Einsatz des SNMP in der IT-basierten Fernsehproduktion

Hauptseminar Sommersemester 2005: Audiovisuelle Technik

Thema (21)

Technische Universität Ilmenau

Fakultät für Elektrotechnik und Informationstechnik

Institut für Medientechnik

Prof. Dr.-Ing. H.-P. Schade

Betreuer: Dr. Eckhardt Schön

Eingereicht von:

Michael Federspiel

Strasse des Friedens 11

98693 Ilmenau

Ilmenau, den 8.6.2005

Inhaltsverzeichnis:

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ASN.1	Abstract Syntax Notation One
DVB	Digital Video Broadcasting
FDDI	Fibre Distributed Data Interface
HP	Hewlett-Packard GmbH
IBM	IBM Deutschland GmbH
ISO	International Standards Organization
LAN	Local Area Network
MD5	Message Digest Algorithm 5
MIB	Management Information Base
OID	Object Identifier
OSI	Open Systems Interconnect
PDU	Protocol Data Unit
QNX	unixoides Echtzeitbetriebssystem
RFC	Request for Comments
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

1 Einleitung

Die Sendertechnik für den Hör- und Fernsehfunk wird zunehmend digitalisiert. Die bisherigen Schnittstellen, wie zum Beispiel serielle Fernwirk- und Feldbusschnittstellen, werden zunehmend von netzwerkfähigen Schnittstellen, basierend auf dem „Simpel Network Management Protokoll“ (SNMP), verdrängt.

Das SNMP dient als Mechanismus zur Bereitstellung und zum Transport von Managementinformationen zwischen Komponenten innerhalb eines LAN. Es ermöglicht die Abfrage von Parametern oder die Überwachung von bestimmten Zuständen der Komponenten.

Das SNMP ist nicht neu. Es wurde bereits im Mai 1990 im RFC 1157 veröffentlicht, um netzwerkfähige Geräte und Netzwerkkomponenten zu managen. Nach und nach traten jedoch einige Mängel auf. Abfragen von Managementinformationen, die in Form von Tabellen vorlagen, waren aufwändig. Ebenso waren die standardisierten Sicherheitsmaßnahmen nur sehr rudimentär. 1993 wurde Version 2 in 12 verschiedenen RFCs vorgestellt. Neben der Möglichkeit der Datenverschlüsselung, wurden auch Zeitstempel integriert, die eine Wiederholung einer gültigen Nachricht zu einem späteren Zeitpunkt verhindern sollen. Seit 1997 besteht es in Version 3 (SNMPv3). Bei Version 3 handelt es sich jedoch nicht um einen grundlegend neuen Ansatz, sondern in erster Linie um die Zusammenführung von Version 1 und 2, welche nicht kompatibel sind.

2 Grundlagen

2.1 Aufbau

Man unterscheidet zwischen SNMP-Manager und SNMP-Agent. Der SNMP-Manger, oder auch Managementstation genannt, interagiert mit dem Agent über das SNMP.

