Konzeption eines modularen und vernetzten Zugangskontrollsystems auf Basis der Produktfamilie SIPORT.

Thomas J. Wilke

03.06.1996

Zusammenfassung

Die vorliegende Diplomarbeit beschreibt Zielsetzungen und Konzeption für ein Zugangskontrollsystem des Produktbereichs SIPORT, dessen Leistungs- und Sicherheitsniveau frei konfigurierbar ist und bereits vorhandene Komponenten integriert.

Nach einer Einleitung, die in die Thematik einführt, wird eine Systembegründung gegeben und eine Systemanalyse dargestellt, welche die Basis für den darauffolgenden Systementwurf darstellt. Den Abschluß bildet ein Ausblick auf vorgesehene und denkbare Erweiterungen, die zusätzliche Themenbereiche bis hin zu einem hoch integrierten System abdecken.

Grundlage für diese Arbeit sind konkrete Projekte der SIEMENS AG, Abteilung ANL 425-KRK, Arbeitsgruppe Systemsoftwareentwicklung SIPORT unter der Leitung von Herrn Dipl. Ing. Hans Joachim Mundt. Die Arbeit wurde von der Universität Karlsruhe durch Herrn Prof. Dr.-Ing. Zorn und von der SIEMENS AG durch Herrn Dipl-Ing. Mundt betreut.

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einleitung

Der Produktbereich SIPORT der SIEMENS AG befaßt sich mit der Einrichtung, Wartung, Entwicklung und Produktpflege von Zugangskontrollsystemen, die in unterschiedlichen Einsatzgebieten mit variierenden Sicherheitsniveaus zur Anwendung kommen. Drei wesentliche thematische Einsatzkategorien sind :

1. **Dokumentation** im Bereich Arbeitszeiterfassung, Gerätewartung und Einsatz.
2. **Objektschutz** von Werksgeländen, Gebäuden, gelegentlich genutzten Räumen (Aktenlager oder ähnliches), Archiven, Labors, Rechenzentren mit Sicherheitsbereichen und Datenarchiven, Banken mit verschiedenen Sicherheitsbereichen, Museen, Fertigungsstätten mit Sicherheits- und Gefährdungsbereichen, Informationssystemen zur Eingabe, Ausgabe oder Änderung von Daten, Militär mit Bereichen besonderer Geheimhaltung.
3. **Nutzungsberechtigungen für Dienstleistungen (DNB[1])** auf Wert- oder Kreditbasis für Transportdienste (öffentliche Verkehrssysteme, Beförderungseinrichtungen von Skigebieten), Verleihdienste (Büchereien, Sportausrüstungen, ...), Eintritt (Schwimmbäder, Freizeitparks, Messen, ...), Benutzung von Schließfächern, Parkplätzen, Kantinen, Hotelzimmern, etc.

Die meisten Systeminstallationen, insbesondere mittlere oder große, decken mehrere der genannten Themenbereiche ab. Sie zeigen die Tendenz für zukünftige Systemarchitekturen auf, hin zu einer Systemintegration interthematischer, bisher autonomer Teilsysteme, die in ihrem Zusammenwirken ein makroskopisches Gesamtsystem bilden.

Die wesentliche Funktionsweise eines Zugangskontrollsystems kann durch die folgenden Grundfunktionen beschrieben werden:

1. **Registrierung bzw. Verifizierung** der Berechtigung oder Identität. Dies wird häufig mit Plastikkarten und Kartenlesern an den Kontrollstellen durchgeführt. Drei Kartentypen sind gebräuchlich :
   - *Barcodekarten*; Karten, mit einem Strichcode.
   - *Magnetstreifenkarten*; Karten mit einem Magnetstreifen, der gelesen und beschrieben werden kann.

[1] Im weiteren Text wird DNB abkürzend für Dienstleistungsnutzungsberechtigungen verwendet.

- *CHIP-Karten*; mit passiver Speicherelektronik oder aktivem Prozessor und Speicher.

Die Karten werden in den Leser gesteckt, der per Oberflächenabtastung (Barcodekarten), induktiv (Magnetstreifen-, CHIP-Karten), durch Infrarotabtastung oder mit elektrischen Kontakten (CHIP-Karte) die Karten liest und/oder beschreibt. Die gelesenen Daten der Karte werden geprüft und je nach System gespeichert und Änderungen gegebenenfalls auf die Karte geschrieben. Barcodekarten werden kaum noch eingesetzt: sie können lediglich gelesen werden, lassen sich relativ leicht duplizieren und sind kaum billiger als Magnetstreifenkarten. Welcher Kartentyp zum Einsatz kommt, hängt von den geforderten Eigenschaften wie Speicherkapazität, Schreib- und Lesegeschwindigkeit, Rechengeschwindigkeit (bei aktiven Prozessorkarten), Handhabungskomfort sowie vom Preis ab. Besonders hohe Benutzerakzeptanz genießen berührungsfreie CHIP-Karten. Diese Karten müssen lediglich in eine definierte Umgebung des Lesers gebracht werden, um gelesen oder beschrieben zu werden. Man unterscheidet:

- "Proximity-Karten", auf die in 4 bis 10 Zentimetern Abstand von der Leserantenne lesend und schreibend zugegriffen werden kann,
- "Handsfree-Karten", die in einem Umkreis bis zu einem Meter von der Leserantenne gelesen und derzeit in einem Abstand von 4 bis 10 Zentimetern beschrieben werden können. In absehbarer Zeit wird es jedoch auch Karten mit gleichem Lese- und Schreibabstand geben.

Alternativ oder zusätzlich zu den Karten werden entweder einzelne oder in Kombination mehrere Überprüfungsmethoden verwendet, wie Validierung eines persönlichen Codes, Fingerabdruckvergleich, biometrische Verfahren oder Bildvergleich.

2. **Reaktion auf die Registrierung bzw. Verifizierung.** Mit Hilfe von Zustandsdaten und des Auswertungsergebnisses der Registrierung bzw. Verifizierung an der Kontrollstelle wird durch das Zugangskontrollsystem berechnet, welche Prozesse als Reaktion zu starten sind. Die Komplexität und Thematik der Reaktion kann je nach System, Kontrollstelle und Ereignis variieren. Das Öffnen oder Schließen von Barrieren, die Auslösung eines Alarms oder die Anzeige eines Textes auf einem Display sind Beispiele für einfache Reaktionen. Komplexere Varianten könnten aus einer Folge von Zustandsüberprüfungen und -änderungen bestehen, die vor und/oder nach Öffnung oder Schließung einer Barriere durchgeführt werden. Das Beispiel eines Forschungslabors, in dem sich Besucher nur in Begleitung von autorisierten Betriebsangehörigen aufhalten dürfen, soll zur Veranschaulichung dienen. Versucht der letzte autorisierte Mitarbeiter, das Labor über die Ausgangskontrolle zu verlassen, prüft das System, ob sich noch Besucher im Labor aufhalten. Fällt die Prüfung positiv aus, bleibt die Tür verschlossen, und es wird dem Laboranten auf einem Display an der Kontrollstation mitgeteilt, aus welchem Grund die Sperrung erfolgt. Hält sich kein Besucher mehr im Labor auf, wird die Ausgangstür geöffnet, die Raumbeleuchtung abgeschaltet, geöffnete Fenster geschlossen, die Alarmanlage scharf gemacht und das Sicherheitspersonal

informiert, daß alle Angestellten die Laborräumlichkeiten verlassen haben. Man kann sich leicht vorstellen, daß noch kompliziertere Prämissen und Reaktionen für andere Bereiche des Objektschutzes oder bei DNB-Systemen notwendig sind.

Die beschriebene Grundfunktionalität wird sich für die Benutzer zukünftiger Zugangskontrollsysteme nicht wesentlich ändern. Allerdings werden sich erhebliche Änderungen in der Arbeitsweise zukünftiger Systeme vollziehen. Großer Entwicklungsbedarf besteht in der ständigen Sicherstellung der Systemintegrität und der intelligenten Umsetzung der Sicherheitspolitik, bei der das System selbständig Prämissen und Reaktionen auf Ereignisse entwickelt, Sicherheitslöcher erkennt und beseitigt. Für DNB-Systeme werden sogenannte Multifunktionskarten eingeführt, die es ermöglichen, mit einer einzigen Karte mehrere Zugangskontrollsysteme unterschiedlicher Dienstanbieter zu benutzen, die selbst Systeme verschiedener Hersteller einsetzen.

