FAKULTÄT FÜR !INFORMATIK

Network Management Techniques in Facility Management

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Informatik

ausgeführt von

Dietmar Ruzicka
Matrikelnummer 9627019

am:
Institut für Softwaretechnik und Interaktive Systeme

Betreuung:
Betreuer: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Gerald Futschek

Wien,

_____ _____

(Unterschrift Verfasser) (Unterschrift Betreuer)

Kurzfassung

Facility Management und Netzwerk Management sind zwei große Managementdisziplinen. Während Facility Management sich als allumfassendes ganzheitliches Management von Immobilien darstellt, beschränkt sich Netzwerk Management auf die Nutzungsphase der Ressourcen. Diese Ressourcen sind das Gebäude selbst, das Grundstück worauf es steht und alle Einrichtungen innerhalb, etwa ein Server in der EDV. Die der Arbeit zu Grunde liegende Frage ist, können Network Management Techniques im Facility Management vorteilhaft zur Anwendung kommen? Die Untersuchung der Definitionen von Facility Management und Netzwerk Management in den Normen und die konstruktive Methode der praktischen Umsetzung der These zeigen: Die fünf Funktional Areas aus dem Netzwerkwerk Management definierten Techniken, die in den Nutzungsphase einer Immobile sehr gut anwendbar sind. Die fünf Areas: Fault, Configuration, Accounting, Performance und Security Management können in den drei Bereichen Technisches, Infrastrukturelles und Kaufmännisches Gebäude Management viele Aufgaben übernehmen. Gebäude Management deckt die Nutzungsphase, die kostenintensivste und längste Phase des Facility Management, vollständig ab. Die praktische Umsetzung im Hotelumfeld belegt die Anwendbarkeit der Ideen.

Abstract

Facility Management and Network Management are both huge management disciplines. While Facility Management is illustrated in an all-encompassing way, Network Management is limited to the utilisation of resources. Those resources are the building itself, the estate or everything inside the object. The basic research question is. May Network Management Techniques used advantageously in Facility Management? The analysis of the definition of Facility Management and Network Management and the constructive method of practical implementation leads to: The five functional areas of Network Management define techniques, which are very advantageous during the utilisation phase of a building. The five areas, Fault, Configuration, Accounting, Performance and Security Management get to do lots of duties and responsibilities in the three divisions Technical, Infrastructural and Commercial Property Management. Property Management covers the whole utilisation phase of Facility Management, which is the longest and most cost-intensive period. The implementation of Network Management in Facility Management in the hospitality branch proves its benefit.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien,

Inhaltsverzeichnis

Abkürzungsverzeichnis

AA	Analogausgang
AE	Analogeingang
AVA	Ausschreibung, Vergabe und Abrechnung
BOOTP	Bootstrap Protocol
CAFM	Computer Aided Facility Management
CIM	Common Information Model
CMI	Cordless Multicell Integration
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMISE	Common Management Information Service Element
CP	Communication Processor
CPU	Central Processing Unit
DA	Digitalausgang
DE	Digitaleingang
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung
DTMF	Distributed Management Task Force
EDV	Elektronische Datenverarbeitung
EM	Erweiterungsmodul
ERP	Enterprise Resource Planning
HHSC	HiPath Hospitality Service Center
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IAB	Internet Activity Board
IP	Internet Protocol
ISO	International Standards Organization

IT	Informations Technologie
ITU	International Telecommunication Union
LAN	Local Area Network
LSB	Least Significant Bit
MAC	Media Access Control
MIB	Management Information Base
MIS	Management Information System
MSB	Most Significant Bit
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NMS	Network Management System
NRPE	Nagios Remote Plugin Executor
NSCA	Nagios Service Check Acceptor
OID	Object Identifier
OSI	Open Systems Interconnection
PC	Personal Computer
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PMS	Property Management Systems
RFC	Request For Comment
RFID	Radio Frequency Identification
SM	Sondermerker
SNMP	Simple Network Management Protocol
SPS	Speicherprogrammierbare Steuerung
TCP	Transmission Control Protocol
TMN	Telecommunication Management Network
UDP	User Datagram Protocol
V	Verfügbarkeit
VMS	Voice Mail Systems
XML	Extended Markup Language

Tabellenverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einleitung

Lässt man folgende Anforderungsbeschreibung, des HiPath Hospitality Service Center, kurz HHSC, einen im Bereich Netzwerk Management erfahren Informatiker lesen, so wird er diese als Anforderung an ein Netzwerk Management System verstehen. Die Beschreibung enthält zentrale Elemente aus dem Netzwerk Management. Fehlererkennung, Poll-based Management und das Konzept der Alarmierung sind zentrale Forderungen des Fault Management, der wichtigsten Functional Areas des Netzwerk Management.

„Das Facility Management ermöglicht über potentialfreie Kontakte eine Erkennung von Störungen in technischen Einrichtungen. Es erkennt Fehler automatisch und benachrichtigt das zuständige Personal. Die Anschaltung der potentialfreien Kontakte geschieht über eine LAN-Box. Das Facility Management fragt in einem konfigurierbaren Intervall die Kontaktzustände der LAN-Box ab und triggert nach einer Pegeländerung der Kontakte einen Meldungsvorgang. Jedem Kontakt kann hierbei ein frei definierbarer Text, als Meldung zugeordnet werden. Die Konfiguration wird in einem getrennten Bereich der Datenbank gespeichert. Soll eine Meldung verschickt werden so werden nach dem Benachrichtigungsplan Displaymeldungen an die zuständigen Endgeräte geschickt.“ [HHSCP]

Das HiPath Hospitality Service Center des Hersteller Siemens ist eine Customer Relationship Management Applikation für das Hotelgewerbe. Das HiPath Hospitality Service Center kombiniert die Kommunikationsmöglichkeiten von HiPath-IP-Telefoniesystemen mit einem Paket von Hotel-Service-Anwendungen und bietet auch Schnittstellen zu Gebäudemanagementsystemen. Die Applikation unterstützt

das Hotelgewerbe bei der Definition und der Verfolgung von Service-Aufträgen, im Call Control Center, beim Management von Kundenbeziehungen und bei Buchungsfunktionen. Die oben zitierte Anforderungsbeschreibung stammt aus dem Pflichtenheft von HHSC. Diese Schnittstelle zu Gebäudemanagementsystemen ist zu implementierten. Die Idee Anforderungen aus dem Facility Management mit Werkzeugen und Techniken aus dem Netzwerk Management zu erfüllen ist die Motivation für diese Arbeit.

Facility Management und Netzwerk Management sind allgemeine breit verwendete Begriffe. Es gibt viele unterschiedliche Interpretationen. So ist es üblich Mitarbeiter im Bereich der Gebäudereinigung als Facility Manager zu bezeichnen, eine sehr schmeichelnde Bezeichnung. Eine andere Frage ist, entspricht Facility Management der Gebäudeautomation? Auch dem Begriff Netzwerk Management kommt in unserer modernen, vernetzten Welt eine besondere Bedeutung zu. Doch was ist Netzwerk Management genau?

1.1 Aufgabenstellung

Die der Arbeit zu Grunde liegende Fragestellung ist kann man Network Management Techniques im Facility Management vorteilhaft anwenden. Beide Managementdisziplinen sind genormt. An Hand dieser Normen soll festgestellt werden welche Bereiche abgedeckt werden. Die praktische Umsetzung wird als konstruktive Methode angewandt. Das Ergebnis der Implementierung wird auf den Einsatz von Network Management Techniques hin untersucht.

Kapitel 2

Hintergrundinformation zu Network Management und Facility Management

2.1 Network Management

Allgemeine Definitionen des Begriffs Management beinhalten in der Regel die Planung, das Organisieren, das Monitoring, die Verrechnung und das Controlling von Aktivitäten und Ressourcen. In den Netzwerk Management Standards der International Standards Organization (ISO) und des Internet Activities Board (IAB) liegt der Fokus auf dem Monitoring, der Verrechnung und dem Controlling von Aktivitäten und Ressourcen in Netzwerken. Die Aspekte Planung und Organisation sind nicht Teil der Betrachtungen. Das ist erstaunlich, schließlich ist eine gute Planung und Organisation eine wichtige Voraussetzung für ein gutes Funktionieren des Netzwerkes, bzw. die Existenz des Netzes selbst. Ziel des Netzwerkmanagement ist es für den Benutzer die erforderlichen Ressourcen, zuverlässig und in ausreichendem Maße zur Verfügung stellen zu können. Die Definition des Begriffs Netzwerkmanagement im Siemens Communications Lexikon [SCL05] sieht Netzwerkmanagement als Lieferant von Informationen, welche die Grundlage für die Planung und Organisation von bilden.

„Netzwerkmanagement umfasst alle Funktionen und Komponenten zur Überwachung und Steuerung von Netzwerken. Zu den Aufgaben des Netzwerkmanagements gehören daher unter anderem das Sammeln von Informationen über die Nutzung des Netzes durch die angeschlossenen Stationen, die Erstellung von Berichten und Statistiken für die Planung, den Betrieb, den Ausfall und die Wartung, die Konfiguration des Netzes und damit verbundene Konfigurationsänderungen, die Leistungs-, Ereignis- und Fehlerüberwachung. In Verbindung mit der offenen Kommunikation legte die ISO fünf Funktionsbereiche für das Netzwerkmanagement fest: Fehlermanagement, Leistungsmanagement, Konfigurationsmanagement, Abrechnungsmanagement und Sicherheitsmanagement.“ [SCL05]

In den folgenden Teilen des Kapitels werden nach einem kurzen Überblick zum Thema die Netzwerkmanagement Standards der ISO und die entsprechenden Internet Protokolle des IAB betrachtet. Der Fokus liegt auf den Open Systems Interconnection (OSI) network management standards. Das Internet Engineering Task Force (IETF) Simple Network Management Protocol ist das am weitesten verbreitete und verwendete Protokoll im Netzwerkwerkmanagement und darf daher hier nicht fehlen. Extra besprochen und besonders genau erörtert werden die fünf Functional Areas, siehe Abbildung 1, aus dem Funktionsmodell des OSI Netzmanagement. Sie bilden die Grundlage für die Untersuchung der Network Management Techiques in Facility Management. Und es wird erläutert welche zentrale Rolle die fünf Bereiche und deren Funktionen in der Implementierung des Facility Management im HiPath Hospitality Service Center (HHSC), dem praktischen Teil dieser Arbeit spielen.

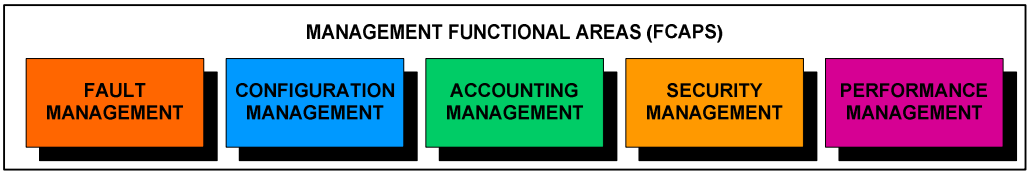


Abbildung 1 [ITU X.700] OSI Management Framework

„*Management of a system is concerned with supervising and controlling the system so that it fulfills the requirements of both owners and users of the system*" [Slom94]

Die Aufgabe und das Ziel des Network Management ist es dem Benutzer des vernetzten Systems alle erforderlichen Ressourcen zuverlässig und in ausreichendem Maße zur Verfügung zu stellen. Im Interesse des Betreibers sollen diese Aufgaben und Ziele möglichst effizient erreicht werden. Ein sehr wesentlicher Aspekt des Managements ist das Überwachen und das Kontrollieren des Systems um einen zuverlässigen Betrieb sicher zu stellen. Für diese Überwachung ist ein Manger oder ein Managementsystem erforderlich, das die eingesetzten Ressource überwacht, Nachrichten empfängt und diese auch beeinflussen kann. Dazu tauschen die Systeme Informationen aus. Kontrollinformationen, Anweisungen, Anfragen und Befehle sind vom Manager zum überwachten Gerät unterwegs und deren Antworten werden nach dem Bearbeiten wieder retour geschickt. Hochwertigere Komponenten können auch ohne Aufforderung autark bei bestimmten Ereignissen oder Fehlfunktionen Statusinformationen oder Alarmnachrichten an das Managementsystem schicken. Die Netzwerkmanagement Standards geben vor wie die Managementinformation kodiert und interpretiert wird und in welcher Form diese verpackt und über das Netzwerk transportiert wird. Es gibt gegenwärtig in der Informationstechnologie (IT) Branche eine sehr große Menge an unterschiedlichen Produzenten, welche die verschiedensten Produkte herstellen. Dank der Standards, sie legen fest wie die Kommunikation im Netzwerk funktioniert, ist es möglich die Komponenten aller Hersteller im Verbund zu betreiben. Die Netzwerk Management Standards bilden analog die Grundlage für einen Austausch von Managementinformationen und erlauben die Einbindung von Komponenten unterschiedlicher Hersteller, wenn diese die Standards implementieren.

Morris Sloman hat den Informationsfluss in [Slom94] wie in Abbildung 2 dargestellt.

Abbildung 2 [Slom94] Management Information Flow

Die Management Policies legen fest wie die Ressourcen zu monitoren sind und wie auf Events reagiert werden soll. Die Manager Role interpretiert die Richtlinien und steuert und überwacht die Resources nach diesen Vorgaben. So entsteht ein Arbeitsablauf vergleichbar mit einem Regelkreis. Abbildung 3 Zeigt den Management activity loop, wie ihn Sloman in [Slom94] darstellt.

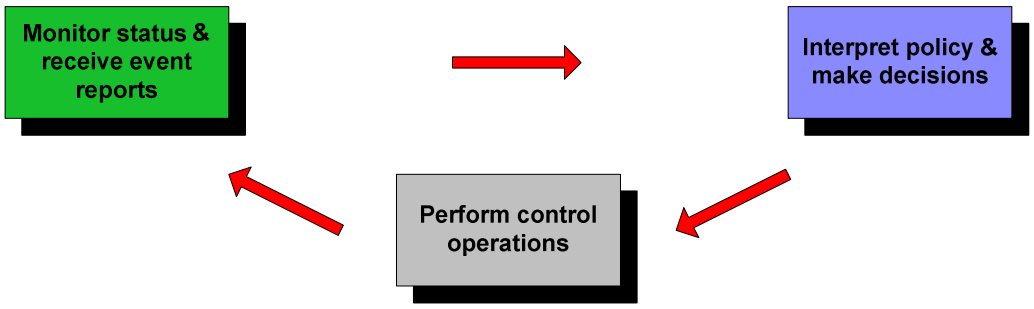


Abbildung 3 [Slom94] Management activity loop

Ein praktisches Beispiel ist das Management des verfügbaren Speicherplatzes in einem Speichersystem, beispielsweise einer Network Attached Storage (NAS). Die Auslastung des Systems wird überprüft. Steigt der benutzte Speicherplatz über eine bestimmten Schwellenwert greift der Manager ein. Entsprechend der Policies wird vorerst versucht unnötige oder veraltete Daten zu löschen oder zu archivieren. Reicht diese Maßnahme nicht aus wird das Storagesystem erweitert. Das kann natürlich wieder Einfluss auf andere Systeme, wie das Sicherungssystem haben, eventuell muss auch hier angepasst werden.

2.1.1 Open Systems Interconnection (OSI) Network Management Framework

Das OSI Network Management Framework umfasst eine Reihe von Standards und Definitionen. Die [ITU-T X.700] oder die idente ISO/IEC 7498-4, bzw. [ITU-T X.701] oder die idente ISO/IEC 10040 Dokumente liefern einen allgemeinen Überblick über die OSI-Verwaltungsstandards und bilden die Gesamtstruktur für die OSI Verwaltungsoperationen. Eine vollständige Liste der Standards sind in Anhang A Standards aufgelistet.

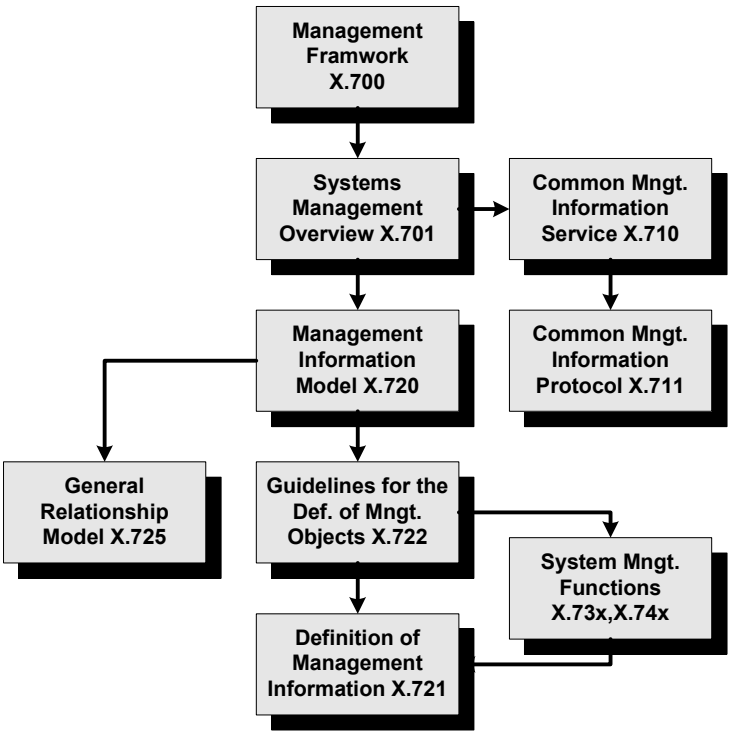


Abbildung 4 [ITU-T X.701] Beziehungen der OSI Standards

Das grundlegenden Verwaltungsdokument ist [ITU-T X.700] ITU-T

X.700 Management Framework for Open System Interconnection. Es liefert die Konzepte und Definitionen für die OSI-Verwaltung und führt auch die fünf wichtigsten Functional Areas der OSI Verwaltung ein.

Die 5 grundlegenden Konzepte sind:

Users' requirements of OSI management

Die Netzwerkmanger müssen ihre Netze planen, organisieren, betreuen, kontrollieren und deren Benutzung abrechnen können. Auf geänderte Anforderungen der Benutzer muss rechtzeitig reagiert werden können. Die Netzwerkkomponenten müssen ein vorhersagbares Kommunikationsverhalten an den Tag legen, außerdem Informationen vor unbefugtem Zugriff schützen und Authentifizierung unterstützen.

Die unterstützenden Managementtools sind abhängig von den Anforderungen unterschiedlich komplex und können lokal als auch verteilt operieren.

The OSI management environment

Der OSI Management Environment beschreibt die Werkzeuge und Dienste, die für die Überwachung, Steuerung und Koordination verteilter Netze benötigt werden. Das Management Umfeld berücksichtigt Management Interessen in der Informationsbeschaffung, der Ausübung der Kontrolle und kennt die Konfiguration aller Netzwerkkomponenten und deren Status. Die einzelne Komponente kann selbst am autonom am Management teilnehmen oder im Verbund koordiniert mit anderen Geräten Management Aktivitäten ausführen.

Managed objects, their attributes and operations

Aus der Sicht des OSI Management ist ein Managed Object eine Ressource die Gegenstand des Managements ist, beispielsweise ein Router, aber auch dessen Verbindungen, Leitungen. Eine Manged Object ist die abstrakte Sicht auf eine Ressource. Sie repräsentiert die Eigenschaften der Ressource für das Management.

Ein Managed Object wird durch seine Eigenschaften, die Verbindung zu anderen Objekten, seine Events und welche Operationen ausgeführt werden können definiert.

Eine Reihe von Manged Objects eines Systems und deren Eigenschaften bilden die Management Information Base (MIB) des Systems.

Management relationships between open systems

Das OSI Management wird erreicht durch lokale Operationen und durch die Kooperation verschiedener Systeme im Verbund. Dabei nimmt ein System die Manager Role ein und andere die Agent Role.

Operation und Nachrichten definieren den OSI Management Informationsfluss zwischen den Systemen.

OSI management functional areas

Ein hierarchischer Ansatz bei der Untersuchung der Network Management Key Requirements führte das OSI System Management Team zu fünf wesentlichen Funksbereichen. Das Kürzel FCAPS fasst diese Bereiche zusammen und steht für:

- **F**ault Management
- **C**onfiguration Management
- **A**ccounting Management
- **P**erformance Management
- **S**ecurity Management

Die Functional Areas werden unter Kapitel 2.1.3 FCAPS im Detail besprochen.

Ein weiters grundlegendes Dokument ist [ITU-T X.701] Systems management overview. Es definiert vier Aspekte des Systems Management Model:

- Communication Model
- Information Model
- Organisation Model
- Functional Model

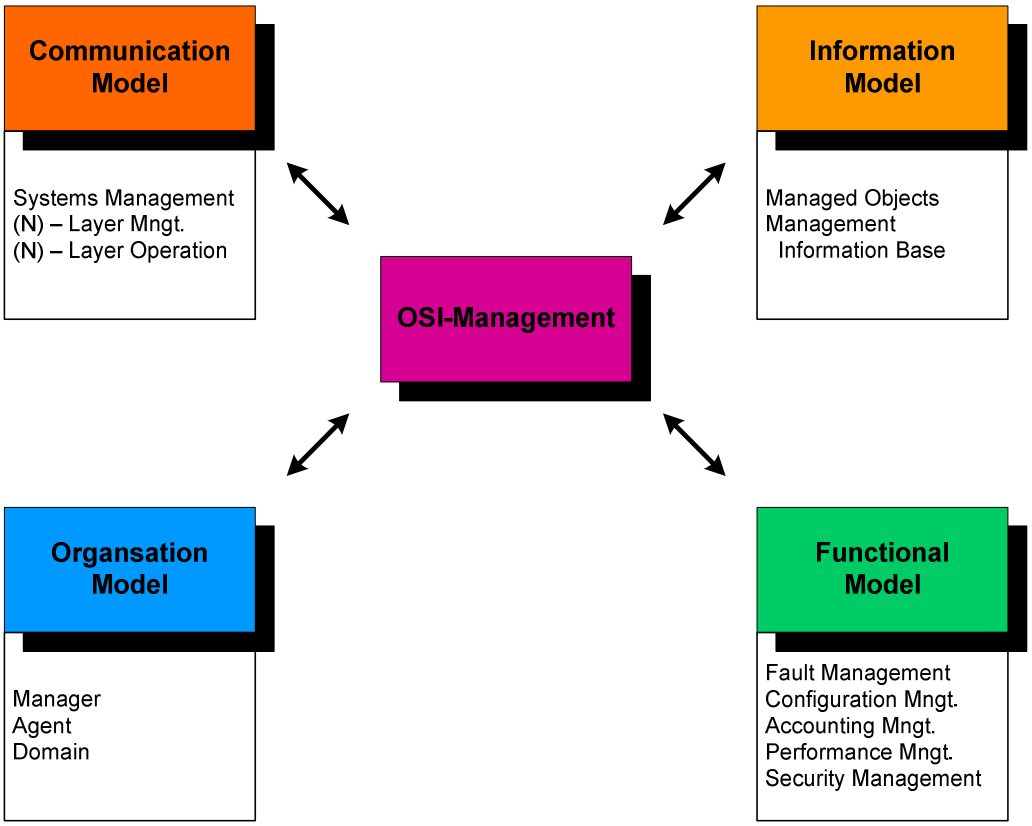


Abbildung 5 Modelle des OSI-Management

Organisation Model

Das Organisation Model definiert die Manager Role und die Agent Role und deren Beziehungen untereinander.

