hat sich der Verfasser entschlossen, zunächst eine für das Projekt passende, pragmatische Begriffsbestimmung zu finden.

Zu Beginn der Zusammenarbeit mit BMW, insbesondere mit Herrn Klaus Kastenmeier, der in der LAN-Gruppe der Abteilung FI-21 für das Netzmanagement zuständig ist, wurden anläßlich einer Besprechung des BMW-LANs

- dessen *physische* Netzstruktur (z.B. im Local-Bereich: LAN-LAN-Verbindungen) und
- dessen *logische* Netzstruktur (z.B. logische Kanäle im Remote-Bereich: LAN-WAN-Verbindungen)

erörtert; dabei erwies es sich als sinnvoll, auch bei der neuen Definition der Verfügbarkeit zwei wesentliche Bereiche zu unterscheiden, nämlich

1. die *physikalische Verfügbarkeit* und
2. die *logische Verfügbarkeit*.

Außerdem sollen für beide Bereiche jeweils zwei Sichten betrachtet werden, und zwar

a) die Verfügbarkeit *aus Sicht der Benutzer* eines Netzes, d.h. Einschränkungen der Verfügbarkeit, die Auswirkungen auf die Benutzer haben, und

b) die Verfügbarkeit *aus rein technischer Sicht*, d.h. Einschränkungen der Verfügbarkeit aus technischen Gründen, wobei die Auswirkungen auf die Benutzer unberücksichtigt bleiben.

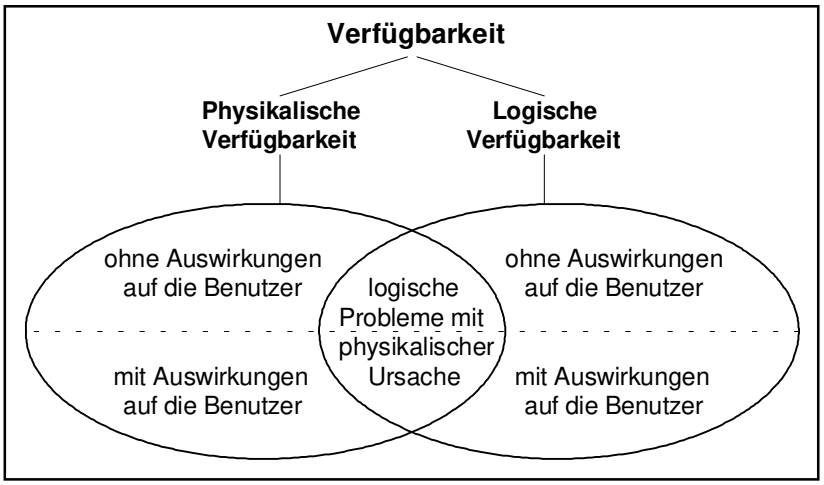

Abbildung 1.1: Definition des Begriffes Verfügbarkeit

Aufgrund der Vielfalt der möglichen Einflüsse auf die Verfügbarkeit läßt sich eine Überschneidung der beiden Verfügbarkeitsbereiche und der zugehörigen Sichten nicht ausschließen, wie Abbildung 1.1 verdeutlicht.

1.2.1 Definition „physikalische Verfügbarkeit“

Definition: *Ein Netz (bzw. Gerät, Port) ist **verfügbar im Sinne der physikalischen Verfügbarkeit aus Sicht der Benutzer bzw. Techniker**, die damit direkt (betrifft z.B. Datenendgeräte) und/oder indirekt (z.B. Router) arbeiten, wenn diese **keine Betriebsausfälle** feststellen können.*

Beim Verfügbarkeitsbereich *physikalische Verfügbarkeit* geht es also um von Benutzern bzw. netzüberwachenden technischen Abteilungen feststellbare Betriebsausfälle mit beliebiger Ursache; diese Definition entspricht in etwa dem üblichen Verständnis von Verfügbarkeit.

1.2.2 Definition „logische Verfügbarkeit“

Definition: *Ein Netz (bzw. Gerät, Port) ist **verfügbar im Sinne der logischen Verfügbarkeit aus Sicht der Benutzer bzw. Techniker**, die damit direkt und/oder indirekt arbeiten, wenn diese **keine Einschränkungen bezüglich der Qualität** (z.B. Antwortzeit, Performance, Durchsatz, Auslastung, Fehlerhäufigkeit) des Netzes (Gerätes, Ports) feststellen können.*

Beim Verfügbarkeitsbereich *logische Verfügbarkeit* hat folglich die Qualität eine übergeordnete Bedeutung. Dieser Aspekt wurde deshalb in die Begriffsbestimmung aufgenommen, weil Minderungen der Netzqualität direkten, nachteiligen Einfluß auf den für die Benutzer bzw. Techniker relevanten Netzzustand hat.

Beispiel: Würde man die logische Verfügbarkeit nicht in die Verfügbarkeit mit einbeziehen, so wären derart groteske Aussagen wie „unser Netz war am 1. April zu 100% verfügbar“ möglich, obwohl an diesem Tag z.B. die durchschnittliche Antwortzeit (etwa aufgrund von Protokollproblemen) bei *fünf Minuten* (statt der sonst üblichen *fünf Sekunden*) lag.

1.3 Überblick

Wie bereits im Abschnitt „Motivation, Ziel des Projektes, Szenario“ auf Seite 2 angedeutet, entspricht das Vorgehen dem Top-Down-Verfahren; in diesem Sinne ist auch die vorliegende Arbeit gegliedert:

- **Kapitel 2** befaßt sich mit der *Einordnung einer Verfügbarkeitsdokumentation in ein vorhandenes Rahmenbetriebskonzept*:
  - Anwendung des Rahmenbetriebskonzeptes durch Instantiierung;
  - globale mit einer Verfügbarkeitsdokumentation verfolgte Ziele;
  - Ansätze zur Sicherung der Qualität der Verfügbarkeit und der diesbezüglich zu erstellenden Dokumentation;
  - grundsätzliche Implementierungsalternativen beim Werkzeugkonzept.
- **Kapitel 3** beschäftigt sich mit *wesentlichen Anforderungen* an eine Verfügbarkeitsdokumentation:
  - Anforderungen der Empfänger (Nutzer), die dazu in Zielgruppen innerhalb einer Netzbetreiberorganisation unterschieden werden;
  - Anforderungen an die benötigten Daten (z.B. Fehlerklassifizierung, Integration, Archivierung) und Datenquellen (z.B. Netzmanagementsysteme);
  - Präsentation (Layout).
- **Kapitel 4** liefert die *theoretischen Grundlagen* zur Realisierung einer Verfügbarkeitsdokumentation:
  - Herleitung der zur Erstellung erforderlichen Ablauforganisation von
    i) dem ISO/IEC-Eventmanagement-Modell und
    ii) den Anforderungen aus den Kapiteln 2 und 3;

- Erörterung von Sonderfällen (spezielle Netzzustände);
- Grundlagen zur Präsentation (Diagramme) und zur mathematischen Analyse (z.B. Ermitteln von Trends).

- **Kapitel 5** zeigt die *technischen Grundlagen* zur Realisierung einer Verfügbarkeitsdokumentation auf:
  - Realisierung und Implementierung der in Kapitel 4 hergeleiteten Ablauforganisation;
  - Beispiele für Auswertungen.

- **Kapitel 6** beschreibt *die alternative Nutzung des vorliegenden Konzeptes* anhand zweier im integrierten Netzmanagement immer häufiger anzutreffender passiver Werkzeuge, die als Ergänzungen der üblichen Netzmanagementsysteme (= aktive Werkzeuge) anzusehen sind, nämlich
  i) Performancemanagement-Systeme und
  ii) Trouble-Ticket-Systeme.

- **Kapitel 7** enthält einen *Ausblick*:
  i) weitere Entwicklung der Netzverfügbarkeit;
  ii) Erläuterung der gesetzlichen Vorschriften (Bundesdatenschutzgesetz), die bei der Erfassung und Verarbeitung von Verfügbarkeitsdaten zu beachten sind;
  iii) Hinweise auf mögliche Anschlußarbeiten.

2 Verfügbarkeitsdokumentation in einem Rahmenbetriebskonzept

Dieses Kapitel behandelt die Instantiierung, d.h. die praktische Anwendung eines Rahmenbetriebskonzeptes zur Erstellung einer Verfügbarkeitsdokumentation im LAN(WAN)-Bereich.

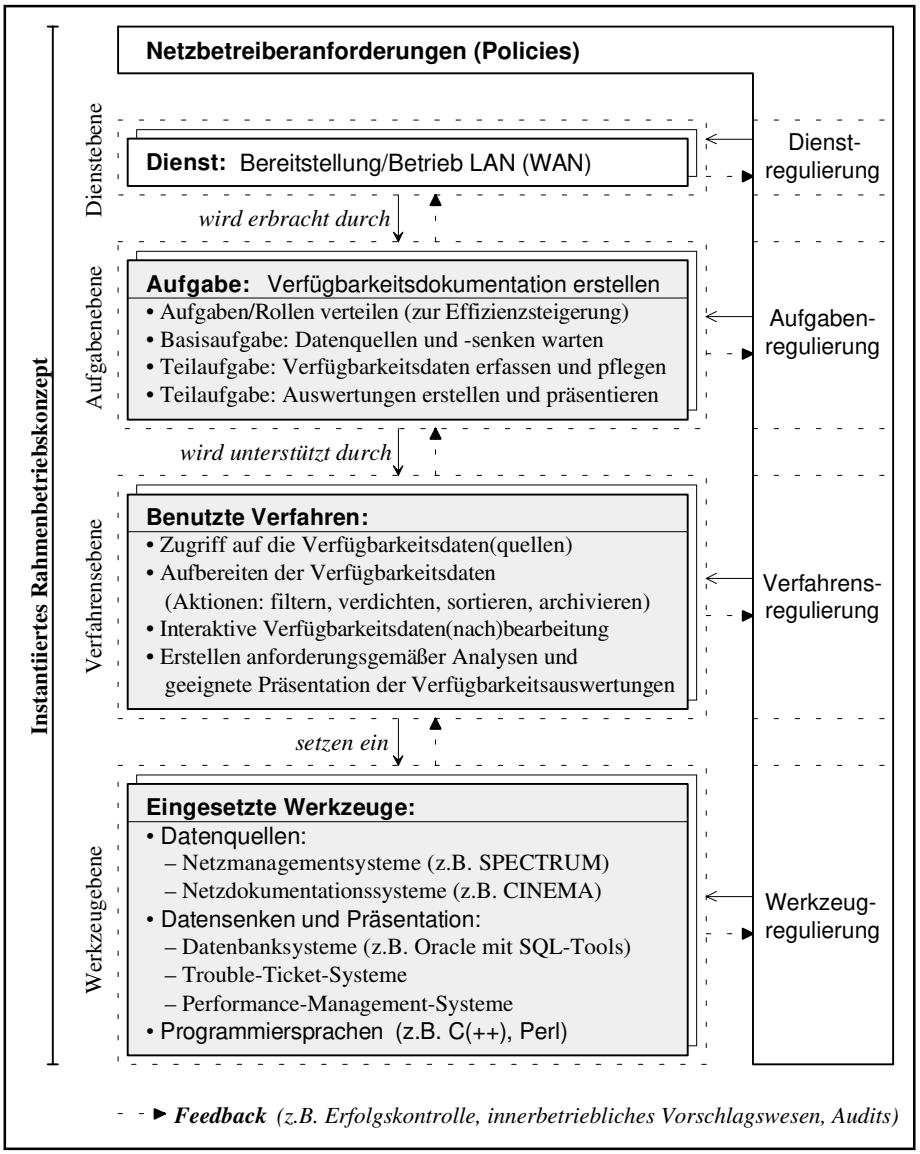

Abbildung 2.1: Instantiiertes Rahmenbetriebskonzept

Die in dieser Arbeit verwendeten theoretischen Grundlagen des Rahmenbetriebskonzeptes, das aus den elementaren Bestandteilen (Objekten)

1. Dienst,
2. Aufgabe,
3. Verfahren und
4. Werkzeug

besteht, sind in [RBK] beschrieben und werden hier nur insoweit wiederholt, als dies zum allgemeinen Verständnis erforderlich ist.

In Abbildung 2.1 sind die im Rahmen der vorliegenden Arbeit besonders relevanten Ebenen des Rahmenbetriebskonzeptes grau unterlegt dargestellt; auf sie wird in diesem Kapitel speziell eingegangen.

2.1 Das instantiierte Dienstleistungskonzept

Im Dienstleistungskonzept werden die Dienstleister und die Dienstnutzer sowie deren Dienstleistungsbeziehungen definiert.

Jeder Dienst wird durch

- seinen Inhalt,
- Dienstgütevereinbarungen und
- abrechnungstechnische Meßgrößen

charakterisiert.

Eine wesentliche Anforderung der Anwender (= Kunden) an den Quality of Service des Dienstes „Bereitstellung/Betrieb LAN (WAN)“ ist, vom Netzbetreiber (= Dienstleister) eine möglichst hohe Verfügbarkeit der benutzten Netzinfrastruktur (vertraglich) zugesichert zu bekommen. Um überhaupt in der Lage zu sein, seinen Kunden für diesen Quality of Service eine bestimmte Mindestverfügbarkeit garantieren zu können, muß der Dienstleister die Verfügbarkeit im LAN(WAN)-Bereich messen und analysieren. Die dazu erforderlichen Maßnahmen werden in Form von Aufgaben im nächsten Abschnitt beschrieben.

- Die Initiierung des Auftrages, d.h. das Anfordern des Dienstes, einen LAN(WAN)-Anschluß bereitzustellen, erfolgt durch den Anwender, d.h. es handelt sich hier um eine *explizite Initiierung*.
- Als Dienstleister für den Dienst „Bereitstellung/Betrieb LAN (WAN)“ tritt die LAN- bzw. WAN-Gruppe auf.

  Beispiel: Bei BMW gehören die LAN-Gruppe und die WAN-Gruppe zur Abteilung Networkinfrastructure (FI-21), die zur Hauptabteilung FI-2 zählt, welche wiederum Teil des Bereichs FI ist.

- Der Dienst wird sowohl innerhalb von FI-21 als auch abteilungsübergreifend in Anspruch genommen, d.h. es handelt sich um einen *internen und externen Dienst.*

2.2 Das instantiierte Lokale Betriebskonzept

Dienste definieren eine Schnittstelle zu den (externen und internen) Anwendern. Zum systematischen und strukturierten Erbringen von Diensten werden durch Informationsflüsse miteinander verbundene Aufgaben als kontrollierbare und steuerbare Einheiten innerhalb einer Organisationseinheit festgelegt.

Durch dieses Konzept erreicht man

- eine erheblich erhöhte Transparenz der betrieblichen Ablauforganisation, so daß die Zusammenarbeit der Mitarbeiter erleichtert und ihre Motivation gesteigert wird;
- eine größere Effektivität und Effizienz betrieblicher Prozesse (Aufgaben und Verfahren);
- einen höheren Quality of Service als Resultat der verbesserten Qualitäten der an der Diensterbringung beteiligten Aufgaben (Mitarbeiter).

Bei der Messung der Verfügbarkeit eines Netzes und seiner Komponenten sowie der Bereitstellung von diesbezüglichen Analysen, Statistiken und graphischen Auswertungen handelt es sich um eine Aufgabe im Sinne des Lokalen Betriebskonzeptes, die in den Bereichen Controlling und Quality of Service zur Erfüllung des Dienstes „Bereitstellung/Betrieb LAN (WAN)“ beiträgt.

Im folgenden wird diese Aufgabe kurz mit „Verfügbarkeitsdokumentation erstellen“ bezeichnet.

2.2.1 Regulierung, Ziele und Träger der Aufgabe

In den nachstehenden Unterabschnitten werden die

1. Regulierung (siehe unten),
2. Ziele (Seite 10) und
3. Träger (Seite 11)

der Aufgabe „Verfügbarkeitsdokumentation erstellen“ näher erläutert.

2.2.1.1 Aufgabenregulierung

Die Aufgabenregulierung

- übernimmt das Festlegen der Aufgabenträger (Rollenverteilung, vergleiche Unterabschnitt „Aufgabenträger“ auf Seite 11);

- überwacht und regelt das Erreichen bzw. Einhalten der Ziele der Aufgabe, die im nächsten Unterabschnitt behandelt werden;
- legt die Qualität fest, mit der eine Aufgabe zu erledigen ist.

Dabei spielt insbesondere eine vorgegebene Begrenzung der Arbeitszeit, die von den beteiligten Mitarbeitern zum Erbringen dieser Aufgabe aufgewendet werden darf, für die erreichbare Qualität und Quantität der Verfügbarkeitsdokumentation sowie auch für die eingesetzten Verfahren eine entscheidende Rolle; darauf wird im Abschnitt „Das instantiierte Verfahrenskonzept“ auf Seite 19 eingegangen.

2.2.1.2 Ziele der Aufgabe

Das übergreifende Ziel der Aufgabe „Verfügbarkeitsdokumentation erstellen“ ist, im wesentlichen zwei Zielgruppen (Nutzer) mit den von ihnen angeforderten Verfügbarkeitsinformationen zu versorgen:

- dem *Management des Unternehmens* soll mit aussagekräftigen Informationen das Finden und Verfolgen von geeigneten Strategien zur Erreichung der Unternehmensziele erleichtert werden, z.B. durch Effektivitäts-/Effizienzsteigerung, Kostenminimierung usw.;
- die *technischen Abteilungen* LAN(WAN)-Gruppe und Kundendienst sollen durch detaillierte Auswertungen informiert werden, um den Quality of Service zu gewährleisten, d.h. am Erbringen des Dienstes mitzuwirken.

Weitere Ziele der Aufgabe

- **Verifikation von Serviceverträgen mit Verfügbarkeitsklauseln**

  Für einen Netzbetreiber ist es von großer Bedeutung, das Einhalten der mit seinen Kunden und Lieferanten (z.B. dem Netzbetreiber Deutsche Telekom) abgeschlossenen Serviceverträge, die Verfügbarkeitsklauseln enthalten, zu überprüfen.

  In derartigen Verfügbarkeitsklauseln können unter anderem die folgenden Punkte geregelt sein:

  – *Zusage einer bestimmten Mindestverfügbarkeit* des dem Kunden (bzw. vom Lieferanten) bereitgestellten Netzes oder Netzzugangs;

  – *Festschreibung der maximalen Reaktionszeit* des Netzbetreibers nach dem Melden einer Störung durch den Kunden; aufgrund dieser vertraglichen Vereinbarungen muß dem Netzbetreiber eine Verfügbarkeitsdokumentation bereitgestellt werden, die bei Kundenreklamationen — im Einzelgespräch mit dem betreffenden Kunden — jederzeit (vor allem bei aktuellen Ereignissen) Online abgefragt oder (eventuell bei weiter zurückliegenden Ereignissen) auch in ausgedruckter Form in einem Ordner vorhanden und regelmäßig zu aktualisieren ist.

- **Erleichtern der Netzinfrastrukturplanung**

  Dieses strategische Ziel bedeutet, durch eine geeignete Verfügbarkeitsdokumentation den Einsatz der Ressourcen effektiver zu gestalten mit dem Ziel, zu einer Optimierung der Netzinfrastruktur und damit der Verfügbarkeit beizutragen.

Beispiel: Wenn Standorte, deren Verfügbarkeit ständig unterhalb einer gewissen Toleranzschwelle liegt, aus der Dokumentation hervorgehen, können entsprechende Änderungen der Netzarchitektur zur Erhöhung der Verfügbarkeit in die Wege geleitet werden.

- **Erreichen einer möglichst hohen Qualität der Verfügbarkeitsdokumentation**

  Dieses strategische Ziel bedeutet,

  – einen hohen, den jeweiligen Nutzeranforderungen gerecht werdenden Informationsgehalt sowie

  – einen schnellen und unkomplizierten Zugriff auf die gesuchten Informationen

  zu bewerkstelligen, um dadurch die Transparenz des Quality of Service Verfügbarkeit im Sinne eines kontinuierlichen Verbesserungsprozesses (KVP, KAIZEN) ([KPMG]) ständig weiter zu verbessern. Das heißt für einzelne Mitarbeiter sowie Arbeitsgruppen, sich in kreativitätsfördernden sogenannten Qualitätszirkeln anhand von Qualitäts-Checklisten um eine kontinuierliche Verbesserung der Abläufe und Arbeitsergebnisse dauerhaft zu bemühen, um sich so selbständig zu verbessern und in der Lage zu sein, sofort flexibel auf Änderungen in der Umwelt des Unternehmens (z.B. sich ändernde Kundenwünsche) zu reagieren — man spricht hier vom Konzept der „lernenden Organisation".

  Beispiel: Bei BMW laufen Kundenbeschwerden bezüglich des Einhaltens der Serviceverträge häufig beim Abteilungsleiter von FI-21 ein. Laut Vertrag muß beispielsweise innerhalb von zwei Stunden nach dem Melden einer Störung durch den Kunden eine Reaktion des Netzbetreibers erfolgen. Der Abteilungsleiter ist dann im Hinblick auf die Durchsetzung seiner Interessen — d.h. Servicevertrag wurde eingehalten, obwohl der Kunde das Gegenteil behauptet (unzutreffende Reklamationen kommen leider nicht selten vor!) — in der Einzeldiskussion mit dem Kunden auf eine Verfügbarkeitsdokumentation als Argumentationsgrundlage angewiesen.

- **Verteilen der erstellten Verfügbarkeitsdokumentation**

  Das Verteilen an die Empfänger innerhalb und außerhalb der Netzbetreiberorganisation sollte reibungslos, flexibel und ohne großen personellen Aufwand durchgeführt werden, der Zugriff auf die Dokumentation ist für bestimmte Nutzer zu ermöglichen bzw. auch einzuschränken (Beachten von Datenschutz- und Datensicherheitsvorschriften).

2.2.1.3 Aufgabenträger

Aufgabenträger ist diejenige Stelle, welche für den LAN(WAN)-Betrieb zuständig ist, da dort alle Daten des Netzes über die eingesetzten Netzmanagementsysteme zusammenlaufen.

Die Aufgabe „Verfügbarkeitsdokumentation erstellen" läßt sich zum Zwecke der besseren Übersicht in Teilaufgaben untergliedern und Mitarbeitern zuordnen (Rollenverteilung), wobei besonders darauf geachtet werden sollte, daß alle Mitarbeiter jeweils über die zur Erfüllung der ihnen zugewiesenen Teilaufgaben entsprechende Qualifikation aufweisen, um ihre Motivation und die Qualität der Arbeitsergebnisse weder durch Über-, noch durch Unterforderung zu gefährden:

- **Steuernde-Aufgabe**

  Diese Aufgabe koordiniert und kontrolliert den anforderungsgemäßen Ablauf der anschließend aufgeführten (Teil-)Aufgaben zur Diensterbringung; sie ist dem Leiter der LAN- und WAN-Gruppe zuzuordnen.

- **Basisaufgabe**

  Dabei handelt es sich um eine Aufgabe, die nicht direkt einer Diensterbringung zugerechnet werden kann: um Verfügbarkeitsdaten zu erhalten, muß ein Mitarbeiter dafür sorgen, daß geeignete Netzmanagementsysteme (z.B. SPECTRUM) vorhanden und durch ordnungsgemäßes Warten im ständigen, möglichst störungsfreien Einsatz sind; dies gilt auch für benötigte Datenbanksysteme (z.B. CINEMA, Oracle), Trouble-Ticket-Systeme und Performancemanagement-Systeme.

- **Weitere Teilaufgaben**
  - Regelmäßiges, zuverlässiges Erfassen, Pflegen und Überwachen der von den Netzmanagementsystemen bereitgestellten Verfügbarkeitsdaten durch jeweils einen Mitarbeiter; da die Mitarbeiter diese (unangenehme) Arbeit untereinander aufteilen werden, sollte zur Erreichung einer hohen Qualität der Verfügbarkeitsdokumentation unbedingt eine Absprache (Schichteinteilung) der Mitarbeiter untereinander erfolgen, so daß immer zumindest ein Mitarbeiter anwesend ist, der die erforderliche Qualifikation zur Übernahme dieser Aufgabe hat.
  - Regelmäßiges Erstellen und Präsentieren der Verfügbarkeitsauswertungen.

2.2.2 Qualitätssicherungssysteme

Der Dienst „Bereitstellung/Betrieb LAN (WAN)“ stellt im Bereich der Verfügbarkeit an die Qualität, welche mit Hilfe von Qualitätssicherungssystemen verbessert werden soll, Anforderungen im wesentlichen auf zwei Gebieten:

- Qualitätsanforderungen an die Verfügbarkeit des Netzes und seiner Komponenten sowie
- Qualitätsanforderungen an die zu erstellende Verfügbarkeitsdokumentation.

Definition: *Ein **Qualitätssicherungssystem**[1] beinhaltet die Aufbauorganisation, Verantwortlichkeiten (= Aufgaben im Rahmenbetriebskonzept), Abläufe, Verfahren und Mittel (= Werkzeuge) zur Verwirklichung des Qualitätsmanagements.*

In den folgenden Unterabschnitten werden drei erfolgversprechende Methoden aufgezeigt, mit deren Hilfe sich die beiden oben genannten Qualitätsanforderungen in einem Unternehmen erreichen, sichern und dann kontinuierlich weiter verbessern lassen:

1. Qualitätssicherung nach der DIN-ISO-Normenreihe 9000 (siehe Seite 13f.);
2. Qualitätsaudit nach DIN ISO 10 011 (Seite 16f.);
3. Umfassendes Qualitätsmanagement (TQM) (Seite 17f.).

Anmerkung 1: *Diesen drei Methoden ist gemeinsam, daß ihre konsequente Einführung in einem Unternehmen zu einem anfangs nicht zu unterschätzenden Aufwand führt — eine Eintrittsbarriere, vor der in Deutschland leider immer noch viele Unternehmen zurückschrecken —, der jedoch schon mittelfristig zu erheblichen Effizienzsteigerungen und damit zu Kostenentlastungen der Unternehmen beitragen wird.*

[1] In der Literatur findet man häufig die Abkürzung QS-System.

Die Normen selbst enthalten teilweise schon Empfehlungen zur Begrenzung des Aufwandes wie „(…) Das Qualitätssicherungssystem sollte nur so umfassend sein, wie dies zum Erreichen der Qualitätsziele notwendig ist (…)“.

Anmerkung 2: Die Relevanz der Qualitätssicherungssysteme für die vorliegende Arbeit zeigt sich auch darin, daß BMW die Verfügbarkeitsdokumentation als eines von mehreren derzeit laufenden und geplanten TQM-Projekten durchführt.

2.2.2.1 Qualitätssicherung nach der DIN-ISO-Normenreihe 9000

Für die Verbesserung und Sicherung der Qualitätsanforderungen

- „hohe Verfügbarkeit“ (technisch-wirtschaftliche Qualitätsanforderung) und
- „geeignete Verfügbarkeitsdokumentation“ (organisatorische Qualitätsanforderung)

bieten sich die DIN-ISO-Normen der Gruppe 9000 an ([ISO], [LUDST]). Sie beinhalten im Gegensatz zu anderen ISO-Vorschriften keine produktspezifischen (technischen) Gebote, sondern empfehlen betriebliche Strukturen und Abläufe sowie Methoden und Instrumente, mit denen die Qualität gesichert werden kann.

- Die DIN-ISO-Norm 9000 enthält die allgemeinen Zielsetzungen und dient als Leitlinie für die anderen Vorschriften (DIN ISO 9001 bis DIN ISO 9004);
- in der Norm DIN ISO 9001 stehen Qualitätssicherungsnachweise für alle Unternehmensstufen (z.B. Service).

Empfohlen wird als Kernstück des Qualitätssicherungssystems das Erstellen eines sogenannten Qualitätssicherungshandbuchs, in dem die Ziele und die zu treffenden Maßnahmen festgelegt werden, wobei alle die Qualitätsaspekte betreffenden betrieblichen Unterlagen zu verarbeiten und durch eine klare Definition der Unternehmensphilosophie zu ergänzen sind. Die Theorie des Handbuchs muß dann den Arbeitsabläufen (= Verfahren im Rahmenbetriebskonzept) und Verantwortungsbereichen (= Rollenverteilung) zugeordnet und schließlich in die Praxis umgesetzt werden.

Anhand dieser Qualitätsvorgaben kann dann ein Unternehmen seine betrieblichen Abläufe durch eine Jury — z.B. Kontrolleure der Deutschen Gesellschaft zur Zertifizierung von Qualitätssicherungssystemen (DQS) in Frankfurt am Main — auf Effizienz prüfen lassen.

Die folgenden 20 Qualitätssicherungselemente müssen vorhanden sein, um die DIN-ISO-Norm 9001 zu erfüllen:

1. **Verantwortung der obersten Unternehmensleitung für die Qualitätssicherung von Produkten**
   - Qualitätspolitik;
   - Organisation (Verantwortungen und Befugnisse, Mittel und Personal für die Verifizierung, Beauftragter der obersten Leitung);
   - Review des Qualitätssicherungssystems durch die oberste Leitung.

*Bemerkung: In der Internationalen Norm wird der Ausdruck „**Produkt**“, sofern dies passend ist, auch zur Bezeichnung einer **Dienstleistung** verwendet (eine Dienstleistung ist nach [DIN ISO 8402] ein immaterielles Produkt).*

2. Aufbau eines geordneten Systems zur Qualitätssicherung

Ausarbeiten und effektives Verwirklichen dokumentierter Verfahren im Qualitätssicherungssystem.

3. Vertragsüberprüfung

Untersuchen und Dokumentieren der mit einem Auftrag verbundenen Qualitätsanforderungen.

Beispiel: Verfügbarkeitsklauseln (vergleiche Abschnitt 2.2.1.2 auf Seite 10).

4. Designlenkung

Berücksichtigen der Qualitätsaspekte bei

- Entwicklung,
- Konstruktion,
- Verifizierung und
- Änderung

des Produktdesigns.

Bemerkung: „Design“ kann „Entwicklung“, „Berechnung“, „Konstruktion“ bzw. deren Ergebnis, „Entwurf“, „Gestaltung“ oder „Konzept“ usw. einschließen und entsprechend benannt werden.

5. Lenkung der Dokumente

Anweisungen über

- Erstellung,
- Verteilung,
- Änderung,
- Archivierung usw.

wichtiger Dokumente.

6. Beschaffung

Qualitätssicherung bei beschafften Produkten durch

- Beurteilen von Unterlieferanten;
- Beschaffungsangaben (klare Beschreibung des bestellten Produktes im Beschaffungsdokument);
- Verifizieren von beschafften Produkten.

7. Vom Auftraggeber bereitgestellte Produkte

Qualitätssicherung für Teile oder Materialien, die zur Mitverarbeitung geliefert werden.

8. Identifikation und Rückverfolgbarkeit von Produkten

Kennzeichnen der Produkte, die es z.B. bei Fehlern erlaubt, den „Werdegang“ zu rekonstruieren.

9. Prozeßlenkung (in Produktion und Montage)

Planen und Festlegen von Produktionsprozessen, welche die Qualität direkt beeinflussen, durch

- dokumentierte Arbeitsanweisungen;
- Überwachung und Lenkung;
- Genehmigung von Prozessen und Einrichtungen;
- Kriterien für die Arbeitsausführung, die in größtmöglichem praktischen Umfang mittels schriftlicher Anweisungen oder typischer Muster vorgegeben werden müssen.

10. Prüfungen

Dokumentierte Eingangs-, Zwischen- und Endprüfungen der Produktqualität.

11. Prüfmittel

- Auswahl,
- Kalibrierung,
- Überwachung und regelmäßige Überprüfung usw.

der Prüfmittel (= Prüfhardware und -software).

12. Prüfstatus

Sicherstellen, daß der Prüfzustand eines Produktes jederzeit erkennbar ist.

13. Lenkung fehlerhafter Produkte

- Identifikation,
- Dokumentation (Erfassung),
- Bewertung (Kennzeichnung) und
- Aussonderung bzw. Weiterbehandlung

der fehlerhaften Produkte.

14. Korrekturmaßnahmen

- Analyse von Fehlerursachen;
- Mängel abstellen und Wiederholungsfehler vermeiden durch
  * Veranlassen von Fehlerverhütungs- und Überwachungsmaßnahmen sowie
  * gegebenenfalls Verfahrensänderungen.

15. Handhabung, Lagerung, Verpackung und Versand

16. Qualitätsaufzeichnungen

Festlegen der zu dokumentierenden Arbeiten und Prüfungen.

17. Interne Qualitätsaudits[1]

Dokumentation der Ergebnisse von Mitarbeiterbefragungen zur Qualität und ihrer Verbesserung (siehe dazu den folgenden Abschnitt 2.2.2.2).

18. Schulung

Vorschreiben der notwendigen Qualifikationen und entsprechende Ausbildung.

19. Kundendienst

- Verfahren zum Ausführen und Aufrechterhalten des Kundendienstes einrichten;
- Verifizieren, daß Kundendienst und Wartungspersonal die festgelegten Anforderungen erfüllen.

20. Statistische Methoden

Verfahren einführen, welche angemessene statistische Methoden bestimmen, die zum Verifizieren der Eignung der Produkte zur Bewältigung der Unternehmensziele erforderlich sind.

2.2.2.2 Qualitätsaudit nach DIN ISO 10 011

Die im vorigen Abschnitt vorgestellte Normenreihe DIN ISO 9000 betont die Bedeutung des Qualitätsaudits als wichtiges Führungsinstrument zur Erreichung der im Rahmen der Politik der Organisation gesteckten Ziele. Daher veröffentlichte das Technische Komitee TC 176 („Quality Management and Quality Assurance“) der ISO mit der Internationalen Norm DIN ISO 10 011 Regeln für Qualitätsaudits.

Definition: *Ein **Qualitätsaudit** ist eine systematische und unabhängige Untersuchung, um festzustellen, ob die qualitätsbezogenen Tätigkeiten sowie die damit zusammenhängenden Ergebnisse den geplanten Vorgaben entsprechen und ob diese Vorgaben effizient verwirklicht und geeignet sind, die Ziele zu erreichen.*

Anmerkung: *Das Qualitätsaudit wird typischerweise auf ein Qualitätssicherungssystem oder Elemente davon, auf Verfahren und auf Dienstleistungen angewendet; es ist jedoch nicht darauf beschränkt; man spricht dann von „Systemaudit“, „Verfahrensaudit“, „Dienstleistungsaudit“.*

Die Norm DIN ISO 10 011 besteht aus drei Teilen:

- **DIN ISO 10 011, Teil 1: „Auditdurchführung“**

  Dieser Teil gibt einen an die Erfordernisse der einzelnen Anwender anpaßbaren Leitfaden für das Durchführen eines Qualitätssicherungssystem-Audits in einer Organisation:

  – *Auditziele:*
    * Verifizieren der Elemente des Qualitätssicherungssystems und deren Wirksamkeit, die festgelegte Qualität zu erzielen mit der Anforderung, das Qualitätssicherungssystem zu verbessern;

[1] audit (lat.) = er/sie/es hört, stellt eine Untersuchung an.

    * Überprüfen der laufenden Erfüllung von Vertragsverhältnissen mit Kunden bzw. Lieferanten.
  - *Aufgaben und Verantwortlichkeiten:*
    * Auditoren (Auditteam, Verantwortlichkeiten des Auditors und des Auditleiters, Unabhängigkeit des Auditors, Tätigkeiten des Auditors);
    * Auftraggeber des Audits;
    * auditierte Organisation.
  - *Auditdurchführung:*
    * Einleiten des Audits (Umfang, Häufigkeit);
    * Vorbereiten des Audits (Auditplan, Aufgabenzuordnung im Auditteam, Arbeitsdokumente);
    * Ausführen des Audits (Einführungsgespräch, Untersuchung, Schlußgespräch);
    * Auditdokumente (Auditbericht, Inhalt des Berichts, Verteilung des Berichts, Aufbewahrung der Unterlagen).
  - *Auditabschluß und Weiterverfolgung von Korrekturmaßnahmen.*

- **DIN ISO 10 011, Teil 2: „Qualifikationskriterien für Auditoren“**

  Damit Audits von Qualitätssicherungssystemen nach DIN ISO 10 011, Teil 1, wirksam und einheitlich durchgeführt werden können, ist für die Qualifizierung der Auditoren das Erfüllen von Mindestkriterien erforderlich, die in diesem zweiten Teil der DIN ISO 10 011 beschrieben werden.

- **DIN ISO 10 011, Teil 3: „Management von Auditprogrammen“**

  Jede Organisation, in der laufend Qualitätssicherungssystem-Audits gemäß den Teilen 1 und 2 der DIN ISO 10 011 durchgeführt werden, sollte einen grundsätzlichen Leitfaden zum umfassenden Management von Qualitätssicherungssystem-Auditprogrammen verwenden, den dieser dritte Teil der DIN ISO 10 011 liefert.

2.2.2.3 Umfassendes Qualitätsmanagement (TQM)

Um ein hohes Perfektionsniveau zu erreichen, ist es notwendig, die Qualitätsaspekte automatisch und von Anfang an mit in den Betriebsablauf einzubeziehen. So entstehen systematische und ganzheitliche Konzepte für das sogenannte *Umfassende Qualitätsmanagement (Total Quality Management, TQM)* ([LUDST 1], [WILDEM]), deren Grundlagen auf vor allem von amerikanischen Wissenschaftlern erarbeitete Theorien der 50er Jahre zurückreichen.

Die Europäische Stiftung für Qualitätsmanagement (European Foundation for Quality Management, EFQM), die von vierzehn europäischen Konzernen im Jahre 1988 gegründet wurde, hat das TQM-Modell ausgearbeitet. Die organisatorischen Grundlagen des Modells stammen von den bereits in Abschnitt 2.2.2.1 auf Seite 13f. vorgestellten DIN-ISO-Normen der Reihe 9000, die vom TQM-Modell um Kriterien bezüglich des wirtschaftlichen Erfolges einer Organisation(seinheit) erweitert werden.

Aus Abbildung 2.2 geht die Gewichtung der anschließend beschriebenen neun Kriterien innerhalb des TQM-Konzeptes hervor:

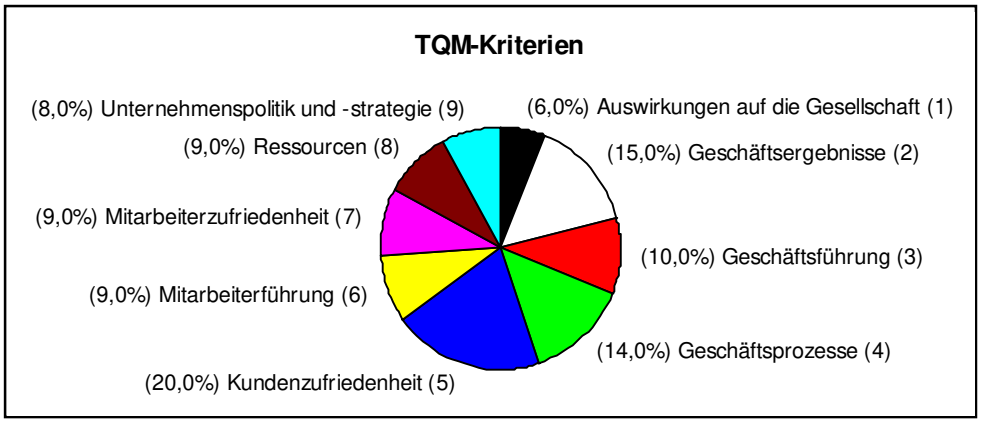

Abbildung 2.2: Gewichtung der TQM-Kriterien

- **Kriterium „Auswirkungen auf die Gesellschaft“ (1)**

  Dieses Kriterium betrifft die erreichten bzw. anvisierten Ergebnisse des unternehmerischen Handelns.