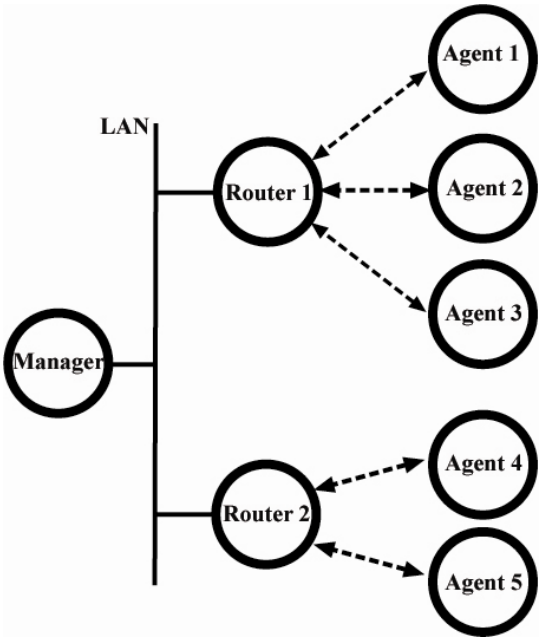

Abbildung 1: Aufbau eines LAN /11/

Die Grundlage zur Kommunikation bietet ein LAN. Somit muss jede Komponente an ein Netzwerk angeschlossen sein. Das SNMP baut in der Anwendungsschicht auf das TCP/IP Modell auf. Damit wird der Einsatz in nahezu allen Netzwerktechnologien der IT möglich. Das Netzmanagement erfolgt an Managementstationen. Es handelt sich dabei um Rechner mit spezieller Managementsoftware. Die Managementstationen setzen Anfragen an den Agent ab und erhalten Antwort. Um die Überwachung zu vereinfachen werden grafische Benutzer-Interfaces benutzt. Agents in einer Netzwerkstruktur können Hosts, Router, Bridges und Switches sein, um nur einige Beispiele zu nennen. Im Bereich der Fernsehproduktion können neben den normalen Netzwerkkomponenten auch DVB-T Sender oder dergleichen überwacht werden. Einzige Vorraussetzung ist, dass der Agent einen SNMP-Managementprozeß ausführt und natürlich an das LAN angeschlossen ist.

Neben den oben genannten angeforderten Statusmeldungen gibt es auch noch „Traps“. Dabei handelt es sich, wie der Name schon andeutet, um Fallen, die zuschnappen sobald ein Ereignis zu trifft. Diese Meldungen sind UDP-Datagramme. Sie werden somit durch das Empfangssystem nicht quittiert (Fire and Forget). Es bleibt zu hoffen, dass die Meldung auch wirklich angekommen ist, da es sich hierbei oft um Störungsmeldungen handelt. Um einen Verlust von wichtigen Meldungen auszuschließen, wird häufig das „Polling“ angewendet. Beim „Polling“ werden Agents gezielt in Zyklen abgefragt.

2.2 Management Information Base

Die Voraussetzung für eine herstellerübergreifende Kommunikation schafft die Management Information Base (MIB). Sie ist eine Art Datenbank in der der Hersteller des Agenten wichtige Variablen definiert. Diese Variablen werden in Zusammenhang mit dem SNMP Objekte genannt. Abweichend vom Namen haben diese Objekte nur einen Zustand aber keine Methoden. Variablen oder Objekte können Inventar-informationen oder beliebige Messwerte sein. Durch eine MIB lässt sich so die gesamte Funktionalität einer Komponente ausdrücken.

1988 erschien im RFC 1066 die erste Gruppe von managebaren Objekten. Die MIB-I – aus heutiger Sicht - enthielt acht Objektgruppen mit ca. 100 Objekten.

Im Mai 1990 wurden im RFC 1158 mit der MIB-2, drei neue Objektgruppen und weitere Objekte eingeführt.

Es gibt bereits von Anfang an drei Möglichkeiten zur dynamischen Erweiterung:

1. Die Veröffentlichung einer neuen MIB-Spezifikation
2. Die Benutzung der experimentellen Gruppe
3. Die Benutzung der privaten Objektgruppe im Management-Subtree

Im März 1991 wurde die MIB-2 noch einmal überarbeitet und an das RFC 1212 angepasst. Ein neuer Objektindentifikator wird nicht eingeführt.

2.2.1 Struktur

Eine MIB ist hierarchisch aufgebaut. Jedes „Managed Object“ lässt sich in einer Baum-struktur darstellen, durch welche eine weltweit eindeutige Kennung der Klassen

möglich wird. Die Wurzel des Baumes wird überwacht durch die ISO. Teilbäume werden wiederum durch andere Organisationen verwaltet.