Die Themenbereiche Systemintegrität und intelligente Umsetzung der Sicherheitspolitik sind Schlüsselgebiete, an denen die Qualität zukünftiger Zugangskontrollsysteme zu messen sind. Um effiziente und praktikable Lösungen anbieten zu können, wird der Einsatz von Methoden und Theorien der Bereiche Systemtechnik und -sicherheit, kognitive und deduktive Systeme sowie Riskmanagement unerläßlich sein.

Kapitel 2

Systembegründung

Die Systembegründung befaßt sich mit den Zielen und Randbedingungen des neuen SIPORT-Zugangskontrollsystems; hieraus werden Konzeptionsrichtlinien entwickelt und eine Einsatzbegründung für Entwicklungswerkzeuge und Implementierungskomponenten gegeben. Mögliche Einsatzsituationen und Verwendungsmöglichkeiten des neuen Zugangskontrollsystems werden am Beispiel dreier konkreter Einsatzszenarios beschrieben und diskutiert.

2.1 Zielvorstellung und resultierende Konzeptionseigenschaften.

Aufgrund der praktischen Erfahrungen mit dem bestehenden SIPORT- Zugangskontrollsystem, welches bei größeren Systeminstallationen Flexibilitätsengpässe aufzeigt, entschloß man sich bei Siemens im Herbst 1995 zu einer Neuentwicklung. Zielsetzung dieser Neuentwicklung ist es, für existierende und neue Produktbereiche über ein System zu verfügen, mit dem die gegenwärtigen Ansprüche leichter umgesetzt und zukünftige Anforderungen besser bewältigt werden können. Zur Realisierung eines solchen Systems setzt man auf eine Architektur, die zum einen eine große Flexibilität in den Bereichen Leistungs-, Größen- und Sicherheitsskalierbarkeit bietet, zum anderen in der Lage ist, autonome Teilsysteme zu einem großen Gesamtsystem zu integrieren.

Die wohl wichtigste Forderung von seiten des Produktmanagements an die Entwickler war, so schnell als möglich ein stabiles Grundsystem zu entwickeln. Es soll die elementaren Aufgaben der Zutrittskontrolle abdecken und in seiner Funktionalität nach und nach kohärent zur Basisarchitektur erweitert werden können. Ein Baukastensystem von Funktionseinheiten soll entstehen, welches die Möglichkeit bietet, Systeminstallationen auf die unterschiedlichsten Anforderungsprofile der Zutrittskontrollthematik zu konfigurieren. Eine weitere wichtige Anforderung an das neue System ist eine umfassende Systemsicherheit. Sie muß zum einen Fehlertoleranz des Gesamtsystems bei Ausfall einer oder mehrerer Komponenten gewährleisten, der durch physikalische oder implementierungsbedingte Mängel sowie durch mutwillige Sabotageakte begründet sein kann. Zum anderen muß sie Angriffen von autorisierten oder unautorisierten Personen widerstehen können, die versuchen, das System aktiv oder passiv zu bedrohen oder gar dessen Funktionsweise durch Modifikationen von Teilen zu ändern. Kompatibilität zu gängigen Standards, der Betrieb von heterogenen Rechnersystemen in

Installationskonfigurationen sowie Codeverifizierbarkeit zur Erlangung von Qualitäts- oder Sicherheitszertifikaten sind weitere Systemeigenschaften, die beim Systementwurf berücksichtigt werden sollen.

Die geschilderten Zielvorstellungen über die Eigenschaften und Funktionalität des neuen SIPORT-Zugangskontrollsystems sollen durch die folgenden Konzeptionseigenschaften und -richtlinien konkretisiert werden:

- **Offene Systemarchitektur,** die die schnelle Verfügbarkeit des elementaren Systems sicherstellen und zukünftige Systemerweiterungen und Modularität ermöglichen soll, durch:

  1. Bereitstellung von Methoden, Funktionen und Schnittstellen zur Integration von systemfremden und autonom arbeitenden Komponenten.
  2. Offenlegung von Wirkungsprinzipien und Schnittstellen, um andere Entwickler in die Lage zu versetzen, kompatible Subsysteme und Funktionsmodule zu entwickeln.

- **Schichtenarchitektur,** die dem System hohe Sicherheit, Flexibilität und Aktualität verleihen soll, da sie:

  1. System- und Codestabilität erhöht sowie systematische Fehlerdeduktion unterstützt: der Code jeder Schicht kann nur auf den der jeweils darunterliegenden zugreifen. Jede Schicht, beginnend bei der untersten, kann eine nach der anderen systematisch geprüft und korrigiert werden, bis das System stabil läuft.
  2. effiziente und leichte Portabilität auf andere Rechner-, Netzwerkarchitekturen, Betriebssysteme und Netzwerkprotokolle sicherstellt.
  3. ständige Fortentwicklung aller Ebenen ermöglicht, ohne darüber- oder darunterliegende Schichten direkt beeinflussen zu müssen.

- **Mikrokern,** der es ermöglicht, zukünftige Hardwarekomponenten ins System kohärent einzubinden. Es handelt sich um einen Miniserver, der die elementarsten Funktionen des Systemkerns bereitstellt. Er kann auf kleinen Rechnerplattformen mit geringer Rechenleistung und/oder geringem System- bzw. Massenspeicher arbeiten, so daß er als Firmware-Aufsatz in Lesern oder anderer Peripherieelektronik eingesetzt werden kann.

- **Modulare Funktionskomponenten** werden durch abgeschlossene Module repräsentiert. Jedes dieser Module ist eigenständig und stellt ein API zur Verfügung, das von anderen Komponenten oder Anwenderapplikationen — sofern sie Rechte dazu besitzen — benutzt werden kann. Die Abgeschlossenheit ermöglicht einzelne Modulzertifizierungen im Hinblick auf Sicherheits- und Qualitätseinstufung. Da die Komponenten in beliebiger Kombination und Anzahl arbeiten, ist eine beliebige Funktionskonfiguration und Größe konkreter realer Systeme möglich.

- **Verteilte Systemarchitektur**, ermöglicht die Leistungs- und Sicherheitsskalierbarkeit. Leistungssteigerung kann durch

1. den Einsatz schnellerer Hardwarekomponenten und/oder besserer Algorithmen,
2. die Erhöhung der Anzahl von eingesetzten Hardwarekomponenten

erreicht werden. Das neue SIPORT-System soll beide Varianten abdecken. Die erste durch die einfache Portierbarkeit bzw. Modularität und die zweite durch die Fähigkeit zum "distributed computing".
Im Bereich Sicherheit ermöglicht sie Integritätsprüfung und Fehlertoleranz von Komponenten des Systems. Effizientere Nutzung der Hardwareressource ist möglich, und die schrittweise Erweiterung bestehender Installationen gestaltet sich einfach.

- **Verwendung von und Kompatibilität zu Standards** soll die Portabilität und Stabilität erhöhen sowie die Entwicklungszeit verkürzen. Es wird, nach Prüfung der Zweckmäßigkeit, auf bewährte Komponenten aufgesetzt. Man baut auf Methoden und Wirkungsprinzipien, die bereits ausreichend Stabilität bewiesen haben und gängig eingesetzt werden.

- **Codemanagement.** Es soll die Qualität und Entwicklungseffizienz der Software dokumentieren und analysieren helfen, die Wartbarkeit und Weiterentwicklung sichern, die Erstellung von Anwenderhandbüchern unterstützen und Know-how akkumulieren und schützen. Es ist Grundlage für Zertifizierungen in den Bereichen Qualitätssicherung und Sicherheitseinstufung.