- **Kriterium „Geschäftsergebnisse“ (2)**

  Sowohl finanzielle Resultate als auch andere Kriterien (z.B. Umweltschutz, Marktanteil, Entwicklungs-/Durchlaufzeiten) gehen hier ein.

- **Kriterium „Geschäftsführung“ (3)**

  Art der Initiierung und Durchsetzung des Qualitätsstrebens durch das Management (z.B. mit Hilfe von Benchmarking, d.h. Vergleichen von Schlüsselbereichen des eigenen Unternehmens mit denen der wichtigsten Konkurrenten am Markt).

- **Kriterium „Geschäftsprozesse“ (4)**

  Sämtliche wertschöpfenden Tätigkeiten im Unternehmen (Entwicklung → Fertigung → Service).

- **Kriterium „Kundenzufriedenheit“ (5)**

  Zuverlässigkeit, Langlebigkeit, Wartungsfreundlichkeit, termingerechte Lieferung, Kundendienst usw.; eine unerläßliche Basis für das Erfüllen dieses Kriteriums stellen die Kriterien (6) und (7) dar.

- **Kriterien „Mitarbeiterführung“ (6) und „Mitarbeiterzufriedenheit“ (7)**

  Arbeitsbedingungen, Kommunikation, Leistungsanerkennung, Führungsstil, Aus-/Weiterbildung, Aufgaben-/Verantwortungs-Delegation, Förderung der aktiven Mitwirkung (innerbetriebliches Vorschlagswesen), Informationsaustausch usw.

- **Kriterium „Ressourcen“ (8)**

  Bestmöglicher Einsatz der verfügbaren finanziellen Mittel, Materialien, Informationen, Technologien und Personal.

- **Kriterium „Unternehmenspolitik und -strategie“ (9)**

  Leitbild und Ausrichtung des Unternehmens, das von den Erwartungen der Öffentlichkeit an das Unternehmen beeinflußt wird.

2.2.3 Vom Lokalen Betriebs- zum Verfahrenskonzept

Die Beziehungen und Abhängigkeiten zwischen dem instantiierten Lokalen Betriebskonzept und dem im nächsten Abschnitt besprochenen instantiierten Verfahrenskonzept verdeutlicht Abbildung 2.3:

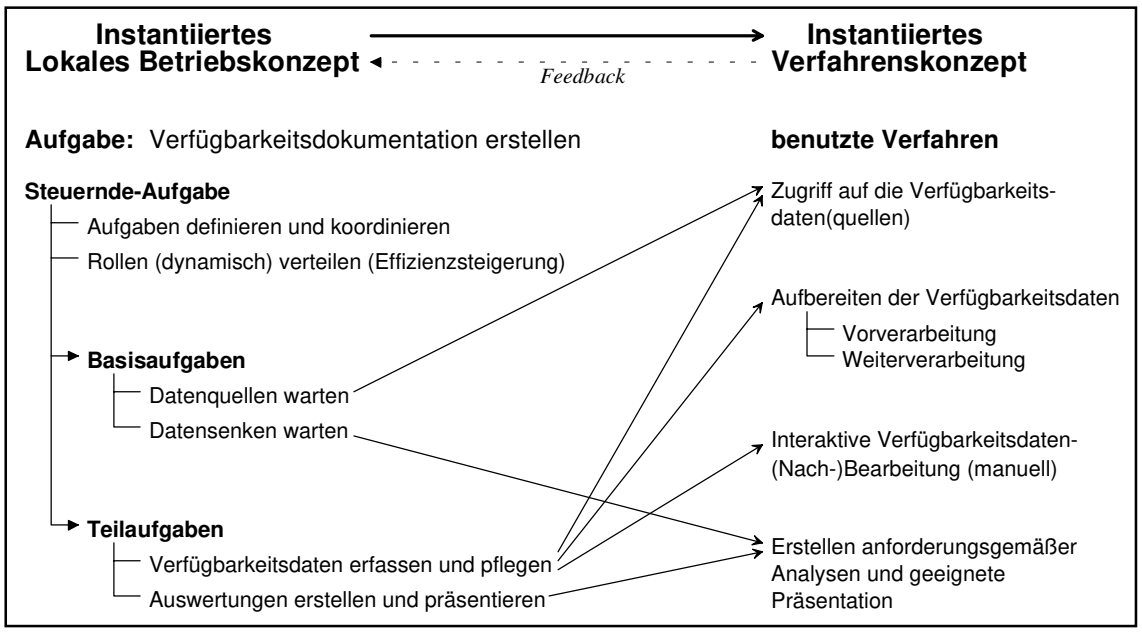

Abbildung 2.3: Beziehungen — Lokales Betriebs- und Verfahrenskonzept

2.3 Das instantiierte Verfahrenskonzept

Im Verfahrenskonzept werden die zur Erledigung der Aufgaben nötigen Verfahren, deren möglichst effektiver Einsatz sichergestellt werden soll, beschrieben.

Verfahren setzen sich aus einer ökonomischen Abfolge von technischen Arbeitsschritten (Tätigkeitsabfolgen, Aktionen) zusammen.

2.3.1 Verfahrensregulierung

Die Aufgabe der Verfahrensregulierung besteht in

- der Auswahl geeigneter lokaler und globaler Verfahren und Bereitstellung konkreter Verfahren;
- dem Festlegen der Zusicherungen, mit denen ein Verfahren abzulaufen hat.

Auf die hierzu nötigen Entscheidungskriterien wird bei den Verfahren, die im folgenden Abschnitt einzeln vorgestellt werden, eingegangen.

Die in der täglichen Arbeit benutzten Verfahren sollten immer in enger Zusammenarbeit mit den Mitarbeitern, die mit diesen Verfahren arbeiten, abgestimmt werden (Rückkopplung, Feedback).

2.3.2 Definition der benutzten Verfahren

Nach der Analyse der Verfügbarkeitsproblematik im LAN- und WAN-Bereich, die mit Hilfe des Rahmenbetriebskonzeptes durchgeführt wurde, sind die hieraus resultierenden vier Verfahren (vergleiche Abbildung 2.1 auf Seite 7) in den folgenden Unterabschnitten detailliert zu beschreiben.

2.3.2.1 Verfahren „Zugriff auf die Verfügbarkeitsdaten(quellen)“

Durch dieses lokale Verfahren wird festgelegt, wie der Export der für die Verfügbarkeitsdokumentation relevanten Daten aus den Datenquellen (Netzmanagementsysteme und Netzdokumentationssysteme) zu realisieren ist.

Die Verfahrensregulierung muß hierbei eine Entscheidung von erheblicher Tragweite fällen, und zwar, ob dieser Export

- rein manuell oder
- vollautomatisiert (Online-Betrieb)

ablaufen soll. Dabei sind die aufgeführten Kriterien zu berücksichtigen:

- Die *geforderte Qualität und Quantität* der exportierten Verfügbarkeitsdaten
  - Aktualität:
    * Relativ große Verzögerung beim manuellen Export;
    * Realzeitdaten beim vollautomatisierten Export.
  - Akzeptierte Fehlertoleranz:

    Je höher der manuelle Anteil am Datenexport, desto größer ist das Risiko von Verfälschungen der Daten aufgrund von Flüchtigkeitsfehlern bei der Eingabe, desto niedriger folglich die erreichbare Qualität.
  - Genehmigte Arbeitszeit:

    Die Arbeitszeit, welche die Mitarbeiter nach Vorgabe der Aufgabenregulierung für die Verfügbarkeitsdokumentation aufwenden dürfen (je weniger Zeit die Mitarbeiter beanspruchen dürfen, umso höher muß die Automatisierung des Exports sein, wenn eine bestimmte Qualität und Quantität erreicht werden soll).

    Beispiel: Je weniger Zeit in den manuellen Export investiert wird (bei vollständigem Verzicht auf einen automatischen Export), desto ungenauer sind die so erfaßten Verfügbarkeitsdaten, da nur noch größere Ausfälle exportiert werden können (z.B. Ausfälle, die länger als 30 Minuten gedauert haben).
- Der *Aufwand*, welcher in die *Implementierung eines Datenexportmoduls* investiert werden darf; hier wird ein Kompromiß zu schließen sein zwischen

- einem einmalig relativ hohen technischen Realisierungsaufwand, der in einem permanenten relativ niedrigen personellen Aufwand resultiert (beim vollautomatisiert ablaufenden Verfügbarkeitsdatenexport, der aufgrund der Menge und der Forderung nach Aktualität der exportierten Daten angestrebt werden sollte);
- einem relativ geringen einmaligen technischen Realisierungsaufwand, der mit einem permanenten hohen personellen Aufwand erkauft wird (beim rein manuell durchgeführten Export).

2.3.2.2 Verfahren „Aufbereiten der Verfügbarkeitsdaten“

Dieses lokale Verfahren legt das *automatische* Aufbereiten der Verfügbarkeitsdaten fest:

- Effiziente sowie flexibel nach den Nutzeranforderungen konfigurierbare *Auswahl und Filterung* der für die Verfügbarkeitsdokumentation relevanten Daten aus dem gewaltigen Strom der von den Datenquellen — insbesondere von den Netzmanagementsystemen — ständig neu eintreffenden Daten (Events);
- *Sortieren* der Daten (z.B. nach Ausfalldatum und -uhrzeit aufsteigend geordnet);
- *Verdichten/Reduzieren* der Daten, um
  - ein sparsames Speichern in Archivtabellen auf dem Sekundärspeicher zu ermöglichen und
  - die interaktive Verfügbarkeitsdaten(nach)bearbeitung (siehe den nächsten Unterabschnitt 2.3.2.3) zu entlasten.

Auch bei diesem Verfahren muß die Verfahrensregulierung einen Kompromiß finden zwischen

- einmaligem Aufwand der Realisierung (Implementierung) und
- permanenten manuellen Aufwand, der sich bei unüberlegt vorgenommenen Einsparungen bei diesem Verfahren besonders nachteilig bei dem im nächsten Unterabschnitt 2.3.2.3 beschriebenen Verfahren bemerkbar macht.

2.3.2.3 Verfahren „Interaktive Verfügbarkeitsdaten(nach)bearbeitung“

Dieses globale Verfahren bestimmt die *manuell* durchzuführenden Maßnahmen zur Verbesserung der Qualität der Verfügbarkeitsdokumentation.

Hierzu gehören:

- Eintragen der Ursache von Ausfällen;
- Erfassen von Zeiten geplanter Ausfälle (z.B. Wartung, Umzüge);
- Behandeln von Sonderfällen (z.B. bestimmte Netzzustände) und Durchführen von manuellen Korrekturen (z.B. bei Störungen des Netzmanagementsystems).

2.3.2.4 Verfahren „Erstellen anforderungsgemäßer Analysen / Präsentation“

Dieses globale Verfahren legt folgendes fest:

- Erstellen geeigneter Auswertungen und Analysen in Form von Tabellen und Diagrammen (Reports), welche die Anforderungen der Empfängerzielgruppen (z.B. „Management“ und „Technik“) erfüllen;
- Verteilen (Zugänglichmachen) der Auswertungen an die Empfänger innerhalb und außerhalb der Netzbetreiberorganisation, wobei die Datenschutz- und Datensicherheitsbestimmungen zu beachten sind.

2.3.3 Vom Verfahrens- zum Werkzeugkonzept

Die Beziehungen und Abhängigkeiten zwischen dem instantiierten Verfahrenskonzept und dem im nächsten Abschnitt besprochenen instantiierten Werkzeugkonzept verdeutlicht Abbildung 2.4:

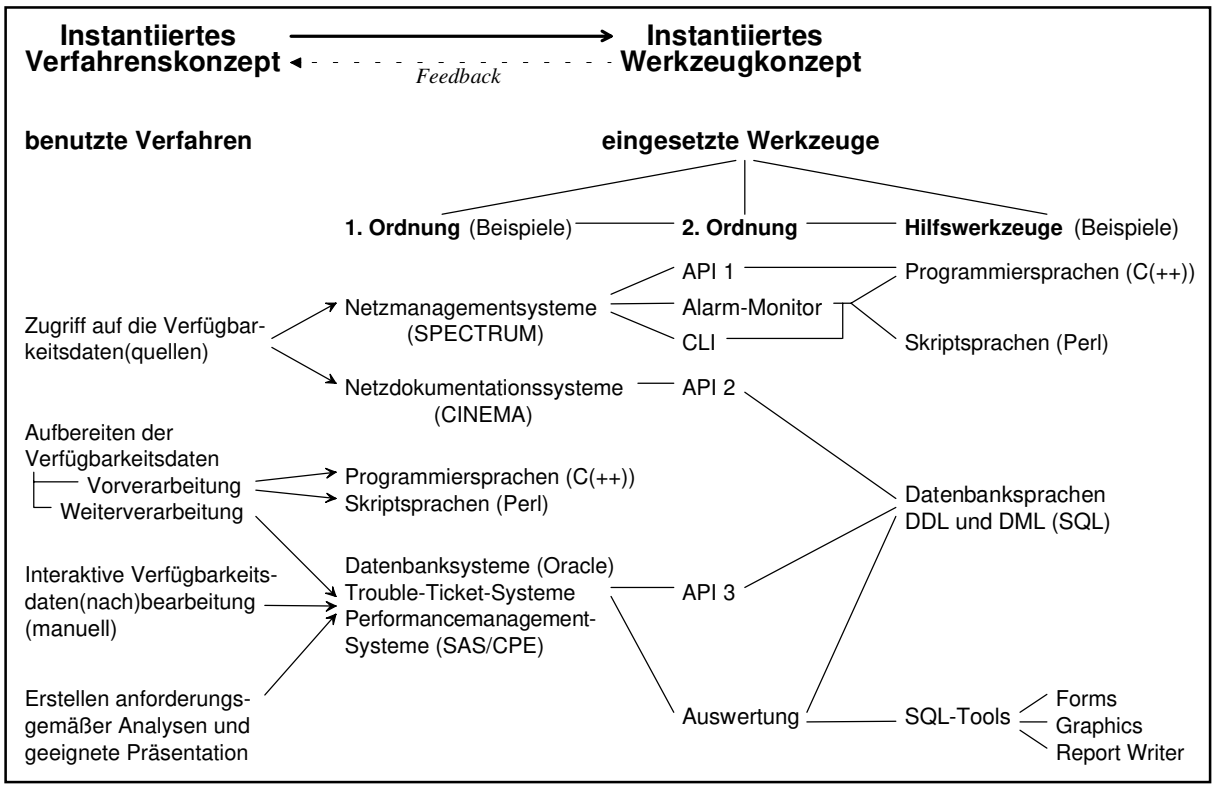

Abbildung 2.4: Beziehungen — Verfahrens- und Werkzeugkonzept

Anmerkungen zu Abbildung 2.4:

1. Verwendete Abkürzungen (in alphabetischer Reihenfolge):
   - API = Application Programming Interface;
   - CLI = Command Line Interface;

- DDL = Data Definition Language (Programmiersprache für die Definition von Datenstrukturen, beispielsweise zum Anlegen von Tabellen);
- DML = Data Manipulation Language (Programmiersprache für den Zugriff auf Datenbestände);
- SQL = Structured Query Language (standardisierte Datenbanksprache, welche die Funktionalität von DDL und DML anbietet).

2. Bei dem unter den untergeordneten Werkzeugen aufgeführten „Alarm-Monitor“ handelt es sich um ein beim Netzmanagementsystem SPECTRUM mitgeliefertes Demonstrationsprogramm — ein Dämonprozeß, der unter Verwendung der API 1 (hier: asynchrones SpectroSERVER-API, SS-API) implementiert wurde.

2.4 Das instantiierte Werkzeugkonzept

Die unterste Ebene des Rahmenbetriebskonzeptes (Abbildung 2.1 auf Seite 7) repräsentiert das Werkzeugkonzept, welches die zur Realisierung der Verfahren eingesetzten Werkzeuge beschreibt.

2.4.1 Werkzeugregulierung

Die Aufgabe der Werkzeugregulierung besteht in der

1. Entscheidung über die einzusetzenden Werkzeuge, die — analog der Verfahrensregulierung — möglichst erst nach Einholen der Meinungen der Mitarbeiter, die mit den jeweiligen Werkzeugen arbeiten, gefällt werden sollte;
2. Bereitstellung aktueller Versionen der Werkzeuge.

Ein grundlegendes Problem für die Werkzeugregulierung ist der obige Punkt 1. Im Rahmen dieser Arbeit kann auf die für eine globale Plattform(System-)Entscheidung erforderlichen Kriterien und Anforderungen nur am Rande eingegangen werden, da hierzu eine genaue Evaluierung und Gegenüberstellung einer möglichst großen Anzahl marktgängiger Produkte erforderlich ist (vergleiche dazu den Abschnitt „Weitere Arbeiten“ auf Seite 114); vielmehr soll anschließend auf zwei grundsätzliche Implementierungsalternativen hingewiesen werden.

2.4.2 CLI-Ansatz versus API-Ansatz

Wie aus Abbildung 2.4 hervorgeht, lassen sich als Werkzeuge (2. Ordnung) für die Integration (Kopplung) von Netzmanagementsystemen mit anderen Plattformen (Systemen, Produkten), die im Rahmen der Erstellung einer Verfügbarkeitsdokumentation durchzuführen ist,

- ein Command Line Interface (CLI) oder
- ein Application Programming Interface (API)

einsetzen; diese Werkzeuge basieren auf zwei grundsätzlichen implementierungstechnischen Alternativen ([LEWIS]), nämlich

- dem Command-Line-Interface-Ansatz (CLI-Ansatz) und
- dem Application-Programming-Interface-Ansatz (API-Ansatz),

die im folgenden erläutert und bewertet werden sollen.

2.4.2.1 Der CLI-Ansatz

Beim CLI-Ansatz werden die eingesetzten Systeme über die Kommandozeile integriert, d.h. ein Systemkommando kann über die Befehlszeile so einfach wie ein UNIX-Befehl eingegeben werden.

Beispiel: Beim Netzmanagementsystem SPECTRUM (vergleiche [SPEC_C]) bewirkt der CLI-Befehl `show alarms` im Erfolgsfalle die Ausgabe aller aktiven Alarme auf STDOUT und den Rückkehrcode 0, während bei einem Fehler die Fehlermeldung auf STDERR gedruckt wird und der Rückkehrcode ungleich 0 ist.

1. Voraussetzungen des CLI-Ansatzes

Jedes zu integrierende System muß

- über einen Satz von Prozeduren verfügen, welche den Betrieb des Systems von der Kommandozeile aus erlauben;
- Anbindungsmöglichkeiten anbieten, welche die Ausführung einer Prozedur vom Produkt selbst aus erlauben.

2. Vorteile des CLI-Ansatzes

- CLI ist häufig ein Bestandteil der Grundausstattung eines Systems;
- Prozeduren können in jeder Programmiersprache (C(++), Prolog, Skriptsprachen usw.) geschrieben werden;
- Prozeduren können einzeln getestet und ausgeführt werden;
- relativ kurze Einarbeitungszeiten;
- relativ schnelle Erstellung von Prototypen (dies gilt nach den bisherigen Erfahrungen des Autors — vergleiche [EGERER] — besonders dann, wenn Skriptsprachen wie z.B. Perl für die Implementierung verwendet werden);
- relativ geringe (finanzielle) Verluste, falls ein Projekt aufgegeben werden sollte.

3. Nachteile des CLI-Ansatzes

- Gefahr einer zu niedrigen Performance in gewissen Anwendungen;
- der Integrationsgrad wird durch den in jedem System vorhandenen Satz von Prozeduren und Anbindungsmöglichkeiten begrenzt;
- Problematik von Datensicherheit und Datenschutz.

2.4.2.2 Der API-Ansatz

Beim API-Ansatz erfolgt die Integration der eingesetzten Systeme über den Quellcode, d.h. für Entwurf und Implementierung der Integrationssoftware werden die zu jedem System mitgelieferten bzw. als Zusatz erhältlichen Module und Funktionen verwendet.

1. **Anforderungen des API-Ansatzes**

   Jedes zu integrierende System muß

   – über eine API verfügen, wobei heute die meisten Anwendungen auf der Programmiersprache C(++) basieren,

   – oder eine vergleichbare Schnittstelle anbieten, deren Prozeduren auf eine möglichst unkomplizierte Art und Weise in C(++)-Code eingebettet werden können.

   Beispiel: Embedded SQL.

2. **Vorteile des API-Ansatzes**

   – Die optimale Performance kann erreicht werden;

   – der Integrationsgrad ist nicht durch die vorhandenen Prozeduren und Anbindungsmöglichkeiten begrenzt;

   – Datensicherheit und Datenschutz können je nach Erfordernis berücksichtigt und realisiert werden.

3. **Nachteile des API-Ansatzes**

   – API ist nicht immer ein Bestandteil der Grundausstattung eines Systems und muß dann zusätzlich erworben werden;

   – für die API ist ein dazu kompatibler Compiler erforderlich, der eventuell ebenfalls gekauft werden muß;

   – die zu integrierenden Systeme müssen kompatible APIs aufweisen;

   – relativ lange Einarbeitungszeiten;

   – relativ lange Entwicklungszeiten;

   – relativ hohe (finanzielle) Verluste bei Aufgabe eines Projektes.

2.4.2.3 Folgerung und Empfehlung

Aufgrund der aufgeführten Vor- und Nachteile des CLI- bzw. API-Ansatzes sollte bei der Entwicklung von Integrationssoftware versucht werden, das Beste der beiden Ansätze zu kombinieren, indem man dabei folgende Vorgehensweise wählt:

1. Zunächst sollte mit Hilfe des CLI-Ansatzes ein Prototyp entwickelt werden, falls nicht schon von vornherein feststeht, daß die benötigte Funktionalität oder Performance mit den zur Verfügung stehenden CLI-Befehlen nicht erreichbar ist.

2. Falls der CLI-Prototyp erstellt wurde und sich erst dann zeigt, daß er keine befriedigende Performance oder Funktionalität aufweist, so kann die für ihn bereits erarbeitete Softwarespezifikation zumindest als Grundlage für das Erstellen einer effizienteren Integrationssoftware dienen, die auf dem API-Ansatz basiert.

2.4.3 Definition der eingesetzten Werkzeuge

Wie aus Abbildung 2.1 auf Seite 7 hervorgeht, werden im Werkzeugkonzept drei wesentliche Werkzeug(gruppen) eingesetzt.

2.4.3.1 Werkzeug „Datenquellen“

Hierzu gehören

1. *Netzmanagementsysteme* zur Bereitstellung der Verfügbarkeitsdaten, die eine exakte Berechnung der Ausfalldauer und deren problemlose Zuordnung zu den betroffenen Geräten erlauben müssen:
   – Fehlerinformation (Zeitangaben, Fehlersymptom);
   – Netzkomponenten-Identifikationsinformation.
2. *Netzdokumentationssysteme* zur topologischen Zuordnung der Verfügbarkeitsdaten (z.B. von einem Ausfall betroffene Orte) und als Lieferant zusätzlicher Informationen über das Netz und seine Komponenten (z.B. Komponentenhersteller, Netztyp).

Anmerkung zu 2.:

Ein von BMW im Jahr 1988 selbst entworfenes und seitdem ständig weiterentwickeltes Werkzeug für

- Netzdokumentation,
- Problemmanagement,
- Installationssteuerung und
- Umzugsmanagement

ist das „CINEMA“-System (computer integrated network management and administration[1], [CINEMA]), das aufgrund seiner existentiellen Bedeutung für einen geordneten Netzbetrieb bei BMW im folgenden kurz charakterisiert werden soll:

a) Technische Spezifikation von CINEMA:
   – Verwendung des Standard-Datenbanksystems Oracle (Version 6);
   – Hardware: VM-Host-Rechner;
   – DDL/DML: Standard-SQL;
   – Datensicherung: regelmäßig durchgeführt;
   – Zugang: X11 mit 3270-Emulation für die bei BMW noch sehr verbreitet eingesetzten Text-Terminals;
   – Implementierung: Programmierwerkzeug mit Oracle-API (REXX mit Pro*REXX).

b) Grundsätzliche Kriterien bei der Entwicklung dieses leistungsfähigen Werkzeugs:
   – alle Netztopologien in einem Werkzeug abbilden;

[1] Zuerst war „CINEMA“ die Abkürzung für „computer integrated network management“.

- Redundanz vermeiden;
- „Zettelwirtschaft“ ablösen;
- „Wanninger-Effekt“ durch effizientes Weiterleiten (Routen) von Störungsmeldungen vermeiden;
- allgemein: bessere Transparenz.

2.4.3.2 Werkzeug „Datensenken und Präsentation“

Hierzu gehören

- Datenbanksysteme,
- Trouble-Ticket-Systeme und
- Performancemanagement-Systeme,

die zur

- Speicherung (Archivierung),
- interaktiven (Nach-)Bearbeitung und
- Darstellung (Präsentation)

der aufbereiteten Verfügbarkeitsdaten gemäß den Anforderungen der Nutzer an eine Verfügbarkeitsdokumentation eingesetzt werden.

2.4.3.3 Werkzeug „Programmiersprachen“

Mit diesem Werkzeug werden Schnittstellen implementiert für

- den geeigneten Zugriff auf die Werkzeuge,
- die Vorverarbeitung der von den Datenquellen bereitgestellten Verfügbarkeitsdaten und
- die notwendige Integration der Werkzeuge.

Die Werkzeugregulierung bestimmt hierbei die einzusetzende(n) Programmiersprache(n), wobei sie bei ihrer Entscheidung die folgenden Punkte berücksichtigen sollte:

- den gewählten Implementierungsansatz (vergleiche dazu die Unterabschnitte „Der CLI-Ansatz“ auf Seite 24 und „Der API-Ansatz“ auf Seite 25) als ein primäres Kriterium für die Wahl der Programmiersprache;
- die Verbreitung und den Bekanntheitsgrad einer Programmiersprache im Unternehmen (wichtig für die spätere Pflege und Weiterentwicklung der Software).

  Beispiel: Die aufgrund ihrer Syntax und Semantik für die Verarbeitung von textuellen Daten geeignete Skriptsprache Perl darf bei BMW nicht verwendet werden; es ist mit der im Unternehmen besser bekannten Programmiersprache C(++) zu arbeiten.

3 Anforderungen an eine Verfügbarkeitsdokumentation

In Kapitel 2 wurden bereits die von einer Netzbetreiberorganisation mit einer Verfügbarkeitsdokumentation verfolgten globalen Ziele dargestellt. Dieses Kapitel gliedert diese Ziele und entwickelt daraus sechs wesentliche Anforderungen an eine Verfügbarkeitsdokumentation, die jeweils anhand von Beispielen aus dem Hause BMW konkretisiert werden:

1. Anforderungen der Empfänger (Nutzer) an eine Verfügbarkeitsdokumentation (siehe unten);
2. Anforderungen an die für eine Verfügbarkeitsdokumentation benötigten Daten und Klassifizierung aufgetretener Fehler (Ausfälle) (siehe Seite 32f.);
3. Anforderungen an die eingesetzten Verfügbarkeitsdatenquellen (siehe Seite 37f.);
4. Anforderungen an eine Präsentation (Layout) der Verfügbarkeitsdokumentation (siehe Seite 39);
5. Anforderungen an eine (Verfügbarkeits-)Datenintegration (siehe Seite 39f.);
6. Anforderungen an eine Archivierung der Verfügbarkeitsdaten (siehe Seite 41f.).

3.1 Anforderungen der Empfänger

Die bereits in Abschnitt „Das instantiierte Lokale Betriebskonzept“ auf Seite 9f. dargestellten Ziele der Aufgabe „Verfügbarkeitsdokumentation erstellen“ sollen im folgenden in Form von Anforderungen der dazu in Gruppen mit ähnlichen Bedürfnissen eingeteilten Empfänger (Nutzer) der Verfügbarkeitsdokumentation genauer spezifiziert werden.

Um die realen Bedürfnisse der Empfänger möglichst neutral und unbeeinflußt erfassen zu können, sollten bei deren Befragung eventuelle Einschränkungen technischer bzw. organisatorischer Art (z.B. bezüglich der von Netzmanagementsystemen bereitgestellten Daten bzw. eines erheblichen manuellen (Nach-)Bearbeitungsaufwandes) zunächst unberücksichtigt bleiben (sogenanntes Top-Down-Vorgehen). In der später durchgeführten Realisierungsphase werden die erlangten Erkenntnisse in Anforderungen an Verfahren und Werkzeuge umgesetzt, soweit dies die technischen und organisatorischen Gegebenheiten zulassen (Bottom-up-Vorgehen, Feedback).

Bevor dieses jedoch geschehen kann, muß zunächst die Vielzahl der Empfänger klassifiziert werden, d.h. es sind Zielgruppen zu bilden.

3.1.1 Empfänger-Zielgruppen

Zur Bildung von Empfänger-Zielgruppen kann folgendermaßen vorgegangen werden:

1. Beantworten von Fragen zur Zielgruppenbildung:
   - Welche Personen(gruppen) sind Adressaten der Auswertungen?
   - Welche Gemeinsamkeiten bestehen zwischen diesen Personen (Aufgaben, Ziele)?
2. Befragen repräsentativer Vertreter aller dabei ermittelten Zielgruppen nach ihren Ansichten bezüglich des Zwecks der für sie zu erstellenden Auswertungen:
   - Wozu sollen die Auswertungen beitragen?
   - Wozu werden die Auswertungen benötigt?

Das Ergebnis dieser Umfrage könnte wie folgt aussehen:

In größeren Netzbetreiberorganisationen kann im allgemeinen von zwei Zielgruppen ausgegangen werden, die an die Auswertungen völlig unterschiedliche Ansprüche bezüglich Detailliertheit und Komplexität stellen, da sie differierende Ziele verfolgen:

1. **Zielgruppe: „Management“ (= Abteilungsleitung)**

   Forderung einer allgemein verständlichen, schnell zu überblickenden Übersicht (siehe Abschnitt 3.1.3 auf Seite 31).

   Beispiel: Bei BMW umfaßt diese Zielgruppe im wesentlichen den Abteilungsleiter von FI-21, den Hauptabteilungsleiter von FI-2 und den Bereichsleiter von FI.

2. **Zielgruppe: „Technik“ (= Netzbetreiber)**

   Forderung einer detaillierten Darstellung (siehe Abschnitt 3.1.4 auf Seite 31f.).

   Beispiel: Bei BMW umfaßt diese Zielgruppe im wesentlichen die Gruppenleiter von FI-21 (LAN-, WAN-, SNA-Gruppe) und deren Mitarbeiter.

3.1.2 Allgemeine Anforderungen an Auswertungen

Bei der Befragung der Empfänger-Zielgruppen ergaben sich folgende gemeinsame Anforderungen an Auswertungen der Verfügbarkeit:

- Klassifizieren von Fehlerursachen (Näheres dazu im Abschnitt 3.2.3 auf Seite 33f.).
- Monats- und Jahres-Auswertungen sollen automatisch, Tages-Auswertungen dagegen nur auf besonderen Wunsch (z.B. direkt über die eingesetzten Netzmanagementsysteme) erstellt werden.
- Ermöglichen einer Verfügbarkeitsanalyse mit Hilfe von quantitativen Prognosen (z.B. Trendberechnung): siehe dazu den Abschnitt „Mathematische Verfahren zur Verfügbarkeitsanalyse“ auf Seite 61f.).

- Flexible Gestaltung, Modifizierbarkeit, Erweiterbarkeit.
- Berücksichtigen von vorhandenen Backup-Möglichkeiten (redundanten Pfaden).
- Einführen einer *Gewichtungsfunktion* (zur Realisierung siehe den Abschnitt „Definitionen zur Berechnung der physikalischen Verfügbarkeit“ auf Seite 90f.), welche die Vergabe von Prioritäten (z.B. an FDDI-Subnetze, Rechenzentrumsnetze, Servernetze) ermöglicht, um damit deren Bedeutung im Netz in der Verfügbarkeitsdokumentation berücksichtigen zu können:
  - besondere Auswertungen für „gewichtige“ Ports;
  - je eine Darstellung mit und ohne Berücksichtigung der Priorität.
- Neben der Gewichtung soll eine Möglichkeit vorhanden sein, den *Schweregrad* (prozentual, Vorgabe: 100%) gewisser aufgetretener Fehler, d.h. deren Auswirkung auf den Netzbetrieb, individuell einzugeben (zur Realisierung siehe den Abschnitt „Definitionen zur Berechnung der physikalischen Verfügbarkeit“ auf Seite 90f.); dabei sind die in der Definition der Verfügbarkeit genannten zwei Sichten zu unterscheiden:
  a) *Aus Sicht der Benutzer* sind nur die von ihnen feststellbaren Ausfälle interessant, deren Auswirkungen auf den betrieblichen Ablauf — d.h. ihre Schweregrade — zu bewerten sind.

     Beispiel: Auf diese Weise kann bei einem Ausfall berücksichtigt werden, ob eine Backup-Möglichkeit vorhanden und erfolgreich war (z.B. Schweregrad = 50%) oder nicht (Schweregrad = 100%).

  b) *Aus Sicht der Techniker* ist jeder aufgetretene Ausfall mit 100% zu bewerten, unabhängig davon, wie stark die Benutzer von dem Ausfall betroffen sind.
- Spezielle Auswertungen mit Differenzierung zwischen Local- und Remote-Bereich.
- Auswertung der logischen Verfügbarkeit, d.h. Netzstatistiken (wie beispielsweise Auslastung, Fehlerrate): siehe dazu den Abschnitt „Dokumentation der logischen Verfügbarkeit“ auf Seite 99f.
- Die Anzahl der in gewissen Diagrammen darzustellenden Datenreihen sollte begrenzt werden, um die Übersichtlichkeit nicht zu gefährden.

  Beispiel: Auflistung der fünf am häufigsten aufgetretenen Fehler und kumulierte Darstellung aller übrigen Fehler unter dem Punkt „Sonstige“.
- Zusammenfassen (Kumulieren, Verdichten) von zyklischen Ausfällen, das sind Fehler, die sich bei der gleichen Netzkomponente innerhalb einer gewissen, benutzerkonfigurierbaren Zeitspanne (z.B. 60 Sekunden) wiederholen (siehe Abschnitt „Empfehlung zum Realisieren der Realzeit-Verdichtung“ auf Seite 73).
- Gemessenen (tatsächlichen) Werten könnten in den Auswertungen jeweils die geplanten Größen (Sollgrößen, z.B. interessant bei Wartungszeiten) gegenübergestellt werden.

3.1.3 Anforderungen des „Managements“ an Auswertungen

Da sich die Zielgruppe „Management“ aus Zeitgründen im allgemeinen nicht für Einzelheiten interessiert, sind ihr Auswertungen zur Verfügung zu stellen, die einen schnellen Überblick ermöglichen:

- *allgemeine Verfügbarkeitsauswertung:* wesentliche Ausfallursachen mit Differenzierung Local-/Remote-Bereich;
- *Lokalisieren der Ausfälle:* Darstellung der von Ausfällen am meisten betroffenen Orte und Kunden des Netzbetreibers;
- *Gerätespezifizierung:* Hersteller, Typ und Modell der Netzkomponenten, welche die meisten Ausfälle aufweisen.

Das Management soll durch die Verfügbarkeitsdokumentation unterstützt werden bei strategischen Entscheidungen wie:

- Netzinfrastruktur-Investitionen;
- Personaleinsatz für Wartung, Störungsannahme, Reparatur (technischer Kundendienst);
- Vorgaben betreffend den Quality of Service des Dienstes „Bereitstellung/Betrieb LAN (WAN)“, d.h. z.B. eine bestimmte Verfügbarkeit zu erreichen und zu garantieren, Wartungszeiten einzuhalten bzw. zu verringern.

Weitere Ziele sind:

- Vermeiden von Produktivitätseinbußen durch Einschränkungen der logischen Verfügbarkeit (z.B. Engpässe im Netz);
- Vermeiden von Wiederholungsfehlern (z.B. durch Dynamisieren der Wartungsintervalle);
- Verifizierbarkeit des Einhaltens der mit den Kunden geschlossenen Verträge (vergleiche dazu den Abschnitt „Ziele der Aufgabe“ auf Seite 10f.).

3.1.4 Anforderungen der „Technik“ an Auswertungen

Die Zielgruppe „Technik“ erhält alle obigen Auswertungen und zusätzlich solche, die mehr technische Details enthalten:

- **Bereich physikalische Verfügbarkeit**
  - Prozentualer Anteil einzelner Fehler an der gesamten Ausfallzeit.
  - Verfügbarkeit bestimmter zu Gruppen zusammenfaßbarer Router und Ports:
    * Verfügbarkeit des FDDI-Backbones, d.h. Verfügbarkeit der FDDI-Brouter-Ports;
    * Verfügbarkeit des Local-Bereiches (z.B. Ethernet-, Token-Ring- und FDDI-Brouter-Ports);
    * Verfügbarkeit des Remote-Bereiches (z.B. serielle Brouter-Ports);
    * Verfügbarkeit der Token-Ring-Anbindungen.

  - MTBF (Mean Time Between Failures) für bestimmte Netzkomponenten.
  - MTTR (Mean Time To Repair) für bestimmte Netzkomponenten.
  - Darstellung der am häufigsten auftretenden Fehler.
  - Darstellung der häufigsten Fehler der von Ausfällen am meisten betroffenen Orte.
  - Bereitstellung von Ausfalldaten für Wartung und Reparatur.
  - Übersicht über durchschnittliche Dauer und Anzahl der aufgetretenen Ausfälle.
- **Bereich logische Verfügbarkeit**
  - Spitzenauslastung.
  - Statistische Daten einzelner Router/Ports.

3.2 Anforderung: benötigte Verfügbarkeitsdaten

Dieser Abschnitt behandelt die für eine Verfügbarkeitsdokumentation erforderlichen Daten. Dazu gehören nach der Definition der Verfügbarkeit in Abschnitt 1.2 auf Seite 3f.

1. Daten der physikalischen Verfügbarkeit und
2. Daten der logischen Verfügbarkeit.

Vervollständigt wird ein Verfügbarkeitsdatenbestand schließlich mit

3. Daten über aufgetretene Fehler und deren Klassifizierung.

3.2.1 Daten der physikalischen Verfügbarkeit

Für die Dokumentation der physikalischen Verfügbarkeit werden die folgenden Daten benötigt, um die Anforderungen der Zielgruppen zu erfüllen:

- **Ausfall-/Fehlerinformation**
  - Exakte Zeitangaben (Beginn, Ende, Dauer).
  - Eindeutig differenzierte Fehlersymptome.

    Beispiele: – Link-down- und Link-up-Trap von einem Brouter;
    – Contact-lost- und Contact-Meldung eines Netzmanagementsystems.
  - Genaue Spezifikation der Ursache für einen Ausfall einer Netzkomponente (in Form eines Zahlencodes, um eine spätere Auswertung zu erleichtern).

    Beispiele: Stromausfall, Wartung, defekte Kabelverbindung.
- **Identifikationsinformation**

  Genaue Spezifikation der ausgefallenen Netzkomponente.

  Beispiel: – Name der ausgefallenen Komponente (z.B. erhältlich über einen Domain Name Service);
  – bei Ports zusätzlich eine Port-Identifizierung.

- **Zusätzliche Netzdokumentationsinformation**

  Zusatzinformationen für die spätere Auswertung:

  – Topologieinformation.

    Beispiele: – Standort der ausgefallenen Komponente;
    – an die ausgefallene Komponente angeschlossene Orte;
    – vom Ausfall der Komponente betroffene Kunden des Netzbetreibers.

  – Zusätzliche Komponenteninformation.

    Beispiele: – Hersteller, Typ und Modell der ausgefallenen Komponente;
    – Gewichtung (Priorität) der Komponente;
    – Gruppierungsinformation (z.B. Gruppen Ethernetkomponenten, FDDI usw.).