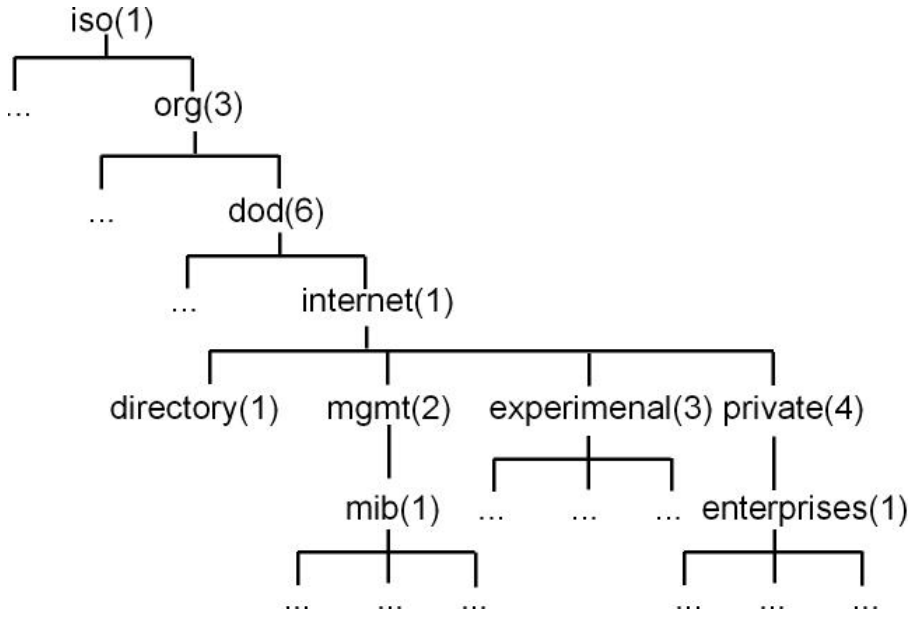

Abbildung 2: MIB-Baumstruktur /4/

1. Unter dem directory(1)-Knoten sollen Implementierungen des ISO/OSI-Directory-Dienstes eingefügt werden.
2. Der mgmt(2)-Knoten ist die Wurzel für alle standardisierten Managed Objects und somit auch für die bereits angesprochene MIB-II, die im Knoten mib(1) beginnt.
3. Der experimental(3)-Knoten bietet die Möglichkeit, Managed Objects vor der endgültigen Standardisierung zu testen.
4. Im private(4)-Teilbaum schließlich haben Unternehmen die Möglichkeit, für sich einen Namensraum eintragen zu lassen, unter dem sie ihre eigenen, proprietären Managed Objects entwickeln können. So gehört der Knoten ibm(2) unter dem enterprise(1)-Knoten zu IBM, wohingegen DEC auf der gleichen Ebene den Knoten dec(36) registriert hat.

Quelle: Lehr und Übungsbuch TELEMATIK /4/

Durch diese Baumstruktur entsteht auch der Objectidentifier (OID).

Definition: Die Verkettung – der durch einen Punkt getrennten Nummern – bezeichnet man als Object-Identifizierer, kurz OID.

So existiert zum Bespiel der OID 1.3.6.1.4.1.231 der Firma „Siemens Nixdorf Informationssysteme AG“ (iso.org.dod.internet.private.enterprises). Die OID 1.3.6.1.2.1.1.3. steht für das Objekt sysUpTime. Man kann für Objekte Lese- oder Schreibrechte, beides oder keins von beiden definieren. Als De-facto-Standard in der IT-Welt gelten MIB-I und MIB-II, wobei MIB-I eine Untermenge aus MIB-II darstellt. Alles was nicht in diesem Grundvorrat vorhanden ist, wird herstellerspezifisch in einer privaten MIB spezifiziert. Damit ergeben sich für vergleichbare Geräte von verschiedenen Herstellern, unterschiedliche MIBs. Registrierung und Vergabe der Private Enterprise-Nummern erfolgen durch die „Internet Assigned Numbers Authority“, www.iana.org.

Erste Schritte zur Standardisierung im Bereich Senderanlagen sind bereits eingeleitet.