Abbildung 6 [Blac92] OSI management processes

Der Agent Process ist das Interface über welche der Managing Process mit den Managed Objects kommunizieren kann. Der Managing Process ist verantwortlich für die Management Aktivitäten. Der Agent Process führt die Management Funktionen am Managed Object auf Anforderung des Managing Process aus.

Information Model

Das Information Model setzt sich mit den Begriffen Managed Objects und der Management Information Base auseinander. Diese wurden bereits mit dem Konzept „Managed objects, their attributes and operations“ beschrieben.

Communication Model

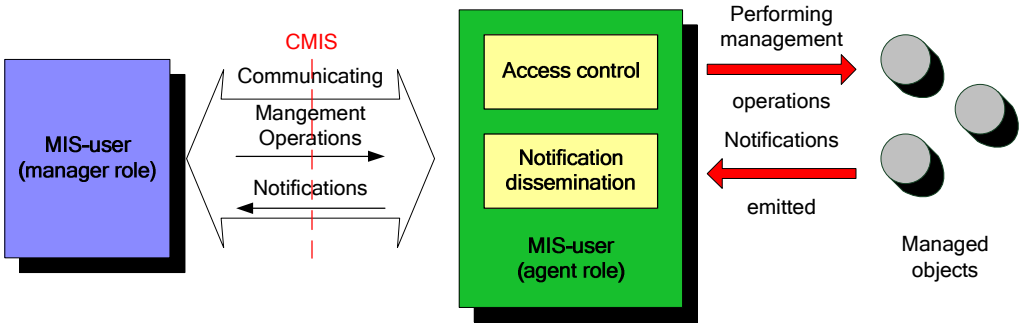


Abbildung 7 [ITU-T X.701] System management interactions

Das generelle OSI Kommunikationsservice für das System Management ist das Common Management Information Service (CMIS) mit dem entsprechenden Common Management Information Protocol (CMIP).

Die zwei Aspekte der Kommunikation:

- Request für Management Operations und Notfications,
  Polling-based Management

  Auf Anforderung Manager Role werden Informationen über die Manged Objects eingeholt oder Operationen ausgeführt.

- Dissemination von Notifications, Event-based Management

  Ohne Anforderung, sondern durch ein eintretendes Event getriggert verschickt die Agent Role Nachrichten an die Manager Role.

Functional Model

Das Functional Model beschäftigt sich mit den fünf Functional Areas, Fault management, Accounting Mangement, Performance Management und Security Management. Die Functional Areas werden unter Kapitel 2.1.3 FCAPS im Detail besprochen.

2.1.2 Internet Engineering Task Force (IETF) Simple Network Management Protocol (SNMP)

In der Praxis des Netzwerkmanagement ist das Simple Network Management Protocol (SNMP) das am weitesten verbreitete Kommunikationswerkzeug. SNMP ermöglicht den Austausch von Management Informationen zwischen Netzwerkgeräten. Es erlaubt das Überwachen als auch das Konfigurieren von Netzwerkkomponenten Das Protokoll ist Teil der Transmission Control Protocol/Internet Protocol (TCP/IP) Suite. Eine Reihe von Standards und Spezifikationen definieren SNMP, dessen zugehörige Funktionen und Datenbanken. Die drei grundlegendsten und wichtigsten sind von der IETF folgende Request For Comments (RFC) Dokumente:

- RFC 1155 Structure and Identification of Management Information for TCP/IP-based internets, Mai 1990
- RFC 1156 Management Information Base for Network Management of TCP/IP-based internets, Mai 1990
- RFC 1157 A Simple Network Management Protocol, Mai 1990

Ein via SNMP gemanagtes Netzwerk besteht aus den drei Schlüsselkomponenenten: Managed Devices, Agents und aus dem Network Management System (NMS).

SNMP Komponenten

Ein Managed Device ist eine mit einem SNMP Agent ausgestattete Netzwerkkomponente, die mit einem SNMP Netzwerk verbunden ist. Diese Komponenten sammeln und speichern die Management Informationen. Sie stellen diese Informationen dem Network Management System via SNMP zur Verfügung. Router, Switches, Drucker, Server, etc. sind übliche Komponenten. Sie werden auch in der Literatur als Network Element bezeichnet.

Ein Agent ist ein Netzwerk Management Software Modul. Dieses Modul läuft in dem Managed Device. Der Agent hat Zugriff auf die lokalen Management Informationen und übersetzt diese SNMP konform.

Ein Netzwerk Management System ist eine Software, die Netzwerkkomponenten überwacht und steuert und die zugehörige Hardware stellt erforderlichen Ressourcen zur Verfügung.

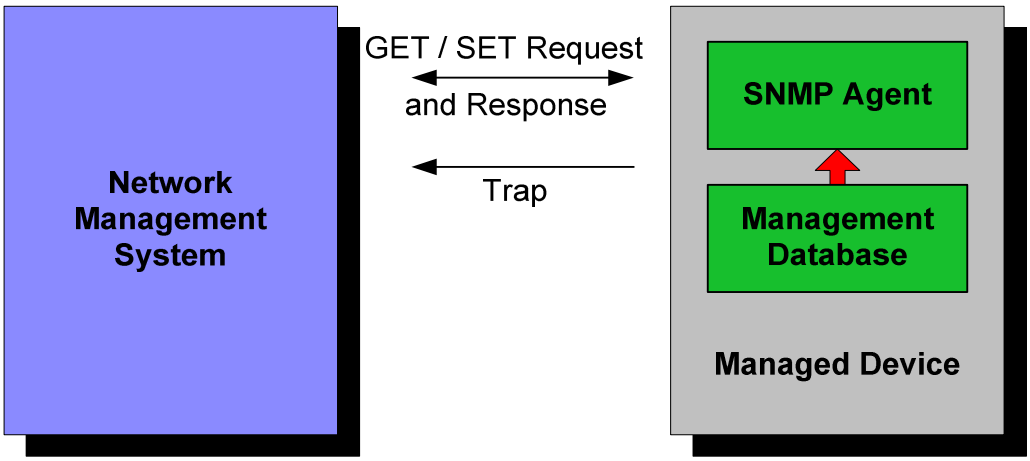


Abbildung 8 Network Management System, SNMP Agent und Managed Device

SNMP Kommandos

Die drei grundlegendsten und wichtigsten Kommandos im SNMP Protokoll sind der Get Request/Response, der Set Request/Response und der Trap.

Das Get Kommando wird von der Network Management System Software für das Monitoring der Managed Devices eingesetzt. Dazu versendet das System eine GetRequestPDU (Protocol Data Unit). In dieser Protocol Data Unit ist die Anfrage an den Agent verpackt. Die Anfrage kann die Werte einer oder mehrer Object Identifier (OID) des Agents fordern. Der Agent beantwortet den Request mit der GetResponsePDU, die den gewünschten Wert enthält.

Mit dem Set Kommando kann das Network Management System Werte in Object Indentifier des Agents setzen. Hier schickt das System eine SetRequestPDU an den Agent. Dieser setzt den Wert und schickt eine GetResponsePDU an das System zurück.

Der Agent benutzt das Trap Kommando um asynchron das Network Management System über Ereignisse zu informieren. Tritt ein entsprechender Vorfall auf sendet der Agent eine TrapPDU. Der Agent erwartet auf seine TrapPDU keine Antwort. Das Network Management System wertet die Information aus und leitet die erforderlichen Maßnahmen dazu ein.

Ein SNMP Get entspricht dem Poll-driven Management, während die SNMP Traps ein Event-driven Management realisieren.

SNMP Management Information Base

Die Management Information Base (MIB), die Management Database, beinhaltet eine Reihe von Management Informationen und organisiert diese hierarchisch. Object Identifier (OID) identifizieren die einzelnen Werte eindeutig, man spricht von Managed Objects. Die Managed Objects repräsentieren die Attribute, die Charakteristik des Managed Devices. Sie enthalten ein oder mehrere Objektinstanzen, die Variablen. Die MIB Hierarchie kann übersichtlich als Baum dargestellt werden. Die top-level OIDs sind an die verschiedenen Standards Organisationen vergeben. Hardware- und Softwarehersteller können eigene Äste für deren Produkte definieren.

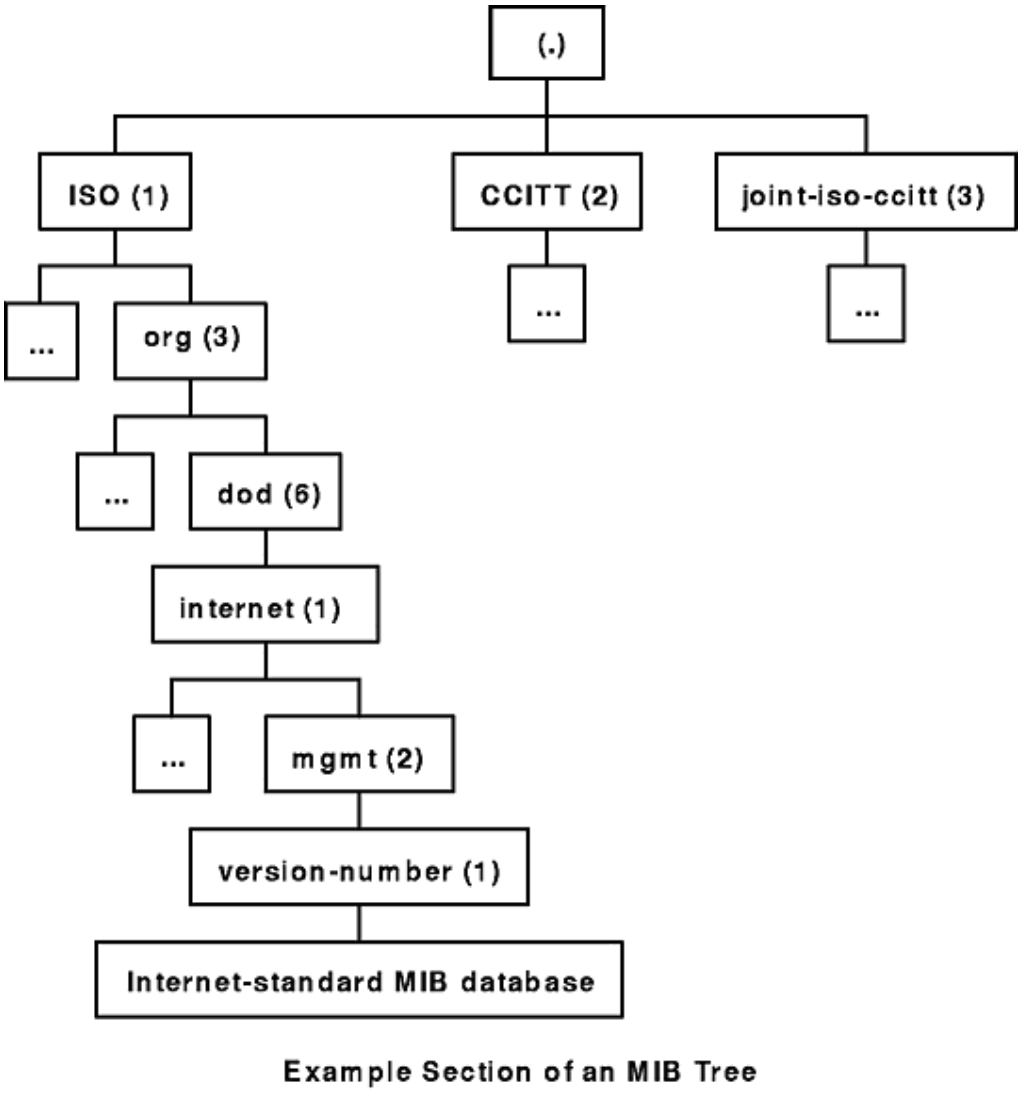


Abbildung 9 [CIBM08] Example Section of an MIB Tree

2.1.3 FCAPS

Fault Management

Fault Management ist die proaktive Unterbindung bzw. Erkennung, Isolierung und Behebung von anormalem Verhalten im Netzwerk. Es ist das Bestreben mögliche Probleme in einem Netzwerk im Vorfeld zu finden und zu lösen, bevor sie zu realen Problemen werden. Es beinhaltet das Konzept der Alarme. Diese Alarme verständigen den Netzwerkmanager wenn kritische Schwellwerte überschritten werden. Ein Ziel des Fault Management ist es auf Basis von Trendanalysen Fehler und Änderungen im Zustand vorab zu erkennen um die Verfügbarkeit für den User sicherzustellen.

Das Fault Management ist wahrscheinlich die am weitesten verbreitete und am häufigsten implementierte Funktional Area des Network Management.

Das OSI Management definiert in [ITU-T X.700] folgende Fault Management Funktionen:

- Ausführen von Diagnose Tests und Abfolgen, Poll-driven Management
- Akzeptieren und bearbeiten von Ereignisnachrichten,
  Event-driven Management
- Alarmmeldungen und Tracking von Fehlern
- Korrigieren von Problemen, falls möglich automatisiert.
- Führen und prüfen von Log Dateien.

Eine Reihe von Tests und Überprüfungen gewinnen Informationen darüber was gerade im gesamten System vor sich geht. Das Netzwerk Management System muss wissen was ein Problem ist und wann kein Problem vorliegt. Schwellenwerte, Thresholds legen die Grenze, wann liegt ein Problem vor, wann ist das Ergebnis der Prüfung im grünen Bereich, also in Ordnung, fest. Diese Werte sind ein wichtiges Konzept im Netzwerkmanagement. In der Praxis konnten sich mehrstufige Schwellenwerte bewähren, beispielsweise bei der Überwachung des freien Speicherplatzes eines Speichersystems. Der erste Threshold, bei 70%iger Auslastung oder 30% freiem Platz löst eine Warnung aus und ein zweiter Schwellenwert, bei 85%iger Auslastung also 15% freiem Speicherplatz löst eine Fehlermeldung aus. In diesem Fall kann der zuständige Administrator rechtzeitig, ohne dass dem Benutzer

bekannt wird, den Platz durch beispielsweise hinzufügen einer weiteren Platte zum Raidsystem auf den Hinweis reagieren. Nicht alle Tests liefern so einfach Informationen wie die Überprüfung der Auslastung eines Speicherplatzes. Dieses Beispiel kann völlig ungefährlich parallel zum normalen Produktionsbetrieb laufen, die Daten liegen ohnehin vor oder der Test benötigt keine, bzw. kaum Ressourcen. Tests, die den Produktionsbetrieb stören, bzw. exklusiven Zugriff auf die Ressourcen benötigen heißen disruptive Tests. Diese können nur offline, exklusiv laufen. Das ist je nach Anforderung beispielsweise in einem Wartungsfenster oder einfacher außerhalb der Bürozeiten möglich.

Bei den Tests, den Überprüfungen kennt man zwei Aspekte der Kommunikation. Das Poll-driven Management und das Event-driven Management.

Beim Polling sammeln viele in regelmäßigen Abständen wiederholte Test Informationen über den Zustand des Systems. Das System in der Manger Rolle veranlasst und steuert diese Überprüfungen. Es ist das aktive System. Diese Tests nehmen Kontakt mit dem System in der Agent Role auf und fordern die Informationen an. Abhängig vom Ergebnis der Tests versendet die Manager Role keine oder eine positive oder eine negative Nachricht an den Administrator. Jeden Morgen in unzähligen Bäckereien, der Bäcker kontrolliert in jedem Ofen regelmäßig den Zustand seiner Brotleibe, die Managed Objects. Dabei achtet der Meister auf die Farbe der Rinde, ist eine ausreichende Bräunung erreicht, ist das Brot fertig. Diese Vorgehensweise entspricht dem Polling. Das Polling ist ein aufwendiger Prozess. So muss der Bäcker zu jedem Ofen hingehen, ihn öffnen, das Brot betrachten, den Ofen wieder schließen und wieder zurück zu seiner ursprünglichen Tätigkeit. Betreibt die Backstube eine Anzahl von Öfen, so erhöht sich natürlich der Aufwand der Überprüfung mit jedem weiteren Ofen.

Beim Event-driven Management übernimmt das System in der Agent Role den aktiven Part. Der Agent misst laufend Daten und bei überschreiten eines gewissen Schwellenwertes benachrichtigt der Agent das System in der Manager Role. Diesmal hat unser Bäcker viel Geld in seine Öfen investiert. Diese Öfen sind mit einem Thermometer, welches die Temperatur im Inneren des Brotleibes messen kann ausgestattet. Der Ofen beobachtet die Temperatur, bei Erreichen eines bestimmten Wertes im Inneren gilt das Brot als fertig und der Ofen verständigt den Bäcker über einen akustischen Alarm.

Für das Management und den Administrator ist eine gute Übersicht über den Status des Netzwerkes von großer Bedeutung. Wissen was los ist gehört zu den wichtigsten

Aufgaben des betreuenden Personals. Welches System ist gerade ausgefallen, welches Dateisystem läuft über und welcher Serverprozess ist abgestürzt: Das Administrator muss es als erster bemerken, um schnell für Abhilfe zu sorgen. Alle gängigen Netzwerk Management Produkte bieten eine derartige Übersicht. Es ist darüber hinaus auch erforderlich die Aufmerksamkeit auf aktuelle Probleme zu lenken.

Ein überaus wichtiger Aspekt im Fault Management ist ein Alarm und Trouble Ticket System. Ein Alarmsystem hat die Aufgabe das betreuende Personal über Probleme, negative Ereignisse und dessen Behebung aktiv zu informieren. Um zuverlässig und schnell die Informationen zielgerecht transportieren zu können wird gegenwärtig sehr gerne neben Emails auch SMS verwendet. Sehr wichtig ist einem Alarmsystem ist ein gutes Konzept und gute Filtermöglichkeiten. So kann ein verhindert werden, dass wichtige Meldungen in einer Flut von Nachrichten unter gehen. Eine Alarm Shower [Kope97], eine Menge von korrelierten Alarmen muss unbedingt vermieden werden. Unterbricht beispielsweise der Ausfall eines Router die Verbindung zu einem Teil des Netzwerkes, so ist ein gutes Konzept nur den Ausfall des Router mit entsprechender Priorität zu melden und alle Meldungen über die einzelnen nicht erreichbaren Systeme des Subnetzes zu unterbinden.

Ein Tracking von Ereignissen kann sehr gut mit einem Trouble Ticket System realisiert werden. Für jedes Problem, negatives Ereignis wird ein Ticket erzeugt. An Hand dieses Tickets kann nachvollzogen werden, wie der Status der aktuellen Problems ist und ob mit einer baldigen Lösung zu rechnen ist. Die Anzahl der offenen Tickets ist Indikator für den Status des gesamten Systems. Werden in den Tickets auch die Lösungswege aufgezeichnet, so kann das Ticketsystem auch als quasi Wissensdatenbank für eine beschleunigte Problembehebung gleicher oder ähnlicher Probleme dienen.

In der Regel behebt das Administratorenteam die aufgetreten Probleme und Fehler durch manuelles Eingreifen. Viele dieser Tätigkeiten sind Routinetätigkeiten. Routinetätigkeiten sind Handlungen die regelmäßig und immer gleich ausgeführt werden. Sie sind daher potentielle Kandidaten für Automatisierung. Solche Aktionen sind beispielsweise das Neustarten verschiedener Prozesse oder ganzer Systeme, stoppen von hängengebliebenen Prozessen oder Sessions eines Webservers oder einer Datenbank oder Bereinigungsaktivitäten in Dateisystemen. Oft sind diese Managementtätigkeiten direkt in Produkten und Lösungen bereits realisiert und somit auch Teil des Netzwerkmanagements.

Alle Ereignisse, Statusänderungen, Diagnosetests und deren Ergebnisse sind wichtige Informationen und sollen in Logdateien mitprotokolliert werden. Diese Informationen sind eine wichtige Informationsquelle für spätere Auswertungen im Performance Management.

Configuration Management

Configuration Management umfasst die Konfiguration des Netzwerks und dessen Geräte. Diese Disziplin wird auch gerne Capacity Management genannt, weil der Hauptfokus im Umgestalten der Topologie, bzw. im Hinzufügen, Neuverteilen von Ressourcen um ausreichende Kapazitäten zu Verfügung zu stellen liegt. Auch die Automatische Konfiguration wird mehr und mehr zum unersetzbar wichtigen Teil des Netzwerk Management, da die Netze laufend wachsen.

Das ISO Configuration Management wird um fünf Einrichtungen organisiert:

- Objektkonfiguration
  Verwaltet das Hinzufügen, Löschen, Eintragen, Austragen und Benennen der Instanzen der verwalteten Objekte.

- Zustandsverwaltung
  Verwaltet das Untersuchen, Setzen und Benachrichtigen von Änderungen Verwaltungszustandes der verwalteten Objekte

- Attributsverwaltung
  Verwaltet das Untersuchen, Setzen und Benachrichtigen von Änderungen der allgemeinen Attribute der verwalteten Objekte

- Beziehungsverwaltung
  Verwaltet das Untersuchen, Setzen und Benachrichtigen von Änderungen der Beziehungen der verwalteten Objekte

- Softwareverteilung
  Verwaltet die Verteilung der Software und Benachrichtigen über Versionsänderungen, sowie das Auslösen von Urstartprozeduren in einem verwalteten Objekt

Das Configuration Management definiert außerdem die Verwaltungszustände der verwalteten Objekt in [ITU-T X.731]. Vier Zustände sind definiert:

- In Betrieb
  Die Ressource ist nicht in Benutzung, aber funktionsfähig und verfügbar.

- Außer Betrieb
  Die Ressource ist nicht verfügbar oder die hängt von einer anderen Ressource ab, die nicht verfügbar ist.

- Aktiv
  Die Ressource ist für die Benutzung verfügbar und kann Dienste von anderen Ressourcen anzunehmen.

- Beschäftigt
  Die Ressource ist verfügbar, hat aber keine weitere Kapazität für zusätzliche Dienste.