Zur Berechnung der physikalischen Verfügbarkeit siehe Abschnitt „Dokumentation der physikalischen Verfügbarkeit“ auf Seite 90f.

3.2.2 Daten der logischen Verfügbarkeit

Die zur Ermittlung der logischen Verfügbarkeit nötigen Informationen lassen sich einerseits in ausschließlich manuell zu erfassende Daten und andererseits in vollständig automatisch generierte Daten gliedern:

- **Manuell zu erfassende Daten**

  Dazu gehören bestimmte Qualitätskriterien des Netzes, deren Erhebung

  – aufgrund ihres teilweise subjektiven Charakters (z.B. Antwortzeiten) oder

  – aus technischen Gründen (z.B. Protokollprobleme)

  nicht automatisiert werden kann.

- **Automatisch generierte Daten**

  Die zu dieser Gruppe gehörenden Gerätestatistiken (geräteinterne Zähler und Werte), die von gewissen Netzkomponenten selbständig geführt werden, können mit Hilfe von Netzmanagementsystemen abgefragt werden. Wichtig bei diesen Daten ist, eine geeignete Auswahl aus der Vielzahl der z.B. in einer Geräte-MIB (vergleiche etwa [CISCO 1]) enthaltenen Attribute zu treffen, um eine ressourcenschonende Auswertung und Archivierung zu erreichen.

Zur Berechnung der logischen Verfügbarkeit siehe den Abschnitt „Dokumentation der logischen Verfügbarkeit“ auf Seite 99f.

3.2.3 Daten über aufgetretene Fehler (Ausfallursachen)

Fehler(ursachen) stellen eine sehr wichtige Information dar, die aus einer Verfügbarkeitsdokumentation hervorgehen muß. Sie ist manuell nachzutragen (siehe dazu den Abschnitt „Realisierung: die interaktive Daten(nach)bearbeitung“ auf Seite 78f.), da sie von den Netzmanagementsystemen nicht in ausreichendem Maße geliefert wird.

Sie kann

- von der Abteilungsleitung (Management) etwa als Indikator für die Effektivität der Wartung oder für die Zuverlässigkeit bestimmter Netzkomponenten und
- vom Wartungs- und Reparaturpersonal (Technik) beispielsweise für Pflege- bzw. Instandsetzungsmaßnahmen

genutzt werden.

Es gibt bereits einige Definitionen von Fehler(ursachen) in Internationalen Standards der ISO[1] und der CCITT[2]. Die CCITT ist ein permanentes Organ der ITU[3], welche die auf dem Gebiet der Telekommunikation spezialisierte Agentur der Vereinten Nationen ist. Etwa 166 Mitgliedsländer, 68 Telekommunikationsunternehmen, 163 wissenschaftliche und industrielle Organisationen und 39 internationale Organisationen nehmen an der Körperschaft CCITT teil, die weltweit Telekommunikationsstandards — sogenannte Empfehlungen (Recommendations) — veröffentlicht und dabei mit der ISO und der IEC[4] zusammenarbeitet.

Der Internationale Standard [ISO/IEC 10 164-4] (identisch mit der CCITT-Empfehlung [X.733]) definiert:

Error: *Abweichung eines Systems vom normalen Betrieb.*

Fault: *Fehlfunktion/Defekt mit Hardware- oder Software-spezifischen Ursachen.*

Alarm: *Eine Benachrichtigung über einen bestimmten Vorfall; ein Alarm kann — muß aber nicht — einen Error repräsentieren.*

3.2.3.1 Alarm-Basiskategorien nach ISO/IEC 10 164-4

Die im M-EVENT-REPORT-Service in ISO/IEC 9595 allgemein definierten Parameter

- Event Type,
- Event Information und
- Event Reply

werden in [ISO/IEC 10 164-4] detailliert beschrieben; im Rahmen einer Verfügbarkeitsdokumentation sind davon für eine Fehlergrobklassifikation, unter die alle Ausfallursachen eingeordnet werden können, die folgenden interessant:

- Event Type: Definition von fünf Alarm-Basiskategorien;
- Event Information:
  - mögliche Fehlerursache (probable cause),

---

1 International Organization for Standardization.

2 Commité Consultatif International de Télégraphique et Téléphonique.

3 International Telecommunication Union.

4 International Electrotechnical Commission

– Fehler-Schweregrad (perceived severity).

Unerläßlich ist jedoch ein Erweitern (Detaillieren) und Klassifizieren der auftretenden Fehler (Ausfallursachen) mit Vergabe von hierarchisch aufgebauten Fehlercodes. Beim kontinuierlichen Vervollständigen des dabei entstehenden Katalogs müssen alle an der Verfügbarkeitsdokumentation beteiligten Gruppen intensiv mitarbeiten — ein Beispiel für einen auf diese Weise für die BMW-Umgebung erstellten Fehler(ursachen)katalog ist im Abschnitt „Fehlerklassifizierung“ auf Seite 78f. ausgeführt.

Die fünf Alarm-Basiskategorien nach [ISO/IEC 10 164-4]

1. Communications Alarm Type

– Ein Alarm dieses Typs ist hauptsächlich mit den Prozeduren und/oder Prozessen assoziiert, die für den Informationstransport von einem Punkt zum anderen benötigt werden.

– Hier lassen sich unter anderem Fehler einordnen, welche die logische Verfügbarkeit betreffen, beispielsweise Protokollfehler.

– Weitere Beispiele für mögliche Fehlerursachen (aus [ISO/IEC 10 164-4]):

  Verlust des Signals, Verlust eines Pakets, fehlerhaftes Paket, Übertragungsfehler des lokalen/remoten Knotens, Fehler beim Verbindungsaufbau, schlechtes Signal, Kommunikationssubsystemfehler, Kommunikationsprotokollfehler, DTE-DCE-Interface-Fehler, LAN-Fehler.

2. Quality of Service Alarm Type

– Ein Alarm dieses Typs ist hauptsächlich mit einer Verringerung der Qualität eines Services assoziiert.

– Hier lassen sich unter anderem Fehler einordnen, welche die logische Verfügbarkeit betreffen, insbesondere statistische Daten von Geräten, die benutzerdefinierte Qualitätsanforderungen unterschreiten.

– Weitere Beispiele für mögliche Fehlerursachen (aus [ISO/IEC 10 164-4]):

  Antwortzeit zu lang, Warteschlangengröße überschritten, Bandbreite reduziert, Rate der Wiederholungsübertragungen übermäßig, Schwellwert überschritten, Performance schlecht, Überfüllung, Ressource nähert sich oder ist an der Kapazitätsgrenze.

3. Processing Error Alarm Type

– Ein Alarm dieses Typs ist hauptsächlich mit einer Software- oder Verarbeitungs-Fehlfunktion assoziiert.

– Hier lassen sich unter anderem Fehler einordnen, welche die logische Verfügbarkeit betreffen, insbesondere Softwareprobleme und manuelle Eingriffe in den Netzbetrieb (z.B. Reboot eines Brouters).

– Weitere Beispiele für mögliche Fehlerursachen (aus [ISO/IEC 10 164-4]):

  Speicherplatzproblem, Version paßt nicht, beschädigte Daten, CPU-Zeitlimit überschritten, Softwarefehler, Dateifehler, Speicher erschöpft, zugrunde liegende Ressource nicht verfügbar, Anwendungssubsystemfehler, Konfigurations- oder Anpassungsfehler.

4. Equipment Alarm Type

- Ein Alarm dieses Typs ist hauptsächlich mit einer Hardware-Fehlfunktion assoziiert.
- Hier lassen sich unter anderem Fehler einordnen, welche die physikalische Verfügbarkeit betreffen.
- Weitere Beispiele für mögliche Fehlerursachen (aus [ISO/IEC 10 164-4]):

  Problem mit der geräteinternen Stromversorgung, Timing-Problem, Prozessor-Problem, Dataset- oder Modemfehler, Multiplexerproblem, Empfängerstörung, Überträgerstörung, Empfangsfehler, Übertragungsfehler, Ausgabegerätfehler, Eingabegerätfehler, I/O-Gerätfehler, Gerätestörung, Adapterfehler.

5. Environmental Alarm Type

- Ein Alarm dieses Typs ist hauptsächlich mit dem Zustand der Umwelt assoziiert, in der sich die betroffene Hardware befindet.
- Hier lassen sich unter anderem willkürliche (geplante) Ausfälle wie Umbau, Umzug und Wartung einordnen.
- Weitere Beispiele für mögliche Fehlerursachen (aus [ISO/IEC 10 164-4]):

  Temperatur inakzeptabel, Luftfeuchtigkeit inakzeptabel, Heizungs-/Ventilations-/Kühlungssystemproblem, Feuer festgestellt, Überflutung festgestellt, Auslaufen (von Giftstoffen) entdeckt, Druck inakzeptabel, übermäßige Erschütterung, Materialversorgung erschöpft, Pumpe versagt, Absperrtür offen.

Die sechs Fehler-Schweregrade (perceived severity) nach [ISO/IEC 10 164-4]

Der Internationale Standard definiert sechs Fehler-Schweregrade (cleared, indeterminate, critical, major, minor und warning), die als teilweise subjektive Komponente über die interaktive Nachbearbeitung in die Verfügbarkeitsstatistiken eingehen können.

Um derartige Schweregrade mathematisch-statistisch erfassen zu können, ist die Abbildung z.B. auf eine Prozentzahl, also eine prozentuale Bewertung der einzelnen Fehler-Schweregrade erforderlich. Diese Abbildung hat allerdings den Nachteil, subjektiv zu sein.

3.2.3.2 Anforderungen an die Alarm-Behandlung nach ISO/IEC 10 164-5

Der Internationale Standard [ISO/IEC 10 164-5] enthält bereits fünf Anforderungen an die Behandlung von Alarmen:

1. Definition einer flexiblen Alarm-Kontrollinstanz, welche die Auswahl von Alarmmeldungen und deren Weiterleitung an bestimmte Managementsysteme erlaubt;
2. Spezifizieren der Empfänger, an welche die Alarmmeldungen gesendet werden sollen;
3. Spezifizieren eines Mechanismus, um die Alarm-Weiterleitung zu kontrollieren;
4. Veränderbarkeit der Initiierungs- und Weiterleitungsbedingungen von Alarmen durch externe Managementsysteme;
5. Lokalisierbarkeit einer Stelle, zu der Alarmmeldungen gesendet werden können, falls die ursprünglich dafür vorgesehene Stelle nicht verfügbar ist.

3.3 Anforderung: benötigte Datenquellen

Die folgenden drei Unterabschnitte beschreiben verschiedene Möglichkeiten („Datenquellen“), mit deren Hilfe Verfügbarkeitsdatenbestände aufgebaut und gepflegt werden können.

Dabei handelt es sich um die folgenden Datenquellen:

1. Netzmanagementsysteme,
2. Netzdokumentationssysteme,
3. manuelle Eingaben.

3.3.1 Netzmanagementsysteme

Für Netzmanagementsysteme gibt es im wesentlichen zwei Verfahren, um den Netzstatus (physikalische und logische Verfügbarkeit) bzw. sonstige statistische Daten (logische Verfügbarkeit) zu erfassen.

Nr.	Verfügbarkeitsinformation	Beispiel der Repräsentation durch Netzmanagementsysteme	Datenerfassungsverfahren
i)	Störung eines Geräteports	Link-down-Trap*	1.
ii)	Störung eines Gerätes	Contact-lost-Meldung*	2a)
iii)	Attribute aus der Geräte-MIB (logische Verfügbarkeit)	If_In_Octets, If_Out_Octets (= Gesamtanzahl der empfangenen bzw. übertragenen Bytes)	2b)
iv)	Überschreiten eines Schwellwertes (logische Verfügbarkeit)	Schwellwert-Trap*	1. bzw. 2b)

* je nach den benutzten Netzmanagementsystemen generieren diese (wie z.B. SPECTRUM) außerdem noch einen speziellen Alarm

Abbildung 3.1: Repräsentation der Verfügbarkeitsinformation

1. Passives Erfassen des Netzzustandes (physikalische und logische Verfügbarkeit)

Registrieren der von den Geräten gesendeten Traps; dabei wird heute meist — insbesondere bei neueren Geräten — das Simple Network Management Protocol (SNMP, [RFC 1157]) verwendet.

2. Aktives Erfassen

a) *Aktives Erfassen des Netzzustandes (physikalische Verfügbarkeit):*

Netzmanagementsysteme können ständig „Umfragen“, sogenanntes Polling, durchführen, um festzustellen, ob alle überwachten Geräte noch arbeiten; dabei wird an die Agenten dieser Geräte eine Anfrage gesendet, die von diesen zu beantworten ist.

Da das Polling die Netzlast beträchtlich erhöhen kann, hat der Netzadministrator die Möglichkeit festzulegen, ob überhaupt bzw. in welcher Frequenz „gepollt“ werden soll (Pollingzyklus).

Beispiel: jedes Gerät wird einmal pro Minute abgefragt.

b) *Aktives Erfassen sonstiger statistischer Daten (logische Verfügbarkeit):*
Netzmanagementsysteme ermitteln mit Hilfe des Pollings auch die Werte bestimmter Attribute aus der in [RFC 1213] veröffentlichten Standard-MIB[1] (z.B. Auslastung, Durchsatz) und/oder herstellerspezifischer MIBs[2] der überwachten Geräte.

Die mit Hilfe der oben aufgeführten Verfahren 1., 2a) und 2b) erfaßten Informationen können durch Netzmanagementsysteme, wie in Abbildung 3.1 dargestellt, repräsentiert werden.

3.3.2 Netzdokumentationssysteme

Netzdokumentationssysteme sind spezielle Datenbanksysteme, die zum Erfassen, Darstellen und Verwalten der physischen Infrastruktur eines Kommunikationsnetzes eingesetzt werden. Bei den gespeicherten Daten handelt es sich um für einen längeren Zeitraum unveränderliche Informationen über das Netz, die in der Regel manuell gepflegt werden (in [EGERER] ist ein technischer Ansatz zur automatisierten Integration der Daten des Netzdokumentationssystems CINEMA und der des Netzmanagementsystems SPECTRUM beschrieben).

Für die Verfügbarkeitsdokumentation sind im wesentlichen die folgenden Daten aus den Netzdokumentationssystemen relevant:

- Netzdokumentationsdaten zur allgemeinen Erläuterung und Übersetzung der technischen Daten in allgemein verständlichen Klartext (z.B. Übersetzen von IP-Adressen in die von einem Domain Name Service gelieferten Komponentennamen).
- Topologieinformation:
  - Beschreibung der Örtlichkeiten, an denen Netzkomponenten zu finden sind;
  - an eine Komponente angeschlossene Orte und Kunden.
- Zusätzliche Komponenteninformation: z.B. Hersteller, Netztyp.
- Zusätzliche Steuer- und Konfigurationsinformation für die Verfügbarkeitsdokumentation.

3.3.3 Manuelle Eingaben

Um zuverlässige und vollständige Verfügbarkeitsdatenbestände zu erhalten, ist ein nicht zu vernachlässigender Anteil von Eingaben manuell zu erledigen:

- *Nachtragen analyserelevanter Daten*, die nicht durch die bereits beschriebenen Datenquellen (Netzmanagement- und Netzdokumentationssysteme) automatisiert erhältlich sind; dazu gehören
  - Klassifizierung der Ausfallursachen;

---

[1] Bei dieser **MIB (Management Information Base)**, die auch kurz als **MIB-II** bezeichnet wird, handelt es sich bereits um die zweite veröffentlichte Version, welche die erste, zehn Monate zuvor als RFC 1158 veröffentlichte, Standard-MIB für das Internet-Management ersetzt.

[2] Gemeint sind hier sogenannte **Enterprise MIBs** wie z.B. [CISCO 1], die für Netzmanagementsysteme, welche nicht vom Hersteller des überwachten Gerätes selbst unterstützt werden, leider nur schwer, d.h. meist erst mit (großer) zeitlicher Verzögerung, zugänglich sind.

  - Zeiten geplanter Ausfälle (z.B. Umzüge, Wartung).

- *Berücksichtigen von Sonderfällen*, also besonderen Netzzuständen, die zu einer Verfälschung der automatisiert aus dem Netz gewonnenen Verfügbarkeitsdaten führen, durch manuelle Korrekturen (siehe dazu den Abschnitt „Sonderfälle“ auf Seite 53f.).

3.4 Anforderung: Präsentation und Layout der Dokumentation

Nachdem die wesentlichen Anforderungen an eine Verfügbarkeitsdokumentation bestimmt sind, können jetzt detailliertere Anforderungen an Präsentation und Layout der zu erstellenden Auswertungen ermittelt werden.

Dazu sollten die folgenden Fragen beantwortet werden:

- *Zum Inhalt der Auswertungen:*
  - Welche Informationen sollen die Auswertungen enthalten?
  - Wieviel Datenreihen sollen gleichzeitig dargestellt werden?
  - Wie ausführlich sollen Legenden und Beschriftungen (z.B. Kommentartexte) sein?
  - Sind zusätzliche Beschriftungen in den Diagrammen vorgesehen?
- *Zum Layout der Auswertungen:*
  - Welche Art von Diagrammen (Kreis-, Linien-, Säulendiagramme usw.) wird bevorzugt?
  - Können zur Unterscheidung einzelner Datenreihen innerhalb eines Diagramms verschiedene Farben verwendet werden (stehen Farbdrucker und Farbbildschirmgeräte zur Verfügung) oder sind Schwarz-weiß-Graphiken mit unterschiedlichen Schraffuren und/oder Grautönen bzw. Linienarten zu erstellen?

3.5 Anforderung: Datenintegration

Bei großen Netzbetreiberorganisationen gibt es mindestens drei verschiedene Organisationseinheiten (bei BMW handelt es sich z.B. um LAN-, WAN- und SNA-Gruppe sowie Störungsannahme), die sich im Bereich des Problemmanagements mit dem Thema Verfügbarkeit beschäftigen und daher auch mit Verfügbarkeitsdatenbeständen zu tun haben. Ein wesentliches Ziel einer Verfügbarkeitsdatenintegration besteht folglich darin, die Zusammenarbeit dieser Organisationseinheiten auf dem Gebiet des Problemmanagements zu erleichtern (vergleiche Abbildung 3.2).

Dies kann jedoch nur durch eine möglichst weitgehende gemeinsame

- Nutzung und

- Pflege

der Verfügbarkeitsdatenbestände und -dokumentationen geschehen. Voraussetzung dafür ist ein Zusammenführen der bisher poprietär gehaltenen Datenbestände in einen gemeinsamen Datenbestand, soweit dies zur Zielerreichung sinnvoll und technisch durchführbar ist.

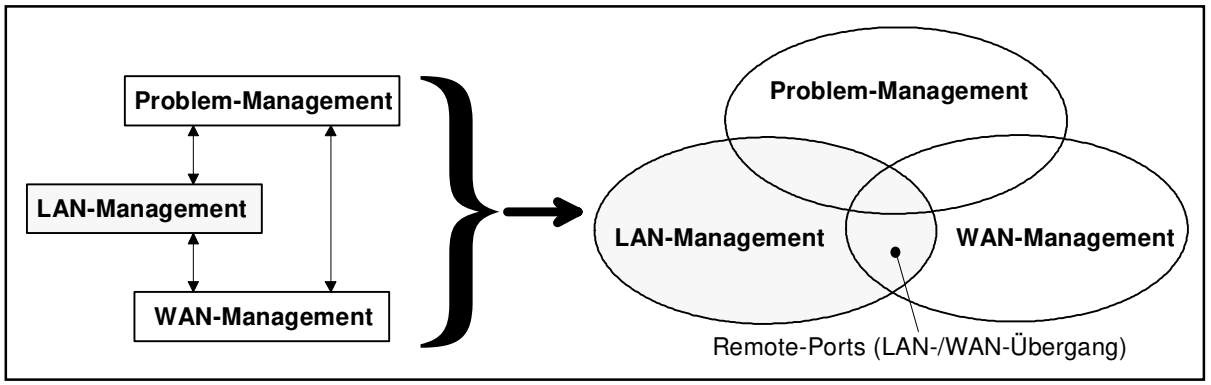

Abbildung 3.2: Kooperation zwischen Problem-, LAN- und WAN-Management

Zur Integration des Problemmanagements sollte die LAN-Verfügbarkeitsdokumentation und die WAN-Verfügbarkeitsdokumentation so effektiv kombiniert werden, daß die Organisationseinheiten LAN- und WAN-Management optimal davon profitieren.

Zu überlegen ist, inwieweit die von den Netzmanagementsystemen gelieferten Verfügbarkeitsdaten direkt in ein manuell geführtes Problemmanagement-Werkzeug (z.B. CINEMA oder ein Trouble-Ticket-System, vergleiche Kapitel 6) automatisch eingetragen werden können.

Die Notwendigkeit einer Datenintegration machen die folgenden Beispiele aus der Netzbetreiberorganisation BMW deutlich:

- Bei der *Ermittlung von Störungsursachen*, die den LAN-WAN-Übergang betreffen, ist eine enge Zusammenarbeit erforderlich zwischen der LAN-Gruppe und der WAN-Gruppe, die bereits — allerdings derzeit noch mühsam manuell über das TIMEVIEW-2000-Fehlerprotokoll ermittelte — Ausfallstatistiken erstellt.

- Bisher versuchte jede dieser Gruppen, *Verfügbarkeitsdokumentationen anzufertigen*, die von den Gruppenleitern und von einzelnen Mitarbeitern gefordert wurden; dabei arbeitete jede Gruppe mit ihren eigenen Statistiken und Werkzeugen, weil man bisher zu wenig darauf geachtet hatte, gemeinsame Verfahren, Werkzeuge und Verfügbarkeitsdatenbestände zu verwenden, obwohl zwischen den Aufgaben der einzelnen Gruppen durchaus Überschneidungen bestehen.

  Beispiel: Remote-Ports in LAN-WAN-Übergängen.
  Physikalische Ausfälle dieser Ports werden durch Netzmanagementsysteme manchmal zuerst der LAN-Gruppe gemeldet, aus technischen Gründen erst etwas später der WAN-Gruppe und schließlich melden Kunden bei der Störungsannahme einen Ausfall. Damit haben sowohl die LAN- als auch die WAN-Gruppe und im Extremfall auch die Störungsannahme je eine Störung zu bearbeiten, d.h. es können drei Störungsmeldungen in drei verschiedenen Abteilungen bearbeitet werden, denen nur eine einzige Ursache wie z.B. ein ausgefallener Remote-Port, zugrunde liegt.

- Bei Problemen (z.B. gewisse Ausfälle von Remote-Ports), die aufgrund ihres häufigeren Auftretens bereits bekannt sind, telefonierte man sich zusammen; die Häufigkeit derartiger Ausfälle wurde jedoch nirgends festgehalten.

  Beispiel: LAN-Gruppe zur WAN-Gruppe: „SPECTRUM meldet einen Ausfall des Remote-Ports 4711 — mach' doch bitte einen Brouter-Reboot!“.

  *Bemerkung: Derartige Probleme eröffnen ein typisches Einsatz-Szenario für **automatische Fehlerbehebungsverfahren**; im obigen Beispiel sollte der Brouter-Reboot ohne Zutun des Personals initiiert werden.*

3.6 Anforderung: Datenarchivierung

Je größer ein Netz ist, desto mehr Ausfälle und damit Alarme treten grundsätzlich auf. Dies gilt insbesondere für den Remote-Bereich, der die Schnittstelle zwischen unternehmenseigenen LANs und dem öffentlichen Netz (beispielsweise der Deutschen Telekom) darstellt.

Bei der Entwicklung von Verfahren zur optimalen Archivierung der Daten sind folgende Punkte zu beachten:

- **Speicherplatzrestriktion**

  Da in jedem DV-System nur eine begrenzte Menge Hintergrundspeicher (z.B. Platten) zur Verfügung steht, müssen geeignete Verfahren zur Filterung, Verdichtung und Reduktion der Daten gefunden werden.

  – *Filterung:* gezielte Auswahl der für die Zielerreichung relevanten Daten;
  – *Verdichtung:* Zusammenfassen von gleichartigen Daten;
  – *Reduktion:* Verminderung eines Datenbestandes durch verfahrensgesteuertes Löschen der für die weitere Archivierung nicht mehr benötigten Daten(sätze).

- **Restriktionen bezüglich der interaktiven (Nach-)Bearbeitung**

  Die archivierten Daten sollten jederzeit möglichst einfach zugänglich und so übersichtlich aufgebaut sein, daß der Schulungsaufwand für die Mitarbeiter gering gehalten werden kann und das Archivierungssystem von ihnen akzeptiert wird.

- **Flexiblitätsrestriktion**

  Die Archive sollten sich leicht an Veränderungen der zu archivierenden Daten(strukturen) (ersetzen, umbenennen, erweitern, verringern) anpassen lassen.

Bei der Auswahl eines Werkzeugs sind folgende Aspekte zu berücksichtigen:

- **Zugriffsrestriktion**

  Jeder Mitarbeiter, der für die Verfügbarkeitsdatenbetreuung verantwortlich ist, muß einerseits Zugang zum verwendeten Werkzeug haben; andererseits sollte das Werkzeug Funktionen zum Schutz vor unbefugtem Zugriff anbieten (Berücksichtigung von Datenschutz- und Datensicherheitsaspekten).

- **Datenhaltungsrestriktion**

  Alle Verfügbarkeitsdaten sollten mit einem Werkzeug, das als Datenserver dient, archiviert werden. Dabei kann jede Organisationseinheit (z.B. LAN-, WAN-Gruppe) ihre eigenen Verfügbarkeitsdaten in einer lokalen Datenbank halten, die für alle Gruppen so zugänglich sein muß, wie dies bei zentralisierter Datenhaltung der Fall wäre (Transparenz). Das heißt, daß sich alle betroffenen Mitarbeiter in einem Unternehmen auf ein einheitliches Werkzeug einigen und dieses später auch einsetzen müssen.

4 Die Ablauforganisation

In diesem Kapitel werden im ersten Abschnitt (siehe unten) zunächst zwei zur Beschaffung und Verarbeitung von Verfügbarkeitsdaten geeignete Modelle für ein Eventmanagement nach einem ISO/IEC-Modell vorgestellt.

Aus diesen Modellen und mit den Anforderungen aus den Kapiteln 2 und 3 wird dann im zweiten Abschnitt (siehe Seite 46f.) eine mögliche Ablauforganisation zur Herstellung der Verfügbarkeitsdokumentation erschlossen (in Kapitel 6 auf Seite 102f. werden zwei Alternativen dazu erörtert).

Der dritte Abschnitt (siehe Seite 53f.) geht auf einige Sonderfälle ein, bei denen ein Nachbearbeiten der erfaßten Verfügbarkeitsdaten erforderlich ist.

Der vierte Abschnitt (siehe Seite 58f.) beschreibt Möglichkeiten der Präsentation und mathematische Verfahren zur Analyse der Verfügbarkeit.

4.1 Modelle für das Eventmanagement

Bevor die Verfügbarkeit berechnet werden kann, müssen zunächst die dazu notwendigen Daten — in der Hauptsache Events — beschafft werden. Zwei Modelle dazu werden in den folgenden beiden Unterabschnitten vorgestellt.

4.1.1 Modell nach ISO/IEC 10 164-5

Einen ersten Ansatz liefert der Internationale Standard [ISO/IEC 10 164-5], der das in Abbildung 4.1 dargestellte „Event Report Management Model“ definiert. Dieses Modell beschreibt die für die Event-Meldung und Event-Verarbeitung zuständigen Objekte sowie Kontrollnachrichten:

1. **Event-Weiterleitungs-Einheiten (Event Forwarding Discriminators, EFDs)**

   Die EFDs entscheiden über eine Weiterleitung selbst und die Art einer Weiterleitung (mit oder ohne Bestätigung) von Event-Berichten an bestimmte Empfänger während gewisser Zeiträume.

- Jede EFD kann eine Zeitplanungs-Einheit (Scheduling Package) zur Bestimmung der Zeitspannen enthalten, in denen Event-Berichte für die Weiterleitung ausgewählt werden.
- Jede EFD spezifiziert Kriterien, die ein Event-Bericht erfüllen muß, um so bald wie möglich an den Empfänger weitergeleitet zu werden.
- Eine EFD ist ein sogenanntes Managed Object (MO, in ISO/IEC 7498-4 definiert) und kann daher Nachrichten versenden, die von allen EFDs wie Event-Berichte weiterverarbeitet werden.

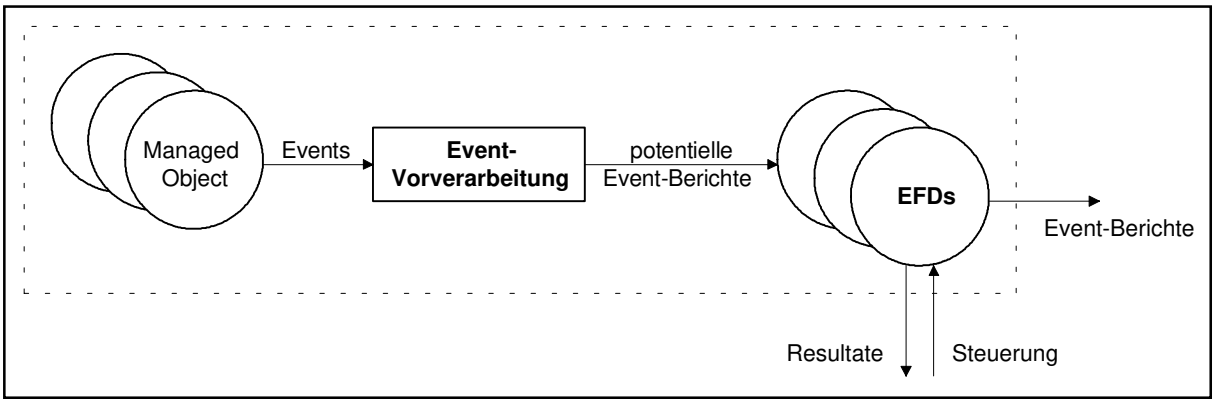

Abbildung 4.1: „Event Report Management Model" nach ISO/IEC 10 164-5

2. Event-Vorverarbeitung

Dieses Objekt empfängt lokale Meldungen und generiert *Event-Berichte (Event Reports)*, die an alle EFDs verteilt werden. Ein Event-Bericht repräsentiert ein lokales EFD-Eingabe-Objekt und ist daher außerhalb des lokalen Systems nicht sichtbar; man spricht deshalb auch von Event-Kapselung.

4.1.2 Erweitertes Modell

Zusammen mit [MANS] läßt sich das ISO/IEC-Modell so erweitern, daß es sich als Grundlage für die zur Erstellung einer Verfügbarkeitsdokumentation notwendigen Event-Verwaltung eignet (siehe Abbildung 4.2).

Die in einem Netz aufgetretenen Events, welche die *Event-Datenquellen* wiedergeben, werden bei diesem Modell zunächst auf einem Medium (aufgrund des möglicherweise hohen Datenaufkommens vorzugsweise eine schnelle Platte oder der flüchtige Speicher) in einer Warteschlange abgelegt.

Die *Event-Weiterleitungs-Einheit* liest diese Event-Daten aus der Warteschlange; dabei wird bei denjenigen Events, die keine besondere Priorität aufweisen, im allgemeinen nach dem Fifo(First-in-first-out)-Verfahren gearbeitet, d.h. die Events, welche zuerst in die Warteschlange aufgenommen wurden (sich also schon am längsten dort befunden haben), werden zuerst aufbereitet und anschließend an die Event-Empfänger weitergeleitet — Events mit Priorität werden entsprechend bevorzugt behandelt.

Die Event-Weiterleitungs-Einheit wird gesteuert und konfiguriert von

- den *Event-Selektions-Kriterien*, wodurch ein impliziter Filter realisiert wird, der nur diejenigen Events zur Aufbereitung und Weiterleitung freigibt, welche die *Event-Empfänger* anläßlich ihrer Registrierung und Identifizierung bei der Event-Abonnement-Verwaltung bestellt haben;
- der *Event-Abonnement-Liste*, welche die Adressen aller Event-Empfänger enthält und die Häufigkeit, mit der sie Events geliefert bekommen möchten.

Sowohl die Event-Selektions-Kriterien als auch die Event-Abonnement-Liste werden nach Vorgabe der *Event-Abonnement-Anforderungen* der Event-Empfänger erstellt; dabei hat die *Event-Abonnement-Verwaltung* die Aufgabe, anhand der von ihr verwalteten Abonnement-Autorisierungs-Information (die sogenannten *Event-Abonnement-Kriterien*), für jeden Event-Empfänger zu überprüfen, ob dieser überhaupt berechtigt ist, die von ihm gewünschten Events zu erhalten (Datenschutz).

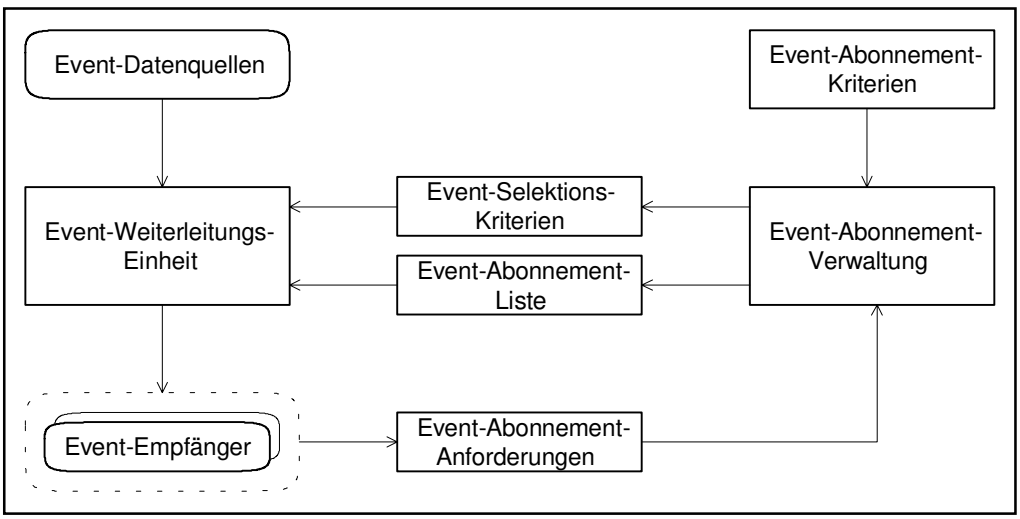

Abbildung 4.2: Erweitertes Eventmanagement-Modell

Das Gesamtziel der Event-Verarbeitung beim Bewältigen, Weiterleiten, Aufbereiten und Verteilen komplexer Events sind möglichst große Effektivität und Effizienz, die [BRAESS] folgendermaßen festlegt:

- *Effektivität* läßt sich definieren als: die „richtigen“ Ziele setzen, die „richtigen“ Dinge tun; Effektivität entspricht dem Output.
- *Effizienz* läßt sich definieren als: die Dinge „richtig“ (d.h. Nutzen-Kosten- bzw. Ertrags-Aufwands-optimal) tun; Effizienz entspricht dem Verhältnis $\frac{\text{Output (z.B. Nutzen, Ertrag)}}{\text{Input (z.B. Kosten, Aufwand)}}$.

4.2 Die Ablauforganisation

Abbildung 4.3 zeigt eine geeignete Ablauforganisation, die

- aus den bisher ermittelten Anforderungen an eine Verfügbarkeitsdokumentation sowie
- unter Zuhilfenahme der im vorigen Abschnitt dargestellten Modelle

abgeleitet wurde:

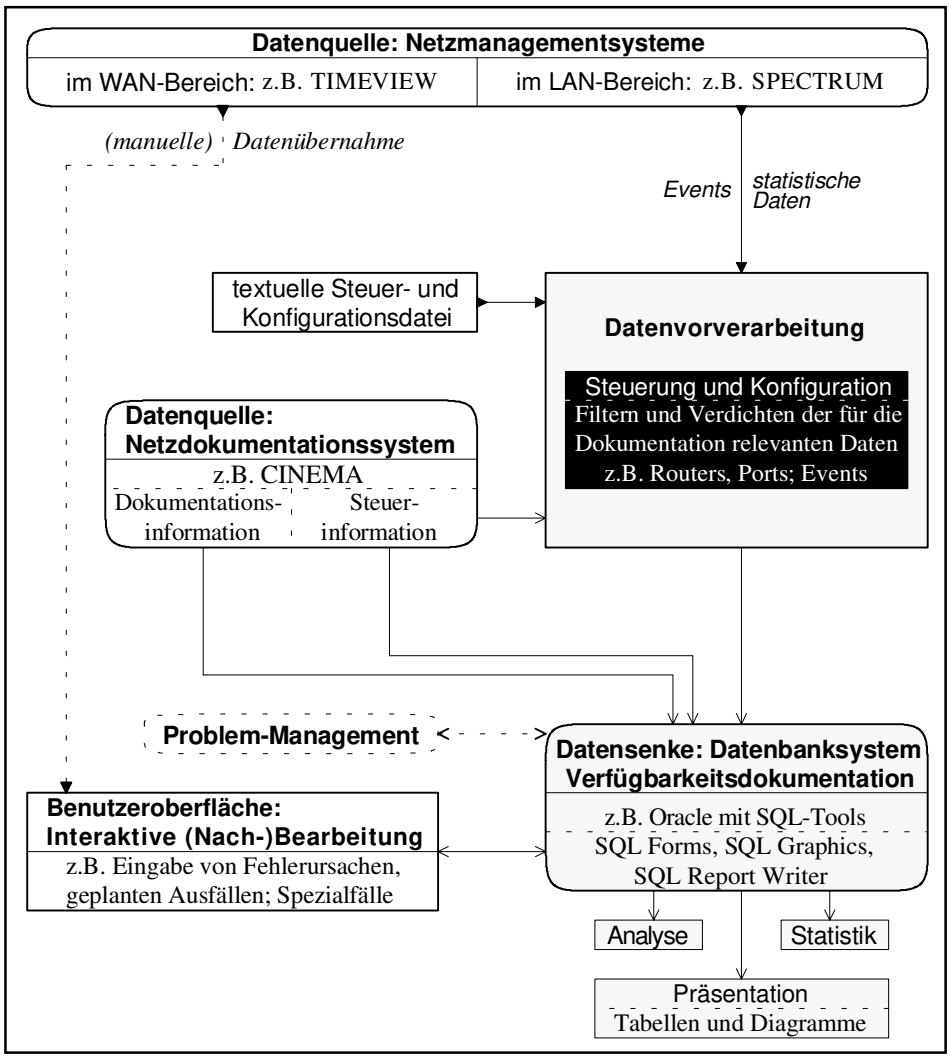

Abbildung 4.3: Ablauforganisation

Überblick über die Ablauforganisation in Abbildung 4.3

Die Ablauforganisation besteht im wesentlichen aus den folgenden vier funktionalen Blöcken (Werkzeugen):

a) *Netzmanagementsysteme* (z.B. SPECTRUM): Quelle der für die Verfügbarkeitsdokumentation benötigten Daten (Events und statistische Daten).

b) *Datenvorverarbeitung:* Filtern und Verdichten der von den Netzmanagementsystemen gelieferten Daten nach den Spezifikationen des Steuer- und Konfigurationsmoduls.

c) *Netzdokumentationssystem* (z.B. CINEMA):
   - Ergänzen der Daten durch Netzdokumentationsinformationen, d.h.
     * Topologieinformation (z.B. Gebäude, Kunden);
     * zusätzliche Netzkomponenteninformation (z.B. Komponentenhersteller, Gerätetyp, Netztyp).
   - Bereitstellen von Steuer- und Konfigurationsinformation.

d) *Lokales Datenbanksystem* (z.B. Oracle mit den SQL-Tools):
   - lokales Speichern und Archivieren der Verfügbarkeitsinformationen;
   - interaktive Daten(nach)bearbeitung;
   - Erzeugen der Verfügbarkeitsdokumentation (Analysen, Statistiken und Präsentation der Auswertungen in Form von Tabellen und Diagrammen).