Die vorgestellten Zielsetzungen und Richtlinien sind nicht immer und überall kompromißlos anzuwenden. Beispielsweise ist die Programmierung einer Benutzerschnittstelle für ein MS Windows System in portierbarem C nicht sinnvoll. Diese Komponente ist sehr speziell. Ihre innere Struktur ist nicht auf andere grafische Benutzeroberflächen wie XWindows übertragbar. Natürlich gibt es Werkzeuge wie Whatcom, die mehrere Plattformen mit demselben Code abdecken. Die Praxis zeigt aber, daß die Einschränkungen und Kompromisse, die bei der Entwicklung mit diesen Werkzeugen gemacht werden müssen, vom Benutzer nicht oder selten toleriert werden. Effizienter ist es, an dieser Stelle 4GL-Sprachen einzusetzen, die aufgrund ihrer mächtigen Funktionen eine schnellere Entwicklung zulassen und in der Regel einen stabileren Code liefern. Auf der anderen Seite wäre es fatal, den Mikrokern in einer 4GL-Sprache oder C++ zu implementieren. Hier muß portabler, POSIX-konformer Code gefordert werden.

Als Anhaltspunkt für die Aufweichung der Richtlinien kann die Schichtebenenzugehörigkeit der zu implementierenden Komponente dienen. Je höher die Ebene, desto eher sollten sinnvolle Kompromisse gemacht werden. Entscheidendes Kriterium ist die Wiederverwendung einer Komponente im System. In der Regel werden Komponenten niedriger Schichten vielfach direkt oder indirekt durch Komponenten höherer Schichten wiederverwendet. Die Funktionen dieser Komponenten müssen daher auf unterschiedlichen Systemplattformen bereitgestellt werden, was eine einfach zu portierende Implementierung erforderlich macht.

Keine Kompromisse sollten beim *Codemanagement* und der *implizierten Codedokumentation* gemacht werden. Sie sollten der Verantwortung eines erfahrenen Entwicklers

übertragen werden. Mit diesem Management lassen sich - sinnvoll betrieben - Probleme frühzeitig erkennen; auch liefert es bei projektrelevanten Entscheidungen wertvolle Hinweise.

2.2 Entwicklungsumgebung und Erstimplementierungskomponenten

Die beschriebene Zielvorstellung des neuen Zugangskontrollsystems birgt erhebliche Fallstricke, die nur durch sorgsame Analyse, Planung, Implementierung und deren ständige Verifikation und Rückkopplung umgangen werden können. Einer dieser kritischen Punkte ist die Auswahl der Basiskomponenten, auf die die Funktionseinheiten des Systems aufgesetzt werden sollen. Erfüllt eine dieser Komponenten die aufgezeigten Leitlinien nicht, können Teile oder die gesamte Zielsetzung nur bedingt oder garnicht verwirklicht werden. Einen weiteren wesentlichen Einfluß haben diese Subsysteme auf die Entwicklungszeit. Je nach Hersteller und Produkt variieren Mächtigkeit und Umfang der unterstützten Funktionen, Verfügbarkeit von Informationen über das System (Dokumentation, Hot-Line, andere Supportdienstleistungen) und die Qualität der einsetzbaren Entwicklungswerkzeuge. Aufgrund der Bedeutung der Basiskomponenten sollen diese im folgenden Abschnitt vorgestellt und eine kurze Begründung für ihren Einsatz gegeben werden.

2.2.1 Hardware

Die Hardwarekomponenten eines Zugangskontrollsystems lassen sich in zwei Kategorien einteilen:

1. passive Komponenten: Sie erfassen, transportieren und/oder transformieren Signale unterschiedlicher physikalischer Ebenen, *ohne* deren logische Bedeutung und/oder Darstellung durch *eigene Rechenleistung* zu verändern. Beispiele sind Sensoren, Detektoren, Stellglieder, visuelle und akustische Baugruppen.

2. aktive Komponenten: Sie erzeugen aus Eingangsgrößen eigenständig — in der Regel mit eigener Rechenleistung — Ausgangsgrößen. Die Eingangs- und Ausgangsgrößen bilden dabei meist unterschiedliche logische Bedeutungsklassen, z.B. Kartenleser, die selbständig prüfen und Entscheidungen generieren.

Rechnersysteme

Rechnersysteme gehören aufgrund ihrer Eigenschaft, über Rechenleistung zu verfügen, der aktiven Klasse an. Alle im System eingesetzten Computer basieren auf einer PC-Architektur. Das Spektrum reicht vom ISA-Bus mit i386-Prozessor bis hin zum PCI-Bus mit Pentium Prozessor. Entscheidende Kriterien für die Wahl dieser aus technischer Sicht in die Jahre gekommenen Architektur sind:

- günstiger Preis
- leichte Verfügbarkeit

- durchgängige binäre Abwärtskompatibilität
- großes Spektrum von Rechnerherstellern, Anbietern von Erweiterungskarten unterschiedlichster Funktionalität; zahlreiche Peripheriegerätehersteller, die durch Treiber und/oder Steckplatinen diese Architektur unterstützen.
- große Produkt- und Entwicklungsressourcen für Software
- große Betriebserfahrung und Stabilität
- einfache Handhabbarkeit durch Plug and Play Technologie moderner Systeme
- große Installationszahlen

Ein Nachteil ist die veraltete Basisarchitektur, die zwar durch schnellere und erweiterte Prozessoren und Bussysteme modernisiert wurde, der jedoch bisher eine moderne, homogene und schnelle Gesamtrechnerarchitektur versagt blieb.

Für leistungskritische Bereiche, die auch durch Mehrprozessorboards im PC-Bereich nicht zu befriedigen sind, sollen DEC-Alpha Workstations und/oder Server eingesetzt werden. Sie besitzen einen bis vier superskalare 64-Bit RISK Prozessoren mit einer Taktung von 166 bis 400 MHz und einem 64-Bit PCI Bussystem.

Netzwerkhardware

Netzwerke bestehen aus passiven Komponenten (Kabel, Stecker, usw.), die durch aktive Komponenten (Bridges oder Gateways) verbunden sein können. Es sollen alle gängigen Netzwerkarchitekturen sowie deren Betrieb in heterogenen Konfigurationen unterstützt werden. Das Spektrum reicht von einfachen seriellen Zweidraht- und analogen Telefonleitungen über Richtfunk, Ethernet, Tokenring bis hin zu ISDN, FDDI und ATM.

Spezielle Zugangskontrollperipherie

Bei Zugangskontrollsystemen werden spezielle Peripheriekomponenten an den Kontrollstellen und sicherheitsrelevanten Raumzonen benötigt. Typische Geräte sind Kartenleser, Fingerprintscanner, Sensoren, Detektoren und Stellglieder. Sie sollen die Einhaltung der Sicherheitspolitik gewährleisten sowie Verstöße erkennen und deren Ursache analysieren helfen.

Komponenten des existierenden SIPORT-Systems. Die Identifikationskomponenten wie Kartenleser und Fingerprintscanner des alten SIPORT-Systems stellen ein Sicherheitsproblem dar, da die Daten der von ihnen registrierten Ereignisse mit einem nur einfach gesicherten Datagrammdienst und unverschlüsselt übertragen werden. Insbesondere die Klartextübertragung kann in Hochsicherheitsbereichen nicht toleriert werden. Die Fehlertoleranz bei Ausfall von Rechnerkomponenten ist hingegen befriedigend.

Die Kartenleser sind passive Komponenten, die durch eine serielle Leitung (RS485) oder Partyline entweder direkt mit einem Rechner oder indirekt über eine Ethernet-Kopplungseinheit (E-Box) und/oder nur über eine Unterstation mit einem Rechner

verbunden sind. Diese Unterstationen, von denen es mehrere Typen und Ausbaustufen gibt, können unabhängig vom Rechner Zugangsberechtigungskontrollen durchführen. Sie sind batteriegepuffert, besitzen einen eigenen Prozessor, Speicher, I/O-Schnittstellen für Sensoren und Stellglieder sowie mitunter ein eigenes Netzwerkinterface. Alle Leser, Sensoren und Stellglieder können nur über Rechner erreicht werden, auf denen ein spezielles Betriebssystem "SIPORT OS-M" läuft. Nur durch das OS-M Betriebssystem können die Unterstationen verwaltet und parametriert werden.