2.2.2 Syntax

Die Daten in einer MIB sind nur hinsichtlich Syntax und Datentypen festgelegt. (Integer, Counter32, Gauge32, Octettstring, Table usw.) Die Codierung gemäß dem Dokument mit dem Titel „Structure and Identfication of Management Information“ erfolgt nach ASN.1 (Abstract Syntax Notation One). ASN.1 wurde mit der Zielsetzung komplexe Datenstrukturen und Informationsgebilde zu beschreiben, in den achtziger Jahren von der ISO veröffentlicht. Es dient zur allgemeingültigen, herstellerübergreifenden, Hardware-unabhängigen Beschreibung von Daten. Bei den Datenobjekten unterscheidet man zwischen Namen und Attributen. Die Namen werden dabei zur eindeutigen Identifizierung der Attribute genutzt.

ASN.1 definiert Regeln die zum Verständnis des SNMP unbedingt erforderlich sind:

- Der Standard beschreibt eine Vielzahl von definierten ASN.1-Typen.
- Die Namen der ASN.1-Typen beginnen immer mit einem Großbuchstaben.

- Bestimmte reservierte Schlüsselworte werden durchgängig in Großbuchstaben dargestellt. Diesen Schlüsselworten kommt innerhalb des Standards eine spezielle Bedeutung zu.
- Bestimmte Namen beginnen mit Kleinbuchstaben. Diese Namen werden nur eingefügt, um das Verständnis der ASN.1 Notation zu erleichtern.

Quelle: Hein&Griffiths /3/

2.2.3 Kommunikation

Das Datenformat basiert entgegen der meisten TCP/IP Protokolle nicht auf definierten Header-Formaten sondern es werden Standardkodierungsvorschriften eingesetzt. Es findet ein Austausch von Nachrichten zwischen den einzelnen Protokollinstanzen statt. In der Regel wird jede Nachricht in einem völlig unabhängigen UDP-Datagramm verschickt. Das UDP ist als Transportmechanismus jedoch nicht zwingend vorgeschrieben. Auch Protokolle wie zum Beispiel TCP, jeder OSI Transport Layer (TP0-TP4) oder auch die Media Access Control-Ebene können zum Transport benutzt werden. Die Nutzung von TCP hat sich jedoch nicht durchgesetzt. Dies liegt an der höheren Belastung der Netzwerkresourcen durch das TCP-Handshakeverfahren.

Applikations-protokolle	Simple Network Management Protocol (SNMP)
Transport-protokolle	User Datagram Protocol (UDP)
Internetwork-Protokolle	IP
Netzzugangs-protokolle	Ethernet FDDI Token Ring

Tabelle 1: Der IP/UDP/SNMP-Protokollstack /3/

Jede Nachricht besteht aus folgenden 3 Teilen:

- Der Versionskennung
- Dem SNMP Community-Namen
- Der Protocol Data Unit (PDU)

Der Community-Name wird durch einen Octett-String dargestellt. Mittels des Community-Namens wird die Zugehörigkeit der Agents und der Manager definiert. Ein Agent führt nur Operationen von Managern aus, wenn dieser der gleichen Gruppe angehört.

Das SNMP unterstützt nur 5 Kommandos:

- Get Request

  Es ermöglicht einem Client die gezielte Abfrage einer bestimmten Variablen in der MIB eines Agent.

- Get Next

  Es ermöglicht einem Client die Abfrage nach einem Wert des in der MIB-Baumhierarchie nachfolgenden Objekts. Diese Funktion eignet sich besonders für das Durchqueren von Tabellen.

- Set Request

  Es ermöglicht einem Client das gezielte Setzen von Variablen in der MIB eines Agent. Positive oder Negative Bestätigung wird als Get Response-Paket zurück gesandt.

- Get Response

  Es ermöglicht einem Agent, alle an ihn gesendeten Get Next Request-, Set Request- oder Get Request Anfragen zu beantworten.

- Event/Trap

  Stellt ein Agent fest, dass ein vorher definierter Zustand eingetreten ist, so verschickt er eine Nachricht vom Typ Trap. Es geht also keine Anfrage vom Client voraus. Initial Traps können dem RFC 1215 entnommen werden.