Stallings [Stal99] hält im Configuration Management noch die mögliche einsatzbedingte unterschiedliche Verwendung ein und derselben Ressource für relevant.

Accounting Management

Accounting Management misst die Verwendung von Netzwerkressourcen mit dem Zweck die Kosten und die Ressourcen zu verteilen.

[ITU-T X.700] Accounting Management Funktionen:

- Informieren der Benutzer über angefallene Kosten und die konsumierten Ressourcen
- Buchungslimits und Tariflisten bezogen auf die Konsumation der Ressourcen
- Gruppierung von Ressourcen für eine Sammelabrechnung

Accounting Management ist vor allem für Telekommunikationsunternehmen, Rechenzentren, etc. relevant. Die Thematik ist jedem Eigentümer eines Mobiltelefons, Festnetztelefons oder jedem Kunden eines Internetserviceproviders hinreichend bekannt.

Die Thematik Accounting Management spielt bei den Untersuchungen dieser Arbeit eine untergeordnete Rolle.

Performance Management

Die Leistungsfähigkeit die Anforderungen vieler Benutzer zufriedenzustellen bestimmt die Performance eines Netzwerkes. Performance Management befasst sich somit mit dem Durchsatz, der prozentueller Auslastung, der Fehlerrate und den Antwortzeiten des Netzwerkes.

Die Netzwerk Management Standards wurden mit Fokus auf Netzwerkverbindungen und Datenleitungen definiert. Im modernen Netzwerk Management werden die Standards etwas weitergehend interpretiert. Die Überwachung der Auslastung, Messung des Durchsatzes und der Antwortzeiten zur statistischen Analyse lassen sich sehr gut allgemein auf andere Systeme, wie beispielsweise Webserver anwenden.

Performance Management Funktionen nach [ITU-T X.700]:

- Sammeln von statistischen Informationen.
- Führen und Untersuchen der Statusinformationen in den Log Dateien.
- Untersuchen der Systemperformance unter realen und theoretischen Bedingungen.
- Wechseln des Betriebsmodus zum Zwecke der Performance Management Aktivitäten.

Die Aufgabe und das Ziel des Netzwerk Management ist es dem Benutzer des vernetzten Systems alle erforderlichen Ressourcen zuverlässig und in ausreichendem Maße zur Verfügung zu stellen. Über die im Fault Management erhobenen Daten können Kennzahlen ermittelt werden um die Ziele zu überprüfen.

In der Prozessautomatisierung [Schi98] wird die Verfügbarkeit V eines Automatisierungssystems definiert:

$$V = \frac{MTBF}{MTBF + MTTR}$$

Die mittlere Zeit zwischen zwei Ausfällen (Mean Time Between Failure MTBF) wird in Relation gestellt mit der mittleren Reparaturzeit (Mean Time To Repair). Die Zeiten können leicht aus den Logdateien des Netzwerk Management Systems gewonnen werden.

Die Verfügbarkeit und die MTBF messen die Zuverlässigkeit einzelner Komponenten oder des gesamten Systems.

Die MTTR ist eine Performance Wert für das Management des gesamten Systems, wie lange benötigt das Team um Fehler zu beheben, bzw. um ein Ticket zu erledigen.

Schwieriger festzustellen ist jedoch der wohl wichtigste Punkt. Wie viele Probleme und Ausfälle sind durch rechtzeitige Maßnahmen im Netzwerk Management ohne Auswirkungen behoben oder verhindert worden.

Die Untersuchung der Systemperformance unter realen Bedingungen ist ein sehr komplexes Unterfangen. Moderne Systeme beispielsweise die Steuerung einer Produktionsanlage sind selbst sehr komplex und sehr viele Komponenten benutzen diese Systeme und erzeugen somit Last. Für eine reale Lastsimulation müsste die Produktion selbst unter maximaler Auslastung laufen zum Test laufen. Das ist ein sehr teures Unterfangen. Eine große Webseite oder ein großer Webshop wird von sehr vielen Benutzern gleichzeitig verwendet. Jeder Benutzer legt ein individuelles Verhalten an. Auf eine Untersuchung unter realen Bedingungen wird in der Regel verzichtet und es wird versucht mit Simulationen möglichst Nahe an reale Bedingungen heranzukommen. Diese Simulationen werden als Testläufe in Laborumgebungen durchgeführt. Nach der erfolgreichen Simulation und erfolgreichen Test kann das System in den Produktionsbetrieb übernommen werden.

Security Management

Security Management ist lt. Definition ein Prozess. Dieser Prozess kontrolliert den Zugriff auf Netzwerkressourcen mit Authentifizierung, Verschlüsselung, Berechtigungsregeln, Firewalls und Einbruchserkennung. Diese Mechanismen beschränken den Zugriff auf Rechner, Netzwerkgeräte, Dateien und Programme abhängig vom User und dessen Zugang. Außerdem informieren sie über Versuche diese zu brechen.

Security Management Funktionen aus [ITU-T X.700]:

- Anlegen, Kontrollieren und Löschen von Sicherheitsservices und -mechanismen.
- Verteilen von sicherheitsrelevanten Informationen.
- Reporting von sicherheitsrelevanten Ereignissen.

In der modernen vernetzten Welt ist Security Management ein sehr zentrales und wichtiges Thema. Im speziellen ist die Thematik bei Internet basierten Diensten von Bedeutung. Die Anzahl der sicherheitssensiblen Applikationen, wie Internetbanking, Austausch von Patientendaten, E-Government, … im World Wide Web ist ständig im steigen. Zugleich steigen auch die Attacken gegen diese. Aktuelle Fortschritte in der sicheren Quantenkryptographie lassen hoffen. Leider ist das Bewusstsein der User im Umgang mit Daten nicht immer ausreichend.

Die Thematik Security Management spielt bei den Untersuchungen dieser Arbeit eine untergeordnete Rolle.

2.2 Facility Management

Sucht man facilities in einem Englisch-Deutsch Wörterbuch, so findet man:

Anlagen, Betriebsanlagen, Einrichtungen, Werkstätten, technische Hilfsmittel und Gerätschaften, Toiletten, Gebäude.

Offensichtlich befasst sich Facility Management mit einer Reihe von Ressourcen. Diese Ressourcen sind das Gebäude selbst das Grundstück worauf es steht und alle Einrichtungen innerhalb.

„*Facility Management ist ein ganzheitliches Management der Immobilien und der materiellen/immateriellen Infrastruktur einer Organisation mit dem Ziel der Verbesserung der Produktivität des Kerngeschäfts.*“ [ÖNORM A7000]

In der [ÖNORM A7000] wird das Facility Management in 3 Gruppen dargestellt:

- Management des Gebäudes
  Energie, Reinigung, Bautechnik, Abfallwirtschaft, Gebäudesicherheit, Betrieb & Instandhaltung

- Management der Immobilie
  Gebäudekostenverrechnung, Gebäudeverwaltung, Steuern & Abgaben, Finanzierung, Versicherungen, Mitabrechnung, Immobilienentwicklung

- Management weiterer Facility Services
  Kopie, Catering, Inventar, Fuhrpark, Post Service, Reiseorganisation, Informationstechnologie, Gesundheit & Sicherheit, Umzugsmanagement

Die German Facility Management Association (GEFMA) definiert Facility Management.

"*Facility Management ist ein unternehmerischer Prozess, der durch die Integration von Planung, Kontrolle und Bewirtschaftung bei Gebäuden, Anlagen und Einrichtungen (facilities) und unter Berücksichtigung von Arbeitsplatz und Arbeitsumfeld ein verbesserte Nutzungsflexibilität, Arbeitsproduktivität und Kapitalrentabilität zum Ziel hat. 'Facilities' werden als strategische Ressourcen in den unternehmerischen Gesamtprozess integriert*." [GEFMA 100]

2.2.1 Die 3 Säulen des Facility Management

Es gibt eine Reihe von Definitionen zu dem Begriff Facility Management. Interpretiert man diese Definitionen gleichartig so erkennt man zu den 3 Säulen des Facility Management wie sie Jens Nävy in [Nävy06] darstellt:

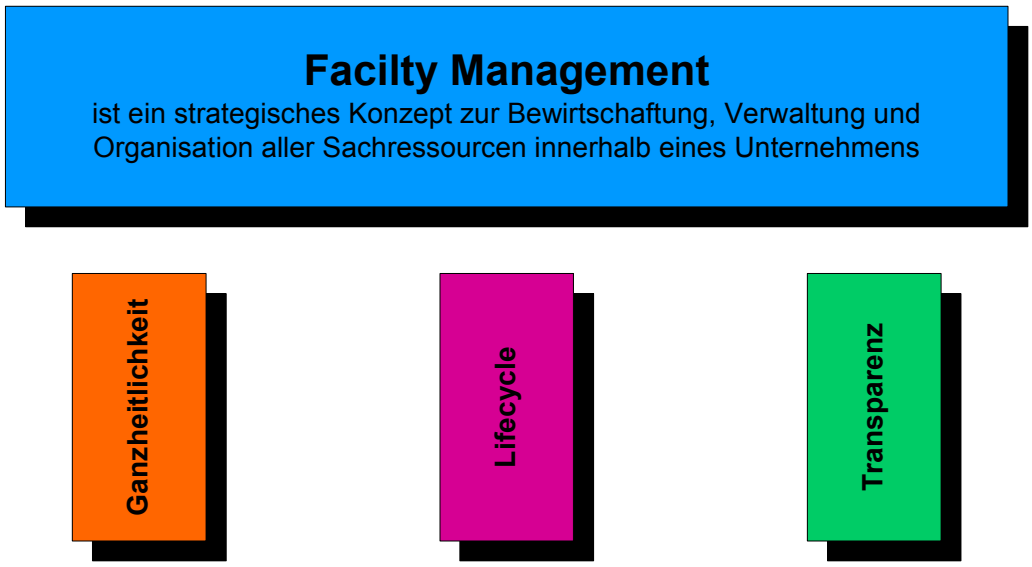


Abbildung 10 [Nävy06] Die drei Säulen das Facility Management

Ganzheitlichkeit

Die ganzheitliche Betrachtungsweise stellt die Sachressource in den Mittelpunkt. Einzelne Abteilung haben unterschiedliche Sichtweisen. Facility Management vereinigt alle in einem umfassenden beschreibenden Datenmodell. Ziel ist es alle Sachressourcen in die Bewirtschaftung einzubeziehen. Die Sachressourcen umfassen alle materielle und immaterielle Objekte. Facility Management ist ein prozessorientierter Ansatz. Die Aktivitäten sind als Geschäftsprozesse abteilungsübergreifend in die Organisation eingebunden.

Lebenszyklus

Der Lebenszyklus eines Gebäudes kann in 5 Phasen unterteilt werden. Die 5 Phasen sind die Konzeption, die Planung, der Bau, die Nutzung und die Verwertung.

Die [ÖNORM A7000] sieht das Facility Management, von Beginn an ganzheitlich den Zusammenhang einzelner Lebenszyklusphasen eines Objektes insbesondere in Sinne der Kosten-Nutzen-Betrachtung koordinierend. So betragen bei den Lebenszykluskosten die Nutzungskosten ein Vielfaches der reinen Errichtungskosten. Diese Nutzungskosten werden großteils im Zuge der Konzeption und Planung vorbestimmt.

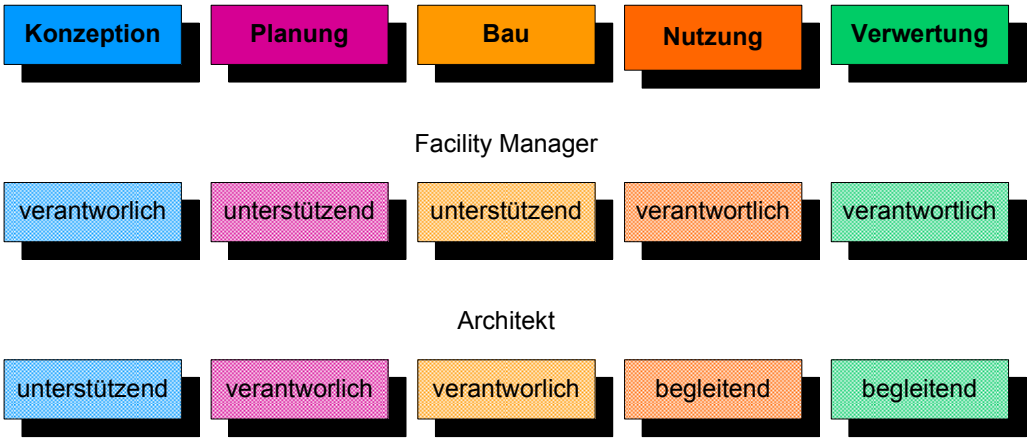


Abbildung 11 [Nävy06] Verantwortung für ein Gebäude in den einzelnen Phasen

Die Verantwortungen in den einzelnen Phasen wechseln. So über nimmt der Facility Manager in den Phasen Konzeption, Nutzung und Verwertung die Hauptverantwortung. Der Manager kann in der für die gesamten Kosten wichtigen Phase der Konzeption seine Verantwortungen in den späteren Phasen Nutzung und Verwertung hinsichtlich der Kosten beeinflussen. Der Architekt übernimmt kompetenzbedingt die Verantwortung in der Planungs- und Bauphase.

Transparenz

Für die Bewirtschaftung von Sachressource benötigt man komplette und genaue Daten für die Entscheidungen die getroffen werden müssen. Das Bereitstellen dieser Informationen in eine zentrale Forderung im Facility Management. Diese umfassende Datenbasis bewirkt Transparenz über das gesamte Anlagevermögen.

2.2.2 Computer Aided Facility Management

Jens Nävy definiert in [Nävy06]:

„Das Begriff Computer Aided Facility Management (CAFM) steht für computergestütztes Facility Management. CAFM ist also ein Werkzeug für das Facility Management. CAFM-Systeme werden zur integrierten und informationstechnischen Unterstützung der Aufgaben im Rahmen von Facility Management-Prozessen eingesetzt.“

Ein CAFM System begleitet das Facility Management in allen Phasen des Lebenszyklus der Facilities. Auf Grund der wechselnden Gesamtverantwortlichen in den Phasen ändern sich auch die Benutzer des Systems. Die Datenhaltung im System wird gemeinsam genutzt, sie soll redundanzfrei sein.

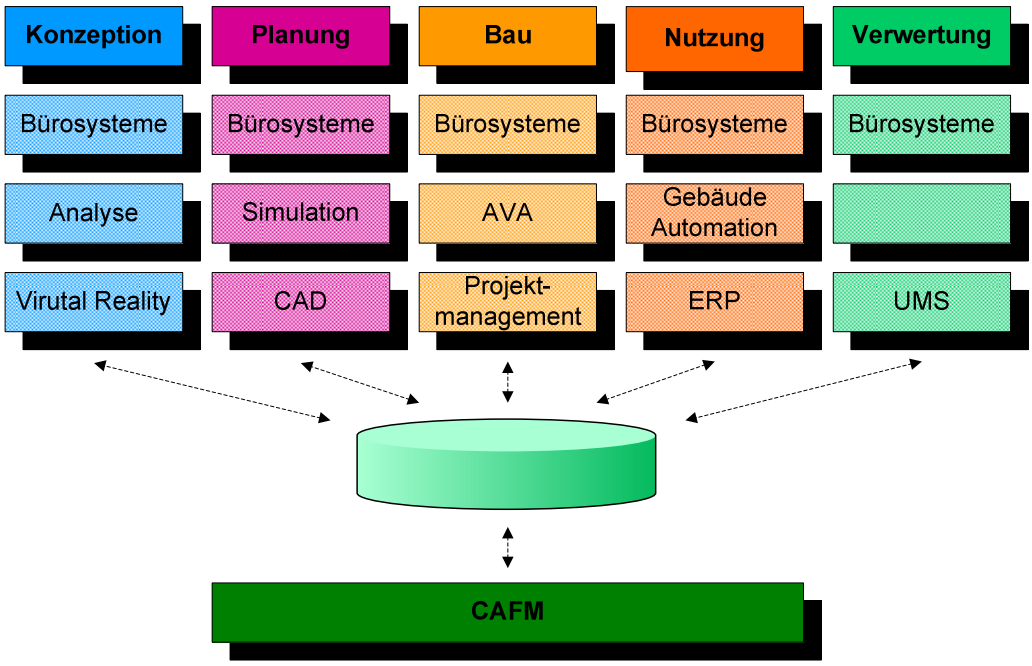


Abbildung 12 IT-Werkzeuge während des Lebenszyklus

In der Abbildung 12 IT-Werkzeuge während des Lebenszyklus erkennt man viele einzelne Softwarewerkzeuge. Diese bleiben selbstverständlich bestehen, jede Phase hat andere Anforderungen und andere Werkzeuge. Man erkennt aber die einheitliche Datenbasis.

2.2.3 Gebäudemanagement

Die Deutsch Industrie Norm [DIN 32736] Gebäudemanagement und Begriffe und Leistungen definiert den Begriff Gebäudemanagement als:

„Gesamtheit aller Leistungen zum Betreiben und Bewirtschaften von Gebäuden einschließlich der baulichen und technischen Anlagen auf der Grundlage ganzheitlicher Strategien. Dazu gehören auch infrastrukturelle und kaufmännische Leistungen.“ [DIN 32736]

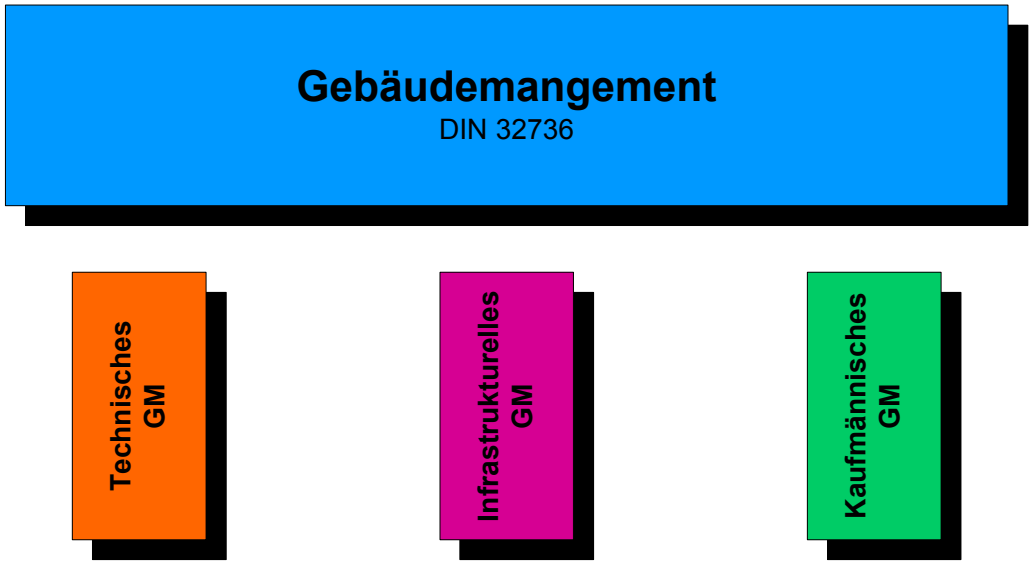


Abbildung 13 [DIN 32736] Leistungsbereiche des Gebäudemanagements

Technisches Gebäudemanagement

Es umfasst alle Leistungen, die zum betreiben und bewirtschaften der baulichen und technischen Anlagen eines Gebäudes erforderlich sind. Diese Leistungen sind nach [DIN 32736]:

- Betreiben
- Dokumentieren
- Energiemanagement
- Informationsmanagement
- Modernisieren
- Sanieren
- Umbauen
- Verfolgen der technischen Gewährleistung

Infrastrukturelles Gebäudemanagement

Es umfasst die geschäftsunterstützenden Dienstleistungen, welche die Nutzung von Gebäuden verbessern. Ein Auszug der Leistungen nach [DIN 32736] sind:

- Datenverarbeitungsdienste
- Interne Postdienste
- Kopier- und Druckereidienste
- Parkraumbetreiberdienste
- Reinigungsdienste
- Sicherheitsdienste
- Winterdienste
- Zentrale Kommunikationsdienste

Kaufmännisches Gebäudemanagement

Es umfasst alle kaufmännischen Leistungen aus den Bereichen Technisches Gebäudemanagement und Infrastrukturelles Gebäudemanagement unter Beachtung der Immobilien Ökonomie. Die Leistungen nach [DIN 32736] sind:

- Beschaffungsmanagement
- Kostenplanung und Kostenkontrolle
- Objektbuchhaltung
- Vertragsmanagement

Kapitel 3

Network Management in Facility Management

Netzwerk Management und Facility Management haben nicht nur den zweiten Teil ihres Namens gemeinsam. Beiden ist das Ziel gemeinsam:

- Ziel ist es die Betriebskosten zu senken, die technische Verfügbarkeit der Anlage zu sichern.

Im Facility Management ist ein weiteres Ziel: der langfristige Werterhalt von Gebäuden und Anlagen. Dieses Ziel lässt sich auf die IT-Branche nicht umsetzten. Die zu managenden Dinge sind schon von Ihrer Art zu unterschiedlich. Ein Gebäude wird für einen Zeitraum in der Größe von Jahrzehnten bis zur Ewigkeit, wenn man den Zweck und die Idee der Pyramiden bedenkt, errichtet. Ein Netzwerk und dessen Computersysteme werden nur für einen Zeitraum von wenigen Jahren geplant. Die IT-Branche ist zu jung und zu schnelllebig. Ein in die Jahre gekommener Computer ist wenn auch noch so schön völlig wertlos. Maximal ein Museum wird vielleicht Interesse haben, wenn es sich um ein Einzelstück handelt. Eine Jugendstilvilla, gut gepflegt und gehegt ist wohl heut mehr wert als bei der Errichtung.

Das gemeinsame Ziel ist also eine hohe Verfügbarkeit und geringe Kosten. Im Facility Management hat die Konzeption und Planung einen sehr wesentlichen Einfluss auf die Betriebkosten in der Nutzungsphase des Lebenszyklus.

Hier stößt man auf einen wesentlichen Unterschied der beiden Managementthemen. Aus Management sicht muss man alle Phasen der zu managenden Ressource betrachten. Das gilt sowohl für das Netzwerk Management als auch für das Facility

Management. Im Netzwerk Management Die Standards der ISO, die auch die Grundlage für die Untersuchung der Network Management Techniques in Facility Management, lassen die Konzeption, Planung und Aufbau außen vor. Netzwerk Management wird als Lieferant von Informationen, die die Grundlage für die Konzeption und Planung sind, gesehen.

Facility Management hingegen wird als ganzheitliches Management verstanden. Es berücksichtigt alle Phasen des Lebenszyklus einer Ressource. Es startet mit der Idee, der Konzeption und endet im Abriss, der Verwertung.