Neue Komponenten. Durch einen neuen aktiven, batteriegepufferten Kartenleser will man auf die Option der Unterstationen verzichten. Der Kartenleser besteht aus einer Steckkartenlesereinrichtung, die unterschiedliche Kartentypen lesen kann, einer PC-Mutterplatine, die eine Netzwerkkarte aufnehmen kann, zwei seriellen Schnittstellen, mehreren Schalteingängen und Relaisschaltausgängen. Optional kann ein Massenspeicher eingebaut, eine Tastatur und ein LCD-Display angeschlossen werden. Für die Softwareentwickler stellt sich der aktive Leser wie ein low-power PC dar. Damit können die Sicherheitsprobleme des alten Systems durch die Verwendung eines Authentifikationsdienstes und eines gesicherten Netzwerkprotokolls eleminiert und so ein homogenes Sicherheitskonzept im gesamten Zugangskontrollsystem verwirklicht werden. Die Erweiterung des Lesers durch einen Kartenleser für berührungsfreie CHIP-Karten gestaltet sich durch seine Integration ins Gehäuse und die Verwendung einer seriellen Verbindung zum Datenaustausch einfach. Die Ausfallsicherheit wird erhöht, da jeder Leser von jedem Rechner durch die Vernetzung dieser Komponenten erreicht werden kann.

Das neue SIPORT-System wird zukünftig Magnetstreifenkarten, induktive, berührungsfreie Chipkarten und Chipkarten mit elektrischen Kontakten unterstützen.

Die Forderung nach schneller Verfügbarkeit macht es notwendig, in der ersten Entwicklungsphase zunächst die existierenden Komponenten zu verwenden. Wird allerdings eine hohe Ausfallsicherheit gefordert, und muß aktiven und passiven Bedrohungen begegnet werden, ist der Einsatz der aktiven Kartenleser unerläßlich.

2.2.2 Betriebssysteme

Die Wahl des Betriebssystems ist eine zentrale Entscheidung. Durch sie wird wesentlich Sicherheitsfunktionalität, Stabilität, Verläßlichkeit, Performance, Konnektivität, Portierbarkeit, Zertifizierbarkeit, zukünftige Erweiterbarkeit mit schnellerer Hardware bzw. Software und die Entwicklungsgeschwindigkeit des neuen Gesamtsystems festgelegt.

Die Anforderungen an ein modernes Betriebssystem sind:

- Unterstützung des Prozeß- und Threadkonzeptes
- Unterstützung von Multiprozessor-Hardware
- Netzwerkfähigkeit
- Mechanismen, um verteilte Systeme aufbauen zu können
- ausgereifte Schutzmechanismen gegen aktive und passive Bedrohungen

- Fehlertoleranzmechanismen für zu verwaltende Betriebsmittel und eigene Teilsysteme
- Unterstützung gängiger Hardwarekomponenten
- Unterstützung gängiger Softwarestandards
- einfache Portierbarkeit auf unterschiedliche Hardwareplattformen
- Unterstützung durch Informationen zur Konfiguration und Betrieb sowie Produktpflege
- Verfügbarkeit von leistungsfähigen und komfortablen APIs, Werkzeugen und Informationen für die Softwareentwicklung

Es gibt gegenwärtig nur wenige Betriebssysteme, die auf Basis der PC-Hardware diese Anforderungen auch nur annähernd erfüllen. Dies sind zum einen UNIX-Systeme, zum anderen Windows NT.

UNIX-Betriebssysteme sind im Workstation-Bereich sehr verbreitet. Einige dieser Systeme bieten ausgereifte und implementierte Kommunikations- und Sicherheitskonzepte, Softwareentwicklungswerkzeuge sowie Betriebssystemstrukturen, die sehr effizient und stabil sind. Ihr großer Nachteil ist, daß die verfügbaren Produkte nicht softwarekompatibel sind, und laufend mehr oder minder aufwendige Portierungen notwendig werden, will man verschiedene Produkte, neue Versionen oder andere Hardwarearchitekturen unterstützen.

OS/2 von IBM erfüllt die elementarsten Anforderungen an ein modernes Betriebssystem. Bei einer früheren Parallelentwicklung zum bestehenden SIPORT-System wurde bereits deutlich, daß OS/2 für die dargestellte Zielsetzung ungeeignet ist. Windows NT erfüllt alle geforderten Attribute eines modernen Betriebssystems und ist bereits auf verschiedenen CISC- und RISC-Rechnerarchitekturen zu Verfügung.

Windows NT

Windows NT verwirklicht viele Konzepte und Paradigmen der modernen Betriebssystemtechnologie. Eine umfassende Beschreibung kann an dieser Stelle nicht gegeben werden. Dennoch sollen die wichtigsten Eigenschaften und Architekturmerkmale schlagwortartig vorgestellt werden:

- Prozeß- und Thread-orientiertes, preemptives Multiprocessing Betriebssystem mit Client/Server-Architektur auf Basis eines Hardware Abstraction Layers (HAL) mit aufgesetztem Mikrokernel
- es ist objektorientiert: alle Ressourcen, Objekte und Subjekte werden durch Objekte repräsentiert und können in einer uniformen Weise benutzt oder manipuliert werden.
- Virtuelles Memory Management, das jedem Prozeß einen Adreßraum von 4 Gigabyte zur Verfügung stellt.
- unterstützt symmetrisches Multiprocessing

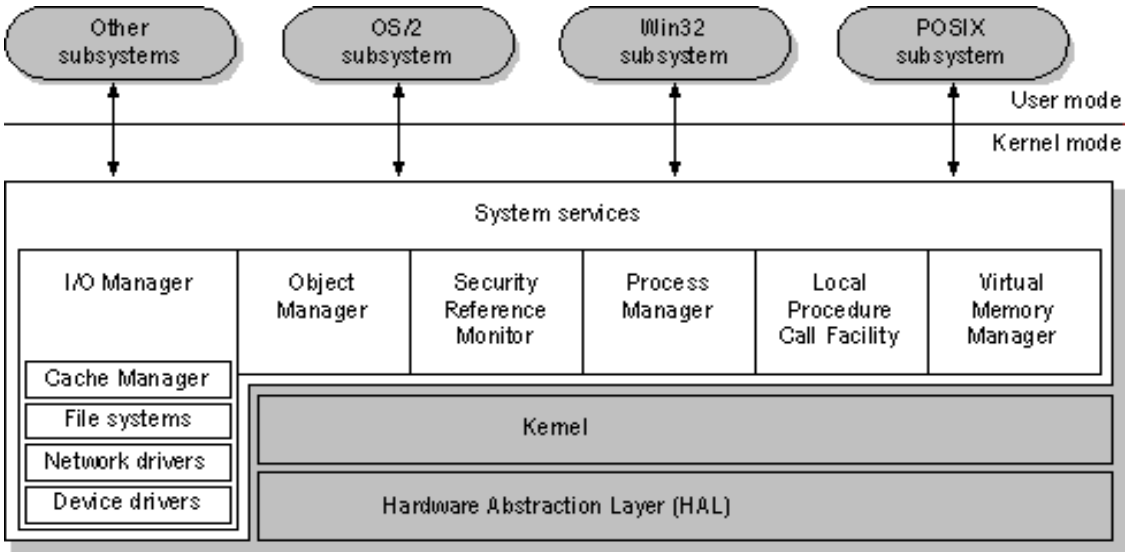
- durch sogenannte "protected subsystems" können MS-DOS, 16-Bit Windows, OS/2 und POSIX Programme unterstützt werden.
- das Sicherheitssubsystem ist vom amerikanischen Verteidigungsministerium C2-zertifiziert.
- unterstützt Unicode
- unterstützt "Structured Exception Handling"
- unterstützt unterbrechungsfreie Stromversorgungseinheit (USV)
- ist multiprotokollfähig: TCP/IP, NetBIOS, IPX
- es werden Winsockets, Named Pipes, Mailslots, RPC, PPP, SLIP, DNS, DHCP-Server und SMNP unterstützt.
- besitzt ein transaktionsorientiertes FileSystem (NTFS), das
  - Partitionen bis zu 2^{64} Clusters zu je 4 kb adressieren kann,
  - Multi Data Streams unterstützt,
  - BTree indexierte Unicode Dateinamen bis 255 Zeichen zuläßt,
  - den POSIX-Dateistandard unterstützt,
  - redundante FATs unterhält,
  - Volume und Stripe-Sets unterstützt,
  - Fehlertolerante Datenträgertreiber besitzt, die RAID von level 0 bis 6 unterstützen,
  - integrierte Datenkompression aufweist.