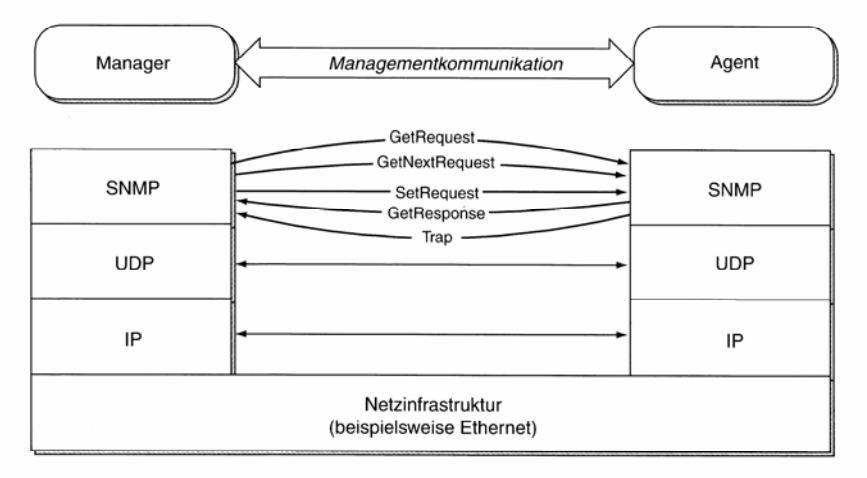

Abbildung 3: Managementkommunikation /4/

3 Die Anwendung

Durch den wachsenden Quotendruck sowohl bei den „Privaten“ als auch den öffentlich-rechtlichen Sendern, sowie den damit verbundenen Personaleinsparungen und natürlich auch der zunehmenden Digitalisierung im Rundfunkbereich, wird der Ruf nach zweckmäßigen digitalen Überwachungs- und Wartungseinrichtungen lauter. Es wird nun möglich eine Vielzahl unterschiedlicher Geräte, sowohl aus dem IT-Bereich als auch dem Broadcastbereich, zu managen. Schwierigkeiten bei der Einbindung der Broadcast-Technik resultieren vorwiegend aus der Vielzahl an Gerätetypen und Herstellern. Alleine im Bereich der Wandler- und Verteiltechnik nutzt man oft mehr als 20 verschieden Gerätetypen. Bei vielen Systemen aus der IT-Branche, wie zum Beispiel OpenView (HP) und Tivoli (IBM), stehen Fähigkeiten für die typische Rundfunkleitwarte nur eingeschränkt zur Verfügung.

Kontroll und Monitoringapplikationen von			
IT-Unternehmen		**Broadcast-Hersteller**	
IBM Tivoli	Netview	Thomson GrassValley	NetCentral
Hewlett Packard	Openview	Harris Corporation	Harris Broadcast Manager
BMC Software Inc.	PATROL	Snell&Wilcox	RollMap/RollCall
Computer Associates International Inc.	Unicenter	Dimetis	Openbroadcast

Tabelle 2: Auswahl einiger SNMP-Applikationen /2/

3.1 Lösungsansätze

Viele Hersteller bieten bereits Systeme für die eigene Hardware an. Meist handelt es sich dabei um einen Manager und ein Monitoringsystem. Hier steht meist die Veränderung von Parametern der Wandler und Verteiler im Vordergrund. Ein zweiter

Ansatz besteht in so genannten Umbrellasystemen. Diese Systeme bieten oft einen erweiterten Umfang wie das Management von Leitungswegen oder Belegungsplanung. Sie übernehmen auch Informationen anderer Systeme und bieten diese in einer Gesamtdarstellung an. Sie werden auch bei Versorgungsunternehmen wie Wasser-, Gas- und Energieversorgung eingesetzt.

3.2 Beispiele für Einzelgeräteüberwachung

iControl von Miranda:

- Überwachung eigener Geräte
- Einbindung von Komponenten der Firma Network.
- Zur Überwachung wird eine Erweiterungskarte (Probe) benötigt. Die Art der Karte richtet sich nach der zu überwachenden Signalform (Audio, Video, digital oder analog).
- Zentrales Element ist der iControl Application-Server.
- Neben dem Alarmmanagement können messtechnische Parameter wie zum Beispiel Waveform und Vektorskop-Monitoring und Audiolevel überwacht werden.
- Darstellung der Ereignisse über Webclients oder auf einer Kaleido-Monitorwand (Miranda).