4.2.1 Identifikation und Korrelation von Netzkomponenten

Die Grundvoraussetzung für eine erfolgreiche Integration von Netzmanagement-, Netzdokumentations- und Datenbanksystemen ist eine eindeutige Identifikation der in den Netzmanagementsystemen gespeicherten Netzkomponenten (Objekten) und eine Korrelation mit denen in der Netzdokumentationsdatenbank.

Dazu sollte mit dem Namen der Netzkomponente (vom Domain Name Service) und bei Ports zusätzlich mit einer speziellen Portbeschreibung (ifDescr aus der Netzkomponenten-MIB) gearbeitet werden, da sich das Verwenden der einzigen weiteren geeigneten Alternative, der IP-Adresse, aus den folgenden zwei Gründen nicht empfiehlt:

1. Obwohl jeder Brouter-Port in der Regel eine eigene IP-Adresse hat, gibt es in Ausnahmefällen auch Ports, denen keine eigene IP-Adresse zugewiesen wurde.

   Beispiel: Bei BMW haben diejenigen Ports, welche die Token-Ring-Segmente mit dem FDDI-Backbone verbinden, keine eigene IP-Adresse.

2. Sternkopplerports haben im allgemeinen keine eigene IP-Adresse.

Zur Realisierung siehe den Abschnitt 5.1 auf Seite 67.

4.2.2 Datenvorverarbeitung

An die Datenvorverarbeitung, die zum Verfahren „Aufbereiten der Verfügbarkeitsdaten“ gehört, sind diese Anforderungen zu richten:

- *Eindeutige Identifikation und Korrelation* der in den Netzmanagementsystemen und im Netzdokumentationssystem vorhandenen Netzkomponenten (siehe oben).

- *Flexible Steuer- und Konfigurierbarkeit* des (im Verfahren „Zugriff auf die Verfügbarkeitsdaten(quellen)“ geregelten) Verfügbarkeitsdatenexports aus dem Netzmanagementsystem durch ein Steuer- und Konfigurationsmodul:
  - Filterung:
    * Ein- und Ausschluß spezieller Events/Fehlersymptome;
    * Ein- und Ausschluß bestimmter Geräte (Ports);
    * für die logische Verfügbarkeit zusätzlich: Ein- und Ausschluß weiterer Geräte(Port)-Attribut(wert)e.
  - Verdichtung:
    Kumulieren gewisser Fehler (zur Realisierung siehe Abschnitt 5.3.3.2 auf Seite 73f.).
- Von elementarer Bedeutung für die Verfügbarkeitsdokumentation ist die Berechnung der Ausfalldauer; dazu müssen die von den Netzmanagementsystemen gelieferten Daten gewährleisten, daß für eine betroffene Netzkomponente Ausfall-Beginn und Ausfall-Ende einander exakt zuordnet werden können.
- Um den (Nach-)Bearbeitungsaufwand zu verringern, sollte das Datenvorverarbeitungsmodul eine unterbrochene Verbindung des Netzmanagementsystems zum Netz feststellen können, damit es die aufgrund der unterbrochenen Verbindung von Netzmanagementsystemen generierten „falschen“ Events ignorieren kann (zur Realisierung siehe Abschnitt 4.3.3 auf Seite 57).
- Übergabe der gefilterten und verdichteten Events an das Datenbanksystem.

Das wichtigste Modul innerhalb Datenvorverarbeitung ist die Steuerung und Konfiguration (siehe Abbildung 4.3), mit dem das Protokollieren der Verfügbarkeitsdaten für die Verfügbarkeitsdokumentation flexibilisiert, d.h. an die Anforderungen der Empfänger anpaßbar gemacht wird. An dieses Modul ist die Anforderung zu stellen, die Vielzahl der von den Datenquellen (Netzmanagementsystemen) kommenden Daten nach benutzerspezifizierbaren Parametern zu filtern, zu verdichten und zu sortieren sowie anschließend an das als Datensenke eingesetzte Datenbanksystem weiterzuleiten.

Für die Realisierung des Steuer- und Konfigurationsmoduls stehen zwei Alternativen zur Wahl, die in den folgenden Unterabschnitten diskutiert werden:

1. Steuerung und Konfiguration über eine Textdatei;
2. Steuerung und Konfiguration über ein Netzdokumentationssystem.

Daran anschließend wird die empfohlene Vorgehensweise für die spätere Realisierung dargestellt.

4.2.2.1 Steuerung und Konfiguration über eine Textdatei

Bei der Entscheidungsfindung bezüglich der Realisierung der Steuerung und Konfiguration der Datenvorverarbeitung über eine Textdatei sind diese Vor- und Nachteile gegeneinander abzuwägen:

- Vorteile dieser Alternative:
  - *Implementierungsaspekt:* der relativ einfache Zugriff auf eine Textdatei ist mit einem relativ geringen Implementierungsaufwand verbunden;
  - *Performanceaspekt:* sehr schneller Zugriff auf die Textdatei.
- Nachteile dieser Alternative:
  - *Konzeptioneller Aspekt:* da in der Steuer- und Konfigurationsdatei eine ganze Reihe von unterschiedlichen Parametern spezifiziert werden soll, muß dazu eine einfache Befehlsstruktur entworfen werden, deren Syntax und Semantik so exakt zu definieren und zu dokumentieren ist, daß jeder Anwender in die Lage versetzt wird, die Textdatei selbständig seinen Wünschen entsprechend zu ändern (ein Beispiel für eine derartige Steuer- und Konfigurationsdatei ist das „Controlfile“ in [EGERER]);
  - *Bedienungsaspekt:* relativ geringer Komfort, da die textuelle Datei umständlich und unübersichtlich mit Hilfe eines Texteditors erstellt und geändert werden muß;
  - *Fehleranfälligkeit:* große Gefahr von Flüchtigkeitsfehlern bei der Eingabe;
  - *Zusammenarbeit mit einem Datenbanksystem:* da durch das Steuer- und Konfigurationsmodul auch das Datenbanksystem kontrolliert werden muß (z.B. Präsentation: Unterscheidung von Diagrammen für den Local- und für den Remote-Bereich), ist im Datenbanksystem eine spezielle textuelle Schnittstelle zu der Steuer- und Konfigurationsdatei zu implementieren.

4.2.2.2 Steuerung und Konfiguration über ein Netzdokumentationssystem

Als Alternative zu einer textuellen Steuer- und Konfigurationsdatei kann bei der Realisierung auch ein Netzdokumentationssystem wie beispielsweise CINEMA benutzt werden. Bei der Entscheidung für diese Möglichkeit sind diese Gesichtspunkte zu berücksichtigen:

- Wenn für die Realisierung diese Alternative gewählt wird, sind die folgenden Änderungen in der bestehenden Netzdokumentationsdatenbank nötig:
  - Erweitern/Ändern aller Tabellen, die für die Spezifikation von Steuer- und Konfigurationsinformationen (z.B. Gewichtung eines Ports) infrage kommen, um geeignete Felder.
  - Entsprechendes Erweitern/Ändern aller Eingabemasken, die von den geänderten Tabellen betroffen sind.
- Vorteile dieser Alternative:
  - *Datenintegrationsaspekt:* die zusätzlichen Steuerinformationen (z.B. Gewichtung eines Gerätes), die Bestandteil eines Netzdokumentationsdatenbestandes sind, können in derselben Datenbank abgelegt werden.
  - *Datenpflegeaspekt:* Änderungen der zusätzlichen Steuerinformationen sind in einem interaktiven Datenbanksystem in der Regel einfacher und weniger fehleranfällig durchführbar als die entsprechenden Änderungen in einer textuellen Datei, bei der schon die Suche nach dem zu ändernden Eintrag mühsam sein kann.

- Nachteile dieser Alternative:
  - *Implementierungsaspekt:* einmaliger Aufwand für die oben beschriebenen erforderlichen Änderungen im Netzdokumentationsdatenbanksystem.
  - *Verfügbarkeitsaspekt:* da zu jedem aufgetretenen Alarm die Gewichtung und andere Netzdokumentationsinformationen des betroffenen Gerätes *Online* in die temporären Eingangstabellen für die spätere Auswertung einzutragen sind, muß das Netzdokumentationssystem ständig verfügbar sein (dieser Nachteil entfällt, wenn die für die Verfügbarkeitsdokumentation erforderlichen Datenstrukturen und Daten in einer lokalen Datenbank gespiegelt werden, wie dieses im Abschnitt „Spiegelung des Netzdokumentationssystems“ auf Seite 51 erörtert ist).

4.2.2.3 Folgerung und Bewertung: empfohlenes Vorgehen

Im Hinblick auf die Datenintegration im Bereich des integrierten Netzmanagements sollte bei der Realisierung versucht werden, für die Steuerung und Konfiguration so weit wie möglich auf eine bereits bestehende Netzdokumentationsdatenbank zurückzugreifen. Als Faustregel könnte man dabei festhalten, alle Datenbestände in der Netzdokumentationsdatenbank abzulegen und zu verwalten, auf die ein Datenbanksystem selbst zugreifen muß; dabei handelt es sich demnach um Daten, die für die Analyse, Statistik und Präsentation der Verfügbarkeitsdokumentation direkt erforderlich sind — nicht zu diesen Daten zählen die von den Netzmanagementsystemen gelieferten Events, d.h. deren Verarbeitung (Filterung, Verdichtung) wird vorzugsweise durch eine Textdatei gesteuert.

Die Konzentration auf die Netzdokumentationsdatenbank mag zwar anfangs in einem größeren Implementierungsaufwand resultieren, da Änderungen in den Datenstrukturen innerhalb der Datenbank durchzuführen sind, was gleichzeitig auch entsprechende Änderungen bei verschiedenen Bildschirmmasken des Netzdokumentationssystems erforderlich macht (derartige Änderungen können teilweise umgangen werden, wenn man die im nächsten Abschnitt vorgestellte Datenspiegelung realisiert). Andererseits verringert sich dadurch jedoch der Aufwand, der durch die Definition von Syntax und Semantik der Textdatei und dem erforderlichen Textdatei-Parser innerhalb der Datenvorverarbeitung entsteht.

Insgesamt ist festzustellen, daß man sich mit der Textdatei (wieder einmal) eine eigene kleine proprietäre Datenbank „züchtet“, die zukünftigen weiteren Integrationsbestrebungen immer im Wege stehen wird.

Die Wahl sollte also auf das Verwenden des Netzdokumentationssystems für den wesentlichen Anteil an der Steuerung und Konfiguration fallen, es sei denn, die Änderung der Netzdokumentationsdatenbank stößt auf unüberwindliche technische Probleme oder organisatorische Hindernisse (z.B. Weisung der Abteilungsleitung).

Auf die technische Realisierung und Implementierung wird im Abschnitt „Realisierung: die Datenvorverarbeitung“ auf Seite 69f. genau eingegangen.

4.2.3 Spiegelung des Netzdokumentationssystems

Die Anforderungen an das eingesetzte Netzdokumentationssystem wurden bereits im Abschnitt 3.3.2 auf Seite 38 dargelegt. Dieser Abschnitt beleuchtet Vor- und Nachteile einer Spiegelung der relevanten Daten(strukturen) des Netzdokumentationssystems.

Bisher wurde die Realisierung

- der Steuerung/Konfiguration und
- der Datenergänzung mit verfügbarkeitsrelevanten Netzdokumentationsinformationen

über einen direkten Zugriff auf ein Netzdokumentationssystem beschrieben.

Eine Alternative dazu, die man bei der Planung berücksichtigen sollte, ist die Spiegelung aller aus dem Netzdokumentationssystem benötigten Datenstrukturen und Daten in der *lokalen* Datenbank, die als Datensenke für die Verfügbarkeitsdokumentation eingesetzt wird:

- **Vorteile dieser Methode**
  - Lokale Datenhaltung:
    * keine Erhöhung der Netzlast im Tagesbetrieb,
    * keine Zusatzbelastung des Netzdokumentationssystems im Tagesbetrieb,
    * größere Performance.
  - Deutliche Verbesserung der Betriebssicherheit der Verfügbarkeitsdokumentation:

    besteht dagegen eine direkte Abhängigkeit von der Verfügbarkeit des Netzdokumentationssystems, so wird bei jedem Ausfall des Netzdokumentationssystems auch die Verfügbarkeitsdokumentation unterbrochen, da auf die für ihren Betrieb notwendigen Daten nicht mehr zugegriffen werden kann.

    Beispiel: Die im Netzdokumentationssystem abgelegte Gewichtung einer Komponente entscheidet in der Datenvorverarbeitung (Filterung) darüber, ob die Daten dieser Komponente in die Dokumentation übernommen werden sollen.
  - Die Implementierung ist unabhängig von der gewählten Alternative (Transparenz).
- **Nachteile dieser Methode**
  - Höherer Hintergrundspeicherbedarf durch die Datenspiegelung (redundante Datenhaltung).
  - Regelmäßige automatisierte Aktualisierung der lokalen Datenbank mit den Netzdokumentationssystem-Daten im Stapelbetrieb (vorzugsweise nachts) erforderlich.
  - Bei Änderungen im Netzdokumentationssystem, die *gleichzeitig* auch für die Verfügbarkeitsdokumentation wirksam werden sollen, ist darüber hinaus auch eine sofortige Aktualisierung der lokalen Datenbank wünschenswert, die bestimmte Benutzer bei Bedarf jederzeit anstoßen können. Bevor ein Mitarbeiter von dieser Aktualisierungsmöglichkeit Gebrauch macht, sollte er sich darüber im Klaren sein, daß die Spiegelung kurzzeitig sowohl die Netzlast als auch die Auslastung des Netzdokumentationssystems in die Höhe treiben wird.

    Beispiel: Die sofortige Aktualisierung der lokalen Datenbank ist sinnvoll, wenn bestimmte Komponenten aufgrund unvorhergesehener Ereignisse unverzüglich von der weiteren Verfüg-

barkeitsdatenerfassung ausgeschlossen werden müssen, um für diese eine eventuell aufwendige nachträgliche manuelle Korrektur der erfaßten Daten zu vermeiden.

- **Folgerung und Empfehlung**

  Insbesondere dann, wenn keine Engpässe bezüglich des Hintergrundspeichers zu befürchten sind, überwiegen nach Ansicht des Verfassers die genannten Vorteile der Datenspiegelung in der lokalen Datenbank; in diesem Fall sollte bei der Realisierung diese Methode gewählt werden.

4.2.4 Datenbanksystem und interaktive Daten(nach)bearbeitung

Das lokale Datenbanksystem (z.B. Oracle) ist

1. Datensenke für die Speicherung der Verfügbarkeitsdaten in temporären Eingangstabellen (zur Realisierung siehe Abschnitt 5.5.2 auf Seite 81f.) und eventuell spätere Archivierung in Archivtabellen (Abschnitt 5.5.3 auf Seite 87f.);
2. Werkzeug für die interaktive Verfügbarkeitsdaten(nach)bearbeitung;
3. Analyse-, Statistik- und Präsentationswerkzeug (z.B. Verwendung der SQL-Tools: SQL Forms, SQL Graphics und SQL Report Writer) (Abschnitt 5.6 auf Seite 89f.).

Benutzerschnittstelle: die interaktive Daten(nach)bearbeitung

Die Güte der interaktiven Verfügbarkeitsdaten(nach)bearbeitung (Abschnitt 5.5 auf Seite 78f.) hat großen Einfluß auf die erreichbare Qualität der späteren Auswertungen und sollte daher möglichst regelmäßig und zuverlässig durchgeführt werden, da hier

- Korrekturen (bei „falschen Fehlermeldungen“ der Netzmanagementsysteme) und
- Erweiterungen (Fehlerklassifikation)

des Datenbestandes vollzogen werden.

Außerdem soll die *Benutzerschnittstelle als Alarm-Monitor* die entsprechenden von den Netzmanagementsystemen angebotenen Alarm-Views ersetzen, da sie zu jedem Event auch die zugehörigen Netzdokumentationsinformationen bereitstellt.

Deshalb ist eine *möglichst kurze Durchlaufzeit der Events* — d.h. eine möglichst geringe Zeitspanne (wenige Sekunden) zwischen dem Auflaufen eines Events in den Netzmanagementsystemen bis zum Eintreffen der Daten im Datenbanksystem — eine entscheidende Anforderung an die Ablauforganisation. Dies kann man nur durch eine *Online-Verbindung* des Datenbanksystems über die Datenvorverarbeitung mit den Datenquellen erreichen.

Ein weiterer Grund für die Forderung nach einer kurzen Durchlaufzeit der Events liegt in der *Gewährleistung einer effektiven Datennachbearbeitung*: der damit beauftragte Mitarbeiter muß beispielsweise die Ursache eines Ausfalls eintragen; dies ist in der Praxis allerdings nur zeitnah zum Auftreten eines Events durchführbar ist, da andernfalls (z.B. beim Datenbank-Aktualisieren im Stapelbetrieb über Nacht) die manuell nachzutragenden Daten zunächst aufgeschrieben werden müßten und erst später in die Datenbank eingetragen werden könnten, was den Bearbeitungsaufwand annähernd verdoppeln würde.

Vorteile des Online-Aktualisierens der Datenbank:

- Alle für Störungsentgegennahme und -bearbeitung zuständigen Organisationseinheiten (z.B. LAN-/WAN-Gruppe und Störungsannahme) können sich aufgrund der im Datenbanksystem angebotenen, jederzeit aktuellen Informationen an der Behebung eines Fehlers beteiligen.
- Allen das System nutzenden Abteilungen steht für jede Störung genau ein Bezugsobjekt im Datenbanksystem zur Verfügung, so daß Mehrfacherfassung und Mehrfachbearbeitung derselben Störungsmeldung vermieden werden.

4.3 Sonderfälle

Im folgenden werden einige Sonderfälle beschrieben, die bei der interaktiven Datennachbearbeitung eventuell besonderer Behandlung bedürfen (d.h. in den temporären Eingangstabellen im Datenbanksystem sind dabei gegebenenfalls zusätzliche manuelle Korrekturen erforderlich):

1. Probleme im FDDI-Ring (siehe unten):
   i) Kabelunterbrechungen (Leitungsprobleme);
   ii) Brouter-Probleme.
2. Verlorengegangene Traps (Abschnitt 4.3.2 auf Seite 56).
3. Zugang des Netzmanagementsystems zum Netz unterbrochen (Abschnitt 4.3.3 auf Seite 57).

4.3.1 Probleme im FDDI-Ring

Der FDDI-Standard zeichnet sich aufgrund von Redundanzen und Überbrückungsmöglichkeiten fehlerhafter Komponenten durch ein hohes Maß an Ausfallsicherheit und hohe Verfügbarkeit aus:

- **Gegenläufig operierender Doppelring (Redundanz)**

  Bei einer Kabelunterbrechung — von Glasfaserkabelbrüchen werden in nahezu allen Fällen Primär- und Sekundärring gleichzeitig betroffen — schalten die FDDI-Ports der beiden an die Bruchstelle angrenzenden Brouters (z.B. die Brouters 6 und 7 in Abbildung 4.4) automatisch auf Backupbetrieb und verwenden damit den — im störungsfreien Betrieb ungenutzten — Sekundärring durch Verbinden der beiden noch intakten Teilringe zu einem etwa doppelt so langen, wieder voll funktionsfähigen einzelnen Ring.

- **Optischer Bypass (Überbrückungsmöglichkeit fehlerhafter Komponenten)**

  Beim Ausfall einer Station, die über einen solchen Bypass verfügt, kommt es zu einer Überbrückung des FDDI-Ports, indem die Eingangsfaser des Primärringes auf die Ausgangsfaser durchgeschaltet und damit die gestörte Komponente überbrückt wird.

Die BMW-FDDI-Brouter-Ports sind nicht mit optischen Bypasses ausgerüstet, weil diese eine ungenügende Zuverlässigkeit aufweisen, die ihren hohen Preis nicht rechtfertigt; daher kann hier die Verfügbarkeit

1. von Kabelunterbrechungen (siehe Abschnitt 4.3.1.1) und
2. von Brouter-Problemen (siehe Abschnitt 4.3.1.2)

in gleichem Maße eingeschränkt werden.

Für die Verfügbarkeitsdokumentation und die Fehlerbehebung ist die Ursache der reduzierten Verfügbarkeit und damit das Unterscheiden zwischen Kabelunterbrechungen und Brouter-Problemen wichtig.

4.3.1.1 Kabelunterbrechungen

1. Fallstudie: eine oder mehrere Kabelunterbrechungen (✂) zwischen zwei benachbarten Brouters (siehe Abbildung 4.4)

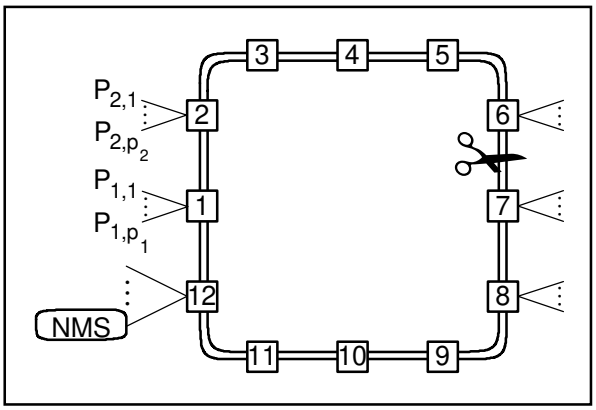

Abbildung 4.4: FDDI-Ring mit einer Kabelunterbrechung — keine Teilringbildung

- *Auswirkung auf die Verfügbarkeit des FDDI-Ringes:* keine (wegen der vollautomatischen Backup-Funktion der FDDI-Brouter-Ports).
- *Datenquelle:* diesbezügliche Daten werden von einem speziellen Netzmanagementwerkzeug (z.B. SpectroWatch) geliefert, das den sogenannten Wrap-Status der FDDI-Brouter-Ports, d.h. das Durchschalten auf den Sekundärring (Backup), überwacht.
- *Art und Umfang der notwendigen Korrektur der temporären Tabellen:* keine.

2. Fallstudie: Kabelunterbrechungen (✂) an mindestens zwei Stellen, zwischen denen sich mindestens ein Brouter befindet (siehe Abbildung 4.5)

- *Auswirkung auf die Verfügbarkeit des FDDI-Ringes:* Zerfall des Backbones in mindestens zwei Teilringe[1], die für sich voll funktionsfähig bleiben mit der Einschränkung, daß keine Kommunikation untereinander mehr möglich ist.

[1] Wenn sich im Extremfall genau ein Brouter zwischen den Bruchstellen befindet, so liegt ein „Teilring“ vor, der aus genau einem Brouter besteht.

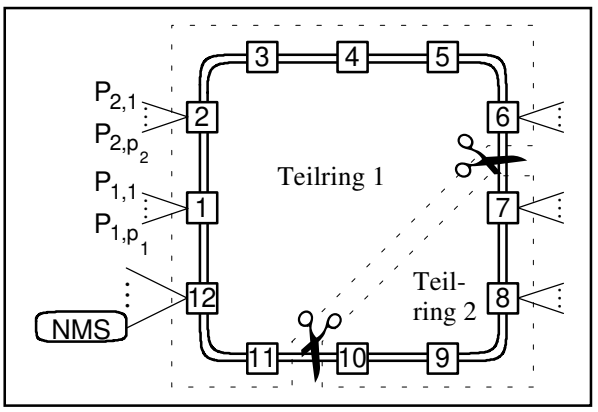

Abbildung 4.5: FDDI-Ring mit zwei Kabelunterbrechungen — Teilringbildung

- *Datenquelle:* diesbezügliche Daten werden neben SpectroWatch auch vom Netzmanagementsystem (durch eine Contact-lost-Meldung) geliefert.
- *Art und Umfang der notwendigen Korrektur der temporären Tabellen:* abhängig vom Standort des Netzmanagementsystems (NMS).

4.3.1.2 Brouter-Probleme

Ein vom Netzmanagementsystem gemeldeter Verbindungsverlust zu einem Brouter (Contact lost, Node down) kann zwei unterschiedliche Ursachen haben, die verschieden behandelt werden müssen:

1. **Fallstudie: Nach einer Contact-lost-Meldung genau eines Brouters tritt ein Restart-Trap und dann eine Contact-Meldung auf (siehe Abbildung 4.6)**

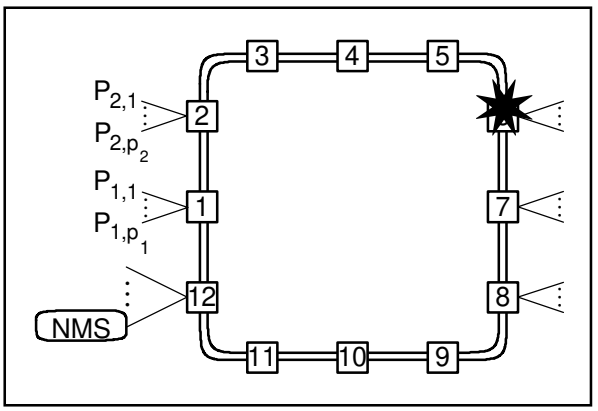

Abbildung 4.6: Problem mit dem Brouter 6 — keine Teilringbildung

- *Ursache:* Brouter-Problem (✷), Leitungsproblem kann ausgeschlossen werden.
- *Auswirkung auf die Verfügbarkeit:* der Brouter und alle seine Ports waren nicht verfügbar.
- *Art und Umfang der notwendigen Korrektur der temporären Tabellen:* bei allen Ports des betroffenen Brouters sind automatisch dessen Ausfalldaten zu berücksichtigen.

2. Fall: Contact-lost-Meldungen von mindestens drei benachbarten Brouters (siehe Abbildung 4.7)

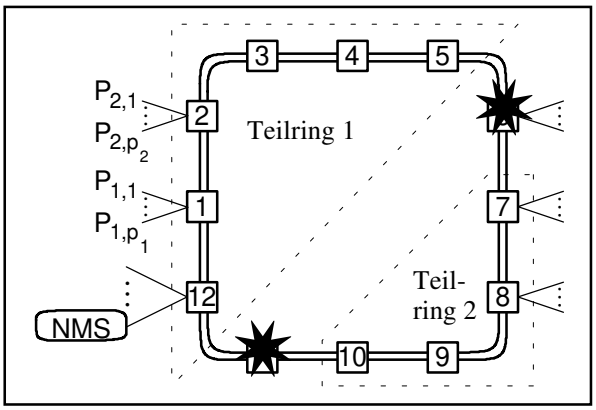

Abbildung 4.7: Probleme mit den Brouters 6 und 11 — Teilringbildung

- *Ursache:* Brouter-Problem (✷), Leitungsproblem kann nicht ausgeschlossen werden; daher ist eine manuelle Ermittlung der tatsächlichen Ursache notwendig.
- *Auswirkung auf die Verfügbarkeit des FDDI-Ringes:* Zerfall des Backbones in mindestens zwei Teilringe.
- *Art und Umfang der notwendigen Korrektur der temporären Tabellen:* abhängig vom Standort des Netzmanagementsystems (NMS); aus Sicht des Netzmanagementsystems sind keine Aussagen mehr über die Verfügbarkeit der (vom Netzmanagementsystem aus) nicht erreichbaren Teilringe möglich.

4.3.2 Verlorengegangene Traps

Netzmanagementsysteme verwenden das immer häufiger für das Netzmanagement eingesetzte Simple Network Management Protocol (SNMP) für ihre Kommunikation mit den verschiedensten Netzkomponenten. SNMP wurde am 10.05.1990 überarbeitet durch den [RFC 1157], der den RFC 1098 vom 01.04.1989 ersetzt (der RFC 1067 vom 01.08.1988 war die erste Veröffentlichung dieses Protokolls). Am 03.05.1993 wurde der SNMPv2-Standard in den RFCs 1441 bis 1452 publiziert.

Einer der Gründe, warum SNMP (Version 1) von nahezu allen Netzkomponentenherstellern unterstützt wird, besteht darin, daß es trotz seiner Einfachheit (es gibt nur die fünf Management-Operationen `get-request`, `get-next-request`, `get-response`, `set-request` und `trap`) das Management einer breiten Vielfalt von Komponenten ermöglicht.

SNMP erhebt nur geringe Anforderungen an die zugrunde liegenden Kommunikationsdienste ([GERING]). Es arbeitet über einen verbindungslosen Dienst, der vom User Datagram Protocol (UDP) und dem Internet-Protokoll (IP) zur Verfügung gestellt wird. Die Größe eines UDP-Pakets wird durch das Internet-Routing-Netz vorgegeben. Da der IP-Standard von Anwendungen verlangt, unter normalen Bedingungen Pakete von mindestens 484 Oktetts übertragen

zu können, darf der Sender einer Nachricht annehmen, daß SNMP-Pakete, deren Länge in der Praxis auf 484 Oktetts begrenzt ist[1], beim Empfänger ankommen.

Wie es für verbindungslose Dienste charakteristisch ist, besteht keine Möglichkeit, den Datenfluß zwischen einem Agenten einer Netzkomponente und einem Empfänger (z.B. ein Netzmanagementsystem) zu kontrollieren — weder IP noch UDP signalisieren dem Sender bzw. Empfänger verlorene oder vom Netz weggeworfene Pakete. Derartige Paketverluste können beispielsweise entstehen, wenn

- der Empfänger nicht verfügbar ist,
- das Paket für die Übertragung über ein Zwischensystem zu groß ist,
- eine Netzüberlastung (Stausituation) vorliegt.

Die für die Ermittlung der Verfügbarkeit wichtigen SNMP-Traps sind also unbestätigt und werden als Datagramme übermittelt, so daß ein Agent keinen Hinweis erhält, wenn das Netzmanagementsystem nicht verfügbar und ein Trap daher nicht registriert wurde.

Dieses Problem kann jedoch vom Netzmanagementsystem gelöst werden, indem es durch aufeinanderfolgende `get-request-` und `get-next-request`-Operationen vom Agenten Daten anfordert (sogenanntes Polling). Durch ein in regelmäßigen zeitlichen Intervallen durchgeführtes Polling der Netzmanagementsysteme sollte die physikalische Verfügbarkeit von Ports auch dann automatisch festgestellt werden können, wenn die zur Berechnung der Verfügbarkeit notwendigen korrespondierenden Link-up- und Link-down-Traps der verschiedenen Netzkomponenten (z.B. Brouter) die Netzmanagementsysteme nicht erreichen. Dies setzt natürlich voraus, daß keine Leitungsprobleme zwischen Netzmanagementsystem und Netz vorliegen (Näheres dazu ist im nächsten Abschnitt 4.3.3 zu finden).

Das Pollingintervall ist vom Netzbetreiber seinen Ansprüchen gemäß zu konfigurieren, wobei zu berücksichtigen ist, daß ein relativ hoher Aktualitätsgrad der Netzdaten im Netzmanagementsystem eine relativ hohe Netzlast nach sich zieht (Trade-off); hier ist also ein angemessener Kompromiß zwischen der durch das Polling erzeugten Netzlast einerseits und der Datenaktualität andererseits zu finden.

4.3.3 Zugang des Netzmanagementsystems zum Netz unterbrochen

- *Ursache:* Ausfall des Brouters oder Ports, der das Netzmanagementsystem mit dem FDDI-Backbone verbindet (z.B. Brouter 12 oder der Port $P_{12,p_{12}}$ in Abbildung 4.5).
- *Auswirkung auf die Verfügbarkeit:* keine; die tatsächliche Verfügbarkeit kann aus Sicht des Netzmanagementsystems nicht mehr festgestellt werden.
- *Folge:* das gesamte Netz ist für das Netzmanagementsystem nicht mehr verfügbar (Contact-lost-Meldungen für alle Brouters); dabei muß unbedingt verhindert werden, daß diese „falschen Fehlermeldungen“ in die Tabellen eingetragen werden (ein Lösungsvorschlag ist im Abschnitt 5.3.3.3 auf Seite 73 zu finden).

---

[1] Zitat aus [RFC 1157]: „`An implementation of this protocol need not accept messages whose length exceeds 484 octets. However, it is recommended that implementations support larger datagrams whenever feasible`“.

- *Art und Umfang der notwendigen Korrektur der temporären Tabellen:* abhängig davon, ob der Lösungsvorschlag realisiert wurde; ist dies nicht der Fall, müssen die falschen Einträge in den Tabellen manuell bereinigt werden, um die spätere Verfügbarkeitsdokumentation nicht zu verfälschen.

4.4 Dokumentation: Präsentation und mathematische Analyse

In diesem Abschnitt werden Verfahren aufgezeigt, mit deren Hilfe die Verfügbarkeitsdokumentation erstellt werden kann:

1. Der erste Unterabschnitt beschäftigt sich mit den verschiedenen Möglichkeiten, Datenreihen graphisch festzuhalten (siehe unten).
2. Der zweite Unterabschnitt beinhaltet eine Auswahl mathematischer Verfahren, die es ermöglichen, die Vielzahl von Daten in einem Diagramm zu analysieren (siehe Seite 61f.).

4.4.1 Grundsätzliches über Diagramme

Ein Diagramm ist eine graphische Darstellung von zahlenmäßigen Abhängigkeiten zwischen zwei oder mehreren Datenreihen.

Ein Diagramm läßt sich, wie aus Abbildung 4.8 hervorgeht, aus sechs Hauptobjekten zusammensetzen, die teilweise wiederum aus mehreren Einzelobjekten bestehen:

Hauptobjekt	**Einzelobjekte**
Achse	Rubrikenachse, Größenachse
Datenreihe	einzelne Datenreihen
Datenpunkt	einzelne Datenpunkte
Legende	(keine)
Beschriftung	Diagramm-Überschrift, Rubrikenachsenbeschriftung, Größenachsenbeschriftung, einzelne Größenbeschriftungen, freie* Beschriftungen
freie* Linie	einzelne freie* Linien

* unter *freien* Objekten sind manuell in ein Diagramm eingefügte zusätzliche Beschriftungen und Linien zu verstehen

Abbildung 4.8: Die Objekte eines Diagramms

Jede Datenreihe setzt sich

- aus den *Rubriken* und
- den diesen Rubriken zugeordneten numerischen *Größen*

zusammen, die auf der *Rubrikenachse*[1] bzw. der *Größenachse*[2] aufgetragen werden.

- Die Rubriken stellen in einem Diagramm die meist textuellen Beschriftungen der Rubrikenachse dar.
- Die zwischen den Rubriken und der Größenachse bestehenden Beziehungen werden im Diagramm durch Formen (Säulen, Balken usw.) oder Markierungen wiedergegeben, wobei sich die einzelnen Datenreihen durch eindeutige Farben bzw. Graustufen und/oder Schraffierungen unterscheiden sollten.

4.4.1.1 Achsen

Jedes Diagramm weist eine Rubrikenachse (Abszisse) und mindestens eine Größenachse (Ordinate) auf.

- **Rubrikenachse**

  Die in gleich große Beschriftungsfelder (Rubriken) segmentierte Rubrikenachse weist eine bestimmte Semantik auf:

  – zeitspezifisch (Zeitachse),
  – ortspezifisch,
  – objektspezifisch.

  Eine Rubrik kann sein:

  – ein bestimmter Zeitabschnitt (z.B. Tag, Wochentag, Monat);
  – ein bestimmter Ort (z.B. Werk);
  – ein bestimmtes Objekt (z.B. Netzkomponente).

- **Größenachse**

  Die Größenachse besteht aus einem Zahlenstrahl, auf dem die den Rubriken zugeordneten numerischen Größen aufgetragen sind.

4.4.1.2 Grunddiagrammarten

Abhängig von der Art der darzustellenden Daten sind für aussagekräftige Graphiken unterschiedliche Diagrammarten zu verwenden; daher werden im folgenden Kriterien für die Auswahl und Zusammensetzung der in vielen kommerziellen Graphikpaketen enthaltenen Grunddiagrammarten beschrieben.

- **Balkendiagramme (horizontal) und Säulendiagramme (vertikal)**
  – geeignet für den Vergleich einzelner Werte miteinander;
  – in der Regel ungeeignet für die Darstellung des Verhältnisses einzelner Werte zum Gesamtwert.

  Beispiel: Vergleich der Werte für bestimmte Zeitabschnitte (z.B. Tage, Monate) miteinander.

[1] Im allgemeinen wird damit die x-Achse (Abszisse) bezeichnet.

[2] Im allgemeinen wird damit y-Achse (Ordinate) bezeichnet.

Darstellungsmöglichkeiten:

- *nicht gestapelt* [1]*:* jede Rubrik umfaßt mehrere Säulen, die jeweils die dieser Rubrik zugeordneten Werte der Datenreihen darstellen.

  Beispiel: Siehe Abbildung 5.24 auf Seite 97.

- *gestapelt:* jede Rubrik enthält eine kumulierte Säule, die aus den zugehörigen Werten der Datenreihen besteht, d.h. die Höhe der Säule ist gleich der Summe der zu dieser Rubrik gehörenden Einzelwerte.
- *100% aufgestapelt:* wie gestapelt, wobei jede Säule die gleiche Höhe (= 100%) hat und die Einzelwerte mit ihrem prozentualen Anteil ersichtlich sind.

  Beispiel: Siehe Abbildung 5.18 auf Seite 95.

- **Flächendiagramme**
  - stellen Veränderungen über einen Zeitraum dar, wobei die Höhe der Werte in einer zeitabhängigen Datenreihe hervorgehoben wird.
- **Kreisdiagramme**
  - verdeutlichen das Verhältnis einzelner Teile zu einem Ganzen;
  - pro Kreisdiagramm kann jeweils nur eine Datenreihe dargestellt werden.

  Beispiel: Siehe Abbildung 5.20 auf Seite 96.
- **Liniendiagramme**
  - zur Wiedergabe der allgemeinen Tendenz über einen bestimmten Zeitraum;
  - besonders geeignet zur Präsentation einer großen Anzahl von Datenpunkten.

  Beispiel: Siehe Abbildung 5.27 auf Seite 100.
- **Radardiagramme**
  - spezielles Liniendiagramm, dessen Achsen sternförmig von einem Punkt ausgehen, wobei jede Achse eine Datenreihe darstellt;
  - gut geeignet zum Aufzeigen von Symmetrie oder Übereinstimmung von Daten, Radardiagramme die Daten als Funktion der Entfernung von einem zentralen Punkt auftragen.
- **Punktdiagramme**[2]
  - werden hauptsächlich für die Abbildung statistischer Daten benutzt, um die Beziehungen zwischen zwei Variablen hervorzuheben.
- **Spannweitendiagramme**[3]
  - halten die oberen und unteren Werte für einzelne Zeitabschnitte, sowie die Entwicklung über einen gesamten Zeitraum fest.

---

[1] Für den Begriff „gestapelt“ ist auch das Synonym „gestaffelt“ gebräuchlich, im Englischen „stacked“.

[2] Synonym: „XY-Diagramme“.

[3] Synonym: „Aktiendiagramme“.

- **Verbunddiagramme**[1]
  - bestehen aus zwei sich überlagernden oder nebeneinander angeordneten Diagrammen;
  - geeignet zum Vergleich verschiedener Arten von Daten in einem Diagramm.

  Beispiel: Siehe Abbildung 5.23 auf Seite 97.

- **3D-Diagramme**
  - dreidimensionale Darstellung von Balken-, Säulen-, Flächen-, Kreis-, Linien- und Verbunddiagrammen;
  - nach Ansicht des Autors effektvoll für Marketingzwecke (z.B. in Werbeprospekten);
  - nach Ansicht des Autors weniger geeignet für die tägliche Arbeit, da die Übersicht schnell verloren geht und exakte Werte einzelner Datenpunkte wegen der 3D-Verzerrung kaum abzulesen sind.