Die Tatsache, dass das Facility Management in der Regel als Gebäudemanagement missverstanden wird, Gebäudemanagement sich nur der Phase der Nutzung widmet und die Standards im Netzwerkmanagement ebenfalls nur die Nutzungsphase eines Netzwerkes und dessen Ressourcen behandelt, legt nahe diese Betrachtung der Network Management Techniques in Facility Management ebenfalls auf das Gebäudemanagement und die Nutzungsphase zu beschränken.

In der Literatur des Facility Management findet man ab und an die Thematik Netzwerk Management erwähnt. In der Regel wird das Netzwerk Management als Teil des Facility Management im Bereich des Infrastrukturellen Gebäudemanagements bei den Datenverarbeitungs-Diensten beschrieben. Jens Nävy sieht in [Nävy06] Netzwerk Management als ein CAFM-System und es unterstützt so das Facility Management. Es wird in der gleichen Kategorie, Aktive Systeme, wie die Gebäudeautomation genannt.

Wie Network Management Techniques aber als Techniken im Facility Management hilfreich sein können wurde bisher noch nicht untersucht. Die fünf Funktional Areas des OSI Management sollen in den drei Säulen des Gebäudemanagement verwendet werden.

3.1 Network Management im Technischen Gebäudemanagement

Betreiben ist die erste genannte Leistung im Technischen Gebäudemanagement. Das Betreiben eines Netzwerkes ist die ureigentlichste Aufgabe des Netzwerk Managements. Überwachen, Instandhalten, Beheben von Störungen ist klassisches Fault Management. Außerbetriebnehmen, Inbetriebnehmen und Wiederinbetriebnehmen ist klassisches Configuration Management.

Dokumentieren wird in der [DIN 32736] als die erforderliche Erfassung, Speicherung und Fortschreibung aller Daten und Informationen wie Verbrauchsdaten, Betriebsprotokolle, Wartungsprotokolle beschrieben. Die Forderung der Erfassung, Speicherung und Fortschreibung der Daten ist im Fault Management definiert und kann hier eingesetzt werden. Betriebs und Wartungsprotokolle können aus den gespeicherten Informationen des Ticketsystems ebenfalls aus dem Fault Management generiert werden, wenn Wartungsaktivitäten als Ticket erfasst werden.

Das Energiemanagement beinhaltet unter anderen die Leistungen Analyse des Energieverbrauchs und das Nachweisen der Einsparungen. In der Analyse des Energieverbrauchs kann über Messungen aus dem Fault Management der Verbrauch festgestellt werden. Das Performance Management kann die Einsparungen durch Reports und Grafiken nachweisen.

Zum Informationsmanagement gehören die Leistungen Erfassen, Auswerten, Weiterleiten und Verknüpfen von Informationen und Meldungen. Erfassen, Auswerten und Weiterleiten von Informationen sind Aufgaben aus dem Fault Management. Erfasst werden Daten über Poll-driven Management oder Event-driven Management, bewertet werden die Daten über Thresholds und weitergeleitet als Nachricht im Alarmsystem.

Für die Themen Modernisieren, Sanieren und Umbauen hat das Netzwerk Management nicht direkt Konzepte. Indirekt können aber die gewonnen Informationen aus dem Fault Management und dem Performance Management die Grundlage für Entscheidungen sein. Wo bzw. welche Systeme sollen modernisiert, weil zu wenig performant, werden. Saniert muss werden, weil zu viele Fehler, die Mean Time Between Failure ist zu gering, auftreten.

Das Verfolgen der Gewährleistung kann einfach durch ein Attribut Ende der Gewährleistungsfrist, das mit dem Managed Object gespeichert wird ermöglicht werden. Tritt ein Fehler auf wird automatisch überprüft ob das defekte Geräte noch in Gewährleistung ist. Das ist eine übliche Vorgehensweise in der Praxis des Netzwerk Management.

3.2 Network Management im Infrastrukturellen Gebäudemanagement

Der Einsatz von Netzwerkmanagement in den Datenverarbeitungs-Diensten wird in der Literatur zum Facility Management oft genannt. Das Netzwerk Management kommt aus der EDV.

Die Internen Postdienste werden soweit sie elektronische möglich sein in der Regel per Email erledigt. Email ist ein Dienst der Datenverarbeitung und dort wird auch Netzwerk Management betrieben. Für nicht elektronische Post würde sich anbieten die Kuverts mit RFID Chips zu versehen und bei den Postein- und Postausgangstellen der Abteilungen Sensoren zu installieren. Kommt ein RFID Kuvert in der Empfangsbereich eines Sensors sendet dieser über Event-driven Management, einem Kommunikationsaspekt aus dem Fault Management, die Ortsbezeichnung an der sich die Post gerade befindet. So kann die jederzeit der Ort einer Sendung festgestellt werden.

Die Geräte der Kopier- und Druckereidienste werden üblicherweise von den EDV-Abteilungen betrieben und sind daher im über das Netzwerk Management überwacht.

Parkraumbetreiberdienste, eine sehr gute Anwendungsmöglichkeit für das Accounting Management. Über die Mechanismen im Accounting Management kann eine Abrechung der benutzten Parkplätze realisiert werden. Über eine Kennzeichenerkennung in den Ein- und Ausfahrten wird über Techniken aus dem Security Management die Zufahrt erlaubt oder verweigert und gleichzeitig die Zeiten und das Kennzeichen für eine Abrechnung per Event-driven Management an das Accounting Management gemeldet.

Sicherheitsdienste: Zutrittskontrollen fallen in den Bereich des Security Managements. Die Objektüberwachung übernehmen Alarmsysteme die über das Fault Management überwacht werden. Stellt eine Alarmanlage einen unerlaubten Zutritt fest kann über das Alarmsystem des Fault Management das

Sicherheitspersonal alarmiert werden. Die vorgeschriebenen Reaktionszeiten können über die Techniken aus dem Performance Management kontrolliert werden.

Fällt die Temperatur unter einen bestimmten Schwellenwert alarmiert das Fault Management das zuständige Personal.

3.3 Network Management im Kaufmännischen Gebäudemanagement

Network Management Techniques lassen sich im Beschaffungsmanagement, dem Vertragsmanagement und bei der Kostenplanung nicht einsetzen.

Accounting Management Techniques sind jedoch gut in der Objektbuchhaltung einsetzen. Mieten beispielsweise lassen sich gut im Accounting Management abrechnen.

Kapitel 4

Praktische Umsetzung mit Nagios im Projekt HHSC

4.1 HHSC

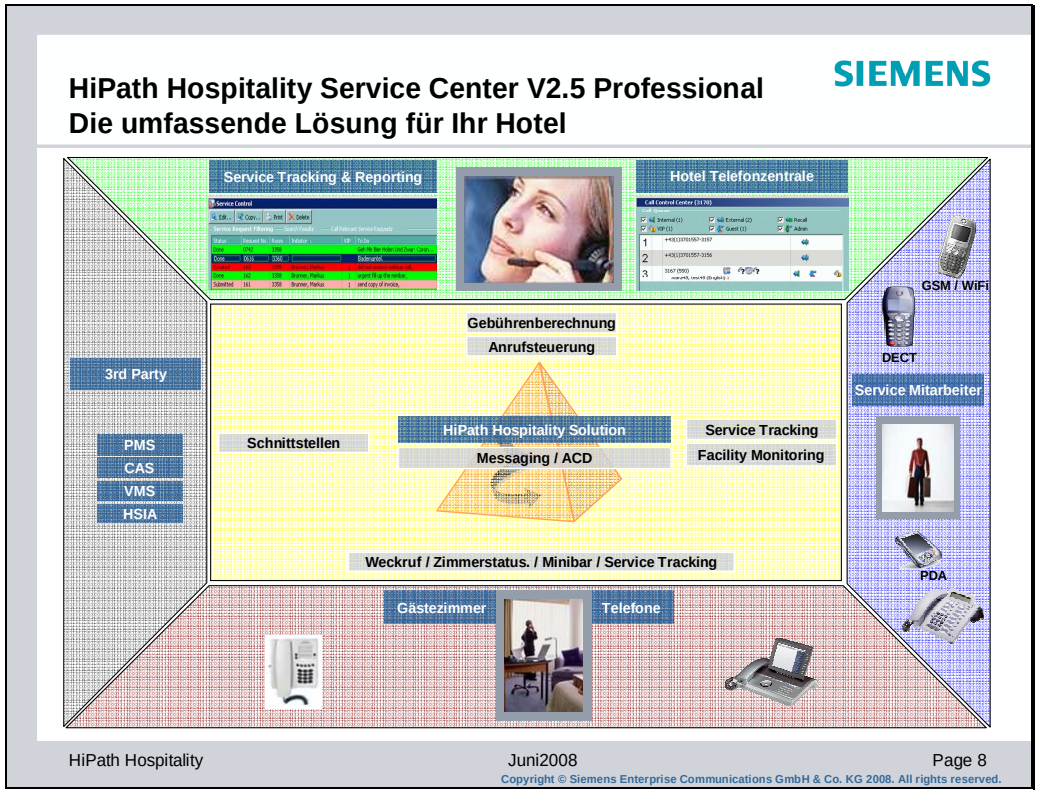


Abbildung 14 [Asch08] HHSC Übersicht

HiPath Hospitality Service Center (HHSC) ist eine Client/Server-Applikation für das Hotelgewerbe. Es kombiniert die Kommunikationsmöglichkeiten von Siemens HiPath-IP-Systemen mit einem Paket von Hotel-Service-Anwendungen und bietet auch Schnittstellen zu:

- Hotel Property Management Systems (PMS)
- Call Accounting Systems
- Gebäudemanagement (Facility Management)
- Voice Mail Systems (VMS)
- etc.

HHSC unterstützt die Telefoniefunktionen in Hotels und nutzt die Integrationsmöglichkeiten von zentralen Datenquellen. Das System bietet eine Vielzahl von Funktionen für Beherbergungsbetriebe:

- Definition und Verfolgung von Service-Aufträgen
- Anrufsteuerungszentrale
- Management von Kundenbeziehungen

HHSC ist sowohl für mittlere und große Hotels als auch für Hotelketten konzipiert. Es unterstützt den Front Office Client als Personal Computer (PC) Applikation, die Personal Digital Assistant (PDA)- oder Laptop-Konsole für Gäste und PDAs für Hotelangestellte. Die Hotelbelegschaft kann anstelle eines PDA auch ein Cordless Multicell Integration (CMI), auch bekannt als Digital Enhanced Cordless Telecommunications (DECT), bzw. tragbares Schnurlostelefon oder ein Siemens Optiset-Tischtelefon benutzen.

Die Benutzer in der Rezeption arbeiten mit dem HHSC Front Office Client und sind verantwortlich für die Anrufsteuerung (mittels HHSC Call Control) und die Erfassung und Weiterleitung von Service-Aufträgen (mittels HHSC Service Tracking) sowie über ein Hotel Property Management Systems (PMS) für das Ein- und Auschecken von Hotelgästen, das Vormerken von Reservierungen und die Ausfertigung der Rechnungen.

Die Service-Mitarbeiter, die PDAs, CMI- oder Optiset-Telefone benutzen, nehmen Service-Aufträge entgegen und führen die Aufträge, für die sie verantwortlich sind, aus und bestätigen sie.

Speicher Programmierbare Steuerungen (SPS) sind über das gesamte Hotel verteilt und sammeln Informationen über den Status über die an den Eingängen angeschlossenen Sensoren. Diese SPS Boxen sind über eine Ethernetschnittstelle am Netzwerk angeschlossen. Das Facility Management sammelt die Statusinformationen ein und präsentiert den Status im Front Office Client und meldet Probleme über den Messagehandler an die Service Mitarbeiter als Alarm oder per Ticket über das Service Tracking.

4.1.1 HHSC Facility Management

Das HHSC Facility Management ist die Praktische Umsetzung von Netzwerk Management Technologies im Bereich Facility Management. Das Modul wird detailliert im Kapitel Praktische Umsetzung mit Nagios im Projekt HHSC beschrieben.

4.1.2 HHSC Call Control

Die eigentliche Aufgabe des HiPath Hospitality Service Center ist es eine Schnittstelle zwischen dem Switch, der Telefonanlage und Front Office-System ist einem Hotel zu bilden. Der zentrale Schirm für das Personal in der Rezeption und/oder Vermittlung ist daher das Call Control oder das Anrufsteuerungszentrale Fenster.

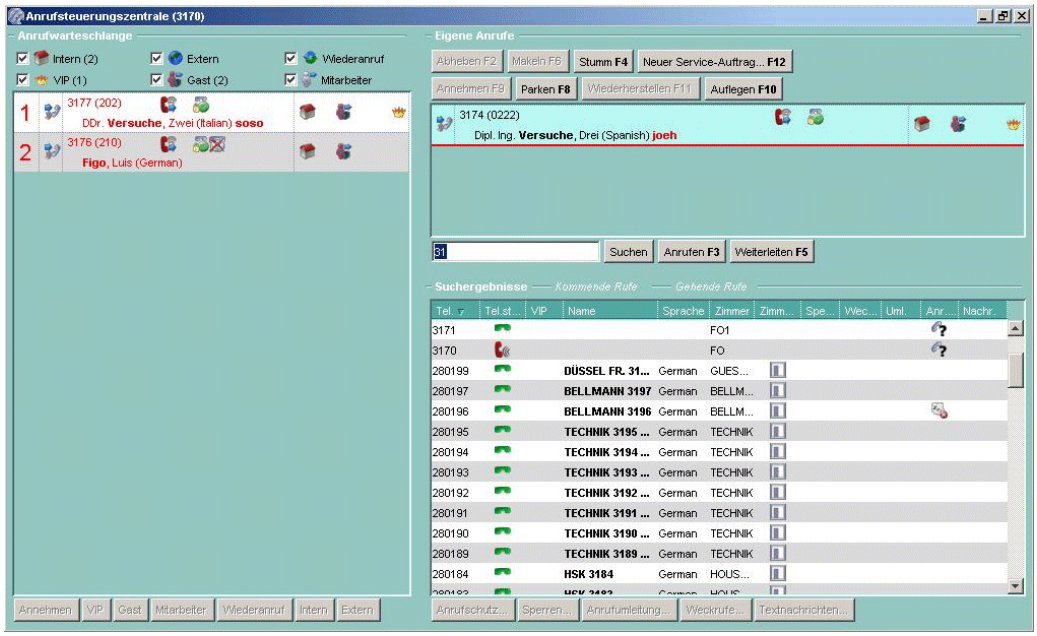


Abbildung 15 [HHSC-B] Anrufsteuerungszentrale mit Anrufwarteschlange

In der Anrufsteuerungszentrale kann der Benutzer Anrufe beantworten, den aktuellen Anrufer stumm schalten, weiter verbinden, zwischen Anrufen hin- und herschalten oder einen neuen Service Auftrag für einen Gast initiieren. In den Suchergebnissen werden Details zu den Nebenstellen, bzw. Gästen aus der Datenbank angezeigt.

4.1.3 HHSC Interface

Das HHSC Interface ist die Schnittstelle zu einer Reihe von Property-Management-Systemen. Über diese Schnittstelle werden Informationen zwischen den Systemen ausgetauscht. Gast-Daten werden in dem Property-Management-System erfasst und an HHSC übertragen, ebenfalls Check-In und Check-Out Daten, etc. HHSC hingegen versorgt das PMS mit Telefongebühren, Internetgebühren, usw.

Diese Abrechnungsdaten sind für die Accounting Management Thematik relevant.

4.1.4 HHSC Service Tracking

Abbildung 16 [Asch08] HHSC Service Tracking

Mit der Service-Auftragsverfolgung können Serviceanfragen von Hotelgästen, automatisch generierte Tickets aus dem Facility Management aber auch administrative Arbeitsanweisungen erfasst und als Service-Aufträge an das zuständige Service-Personal weitergeleitet werden.

Der Fortschritt bei der Erledigung eines Service-Auftrags lässt sich zentral verfolgen, und der Grad der Zufriedenheit des Gastes mit der Erledigung kann erfasst werden.

Im Nachhinein lassen sich durch Erzeugung spezieller Arbeitsauftragslisten oder anderer Reports statistische Auswertungen und Detailstudien bzgl. der ausgeführten Aufträge vornehmen.

Das Service Tracking wird als Ticket System für das Facility Management eingesetzt.

4.1.5 Arbeitsauftragslisten

HHSC bietet Berichte über bestimmte Arbeitsabläufe und Tätigkeiten. Es werden Berichte bzgl. Service-Aufträgen und Weckrufen in Listenform angeboten.

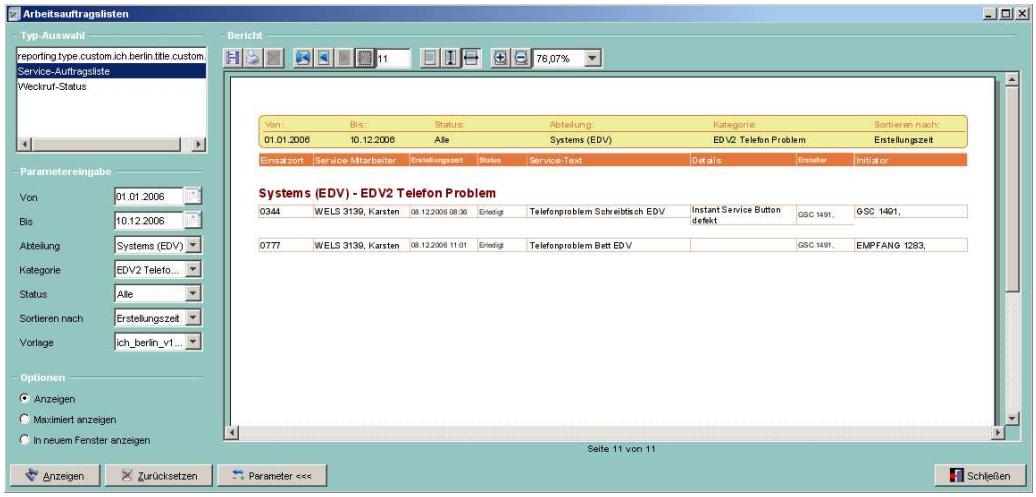


Abbildung 17 HHSC Arbeitsauftragslisten

Hier ein Beispiel zu den Service Auftragslisten.

Das Konzept von HHSC sieht aber auch das Einbringen individuell gestalteter Arbeitsauftragslisten vor. Solche Listen werden über XML-Dateien und Vorlagen definiert. Die Arbeitsauftragslisten werden aus der Datenbank live generiert. Sie dienen daher zur Übersicht und sind nicht für statistische Auswertungen wie im Performance Management verlang vorgesehen. Für diesen Zweck steht das Management Information System zur Verfügung. Die Daten für dafür werden in einem Batch-Job aufbereitet und in einer extra Datenbank gespeichert.

4.1.6 Management Informations System

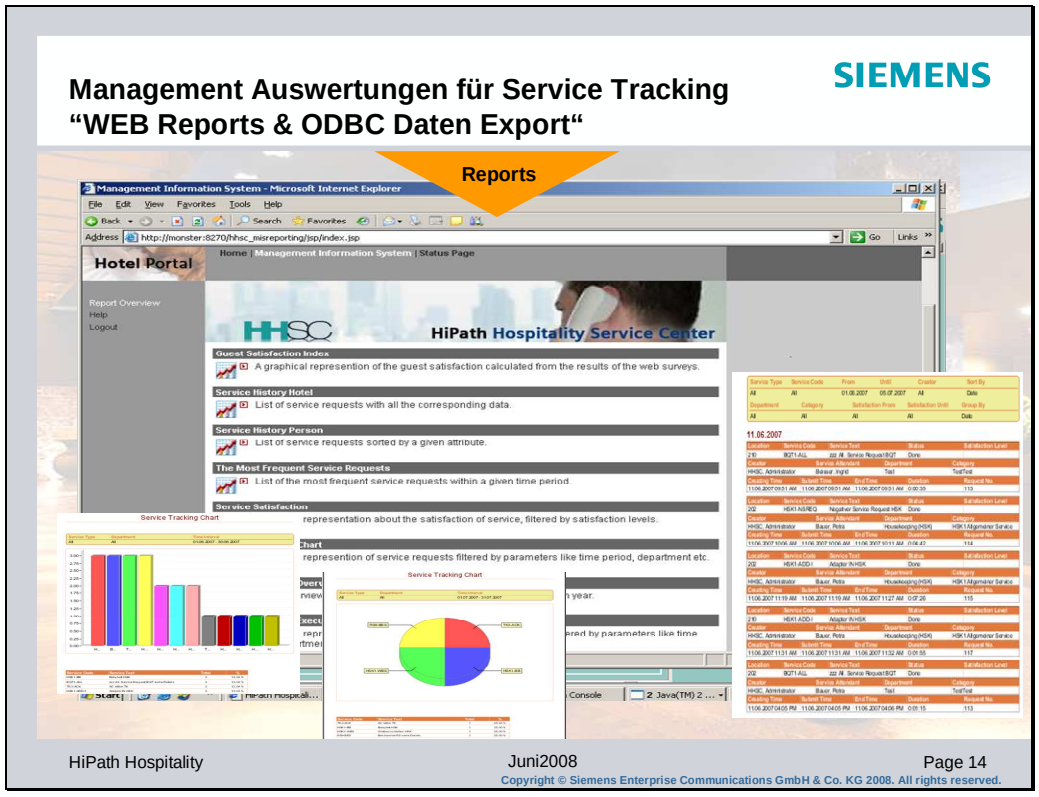


Abbildung 18 [Asch08] HHSC Management Information System

Das Management-Informations-System ist ein Werkzeug, das Informationen bereit stellt, die für Planungen und Entscheidungen im Hotel-Management hilfreich sind. Das Management-Informations-System gibt im Wesentlichen Auskunft zu den Aufträgen, die automatisch erstellt oder im Hotel angefordert und erledigt worden sind. Das Konzept von HHSC sieht aber auch das Einbringen individuell gestalteter Auswertungen vor, wenn solche erforderlich sind. Solche Auswertungen werden über XML-Dateien und Vorlagen definiert.

Damit die bei der Erstellung von MIS-Auswertungen erforderlichen Berechnungen stets auf einem konsistenten Datenbestand basieren, wird für diese Berechnungen nicht der gerade aktuelle Inhalt der HHSC-Datenbank, sondern ein von der HHSC-Datenbank völlig unabhängiges "Abbild" dieser Datenbank herangezogen. Diese MIS-spezifische Datenbank wird von MIS in regelmäßigen Zeitabständen produziert: Zum ersten Mal automatisch beim Start des HHSC Systems auf dem Server, danach zyklisch in festzulegenden Zeitintervallen Mit Hilfe des jeweils neuesten Abbilds führt das Management-Informations-System vorab auch gleich die (mitunter zeitaufwändigen) Berechnungen durch, die bei der Erstellung von

Auswertungen erforderlich sind, und hinterlegt die Ergebnisse in dem Abbild; dadurch kann bei der eigentlichen Erstellung von Auswertungen auf die bereits fertig aufbereiteten Daten zugegriffen und eine komplexe Kalkulation vermieden werden, was das Zeitverhalten verbessert.