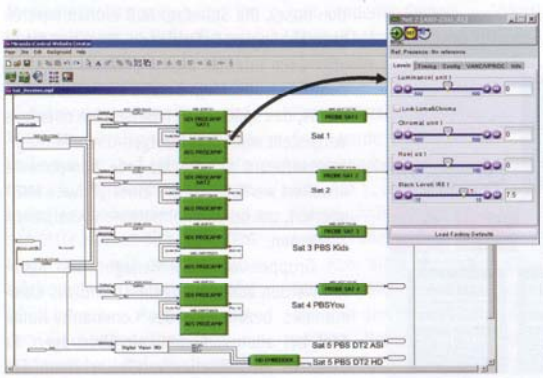

Abbildung 4: iControl von Miranda /2/

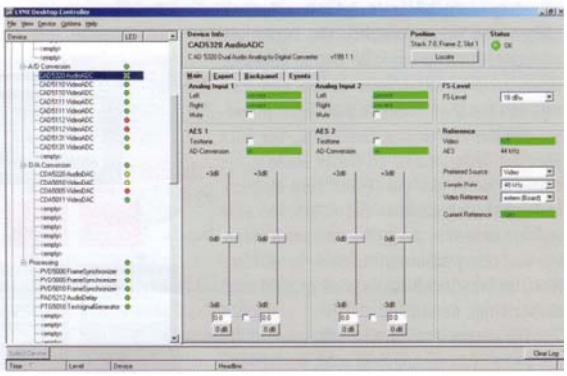

Abbildung 5: Lynx Desktop-Controller /2/

Lynx Desktop-Controller von Lynx-Technik AG

- Auch hier können die eigenen Geräte mittels einer Zusatzkarte, dem Master Controller, in den Einschubträgern überwacht werden.
- Kenngrößen können dargestellt und extern geändert werden.
- Basis ist SNMPv1
- Es können auch Traps versendet werden.

Gyda von Network

- Der Rack-Controller überwacht und ändert die Systemparameter.
- Übersichtliche und nahezu selbsterklärende Bedienoberfläche
- Basis ist SNMPv1
- Es können auch Traps versendet werden.

3.3 Beispiele für Umbrellasysteme

Open Monitoring von Dimetis

- Aus realisierten Projekten unter dem Namen Open Monitoring gingen einige Softwaretools hervor.
- Es handelt sich um drei Module die auch einzeln genutzt werden können.
- Es werden die unterschiedlichsten Arten von Produkten und Herstellern im professionellen Broadcastbereich unterstützt.
- Basis des Systems ist unter anderem, dass viele Systeme bereits über Submangementsysteme verfügen.
- Das System basiert auf einer Datenbank – vornehmlich auf SNMP – die aber auch für parallele und serielle Schnittstellen einsetzbar ist.
- Über benutzerspezifische Anzeigen können alle kritischen Elemente eines Systems überwacht werden.

- Die Anzeige ist sowohl im Detailgrad als auch bei der Art der Grafiken frei gestaltbar.

NetCentral IV von Thomson

- Das System ist für den Einsatz in Broadcastumgebungen konzipiert.
- Überwachung von IT-Strukturen nur mit erheblichem Mehraufwand.
- Es können Produkte von Thomson/Grass Valey und anderer Hersteller überwacht werden.
- Im Gegensatz zu Dimetis dient das System nur der Überwachung und Alarmierung.
- Die Visualisierung ist nahezu selbsterklärend.
- Darstellung als Gestellansicht und Blockdiagramm.
- Die üblichen Auswertungslisten in Tabellenform sind vorhanden.