4.4.2 Mathematische Verfahren zur Verfügbarkeitsanalyse

Definition: *Unter der Analyse*[2] *der Verfügbarkeit mit mathematischen Verfahren ist ihre Untersuchung unter Berücksichtigung ihrer mathematisch erfaßbaren Teilaspekte (wie beispielsweise Regelmäßigkeiten oder Trends) zu verstehen.*

Die Analyse soll damit zur Erreichung der bereits im Abschnitt „Ziele der Aufgabe“ auf Seite 10f. dargestellten Zielsetzung einer Verfügbarkeitsdokumentation beitragen.

Bei der Analyse muß die ihr jeweils zugrunde liegende Verfügbarkeitsdatenreihe derart dargestellt werden, daß die folgenden beiden Kriterien erfüllt werden:

- Tendenz-Analyse:

  aus der Auswertung sollte für die Analyse möglichst einfach ablesbar sein, welche Tendenz (fallend, gleich bleibend, steigend oder nicht eindeutig) die von dieser Datenreihe abgebildete Verfügbarkeit aufweist.

- Analyse der quantitativen Prognosen:

  eine weitergehende auf mathematische Verfahren (z.B. Berechnung künftiger Trends) aufbauende quantitative Prognose sollte analysiert werden können.

Mathematische Verfahren, die sich zur Analyse der Verfügbarkeit eignen, müssen die nachstehenden Gegebenheiten der Verfügbarkeitsdatenreihen berücksichtigen:

- Große Datenquantität:

  die Verfügbarkeitsdatenreihen bestehen häufig aus sehr vielen Einzeldaten (sogenannten Beobachtungen[3]), die in einem Diagramm übersichtlich darzustellen sind.

---

1 Synonym: „Mischdiagramme“.

2 analysis (griech.) = Auflösung.

3 Eine Beobachtung ist nach [HEINEN] definiert als eine „planmäßige Erfassung sinnlich wahrnehmbarer Tatbestände ohne Einflußnahme auf den Beobachtungsbereich“.

- Starke Schwankungen (Volatilität[1]) der Einzelwerte:

  Besonders im Bereich der Verfügbarkeit treten üblicherweise stärker voneinander abweichende, aufeinanderfolgende Einzelwerte auf, was bei ihrer Abbildung in einem Liniendiagramm zu einem sehr volatilen Graphen führt.

Beispiel: Für eine Jahresauswertung der Verfügbarkeit steht eine Datenreihe mit Daten für jeden einzelnen Tag, also 365 bzw. 366 Beobachtungen, zur Verfügung. Stellt man diese in einem Diagramm dar, kann eine so extreme Zick-Zack-Kurve von der Verfügbarkeit entstehen, daß kaum ein Trend auszumachen und schon gar keine Trendprognose möglich ist (vergleiche dazu Abbildung 5.25 auf Seite 98).

In der mathematischen Statistik gibt es eine Vielzahl von Verfahren, die alle — durch geeignete Zusammenfassung und teilweise auch Gewichtung von Daten — Trends in den zugrunde liegenden Datenreihen aufzeigen und quantitative Prognosen erleichtern können, wobei immer ein Kompromiß zu schließen ist zwischen

- dem Wunsch nach einer guten Glättung der zufälligen Schwankungen (Volatilität der Verfügbarkeitseinzeldaten) und
- einer hinreichenden Reaktionsfähigkeit auf grundlegende (Trend-)Änderungen der Verfügbarkeit.

Im folgenden werden diese Funktionen und Notation verwendet:

- Es sei eine Verfügbarkeitsdatenreihe v gegeben, die aus n Einzelwerten (Beobachtungen) $v_1, \ldots, v_n$ bestehen, wobei
  - v_1 der Wert der ältesten (ersten) Beobachtung und
  - v_n der Wert der jüngsten (letzten) Beobachtung

  von v seien.
- Weiter sei m ($m << n$) die Anzahl der Beobachtungen, aus denen jeweils ein gleitender Durchschnittswert berechnet werden soll (Zusammenfassung).

1. Einfacher gleitender Durchschnitt (Simple Moving Average, SMA[2])

- Der SMA berechnet jeweils das arithmetische Mittel aus einer vorgegebenen festen Anzahl m von Einzeldaten; in der graphischen Darstellung erhält man eine Linie[3], die um so glatter wird, je mehr Beobachtungen jeweils der Berechnung eines einzelnen SMA-Wertes zugrunde gelegt werden.
- Es seien
  - b, $1 \le b \le n-m+1$, der Index derjenigen Beobachtung, bei dem die Berechnung eines SMA-Wertes *beginnt*;
  - $e := b+m-1$ der Index derjenigen Beobachtung, bei dem die Berechnung eines SMA-Wertes *endet*.

---

1 volare (lat.) = fliegen, sich schnell bewegen.

2 Man findet häufig auch die Abkürzung „MA“, wenn der einfache gleitende Durchschnitt gemeint ist.

3 Daher sind beim SMA die Begriffe „Glättungsfunktion“ bzw. „Glättungslinie“ für seine graphische Darstellung ebenfalls verbreitet.

– Dann gilt: $\mathrm{SMA}(v, b, e) := \frac{\sum_{t=b}^{e} v_t}{e-b+1} = \frac{\sum_{t=b}^{e} v_t}{m}$.

– Damit lassen sich für die gegebenen n Einzelwerte die folgenden (n–m+1) SMA-Werte SMA(v, 1, m), SMA(v, 2, m+1), SMA(v, 3, m+2), …, SMA(v, n–m+1, n) berechnen.

Bemerkung: *Um Rechenzeit zu sparen, sollten nach der Berechnung des ersten SMA-Wertes nach der obigen Formel alle weiteren folgendermaßen optimiert errechnet werden:*

$$\mathrm{SMA}(v, b+1, e+1) = \frac{m \cdot \mathrm{SMA}(v, b, e) - v_b + v_{e+1}}{m}.$$

Beispiel: Siehe Abbildung 5.25 auf Seite 98.

2. Gewichteter gleitender Durchschnitt (Weighted Moving Average, WMA)

– Der WMA ist dem SMA ähnlich; der einzige Unterschied besteht darin, daß *zeitlich jüngere Beobachtungen jeweils stärker gewichtet* werden; die Gewichtungen sind proportional zum Alter der Beobachtung.

– Die Indizes b und e seien analog dem SMA definiert.

– Dann gilt: $\mathrm{WMA}(v, b, e) := \frac{\sum_{t=b}^{e} \frac{v_t}{e+b-t+1}}{\sum_{i=1}^{e-b+1} \frac{1}{i}} = \frac{\sum_{t=b}^{e} \frac{v_t}{m+b-t}}{\sum_{i=1}^{m} \frac{1}{i}}$.

3. Exponentiell gewichteter gleitender Durchschnitt (Exponential Moving Average, EMA)

– Die Beliebtheit dieser Analyse- und Prognosetechnik gründet sich auf
  * ihre methodische Einfachheit und
  * den geringen Speicherplatzbedarf.

Der Prognosewert EMA(v, i, α) ergibt sich bei der exponentiellen Glättung (exponential smoothing), indem man zum vorherigen Vorhersagewert EMA(v, i–1, α) den mit dem Glättungsfaktor α multiplizierten Vorhersagefehler addiert, wobei der Vorhersagefehler definiert ist als Differenz zwischen dem tatsächlichen Wert v_{i-1} und dem vorherigen Prognosewert EMA(v, i–1, α).

– Der Glättungsfaktor α ($0 \le \alpha \le 1$) bewirkt die Anpassung der Prognose an die jüngste Entwicklung der Verfügbarkeit:
  * bei $\alpha = 0$ wird der Prognosefehler nicht berücksichtigt — die Entwicklung wird als konstant angenommen, d.h. das Modell reagiert nicht auf Verfügbarkeitsschwankungen;
  * bei $\alpha = 1$ wird der Prognosewert um den vollen Prognosefehler korrigiert — die neuesten Verfügbarkeitswerte werden stark berücksichtigt, was zu größeren Prognoseschwankungen führen kann.

  Die Wahl von α hängt damit wesentlich von der Anzahl Einzeldaten (Beobachtungen) ab, die in die Berechnung mit signifikantem Einfluß eingehen sollen. Als Wert für den Glättungsfaktor erweist sich in vielen Fällen $0{,}2 \le \alpha \le 0{,}5$ als brauchbar.

– Dann gilt:

$$\mathrm{EMA}(v,i,\alpha) := \left\{ \begin{array}{ll} v_1 & \text{für } i = 1 \\ \mathrm{EMA}(v,i-1,\alpha) + \alpha(v_{i-1} - \mathrm{EMA}(v,i-1,\alpha)) & \text{für } 1 < i \le n \end{array} \right\} =$$

$$= \left\{ \begin{array}{ll} v_1 & \text{für } i = 1 \\ (1-\alpha)\cdot \mathrm{EMA}(v,i-1,\alpha) + \alpha v_{i-1} & \text{für } 1 < i \le n \end{array} \right\}.$$

Bei nicht-rekursiver Darstellung wird die exponentielle Gewichtung deutlich:

$$\mathrm{EMA}(v,i,\alpha) = \underbrace{(1-\alpha)^{i-1}\cdot \mathrm{EMA}(v,1,\alpha)}_{\to 0 \text{ für große } i} + \sum_{k=2}^{i} (1-\alpha)^{i-k}\alpha v_{k-1} \text{ für } i > 1.$$

Bemerkung: *Aufgrund seines für das Ergebnis nicht signifikanten Einflusses kann man den Start-EMA-Wert* $\mathrm{EMA}(v, 1, \alpha)$ *auch gleich* 0 *setzen.*

5 Technische Erstellung einer Verfügbarkeitsdokumentation

Dieses Kapitel beschreibt mit Hilfe der benutzten technischen Verfahren und eingesetzten Werkzeuge einen Lösungsansatz für die Erstellung einer Verfügbarkeitsdokumentation für den LAN- und WAN-Bereich nach Maßgabe der bisher erarbeiteten Ergebnisse:

1. der erste Abschnitt auf Seite 67f. zeigt, wie die zur Integration erforderliche Identifikation und Korrelation von Netzkomponenten in den Netzmanagementsystemen und dem Netzdokumentationssystem realisiert werden kann;
2. im zweiten Abschnitt auf Seite 68f. werden die von dem bei BMW als Verfügbarkeitsdatenquelle eingesetzten Netzmanagementsystem SPECTRUM offerierten Datenexport-Alternativen beleuchtet;
3. der dritte Abschnitt auf Seite 69f. beschreibt die Realisierung der Datenvorverarbeitung;
4. das als Datensenke dienende (Oracle-)Datenbanksystem ist Thema des vierten Abschnitts auf Seite 77f.;
5. im fünften Abschnitt auf Seite 78f. wird die Realisierung der interaktiven Daten(nach)bearbeitung und der Fehlerklassifizierung behandelt;
6. der letzte Abschnitt auf Seite 89f. demonstriert die Realisierung von Verfügbarkeitsstatistiken und -diagrammen.

Einige Daten zur Netzinfrastruktur bei BMW

Der LAN-Verbund bei BMW besteht aus einem FDDI-Backbone mit derzeit 14 Cisco-Brouters der Serie 7000. Zu unterscheiden ist dabei der *Local-Bereich* (LAN-LAN-Anbindungen: Kernbereich München) und der *Remote-Bereich* (LAN-WAN-Anbindungen: Außenstellen, Werke und internationale Verbindungen).

- **Local-Bereich**
  - Hier sind derzeit 9 Cisco-Brouters mit ca. 60 Ports (Ethernet-, Token-Ring- und FDDI-Anbindungen) installiert.
- **Remote-Bereich**
  - Hier sind derzeit 5 Cisco-Brouters mit ca. 40 seriellen Ports (Übertragungsraten 2,4 / 7,2 / 9,6 / 28 / 48 / 64 / 256 / 512 kbps) installiert.

– Für den WAN-Verbund ist zwar primär die WAN-Gruppe zuständig, welche den Ausfall von physischen Leitungen (vor allem die von der Deutschen Telekom gemieteten Leitungen) und Knoten im WAN mit einem proprietären System (TIMEVIEW 2000) überwacht; allerdings kommt es manchmal vor, daß sie Ausfälle von logischen Kanälen im LAN-WAN-Übergang aus technischen Gründen erst verspätet feststellt. Bei derartigen Ausfällen, die sich bei den betroffenen Benutzern durchaus unangenehm bemerkbar machen, kann sich die folgende Konstellation ergeben:
  * WAN-Gruppe: „Bei uns läuft alles problemlos: die physikalische Leitung steht“ versus
  * LAN-Gruppe: „Wir haben einen physikalischen Ausfall: Port-Link-down“.

  Bemerkung: Demnach erhält die LAN-Gruppe, die mit SPECTRUM sowohl Ausfälle der Postleitung als auch Ausfälle logischer Kanäle feststellen kann, in diesem Bereich zuverlässigere Daten, die sich daher für die Auswertung besser eignen.

Überblick: der Datenflußplan

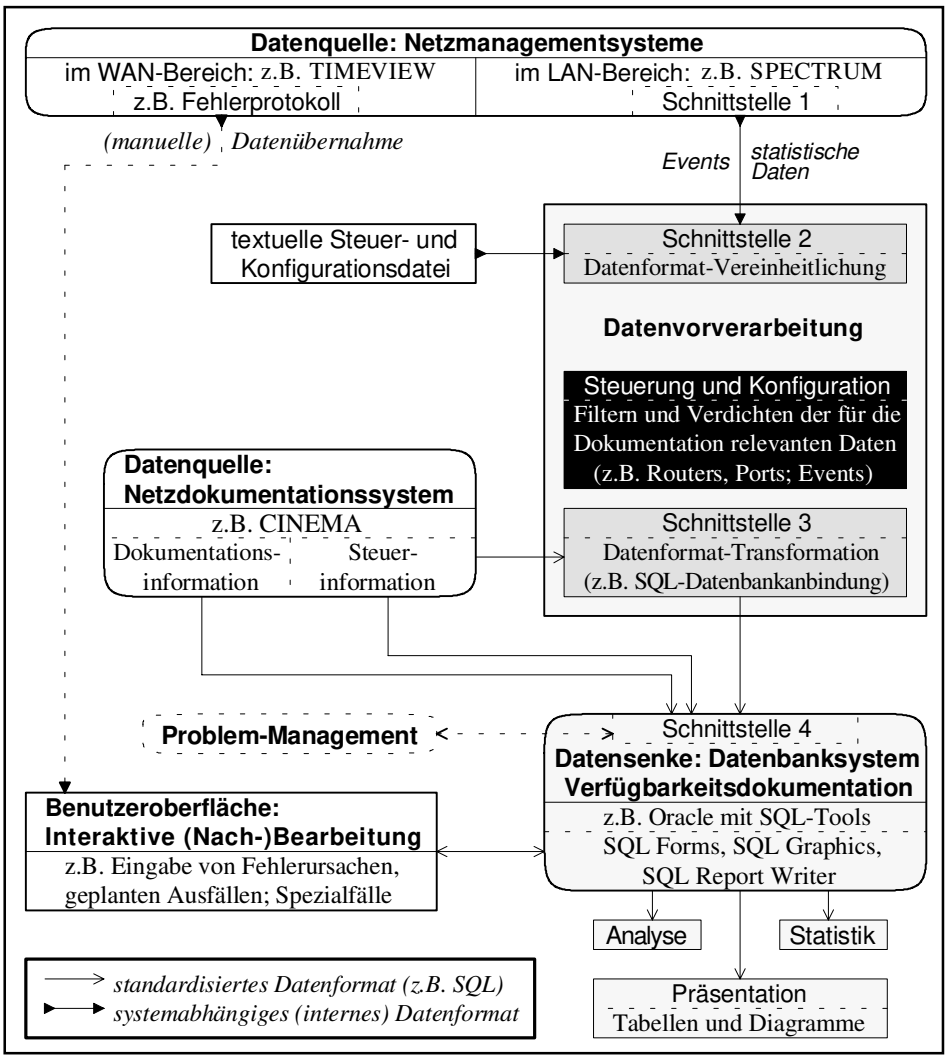

Abbildung 5.1: Datenflußplan

Die Datengewinnungsbasis des gesamten Projektes besteht aus möglichst flexiblen Anbindungen zu den Datenquellen (SPECTRUM, CINEMA) einschließlich Datenvorverarbeitung sowie zu der Datensenke (SQL-Datenbanksystem). Diese Anbindungen und alle erforderlichen Schnittstellen verdeutlicht der Datenflußplan in Abbildung 5.1.

Sobald diese Basis implementiert ist sowie fehlerfrei und stabil läuft, kann die weitere Realisierung (insbesondere die graphische Auswertung) je nach Wunsch stufenweise erfolgen. Die Implementierung wird seit September 1994 im Rahmen von zwei Fortgeschrittenenpraktika durchgeführt, wobei die in diesem Kapitel beschriebenen Anforderungen zugrunde gelegt werden.

Bemerkung: *Für die Realisierung wurde die bereits im Abschnitt „Spiegelung des Netzdokumentationssystems“ auf Seite 51 erörterte Alternative der Datenspiegelung gewählt. Im folgenden wird trotzdem noch von CINEMA gesprochen, um die Herkunft der entsprechenden Daten zu verdeutlichen.*

5.1 Realisierung: Identifikation der Netzkomponenten

Bei der zur Integration erforderlichen Identifikation und Korrelation von Netzkomponenten in den Netzmanagementsystemen (SPECTRUM, NetView/6000) und dem Netzdokumentationssystem (CINEMA) ist zu beachten, daß es sich bei CINEMA um ein ausschließlich manuell gepflegtes System handelt. Daher bestehen bei dem aufgrund der Ausführungen des Abschnitts 4.2.1 zu einer eindeutigen Identifkation verwendeten Namen einer Netzkomponente und ihrer Portbeschreibung geringe Differenzen in der Schreibweise, die einen einfachen Textvergleich zur Entscheidung, ob es sich bei zwei Komponenten in den Netzmanagementsystemen und in CINEMA um identische Objekte handelt, unmöglich macht:

- *Name:*
  - Name eines Cisco-Brouters in SPECTRUM: z.B. „`br7011.muc`“ (genauso ist er auch im Domain Name Service verzeichnet).
  - In CINEMA (und NetView/6000): z.B. „`br7011`“.
- *Portbeschreibung:*
  - Die für die Portbeschreibung verwendete MIB-Variable ifDescr[1] weist bei Cisco-Brouters[2] die Syntax „`NS/P`“ oder „`NS`“ (z.B. „`Ethernet2/0`“ bzw. „`Token-`

[1] [RFC 1213] definiert die Variable `ifDescr` folgendermaßen: „`A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface`“.

[2] Auszug aus [CISCO 1]:

```
locIfDescr OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
         "User configurable interface description."
    ::= { lifEntry 28 }
```

Ring1“) und folgende Semantik auf, die von den Netzmanagementsystemen unverändert übernommen wird:

* N spezifiziert den Netztyp des Ports (z.B. „Ethernet“ bzw. „TokenRing“);
* S, $0 \leq S \leq 99$, spezifiziert die Nummer des Brouterslots (z.B. „2“ bzw. „1“);
* P, $0 \leq P \leq 99$, spezifiziert gegebenenfalls die Nummer des Ports auf der Karte im Slot S (z.B. „0“).

– In CINEMA weicht hier nur die Schreibweise von N ab (z.B. „E2/0“ bzw. „T1“).

- *Lösungsvorschlag:*
  Zwei Komponenten sind genau dann identisch, wenn
  i) ihre Namen bis auf das Suffix (z.B. „.muc“) übereinstimmen *und*
  ii) ihre Portbeschreibungen nur in der Schreibweise des Netztyps (N) differieren.

5.2 Datenquelle: Netzmanagementsystem

Aus dem derzeit bei BMW im LAN-Bereich eingesetzten Netzmanagementsystem SPECTRUM Version 2.0 (Patchlevel 7), das die wesentliche Quelle aktueller Netzdaten für die Verfügbarkeitsdokumentation darstellt, werden die Verfügbarkeitsdaten (Events und statistische Daten) exportiert:

- Identifikationsinformation zumindest mit folgenden Attributen:
  – Name (z.B. Name eines Brouters: „br7011.muc“).
  – Bei Ports zusätzlich: Portbeschreibung (ifDescr).
- Fehlerinformation zumindest mit folgenden Attributen:
  – Exakte Zeitangaben über den Beginn und das Ende jedes Ausfalls.
  – Fehlersymptome, die jeweils Beginn und Ende eines Ausfalls derart markieren, daß daraus eine Ausfalldauer errechnet werden kann.
  – Cisco-MIB-Variable locIfReason[1] zur genaueren Spezifikation einer Statusänderung eines Cisco-Brouterport-Traps.
    Beispiel: Ein geplanter Ausfall eines Ports liegt vor, wenn locIfReason = administratively down, d.h. der Port-Link-down wurde von jemandem gezielt erzeugt.
  – Für die logische Verfügbarkeit: ausgesuchte statistische Daten aus den MIBs der Netzkomponenten.

[1] Auszug aus [CISCO 1]:

```
locIfReason OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "Reason for interface last status change."
    ::= { lifEntry 20 }
```

Abbildung 5.2 zeigt die von SPECTRUM angebotenen Alternativen, Verfügbarkeitsdaten zu exportieren, und Vorschläge für Programmiersprachen, mit denen vorzugsweise auf diese Alternativen zugegriffen werden kann:

Nr.	Werkzeug-Alternative	geeigneter Zugriff über
1	Alarm-Monitor	z.B. Skript-Sprache Perl
2	Command Line Interface (CLI)	z.B. Skript-Sprache Perl
3	Protokolldateien (Logfiles), die vorher durch die grafische Benutzeroberfläche (GUI) SpectroGRAPH erzeugt werden müssen	z.B. Skript-Sprache Perl
4	Application-Programming-Interface des SpectroSERVERs (SS-API)	C++ obligatorisch

Abbildung 5.2: Daten-Export- und Zugriffsalternativen von SPECTRUM

Im Abschnitt „Anbindung zum Netzmanagementsystem“ (siehe unten) wird auf die Wahl der geeigneten Alternative eingegangen.

5.3 Realisierung: die Datenvorverarbeitung

Das Datenvorverarbeitungsmodul, welches, wie aus Abbildung 5.1 auf Seite 66 hervorgeht, aus den drei wesentlichen funktionalen Blöcken

- Anbindung zum Netzmanagementsystem (Schnittstelle 2),
- Steuerung/Konfiguration und
- Anbindung zum Datenbanksystem und Netzdokumentationssystem (Schnittstelle 3)

besteht, muß die bereits in Abschnitt 4.2.2 auf Seite 47f. genannten Anforderungen erfüllen.

5.3.1 Anbindung zum Netzmanagementsystem

Da sich das als Datenquelle eingesetzte Netzmanagementsystem ändern kann, ist die Schnittstelle zwischen dem Netzmanagementsystem und der Datenvorverarbeitung (= Schnittstelle 2 in Abbildung 5.1) möglichst so zu realisieren, daß sie unabhängig von der verwendeten Datenquelle immer Daten im gleichen Format an die Datenvorverarbeitung weiterreicht. Dies hat den großen Vorteil, daß der Pflegeaufwand bei Änderungen der Datenquellen verringert wird, weil die Implementierung der Datenvorverarbeitung und die Definition von Syntax und Semantik des Steuer- und Konfigurationsmoduls weitgehend datenquellenunabhängig realisiert werden können.

Die Schnittstelle 2 muß die Verfügbarkeitsdaten über die Schnittstelle 1 (siehe Abbildung 5.1) aus SPECTRUM exportieren und in einem einheitlichen Format an das Konfigurations- und Steuermodul weiterreichen.

Für die Realisierung der Schnittstelle 1 kommt nur das SpectroSERVER-API (SS-API) infrage, da die übrigen Alternativen (Abbildung 5.2) nicht die geforderte Funktionalität anbieten:

1. Der Alarm-Monitor scheidet aus, weil die von ihm gelieferte Komponenten-Identifikationsinformation unvollständig ist.
2. Das CLI (vergleiche [SPEC_C]) bietet zwar eine vollständige Komponenten-Identifikationsinformation, jedoch ist die Funktionalität des Zugriffs auf die Alarm- und Eventinformation ungenügend:
   - Mit dem CLI-Befehl `show alarms` sind nur die zum Zeitpunkt der Anfrage aktiven Alarme erhältlich; dies hat zur Folge, daß Alarme zwischen den einzelnen Anfragen nicht erfaßt werden können.
   - Mit dem CLI-Befehl `show events` werden *alle* in der SPECTRUM-Datenbank gespeicherten Events angezeigt; die Spezifikation eines Filters, der nur diejenigen Events passieren läßt, welche innerhalb einer angegebenen Zeitspanne aufgetreten sind, ist bei diesem Befehl nicht möglich. Ein externes Filtern scheidet aus, da hierzu zunächst die gewaltige Zahl von Events über das Netz transportiert werden müßte (hohe Netz- und Systembelastung).
3. Die Protokolldateien müssen zuerst erzeugt werden; dadurch ist die geforderte Aktualität der Verfügbarkeitsdaten im Oracle-Datenbanksystem nicht mehr erreichbar.

5.3.2 Steuerung und Konfiguration

Aufgrund der Ausführungen und Folgerung des Abschnitts „Datenvorverarbeitung“ auf Seite 47f. erscheint zur Steuerung und Konfiguration der Datenvorverarbeitung eine Kombination aus Verwendung einer Textdatei und Nutzung des Netzdokumentationssystems CINEMA sinnvoll.

5.3.2.1 Steuerung und Konfiguration durch eine Textdatei

Die Textdatei enthält

- die Spezifikation der von den Netzmanagementsystemen gelieferten Events, die Informationen enthalten, die für die Verfügbarkeitsdokumentation relevant sind; alle übrigen Events und sonstigen von den Netzmanagementsystemen selbst generierten Meldungen müssen von der Datenvorverarbeitung aus dem an das Datenbanksystem weitergeleiteten Datenstrom herausgefiltert werden;
- die Portadresse des Brouterports, der das Netzmanagementsystem versorgt, um eine unterbrochene Verbindung und die daraus resultierenden Verfälschungen der temporären Eingangstabellen zu vermeiden;
- die Zeitspanne in Sekunden, innerhalb der zwei auftretende Fehler derselben Netzkomponente zu einem einzigen zusammenzufassen sind (Verdichtung, siehe Seite 73).

5.3.2.2 Steuerung und Konfiguration durch CINEMA

Das Netzdokumentationssystem CINEMA hat den Großteil der Steuerung und Konfiguration der Datenvorverarbeitung zu erledigen. Daher sind einige Anpassungen erforderlich, die auf zwei Arten realisiert werden können:

1. Änderungen/Ergänzungen der Datenstruktur von CINEMA und aller davon betroffenen Bildschirmmasken.

2. Verwendung eines unbenutzten Feldes für die zusätzlichen Steuer- und Konfigurationsinformationen, wobei mehrere unterschiedliche Daten, die üblicherweise eigene Felder innerhalb der CINEMA-Datenstruktur beanspruchen würden, einfach durch Semikolon getrennt im unbenutzten Feld eingetragen werden können.

Bei BMW soll zunächst die zweite Methode verwendet werden, da die erste Alternative mit einem nicht unerheblichen Realisierungsaufwand verbunden wäre — insbesondere durch die erforderliche Änderung der Bildschirmmasken, die jeweils programmiert werden müßte. Diese Methode ist nur aufgrund der ungünstigeren Übersichtlichkeit bei der Eingabe der Steuer- und Konfigurationsdaten im unbenutzten Feld von Nachteil; durch das Bilden einer sogenannten View — d.h. einem für diesen Anwendungszweck maßgeschneiderten Ausschnitt aus der gesamten Datenstruktur — ist beim Zugriff auf diese Daten kein Unterschied zu der 1. Alternative feststellbar (Transparenz) und daher der spätere Umstieg auf die 1. Methode ohne Änderungen beim Zugriff möglich.

Die folgenden Steuer- und Konfigurationsparameter sollen in CINEMA realisiert werden:

1. Spezifikation der Gewichtung (Priorität) der Ports.

2. Spezifikation der zu überwachenden Netzkomponenten (z.B. Brouters und Ports), von denen Daten zu übernehmen sind; dies wird über die Spezifikation der Gewichtung realisiert, so daß nur die Netzkomponenten überwacht werden, deren Gewichtung ungleich Null ist.

3. Optionale Zusatzangaben bei jedem Port für die späteren Auswertungen:
   - Spezifikation der durch einen Port versorgten Kunden (z.B. BMW-Bank) über eine Kundennummer (hierfür muß eine weitere Tabelle mit den Feldern „Kundennummer“ und „Kundenname“ angelegt werden).
   - Spezifikation der durch einen Port versorgten Orte (z.B. Gebäude).
   - Spezifikation, ob zu einem Port ein Backup existiert (= 1) oder nicht (= 0).
   - Spezifikation des Netzinfrastrukturtyps der Netzkomponente (siehe Abbildung 5.3):

Kennbuchstabe	Netztyp
E	Ethernet
F	FDDI
T	Token Ring
W	WAN

Abbildung 5.3: Kennbuchstaben für die Wahl des Netzinfrastrukturtyps

damit kann beim Auftreten eines Fehlers sofort entschieden werden, wer (LAN-, WAN-, SNA-Gruppe, Wartungspersonal usw.) für dessen Behebung sowie die interaktive Nachbearbeitung zuständig ist und entsprechend informiert werden muß.

– Spezifikation des Typs der Auswertungen, in welche die Daten der betreffenden Netzkomponente eingehen sollen (siehe Abbildung 5.4):

Kennbuchstabe	Typ der Auswertung
B	Backbone
L	Local-Ports
R	Remote-Ports
T	Token-Ring-Ports
W	WAN

Abbildung 5.4: Kennbuchstaben für die Wahl des Auswertungstyps

Bemerkung: Auf diesen Parameter kann verzichtet werden, da er sich durch entsprechende Kombination mehrerer Kennbuchstaben aus Abbildung 5.3 substituieren läßt: `B` *könnte z.B. ersetzt werden durch* `E` & `F` & `T`*).*

5.3.3 Anbindung des lokalen (Oracle-)Datenbanksystems

Die Anbindung des Datenvorverarbeitungsmoduls an das lokale (Oracle-)Datenbanksystem erfolgt über die in Abbildung 5.1 auf Seite 66 dargestellte Schnittstelle 3.

5.3.3.1 Aktualisieren der temporären Eingangstabellen

Die Schnittstelle 3 hat die Funktion, die gefilterten und dann in einem einheitlichen Format vom Steuer- und Konfigurationsmodul gelieferten aufbereiteten Verfügbarkeitsdaten *im Online-Betrieb* zu übernehmen und mit Hilfe von embedded-SQL-Befehlen in die temporären Eingangstabellen im Datenbanksystem, deren Struktur im Abschnitt 5.5.2 auf Seite 81f. dargestellt ist, einzutragen; dabei wird nach folgendem Schema vorgegangen:

1. **Fall: Event, der den *Beginn eines Ausfalls* markiert (z.B. Link-down-Trap)**

   Hierbei handelt es sich um eine neue Störung; daher erfolgt die Anlage eines neuen Datensatzes, der mit der eindeutigen Identifizierung und dem Ausfallzeitpunkt der betreffenden Komponente vorbelegt wird. Die erforderlichen Ausnahmen von diesem Verfahren werden anschließend in den Abschnitten 5.3.3.2 und 5.3.3.3 beschrieben.

2. **Fall: Event, der das *Ende eines Ausfalls* markiert (z.B. Link-up-Trap)**

   Hierbei können zwei Unterfälle auftreten:

   a) *„Normalfall“:* es existiert *eine bereits in* **1.** *eingetragene korrespondierende Störung*; dann wird im bereits vorhandenen Datensatz der Zeitpunkt der Wiederaufnahme des Betriebes der betreffenden Komponente eingetragen.

b) *„Sonderfall“:* es existiert *keine bereits in* **1.** *eingetragene korrespondierende Störung*; dann gibt es keinen passenden Datensatz und damit auch keine Daten über den Ausfall-Beginn, d.h. dieser Event ist für die Auswertung unbrauchbar und daher zu ignorieren.

5.3.3.2 Empfehlung zum Realisieren der Realzeit-Verdichtung

Bei zyklischen Fehlern, die sich bei einer Netzkomponente innerhalb einer benutzerbestimmbaren Zeitspanne (z.B. 60 Sekunden) wiederholen, würde das strenge Vorgehen nach dem oben beschriebenen Verfahren zu einer gewaltigen Anzahl von Datensätzen in den temporären Eingangstabellen führen, die alle zu einem einzigen Fehler gehören. Um dies zu verhindern, muß für eine Realzeit-Verdichtung in den temporären Eingangstabellen gesorgt werden, die insbesondere zu

- einem geringeren manuellen Aufwand und
- einer besseren Übersichtlichkeit

der interaktiven Nachbearbeitung (siehe Abschnitt 5.5 auf Seite 78f.) führt und folgendermaßen realisiert werden kann:

Wenn bei derselben Netzkomponente innerhalb der in der textuellen Steuer- und Konfigurationsdatei (siehe Abschnitt 5.3.2.1 auf Seite 70) spezifizierten Zeitspanne (z.B. 60 Sekunden) ein weiterer Fehler auftritt, wird im Datenbanksystem — abweichend von dem im vorigen Abschnitt 5.3.3.1 beschriebenen 1. Fall — *kein* neuer Datensatz angelegt, sondern nur der schon beim ursprünglichen Fehler angelegte aktualisiert, so daß der bereits eingetragene Ausfall-Ende-Zeitpunkt mit dem neuen Ausfall-Ende-Zeitpunkt überschrieben wird.

Ein Verfahren zur stufenweisen Reduktion und Archivierung des Verfügbarkeitsdatenbestandes ist im Abschnitt „Die Archivtabellen“ auf Seite 87 beschrieben.

5.3.3.3 Empfohlene Behandlung von Contact-lost-Meldungen

Meldungen eines Netzmanagementsystems über den Verlust der Verbindung zu einer Netzkomponente („Contact lost“ bei SPECTRUM bzw. „Node down“ bei NetView/6000), können zwei Ursachen haben:

1. „Normalfall“: Störung der Komponente;
2. „Sonderfall“: Zugang des Netzmanagementsystems zum Netz unterbrochen (vergleiche Seite 57).

Der 1. Fall ist unkritisch und bedarf keiner weiteren Sonderbehandlung.

Beim 2. Fall dagegen muß verhindert werden, daß diese „falsche Fehlermeldung“ in die temporären Eingangstabellen gelangt; dazu wird das folgende Verfahren vorgeschlagen:

Jedesmal, wenn das Datenvorverarbeitungsmodul vom Netzmanagementsystem eine derartige Meldung erhält, überprüft es (beispielsweise mit Hilfe des Ping-Befehls), ob die Leitung zu

dem Brouter-Port, der das Netzmanagementsystem mit dem Netz verbindet, noch steht — ist dies nicht der Fall, wird die Meldung ignoriert. Die Adresse dieses Brouter-Ports wird dem Modul über die textuelle Steuer- und Konfigurationsdatei übergeben.

5.3.4 Berechnen der Ausfalldauer am Beispiel von Cisco-Brouters

Die folgenden Traps von Cisco-Brouters sind für die physikalische Verfügbarkeit zu erfassen und auszuwerten (Auszug aus [CISCO]):

```
coldStart TRAP-TYPE
    ENTERPRISE  snmp
    VARIABLES   { sysUpTime, whyReload }
    DESCRIPTION
                "A coldStart trap signifies that the sending
                protocol entity is reinitializing itself such
                that the agent's configuration or the protocol
                entity implementation may be altered."
    ::= 0

-- Cisco does not generate warmstart traps

linkDown TRAP-TYPE
    ENTERPRISE  snmp
    VARIABLES   { ifIndex, ifDescr, ifType, locIfReason }
    DESCRIPTION
                "A linkDown trap signifies that the sending
                protocol entity recognizes a failure in one of
                the communication links represented in the
                agent's configuration."
    ::= 2

linkUp TRAP-TYPE
    ENTERPRISE  snmp
    VARIABLES   { ifIndex, ifDescr, ifType, locIfReason }
    DESCRIPTION
                "A linkUp trap signifies that the sending
                protocol entity recognizes that one of the
                communication links represented in the agent's
                configuration has come up."
    ::= 3
```

Bei Ausfällen von Cisco-Brouters und deren Ports können demnach die in Abbildung 5.5 aufgeführten vier Fälle auftreten; damit ergibt sich die Ausfalldauer als zeitliche Differenz zwischen einem Eintrag in der Spalte „Ausfall-Beginn“ und dem zugehörigen (d.h. in der gleichen Zeile stehenden) Eintrag in der Spalte „Ausfall-Ende“.

Nr.	korrespondierende Events für		ausgefallene Komponente
	Ausfall-Beginn	Ausfall-Ende	
1	Link-down-Trap*	Link-up-Trap*	ein einzelner Port (nicht Token-Ring)
2	Link-down-Trap* (Sonderbehandlung erforderlich)	Link-up-Trap*	ein einzelner Token-Ring-Port
3	Contact-lost-Meldung**	Contact-Meldung**	der gesamte Brouter
4	Contact-lost-Meldung**	Cold-Start-Trap*	der gesamte Brouter

* von einem Gerät gesendeter SNMP-Trap, der vom Netzmanagementsystem wiedergegeben wird

** Hinweis eines Netzmanagementsystems (hier: SPECTRUM), daß es mit Hilfe des durchgeführten Pollings eine Zustandsänderung eines Gerätes festgestellt hat (bei IBMs NetView/6000 lauten die entsprechenden Meldungen „Node down“ bzw. „Node up“)

Abbildung 5.5: Korrespondierende Events zur Berechnung der Ausfalldauer

Berechnung der Ausfalldauer nach Abbildung 5.5 (Auszüge aus der Event-Protokolldatei „Event Log“ von SPECTRUM):

1. Zu Nr. 1 in Abbildung 5.5: Vollständiger Zyklus (mit den von SPECTRUM generierten Alarmen) — Link-down- bis Link-up-Trap bei Ports (gilt nicht für Token-Ring-Ports)

Erläuterung zum Event Log:

- es handelt sich um einen Port mit dem (SPECTRUM-spezifischen) ModelTypeName `Gen_IF_Port`,
- interne laufende Port-Nummer (ifIndex): `8`,
- Portbeschreibung (ifDescr): *Ethernet-Port Nummer* `0` *auf der Karte im Slot Nummer* `2`,
- Brouter-Name: `br7011.muc`, Brouter-ModelTypeName: `Rtr_Cisco`.

i) SPECTRUMs Wiedergabe des Brouter-Link-down-Traps:

```
Tue 17 May, 1994 - 9:37:33 A(n) Rtr_Cisco device, named br7011.muc,
has detected a Communication Link Down. ifIndex = 8. ifDescr =
Ethernet2/0. ifType = 6. locIfReason = Keepalive failed. (event
[00220001])
```

ii) SPECTRUM-generierter zugehöriger gelber Alarm für den Brouter:

```
Tue 17 May, 1994 - 9:37:33 - Alarm number 1442 generated for device
br7011.muc of type Rtr_Cisco. Current condition is YELLOW. (event
[00010701])
```

iii) SPECTRUM-Meldung für den ausgefallenen Port:

```
Tue 17 May, 1994 - 9:37:33 Communication Link Down for Gen_IF_Port
port, named br7011.muc. locIfReason = Keepalive failed. (event
[00220003])
```

iv) SPECTRUM-generierter roter Alarm für den ausgefallenen Port:

```
Tue 17 May, 1994 - 9:37:35 - Alarm number 1443 generated for device
br7011.muc of type Gen_IF_Port. Current condition is RED. (event
[00010701])
```

v) SPECTRUMs Wiedergabe des Brouter-Link-up-Traps:

```
Tue 17 May, 1994 - 9:37:35 A(n) Rtr_Cisco device, named br7011.muc,
has detected a Communication Link Up. ifIndex = 8. ifDescr =
Ethernet2/0. ifType = 6. locIfReason = Keepalive OK. (event
[00220002])
```

vi) Löschen des zugehörigen von SPECTRUM generierten gelben Alarms ii) für den Brouter:

```
Tue 17 May, 1994 - 9:37:35 - Alarm number 1442 cleared for device
br7011.muc of type Rtr_Cisco. (event [00010702])
```

vii) SPECTRUM-Meldung für den wieder erreichbaren Port:

```
Tue 17 May, 1994 - 9:37:35 Communication Link Up for Gen_IF_Port
port, named br7011.muc. locIfReason = Keepalive OK. (event
[00220004])
```

viii) Löschen des zugehörigen von SPECTRUM generierten roten Alarms iv) für den wieder erreichbaren Port:

```
Tue 17 May, 1994 - 9:37:35 - Alarm number 1443 cleared for device
br7011.muc of type Gen_IF_Port. (event [00010702])
```

Resultat: Dieser Ausfall des Ports dauerte 2 Sekunden, nämlich von i) *bis* v).