Das Management Informations System deckt einige der in der Functional Area Performance Management definierten Funktionen. Die Datenbank der MIS Systems speichert generierte und gesammelte statistische Informationen. Das System kann auch auf historischen Statusinformationen aus dem Nagios zugreifen.

4.1.7 HHSC Maintenance GUI

Für administrative Zwecke steht im HHSC eine getrennte Maintenance GUI am Server zur Verfügung. Dieses Tool ist ermöglicht die technische und logische Konfiguration des Softwaresystems in einer grafischen Oberfläche. Das Programm dient außerdem auch zur Wartung und Fehleranalyse. Es ermöglicht die Definition von Traces durch die Kombination bestimmter und definierbarer Trace-Themen und die Aktivierung dieser Traces im Fehlerfall.

Das führen und analysieren von Logdateien ist eine Forderung im Network Management, im speziellen im Fault und Performance Management.

4.2 Nagios

Die Netzwerküberwachungssoftware Nagios liegt mittlerweile in der Version 3 vor. Das in der Programmiersprache C implementierte Open Source Projekt wurde 1999 unter dem Namen Netsaint von Ethan Galstad gestartet. Die Zielplattform ist Linux. Diese Arbeit basiert auf der Version 2, welche zu Beginn dieser Arbeit aktuell war. Nach der Unix Philosophie setzt sich das Paket aus vielen Teilprogrammen zusammen. Der Hauptteil ist der Nagios Core, ein Webinterface stellt die gesammelten Informationen im Browser übersichtlich dar, viele Plugins sammeln Informationen und etliche Addons wie der Nagios Remote Plugin Executor, NRPE oder der Nagios Service Check Acceptor, NSCA ermöglichen verteiltes Überwachen und vieles mehr.

Die Kernkompemente, in der Dokumentation als Nagios Process oder Core Logic bezeichnet, ist der zentrale Prozess. Er sammelt Informationen über den Zustand der Manged Objects mit Hilfe von Plugins, bereitet die Daten auf und schreibt sie in Logdateien nieder. Wenn er ein Problem erkennt, sendet der zentrale Prozess eine Nachricht an die zuständigen Administratoren.

Das Webinterface und seine CGI-Skripte lesen die gesammelten Informationen aus den Files aus uns stellen sie übersichtlich dar.

Über eine Named Pipe, genannt External Command File lassen sich zusätzliche Kommandos an den Nagios-Prozess senden. Diese Schnittstelle nutzt auch das Webinterface: Es schreibt Befehle in die Pipe-Datei, Nagios liest sie und führt sie aus.

Der Nagios-Prozess wird über Textdateien konfiguriert.

Die Anforderungen für HHSC machen viele weitreichenden Änderungen an dem Nagios Core notwendig. So wurden die Konfigurations- und Log-Dateien durch eine Datenbank ersetzt, ebenso neben dem External Command File eine eigene Tabelle für die externen Befehle eingeführt. Die Präsentation der Status der Manged Objects erfolgt in der GUI in Echtzeit, ebenso die Konfiguration über eine AdministrationsOberfläche. Außerdem wurde eine große Schwachstelle im Nagios, der Status der beobachteten Objekte wurde bisher nur im RAM, random access memory, gehalten und nur in regelmäßigen Abständen in ein Status File gesichert, zusätzlich mit jedem Neustart ebenfalls. Jede Änderung an der Konfiguration erfordert eine Neustart des Core Prozesses. Jede Statusänderung wird jetzt sofort mit

der Datenbankschnittstelle in die Datenbank geschrieben. Diese ist daher persistent synchron mit dem im Speicher gehaltenem Status. Auch die Managed Object wurden für die Anforderungen erweitert.

4.2.1 Managed Objects

Host

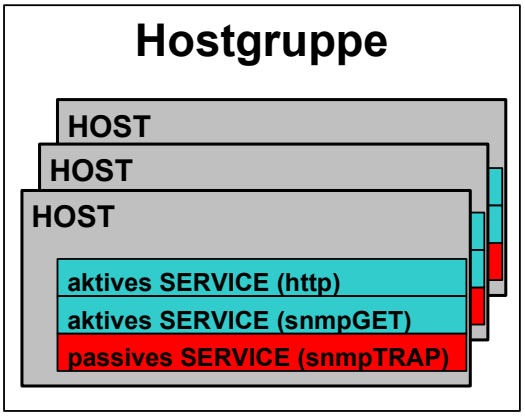


Abbildung 19 Nagios Managed Object Host

Ein Host ist typischerweise ein über das Netzwerk erreichbares Gerät. Diese Geräte sind über eine eindeutige Adresse ansprechbar. Typische Vertreter dieser Klasse sind Computer, Server oder Arbeitsstationen, Netzwerkgeräte, wie Router, Switches, usw. Jedes an ein Netzwerk angeschossenes Gerät stellt somit einen Host dar. Der Status der Hosts wird in der Regel mit einem Internet Control Message Protocol (ICMP) Ping überprüft, der sogenannte Hosttest. Die eigentliche Aufgabe der Devices sind die angebotenen Services. Sie werden als Objekt Service extra konfiguriert und dem Host zugeordnet. Die Überprüfung der Services erfolgt nur wenn der Host selbst erreichbar ist, eine Maßnahme zu Vermeidung unnötiger Last und Alarm Shower. Die Gebäudeüberwachung von HHSC verwendet Hosts. Es sind die Speicherprogrammierbaren Steuerungen selbst, die Eingänge der Box sind die Services.

Hostgruppen fassen Hosts gleicher Art zusammen und ermöglichen die Interaktion mit allen Hosts eine Gruppe mit einem Befehl. Hostgruppen kommen im HHSC Facility Management nicht zum Einsatz.

Die Konfiguration der Hosts wird der Hoststruktur definiert. Sie umfasst eine Reihe von Attributen, wie den Hostname, die Hostadresse und eine Reihe von

Einstellungen für das Management der Komponenten, wie das Plugin für die Statusüberprüfung, die Zeitperiode zur der geprüft oder alarmiert werden soll.

Die Hoststruktur von Nagios wurde für das Facility Management aus HHSC erweitert. So sind folgende Attribute hinzugekommen:

Attribut	**Bedeutung und Verwendung im HHSC**
Alarmid	Eindeutige AlarmID pro SPS.
Problem_message	SPS spezifische Nachricht im Fehlerfall.
Recovery_message	SPS spezifische Nachricht bei recovery.
Problem_serverity	SPS spezifischer Schweregrad im Fehlerfall: Fatal, Error, Warning, Information
Servicetracking_enabled	Automatisches generieren eines Service Tickets im Fehlerfall
Serviceid	Service Ticket Type
Locationid	Installationsort der SPS

Tabelle 1 Nagios für HHSC erweiterte Hoststruktur

Hosttest überprüfen den Status des Devices. Nagios definiert mehrere mögliche Zustände:

Zustand	**Bedeutung**	**Verwendung im HHSC**
Up	Der Hosttest ist erfolgreich, das Gerät ist ansprechbar.	Als Zustand OK
Down	Das Gerät ist ausgeschaltet oder nicht mit dem Netzwerk verbunden.	Als Zustand kritisch
Unreachable	Das Gerät ist nicht erreichbar. Es kann keine Aussage über den Status getroffen werden. z.B. ein Router ist ausgefallen, das Netzwerksegment, an welches der Host angeschlossen ist, nicht erreichbar.	Als Zustand unbekannt

Tabelle 2 Nagios Hostzustände

Service

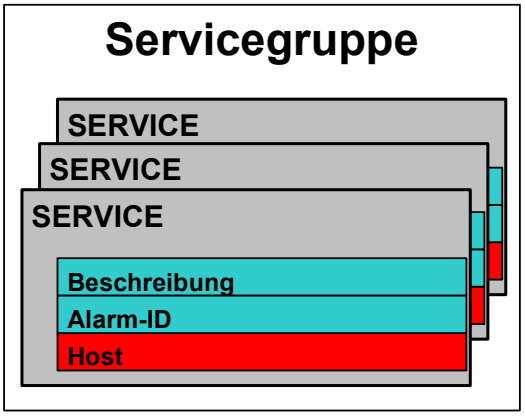


Abbildung 20 Nagios Managed Object Service

Ein Service ist von einem Host angebotener Dienst, oder eine Eigenschaft des Geräts. Nagios kennt die Typen, aktive Services (synchron) und passive Services (asynchron).

Aktive Services werden in regelmäßigen Intervallen abgefragt, das entspricht Poll-driven Management. Nagios ist aktiv. Ein Beispiel für aktive Services wäre ein SNMP-Get. Ein Plugin führt die aktiven Diagnosetests aus und sammelt die Statusinformationen. Das Plugin wird sofern möglich am Netzwerk Management Server aus geführt. Wenn das Plugin lokal am Host ausgeführt werden muss, wird der Test über den NRPE angestoßen.

Passive, asynchrone Services werden nicht regelmäßig überprüft. Nagios erwartet eine Nachricht wenn sich der Zustand des Services ändert, das entspricht Event-driven Management. Nagios ist passiv. Ein Beispiel für passive Services wäre ein SNMP-Trap.

Die Gebäudeüberwachung von HHSC verwendet Services. Es sind die Eingänge der Speicherprogrammierbaren Steuerungen. Das Facility Monitoring empfängt Event-driven Statusänderungen der Eingänge von der SPS-Box, wenn die SPS-Box persistent konfiguriert ist und ansonsten verwendet es Polling für die Zustandsüberprüfungen.

Die Konfiguration der Services wird der Servicestruktur definiert. Sie umfasst eine Reihe von Attributen, wie den Hostname (der Host, der das Serive anbietet), die Servicedescription und eine Reihe von Einstellungen für das Management der Komponenten, wie das Plugin für die Statusüberprüfung, ob das Service aktiv und in

welchen Intervallen geprüft werden soll oder passiv auf Events gewartet werden soll, die Zeitperiode zur der geprüft oder alarmiert werden soll.

Die Servicestruktur von Nagios wurde für das Facility Management aus HHSC erweitert. So sind folgende Attribute hinzugekommen:

Attribut	**Bedeutung und Verwendung im HHSC**
Alarmid	Eindeutige AlarmID pro Eingang.
Problem_message	Eingangs spezifische Nachricht im Fehlerfall.
Recovery_message	Eingangs spezifische Nachricht bei recovery.
Problem_severity	Eingangs spezifischer Schweregrad im Fehlerfall: Fatal, Error, Warning, Information
Servicetracking_enabled	Automatisches generieren eines Service Tickets im Fehlerfall
Serviceid	Service Ticket Type
Locationid	Installationsort des Sensors

Tabelle 3 Nagios für HHSC erweiterte Hoststruktur

Definierte Zustände:

Zustand	Bedeutung	Verwendung im HHSC
Up	Der Test war erfolgreich, der Dienst verfügbar.	Als Zustand OK
Warning	Der Test ist erfolgreich, der festgestellte Zustand ist jedoch nicht der erwartete.	Nicht verwendet
Critical	Der Test ist nicht erfolgreich oder der festgestellte Zustand ist kritisch. Es besteht Handlungsbedarf.	Als Zustand kritisch
Unknown	Es kann keine Aussage über der Zustand getroffen werden.	Als Zustand unbekannt

Tabelle 4 Nagios Service Zustände

Den Zustand einer Komponente kennt Nagios in zwei Typen: Soft State und Hard State. Damit unterscheidet es reale Probleme und kurzfristige Störungen. Ein Zustandswechsel hat unterschiedliche Folgen, je nachdem, ob er im Soft oder Hard State geschieht. Bemerkt ein Plugin eine Störung bei einem Host oder einem Service, dann wechselt diese Komponente zunächst in den jeweilige Soft State. Erkennt Nagios bei weiteren Tests den Status „OK“ noch bevor die Komponente der Schwellenwert, im HHSC „Max. Anzahl Prüfungen“, erreicht, beendet das Programm den Soft State, ohne eine Nachricht zu generieren. Es lag also kein konkretes Problem vor, möglicherweise nur ein Messfehler. Sind zu viele Tests fehlgeschlagen, wechselt der Statustyp in den Hard State. Der Nagios-Prozess stößt daraufhin die Notifikationslogik an. Das Konzept der Soft und Hard State ist nur für das Poll-driven Management von Relevanz. Beim Event-driven Management geht man davon aus, dass ein gemeldetes Event ein reales ist.

Für automatisch angestoßene Reparaturversuche gibt es im Nagios das Konzept des Event Handler. Dieser Event Handler ist ein frei definierbares externes Programm. Dieses Programm oder Skript übernimmt die automatischen Reparaturversuche. Über interne Macros können dem Eventhandler zusätzliche Informationen übergeben werden. Diese Informationen, die Anzahl der nicht erfolgreichen Prüfungen, der Zeitpunkt des letzten OK Status, das Ergebnis, die Ergebnisdetails des letzten Pluginsaufrufs, etc. können das Verhalten des Eventhandlers beeinflussen. Der

Eventhandler wird im Gegensatz zur Notifikationslogik auch in Soft States aufgerufen. Der Watchdog, das automatische Recovery Tool von HHSC bedient sich dieser Funktion.

Kontakt

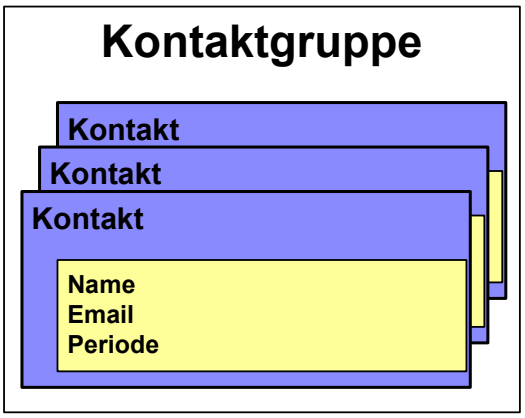


Abbildung 21 Nagios Kontakte

Ein Kontakt ist eine für das überwachte System zuständige Person.

Eine Kontaktgruppe umfasst ein oder mehrere Kontakte. Die Mitglieder dieser Gruppen werden durch Nachrichten über erkannte Probleme, oder deren Lösung informiert.

4.2.2 Nachrichten

Ändert sich der Zustand eines Hosts oder eines Services werden Nachrichten erzeugt und an die dem Host oder Service zugeordneten Kontaktgruppen versandt.

Zustandsänderungen bei Hosts:

Änderung	Bedeutung	Verwendung im HHSC
Up	Das Gerät funktioniert wieder, recovery, positiver Zustand.	Als Wiederherstellung
Down	Das Gerät ist down, nicht positiver Zustand.	Als Problem
Unreachable	Das Gerät ist nicht erreichbar.	Nicht verwendet
Flapping	Das Gerät ändert laufend seinen Status	Nicht verwendet

Tabelle 5 Nagios Zustandsänderungen bei Hosts

Zustandsänderungen bei Services:

Änderung	**Bedeutung**	**Verwendung im HHSC**
Up	Der Test ist erfolgreich, der Dienst funktioniert wieder, recovery, positiver Zustand.	Als Wiederherstellung
Warning	Der Test ist erfolgreich, der festgestellte Zustand ist jedoch nicht der erwartete, nicht positiver Zustand.	Nicht verwendet
Critical	Der Test ist nicht erfolgreich oder der festgestellte neue Zustand ist kritisch. Es besteht Handlungsbedarf.	Als Problem
Unknown	Es kann keine Aussage über der Zustand getroffen werden.	
Flapping	Es kommen laufend unterschiedliche Testergebnisse über den Status.	Nicht verwendet

Tabelle 6 Nagios Zustandsänderungen bei Services

Typen von Nachrichten

Nagios unterscheidet zwischen Host- und Servicenachrichten. Hostnachrichten informieren über eine Zustandsänderung eines Hosts. Servicenachrichten informieren über eine Zustandsänderung eines Services. Wie beim Eventhandler können über interne Makros zusätzliche Informationen übergeben werden. Diese Makros sind für die Anforderungen im Facility Management erweitert worden. So wird bei Nachrichten im Facility Management die AlarmID, die Problem- oder Recoverynachricht mitgegeben. Das Service Tracking des HHSC wird als Ticket System verwendet. Die Tickets werden mit der Notifikationslogik des Nagios erzeugt. Die ebenfalls neuen Macros für die LoctationID und ServiceID ermöglichen das automatische generieren der Tickets.

Der Facilitymonitor im HHSC zeigt den Status der SPS und deren Eingänge dar. Statusänderungen sollen möglichst schnell im Monitor angezeigt werden können. Der Client Controller ein zentrales internes Modul im HHSC Core kann über Nachrichten an die möglicherweise vielen verteilten Front Offices Informationen schicken. Die Notifikationslogik kennt alle Statusänderungen und verschickt entsprechend den Filtern die Nachrichten. Es lag daher nahe die Notifiaktionslogik zu erweitern und die Updates an den Clientcontroller zu schicken, welcher diese an die Front Office GUI weiterleitet. Der Nagios Core gibt die Informationen direkt an den Client Controller über eine SOAP Call weiter. Jede harte Zustandsänderung wird über diesen Weg an den Facility Monitor in den Front Office GUIs transportiert.

Nachrichtenfilter

Jede Änderung des Hard Zustands eines Hosts oder eines Services erzeugt eine Nachricht. Um die Kontakte zielgerecht informieren zu können verfügt Nagios über eine große Gruppe von Filtern.

Systemweit, global kann das Versenden von Nachrichten aktiviert oder deaktiviert werden.

Es besteht die außerdem Möglichkeit für jedes Objekt individuell das Versenden von Nachrichten zu beeinflussen:

Filter	Funktion	Verwendung im HHSC
aktiviert /deaktiviert	Der Versand von Nachrichten ist für diese Objekt aktiv oder inaktiv	Als Meldungen aktiviert /deaktiviert
downtime	Der Host, das Service werden gewartet, es werden für die Dauer der Wartung keine Nachrichten versendet	Nicht verwendet
Status-gesteuert	Abhängig vom Status des Objekts wird benachricht oder die Nachricht gefiltert. Optionen für einen Host: down, unreachable recovery, flapping oder keine. Optionen für ein Service: warning, critical, unknown, recovery, flapping oder keine.	Fix konfiguriert, nach den verwendeten Status im HHSC
Zeit-gesteuert	Es können Zeitperioden definiert werden, in welchen Nachrichten versendet werden sollen.	Als Meldungsperiode
Kontakt-bezogen	Es werden Nachrichten nur an die definierten Kontaktgruppen versendet.	Automatisch konfiguriert für HHSC_MessageHandler, HHSC_ServiceTracking, HHSC_disaster

Tabelle 7 Nagios Objektbezogene Nachrichtenfilter

Weiters ist es möglich den Nachrichtenfilter für jeden Kontakt individuell anzupassen:

Filter	Funktion	Verwendung im HHSC
aktiviert /deaktiviert	Der Versand von Nachrichten ist für diesen Kontakt aktiv oder inaktiv	Nicht verwendet
Status-gesteuert	Abhängig vom Status wird benachricht oder die Nachricht gefiltert. Optionen für einen Host: down, unreachable recovery, flapping oder keine. Optionen für ein Service: warning, critical, unknown, recovery, flapping oder keine.	Fix konfiguriert, nach den verwendeten Status im HHSC
Zeit-gesteuert	Es können Zeitperioden definiert werden, in welchen Nachrichten versendet werden sollen.	Als Meldungsperiode des Nachrichtenwegs

Tabelle 8 Nagios Kontaktbezogene Nachrichtenfilter

Wiederholungen

Das Netzwerkmanagementsystem erwartet auf eine nicht positive Nachricht ein Acknowledge. Bleibt diese aus wird die Nachricht weiterhin entsprechend den definierten Intervallen versendet.

Das Acknowledge ist eine zentrale Anforderung von HHSC an das Meldungssystem. Die Acknowledge Logik wurde um für Anforderungen der AlarmID erweitert.

Intervalle

Die Dauer zwischen zwei nicht positiven Nachrichten ist für jeden Host und für jedes Service individuell konfigurierbar.

Eskalation

Eskalation von Nachrichten bedeutet, dass das wiederholte Versenden von Nachrichten individuell konfiguriert werden kann. Das heißt es können einzelne Wiederholungen oder eine Reihe von Wiederholungen an unterschiedliche Kontakte und somit unterschiedliche Wege versendet werden.

Ein Beispiel:

Nagios hat ein Problem festgestellt. Es soll nun die erste Nachricht an den zuständigen Administrator per Email versendet werden, die zweite und dritte soll in einem Intervall von 5 Minuten per SMS raus gehen. Wird noch immer nicht reagiert wird jeder Administrator alle 15 Minuten per Popup auf dem Desktop informiert.

Eskalationen werden im HHSC nicht verwendet.

Sonderfall volatile Services

Bei volatile Services wird nicht nur bei Änderungen des Status, sondern auch bei einer Änderung der mitgelieferten Information im Fehlerfall alarmiert.

Volatile Services werden im HHSC nicht verwendet.

4.2.3 Die Nagios (Facility Management) Datenbank

Die Datenbank für das Facility Management im HHSC umfasst 42 Tabellen. 26 sind Tabellen für die Konfiguration, je 7 Tabellen für den Status und die History von Services und Hosts und 2 Tabellen für die Kommunikation Nagios – HHSC und Nagios – Persistente SPS Verbindung.

Nagios verwendet für die Konfiguration und die persistente Speicherung der Statusinformationen Textfiles. Diese Textfiles sind nur am Nagios Server verfügbar. Textfiles sind nicht für mehrfach Zugriffe verwendbar. Für eine ordentliche Verwendung des Netzwerk Managements System Nagios ist eine zuverlässige Speicherung der Konfigurations- und Statusdaten erforderlich. Außerdem müssen die Informationen sicher auch anderen Systemen, neben dem Nagios Core verfügbar gemacht werden können. Das für diese Zwecke am besten geeignete Werkzeug ist eine Datenbank. Nachdem HHSC bereits mit der Datenbank MySQL arbeitetet und diese Datenbank frei verfügbar ist kommt auch MySQL für die Facility Management Datenbank zum Einsatz.

Nagios verwendet für die Konfiguration verschiedene Typen von Konfigurations- und Statusdateien:

- Main Configuration File
  Es definiert Konfigurationen für den Nagios Core selbst. Es blieb daher erhalten und um die Konfiguration der Datenbankschnittstelle erweitert.