Signacontrol EP 2000 von Erwin Peters Systemtechnik GmbH

Das offene Leitsystem „Signacontrol EP2000“ verfügt über modulare Kommunikationsprozessoren in Hard- und Software.

Die Kommunikationsprozessoren wandeln alle Informationsobjekte der angeschlossenen Geräte in Leitsystemobjekte.

Systemerweiterungen und Ergänzungen lassen sich problemlos integrieren. Neben den umfangreichen Tools zur vollgraphischen Prozessvisualisierung bietet das System Zugriff auf Web-Applikationen. Dies ist sinnvoll, da heute viele Komponenten weitere Einstellungen über ein Webinterface zulassen.

Dieses System basiert auf einem unter QNX laufenden Server und dem EP2000 Leitplatz. Auf Grund der bestehenden Problematik der unbestätigten Traps wurde bisher nur das Pollingverfahren implementiert. Ein Nachrüsten ist vorgesehen und jederzeit nachrüstbar. Um jedoch von Problemen unterrichtet zu werden, fragt der Kommunikationsprozessor die Agenten in regelmäßigen Abständen per Get-Befehl ab. Die Zykluszeit ist frei wählbar.

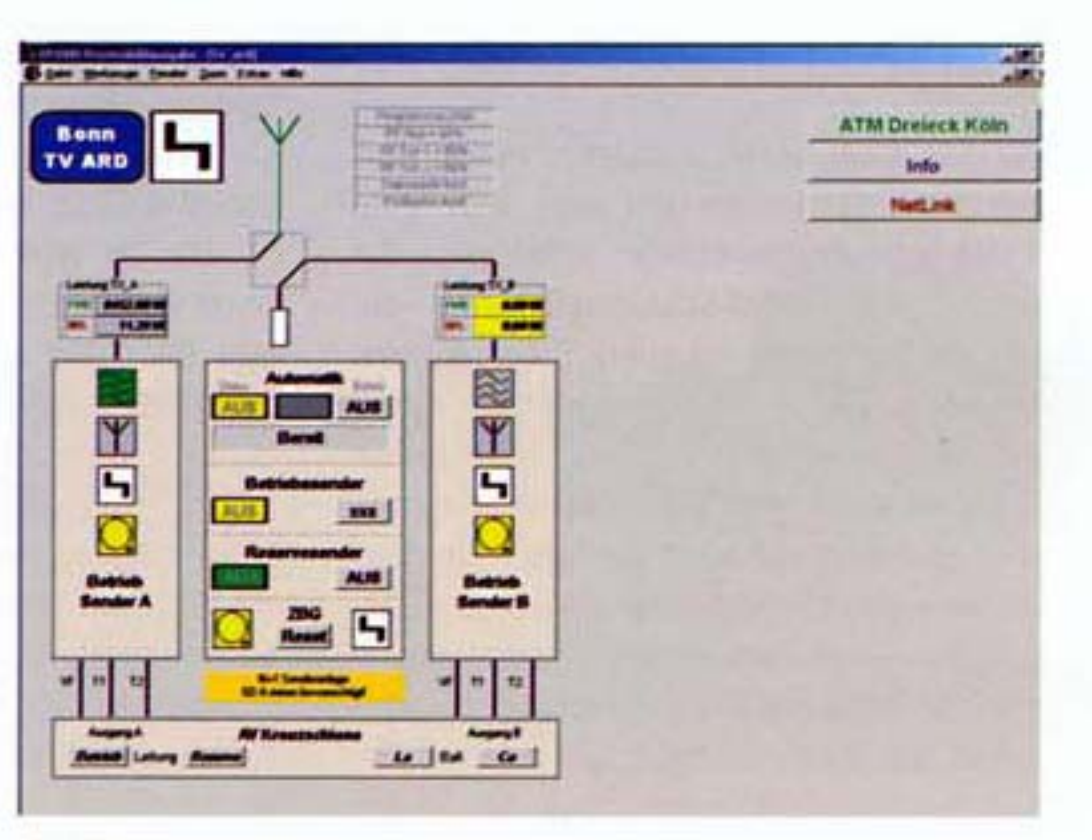

Abbildung 6: dynamisches Prozessbild des EP2000 /1/

Zusätzlich werden beim WDR drei ATM-Switche des WDR-Backbone-ATM Rings überwacht.