2. Zu Nr. 2 in Abbildung 5.5: Zyklus (ohne Alarme) — Link-down- bis Link-up-Trap bei Token-Ring-Ports

i) `Tue 08 Mar, 1994 - 7:50:51 - A(n) Rtr_Cisco device, named br0181.muc, has detected a Communication Link Down. ifIndex = 4. ifDescr = TokenRing0. ifType = 9. locIfReason = Keepalive failed. (event [00220001])`

ii) `Tue 08 Mar, 1994 - 7:51:01 - A(n) Rtr_Cisco device, named br0181.muc, has detected a Communication Link Down. ifIndex = 4. ifDescr = TokenRing0. ifType = 9. locIfReason = initializing. (event [00220001])`

iii) `Tue 08 Mar, 1994 - 7:51:10 - A(n) Rtr_Cisco device, named br0181.muc, has detected a Communication Link Up. ifIndex = 4. ifDescr = TokenRing0. ifType = 9. locIfReason = up. (event [00220002])`

Bemerkung: *Bei ausgefallenen Token-Ring-Ports versucht der Brouter, den Port während der gesamten Dauer des Ausfalls ständig wieder in Betrieb zu setzen; dabei wird der obige Zyklus* i) *bis* iii) *mehrmals in einer Minute durchlaufen. Aufgrund der in der Datenvorverarbeitung vorgenommenen Realzeit-Verdichtung (siehe Abschnitt 5.3.3.2 auf Seite 73) stellt dies jedoch kein Problem dar, d.h. es wird nur ein einziger Datensatz erzeugt.*

Achtung: *Zu dem in Abhängigkeit von der Ausfallursache (z.B. lockerer Stecker) eventuell zusätzlich auftretenden Link-down-Trap* ii), *welcher durch* `locIfReason = initializing` *gekennzeichnet ist, gibt es keinen korrespondierenden Link-up-Trap; daher darf er keinen Eintrag in der temporären Eingangstabelle verursachen, ist also durch die Datenvorverarbeitung unbedingt herauszufiltern, da andernfalls ein unvollständiger Datensatz entstünde, der manuell gelöscht werden müßte.*

Resultat: *Dieser Teil des Ausfalls des Token-Ring-Ports dauerte 5 Sekunden, nämlich von* i) *bis* iii).

3. **Zu Nr. 3 in Abbildung 5.5: Zyklus (ohne Alarme) — Contact-lost- bis Contact-Meldung:**

   i) `Wed 28 Sep, 1994 - 10:21:21 - Contact has been lost with device test7000.muc of type Rtr_Cisco. (event [00010302])`

   ii) `Wed 28 Sep, 1994 - 10:21:26 - Device test7000.muc of type Rtr_Cisco has been contacted. (event [00010301])`

   Resultat: Dieser Ausfall des Brouters dauerte 5 Sekunden, nämlich von i) *bis* ii).

4. **Zu Nr. 4 in Abbildung 5.5: Zyklus (ohne Alarme) — Contact-lost-Meldung bis Cold-Start-Trap:**

   i) `Wed 28 Sep, 1994 - 11:00:56 - Contact has been lost with device test7000.muc of type Rtr_Cisco. (event [00010302])`

   ii) `Wed 28 Sep, 1994 - 11:01:55 - A(n) Rtr_Cisco device, named test7000.muc, has been cold started. SystemUpTime = 5118. event [00010013])`

   Resultat: Dieser Ausfall des Brouters dauerte 59 Sekunden, nämlich von i) *bis* ii).

5.4 Datenbanksystem und Anbindungen

Das Datenbanksystem bildet die gemeinsame Datensenke für die gesamte Verfügbarkeitsdokumentation; für die Integration des Datenbanksystems sind die in den folgenden Unterabschnitten behandelten Spezifikationen zu realisieren:

1. SQL-Kopplung mit dem Netzdokumentationssystem CINEMA;
2. Anbindung zum Problemmanagement.

5.4.1 Kopplung mit dem Netzdokumentationssystem

Da es sich beim Netzdokumentationssystem CINEMA ebenfalls um ein Oracle-SQL-Datenbanksystem handelt, kann die Kopplung vollständig über SQL erfolgen, so daß keine Schnittstelle im Sinne einer Datenformat-Transformation zu implementieren ist.

Bevor die Kopplung durchgeführt werden kann, sind zunächst die in CINEMA enthaltenen Netzdokumentationsdatenbanktabellen teilweise zu erweitern, wie dies im Abschnitt 5.3.2.2 auf Seite 71 beschrieben ist.

Bemerkung: *Eine erste Messung ergab, daß die auf Seite 51 erörterte Spiegelung der relevanten CINEMA-Daten(strukturen) auf die lokale Oracle-Datenbank ca. 20 Minuten dauert. Dabei ist allerdings zu berücksichtigen, daß noch mehr Daten(strukturen) kopiert werden, als für die Verfügbarkeitsdokumentation erforderlich sind; d.h. die Dauer einer Spiegelung kann noch verkürzt werden.*

5.4.2 Anbindung an das BMW-Problemmanagement

Die Verwendung des Datenbanksystems als Datenserver für das BMW-Problemmanagement-Werkzeug als weiterer Schritt in Richtung Datenintegration im integrierten Netzmanagement bedarf genauer Analysen, die jedoch sowohl den Rahmen dieser Arbeit sprengen als auch über das Thema hinausgehen würden (vergleiche den Abschnitt „Weitere Arbeiten“ auf Seite 114).

5.5 Realisierung: die interaktive Daten(nach)bearbeitung

Dieser Abschnitt beschreibt die für die Realisierung der interaktiven Daten(nach)bearbeitung erforderlichen Werkzeuge:

- der erste Unterabschnitt geht ausführlich auf die bei der interaktiven (Nach-)Bearbeitung erforderliche Fehlerklassifizierung ein;
- die Unterabschnitte zwei und drei spezifizieren die im Datenbanksystem für die Speicherung und interaktive (Nach-)Bearbeitung der Verfügbarkeitsdaten nötigen Tabellen;
- der vierte Unterabschnitt faßt alle erforderlichen Tabellen in einer Übersicht zusammen.

5.5.1 Fehlerklassifizierung

Bei der Fehlerklassifizierung muß jedem einzelnen Fehler ein Kürzel zugewiesen werden, um

- die Eingabe effizienter zu gestalten und
- eine spätere fehlerspezifische Auswertung

zu ermöglichen.

Daher wird für das Kürzel ein Zahlencode verwendet, dem — wie bereits im Abschnitt 3.2.3.1 auf Seite 34 vorgeschlagen — die in ISO/IEC 10 164-4 definierten Alarm-Basiskategorien zugrunde gelegt werden. Durch die zusätzliche Verwendung von mehreren Hierarchieebenen bei diesem Code lassen sich auf einfache Weise weitere Fehler-Untergruppen bilden, so daß die Mitarbeiter zu einem Fehler den zugehörigen Code schneller finden und auch die spätere Auswertung einfacher wird.

Der hier verwendete dreistufig-hierarchisch aufgebaute fünfstellige Zahlencode hat die Syntax „`BUF`“ (Basiskategorie — Untergruppe — Fehlernummer) und folgende Semantik:

1. `B`, $0 \leq B \leq 5$, ist die Nummer der Basiskategorie, wobei der Vorgabewert 0 einen unbekannten Fehler repräsentiert;

2. `U`, `00` ≤ `U` ≤ `99`, ist die Nummer der Untergruppe in der Basiskategorie `B`, wobei der Vorgabewert `00` für „allgemein“ steht, d.h. der Fehler kann nicht einer Untergruppe zugeordnet werden;

3. `F`, `00` ≤ `F` ≤ `99`, ist die Nummer des Fehlers in der Untergruppe `U`, wobei der Vorgabewert `00` für „allgemein“ steht, d.h. der Fehler kann nicht einer Nummer zugeordnet werden.

Die folgenden fünf Abbildungen 5.6 bis 5.10 zeigen Beispiele für die Fehlerklassifizierung beim Netzbetreiber BMW für die fünf Basiskategorien, für die in der (Oracle-)Datenbank eine spezielle Fehlercode-Tabelle mit den Datenbankfeldern „Fehlercode“ und „Semantik“ angelegt werden sollte:

B	U	F	Semantik (***Basiskategorie*** — **Untergruppe** — Fehlernummer)
0	00	00	***unbekannter Fehler*** *(allgemein)*
1	00	00	***Communications Alarm Type*** *(allgemein)*
1	01	00	**Verluste** (allgemein)
1	01	01	Signalverlust
1	01	02	Paketverlust
1	02	00	**Protokollfehler** *(allgemein)*
1	02	01	IP
1	02	02	DECNET
1	02	03	LAT
1	02	04	SNA

Abbildung 5.6: Untergliederung der Basiskategorie „Communications Alarm Type“

B	U	F	Semantik (***Basiskategorie*** — **Untergruppe** — Fehlernummer)
2	00	00	***Quality of Service Alarm Type*** *(allgemein)*
2	01	00	**Schwellwert** *(allgemein)*
2	01	01	CPU-Auslastung
2	01	02	Fehlerrate
2	01	03	Leitungsauslastung
2	01	04	Übertragungswiederholung (Retransmission)
2	02	00	**Performance** *(allgemein)*
2	02	01	Antwortzeit
2	02	02	Verweilzeit von Paketen (Delay)

Abbildung 5.7: Untergliederung der Basiskategorie „Quality of Service Alarm Type“

B	U	F	Semantik (***Basiskategorie*** — **Untergruppe** — Fehlernummer)
3	00	00	***Processing Error Alarm Type*** *(allgemein)*
3	01	00	**Konfiguration** *(allgemein)*
3	01	01	Hardware Netzkomponente (z.B. Jumper)
3	01	02	falsche Hardware-Version
3	01	03	Software Netzkomponente (z.B. falsche Parameter)
3	01	04	falsche Software-Version
3	02	00	**Softwarefehler** *(allgemein)*
3	03	00	**Restart/Boot** *(allgemein)*
3	03	01	Netzkomponente
3	03	02	Port
3	03	03	Netz-Software
3	03	04	Karte

Abbildung 5.8: Untergliederung der Basiskategorie „Processing Error Alarm Type“

B	U	F	Semantik (***Basiskategorie*** — **Untergruppe** — Fehlernummer)
4	00	00	***Equipment Alarm Type*** (allgemein)
4	01	00	**Hardware-Problem Netzkomponente** *(allgemein)*
4	01	01	Netzteil
4	01	02	Gehäuse/Chassis
4	01	03	Interface-Karte
4	01	04	Interface-Port
4	01	05	Bus-System
4	01	06	Lüfter
4	01	07	CPU
4	01	08	Speicher
4	01	09	Stecker
4	01	10	Geräte-Sicherung
4	02	00	**Leitungsproblem LAN** *(allgemein)*
4	03	00	**Leitungsproblem WAN** *(allgemein)*

Abbildung 5.9: Untergliederung der Basiskategorie „Equipment Alarm Type“

B	U	F	Semantik (***Basiskategorie*** — **Untergruppe** — Fehlernummer)
5	00	00	***Environmental Alarm Type*** *(allgemein)*
5	01	00	**geplante Ausfälle** *(allgemein)*
5	01	01	Umbau
5	01	02	Umzug
5	01	03	Wartung
5	02	00	**externe Stromversorgung** *(allgemein)*
5	02	01	Gebäude
5	02	02	Verteilerschrank
5	02	03	Netzkabel
5	02	04	Sicherung
5	03	00	**Umwelteinflüsse** *(allgemein)*
5	03	01	Überhitzung
5	03	02	Wassereinbruch
5	03	03	Brand

Abbildung 5.10: Untergliederung der Basiskategorie „Environmental Alarm Type“

5.5.2 Die temporären Eingangstabellen

Die interaktive Daten(nach)bearbeitung erfolgt direkt über die temporären Eingangstabellen des Datenbanksystems. Dabei wird sowohl für den LAN-Bereich (Bearbeiter: LAN-Gruppe) als auch für den WAN-Bereich (Bearbeiter: WAN-Gruppe) eine an die jeweiligen gruppenspezifischen Bedürfnisse angepaßte Bildschirmmaske verwendet, die beide ohne großen Aufwand mit Hilfe eines Maskengenerators (SQL Forms) erstellt werden können.

Der Inhalt der temporären Eingangstabellen kann in bestimmten, von der Größe des zur Verfügung stehenden Hintergrundspeichers abhängigen Zeitabständen (z.B. einmal pro Monat) in die Archivtabellen (siehe Abschnitt 5.5.3 auf Seite 87f.) übertragen und anschließend gelöscht werden.

5.5.2.1 Die Übersichts-Bildschirmmaske

Bei der Übersichts-Bildschirmmaske handelt es sich um ein Fenster, das bei jedem Einstieg in die interaktive Daten(nach)bearbeitung erscheint und die in Abbildung 5.11 dargestellten Felder enthält.

Von der Implementierung her gesehen stellt die Übersichts-Bildschirmmaske das Ergebnis einer speziellen Sicht (View) auf bestimmte Felder der in den temporären LAN- und WAN-Eingangstabellen vorhandenen Datensätze dar.

LAN-/ WAN-Gruppe (L/W)	Nr.	Ausfall-/Fehler-information			Identifikationsinformation		Netz-typ	ange-schlossene Orte	Kunden-Nr.
		Beginn	Ende	Dauer	LAN: Name WAN: WAN-Nr.	LAN: ifDescr WAN: —			

Abbildung 5.11: Felder der Übersichts-Bildschirmmaske

Erläuterungen zu den einzelnen Feldern in Abbildung 5.11:

- „LAN-/WAN-Gruppe“
  Von der Datenbank eingetragener Indikator zur Unterscheidung von Datensätzen, die von der LAN-Gruppe erfaßt wurden („`L`“), von denen, die von der WAN-Gruppe erfaßt wurden („`W`“).
- „Identifikationsinformation“
  Inhalt abhängig von der Datensatzherkunft (LAN- oder WAN-Gruppe):
  - LAN-Gruppe: „Name“ und bei Ports zusätzlich die Portbeschreibung „ifDescr“ (siehe Abschnitt 5.5.2.2 auf Seite 83f.);
  - WAN-Gruppe: nur Angabe der „WAN-Nr.“ (siehe dazu Abschnitt 5.5.2.3 auf Seite 86f.), das andere Feld bleibt leer.
- Die Semantik aller übrigen Felder wird in den Abschnitten 5.5.2.2 auf Seite 83f. bzw. 5.5.2.3 auf Seite 86f. beschrieben.

Leistungsmerkmale der Übersichts-Bildschirmmaske

- Schnelle Übersicht über alle vorhandenen Datensätze, wobei der Anwender z.B. folgende Selektionen vornehmen kann:
  - Standardvorgaben (nach dem Einstieg in die interaktive Daten(nach)bearbeitung):
    * die Datensätze werden aufsteigend sortiert angezeigt, wobei als Sortierkriterium der Ausfall-Beginn dient;
    * Anzeige aller noch nicht quittierten (nachbearbeiteten) Datensätze;
    * Anzeige aller Datensätze, die eine bestimmte Mindestausfalldauer einer Komponente beinhalten (Standardvorgabe: z.B. fünf Minuten).
  - Anzeige aller Datensätze, die um einen bestimmten Zeitpunkt herum aufgetreten sind.
  - Anzeige aller Datensätze der LAN-Gruppe.
  - Anzeige aller Datensätze der WAN-Gruppe.
- Angabe von zusätzlichen Selektionskriterien, um bestimmte Ausfälle zu finden, wie beispielsweise
  - Datum,
  - Uhrzeit,
  - Ausfallursache,

  - ausgefallene Komponente,
  - Netztyp.

- Direkte Daten(nach)bearbeitung oder vollständiges Ansehen eines Datensatzes durch einfaches Markieren der betreffenden Zeile (Anklicken mit der Maus).

Aufgrund dieser umfangreichen Leistungsmerkmale ist die Funktionalität der Übersichts-Bildschirmmaske dem Alarmfenster (Alarm-View) der bisherigen Netzmanagementsysteme in folgenden Punkten überlegen:

- Online-Anzeige von Topologiedaten (angeschlossene Orte und Kundennummern).
- Ein besonderer Vorteil gegenüber SPECTRUM besteht darin, daß Alarmmeldungen in der Übersichts-Bildschirmmaske bis zu ihrer manuellen Quittierung angezeigt werden — bei SPECTRUM dagegen erscheinen immer nur die gerade aktiven Alarme, so daß viele Alarme von den Mitarbeitern erst gar nicht bemerkt werden, da sie das Alarmfenster nicht ununterbrochen beobachten können.

Daher ist es sinnvoll, künftig verstärkt mit der Übersichts-Bildschirmmaske zu arbeiten, zumal über diese auch die interaktive Daten(nach)bearbeitung erfolgt.

5.5.2.2 Die temporäre Eingangstabelle für den LAN-Bereich

Abbildung 5.12 zeigt die der LAN-Bildschirmmaske zugrunde liegende Tabelle:

Nr.	Identifikations-information		Ausfall-/Fehlerinformation						Backup-information	
	Name	Port-Id. (ifDescr)	Be-ginn	Ende	Dauer	Ursache: Erläu-terung	Ursache: Code	Schwe-re (in %)	vorhanden	Ausfall

Topologieinformation			Zusätzliche Komponenteninformation						Mit-arbeiter	Quit-tung
Kun-den-Nr.	ange-schlos-sene Orte	Standort (W., G., E., S., R.)	Ge-wich-tung	Hersteller	Typ	Modell	Netz-typ	Auswer-tungstyp		

Abbildung 5.12: Temporäre Eingangstabelle für den LAN-Bereich

Beim Eintragen von Daten sind zwei Fälle zu unterscheiden:

1. **„Normalfall“: interaktives Nachbearbeiten von bereits angelegten Datensätzen in der temporären Eingangstabelle**

   In diesem Fall werden die in Abbildung 5.12

- hellgrau unterlegten Spalten automatisch mit den von den Netzmanagementsystemen gelieferten Daten gefüllt,
- schwarz unterlegten Spalten automatisch vom Datenbanksystem selbst vorgegeben,
- dunkelgrau unterlegten Spalten automatisch durch direkte Datenübernahme (Lesen) aus dem Netzdokumentationssystem CINEMA bzw. der lokalen Spiegelung gefüllt,
- nicht unterlegten (weißen) Spalten durch den für die interaktive Daten(nach)bearbeitung zuständigen Mitarbeiter bearbeitet.

2. „Sonderfall“: vollständig manuelles interaktives Erfassen von Datensätzen

Für diesen Fall muß dem Mitarbeiter, der jeweils mit der interaktiven Daten(nach)bearbeitung beauftragt ist, ermöglicht werden, jederzeit Datensätze je nach Erfordernis (vergleiche Abschnitt „Sonderfälle“ auf Seite 53f.)

- neu anzulegen,
- zu löschen und
- Änderungen in allen Spalten (mit Ausnahme der Spalte „Mitarbeiter“) — auch der gegebenenfalls bereits durch Netzmanagement-/Datenbanksysteme gefüllten — vorzunehmen.

Erläuterungen zu den einzelnen Feldern in Abbildung 5.12

1. „Nr.“

Für spätere Referenzzwecke (z.B. für das Problemmanagement) wird eine eindeutige fortlaufende Numerierung benötigt, die automatisch vom Datenbanksystem für alle temporären Eingangstabellen *gemeinsam* generiert wird, um auszuschließen, daß in zwei verschiedenen Tabellen (LAN-/WAN-Bereich) Datensätze mit identischen Nummern angelegt werden.

2. „Identifikationsinformation“

Identifizierung der ausgefallenen Komponente gemäß Abschnitt 5.1 auf Seite 67:

- „Name“: Name der ausgefallenen Komponente.
- „Port-Id. (ifDescr)“: Spezifikation des ausgefallenen Ports

  Achtung: *Wenn dieses Feld leer bleibt, wird die spezifizierte ausgefallene Komponente als vollständiges Gerät (z.B. Brouter) und nicht als Port identifiziert.*

3. „Ausfall-/Fehlerinformation“

- „Beginn“: Datum (Format: tt.mm.jjjj) und genaue Uhrzeit (hh:mm:ss) des Ausfall-Beginns.
- „Ende“: Datum (tt.mm.jjjj) und genaue Uhrzeit (hh:mm:ss) des Ausfall-Endes.
- „Dauer“: Dauer des vom Datenbanksystem aus den Spalten „Beginn“ und „Ende“ berechneten Ausfalls in Minuten und Sekunden (mmmmm:ss).
- „Ursache“: Spezifikation der Ausfall-/Fehlerursache.

  * „Erläuterung“: Textfeld, in dem die Ursache des Ausfalls/Fehlers und/oder Fehlerbehebungsmaßnahmen optional (z.B. bei besonderen Vorfällen) durch zusätzliche Erläuterungen genauer spezifiziert werden kann;
  * „Code“: fünfstelliger Zifferncode der Ausfallursache gemäß der Beschreibung im Abschnitt 5.5.1 auf Seite 78f. (Vorgabe: `00000`).
- „Schwere (in %)“: Schweregrad des Fehlers, der z.B. von der Anzahl der ausgefallenen Protokolle bei erfolgreicher Backupschaltung abhängt, im allgemeinen jedoch 100% (Vorgabe).

4. „Backupinformation“

Spezifikation des Backups für die ausgefallene Komponente:

- „vorhanden“: Eintrag einer „1“, falls ein Backup vorhanden ist bzw. „0“, falls nicht.

  Sonderfall: Das Feld kann manuell mit einer „2“ überschrieben werden, falls es sich bei dem zu erstellenden Datensatz um ein Problem der logischen Verfügbarkeit (z.B. Protokollfehler) handelt, bei dem keine physikalische Ursache vorliegt und daher die Backup-Information nicht relevant ist, da bei derartigen Problemen kein Backup verwendet wird.
- „Ausfall“: Spezifikation der Funktionsfähigkeit des Backups und der trotz des Backups ausgefallenen Anwendungen/Protokolle in Form eines zweistufig-hierarchisch aufgebauten Backup-Ausfall-Codes mit der Syntax „`AP`“ und der aus Abbildung 5.13 ersichtlichen Semantik:

A	P	Semantik (**Anwendung** — Protokoll)
0	0	**Backup erfolgreich** *(allgemein)*
1	0	**CATIA** *(allgemein)*
2	0	**LAN** *(allgemein)*
2	1	DECNET
2	2	IP
2	3	LAT
2	4	LLC
3	0	**SNA** *(allgemein)*
4	0	**Sprache** *(allgemein)*
9	9	**Backup ausgefallen** *(allgemein)*

Abbildung 5.13: Syntax und Semantik des Backup-Ausfall-Codes

5. „Topologieinformation“

- „Kunden-Nr.“
  * bei Ports: Nummer des am Port angeschlossenen Kunden;
  * bei Brouters: Nummern aller an den Ports des Brouters angeschlossenen Kunden.
- „angeschlossene Orte“: Spezifikation der von einem Ausfall einer Netzkomponente direkt betroffenen Orte (z.B. Gebäude).

– „Standort (W., G., E., S., R.)“: Spezifikation des Standortes der ausgefallenen Komponente, unterteilt in die Felder Werk, Gebäude, Etage, Segment, Raum (Hinweis für Reparatur- und Wartungspersonal).

6. „Zusätzliche Komponenteninformation“

– „Gewichtung“: Priorität der Netzkomponente.

– „Hersteller“ / „Modell“ / „Typ“: Hersteller, Modell, Typ der Komponente (für spätere komponentenspezifische Auswertungen).

– „Netztyp“: Spezifikation des Netzinfrastrukturtyps gemäß Abbildung 5.3 auf Seite 71.

– „Auswertungstyp“ (optional): Spezifikation des Auswertungstyps gemäß Abbildung 5.4 auf Seite 72.

7. „Mitarbeiter“

Benutzerkennzeichen (Login-Kennung) des für die Nachbearbeitung bzw. Neuanlage des gerade aktiven Datensatzes verantwortlichen Mitarbeiters.

8. „Quittung“

Feld, dessen Markierung die bereits erfolgte Bearbeitung des betreffenden Datensatzes durch einen Mitarbeiter anzeigt und das Datenbanksystem veranlaßt, den betreffenden Datensatz für weitere automatische Einträge von Daten aus den Netzmanagementsystemen (Aktualisierungen) mit Ausnahme der Realzeit-Verdichtung (siehe Abschnitt 5.3.3.2 auf Seite 73) zu sperren.

Achtung: *die Markierung dieses Feldes darf vom Datenbanksystem nur dann akzeptiert werden, wenn die obligatorischen Felder*
– „Beginn“
– „Ende“
– „Identifikationsinformation“
plausible Einträge enthalten.

5.5.2.3 Die temporäre Eingangstabelle für den WAN-Bereich

Abbildung 5.14 zeigt die der WAN-Bildschirmmaske zugrunde liegende Tabelle.

Im WAN-Bereich können Datensätze derzeit nicht (wie im LAN-Bereich) automatisch in das Datenbanksystem übernommen werden.

Daher sind alle Ausfälle vollständig manuell in die der Abbildung 5.14 entsprechenden Eingabemaske einzutragen, wobei die

- schwarz unterlegten Spalten,
- dunkelgrau unterlegten Spalten und
- nicht unterlegten (weißen) Spalten

genauso wie im vorigen Abschnitt 5.5.2.2 auf Seite 83f. beschrieben zu interpretieren und zu behandeln sind.

Erläuterungen zu den einzelnen Feldern in Abbildung 5.14

- „Identifikationsinformation“
  - „WAN-Nr.“: BMW-eigener Code, der die ausgefallene WAN-Komponente/-Leitung eindeutig identifiziert.
- Alle übrigen Felder sind genauso zu interpretieren wie im vorigen Abschnitt 5.5.2.2 auf Seite 83f. beschrieben.

Nr.	Identifikations-information	Ausfall-/Fehlerinformation					Backup-information	
	WAN-Nr.	Beginn	Ende	Dauer	Ursache		vorhanden	Ausfall
					Erläuterung	Code		

Topologieinformation		Zusätzliche Komponenteninformation						Mitarbeiter	Quittung
Kunden-Nr.	angeschlossene Orte	Standort (W., G., E., S., R.)	Hersteller	Typ	Modell	Netztyp	Auswertungstyp		

Abbildung 5.14: Temporäre Eingangstabelle für den WAN-Bereich

5.5.3 Die Archivtabellen

Die Struktur der Archivtabellen für den LAN- und WAN-Bereich ist — wie schon die der temporären Eingangstabellen — auf die speziellen Bedürfnisse der LAN- bzw. der WAN-Gruppe abgestimmt (siehe Abbildung 5.15):

Kopf jeder Zeile (= Datensatz) der Archivtabelle:

Identifikations-information		Topologieinformation		zusätzliche Komponenteninformation					
Name	Port-Id. (ifDescr)	Kunden-Nr.	angeschlossene Orte	Gewichtung	Hersteller	Typ	Modell	Netztyp	Auswertungstyp

Rest jeder Zeile (= Datensatz) der Archivtabelle:

Kumulierungszeitraum	kumulierte Ausfallinformation					Backupinformation	
	Dauer	Anzahl	Code(s)	Erläuterung(en)	Schwere (in %)	vorhanden	Ausfall

Abbildung 5.15: Archivtabelle für den LAN-Bereich

Die Archivtabellen werden in regelmäßigen Abständen mit den zuvor reduzierten Daten aus den temporären Eingangstabellen gefüllt. Die Reduktion kann und sollte mehrstufig durchgeführt werden, indem alle Datensätze, die innerhalb eines in einer Reduktionssstufe definierten Zeitraums („Kumulierungszeitraum“) angelegt worden sind, für jede vorkommende Netzkomponente zu jeweils einem einzigen Datensatz zusammengefaßt werden. Für den Kumulierungszeitraum der Stufe 1 kann z.B. ein Tag, für den der Stufe 2 eine Woche und für den der Stufe 3 ein Monat gewählt werden.

Die Intensität der Reduktion hängt ab von

- der Menge der zu speichernden Datensätze,
- dem vorhandenen Hintergrundspeicher und
- dem geforderten Detailliertheitsgrad der Archivinformationen.

Hier ist ein Kompromiß zu finden zwischen dem Detailliertheitsgrad der archivierten Verfügbarkeitsdatensätze und der Menge an benötigtem Hintergrundspeicher.

Aufgrund der Reduktion dokumentiert jede Zeile der Archivtabelle sämtliche innerhalb des Kumulierungszeitraums bei einer bestimmten Komponente aufgetretenen Ausfälle; sie besteht jeweils aus einem Zeilenkopf und einem Zeilenrest (vergleiche Abbildung 5.15).

5.5.3.1 Zeilenkopf

Der Kopf jeder Zeile der Archivtabelle (vergleiche Abbildung 5.15) enthält alle für die ausgefallene Komponente spezifischen Daten aus der temporären Eingangstabelle für den LAN- bzw. WAN-Bereich:

1. Identifikationsinformation.
2. Topologieinformation.
   Bemerkung: Die Übernahme des Standortes der ausgefallenen Komponente aus den temporären Eingangstabellen in die Archivtabellen ist nicht erforderlich, da diese Informationen nur kurzzeitig für Wartung und Reparatur benötigt werden, für die Auswertung jedoch irrelevant sind.
3. Zusätzliche Komponenteninformation.

5.5.3.2 Zeilenrest

Der Rest jeder Zeile der Archivtabelle (vergleiche Abbildung 5.15) hat folgenden Aufbau:

1. Kumulierungszeitraum: abhängig von der gewählten Reduktionsstufe.
2. Kumulierte Ausfallinformation: Summe der Dauer der während des Kumulierungszeitraums aufgetretenen Ausfälle, deren Anzahl, Fehlercode(s), Erläuterung(en) und Schweregrad des Fehlers.
3. Backupinformation.

5.5.4 Zusammenfassung: die nötigen Tabellen

Zur Realisierung der Verfügbarkeitsdokumentation müssen im Oracle-Datenbanksystem die folgenden Tabellen neu angelegt werden:

1. eine Netztyp-Tabelle (vergleiche Abbildung 5.3 auf Seite 71);
2. optional: eine Auswertungstyp-Tabelle (vergleiche Abbildung 5.4 auf Seite 72);
3. eine Fehlercode-Tabelle (vergleiche die Abbildungen 5.6–5.10 auf den Seiten 79–81);
4. eine Kunden-Tabelle (vergleiche den Abschnitt 5.3.2.2 auf Seite 71);
5. eine Backupcode-Tabelle (vergleiche Abbildung 5.13 auf Seite 85);
6. je eine temporäre Eingangstabelle für den LAN-Bereich (vergleiche Abbildung 5.12 auf Seite 83) und den WAN-Bereich (vergleiche Abbildung 5.14 auf Seite 87);
7. optional (abhängig von dem zur Verfügung stehenden Hintergrundspeicher): je eine Archivtabelle für den LAN-Bereich (vergleiche Abbildung 5.15 auf Seite 87) und den WAN-Bereich mit unterschiedlichen Reduktionsstufen.

Die unter den obigen Nummern 1 bis 5 aufgeführten Tabellen sollten aus folgenden Gründen im Datenbanksystem erstellt und gepflegt werden, obwohl sie für den Dokumentationsbetrieb nicht zwingend notwendig sind:

- *Zugänglichkeit:* alle damit befaßten Mitarbeiter können die Informationen jederzeit über ihren Bildschirm abfragen; außerdem können die Informationen vom Datenbanksystem in Form von Hilfetexten kontextsensitiv bei der Eingabe angeboten werden.
- *Gewährleistung einer ordentlichen Dokumentation (vergleiche [ISO 9000]):* die Tabellen können jederzeit im Online-Betrieb erweitert werden.
- *Plausibilitätsprüfung bei der Eingabe:* jede Eingabe eines Codes bzw. einer Kundennummer kann vom Datenbanksystem sofort auf Plausibilität überprüft werden.

5.6 Realisierung: Statistiken und Diagramme

Die beiden folgenden Unterabschnitte behandeln die Dokumentation

1. der physikalischen Verfügbarkeit (siehe unten), wobei ein Modell für deren Berechnung vorgestellt wird, sowie
2. der logischen Verfügbarkeit (siehe Seite 99f.)

und geben jeweils konkrete Beispiele für die Realisierung sowie einige Diagramme.

5.6.1 Dokumentation der physikalischen Verfügbarkeit

Bemerkung: *Die folgenden Definitionen gehen davon aus, daß die Daten zur Berechnung der Verfügbarkeit aus den Archivtabellen stammen; selbstverständlich können die entsprechenden Daten auch aus den temporären Eingangstabellen genommen werden.*

5.6.1.1 Definitionen zur Berechnung der physikalischen Verfügbarkeit

1. Liegt ein *Geräteausfall* (z.B. Ausfall eines Brouters) vor, so gelten auch alle Ports in diesem Gerät als ausgefallen (vergleiche dazu den Abschnitt „Sonderfälle“ auf Seite 53f.).

2. *Definition des Zeitraums der Auswertung:*
   i) Jeder Darstellungszeitraum besteht aus gleich großen Intervallen, den sogenannten Beobachtungspunkten, von denen jeder einen Datenpunkt im Diagramm repräsentiert;
   ii) t_0 sei der Beginn und t_1 sei das Ende eines so definierten Intervalls eines Gerätes oder Ports;
   iii) $\Delta t := t_1 - t_0$ sei die Länge eines so definierten Intervalls.

   Beispiel: Nimmt man für den Darstellungszeitraum ein Jahr (Jahresauswertung), so kann als Intervall-Länge Δt z.B. ein Monat (d.h. zwölf Beobachtungen (Datenpunkte) je Datenreihe) oder eine Woche (d.h. 52 Beobachtungen (Datenpunkte) je Datenreihe) gewählt werden.

3. *Zuweisung einer Bezeichnung* für alle in der Netzbetreiberorganisation existierenden Geräte bzw. Ports:
   i) g sei die Anzahl dieser Geräte mit den Namen $\{G_1, \ldots, G_g\} =: \mathcal{G}$;
   ii) p_γ ($\gamma = 1, \ldots, g$) sei die Anzahl der Ports im Gerät G_γ;
   iii) $p := \sum_{\gamma=1}^{g} p_\gamma$ sei die Gesamtanzahl der Ports mit den Namen $\{P_{1,1}, \ldots, P_{1,p_1}, \ldots, P_{g,1}, \ldots, P_{g,p_g}\} =: \mathcal{P}$.

4. $G \supseteq \mathcal{G}$ bzw. $P \supseteq \mathcal{P}$ sei die durch das Steuer- und Konfigurationsmodul spezifizierte *Menge genau jener Geräte bzw. Ports, die in die Auswertung (graphische Darstellung) des Zeitraums* Δt *aufgenommen werden sollen.*

5. $\Gamma: (\mathcal{G} \cup \mathcal{P}) \rightarrow Q$ mit $Q \subset \mathbb{Q}^+$ sei die *surjektive Gewichtungsfunktion*, welche — entsprechend dem Abschnitt „Allgemeine Anforderungen an Auswertungen“ auf Seite 30 — jedem Gerät und jedem Port sein Gewicht (= Bewertung) in Form einer nicht-negativen rationalen Zahl zuordnet.

6. $\sigma_{\gamma,t}$ bzw. $\sigma_{\gamma,\pi,t}$ ($\sigma_{\gamma,t}, \sigma_{\gamma,\pi,t} \in [0,1]$ mit $t_0 \le t \le t_1$) sei der zwischen 0% und 100% liegende *(subjektive) Schweregrad eines Ausfalls* des Gerätes G_γ bzw. des Ports $P_{\gamma,\pi}$ gemäß dem Abschnitt „Allgemeine Anforderungen an Auswertungen“ auf Seite 30, wobei folgende Fallunterscheidung zu beachten ist:

i) zur Ermittlung der physikalischen Verfügbarkeit aus *Sicht der Benutzer* ist der Schweregrad aus den Archivtabellen zu übernehmen;

ii) zur Ermittlung der physikalischen Verfügbarkeit aus *Sicht der Techniker* ist der Schweregrad mit 100% anzunehmen.

7. *Definition der willkürlichen (geplanten) Ausfalldauer* W (z.B. Wartung, Umzug):

   i) W_γ bzw. $W_{\gamma,\pi}$ sei die während des Intervalls Δt kumulierte willkürliche (geplante) Ausfalldauer;

   ii) $W_\gamma := \sum_{t_0 \le t \le t_1} w_{\gamma,t}$ bzw. $W_{\gamma,\pi} := \sum_{t_0 \le t \le t_1} w_{\gamma,\pi,t}$, wobei jedes $w_{\gamma,t}$ bzw. $w_{\gamma,\pi,t}$ jeweils die aus der Archivtabelle ermittelte Dauer desjenigen willkürlichen (geplanten) Ausfalls sei, der zum Zeitpunkt t ($t_0 \le t \le t_1$) aufgetreten ist.

   Bemerkung: Bei willkürlichen (geplanten) Ausfällen wird der (subjektive) Schweregrad $\sigma_{\gamma,t}$ *bzw.* $\sigma_{\gamma,\pi,t}$ *immer mit 100% angenommen.*

8. *Definition der sonstigen Ausfalldauer* S:

   i) S_γ bzw. $S_{\gamma,\pi}$ sei die während Δt kumulierte sonstige Ausfalldauer;

   ii) $S_\gamma := \sum_{t_0 \le t \le t_1} s_{\gamma,t} \cdot \sigma_{\gamma,t}$ bzw. $S_{\gamma,\pi} := \sum_{t_0 \le t \le t_1} s_{\gamma,\pi,t} \cdot \sigma_{\gamma,\pi,t}$, wobei jedes $s_{\gamma,t}$ bzw. $s_{\gamma,\pi,t}$ jeweils die aus der Archivtabelle ermittelte Dauer desjenigen Ausfalls sei, der zum Zeitpunkt t ($t_0 \le t \le t_1$) aufgetreten ist.

9. *Definition der Ausfalldauer* A:

   i) A_γ bzw. $A_{\gamma,\pi}$ sei die während Δt kumulierte Ausfalldauer;

   ii) $A := W + S$.

10. *Definition der theoretisch möglichen Betriebsdauer* T:

    T_γ bzw. $T_{\gamma,\pi}$ sei die aus der Archivtabelle ermittelte während Δt kumulierte theoretisch mögliche (= maximale) Betriebsdauer.

11. *Definition der ungestörten Betriebsdauer* U:

    i) U_γ bzw. $U_{\gamma,\pi}$ sei die während Δt kumulierte ungestörte Betriebsdauer;

    ii) $U := T - A$.