- Ressource Files
  Sie speichern user-defined macros. Die Konfiguration dieser Makros sind in der Datenbank in der user_resources Tabelle realisiert. Das HHSC Facility Management verwendet die user-defined macros um die Verbindung zum HHSC zu konfigurieren.

- Object Definition Files
  Diese Files speichern die Konfiguration der im Kapitel 4.2.1 Managed Objects beschriebenen Objekte. Die Datenbank umfasst 26 Tabellen für die Konfiguration und Konfigurationsbeziehungen der einzelnen Managed Objects.

- CGI Konfigurationsfile
  Dieses File speichert Einstellungen für das Webinterface des Nagios Systems.

Das Webinterface ist im Facility Management durch den Facility Montor ersetzt worden. Die Datei ist also hier nicht relvant.

- Objects.cache und retention.dat File
  Nagios speichert in diesen Files die aktuelle Konfiguration der Managed Objects, wie sie im Speicher gehalten wird und die Statusinformation dazu. Das File wird regelmäßig, bzw. bei jedem Stoppen oder Neustarten des Prozesses geschrieben. Über external Commands kann auf den Nagios Core und Teile der Konfiguration, wie beispielsweise das aktivieren oder deaktivieren einzelner Servicetests Einfluß genommen werden. Diese Dateien wurden durch die 7 Tabellen für die Statusinformation abgelöst, bzw. sind sie überflüssig, da die Konfigurationsupdates über external Commands direkt in die Konfiguration übernommen werden.

- Nagios.log
  Der Nagios Core Prozess schreibt sein Aktivitäten in der Logdatei nagios.log mit. Dieses File dient auch als Speicher für historische Daten, wie Ausfälle, Recovery, usw. Eine Archivierungslogik speichert die Informationen regelmäßig in einen Archivordner. Die gesamte Historische Information ist von diesem File in die 7 History Tabellen der Datenbank übersiedelt. Das Logfile wurde jedoch für Diagnosezwecke im reduzierten Umfang beibehalten.

- External Command File
  Der Nagios Core Prozess nimmt wie beschrieben externe Befehle entgegen. Diese Schnittstelle ist als Named Pipe im External Command File implementiert. Die external_command Tabelle in der Datenbank übernimmt die gleiche Rolle ist aber über das Netzwerk verfügbar. Beide werden über Polling ausgelesen. Im Event-based Management wird dem Core Prozess über diese Schnittstelle auch die geänderten Statusinformationen mitgeteilt. So schleicht doch ein Polling Mechanismus in das aus Event basierende Meldungssystem.

  Die Tabelle sps_command hat eine ähnliche Funktion. HHSC bzw. der Nagios Core kommunizieren mit dem HHSCPersistentSPS Prozess über den gleichen Mechanismus über diese Tabelle.

4.3 Das HHSC Facility Management

4.3.1 Am Anfang war das wie

Das Facility Management ermöglicht über potentialfreie Kontakte eine Erkennung von Störungen in technischen Einrichtungen. Es erkennt Fehler automatisch und benachrichtigt das zuständige Personal. Die Anschaltung der potentialfreien Kontakte geschieht über eine LAN-Box. Das Facility Management fragt in einem konfigurierbaren Intervall die Kontaktzustände der LAN-Box ab und triggert nach einer Pegeländerung der Kontakte einen Meldungsvorgang. Jedem Kontakt kann hierbei ein frei definierbarer Text, als Meldung zugeordnet werden.

Die Anforderungen an das Facility Management im HHSC klingt ganz nach einer Anforderungsbeschreibung im Network Management, im speziellen dem Fault Management. Wenn man ein paar Wörter weglässt:

- Das Management ermöglicht eine Erkennung von Störungen in technischen Einrichtungen. Es erkennt Fehler automatisch und benachrichtigt das zuständige Personal. Das Management fragt in einem konfigurierbaren Intervall die Zustände ab und triggert nach einer Änderung einen Meldungsvorgang.

Die Lösung der Aufgabenstellung findet sich in den Funktionen des Fault Management, einer Functional Area des ISO/OSI Network Management:

- Ausführen von Diagnose Tests und Abfolgen, Poll-driven Management
- Alarmmeldungen und Tracking von Fehlern

Die in der Anforderungsbeschreibung genannte LAN-Box ist eine Speicher Programmierbare Steuerung (SPS) der Siemens Simatic S7-200 Serie. Eine SPS verfügt über Ein- und Ausgangkontakte. Das Programm in der SPS beschreibt die Steuerungsaufgaben, die das Gerät übernimmt. Ohne Programm nehmen diese Geräte keine Steuerungsaufgaben war. Im Rahmen des HHSC Facility Management sollen nur die an den Eingängen angeschlossenen Geräte beobachtet werden. Es ist daher irrelevant ob die SPS Steuerungsaufgaben wahrnimmt oder nur zum Anschluss der Sensoren oder Geräte verwendet wird. Über die Erweiterungsmodule EM 221 kann die Anzahl der Eingänge einer Box erweitert werden.

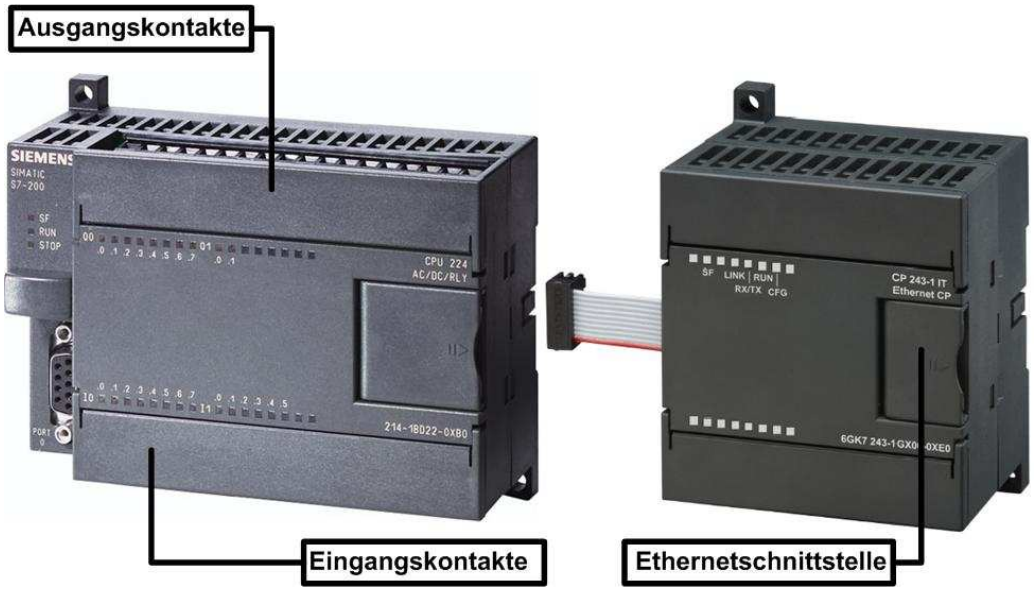


Abbildung 22 Siemens S7 CPU224 mit CP 243-1 IT

Eine Siemens S7-200 Simatic SPS verfügt über keinen Netzwerkanschluss. Als Schnittstelle zum Ethernet kommt der Kommunikationsprozessor CP 243-1 IT zum Einsatz. Mit Hilfe der JAVA S7-Beans-Bibliothek für Advanced- und IT CP kann in einer Java Applikation eine Verbindung mit der SPS hergestellt werden. In dieser mit Benutzer/Passwort gesicherten Verbindung kann auf den Status der Eingänge, der Variablen des laufenden Programms zugegriffen werden.

Für die Kommunikation mit der SPS im Netzwerk muss dem CP 243-1 IT eine IP-Adresse zugeordnet werden. Wenn die Adresse unabhängig vom Programm in der SPS sein soll, muss diese von automatisch von einem zentralen Server vergeben werden. Über die MAC Adresse der Ethernetschnittstelle des Kommunikationsprozessors ist das Gerät eindeutig identifizierbar. Der CP 243-1 IT kann eine Adresse automatisch von einem Bootstrap Protocol (BOOTP) Server beziehen. In der Konfiguration des BOOTP Server kann jedem System aus SPS und CP eine eindeutige IP Adresse über dessen Media Access Control (MAC) Adresse zugeordnet werden. Über die IP Adresse kann dann das Facility Management die Statusinformationen auslesen. Die Zielplattform für HHSC ist Windows, der Windows 2003 Server. Der Windows 2003 Server verfügt über einen Dynamic Host Configuration Protocol (DHCP) der auch BOOTP unterstützt.

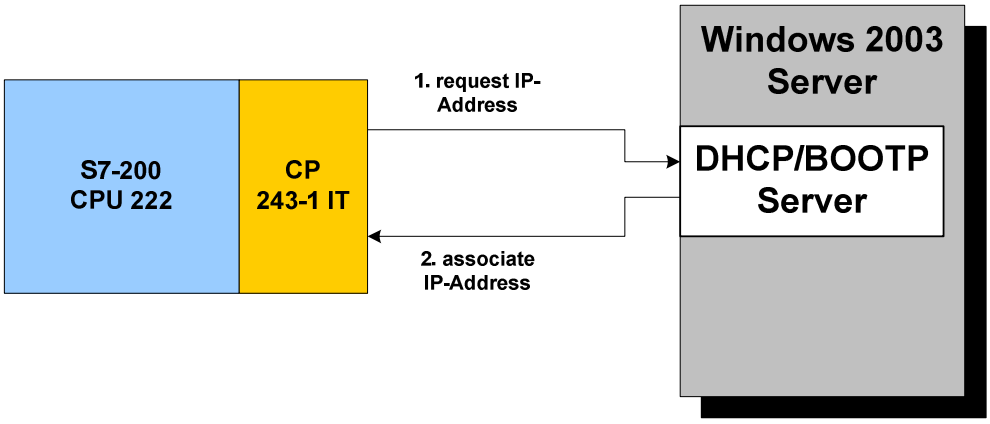


Abbildung 23 SPS - BOOTP Server

Der Nagios-core hat seine Wurzeln im LINUX/UNIX Umfeld. Für einen Betrieb unter Windows benötigt der Nagios Teil des Facility Management ein sogenanntes cygwin Environment. In dieser Umgebung sind der Nagios-core und die benötigten Open Source Plugins problemlos lauffähig. Die HHSC-Module HHSCsendMessage, HHSCServiceTracking, HHSCpersistenSPS und HHSCcheckSPS benötigen wie HHSC den Sun Java Runtime Environment plus den erforderlichen Erweiterungen für SOAP und MySQL.

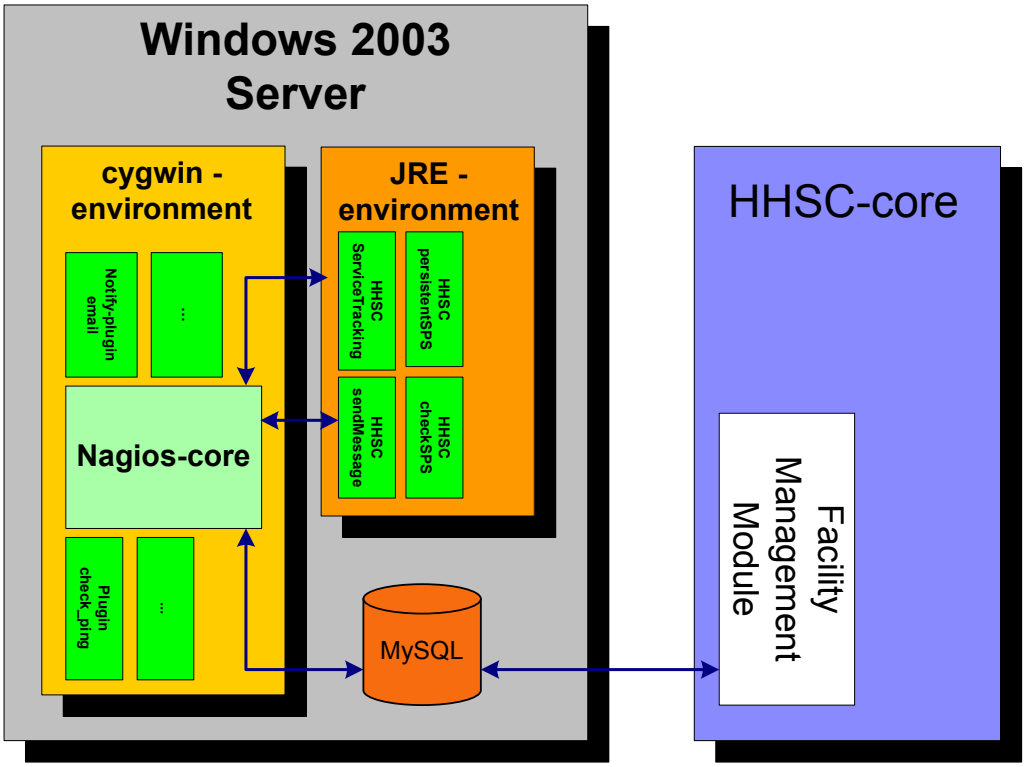


Abbildung 24 HHSC Facility management Environment

4.3.2 OSI Netzwerk Management in HHSC

Im Facility Management sind die Managed Objects die verschiedensten Elemente der Gebäude. Sensoren stellen den Zustand der Manged Objects fest. Typische Vertreter sind Räume, Türen, Fenster, Markisen, Aufzüge, Feuermelder. Deren Zustand messen Start- und Endschalter, Positionsmelder, Temperatursensoren, Rauchmelder. Die abstrakte Sicht repräsentiert die Eigenschaft der Ressource für das Management. Einfache digitale Beispiele sind eine Türe kann offen oder geschlossen sein, eine Markise ausgefahren oder eingefahren sein, ein Alarm kann aktiviert sein oder nicht. Komplexere Analoge Beispiele sind die Temperaturen in einem Raum. Die Schwellenwerte legen gewünschten den Temperaturbereich fest.

Die SPS in Verbindung mit dem Kommunikationsprozessor und dessen inkludierten Webserver übernehmen die Agent Role. Der Webserver bildet die Schnittstelle zur Manger Role und nimmt die Management Aufträge entgegen die SPS führt die Aktionen aus. Die Schnittestelle zu den Managed Objects sind die Eingänge der SPS und der Erweiterungsmodule.

HHSC mit seinem Facility Management Modul und mit dem angebundenen Nagios bilden die Management Role. Gesteuert nach der Konfiguration, den Management Policies werden Statustests von der Agent Role der SPS angefordert und die Ergebnisse entsprechend interpretiert.

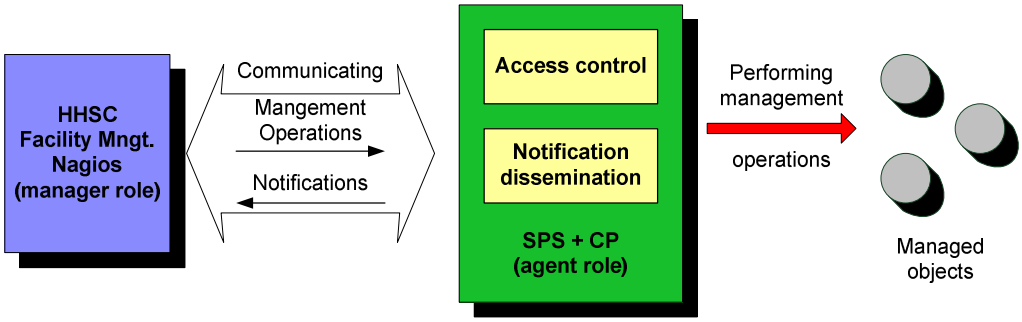


Abbildung 25 [ITU-T X.701] HHSC Facility Management in OSI Management

4.3.3 Das Fault Management in HHSC

Das HHSC Facility Management kann über zwei Wege die Statusinformationen der Managed Objects einholen. Ein Weg ist über Poll-driven Management über das HHSCcheckSPS Plugin realisiert. Den zweiten Weg implementiert das HHSCpersistentSPS Modul. Es baut eine ständige Verbindung mit der SPS auf und meldet Statusänderungen an den Nagios Core weiter. Diese Lösung realisiert Event-driven Management.

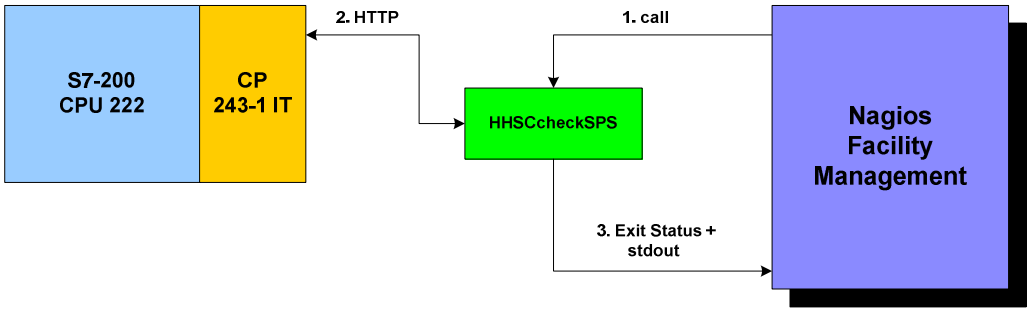


Abbildung 26 HHSC Facility Management Poll-driven Management

Die SPS Box ist im Nagios als Host konfiguriert und die Eingänge als Services. Beim Poll-driven Management wird auf Anforderung zum Auslesen der Statusinformation das HHSCcheckSPS Plugin in einem Call vom Nagios Core gestartet. Das Plugin baut über den Webserver im Kommunikationsprozessor eine Verbindung auf, holt die gewünschten Statusinformationen ein und meldet über den Exit Status und stdout das Ergebnis an Management Role zurück.

Das HHSC Facility Management verwendet ausschließlich digitale Informationen. Schwellenwerte und Thresholds haben in dieser digitalen Verarbeitung keine Bedeutung und brauchen daher nicht behandelt werden.

Die ausgeführten Tests dürften nicht disruptive sein. Es darf nach den Anforderungen an das Facility Management im HHSC kein Einfluss auf die laufenden Steuerungsprogramme genommen werden.

Die Beschränkung des Webservers im Kommunikationsprozessor auf maximal vier gleichzeitige Verbindungen bei einer gleichzeitigen maximalen Ausbaustufe von 110 Eingängen pro SPS stellen sehr hohe Forderungen an das Scheduling. Das rechtzeitige Einholen der Informationen bei geringen Testintervallen über Polling ist überhaupt unmöglich.

Abhilfe schafft das Event-driven Management. Beim Event-driven Management wird nur eine Verbindung zur SPS Box aufgebaut. Diese besteht jedoch dauerhaft, persistent. Sobald eine SPS in der Konfiguration persistent konfiguriert ist richtet der für das Facility Management angepasste Nagios Core ein temporäres Service in Windows ein und starten das Modul HHSCpersistentSPS. Dieses Modul baut zu allen in der Konfiguration als persistent definierten SPS Boxen eine Verbindung auf. Ändert sich der der Status eines Eingangs einer der Boxen, so meldet das Modul die Änderung sofort an die Management Role über die external_command Tabelle der Datenbank weiter. Leider liest der Nagios Core diese external commands per polling ein. Das Intervall ist zwar sehr klein gewählt, eine Sekunde, aber es erhöht die Zeit in worst case vom Eintreten des Events bis zur Meldung im Monitor bzw. zur Alarmeldung enorm. Ungekehrt erfolgt die Einflussnahme des Nagios Core auf das Persistenzmodul ebenfalls über die Datenbank, über die sps_command Tabelle. Diese Kommunikation ist jedoch nicht zeitkritisch.

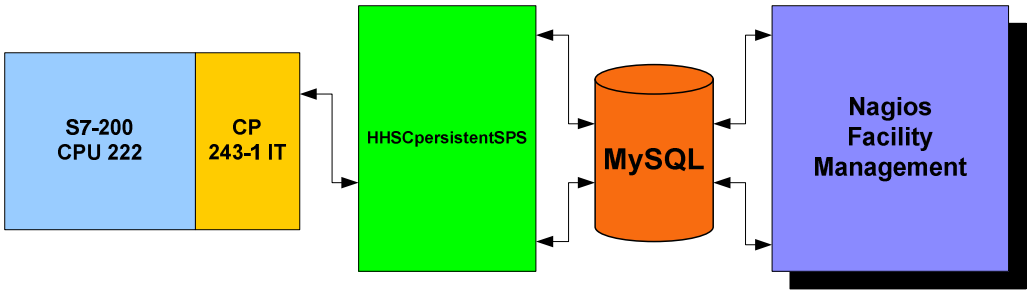


Abbildung 27 HHSC Facility Management Event-driven Management

Ein klassischer Anwendungsfall für Event-driven Management sind Alarme. Ein Beispiel ist eine Notruftaste in Toiletten für körperlich behinderte Personen. Hier ist unmittelbare Hilfe erforderlich. Das Personal muss also sofort alarmiert werden. Mögliche Messfehler oder andere Fehleinflüsse werden ignoriert.

Ein Anwendungsfall für Poll-driven Management sind Öffner und Schließer. Ein Beispiel ist eine Notausgangstüre. Diese Türe sollte eigentlich geschlossen sein und nur im Notfall verwendet werden. Das Personal benutzt die Türe für manche Wege um Umwege zu vermeiden. Ein kurzes öffnen ist also durchaus zulässig. Ist die Türe jedoch länger offen muss überprüft werden weshalb. Ein anderes Beispiel ist ein Windmesser bei einer Markise. Kurze Böen kann die Markise leicht vertragen, stärkeren dauerhaften Wind jedoch nicht. Sie muss eingefahren werden. An Hand des Konzepts der Soft- und Hardstates können diese Anforderungen leicht in Nagios umgesetzt werden.

Alarmmeldungen und Tracking von Fehlern.

Das HiPath Hospitality Service Center verfügt über Meldungssystem und ein Ticketsystem. Das Facility Management benutzt diese Systeme für die Zwecke der Alarmmeldungen und dem Tracking von Fehlern.

Der HHSC MessageHandler kann Nachrichten an alle Benutzeroberflächen (Front Office, PDA, ..), an das Front Office alleine, an den PDA alleine, per SMS oder per Email versenden. Diese Nachrichten können blockierend definiert werden. Das heißt eine weitere Benutzung der Software ist ohne Bestätigung nicht möglich. Ein Zuordnung an eine Rolle oder einzelne Mitarbeite ist möglich. Der Nachrichtensystem kennt 4 Prioritäten: Fatal, Fehler, Warnung und Informationen. Das Facility Management generiert die Nachrichten entsprechend den konfigurierten Prioritäten und Nachrichtentexten. Die Zustellung selbst übernimmt der HHSC MessageHandler.