Eine relativ kurze Zusammenfassung der Architektur und Eigenschaften von Windows NT findet man in [Cor96c], eine sehr anschauliche und ausführliche Darstellung in [Clu93] und [Clu94].

SIPORT OS-M

Das SIPORT OS-M ist ein Echtzeit-Betriebssystem, das beim bestehenden SIPORT--System die Zutrittskontrollkomponenten verwaltet. Da diese Komponenten mitunter vorerst weiterhin verwendet werden sollen, wird OS-M weiterhin eingesetzt. Es wird als autonom arbeitendes Subsystem ins neue Zugangskontrollsystem integriert. Informationen über die interne Organisation und Eigenschaften des OS-M waren weder vom Hersteller noch aus anderen Quellen zu beschaffen. Es arbeitet ausschließlich auf PC-Plattformen und benötigt DOS, um gestartet werden zu können. Seine Funktionen umfassen:

- Verwaltung und Parametrierung der oben beschriebenen Unterstationen
- Verwaltung von Zugangsprofilen und Personenautorisierungen



Abbildung~2.1: Windows NT Executive und seine Komponenten

- statistische Auswertung von Ereignissen
- Priorisierung und Bewertung von Ereignissen
- Verwaltung von Ereignisprofilen
- Erstellung und Ausführung von Batch-Programmen, auf die in Ereignisprofilen referenziert werden kann.

2.2.3 Netzwerkprotokoll

Die Forderung nach beliebiger Größenskalierung des Zugangskontrollsystems erfordert es, ein Netzwerkprotokoll einzusetzen, das erprobtermaßen in der Lage ist, sehr große Netzstrukturen – unabhängig von Übertragungsmedien, Übertragungsverfahren und Vermittlungsverfahren – homogen zu unterstützen und zu verwalten. Mechanismen werden benötigt, die verteiltes Rechnen auf unterschiedlichen Rechner- und Betriebssystemarchitekturen ermöglichen. Es muß an bestehende große nationale oder internationale Computernetze anschließbar sein. Derzeit gibt es nur ein frei zugängliches Netzwerkprotokoll, das die beschriebenen Anforderungen und Eigenschaften erfüllt und selbst zu einem weltweiten Standard geworden ist: TCP/IP, das Protokoll des Internets. Eine tiefergehende Beschreibung über Konzepte, Mechanismen und Implementierungen finden sich in [Com94], [Tho96], [Sta94].

2.2.4 Datenbanksysteme

Die Analyse der Zugangskontrollthematik wird zeigen, daß die benötigten Transaktionen buchungsorientiert sind. Mit zunehmender Systemintegration wird allerdings ein sehr flexibles Datenmodell benötigt, das mit nicht hierarchischen Aggregierungsstrukturen umgehen kann sowie Wiederverwendbarkeit und Rekursivität ermöglicht, um

die themenspezifische Funktionalität homogen ins Gesamtsystem einbetten zu können. Für die Auswahl eines geeigneten Datenbankmanagementsystems kommen daher zwei Datenmodelle in Betracht:

1. das relationale Modell: es ist ein mengenorientiertes Datenmodell. Objekte und Beziehungen der Miniwelt werden durch Strukturierung aus elementaren Datentypen zu Datensätzen (Tupel) modelliert. Mengen gleichartig strukturierter Tupel repräsentieren Relationen, die die Datenbestände bilden. Das relationale Datenmodell zeichnet sich durch seine vergleichsweise leichte Überschaubarkeit und Erlernbarkeit aus.

2. das objektorientierte Modell: Die Objekte bilden eine Gesamtheit von Datenspeicher und Verhaltensrepertoire mit einer zustandsunabhängigen Identität. Daten und Abläufe werden zu einer Einheit verschmolzen. Unter Einbeziehung von Generalisierung und redundanzfreier Aggregierung können anwendungsspezifische Funktionen an Typen gebunden werden (Typisierung). Eine imperative Programmiersprache, die Datendefinition und -manipulation zu einer Einheit zusammenfaßt, ermöglicht die freie Definition monomorpher Operatoren (die Rekursionen einschließen können) und freie Navigation.

Die Entscheidung für das relationale Datenmodell in Form eines SQL Datenbankservers hat mehrere Gründe:

- Die existierenden Produkte sind sehr ausgereift. Für die gegenwärtigen Aufgaben weisen sie eine wesentlich höhere Leistung als verfügbare objektorientierte Datenbankimplementierungen auf.

- SQL ist verbreitet und standardisiert, leicht erlernbar und anwendbar. Objektorientierte Systeme erfordern einen erheblichen Schulungsbedarf der Mitarbeiter.

- Das relationale Modell deckt die gegenwärtigen und die in naher Zukunft zu erwartenden Anforderungen vollkommen ab.

- Mehrere Hersteller bieten genormte SQL-DBMS Implementierungen auf unterschiedlichen Plattformen an.

Beim neuen SIPORT-System soll der Microsoft SQL Server Version 6.0 als zentraler Datenspeicher zum Einsatz kommen. Alternativ sollen auf Kundenwunsch jedoch auch gängige SQL-Serverprodukte anderer namhafter Hersteller verwendet werden können, die den ISO SQL-2-Standard unterstützen.

Der Microsoft SQL Server hat seine Wurzeln in der ehemaligen Zusammenarbeit zwischen Microsoft und Sybase. Er unterstützt den ISO SQL2-Standard und kann bis zu 32 767 Datenbanken verwalten, von denen jede bis zu 1 TB groß und auf maximal 32 Medienfragmente verteilt sein kann. Die Gesamtzahl der verwendbaren physikalischen Medien und die Gesamtgröße jedes logischen Mediums sind unbegrenzt. (Beide Größen sind nur durch die verwendete Anzahl der physikalischen Medien mit einem absoluten Maximum von 32 GB pro logischem Medium begrenzt.) Jedes Medienfragment kann auf einem oder mehreren physikalischen Medien bestehen, wenn irgendeine

Form des Hardware- oder Software-Stripings verwendet wird. Je nach Anwendung und Hardwareumgebung können mehrere hundert Benutzer gleichzeitig bedient werden.

Von den verfügbaren SQL-Servern für Windows NT bindet sich der Microsoft SQL Server derzeit am besten in die Betriebssystemumgebung ein. Er kann die NT-Sicherheitsfunktionen nutzen, wie verschlüsselte Kennwörter, Ablauf von Kennwörtern, domänenweite Benutzerkonten und Windows-basierte Benutzerverwaltung. Benutzer eines SQL-Servers können sich ohne gesonderte Angabe von Login-ID oder Kennwort anmelden. Der Server holt sich die Identifikationsinformationen vom Betriebssystem. Für die Kommunikation mit den Clients verwendet er IPC-Mechanismen wie TCP/IP Windows Sockets, NWLink IPX/SPX und Named Pipes.

Weitere wichtige Eigenschaften sind:

- Triggers
- Stored Procedures
- Benutzerdefinierte Datentypen
- Sensitive Cursors
- Datenbanken können auf austauschbaren Speichermedien abgelegt werden. Dies ermöglicht die Publikation und Verteilung umfangreicher Datenbanken auf preiswerten, schreibgeschützten Medien, wie z. B. CDs. Datenbanken auf austauschbaren Speichermedien lassen sich dynamisch laden und entladen.
- Integrierte Datenreplikation. Mit Hilfe der Replikation können automatisch Kopien von Transaktionsdaten von einem einzelnen Quellserver an einen oder mehrere Zielserver verteilt werden, die sich an einem oder mehreren verteilten Standorten befinden. Ständige Aktualisierungen durch Speichern und Weiterleiten über verteilte Server hinweg erlauben eine Synchronisierung verteilter Daten bei hoher Verfügbarkeit.
- SQL Distributed Management Framework (SQL-DMF) ermöglicht durch eine integrierte Umgebung mit Objekten, Diensten und Komponenten zur Verwaltung von SQL Servern eine anlagenweite Systemadministration. SQL-DMF bietet eine flexible und skalierbare Verwaltungsumgebung, die an spezielle Anforderungen angepaßt werden kann. Es können benutzerbediente Wartungsaufgaben, wie Datenbanksicherung und Warnbenachrichtigungen, durch Dienste übernommen werden, die direkt mit dem SQL Server zusammenarbeiten.