12. *Definition zur Berechnung der physikalischen Verfügbarkeit:*

    i) V_γ bzw. $V_{\gamma,\pi}$ sei die während Δt vorhandene prozentuale physikalische Verfügbarkeit;

    ii) $V := \frac{\text{ungestörte Betriebsdauer U}}{\text{theoretisch mögliche Betriebsdauer T}} \cdot 100\ [\%]$.

5.6.1.2 Folgerungen

In den folgenden Formeln wird jeweils davon ausgegangen, daß eine Menge P von Ports (bzw. eine Menge G von Geräten) gegeben ist, für die im Intervall Δt die physikalische Verfügbarkeit berechnet und graphisch dargestellt werden soll.

1. $U = T - A = T - W - S$.

2. ***Port-Statistik*** *(Geräte-Statistik analog)* ***ohne Berücksichtigung der Gewichtungen:***

   a) *theoretisch mögliche Betriebsdauer* T_P:
   $$T_P = \sum_{P_{\gamma,\pi} \in P} T_{\gamma,\pi};$$

   b) *willkürliche (geplante) Ausfalldauer* W_P:
   $$W_P = \sum_{P_{\gamma,\pi} \in P} W_{\gamma,\pi};$$

   c) *sonstige Ausfalldauer* S_P:
   $$S_P = \sum_{P_{\gamma,\pi} \in P} S_{\gamma,\pi};$$

   d) *Ausfalldauer* A_P:
   $$A_P = \sum_{P_{\gamma,\pi} \in P} A_{\gamma,\pi} = \sum_{P_{\gamma,\pi} \in P} (W_{\gamma,\pi} + S_{\gamma,\pi}) = W_P + S_P;$$

   e) *ungestörte Betriebsdauer* U_P:
   $$U_P = T_P - A_P;$$

   f) *prozentuale physikalische Verfügbarkeit* V_P:
   $$V_P = \frac{U_P}{T_P} \cdot 100\,[\%] = (1 - \underbrace{\frac{W_P}{T_P}}_{(*)} - \underbrace{\frac{S_P}{T_P}}_{(**)}) \cdot 100\,[\%],$$
   dabei ist (*) der Anteil der willkürlichen Ausfälle und (**) der Anteil der sonstigen Ausfälle.

3. ***Port-Statistik*** *(Geräte-Statistik analog)* ***mit Berücksichtigung der Gewichtungen:***

   a) *gewichtete theoretisch mögliche Betriebsdauer* $T_{P_{gewichtet}}$:
   $$T_{P_{gewichtet}} = \sum_{P_{\gamma,\pi} \in P} T_{\gamma,\pi} \cdot \Gamma(P_{\gamma,\pi});$$

   b) *gewichtete willkürliche (geplante) Ausfalldauer* $W_{P_{gewichtet}}$:
   $$W_{P_{gewichtet}} = \sum_{P_{\gamma,\pi} \in P} W_{\gamma,\pi} \cdot \Gamma(P_{\gamma,\pi});$$

   c) *gewichtete sonstige Ausfalldauer* $S_{P_{gewichtet}}$:
   $$S_{P_{gewichtet}} = \sum_{P_{\gamma,\pi} \in P} S_{\gamma,\pi} \cdot \Gamma(P_{\gamma,\pi});$$

   d) *gewichtete Ausfalldauer* $A_{P_{gewichtet}}$:
   $$A_{P_{gewichtet}} = W_{P_{gewichtet}} + S_{P_{gewichtet}};$$

e) *gewichtete ungestörte Betriebsdauer* $U_{P_{gewichtet}}$:

$$U_{P_{gewichtet}} = T_{P_{gewichtet}} - A_{P_{gewichtet}};$$

f) *gewichtete prozentuale physikalische Verfügbarkeit* $V_{P_{gewichtet}}$:

$$V_{P_{gewichtet}} = \frac{U_{P_{gewichtet}}}{T_{P_{gewichtet}}} \cdot 100\,[\%] = (1 - \underbrace{\frac{W_{P_{gewichtet}}}{T_{P_{gewichtet}}}}_{(*)} - \underbrace{\frac{S_{P_{gewichtet}}}{T_{P_{gewichtet}}}}_{(**)}) \cdot 100\,[\%],$$

dabei ist (*) der Anteil der gewichteten willkürlichen Ausfälle und (**) der Anteil der gewichteten sonstigen Ausfälle.

Bemerkung: *Die **gewichtete** prozentuale physikalische Verfügbarkeit läßt sich aus der **ungewichteten** der einzelnen Geräte* (V_γ) *bzw. Ports* ($V_{\gamma,\pi}$) *immer dann, wenn die theoretisch mögliche Betriebszeit* T *für alle Geräte aus* G *bzw. alle Ports aus* P *gleich ist, wie folgt **vereinfacht** **(V')** berechnen:*

$$V'_{P_{gewichtet}} = \frac{\Sigma_{P_{\gamma,\pi} \in P} V_{\gamma,\pi} \cdot \Gamma(P_{\gamma,\pi})}{\Sigma_{P_{\gamma,\pi} \in P} \Gamma(P_{\gamma,\pi})} \cdot 100\,[\%].$$

5.6.1.3 Beispiel zur Berechnung der physikalischen Verfügbarkeit

Zu berechnen sei die physikalische Verfügbarkeit dreier Ports mit den Namen $\{P_{8,1}, P_{8,4}, P_{8,5}\}$ =: P eines Brouters mit dem Namen G_8 während des Intervalls Δt mit den in Abbildung 5.16 gegebenen Daten:

π	$T_{8,\pi}$	$A_{8,\pi}$	$U_{8,\pi}$	$V_{8,\pi}$	$\Gamma(P_{8,\pi})$	$T_{8,\pi_{gewichtet}}$	$A_{8,\pi_{gewichtet}}$	$U_{8,\pi_{gewichtet}}$	$V_{8,\pi_{gewichtet}}$
1	21	1	20	95,24%	1	21	1	20	95,24%
4	24	3	21	87,50%	6	144	18	126	87,50%
5	15	1	14	93,33%	1	15	1	14	93,33%
	T_P	A_P	U_P	V_P		$T_{P_{gewichtet}}$	$A_{P_{gewichtet}}$	$U_{P_{gewichtet}}$	$V_{P_{gewichtet}}$
	60	5	55	91,67%		180	20	160	88,89%

Abbildung 5.16: Beispiel für die Berechnung der physikalischen Verfügbarkeit

Auswertung

- *Ungewichtete prozentuale Verfügbarkeit* V_P der drei Ports während des Intervalls Δt: $V_P \approx 91{,}67\%$.
- *Gewichtete prozentuale Verfügbarkeit* $V_{P_{gewichtet}}$ der drei Ports während des Intervalls Δt unter Berücksichtigung der sechsfachen Gewichtung $\Gamma(P_{8,4})$ des Ports $P_{8,4}$: $V_{P_{gewichtet}} \approx 88{,}89\%$.

Bemerkung: *Die **ungewichtete** physikalische Verfügbarkeit V_P kann aufgrund ihrer Definition*
- *größer (wie in Abbildung 5.16 errechnet) bzw.*
- *gleich oder kleiner (wie in Abbildung 5.17 dargestellt)*

*als die **gewichtete** physikalische Verfügbarkeit $V_{P_{gewichtet}}$ sein.*

1. Ersetzt man in Abbildung 5.16 — ceteris paribus — z.B. die Ausfallzeit $A_{8,1}$ des Ports $P_{8,1}$ durch $A_{8,1} = 3{,}5$, so ergibt sich: $V_P = V_{P_{gewichtet}} = 87{,}5\%$.

2. Ersetzt man in Abbildung 5.16 — ceteris paribus — z.B. die Ausfallzeit $A_{8,1}$ des Ports $P_{8,1}$ durch $A_{8,1} = 7$, so ergibt sich: $V_P \approx 81{,}67\% < V_{P_{gewichtet}} \approx 85{,}56\%$.

Abbildung 5.17 zeigt die prozentualen physikalischen Ausfälle aller im Konfigurationsmodul spezifizierten Ports ohne und mit Berücksichtigung der Gewichtung (Bewertung):

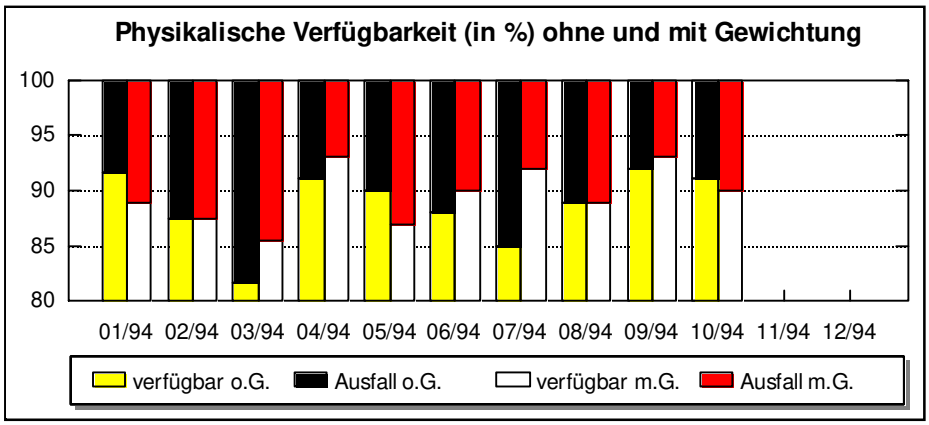

Abbildung 5.17: Physikalische Verfügbarkeit ohne und mit Gewichtung

5.6.1.4 Beispiel-Auswertungen für das „Management“

Dieser und der nächste Abschnitt präsentieren Beispiele für Diagramme, die mit den in der Archivtabelle vorhandenen Verfügbarkeitsdaten nach den Anforderungen der Zielgruppen (Empfänger) „Management“ und „Technik“ erstellt werden können.

Abbildung 5.18 zeigt die prozentuale physikalische Verfügbarkeit, die Anzahl der Ausfallstunden und die geplanten Ausfälle eines Netzes:

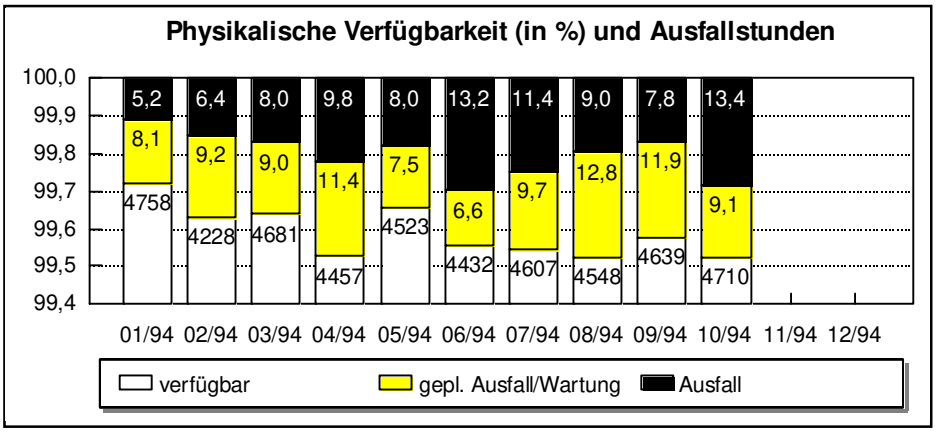

Abbildung 5.18: Physikalische Verfügbarkeit und Ausfallstunden

Abbildung 5.19 präsentiert ebenfalls die prozentualen physikalischen und den Anteil der geplanten Ausfälle, unterscheidet jedoch, ob die Ausfallursache ein Problem des Local-Bereiches (= L) oder des Remote-Bereiches (= R) war:

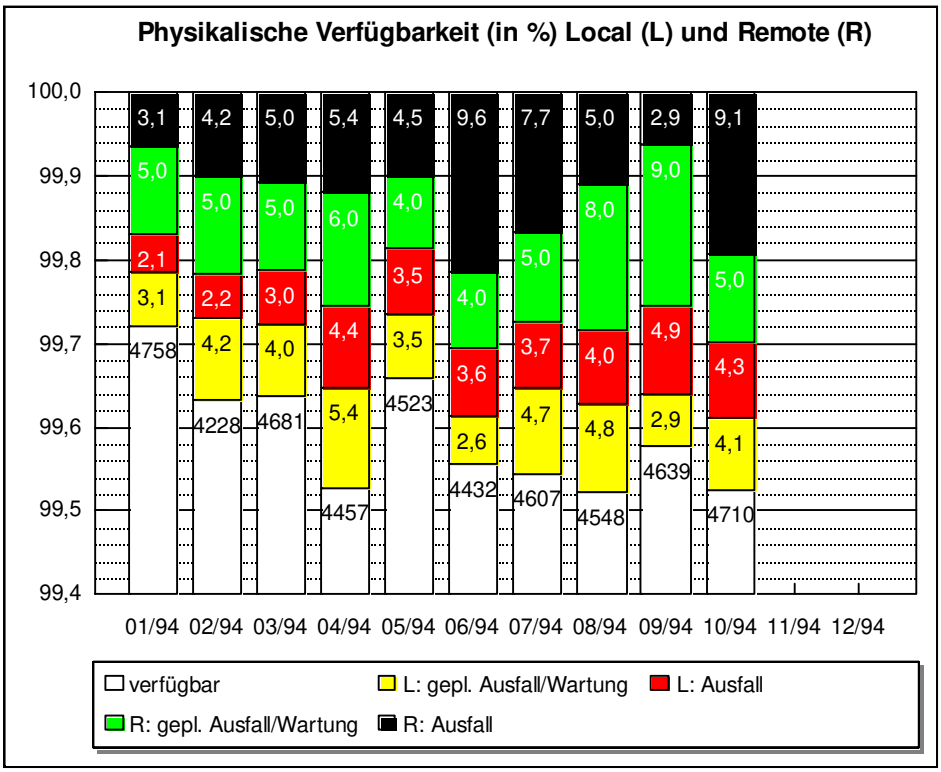

Abbildung 5.19: Physikalische Verfügbarkeit des Local- und Remote-Bereiches

5.6.1.5 Beispiel-Auswertungen für die „Technik“

Die Zielgruppe „Technik“ erhält regelmäßig (z.B. monatlich) für Local- und Remote-Bereich je eine Graphik, aus der die räumliche Verteilung der wichtigsten Ausfälle hervorgeht (vergleiche die Abbildungen 5.20 und 5.21):

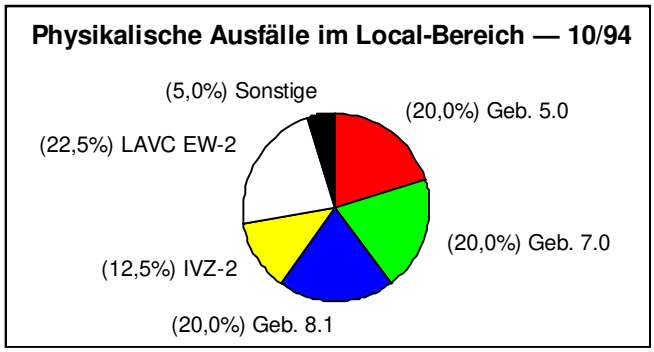

Abbildung 5.20: Örtliche Verteilung der physikalischen Ausfälle im Local-Bereich

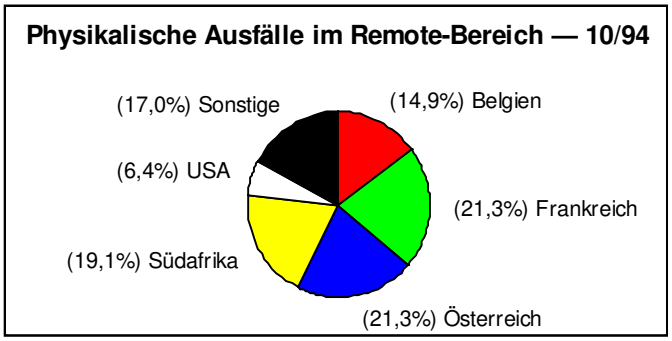

Abbildung 5.21: Örtliche Verteilung der physikalischen Ausfälle im Remote-Bereich

Außerdem erhält die Technik regelmäßig (z.B. monatlich) für Local- und Remote-Bereich je eine Graphik, aus der diejenigen Ausfallursachen hervorgehen, deren prozentualer Anteil am größten ist (vergleiche Abbildung 5.22):

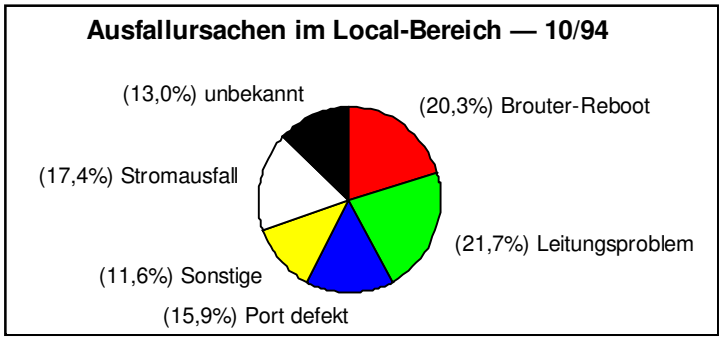

Abbildung 5.22: Ausfallursachen im Local-Bereich

Bemerkung: *Abbildung 5.22 ist ein typisches Beispiel für eine Auswertung, deren Nutzen maßgeblich von der Qualität der interaktiven Daten(nach)bearbeitung abhängt, was sich sofort am Anteil der Ausfälle mit „unbekannter" Ursache widerspiegelt: es handelt sich dabei in den meisten Fällen um Ausfälle, deren Ursache nur deshalb nicht eingetragen werden konnte, weil der gerade für die Nachbearbeitung zuständige Mitarbeiter es versäumte (oder nicht die Zeit hatte), ihr nachzugehen.*

Interessant für die Technik sind auch Auswertungen über Ausfälle spezieller Ports. Abbildung 5.23 zeigt beispielsweise die Verfügbarkeit, die Anzahl der Ausfälle und die geplanten Ausfälle der FDDI-Ports.

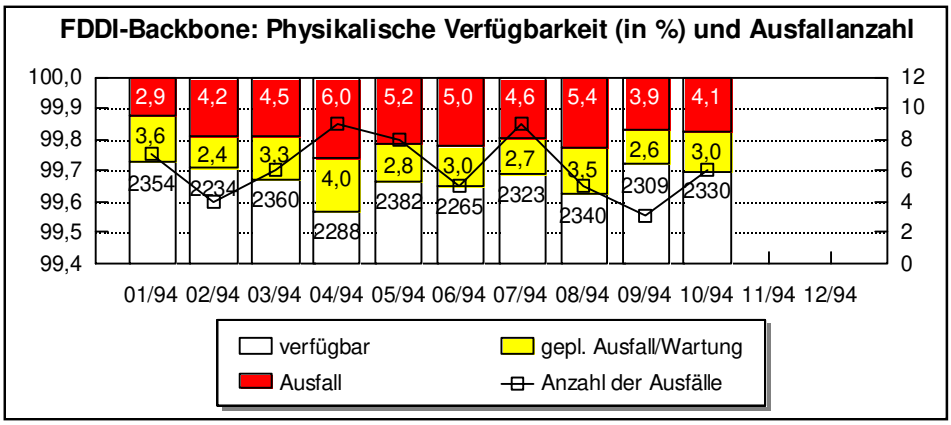

Abbildung 5.23: FDDI-Backbone: Verfügbarkeit und Anzahl der Ausfälle

Abbildung 5.24 stellt die Anzahl und die durchschnittliche Dauer aller aufgetretenen Ausfälle dar (aus der Sicht eines Netzbenutzers ist im allgemeinen eine einzige, dafür aber etwas länger dauernde Störung weniger gravierend, als viele während der gesamten Arbeitszeit auftretende kurze Ausfälle):

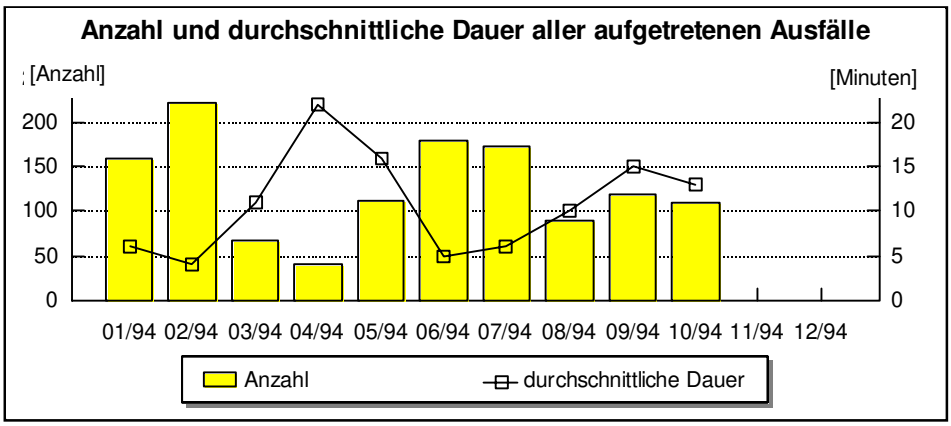

Abbildung 5.24: Anzahl und durchschnittliche Dauer aller aufgetretenen Ausfälle

Abbildung 5.25 veranschaulicht den Nutzen eines gleitenden Durchschnitts (SMA, siehe Seite 61f.) zur Analyse von Verfügbarkeitstrends bei Diagrammen mit relativ vielen Datenpunkten und ziemlich großer Volatilität der einzelnen Beobachtungen:

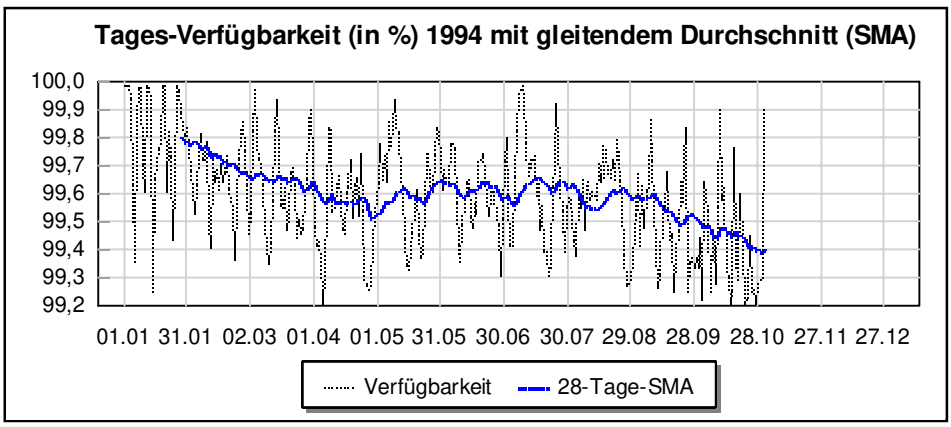

Abbildung 5.25: Tages-Verfügbarkeit mit gleitendem Durchschnitt zur Trendanalyse

Verfügbarkeitstrendanalyse zu Abbildung 5.25:

1. Schon bei oberflächlicher Betrachtung des Diagramms läßt sich anhand des SMA-Verlaufs sofort deutlich ein Abwärtstrend der Verfügbarkeit feststellen (Abbildung 5.26 enthält dazu einige charakteristische Werte).

2. Bei genauerer Analyse kann dieser generelle Abwärtstrend (Primärtrend) in drei Sekundärtrends gegliedert werden:

   i) *Zeitraum bis Ende April 1994:* ständige Verschlechterung der Verfügbarkeit von einem SMA-Wert von rund 99,8% auf ca. 99,5%;

   ii) *Zeitraum von Mitte Mai bis Mitte September 1994:* nach einer Verbesserung des SMA-Wertes um etwa 0,1 Prozentpunkte Anfang Mai wird das erreichte Verfügbarkeitsniveau bei einem SMA-Wert von rund 99,6% gehalten;

   iii) *Zeitraum von Mitte September bis Ende Oktober 1994:* der Seitwärtstrend ii) geht in einen erneuten Abwärtstrend über, wobei der Verfügbarkeits-SMA-Wert bis auf etwa 99,4% absinkt.

Anzahl Datenpunkte (Beobachtungen, bis 31.10.):	304
Maximum der Verfügbarkeit:	99,99%
Minimum der Verfügbarkeit:	99,21%
Mittelwert der Verfügbarkeit:	99,60%
Standardabweichung der Verfügbarkeit:	0,19%
erster 28-Tage-SMA-Wert:	99,80%
letzter 28-Tage-SMA-Wert:	99,41%

Abbildung 5.26: Einige charakteristische Werte zu Abbildung 5.25

5.6.2 Dokumentation der logischen Verfügbarkeit

Wie bereits im vorigen Abschnitt, erfolgt auch hier die

1. Definition der zu erstellenden Auswertungen der logischen Verfügbarkeit und
2. Präsentation einiger Beispiel-Diagramme.

5.6.2.1 Definition der zu erstellenden Auswertungen

Für die weitere Analyse und Statistik sind die Werte bestimmter Attribute aus der MIB der Cisco-Brouters (vergleiche [CISCO 1]) auszuwerten; dazu gehören:

1. Allgemeine Brouter-Statistiken

Für jeden Port der im FDDI-Backbone eingesetzten Brouters sollte eine Auswertung erstellt werden, die folgende Datenreihen enthält:

- CPU-Auslastung.

  Beispiel: Die Cisco-Brouter-MIB-Ganzzahl-Variablen `avgBusy1` und `avgBusy5` liefern einen über 1 bzw. 5 Minuten berechneten exponentiell gewichteten gleitenden Durchschnitt der CPU-Auslastung.

- Puffer-Auslastung.

  Beispiel: Die Cisco-Brouter-MIB-Ganzzahl-Variable `bufferElFree` liefert die Anzahl der gerade freien Puffer.

- Protokollverteilung auf die empfangenen und gesendeten Daten (z.B. für IP und DECNET-Protokoll).

  Beispiel: Die Cisco-Brouter-MIB-Zähler-Variablen `locIfipInOctets` und `locIfipOutOctets` bzw. `locIfdecnetInOctets` und `locIfdecnetOutOctets` enthalten die Anzahl der unter Verwendung des IP bzw. DECNET-Protokolls empfangenen und gesendeten Bytes.

2. Auswertungen für den FDDI-Backbone

Die Gesamtauslastung des FDDI-Backbones läßt sich als Summe der Auslastungen der FDDI-Ports der Cisco-Brouters berechnen.

3. Auswertungen für den Local-Bereich (für jeden nicht-seriellen Local-Port)

Verkehr über die einzelnen Ports der Brouters:

- *Auslastung eines nicht-seriellen Ports (Load, Non-Serial Interface)* LNSI:

$$\text{LNSI} := \frac{\frac{\Delta\text{Gesamtzahl der Bytes des Ports} \cdot 8}{\Delta\text{Sekunden}}}{\text{Bandbreite des Ports}} \cdot 100\ [\%].$$

  Bemerkung: *Man beachte, daß von der Auslastung eines Ports nicht auf die Auslastung des durch diesen Port versorgten Netzes geschlossen werden darf.*

- Statistiken (z.B. von Ethernet, Token Ring, FDDI) wie unter Punkt 4 Buchstaben b bis e beschrieben.

4. Auswertungen für den Remote-Bereich (für jeden seriellen Remote-Port):

a) *Auslastung eines seriellen Ports (Load, Serial Interface)* LSI:

$$\text{LSI} := \frac{\frac{\Delta\text{Maximum der gesendeten oder empfangenen Bytes des Ports} \cdot 8}{\Delta\text{Sekunden}}}{\text{Bandbreite des Ports}} \cdot 100\,[\%].$$

b) *Kollisionsrate (Collision Rate)* CR:

$$\text{CR} := \frac{\Delta\text{Gesamtzahl der von dem Port festgestellten Kollisionen}}{\Delta\text{Sekunden}} \cdot 100\,[\%].$$

Beispiel: Die Cisco-Brouter-MIB-Ganzzahl-Variable `locIfCollisions` liefert die Anzahl der von einem Port festgestellten Kollisionen.

c) *Paketrate (Packet Rate)* PR:

$$\text{PR} := \frac{\Delta\text{Gesamtzahl der Pakete des Ports}}{\Delta\text{Sekunden}}.$$

d) *Fehlerrate (Error Rate)* ER:

$$\text{ER} := \frac{\Delta\text{Gesamtzahl der fehlerhaften Pakete des Ports}}{\Delta\text{Gesamtzahl der Pakete des Ports}} \cdot 100\,[\%].$$

e) *Prozentsatz weggeworfener Pakete (Discard Rate)* DR:

$$\text{DR} := \frac{\Delta\text{Gesamtzahl der weggeworfenen Pakete des Ports}}{\Delta\text{Gesamtzahl der Pakete des Ports}} \cdot 100\,[\%].$$

5.6.2.2 Beispiele für Auswertungen

Dieser Abschnitt stellt Beispiele für Diagramme der logischen Verfügbarkeit vor, für deren Erstellung zum Teil zusätzliche Daten erforderlich sind, welche über die in diesem Kapitel beschriebenen Archivtabellen vorhandenen Verfügbarkeitsinformationen hinausgehen:

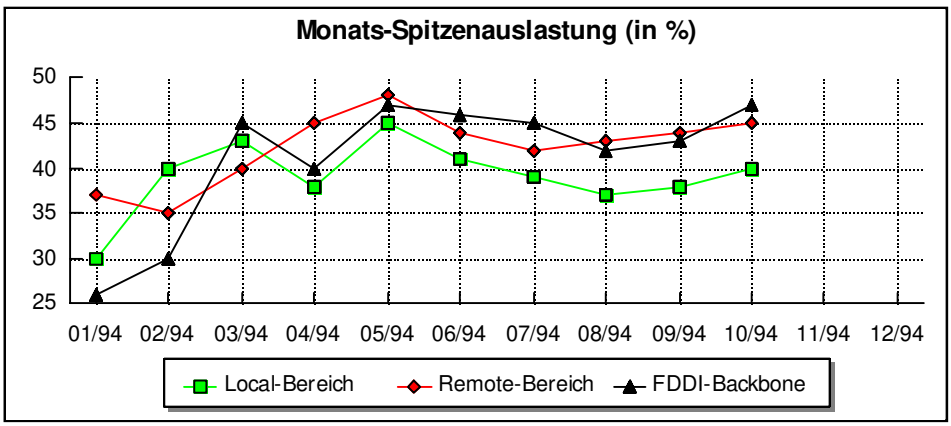

Abbildung 5.27: Monats-Spitzenauslastung

1. Manuelle Datenerfassung

   Gewisse die logische Verfügbarkeit betreffenden Daten (z.B. spezielle Protokollprobleme) müssen manuell erfaßt werden.

2. Automatische Datenerfassung (Gerätestatistiken)

   Auswertungen, welche z.B. die Auslastung betreffen, können analog den Diagrammen der physikalischen Verfügbarkeit formatiert werden (Beispiele zeigen die Abbildungen 5.27 und 5.28).

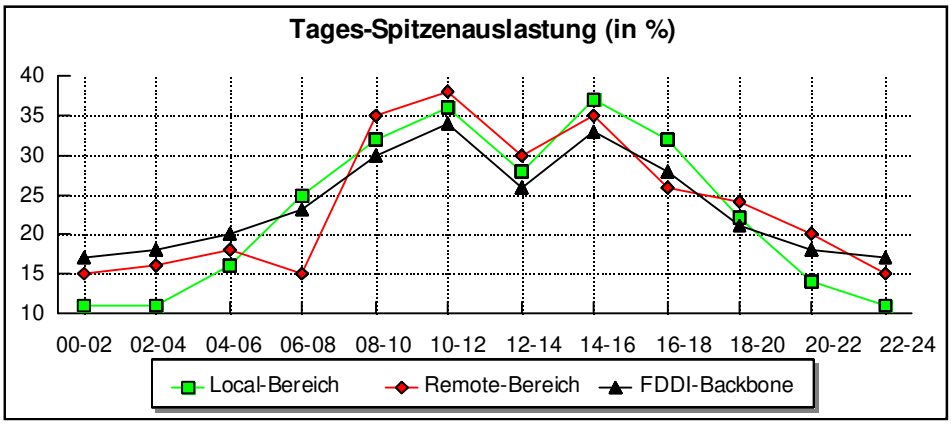

Abbildung 5.28: Tages-Spitzenauslastung

6 Nutzung des Konzeptes im integrierten Netzmanagement

In den Kapiteln 4 und 5 wurde eine Lösung zur Erstellung einer Verfügbarkeitsdokumentation vorgestellt, die als Leitfaden für die Realisierung und Implementierung bei BMW dient und auf einem (Oracle-)Datenbanksystem als Datensenke basiert.

Dieses Kapitel stellt in den Unterabschnitten

1. „Einsatz eines Performancemanagement-Systems“ auf Seite 103f. und
2. „Einsatz eines Trouble-Ticket-Systems“ auf Seite 105f.

zwei dazu alternative Werkzeuge aus dem Bereich des integrierten Netzmanagements vor, die beide für sich in Anspruch nehmen, daß mit ihnen die Verfügbarkeit untersucht und dokumentiert werden kann.

Beide können als passive Werkzeuge nur als Erweiterung bzw. Unterstützung der zu den aktiven Werkzeugen gehörenden herkömmlichen kommerziellen Netzmanagementsysteme (wie beispielsweise SPECTRUM von Cabletron oder auch NetView/6000 von IBM) im Bereich des integrierten Netzmanagements und nicht als eigenständige Netzmanagementwerkzeuge angesehen werden, weil

- sie direkt von den von ihnen als externe Datenquellen genutzten Netzmanagementsystemen abhängig sind und
- mit ihnen häufig kein direktes „Management“ im Sinne eines aktiven Eingreifens in das Netzgeschehen, sondern allenfalls ein — teilweise zeitverzögerter — Überblick über den Netzzustand möglich ist.

Zur Verifikation ihrer Eignung soll in den beiden Abschnitten jeweils nach einer allgemeinen Einführung in diese Werkzeuge anhand der in den vorangegangenen Kapiteln erarbeiteten Anforderungen an eine Verfügbarkeitsdokumentation überprüft und erörtert werden,

- *inwieweit* diese Alternativen dem Konzept zur Erstellung einer Verfügbarkeitsdokumentation entsprechen und
- *ob*, und wenn ja, *wie* das dargelegte Konzept effektiv eingesetzt werden kann, wenn sich eine Netzbetreiberorganisation für den Einsatz dieser Alternativen zur Erstellung einer Verfügbarkeitsdokumentation entscheidet.

6.1 Einsatz eines Performancemanagement-Systems

In diesem Abschnitt wird ein Performancemanagement-System am Beispiel der SAS/CPE[1]-Software ([SAS/CPE]), die vom SAS Institute Inc. in Cary, North Carolina, USA, entwickelt und über Niederlassungen weltweit vertrieben wird, vorgestellt (siehe Abbildung 6.1).

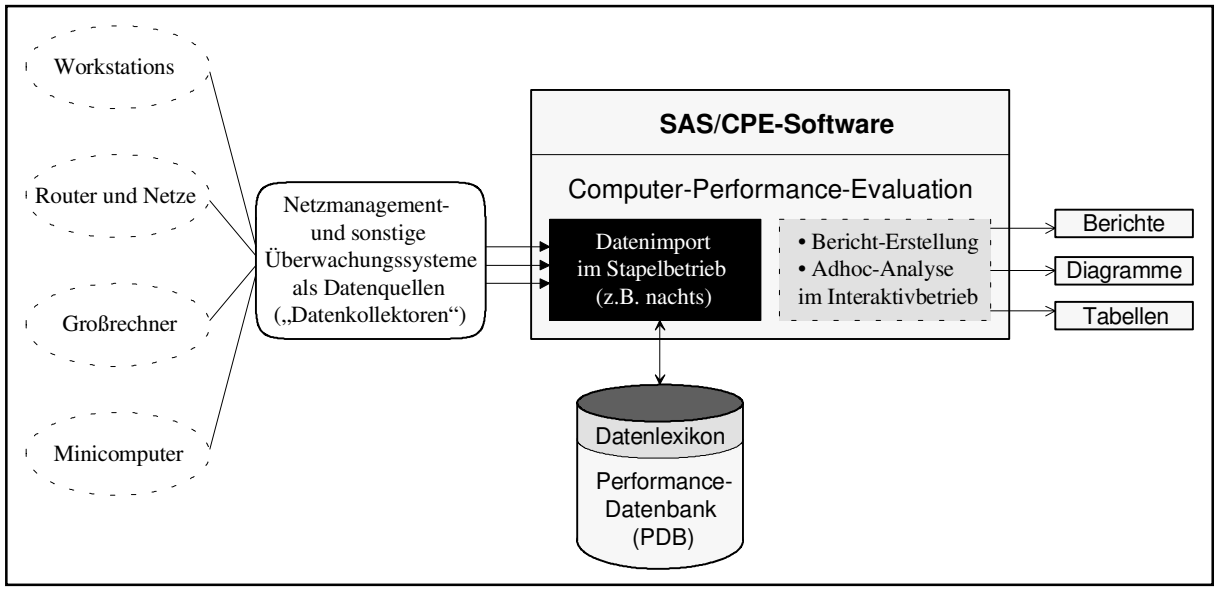

Abbildung 6.1: Überblick über das SAS/CPE-System

Anschließend erfolgt eine Bewertung im Hinblick auf die Verwendbarkeit bezüglich des Konzeptes zur Erstellung einer Verfügbarkeitsdokumentation.

6.1.1 Einführung

Die SAS/CPE-Software für Offene Systeme soll Netz- und Systembetreibern die Erfüllung ihrer Aufgaben

- Performancemanagement und
- Kapazitätsplanung

erleichtern.

Das Performancemanagement-Werkzeug soll dabei die individuellen Bedürfnisse der folgenden vier Zielgruppen befriedigen:

1. **Leiter eines Datenzentrums**

   benötigen regelmäßig Zusammenfassungen und Analysen der Netzaktivität zur Kontrolle der Benutzerproduktivität und des Zustands des bestehenden Netzes.

[1] Von SAS verwendete Abkürzung für „Computer Performance Evaluation“.

2. **Performanceanalytiker**

   sollen eine strategische Ressourcen-Verwaltung erarbeiten, indem sie feststellen, wie sich geplante Änderungen (z.B. mehr Teilnehmer am Netz) auf das Rechnernetz auswirken.

3. **Netzadministratoren**

   sollen „taktisches“ Netzmanagement durchführen, indem sie Probleme identifizieren, untersuchen und lösen.

4. **Kapazitätsplaner**

   sollen die Leistungsfähigkeit des Personals und der Hardware errechnen, wobei sie Vorhersagen bezüglich der Auslastung und Kapazitätsbeschränkungen der eingesetzten Systeme verwenden, um die organisatorischen Kostenziele zu erreichen.

Dazu bietet das SAS/CPE-System technische Verfahren zur effektiven und effizienten Analysierbarkeit großer Datenmengen, mit denen sich eine bessere Ressourcenausnutzung im Bereich der Rechnersysteme und Netze erzielen lassen:

1. **Datenimport in das SAS/CPE-System**

   Wie in Abbildung 6.1 dargestellt, kann die Datenübernahme aus den von SAS als „Datenkollektoren“ (data collectors) bezeichneten Datenquellen ausschließlich im Stapelbetrieb — aufgrund der hohen damit verbundenen Rechnerauslastung[1] vorzugsweise nachts — erfolgen.

   Dabei greift das System direkt auf die von den Datenquellen erzeugten Datendateien zu und setzt diese in das SAS-Datensatzformat um, wobei teilweise (wie z.B. bei SPECTRUM[2] oder der Performance Collection Software PCS von Hewlett-Packard) eine zusätzliche Datenkonvertierungssoftware erforderlich ist, die beim Hersteller des betreffenden Werkzeugs erhältlich ist.