Beim EH 2000 können auch weitere Windows Clients angeschlossen werden.

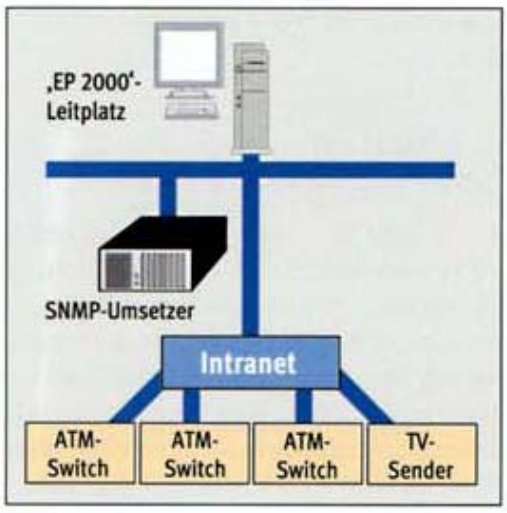

Abbildung 7: Systemstruktur eines (Netz-)Leitsystems /1/

4 Sicherheit

Es sollte zumindest SNMPv3 eingesetzt werden, da diese Version Verschlüsselungsalgorithmen wie MD5 oder SHA integriert hat. Zusätzlich empfiehlt sich der Aufbau eines zusätzlichen LAN. Dies dürfte aus Kostengründen jedoch nicht immer möglich sein. Alternativ kann man auch mit vertretbarem Risiko ein VPN, inklusive den damit verbundenen Sicherheitssystemen wie Verschlüsselung und Firewalls, einrichten.

5 Ausblick

Der WDR betreibt seit 1998 ein „Signacontrol FH6000“-Leitsystem welches zur Überwachung von analogen Sendern genutzt wird. Im Zuge der Digitalisierung wurde dies um die Überwachung von DAB erweitert. Im Rahmen der Einführung von DVB-T wurde als Pilotprojekt das Leitsystem „Signacontrol EP2000“ eingeführt.

Mit SNMP existiert eine umfangreiche und auf den Broadcastbereich sehr gut adaptierbare Technik, die sich in der IT bereits bewährt hat. Eine ganzheitliche Überwachung könnte bereits in kurzer Zeit erreicht werden. Schwerpunkt sollte im Dialog zwischen Sendeanstalten und Systemhäusern liegen, damit die Bedürfnisse der Sender entsprechend umgesetzt werden.

Literaturverzeichnis

/1/ FKT 8-9/2004

/2/ FKT 5/2005

/3/ Mathias Hein, David Griffiths: SNMP, International Thomson Publishing GmbH, ISBN: 3-929821-51-6

/4/ Gerhard Krüger, Dietrich Reschke: Lehr- und Übungsbuch TELEMATIK, Fachbuchverlag Leipzig, ISBN: 3-446-21053-9

/5/ James Martin, Joe Leben: TCP/IP-Netzwerke: Architektur, Administration u. Programmierung, Prentice Hall, ISBN 3-930436-19-1

/6/ Andrew S. Tannenbaum: Computernetzwerke, Prentice Hall, ISBN 3-8272-9536-X

/7/ Datenblätter und Prospekte der Firma Erwin Peters Systemtechnik GmbH

/8/ Produktinformationen von www.miranda.com

/9/ Telefongespräch vom 25.05.2005 mit Dipl.-Ing. Ludmilla Leidag, IRT GmbH, München

/10/ Telefongespräche mit Mitarbeitern der Erwin Peters Systemtechnik GmbH, Bochum

/11/ Jean-Philippe Martin-Flatin: Web-Based Management of IP Networks and Systems, John Wiley & Sons LTD, ISBN 0-471-48702-3

/12/ Herstellerhomepage von Miranda Technologies Inc. http://www.miranda.com