Als lokales DBMS dient die Jet-Engine 3.0. Sie ist wie der SQL-Server ebenfalls transaktionsorientiert, unterstützt SQL92 und die gleichen Sicherheitsmechanismen. Mitunter dient sie dem Client-Rechner als großer Cache für die Serveranfragen. Sie ist eine leistungsfähige Datenbankengine für den lokalen Rechner, benötigt jedoch wesentlich weniger Ressourcen.

Durch die verfügbaren ODBC-Treiber für den SQL-Server als auch für die Jet-Engine können Daten mit anderen Datenbanksystemen und Applikationen ausgetauscht werden, die ODBC unterstützen.

2.2.5 Entwicklungswerkzeuge

Zu Windows NT wird von Microsoft eine gut angepaßte und unterstützende Entwicklungsumgebung bereitgestellt. Sie zeichnet sich durch umfangreiche und mächtige Funktions- und Klassenbibliotheken sowie durch leistungsstarke und komfortable Werkzeuge aus, die alle Belange der Softwareentwicklung, Softwaretestung und des Softwaremanagements abdecken. Codes unterschiedlicher Compiler können bequem untereinander genutzt werden. Zum Teil sind die Werkzeuge ineinander integriert, was die Sicherheit und Effizienz erhöht.

Sprachen und Compiler

Das Developer Studio ist eine Windows-basierte, integrierte Entwicklungsumgebung, die unter anderem Visual C++, Visual Test und einige andere Produkte beherbergt. Sie koppelt Produkte, bietet konfigurierbare Toolbars und einen beliebig anpaßbaren, universellen Editor, der Makros ausführen kann. Die Online-Hilfe bezieht ihre Texte und Artikel zum einen von den mitgelieferten Online-Books, zum anderen von der Developers CD, die in regelmäßigen Abständen von Microsoft veröffentlicht wird und so eine sehr aktuelle und breite Palette von Problemstellungen behandelt. Das Developers Studio arbeitet mit sogenannten Projekten, die alle Dateien verwalten, die mit diesem Projekt zu tun haben. Es kann eine Hierarchie aufgebaut werden, die eine beliebig tiefe Schachtelung zuläßt. Verschiedene Hauptprojekte können Schlüsselprojekte in ihrem Projektpfad aufnehmen und dadurch an deren Ergebnissen partizipieren. Die Projekte werden in Projektdateien beschrieben, die die Dateiextensionen .mdp und .mak besitzen. Die Datei mit der .mak Extension enthält Kommandos, Makrodefinitionen, usw., um die für das Projekt benötigten Maschinencodes zu erzeugen. Das in den .mak Dateien verwendete Format ist kompatibel zu den Dateien des make-Utility der UNIX-Welt. Die .mdp Datei beschreibt Einstellungen der Entwicklungsumgebung, wie Fenstergrößen und -positionen, Breakpoints, Inhalte von Watch-Windows, usw.

Visual C++ 4.0: Visual C++ kann C und C++ Quellcode compilieren. Anhand der Fileextension (.C oder .CPP) wird der Sprachtyp des Quellcodes festgestellt. Er entspricht der ANSI Norm Version 2.1, unterstützt die neuen Standard C++ Templates und besitzt Microsoft Erweiterungen. Neben dem Compiler ist in der Oberfläche ein Ressource Compiler, ein Linker, ein Debugger, ein Source Browser sowie eine Application Wizard integriert, der nach einem Dialog mit dem Programmierer einen Gerüstcode generiert, der dann anschließend ergänzt wird. Weitergehende Informationen findet man in [Mar96] und [Kru96].

Visual Basic 4.0: Visual Basic hat nichts — wie der Name irreführenderweise vermuten läßt — mit der Interpretersprache BASIC zu tun. Es ist vielmehr ein objektorientiertes imperatives Programmierwerkzeug, das seit Version 4.0 durchaus mit anderen renommierten Produkten, wie etwa SQLWindows von Gupta, vergleichbar ist. Es eignet sich hervorragend, um ein Benutzerinterface problemorientiert zu entwerfen und zu implementieren. Die Oberfläche arbeitet ähnlich wie die Developers Suite und integriert andere Produkte. Die Performance des erzeugten Codes kann sich durchaus mit

dem des C++ Compilers messen. Durch sogenannte Add-Ins und OCXe von Drittherstellern kann die ohnehin schon sehr umfangreiche Funktionsbibliothek auf ganz spezielle Bedürfnisse angepaßt und erweitert werden.

Testwerkzeug

Visual Test 4.0 ist ein Werkzeug, mit dem Testpläne erstellt und in Form von Testskripten umgesetzt werden können. Beliebige Testszenarios lassen sich für Windows NT basierte Anwendungen simulieren. Die gesammelten Resultate können grafisch und statistisch ausgewertet werden. Neben quantitativen lassen sich auch qualitative Messungen vornehmen. Außer einer umfangreichen Funktionsbibliothek, die speziell für das Testen von Programmen und Programmsystemen entworfen worden ist, werden den Testern Hilfsmittel an die Hand gegeben, die es ermöglichen, Aktionssequenzen von Benutzern aufzuzeichnen. Dialog-Boxen und Menükontrollstrukturen können festgehalten und verglichen werden, ganze Bildschirmbilder können Pixel für Pixel verglichen werden.

Codemanagement

Hauptaufgabe des Codemanagements ist es sicherzustellen, daß Dokumente und Quellcodes nicht versehentlich zerstört, unerlaubt geändert oder mißbraucht werden; weiterhin sind Vorgänge wie Erstellung, Änderungen, Freigaben und Verwendung zu dokumentieren. Der Mißbrauch erstreckt sich vom Einsatz falscher Versionen von Softwarekomponenten bis hin zur unerlaubten Weitergabe an Dritte. Schon bei der Entwicklung in kleinen Softwareteams ist der Einsatz des Codemanagements nahezu unerläßlich, will man ein effizientes und sicheres Arbeiten im Team ermöglichen. Es unterstützt die Koordinierung der Arbeit und hilft, diese zu analysieren. Mit den gewonnenen Informationen können Probleme wie Verzögerung, Budgetüberziehung usw. frühzeitig im Entstehen erkannt und sinnvolle Gegenmaßnahmen ergriffen werden. Aber nicht nur für die Entwickler, sondern auch für andere Bereiche wie Produktzertifizierung, Support, Wirtschaftlichkeitsanalyse, Marketing, strategische Produktplanung usw. sind die Informationen wichtig, die das Codemangement bereitstellt. Aus diesem Grund sollte "jede Zeile Quellcode und Dokumentation " von der Entstehung über Modifikation und Einsatz bis hin zur Archivierung vom Codemanagement begleitet werden.