Abbildung 28 HHSC Blockierendes Popup des MessageHandlers

Das HHSC ServiceTracking ist ein Ticketsystem mit der Möglichkeit den Fortschritt der Erledigung zu verfolgen.

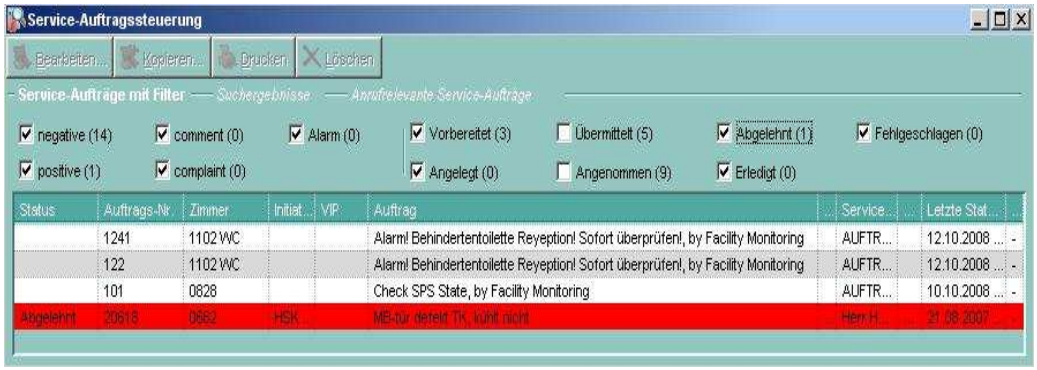


Abbildung 29 HHSC Service Auftragssteuerung

Die Tickets durchlaufen dabei eine Reihe von Status. Beginnend mit vorbereitet oder angelegt. Der Status wechselt zu übermittelt, wenn der Auftrag an den Service Mitarbeiter übermittelt worden ist. Der Service Mitarbeiter hat einen PDA oder ein

tragbares DECT Telefon bei sich. Mit Hilfe des Geräts kann er den Auftrag menügeführt annehmen oder ablehnen. Im positiven Fall nimmt er den Auftrag an. Nach einer positiver Erledigung setzt er ebenfalls menügesteuert den Auftrag auf erledigt. Hat der Mitarbeiter den Auftrag angenommen aber nicht erfolgreich erledigen können setzt er den Status auf fehlgeschlagen und das Front Office Team geniert einen neuen Auftrag oder eskaliert anderweitig.

Nachrichten und Service Aufträge werden in der erweiterten Notifikations Logik des Nagios Core generiert und über die Module HHSCsendMessage, bzw. HHSCServiceTracking per SOAP Call an die entsprechenden Module im HHSC weitergegeben.

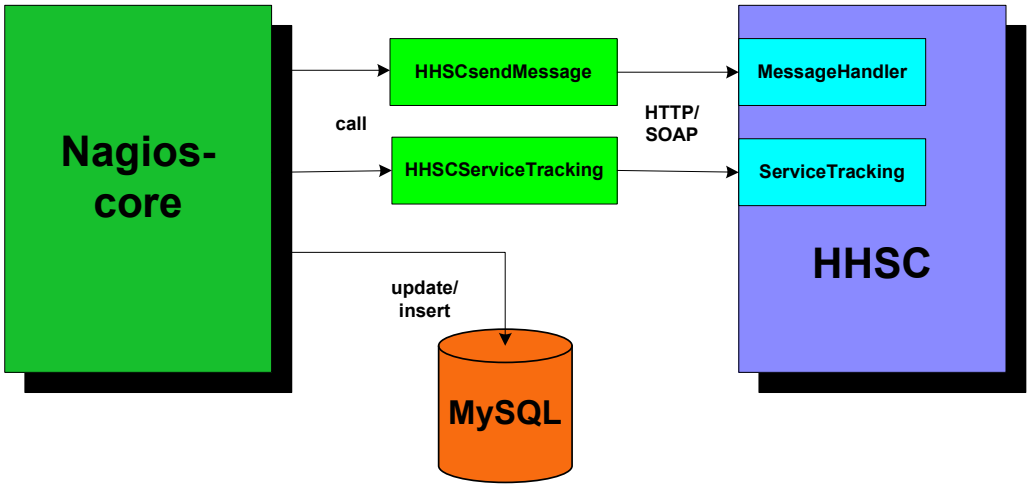


Abbildung 30 HHSC Nagios - Notifaktion Service Tracking

Meldungen bei Ausfall des HHSC MessageHandler:

- Ist der HHSC MessageHandler nicht verfügbar können keine Informationen an HHSC weitergegeben werden. In diesem Fall werden alle Meldungen bezüglich des HHSC MessageHandler über Email an eine konfigurierbare Adresse alarmiert. Nagios-core ruft in diesem Fall email auf. Dieses Tool kann Email über einen SMTP Server versenden.

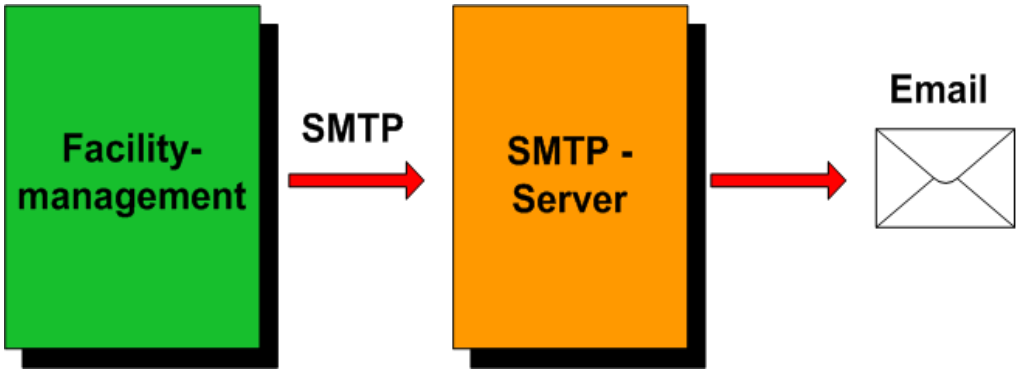


Abbildung 31 HHSC alternative Alarmierung

Der Gebäudemonitor gibt eine Übersicht über die Facility Management angelegten SPS Boxen und deren angeschlossenen Managed Objects. Der Status der SPS oder der Eingänge ist farbcodiert. In diesem Fenster kann der Benutzer einen Alarm im Facility Management per Acknowledge zu Kenntnis nehmen. Ein Acknowledge unterdrückt weitere Wiederholungen des Alarms.

Abbildung 32 HHSC Facility Mangagement Gebäudemonitor

Mittels Doppelklick in der Spalte SPS öffnet sich der automatisch eine Übersicht über die SPS-Box und die angeschlossenen Module. Der Rack Status ist eine Webseite des Kommunikationsprozessors. Er gibt einen Überblick über die SPS Box und die angeschlossenen Module.

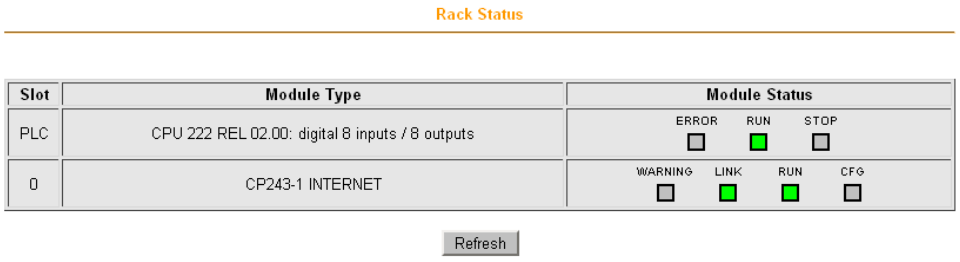


Abbildung 33 Rack Status Webseite des Kommunikationsprozessors

Das Facility Management versorgt den Gebäudemonitor bei jeder Änderung im Status oder der Konfiguration eines Managed Objekts mit den aktuellen Daten. Die Information wird zeitgleich mit den Nachrichten über die Notifikations Logik verschickt. Der Gebäudemonitor wird immer verständigt auch wenn die Benachrichtigung deaktiviert ist. Er repräsentiert somit immer den Stand den Nagios intern über die Managed Objects verwaltet. Der Monitor wird mittels SOAP Calls und über die Client Controller versorgt.

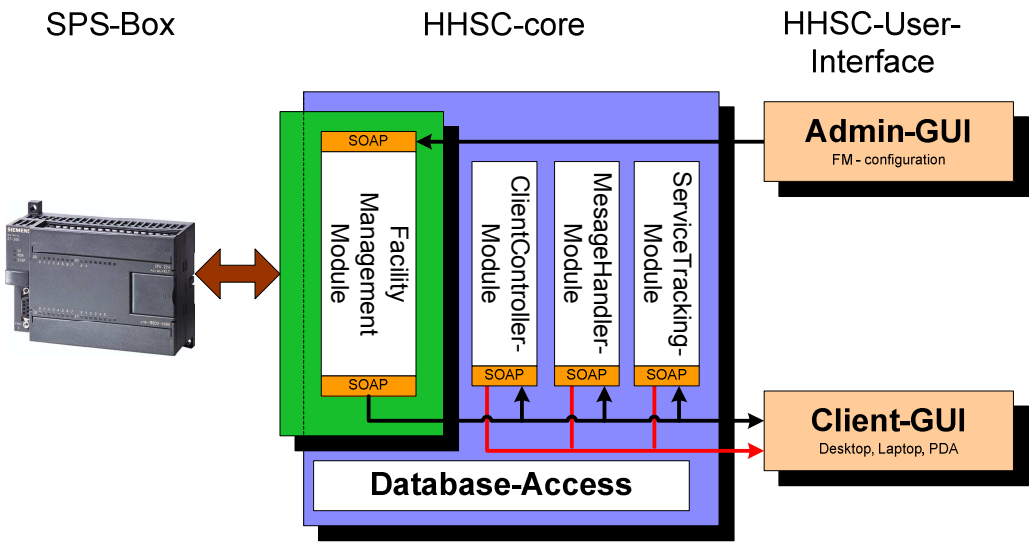


Abbildung 34 HHSC Interaktion Facility Management und GUI

Fehler und Meldungen im Facility Management müssen dieser aktuellen Form der Integration manuell über das Personal im Hotel bearbeitet werden. Die Reaktion auf einen ausgelösten Alarm wird immer manuell erfolgen müssen. Das Ein- und Ausfahren einer Markise ist sicher eine relative einfach zu automatisierenden Tätigkeit.

Automatische Reparaturen werden im HHSC Facility Management im Watchdog durchgeführt. Hier wird die Netzwerk Management Software Nagios auch für Netzwerk Management Aktivitäten verwendet. Das Nagios überwacht nämlich den HHSC Server selbst. Stellt das System einen Fehler durch negative Testergebnisse fest versucht es den HHSC Server Prozess neu zu starten. Der Versuch wird drei mal unternommen. Ebenso ist eine Überwachung der MySQL Datenbanken implementiert.

Die Funktionen führen und prüfen von Log Dateien ist im HHSC selbst über ein eigenes Administrationstool, die Maintenance GUI realisiert. Mit diesem Werkzeug

kann der Administrator Loggingfunktionen einzelner Module mit unterschiedlichen Severities aktivieren und deaktivieren. Auch die Analyse von Logfiles und das Tracking ist möglich. Das Facility Management Modul im HHSC bedient sich dieser Fähigkeiten. Wie im Kapitel 4.2 Nagios beschrieben ist das Logging im Nagios Teil unterschiedlich implementiert.

4.3.4 Configuration Management in HHSC

Die Konfiguration des Facility Management im HHSC erfolgt im der Administrationsoberfläche des Front Office, bzw. der Maintenance Gui. Dem Benutzer, seiner Rolle muss das Recht Gebäudeüberwachungs-Konfiguration zugeordnet sein um die Berechtigung für die Konfiguration zu erhalten.

Die Administrationsoberfläche kommuniziert dabei direkt mit dem HHSC Facility Management Modul innerhalb HHSC. Das Modul schreibt die Konfiguration in die Facility Management Datenbank.

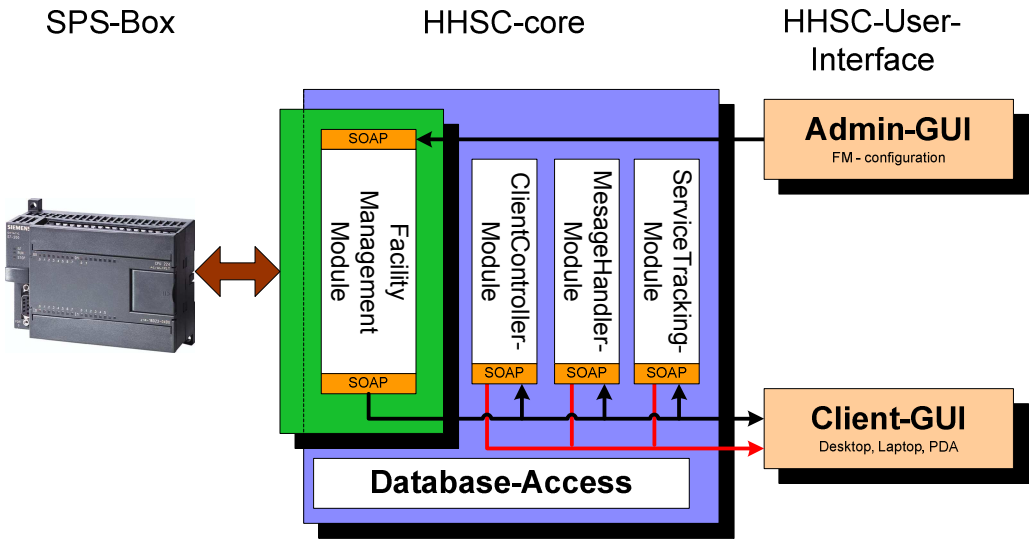


Abbildung 35 HHSC Interaktion Facility Management und GUI

Objektkonfiguration

Die Admin-GUI erlaubt die Konfiguration der SPS-Boxen und deren Eingänge. Die Zeitperioden sind frei definierbar, jedoch die Standard Zeitperiode HHSC_24x7 ist immer vorhanden und kann nicht verändert werden. Die Nachrichtenwege sind vorgegeben. Zeitperioden können frei zugeordnet werden. Unter Nachrichtentyp wird der HHSC MessageHandler und seine Routingfunktionalität eingestellt. Siehe Abbildung 36 HHSC Facility Management Konfiguration.

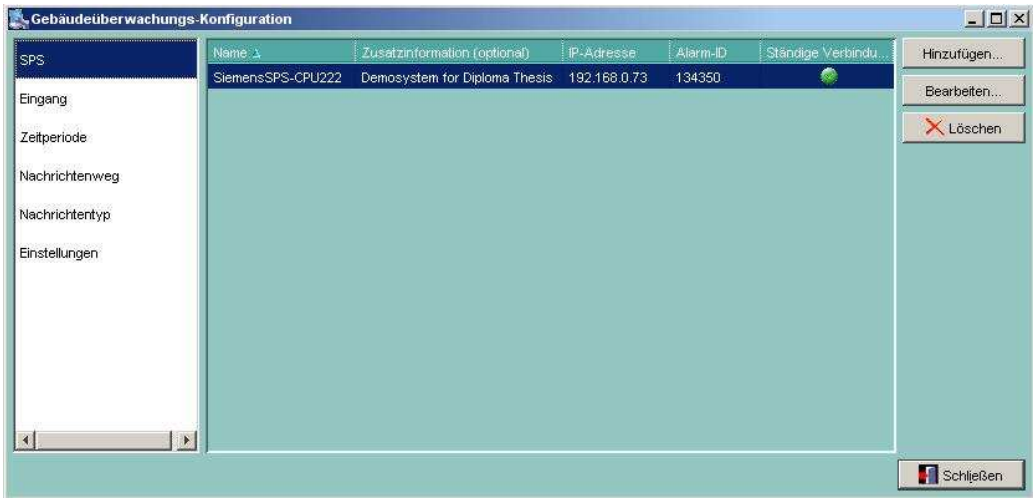


Abbildung 36 HHSC Facility Management Konfiguration

Die Konfiguration des Facility Management im HHSC bietet eine automatische Vorkonfiguration der der SPS inklusive aller Eingänge. Dabei wird die Konfiguration der Box ausgelesen und automatisch ein Polling für den Host, die Box selbst und alle Eingänge eingerichtet. Diese Automatik erkennt den Typ der SPS und die Anzahl und Type der angeschlossenen Module. So kann die Anzahl der verfügbaren Eingänge berechnet werden.

Das HHSC Facility Management Applikationsmodul kommuniziert direkt mit der SPS-Box um die Konfiguration der SPS-Box auszulesen. D.h. es werden die CPUs und die angeschlossenen Module ausgelesen. Diese Informationen sind in den Sondermerkern der S7-200 gespeichert. Das FM benutzt zum Auslesen der Daten die der JAVA S7-Beans-Bibliothek.

S7-200 Sondermerker

In [STEP7] die Hilfe zu Siemens STEP 7-MicroWIN V4.0.1.10 findet man die Dokumentation der Sondermerker. STEP 7-Micro WIN V4.0 ist die Programmierumgebung für die Siemens Simatic S7 SPS Serie.

Die relevante Sondermerker sind SMB6 und SMB8-SMB21:

Symbolischer Name	Adresse	Beschreibung
CPU_ID	SMB6	Gibt die CPU-Modellnummer an
EM0_ID	SMB8	Kennregister Modul 0
EM0_Fehler	SMB9	Fehlerregister Modul 0
EM1_ID	SMB10	Kennregister Modul 1
EM1_Fehler	SMB11	Fehlerregister Modul 1
EM2_ID	SMB12	Kennregister Modul 2
EM2_Fehler	SMB13	Fehlerregister Modul 2
EM3_ID	SMB14	Kennregister Modul 3
EM3_Fehler	SMB15	Fehlerregister Modul 3
EM4_ID	SMB16	Kennregister Modul 4
EM4_Fehler	SMB17	Fehlerregister Modul 4
EM5_ID	SMB18	Kennregister Modul 5
EM5_Fehler	SMB19	Fehlerregister Modul 5
EM6_ID	SMB20	Kennregister Modul 6
EM7_Fehler	SMB21	Fehlerregister Modul 6

Tabelle 9 Sondermerker SMB6 und SMB8-SMB21

SMB6 Kennregister der CPU

Sondermerkerbyte 6 ist der Kennregister der CPU. SM6.4 bis SM6.7 enthalten die Kennung der CPU. SM6.0 bis SM6.3 sind für zukünftige Funktionen reserviert:

SMB6	**MSB**							**LSB**
	7							0
	x	x	x	x	r	r	r	r
SM6.4-SM6.7	0	0	0	0	CPU 212 / CPU 222			
	0	0	1	0	CPU 214 / CPU 224			
	0	1	1	0	CPU 221			
	1	0	0	0	CPU 215			
	1	0	0	1	CPU 216 / CPU 226 (XM)			

Tabelle 10 SMB6 Kennregister der CPU

SMB8-SMB21 Kenn- und Fehlerregister E/A-Modul

Die Sondermerker SMB8 bis SMB21 sind in Bytepaaren für die Erweiterungsmodule 0 bis 6 angeordnet. Das Byte mit der geraden Nummer in einem Paar ist das Kennregister des Moduls. Dieses Byte kennzeichnet den Modultyp sowie die Art und Anzahl der Ein- und Ausgänge. Das Byte mit der ungeraden Nummer in einem Paar ist das Fehlerregister des Moduls. Dieses Byte zeigt jeden in den Ein- und Ausgängen des Moduls erkannten Fehler an.

Der Aufbau der Register:

Kennregister E/A Modul	**MSB**							**LSB**
	7							0
	M	t	t	A	E	E	A	A
Modul vorhanden	0							
Modul nicht vorhanden	1							
Kein intelligentes E/A Modul		0	0					
Intelligentes E/A Modul		0	1					
Reserviert		1	0					
Reserviert		1	1					
Digital				0				
Analog				1				
Keine Eingänge					0	0		
2 AE oder 8 DE					0	1		
4 AE oder 16 DE					1	0		
8 AE oder 32 DE					1	1		
Keine Ausgänge							0	0
2 AA oder 8 DA							0	1
4 AA oder 16 DA							1	0
8 AA oder 32 DA							1	1

Tabelle 11 SMB8-SMB21 Kenn- und Fehlerregister E/A-Modul

Im HHSC kann eine SPS eindeutig über den frei konfigurierbaren Namen benannt werden. Zusätzlich bietet der Alias die Möglichkeit die SPS-Box näher zu beschrieben. Die Konfigurationen des einzelnen Eingangs bietet die gleichen Möglichkeiten, Name und Alias. Die Einstellungen für das Service Tracking erlauben zusätzlich die Angabe des Einsatzortes und der definierte Service Text gibt zusätzlich Auskunft über die Verwendung der Box oder des Eingangs. Die verfügbaren Räume und Service Texte können über Administrationsfunktion von HHSC eingegeben werden.

Änderungen in der Objektkonfiguration verursachen immer einen Reload der Konfiguration im Nagios Core. Die Admin Gui veranlasst diesen durch einen entsprechenden Eintrag in die external_commands Tabelle.

Zustandsverwaltung

Die Verwaltungszustände aus der [ITU-T X.731] sind im Facility Management von HHSC umgesetzt. Die Verwaltungszustände werden aus einer Kombination aus den Einstellungen Prüfungen aktiviert und Meldungen aktiviert erreicht. Prüfungen aktiviert bedeutet die aktive Überprüfung, das Poll-driven Management für dieses Objekt ist aktiviert. Es werden also regelmäßig, konfigurierbar über das Normale Prüfungsintervall, in der konfigurierten Prüfungsperiode aktiv Tests ausgeführt. Meldungen aktiviert bedeutet es werden Nachrichten über Zustandsänderungen des Managed Objects in der gewählten Meldungsperiode mit konfigurierter Meldungspriorität verschickt.

Der Zustand in Betrieb ist repräsentiert durch die Konfigurationseinstellungen Prüfungen aktiviert und Meldungen deaktiviert. Werden Meldungen aktiviert repräsentiert die Konfiguration den Status aktiv. Werden die auch die Prüfungen deaktivert so ist das Managed Object Außer Betrieb.

Der Zustand Beschäftigt macht in dieser Interpretation nicht viel Sinn und ist daher nicht bedacht worden.

Änderungen in der Zustandsverwaltung können über externe commands direkt an den Nagios Core kommuniziert werden. Der modifizierte Nagios Core würde die updates dann in die Konfigurationsdatenbank eintragen. Die Admin Gui geht jedoch den gleichen Weg wie bei der Objektkonfiguration.