   Beispiel: Bei der Datenquelle SPECTRUM handelt es sich um die Statistikdateien (`*.SLA`) und Eventdateien (`*.ELA`), die von einer speziellen von Cabletron gelieferten SAS-Gateway-Software im Stapelbetrieb in das SAS-Datensatzformat umgesetzt werden.

2. **Datenverwaltung innerhalb des SAS/CPE-Systems**

   Die interne Datenverwaltung geschieht mittels der sogenannten *Performance-Datenbank (Performance Data Base, PDB)*, welche die von allen in einer Netzbetreiberorganisation eingesetzten Netzmanagement- und sonstigen Performanceauswertungssystemen importierten Daten zentral sammelt und verwaltet. Die PDB besteht aus einer Gruppe von SAS-Datenbibliotheken, die bei der Datenverarbeitung als eine Einheit gesehen werden.

   Diese Bibliotheken wiederum sind aus Tabellen aufgebaut, von denen jede mit Daten einer bestimmten Semantik gefüllt ist. In den Tabellen findet eine benutzerkonfigurierbare, vom Alter der jeweiligen Daten abhängige Datenreduktion statt, welche die Menge der gespeicherten Daten in mehreren Stufen (Tag, Woche, Monat und Jahr) verringert. Jede Tabelle kann Daten jeder dieser Reduktionsstufen enthalten.

   Ein wichtiger Teil der PDB ist das sogenannte *Daten-Lexikon (data dictionary)*, welches den Inhalt und die vorzunehmende Datenreduktion für jede Tabelle beschreibt.

---

[1] Zitat aus [SAS/CPE]: „***Caution: The job to load data into the PDB can be very time consuming.*** To avoid overloading your workstation while this job runs, it is a good idea to (…) run it as a batch job overnight…“.

[2] SPECTRUM wird von SAS als „network monitor“ (!) bezeichnet.

3. **Datenauswertung und Präsentation**
   Das SAS/CPE-System bietet eine umfangreiche Palette von Diagrammen und Tabellen zur Präsentation benutzerdefinierbarer Auswertungen.

6.1.2 Eignung des SAS/CPE-Systems zur Verfügbarkeitsdokumentation

Das System weist eine große Vielfalt von Funktionen auf und ermöglicht daher eine relativ flexible Anpassung an die speziellen Anforderungen und Bedürfnisse eines Netzbetreibers. Der größte Nachteil für die Verfügbarkeitsdokumentation ist jedoch die Datenaktualisierung im Stapelbetrieb, die eine konsequente und zuverlässige Datennachbearbeitung, wie sie das vorliegende Konzept fordert, unmöglich macht.

Für das ausschließliche Erfassen statistischer Daten im Bereich der logischen Verfügbarkeit dagegen erscheint das System durchaus geeignet. Aufgrund der gewaltigen Menge der erfaßten Daten besteht allerdings die Gefahr, daß man die Übersicht verliert und recht schnell dazu verleitet wird, sich nicht — wie es das vorliegende Konzept verlangt — Gedanken darüber zu machen, welche Daten wirklich benötigt und dokumentiert werden sollen.

6.2 Einsatz eines Trouble-Ticket-Systems

In diesem Abschnitt soll nach einer allgemeinen Einführung in Trouble-Ticket-Systeme gezeigt werden, daß das erarbeitete Konzept zur Erstellung einer Verfügbarkeitsdokumentation auch für den Einsatz eines Trouble-Ticket-Systems im Bereich des integrierten Netzmanagements von Nutzen ist.

6.2.1 Einführung in Trouble-Ticket-Systeme

Trouble-Ticket-Systeme werden im Bereich des Problemmanagements zur Unterstützung der Verfahren Fehlerverfolgung, -behebung und -dokumentation eingesetzt ([VALTA], [HEGER]). Ihre Grundfunktionalität ist dabei das systematische Speichern und Verwalten aller auftretenden Fehler sowie der Maßnahmen, die zu ihrer Behebung geführt haben, als sogenannte *Trouble Tickets* in einer Datenbasis.

Wie Abbildung 6.2 zeigt, greifen die verschiedensten Funktionsbausteine (Bausteine mit Basisfunktionalität und Bausteine mit erweiterter Funktionalität) auf die Datenbasis zu. Diese kann mit einer Wissensdatenbasis innerhalb eines Expertensystems gekoppelt werden, wodurch man eine automatisierte Korrelation von Trouble Tickets auf Fehlerursachen zu erreichen versucht. Jeder Baustein besteht selbst wieder aus einem Funktionsteil und einem Konfigurationsteil, über den die Funktionalität den Bedürfnissen der Nutzer angepaßt werden kann.

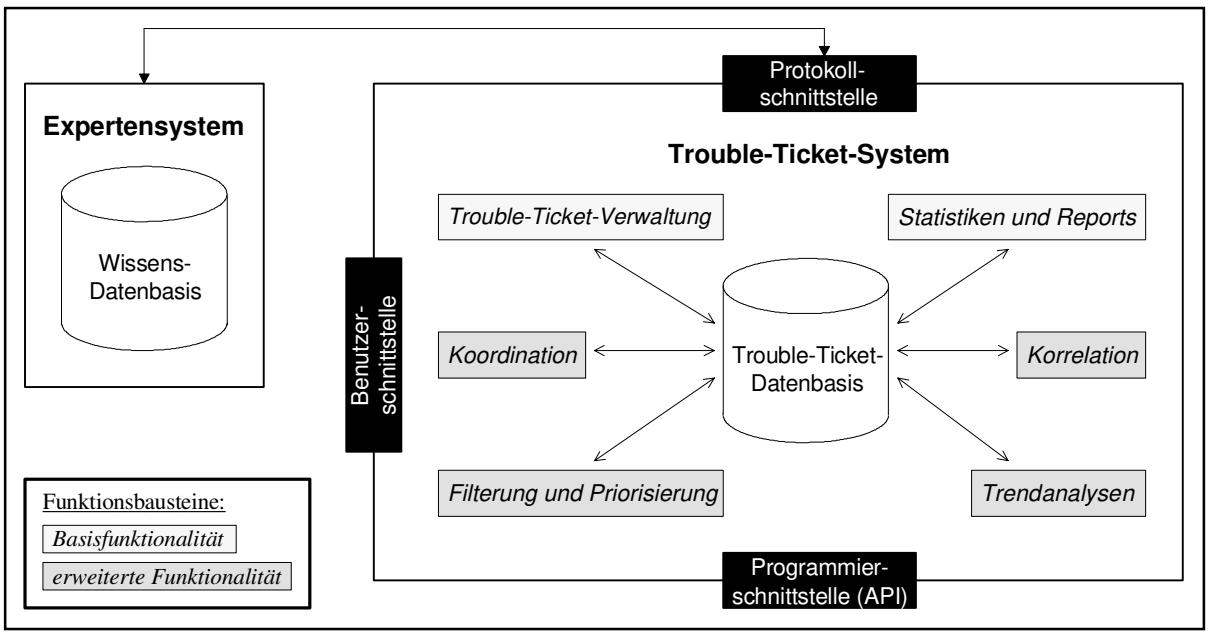

Abbildung 6.2: Aufbau eines Trouble-Ticket-Systems

- **Basisfunktionalität eines Trouble-Ticket-Systems (siehe Abbildung 6.2)**
  - Baustein *Trouble-Ticket-Verwaltung*: ermöglicht das Eintragen, Verändern und Bearbeiten von Trouble Tickets über Zugriffsrechte;
  - Baustein *Statistiken und Reports*: bereitet die in der Trouble-Ticket-Datenbasis liegenden Informationen statistisch auf.
- **Erweiterte Funktionalität eines Trouble-Ticket-Systems (siehe Abbildung 6.2)**
  - Baustein *Koordination*: unterstützt die Kooperation und Kommunikation der Nutzer des Trouble-Ticket-Systems;
  - Baustein *Korrelation*: erleichtert das Auffinden und Gruppieren ähnlicher Trouble Tickets;
  - Baustein *Filterung und Priorisierung*: ermöglicht es, Trouble Tickets nach benutzerkonfigurierbaren Kriterien zu filtern und nach Prioritäten zu bearbeiten;
  - Baustein *Trendanalysen*: erweitert die Funktionalität des Report-Bausteins, indem er gezielt Tendenzen und Entwicklungen aufzeigt.
- **Schnittstellen eines Trouble-Ticket-Systems (siehe Abbildung 6.2)**
  - *Benutzerschnittstelle:* ermöglicht den interaktiven Zugang zur Funktionalität des Trouble-Ticket-Systems;
  - *Protokollschnittstelle:* erlaubt die Kopplung von Fremdsystemen mit dem Trouble-Ticket-System;
  - *Programmierschnittstelle (API):* zur Entwicklung und Anbindung von Funktionsbausteinen.

Standardisierungsarbeiten im Bereich der Trouble-Ticket-Systeme

Aufgrund der zunehmenden Verbreitung von Trouble-Ticket-Systemen wurde sowohl von der CCITT als auch vom IAB[1] die Standardisierung der Zugriffsmöglichkeiten auf die in einem Trouble-Ticket-System verfügbaren Informationen vorangetrieben.

- **Standardisierung der CCITT ([CCITT D565/5])**

  Die CCITT macht Vorschläge zur Standardisierung der Funktionalität und Informationsstruktur eines Trouble-Ticket-Systems, die sich auf das von der ISO entwickelte Managementinformationsmodell stützen; dabei wird die Funktionalität eines Trouble-Ticket-Systems spezifiziert, indem man eine Menge von sogenannten Managed Object Classes (MOCs) (siehe Abbildung 6.3) definiert, auf die der Zugriff mittels des standardisierten Managementprotokolls CMIP[2] erfolgt.

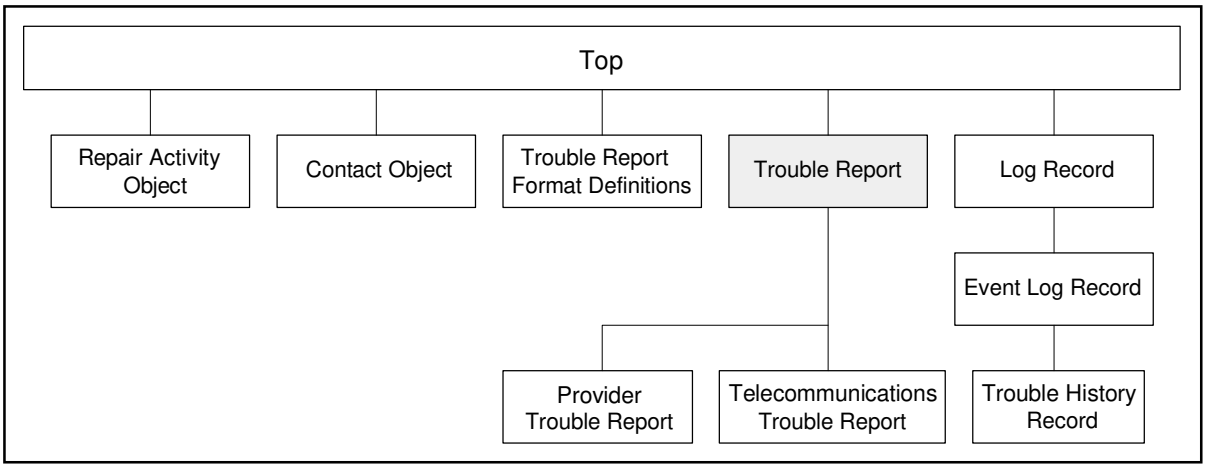

Abbildung 6.3: Vererbungshierarchie zum Trouble Management

  – Arbeiten zur Behebung von Störungsmeldungen lassen sich mit der Objektklasse *Repair Activity* dokumentieren.
  – Die Objektklasse *Contact Object* dient der Speicherung von Daten über Personen (z.B. wer einen Fehler gemeldet hat).
  – Ein Trouble Ticket wird durch ein Objekt der Klasse *Trouble Report* modelliert.
  – Änderungen an einem Trouble Ticket können in einem Objekt der Klasse *Trouble History Record* aufgezeichnet werden.
  – Definition von „Management System Roles“ („Agent Role“ und „Manager Role“), d.h. Festlegung von Aufgaben, die im Agenten und im Manager bei der Realisierung eines Trouble-Ticket-Systems anfallen:
    * Erzeugung von Trouble Reports,
    * Verarbeitung von erzeugten Trouble Reports.

[1] Das Internet Activities Board wurde im Jahr 1983 gegründet.

[2] Common Management Information Protocol (ISO 9596).

- **Standardisierung des IAB ([RFC 1297])**
  - Anforderungen an die Funktionalität eines Trouble-Ticket-Systems aus der Sicht eines Netzbetreibers[1].
  - Datenstruktur und Konfiguration eines Trouble Tickets:
    * obligatorische Felder („fixed fields“),
    * optionale Felder („free-form fields“);
  - Informationsstruktur eines Trouble Tickets;
  - Integration eines Trouble-Ticket-Systems in Fremdsysteme.

6.2.2 Nutzung des Konzeptes bei Trouble-Ticket-Systemen

Abbildung 6.4 zeigt einen Datenflußplan für den Einsatz eines Trouble-Ticket-Systems zur Erstellung einer Verfügbarkeitsdokumentation.

Bemerkung: *Man sollte sich keinesfalls von der im Vergleich zu dem in Kapitel 5 (Abbildung 5.1 auf Seite 66) vorgestellten Datenflußplan weniger komplexen Struktur täuschen lassen und daraus schließen, daß eine Lösung unter Einsatz eines Trouble-Ticket-Systems leichter zu realisieren und daher anzustreben ist.*

Zur Realisierung des Konzeptes sind folgende Anforderungen an ein potentiell einzusetzendes kommerzielles Trouble-Ticket-System zu richten:

1. **Anforderungen an die Trouble-Ticket-Datenbasis**
   - Die Trouble-Ticket-Datenbasis wird als zentrale Datensenke für die Verfügbarkeitsinformationen eingesetzt und substituiert damit das in den Kapiteln 4 und 5 diesbezüglich vorgesehene (Oracle-)Datenbanksystem.
   - Einführen von zwei Arten von Trouble Tickets:
     * Trouble Tickets für den LAN-Bereich, deren Datenstruktur zumindest die Felder der temporären Eingangstabelle für den LAN-Bereich (siehe Abbildung 5.12 auf Seite 83) enthält;
     * Trouble Tickets für den WAN-Bereich, deren Datenstruktur zumindest die Felder der temporären Eingangstabelle für den WAN-Bereich (siehe Abbildung 5.14 auf Seite 87) enthält.
   - Einrichten einiger zusätzlicher Tabellen nach den Anforderungen des Abschnitts „Zusammenfassung: die nötigen Tabellen“ auf Seite 89f.

2. **Anforderungen an die Protokollschnittstelle**
   - SQL-Schnittstelle zur Anbindung von Datenbanksystemen (z.B. Netzdokumentationssystem).
   - Geeignete Schnittstelle zur Anbindung von Netzmanagementsystemen.

---

[1] Es handelt sich um das Merit Network Operations Center (NOC) in Ann Arbor, einer Stadt mit Universität und Forschungsinstituten im Südosten des Staates Michigan, USA.

– Als Alternative muß die Anbindung über ein Management-Gateway (Proxy-Agent) realisiert werden, das sowohl eine Protokollabbildung als auch eine Abbildung der verwendeten Datenstrukturen zwischen Trouble-Ticket-System auf der einen Seite und Netzmanagementsystemen und/oder Datenbanksystem auf der anderen Seite durchzuführen hat.

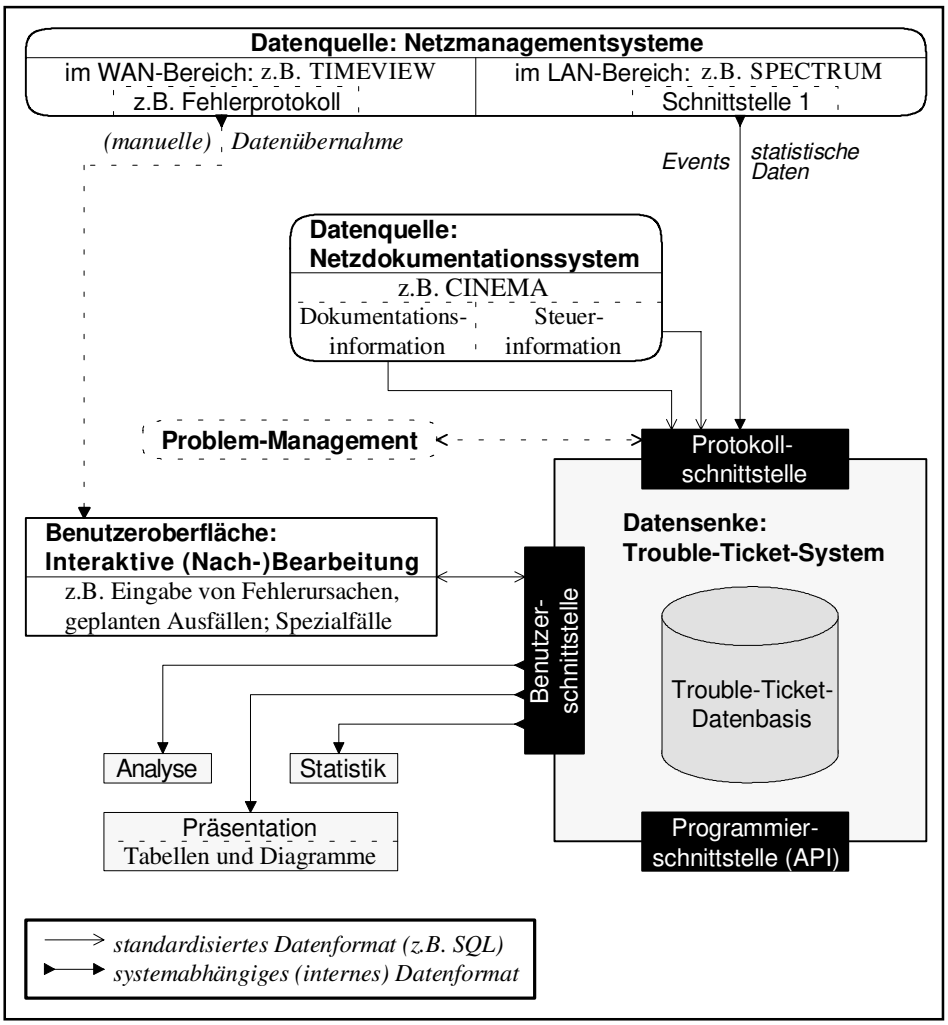

Abbildung 6.4: Verfügbarkeitsdokumentation mit einem Trouble-Ticket-System

3. Anforderungen an die Benutzerschnittstelle

Die Benutzerschnittstelle dient der interaktiven (Nach-)Bearbeitung der in Form von Trouble Tickets vorliegenden Verfügbarkeitsdaten; daher muß ihre Funktionalität den Anforderungen des Abschnitts „Realisierung: die interaktive Daten(nach)bearbeitung“ auf Seite 78f. genügen, um die mit SQL Forms erzeugten Bildschirmmasken sinnvoll ersetzen zu können.

4. Anforderungen an die Programmierschnittstelle (API)

Mit Hilfe der bei den meisten Trouble-Ticket-Systemen zum Standardumfang gehörenden Programmierschnittstelle (API) müssen die Funktionsbausteine (siehe dazu Punkt 5) sowie die übrigen Schnittstellen den Benutzeranforderungen entsprechend konfiguriert und erweitert werden, sofern die vom Hersteller des Trouble-Ticket-Systems mitgeliefer-

te Funktionalität sich als nicht ausreichend erweist, wovon in der Planungsphase in der Regel ausgegangen werden sollte, da dies einen nicht unerheblichen Implementierungsaufwand bedeuten kann.

5. Anforderungen an die Funktionsbausteine

- *Filterung:* die Funktionalität dieses Funktionsbausteins muß den Anforderungen an das Datenvorverarbeitungsmodul entsprechen (siehe dazu den Abschnitt „Realisierung: die Datenvorverarbeitung“ auf Seite 69f.).
- *Priorisierung:* dieser Funktionsbaustein ermöglicht die interaktive Nachbearbeitung von Trouble Tickets nach Prioritätsmerkmalen, wobei sich hier die Gewichtung der Netzkomponenten und die Ausfalldauer anbieten (vergleiche dazu auch den Abschnitt „Die Übersichts-Bildschirmmaske“ auf Seite 81f.).
- *Statistiken und Reports, Trendanalysen:* diese Funktionsbausteine enthalten die technische Grundlage für die über die Benutzerschnittstelle erstellbare Verfügbarkeitsdokumentation; die Funktionalität dieser Bausteine sollte sich nach den im Abschnitt „Realisierung: Statistiken und Diagramme“ auf Seite 89f. genannten Anforderungen richten.

6.2.3 Bewertung, Folgerung

Aufgrund der Ausführungen des vorigen Abschnitts ist festzustellen, daß Trouble-Ticket-Systeme *grundsätzlich* eine sinnvolle Alternative zu der in Kapitel 5 vorgestellten Lösung sein können, weil sich das vorgestellte Konzept (zumindest theoretisch) vollständig umsetzen läßt. Bevor man sich jedoch für den Erwerb eines kommerziellen Trouble-Ticket-Systems entscheidet, sollte man die folgenden Gesichtspunkte genau überprüft haben:

- Bietet das Produkt in der Praxis das nötige hohe Maß an *Flexibilität*, so daß eine Anpassung an die Organisationsstruktur und die Einsatzumgebung (vergleiche die Anforderungen im vorigen Abschnitt 6.2.2) möglich ist (hier genügt es nicht, sich von Hochglanzprospekten überzeugen zu lassen)?
- Weist das Produkt eine ausreichende *Offenheit* auf, so daß es in eine bereits vorhandene Managementumgebung (Netzmanagementsysteme, Netzdokumentationssysteme usw.) integriert werden kann?
- Vorteil dieser Alternative:
  - Einsatz eines kommerziellen Produkts: Unterstützung durch den Hersteller bei der Anpassung an die Umgebung.
- Nachteile dieser Alternative (im Vergleich zum Einsatz eines Datenbanksystems):
  - i) Einarbeitung in ein neues System und dessen Programmierung erforderlich (entfällt beim Einsatz eines (Oracle-)Datenbanksystems, da dieses in vielen Fällen schon vorhanden ist);
  - ii) Mit der Neueinführung des Systems verbundene Kosten: Software, gegebenenfalls zusätzlich nötige Hardware, Personal (entfallen beim Einsatz eines (Oracle-)Datenbanksystems, da dieses meist schon vorhanden ist).

7 Ausblick

In diesem Kapitel soll ein abschließender Blick in die Zukunft der Verfügbarkeitsdokumentation (siehe unten) und deren Beschränkung durch das Bundesdatenschutzgesetz geworfen werden (siehe Seite 112f.).

Der letzte Abschnitt (siehe Seite 114) weist auf einige interessante Folgearbeiten hin.

7.1 Vision „Global-Verfügbarkeitsdokumentation“

Die im Einsatz befindliche Gerätekonfiguration im BMW-Netz erlaubt im LAN-Bereich derzeit nur die Überwachung des FDDI-Backbones mit seinen 14 Cisco-Brouters und deren Local- und Remote-Ports.

Um die Global-Verfügbarkeit (physikalisch und logisch) des Netzes, d.h. die Verfügbarkeit jeder Komponente (vom Backbone über Brouters, Hubs, Bridges usw. bis hin zu den Endgeräten) messen zu können, sind sogenannte „intelligente Geräte“ erforderlich. Man braucht im wesentlichen zwei weitere Ausbaustufen, um an die gewünschten detaillierten Informationen zu gelangen:

1. **Stufe:**

   Ausrüsten eines Hubs pro Segment mit RMON-Agenten (siehe unten) oder Installation spezieller Geräte (sogenannte dedizierte Probes) für die Aufnahme von Statistikdaten.

2. **Stufe:**

   Zusätzliches Ausrüsten jedes Hubs mit Agenten für die Endgeräte-Überwachung, d.h. Einbau einer Karte und Installation einer entsprechenden Software.

Die RMON-MIB ([ERLING], [RFC 1271])

Die Remote Network Monitoring Management Information Base (RMON-MIB), die nach weniger als 18 Monaten Entwicklungszeit am 12.11.1991 als Internet Proposed Standard RFC 1271 veröffentlicht wurde, hat als Erweiterung der SNMP-MIB in der letzten Zeit stärkere Verbreitung gefunden:

1. Es bestand die Anforderung, Protokollanalysatoren, die zur Netzverkehrsüberwachung und in immer stärkerem Maße auch zu teilweise komplexen Analysen der mitprotokollierten Netzdaten eingesetzt werden, *unabhängig von den Geräteherstellern* in das SNMP-Management zu integrieren.

2. RFC 1271 enthält eine genaue Spezifikation des Managements einer Ethernet-Umgebung, für die sich die RMON-Entwickler als ihre erste Netz-Entwicklungsumgebung entschieden haben (eine Erweiterung für die Token-Ring-Architektur wurde von S. Waldbusser am 23.09.1993 als RFC 1513 mit dem Titel „Token Ring Extensions to the Remote Network Monitoring MIB“ veröffentlicht; für FDDI gibt es zwar bisher noch keine derartige Spezifikation, jedoch ist man zuversichtlich, daß die RFC-1271-Struktur auch dafür ausreicht).

Ziele des Remote Network Managements:

- „Offline Operation“: Offline-Betrieb der RMON-Agenten, d.h. Netzdaten dürfen auch dann nicht verlorengehen, wenn die Verbindung des Netzmanagementsystems zu den RMON-Agenten unterbrochen wird;
- „Preemptive Monitoring“: permanente Datensammlung, nicht nur im Fehlerfall;
- „Problem Detection and Reporting“: automatisches Erkennen benutzerkonfigurierbarer Netzzustände, die zu Problemen führen könnten, und gegebenenfalls ihre Speicherung und Weiterleitung an Netzmanagementsysteme;
- „Value Added Data“: da sich die RMON-Agenten direkt auf der überwachten Netzkomponente befinden, können die gelieferten Daten um wichtige Informationen erweitert und damit ihr Nutzen erhöht werden;
- „Multiple Managers“: RMON-Agenten sind auf die Zusammenarbeit mit *mehreren* Netzmanagementsystemen ausgelegt, was besonders für größere Netzbetreiberorganisationen ein entscheidender Vorteil ist.

7.2 Gesetzliche Grenzen der Verfügbarkeitsdaten-Erfassung

Die Realisierung der im vorigen Abschnitt beschriebenen Vision eröffnet die Möglichkeit, auch spezifische Daten über die Arbeit einer Person an ihrem Datenendgerät zu ermitteln und weiterzuverarbeiten (z.B. Benutzungszeiten, Anzahl der übertragenen und empfangenen Bytes, Art der eingesetzten Anwendungen), wobei die Person aufgrund ihrer Zugangskennung exakt identifiziert werden kann.

Aufgrund dieser Identifizierbarkeit der Person gelangt man in den Gültigkeitsbereich des „Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG)“ ([BDSG], BGBl. I S. 201) vom 27.01.1977 (Inkrafttreten am 01.01.1978). Weil die datenschutzrechtlichen Bestimmungen die Informationen, welche einer Verfügbarkeitsdokumentation zugrunde liegen, direkt beeinflussen können und daher schon frühzeitig in die Realisierungsplanung einzubeziehen sind, wird im folgenden kurz das aus sechs Abschnitten bestehende und als Rahmengesetz formulierte BDSG vorgestellt:

1. *Abschnitt: allgemeine Vorschriften (§§ 1–6):*
   - Nach § 1 Abs. 1 ist es Aufgabe des Datenschutzes, „durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung, Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken“;
   - nach § 2 Abs. 1 sind personenbezogene Daten definiert als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.
2. *Abschnitt: Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen (§§ 7–21).*
3. *Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke (§§ 22–30):*
   Nach § 24 ist die Datenübermittlung nur zulässig, wenn sie sich auf
   i) Namen;
   ii) Titel, akademische Grade;
   iii) Geburtsdatum;
   iv) Beruf, Branchen- oder Geschäftsbezeichnung;
   v) Anschrift und
   vi) Rufnummer
   beschränkt.
4. *Abschnitt: Geschäftsmäßige Datenverarbeitung nicht-öffentlicher Stellen für fremde Zwecke (§§ 31–40).*
5. *Abschnitt: Straf- und Bußgeldvorschriften (§§ 41–42).*
   - Straftaten (§ 41): Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe;
   - Ordnungswidrigkeiten (§ 42): Geldbuße bis zu 50.000 DM.
6. *Abschnitt: Übergangs- und Schlußvorschriften (§§ 43–47).*

Das BDSG läßt sich zu den folgenden drei Grundregeln zusammenfassen:

1. *Nach § 3 ist die Verarbeitung personenbezogener Daten* nur zulässig, wenn
   i) das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder
   ii) der Betroffene eingewilligt hat.
2. *Rechte des Betroffenen (allgemein in § 4 geregelt):*
   - Recht auf Auskunft über die gespeicherten Daten (§ 13 bzw. § 26);
   - Recht auf Berichtigung, Sperrung, Löschung der gespeicherten Daten (§ 14 bzw. § 27).
3. *Recht der Datenschutzaufsicht und Kontrolle (§§ 17–21 bzw. §§ 22, 28–30):*
   - Das Einhalten der gesetzlichen Vorschriften wird kontrolliert
     * für nicht-öffentliche Stellen (z.B. BMW) mit mindestens fünf Arbeitnehmern von einem zu bestellenden Beauftragten für den Datenschutz bzw.

    * für den Bereich des Bundes vom Bundesbeauftragten für den Datenschutz;
  - Überprüfen der Datenverarbeitung bezüglich ihrer Erforderlichkeit und Durchschaubarkeit.

7.3 Weitere Arbeiten

Naturgemäß kann diese Arbeit nur einen weiteren Mosaikstein auf dem Gebiet des integrierten Netzmanagements darstellen.

Insoweit ergeben sich auch einige interessante Anschluß-Arbeiten, die auf die vorliegende aufbauen können:

1. Integration der weitgehend automatisch erstellten Verfügbarkeitsdokumentation in das manuell geführte Problemmanagement: Korrelation und Koordination von automatisch und manuell erfaßten Problemdatenbeständen.
2. Zur Auswahl geeigneter Werkzeuge im Bereich des integrierten Netzmanagements, bei der die in der vorliegenden Arbeit gewonnenen Anforderungen an eine Verfügbarkeitsdokumentation berücksichtigt werden sollten:
   - Evaluierung von Trouble-Ticket-Systemen (vergleiche [BERTRAM]);
   - Evaluierung von Netzmanagement-Systemen.

8 Literaturverzeichnis

[BDSG] „Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG)“. BGBl. I S. 201 vom 27.01.1977 (Inkrafttreten am 01.01.1978).

[BERTRAM] Bertram, Dieter: „Analyse bestehender Verfahren des Problemmanagements im Hinblick auf deren Unterstützung durch ein Trouble-Ticket-System“. Diplomarbeit; Technische Universität München — Institut für Informatik, Februar 1995.

[BRAESS] Braess, H.-H.: „Technologie-Management komplexer technischer/industrieller Systeme (unter besonderer Berücksichtigung der Entwicklung)“. Vorlesungsunterlagen; Technische Universität München, Wintersemester 1993/94.

[BUDDEN] Buddendiek, J.; Leßmann, G.: „Systemverfügbarkeit als kritischer Erfolgsfaktor — das Beispiel der Deutschen Terminbörse“. In: HMD — Systemsicherheit, Heft 171/1993, S. 73–84; Forkel-Verlag, Mai 1993.

[CCITT] (Comité Consultatif International de Télégraphique et Téléphonique)

CCITT D565/5 „Trouble Management Function — An overview“. Genf, 26.–30.10.1992.

CCITT X.733 (siehe ISO/IEC 10 164-4).

CCITT X.734 (siehe ISO/IEC 10 164-5).

[CINEMA] „CINEMA“ (diverse Dokumentation). Bayerische Motoren Werke Aktiengesellschaft, 1990/1992/1993.

[CISCO] cisco Systems, Inc.: „cisco Trap MIB“. 18.11.1991.

[CISCO 1] cisco Systems, Inc.: „cisco MIB“. 17.11.1992.

[EGERER] Egerer, R.; Weiß, H.-P.: „Integration der SQL-Datenbank CINEMA in SPECTRUM über ein textuelles Command Line Interface“. Fortgeschrittenenpraktikum; Technische Universität München — Institut für Informatik, September 1993.

[EN] (Europäische Norm der Europäischen Union EU)

EN 29 000 (siehe ISO 9000).

EN 29 001 (siehe ISO 9001).

EN 29 002 (siehe ISO 9002).

EN 29 003 (siehe ISO 9003).

EN 29 004 (siehe ISO 9004).

[ERLING] Erlinger, M. A.: „RMON From Concept to Specification“. In: Hegering, H.-G.; Yemini, Y. (eds.): „Integrated Network Management, III“, S. 73–80; North-Holland, 1993.

[GERING] Gering, M.: „CMIP versus SNMP“. In: Hegering, H.-G.; Yemini, Y. (eds.): „Integrated Network Management, III“, S. 347–359; North-Holland, 1993.

[HALSAL] Halsall, F: „Data Communications, Computer Networks and Open Systems“. Addison-Wesley, 1992.

[HEGER] Hegering, H.-G.; Abeck, S.: „Integriertes Netz- und Systemmanagement“. Addison-Wesley, [1]1993.

[HEINEN] Heinen, E. (Hrsg.): „Industriebetriebslehre“. Gabler, Wiesbaden, [8]1985.

[IAB], [RFC] (Internet Activities Board), (Network Working Group — Request for Comments)

RFC 1155 McCloghrie, K.; Rose, M.: „Structure and Identification of Management Information for TCP/IP-based Internets“ (SMI). 10.05.1990 (ersetzt RFC 1065 vom 01.08.1988).

RFC 1156 McCloghrie, K.; Rose, M.: „Management Information Base for Network Management Information of TCP/IP-based Internets“. 10.05.1990 (ersetzt RFC 1066 vom 01.08.1988).

RFC 1157 Case, J.; Davin, J.; Fedor, M.; Schoffstall, M.: „A Simple Network Management Protocol (SNMP)“. 10.05.1990 (ersetzt RFC 1098 vom 01.04.1989).

RFC 1212 McCloghrie, K.; Rose, M.: „Concise MIB Definitions“. 26.03.1991.

RFC 1213 McCloghrie, K.; Rose, M.: „Management Information Base for Network Management of TCP/IP-based internets: MIB-II“. 26.03.1991 (ersetzt RFC 1158).

RFC 1215 Rose, M.: „A Convention for Defining Traps for use with the SNMP“. 27.03.1991.

RFC 1271 Waldbusser, S.: „Remote Network Monitoring Management Information Base“. 12.11.1991. (Wird ergänzt durch RFC 1513: Waldbusser, S.: „Token Ring Extensions to the Remote Network Monitoring MIB“. 23.09.1993).

RFC 1285 Case, J.: „FDDI Management Information Base“. 24.01.1992.

RFC 1297 Johnson, D.: „NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist ("NOC TT REQUIREMENTS")“. 31.01.1992.

[ISO] (International Organization for Standardization)

DIN ISO 8402 „Qualität; Begriffe“. 1986.

DIN ISO 9000 „Qualitätsmanagement- und Qualitätssicherungsnormen — Leitfaden zur Auswahl und Anwendung“. Dezember 1987 (identisch mit DIN ISO 9000 und EN 29 000; Mai 1990).

DIN ISO 9001 „Qualitätssicherungssysteme — Modell zur Darlegung der Qualitätssicherung in Design/Entwicklung, Produktion, Montage und Kundendienst“. Dezember 1987 (identisch mit DIN ISO 9001 und EN 29 001; Mai 1990).

DIN ISO 9002 „Qualitätssicherungssysteme — Modell zur Darlegung der Qualitätssicherung in Produktion und Montage“. Dezember 1987 (identisch mit DIN ISO 9002 und EN 29 002; Mai 1990).

DIN ISO 9003 „Qualitätssicherungssysteme — Modell zur Darlegung der Qualitätssicherung bei der Endprüfung“. Dezember 1987 (identisch mit DIN ISO 9003 und EN 29 003; Mai 1990).

DIN ISO 9004 „Qualitätsmanagement und Elemente eines Qualitätssicherungssystems — Leitfaden“. Dezember 1987 (identisch mit DIN ISO 9004 und EN 29 004; Mai 1990).

DIN ISO 10 011 „Leitfaden für das Audit von Qualitätssicherungssystemen“. 23.11.1989 (identisch mit DIN ISO 10 011; Juli 1990).
- Teil 1: „Auditdurchführung“;
- Teil 2: „Qualifikationskriterien für Auditoren“;
- Teil 3: „Management von Auditprogrammen“.

ISO 10 164-4 „Information Technology — Open Systems Interconnection — Alarm Reporting Function“. 10.02.1992 (identisch mit CCITT X.733).

ISO 10 164-5 „Information Technology — Open Systems Interconnection — Event Report Management Function“. 10.09.1992 (identisch mit CCITT X.734).

[KPMG] KPMG Unternehmensberatung: „Wie sich Mitarbeiter motivieren lassen“. In: Süddeutsche Zeitung Nr. 187/1994.

[LEWIS] Lewis, L.: „A "Command Line Interface" Approach to the Integration of Third Party Applications with SPECTRUM“. Technical Note ctron-lml-93-02, 20.08.1993.

[LUDST] Ludsteck, W.: „Qualitätssicherung“. In: Süddeutsche Zeitung Nr. 71/1994.

[LUDST 1] Ludsteck, W.: „Umfassendes Qualitätsmanagement“. In: Süddeutsche Zeitung Nr. 76/1994.

[MANS] Mansouri-Samani, M.; Sloman, M.: „Monitoring Distributed Systems“. In: IEEE Network, S. 20–30, November 1993.

[RBK] Abeck, S.; Hegering, H.-G.; Wies, R.: „Rahmenbetriebskonzepte als Voraussetzung für ein betreibergerechtes integriertes Management von Corporate Networks“. In: PIK-Themenheft „Corporate Networks“, Heft 1/1995; K. G. Sauer Verlag.

[ROSE] Rose, M. T.: „The Simple Book: An Introduction to Management of TCP/IP-based Internets“. Prentice Hall, 1991.

[SAS/CPE] „SAS/CPE® Software for Open Systems: Usage and Reference, Version 6, First Edition“. SAS Institute Inc., Cary, NC, USA, [1]Oktober 1993.

[SPEC_C] „SPECTRUM® Command Line Interface (CLI) Software Release Notice 1.00.00 for Sun™ RISC Workstations“. Cabletron Systems Inc., Rochester, NH, USA, Mai 1992.

[SYSTEMS] „Systems 93“. Beilage der Süddeutschen Zeitung Nr. 241/1993, S. 29–40.

[TANEN] Tanenbaum, A. S.: „Computer Networks“. Prentice Hall, [2]1989.

[VALTA] Dreo, G.; Valta, R.: „Einsatz eines integrierten Trouble-Ticket-Systems zur Verbesserung der Fehlerdiagnose“. In: HMD — Systemsicherheit, Heft 171/1993, S. 45–59; Forkel-Verlag, Mai 1993.

[VALTA 1] Apostolescu, V.; Dreo, G.; de Jager, R.; Valta, R.: „Unterstützung der Fehlerdiagnose durch ein Trouble-Ticket-System: Anforderungen, Design und Einsatzerfahrungen“.

[WILDEM] Wildemann, H. *et. al.*: „Richtlinien zur Verleihung "Bayerischer Qualitätspreis" 1994“. Technische Universität München — Lehrstuhl für Betriebswirtschaftslehre mit Schwerpunkt Logistik, 1994.