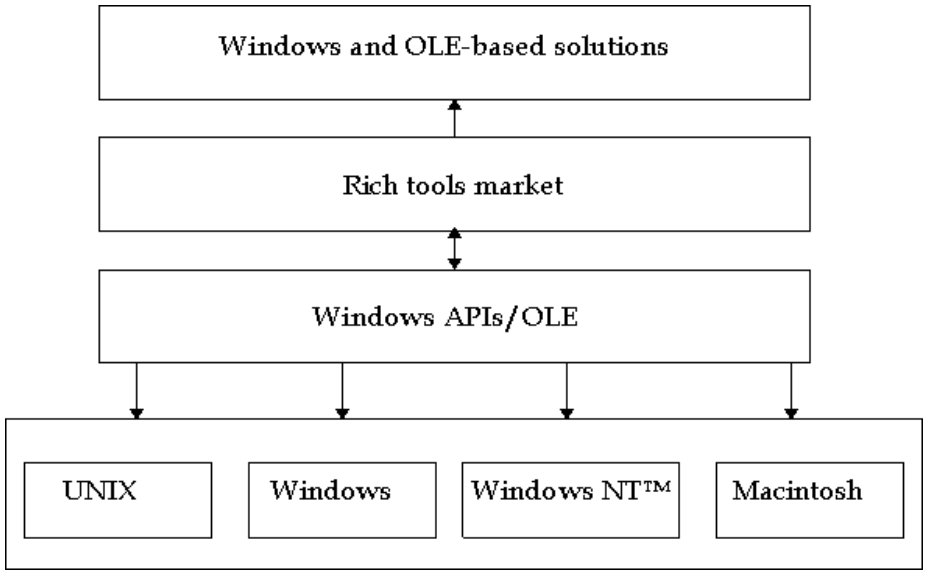
Visual Source Safe 4.0: Visual Source Safe integriert sich homogen in die Visual Basic und Visual C++ Entwicklungsoberflächen und unterstützt deren Projektstrukturen. Neben den obengenannten Aufgaben eines Codemanagements unterstützt es darüberhinaus das Zusammenfügen von Codesegmenten durch spezielle Funktionen. Es kann die Formate gängiger anderer Codemanagement- und Codekonfigurationssysteme lesen und importieren. Front Ends stehen für alle Betriebssystemplattformen zur Verfügung.

DocToHelp: DocToHelp ist eine Makroerweiterung für Word für Windows NT, mit der Programmhandbücher komfortabel erstellt werden können. Um das Online-Hilfe-Sytem von Windows NT nutzen zu können, reformatiert das Makrosystem diese Dokumente derart, daß der "Hilfe-Kompiler" eine entsprechende Online-Hilfe für die Ap-

plikation generieren kann. Die Vorteile liegen in der erheblichen Verkürzung der Erstellung der Online-Hilfe und dem wesentlich geringeren Aufwand, die Informationen in den Handbüchern und der Online-Hilfe des Programms konsistent zu halten. Außerdem braucht der Autor der Handbücher kein Experte auf dem Gebiet der Online-Hilfe-Formatierung zu sein und kann sich auf seine eigentliche Aufgabe konzentrieren.

Middle-Ware

Mit dem WISE-Projekt (Windows Interface Source Environment) deckt Microsoft durch Dritthersteller den Bereich der Middleware für die wichtigste alternative Betriebssystemplattform UNIX ab. Ziel dieses Projektes ist es, Software von jeder für jede Umgebung (NT $\leftrightarrows$ UNIX) entwickeln und bereitstellen zu können.



Abbildung~2.2: WISE ermöglicht eine offene Flexibilität über Plattformen hinweg

Diese Aufgabe soll mit zwei Komponenten bewältigt werden:

1. WISE Software Development Kit (SDK): Die WISE-SDK ist eine Implementierung von Windows APIs auf UNIX APIs. Mit ihr können Entwickler Windows-basierte Anwendungen auf UNIX-Systemen entwickeln, diese compilieren und ablaufen lassen. Sie besteht aus Werkzeugen, um Sourcecode von einem PC auf UNIX zu portieren, und aus Bibliotheken, um Windows Code auf einem UNIX-System zu compilieren. Programmierer, die gleichzeitig für Windows- und UNIX-Systeme entwickeln, können den Programmcode auf Basis der Windows API schreiben. Sie benutzen auf der PC-Plattform die Windows-SDK, auf dem UNIX-System die WISE-SDK. Solch eine Vorgehensweise erfordert eine erhöhte Programmierdisziplin, da kein plattformspezifischer Code geschrieben werden darf, hat jedoch den Vorteil, daß lediglich *ein Code* entwickelt und gewartet werden muß.

2. WISE Emulator: Der WISE Emulator ermöglicht es, bestehende Windows-Anwendungen auf einer Palette von UNIX-Systemen wie Solaris, SCO und HP-

UX laufen zu lassen. Er setzt die Anfragen bzw. Prozessorinstruktionen der Applikation zur Laufzeit auf die UNIX-Plattform bzw. Prozessorplattform um. Natürlich impliziert dies Einschränkungen in der Ausführungsgeschwindigkeit, hat aber den Vorteil, daß kein Quellcode des Programms benötigt wird.

Da die Architekturen und Konzeptionen von Windows NT und UNIX verschieden sind, kann der Code, der spezielle Eigenschaften der darunterliegenden Plattform (Betriebsystem und/oder Hardware) benutzt, nicht angepaßt werden. Detaillierte Darstellung der Unterschiede zwischen NT und UNIX findet man in [Cor96b] und [Cor96c]. Vorteil der WISE-Komponenten ist, daß eine Multiplattform-Unterstützung mit wesentlich geringerem Zeit- und Kostenaufwand möglich ist, und keine Rücksicht auf sich ändernde Versionen des Betriebssystems oder der Hardware genommen werden muß. Nachteil ist, daß nur die Plattformen unterstützt werden, die WISE abdeckt.

2.3 Geplante Einsatzszenarios

Anhand dreier exemplarisch ausgewählter Anwendungsbeispiele soll ein konkreter Eindruck vermittelt werden, welche Randbedingungen, Funktionalitäten, Leistungs- und Sicherheitsanforderungen an ein Zugangskontrollsystem in der Praxis gestellt werden. Die vorgestellten Szenarios sind jeweils Zusammenfassungen von bereits abgeschlossenen und momentan in Umsetzung befindlichen Projekten der jeweiligen Branche. Sie sind Mischungen aus Kunden- bzw. DNB- und Mitarbeiterkontrollsystemen.

2.3.1 Messeveranstaltungen

Messeinstallationen sind die strukturell einfachsten und von den Randbedingungen her unproblematischsten Systemkonfigurationen der vorgestellten Beispiele. Die Sicherheitsanforderungen an die Zugangskontrollsysteme solcher Installationen sind bisher eher gering, allerdings werden hohe Leistungsanforderungen an die Zutrittskontrollstationen gestellt. Der gesamte Kontrollvorgang darf maximal 500 ms dauern. Er beginnt mit dem Einlegen der Karte in den Leser bzw. dem Einbringen der Karte in den Erfassungsbereich des berührungsfreien Lesers und endet mit dem Entriegeln einer Barriere und/oder einer visuellen bzw. akustischen Signalisierung. Außerdem muß die Station diesen Vorgang für einen definierten Zeitraum autark durchführen können, d.h. ohne Verfügbarkeit bestimmter oder aller Rechner des Systems.

An Messeveranstaltungen partizipieren vier Parteien:

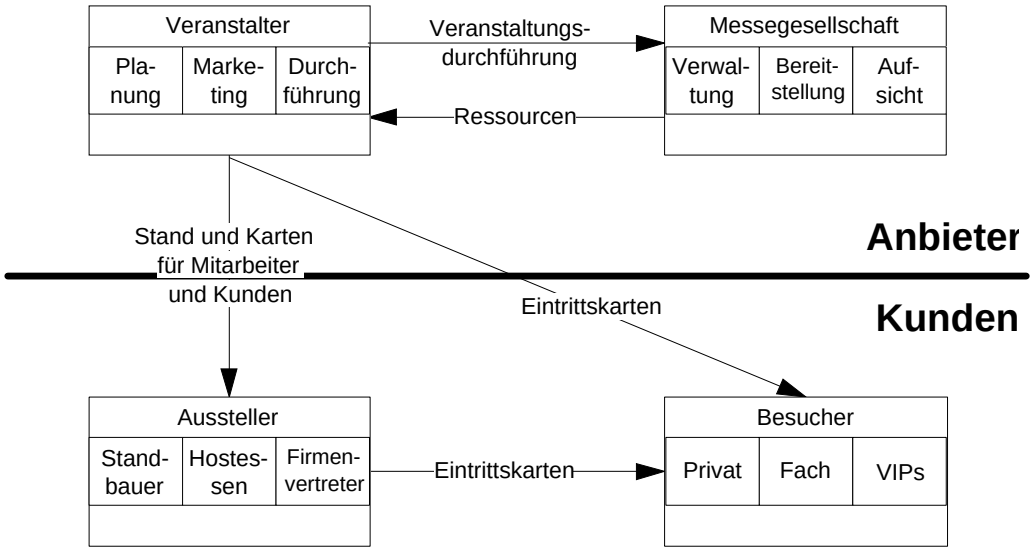
1. Messeveranstalter: Organisation, Durchführung
2. Messegesellschaft: Infrastruktur
3. Aussteller
4. Besucher

Mehr oder minder oft kommt es vor, daß Veranstalter und Gesellschaft dieselbe Person sind. Das ändert jedoch nichts an den prinzipiellen Interaktionsbeziehungen

der Parteien. Die Personengruppen der Parteien bilden in der Regel Untergruppen, die verschiedene Privilegien genießen. Die Hierarchie der Rechtevergabe unter den Parteien einer Messerveranstaltung stellen sich wie folgt dar:

- Messeveranstalter und Messegesellschaft einigen sich auf die Durchführung einer Messe.
- die Messegesellschaft stellt daraufhin dem Veranstalter die entsprechenden Ressourcen und das Know-How zur Verfügung.
- Veranstalter und Aussteller einigen sich über Stand und Karten für Mitarbeiter und Kunden.
- Kunden können Karten vom Veranstalter erwerben oder vom Aussteller erhalten.