Attributsverwaltung

Die Admin Gui unterscheidet nicht zwischen Objektkonfiguration und Attributsverwaltung. Die Funktionsweise ist daher gleich.

Beziehungsverwaltung

Durch die Host – Service , hier SPS – Eingangs Konfiguration ist implizit eine Beziehung konfiguriert. Nagios kennt bei der Konfiguration der Hosts die parents Einstellung. Über die Parentseinstellungen kann eine Netzwerkstruktur mit Routern und Subnetzen abgebildet werden. Die Netze in einem Hotel kommen jedoch in der Regel ohne Router innerhalb des Netzwerkes aus. Aus diesem Grund kommen parents nicht im HHSC Facility Mangagement zum Einsatz.

Softwareverteilung

Ein automatisches Programmieren der SPS via HHSC war angedacht. Diese Funktion macht nur Sinn wenn die SPS keine Steuerungsaufgaben ausführt. Ansonsten würde das Programm in der SPS überschrieben werden. Technisch ist die Programmierung über das Netzwerk möglich. Eine SPS ohne Programm, man spricht vom urgelöschten Zustand, bezieht automatisch eine IP-Adresse von einem BOOTP Server und ist daher auch im urgelöschten Zustand über das Netzwerk erreichbar.

4.3.5 Accounting Management in HHSC

Das Accounting Management im Facility Management ist keine Forderung der Anorderungsbeschreibung des Factility Management im HHSC.

Man trifft Accounting Management dennoch im HHSC. Ein Accounting Management ist bei den Telefongebühren implementiert, in der gegenwärtigen Entry Version auch für Internetgebühren, pre- als auch post-paid.

Denkbare Einsatzmöglichkeiten für zukünftige Erweiterungen sind jedoch ausreichend vorhanden:

- Die Abrechnung von Benutzungszeiten im Hallenbad oder der Sauna beispielsweise. Das Szenario: Der Gast benutzt mit dem Zimmerschlüssel, dieser ist mit RFID ausgestattet, die Sauna oder eine ähnliche Einrichtung. Das betreten und verlassen wird über Radio Frequency Identification (RFID) Sensoren festgestellt. Per Event werden die Ereignisse an das Facility Management Modul gemeldet und die Daten gespeichert. Bei der Abrechnung werden diese Daten herangezogen um die Endsummer der Hotelrechnung zu bestimmen. Ein anderes Szenario gleicher Art wäre in der Parkgarage, mit Erkennung des Kennzeichens des Fahrzeugs des Gastes.

4.3.6 Performance Management in HHSC

Das Management Informations System ist ein Werkzeug für die statistische Aufarbeitung der im laufenden Betrieb erhobenen Daten.

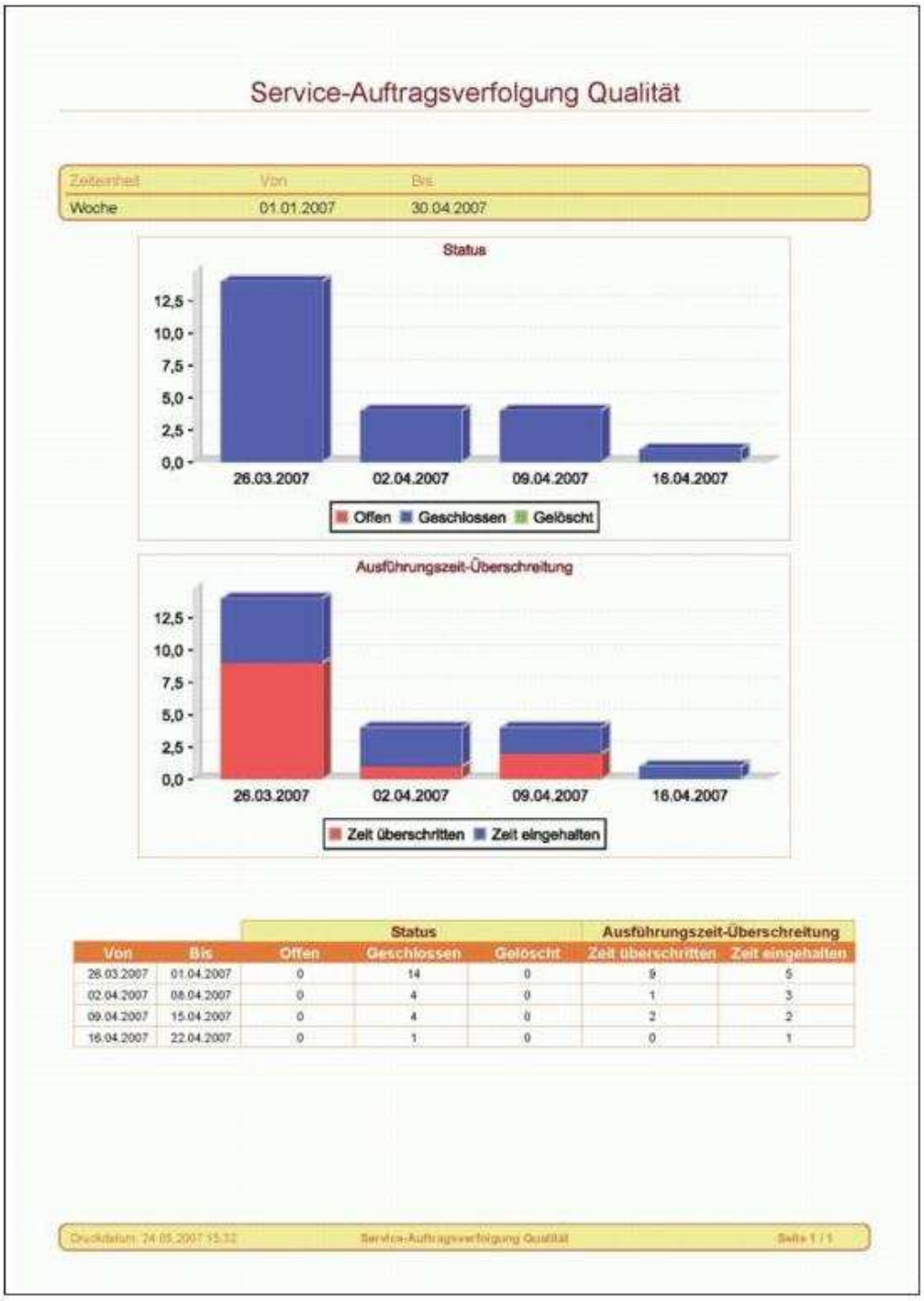
Für den Bereich Facility Management sind vor allem die Auswertung hinsichtlich Service Tracking relevant. Ein Beispiel siehe Abbildung 37 HHSC MIS Auswertung Service Tracking Qualität.

Im ersten drittel des Jahres 2007 wurden alle Serviceaufträge geschlossen. Jedoch nicht alle in der vom Management verlangten Zeit.

Die Kennzahl Verfügbarkeit, wie in 2.1.3 FCAPS definiert kann auf Alarme im Facility Management nicht angewendet werden. Die Mean Time Between Failure hat hier keine Aussagekraft. Die Mean Time to Repair hingeben sehr wohl. Mit dieser Kennzahl kann die Performance wie schnell auf einen Alarm reagiert wurde, bzw. wie schnell dieser behoben wurde gemessen werden.

Performance-, also Lasttests wurden in Produktion von HHSC von der Testabteilung durchgeführt. Die Tests haben Lastsituationen in Richtung Monitoring einer großen Anzahl von Nebenstellen simuliert. Und über Simulationswerkzeuge eine hohe Last an gleichzeitigen Anrufen in dem Switch, der Telefonanlage.

Im Facility Management selbst hatten Performance Tests Probleme beim Poll-based Management einer über Erweiterungsmodule voll bestückte SPS aufgezeigt. Wie bei 4.3.3 Das Fault Management in HHSC bereits besprochen ist ein Polling auf Grund der technischen Begrenzungen des Kommunikationsprozessors mit kleinen Prüfintervallen nicht sinnvoll. Aus diesem Grund wurde die persistente Verbindung mir der SPS-Box implementiert.



		Status			Ausführungszeit-Überschreitung	
Von	Bis	Offen	Geschlossen	Gelöscht	Zeit überschritten	Zeit eingehalten
26.03.2007	01.04.2007	0	14	0	9	5
02.04.2007	08.04.2007	0	4	0	1	3
09.04.2007	15.04.2007	0	4	0	2	2
16.04.2007	22.04.2007	0	1	0	0	1

Abbildung 37 HHSC MIS Auswertung Service Tracking Qualität

4.3.7 Security Management in HHSC

Das Accounting Management im Facility Management ist keine direkte Forderung der Anorderungsbeschreibung des Facility Management im HHSC.

Natürlich sind die Daten in den SPS Boxen über Benutzer/Passwort geschützt. Die Benutzer/Passwort Kombination ist aber im SPS Programm selbst kodiert und auch im Facility Management sind die Werte hardcoded.

Im HHSC selbst gibt es eine eigene Benutzerverwaltung. Der Administrator kann Benutzer/Passwort Konfigurationen festlegen. Über Rolle können den Benutzern Zugriff aus Bereiche im HHSC gewährt oder verweigert werden. Für das Facility Management sind die Rechte „Gebäudeüberwachung“ und „Gebäudeüberwachungs-Konfiguration“ vorgesehen.

Die Produktion von HHSC aktualisiert mit jedem update die sicherheitsrelevanten Informationen in der Release Note. Außerdem werden die verwendete Produkte anderer Hersteller oder aus der OpenSource Gemeinde regelmäßig aktualisiert. Das Produktionsteam wird dazu automatisch mit Sicherheitsreports zu den Verwendeten Produkten informiert.

Ein Denkbarer Einsatz für Security Management im Hospitalitybereich ist ein automatisches oder von Personal beim Checkin manuell konfiguriertes Zutrittssystem mit RFID Zimmerschlüsseln. Je nach Buchung wird der Zugang zur Sauna oder dergleichen Einrichtungen, je nach Bezahlung freigeschalten. Für Seminarhotels im speziellen wäre ein zeitgesteuertes Zutrittssystem für Konferenzräume und Seminarräume eine große Bereicherung. Wer ist nicht schon des öfteren bei Seminaren oder Workshops vor verschlossenen Türen gestanden oder musste sein ganzes Hab und Gut herumtragen weil die Türen zu den Räumen nicht abgeschlossen wurden.

Die Benutzung könnte später über das Accounting Management abgerechnet werden.

Kapitel 5

Zusammenfassung

Hans-Peter Braun zitiert in [Brau07] Krummacker, den Vorsitzenden des deutschen Verbandes für Facility Management:

„*Der Begriff Facility Management ist eindeutig definiert, wird jedoch zur Zeit nicht ausreichend kommuniziert und der beteiligten Fachöffentlichkeit nahegebracht*“

So lässt sich erklären, dass in Regel Gebäudemanagement mit dem Begriff Facility Management verwechselt wird. Der wesentliche Unterschied ist im Gebäude Management werden alle Sachressourcen außer dem Gebäude selbst ausgeschlossen und nur die Nutzungsphase berücksichtigt.

Normen und Richtlinien entstehen in der Regel in einem langwierigen Prozess. Unabhängige Institutionen untersuchen die Thematik. Das Normungsinstitut versucht viele Interessen zu berücksichtigen und definiert Standards in einer Norm oder Richtlinie. Das Ergebnis ist möglichst unabhängig definiert. Daher eigneten sich diese Regelwerke sehr gut als Basis für eine unabhängige Untersuchung der beiden großen Themenblöcke.

Facility Management ist ein ganzheitlicher Managementbegriff. Es behandelt alle Ressourcen rund um eine Immobilie und die materielle/immaterielle Infrastruktur einer Unternehmung. Die Sachressource steht im Mittelpunkt. Betrachtungszeitraum ist der gesamte Lebenszyklus von der Idee, Planung, Bau, Nutzung bis zur Verwertung. Die Nutzung ist längste und kostenintensivste Phase. Das und die Tatsache, dass Netzwerk Management ausschließlich die Nutzungsphase

berücksichtigt, waren der Anlass die Untersuchung auf die Nutzungsphase und das Gebäude Management einzuschränken.

Die wesentlichen Konzepte des Netzwerk Managements hat die ISO im OSI System Management in fünf Functional Areas, kurz FCAPS, zusammengefasst. Das Fault Management überwacht Ressourcen und benachrichtigt im Fehlerfall. Das Configuration Management verwaltet alle Ressourcen. Die Benutzung der Ressourcen wird über das Accounting Management abgerechnet. Das Performance Management überwacht die Verfügbarkeit der Ressourcen. Der Zugriff auf Ressourcen wird vom Security Management gesteuert.

Diese Techniken lassen sich in allen drei Bereichen des Gebäude Managements sehr gut anwenden. Das technische Gebäude Management bietet eine Reihe von Einsatzmöglichkeiten für das Fault, Configuration und Performance Management. Fault, Accounting, Performance und Security Management finden im Infrastrukturellen Gebäude Management Einsatzmöglichkeiten. Während naturgemäß im Kaufmännischen Gebäude Management das Accounting Management im Vordergrund steht.

Die Praktische Umsetzung der Ideen im Hotelumfeld mit HHSC belegt die These in der Praxis. Für diesen Zweck würde das OpenSource Netzwerk Management System Nagios erweitert. Die Anbindung an bestehenden Gebäude Management Systeme wurde an Hand von Steuer Programmierbaren Steuerungen, kurz SPS, realisiert. Die Realisierung zeigt der Einsatz von Poll-driven, als auch Event-driven Management macht auch im Gebäude Management Sinn. So ist ein Alarm am besten mit den Techniken aus dem Event-driven Management anzubinden. Poll-driven Management ist hervorragend geeignet für die Überwachung, beispielsweise einer Markise.

Eine geschickte Verwendung bestehender Module im HiPath Hospitality Service Center bewährte sich bei der Realisierung der Forderung aus den fünf Funktional Areas. So kommen auch alle Techniken aus dem Netzwerk Management im Endprodukt im speziellen im Facility Management zum Einsatz.

Anhang A Standards

Telecommunications Management Network (TMN)

- M.3000 Overview of TMN Recommendations
- M.3010 Principles of a Telecommunications Management Network
- M.3020 TMN Interface Specification Methodology
- M.3100 Generic Network Information Model
- M.3180 Catalogue of TMN Management Information
- M.3200 TMN Management Services: Overview
- M.3300 TMN Management Capabilities
- M.3400 TMN Management Functions

OSI Model and Notation

- ITU-T X.208/ISO-8824 Specification of Abstract Syntax Notation One (ASN.1)
- ITU-T X.209/ISO-8825 Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)

OSI Structure of Management Information

- ITU-T X.700/ISO-7498 Management Framework
- ITU-T X.701/ISO-10040 System Management Overview
- ITU-T X.710/ISO-9595 Common Management Information Services (CMISE)
- ITU-T X.711/ISO-9596-1 Common Management Information Protocol Specification
- ITU-T X.720/ISO-10165-1 Management Information Model
- ITU-T X.721/ISO-10165-2 Definition of Management Information
- ITU-T X.722/ISO-10165-4 Guidelines for the Definition of Managed Objects (GDMO)

OSI Service Elements

- ITU-T X.219/ISO-9072-1 Remote Operations: Model, Notation and Service Definition
- ITU-T X.229/ISO-9072-2 Remote Operations: Protocol Specification
- ITU-T X.217/ISO-8649 Service Definition for the Association Control Service Element
- ITU-T X.227/ISO-8650 Connection-Oriented Protocol Specification for the Association Control Service Element

Systems Management Functions

- X.730/ ISO 10164-1 Object Management Function
- X.731/ ISO 10164-2 State management Function
- X.732/ ISO 10164-3 Attributes for Representing Relationships
- X.733/ ISO 10164-4 Alarm Reporting Function
- X.734/ ISO 10164-5 Event Report Management Function
- X.735/ ISO 10164-6 Log Control Function
- X.736/ ISO 10164-7 Security Alarm Reporting Function
- X.737/ ISO 10164-14 Confidence and Diagnostic Test Categories
- X.738/ ISO 10164-13 Summarization Function
- X.739/ ISO 10164-11 Metric Objects and Attributes
- X.740/ ISO 10164-8 Security Audit Trail Function
- X.741/ ISO 10164-9 Objects and Attributes for Access Control
- X.742/ ISO 10164-10 Usage Metering Function for Accounting Purposes
- X.745/ ISO 10164-12 Test Management Function
- X.746/ ISO 10164-15 Scheduling Function
- X.750/ ISO 10164-16 Management Knowledge Management Function
- X.751/ ISO 10164-17 Changeover Function

Literaturverzeichnis

5.1 Literatur

[Asch08] R. Aschauer, Hospitality Portfolio Präsentation,iSEC, This is a Siemens internal Document not available to the public. Wien, 2008

[Blac92] U. Black, Network Management Standards, 1. Auflage 1992, McGraw-Hill Inc., New York, 1992

[Brau07] H-P. Braun, Facility Management, Erfolg in der Immobilienbewirschaftung, 5. Auflage, Springer-Verlag, Berlin Heidelberg, 2007

[Chie03] G. Chiesa, Network Management, Implementation concept for distributed mobile network architecture, Diploma Thesis Politecnico Di Milano, 2003

[CIBM08] Combined IBM Systems Information Center, http://publib.boulder.ibm.com/infocenter/systems/index.jsp, September 2008

[Cisc03] Cisco Systems Inc., Internetworking Technologies Handbook 4. Auflage, Cisco Press, 2003, Indianapolis, 2003

[HHSC-A] Siemens, HiPath Hospitality Service Center Administrationsanleitung, Version 2.5, delivered with a licensed copy of HHSC, Wien 2007

[HHSC-B] Siemens, HiPath Hospitality Service Center Bedienungsanleitung, Version 2.5, delivered with a licensed copy of HHSC, Wien 2007

[HHSC-S] Siemens, HiPath Hospitality Service Center Servicehandbuch, Version 2.5, delivered with a licensed copy of HHSC, Wien 2007

[HHSCP] Siemens, Pflichtenheft zum HiPath Hospitality Service Center, This is a Siemens internal Document not available to the public.

[Hofm07] J. Hofmann, Masterkurs IT-Management, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden, 2007

[Joze05] N. Jozefiak, Performance of Integrated Network Management Architektures in Next Generation Networks, Dissertation TU Wien, 2005

[Kahl01] H. Kahlen, Facility Management 1, Entstehung , Konzeptionen, Perspektiven, 1. Auflage, Springer Verlag, Berlin Heidelberg, 2001

[Kope97] H. Kopetz, Real-Time Systems, 1. Auflage 1997, Kluwer Academic Publishers, Massachusetts, 1997

[Kris05] V. Krishnamoorthy, Evnet-Driven Service-Oriented Architekture for an Agile and Scalable Network Management System, Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP05), IEEE, 2005

[Li05] Mo Li, Networkmanagement Challenges for Next Generation Networks, Proceedings if the IEEE Conference on Local Computer Networks 30th Anniversary (LCN05), IEEE, 2005

[Mosl01] W. Moslener, E. Rondeau, Facility Management 2, Verfahren, Praxis, Potentiale, 1. Auflage, Springer Verlag, Berlin Heidelberg, 2001

[Nagi08] Nagios, http://www.nagios.org, September 2008

[Nävy06] J. Nävy, Facility Management, 4. Auflage, Springer-Verlag, Berlin Heidelberg, 2006

[Otto06] J. Otto, Wissensintensives Facility Management, 1. Auflage, Expert Verlag, Renningen, 2006

[Rama98] L. Raman, OSI System and Network Management, IEEE Communications Magazine pp. 46-53, März 1998

[Ruzi04] D. Ruzicka, Nagios Alles im Blick, Linux Magazin, Sonderheft 3/2004, 2004

[Scha05] R. Schach, K. Kabitzsch, V. Höschele, J. Otto, Integrieretes Facility Management, 1. Auflage, Expert Verlag, Renningen, 2005

[Schi98] G. Schildt, W. Kastner, Prozeßautomatisierung. 1. Auflage 1998, Springer-Verlag, Wien, 1998

[Schw06] T. Schwenkler, Sicheres Netzwerkmanagement, 1. Auflage 2006, Springer-Verlag, Berlin Heidelberg, 2006

[SCL05] Siemens Communications Lexikon, 10.03.2005 07:29 UTC, http://www.networks.siemens.de/solutionprovider/_online_lexikon/2/f006362.htm, März 2005

[Slom94] M. Sloman, Network and Distributed System Management, 2. Auflage 1996, Addison Wesley, 1994

[Stal99] W. Stalling, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Third Edition, Addison Wesley Longman Inc., Massachusetts, 1999

[STEP7] Online Hilfe zu Siemens STEP 7-MicroWIN V4.0.1.10 Software, Siemens Energy and Automation, Inc. 2008

[Swis96] V. Swisher, Matering Network Management, 1. Auflage 2006, Numidia Press, Fremont, 1996

[Tayl97] E. Taylor, Mulitplatform Network Management, 1. Auflage 1997, McGraw-Hill, New York, 1997

[Zech05] P. Zechel, Facility Management in der Praxis, 5. Auflage, Expert Verlag, Renningen, 2005

5.2 Normen und Richtlinien

[ÖNORM A7000] ÖNORM A7000 Vornorm, Facility Management Grundkonzepte, Ausgabe 2000-12-01, Österreichisches Normungsinstitut, Wien, 2000

[ÖNORM EN ISO 16484-2] ÖNORM EN ISO 16484-2, Systeme der Gebäudeautomation Teil 2 Hardware, Ausgabe 2004-10-01, Österreichisches Normungsinstitut, Wien, 2004

[DIN 32736] Deutsche Norm, DIN 32736, Gebäudemanagement Begriffe und Leistungen, DIN Deutsches Institut für Normung. Berlin 2000

[GEFMA 100] GEFMA 100 Entwurf 2004-07, Facility Management Grundlagen, GEFMA Deutscher Verband für Facility Management e.V., Bonn 2004

[ITU-T X.200] The text of ITU-T Recommendation X.200 was approved on 1st of July 1994. The identical text is also published as ISO/IEC International Standard 7498-1.

[ITU-T X.700] ITU-T Recommendation X.700 and ISO/IEC 7498-4: Information technology – Open Systems Interconnection – Management framework were developed in close collaboration and are technically identical.

[ITU-T X.701] The ITU-T Recommendation X.701 was approved on the 9th of August 1997. The identical text is also published as ISO/IEC International Standard 10040

[ITU-T X.731] The ITU-T Recommendation X.731 State management Function was approved in January 1992. The identical text is also published as ISO/IEC International Standard 10164-2

[RFC1157] Internet Engineering Task Force, Network Working Group, RFC 1157 A Simple Network Management Protocol (SNMP), Mai 1990