Die folgende Abbildung zeigt die genannten Parteien und die Hierarchie ihrer gegenseitigen Rechtevergabe für Messeveranstaltungen. In den einzelnen Symbolen der Parteien sind deren denkbare Personengruppen angedeutet.



Abbildung~2.3: Hierarchie der Rechtevergabe bei Messeveranstaltungen

Je nach Aufgabe und Rolle von Personen in den jeweiligen Parteien muß das Zugangskontrollsystem anhand von Berechtigungsidentifizierungen den nachgefragten Zugang gewähren oder verweigern.

Messebesucher

Der Messebesucher muß mit seiner Eintrittskarte eine Messeveranstaltung betreten können und entsprechend seiner Karte Zutritt zu besonderen Bereichen erhalten sowie spezielle Dienste nutzen können (z.B. Transportdienste, Parkplätze, VIP Lounges usw..). An Informationsterminals kann er mit seiner Karte die für ihn bestimmten Informationen abfragen und Reservierungen oder Anmeldungen für Vorführungen, Symposien oder Workshops vornehmen.

Aussteller

Die Mitarbeiter der Aussteller wie Standbauer, Hostessen und Firmenvertreter müssen vor dem offiziellen Messebeginn die Hallen bzw. Plätze betreten und evtl. mit schweren Fahrzeugen über Sonderportale anfahren können. Sie müssen Zugang zum Informationssystem der Messegesellschaft bekommen, um spezielle Veranstaltungen oder andere für den Messebesucher interessante Informationen bekannt machen zu können.

Messegesellschaft

Die Messegesellschaft stellt die Infrastruktur zur Verfügung, wie Hallen, Parkplätze, Informations- und Kommunikationsmedien, Energieversorgung, Zugangskontrollsystem usw. Sie ist für die Sicherheit auf dem Messegelände und die Durchsetzung der Vorgaben und Regeln des Veranstalters verantwortlich. In ihrer Regie läuft der lokale Kartenverkauf am Messegelände. Mitunter tragen Messegesellschaften auch mehrere Messen gleichzeitig aus. Während und nach einer Messe müssen dem Veranstalter Daten über Anzahl, Eigenschaften und Verhalten der Messebesucher sowie Kassenabrechnungen über den Verkauf von Eintrittskarten und Accessoires (z. B. Anstecker, Regenschirme, Kappen usw.) übermittelt werden können. Neben diesen für die spezifischen Veranstalter bestimmten Daten benötigt die Messegesellschaft vom Zugangskontrollsystem Daten über:

- Anzahl der Personen (Personal, Aussteller, Besucher) auf den Messegeländen und den Unterbereichen (Außengelände, Hallen, Stockwerken)
- Anzahl der Gesamteintritte und Gesamtaustritte pro Zeitabschnitt und Veranstaltung
- Auslastung und Standortbestimmung von speziellen, Personalgruppen (Kassenpersonal, Entscheidungsträger, Sicherheitsdienst, Installateure, usw.)
- Auslastung und Störereignisse der Zutrittskontrolleinrichtungen und Informationsterminals

Messeveranstalter

Der Messeveranstalter ist verantwortlich für die Organisation und führt in Zusammenarbeit mit der Messegesellschaft die Veranstaltung durch. Er erwartet, daß beliebige Tarife und Sonderregelungen durch das Zugangskontrollsystem durchgesetzt werden können, wie :

- Einmaleintrittskarten
- Tageswahlabonnement
- Zeitkarten
- Tageskarten: Halb-, Ganztageskarten u.ä.
- Kombikarte für gleichzeitig stattfindende Anlässe

- Depot- und Wertkarten
- Gesellschaftskarten
- Pressekarten
- Karten für Ehrengäste und VIPs
- Freikarten
- Ausstellerausweise
- Lieferantenausweise

Der Messeveranstalter muß Tarife erstellen können. Je nach Tarif oder Sonderregelung sollen unterschiedliche Kartentypen zu Verfügung stehen. Für Ehrengäste und VIPs sind beispielsweise berührungsfreie Karten vorzusehen. Bei anderen Tarifen sollen Magnetstreifenkarten, Barcodekarten oder CHIP-Karten eingesetzt werden. Der Veranstalter benötigt während und nach der Messe Informationen über:

- Verkauf
- Durchgang
- Anwesenheit (Ausstellerpersonal und Besucher)
- Momentanauskünfte (sollen auf die Minute genau sein)
- Besuchsdauer
- Branchen-, Artikel- und Interessenstatistik
- Länderstatistik
- Kassenstatistik

Das Anforderungsprofil der Messeveranstalter an das Zugangskontrollsystem zeigt, daß neben den eigentlichen Zugangskontrollaufgaben mit den dazugehörigen Konfigurationsmöglichkeiten auch in einem bestimmten Maße Informations- und Auswertungsdienste zur Verfügung gestellt werden müssen. Der Zugang zu diesen Diensten unterliegt je nach Anwenderguppe bestimmten Restriktionen.

2.3.2 Skigebiete

Verglichen mit den Messeveranstaltungen sind die Organisationsstrukturen bei Skigebieten mit ihren Bergbahn- und Liftgesellschaften wesentlich komplexer, Sicherheitsanforderungen höher und Randbedingungen an die Hardwarekomponenten härter. Die Leistungsanforderungen an die Kontrollstationen entsprechen denen bei Messeveranstaltungen. Aufgrund topologischer Gegebenheiten und witterungsbedingter Einflüsse in den Bergen können Kontrollstationen teilweise garnicht oder nur durch Medien vernetzt werden, deren Einrichtung und Betrieb mit erheblichen Kosten verbunden sind

(z.B. Richtfunk) oder die eine relativ geringe Übertragungsrate aufweisen. (z.B. Zweidrahtleitungen). Die Weitläufigkeit der Skigebiete, Anzahl der Kunden und Preise für die Nutzung der Transporteinrichtungen macht passive und aktive Angriffe auf das Zugangskontrollsystem attraktiv, z.B. durch ungesetzliches Duplizieren von Nutzungslegitimationen.

Beim Einsatzszenario Skigebiete sind folgende Parteien beteiligt:

- Transportdienstbenutzer (Skisportler, Wanderer, usw.)
- Agenturen (Reiseveranstalter, Vereinigungen, usw.)
- Transportdiensterbringer (Transportanlagenbetreiber)
- Transportdienstanbieter (Marketingorganisationen, Transportanlagenbetreiber, Betreiberkonsortien, usw.)

In der Regel sind Transportdiensterbringer und Transportdienstanbieter dieselbe Person. Neben diesen Transportdienstanbietern gibt es auch Pools bzw. Skipools. Sie stellen eine Gemeinschaft von Transportdienstanbietern dar, die Skipässe herausgeben, mit denen Transportdienstbenutzer die von der Gemeinschaft vertretenen Transportdiensteinrichtungen nutzen können. Die Hierarchie der Rechtevergabe bei der Skithematik kann wie folgt beschrieben werden:

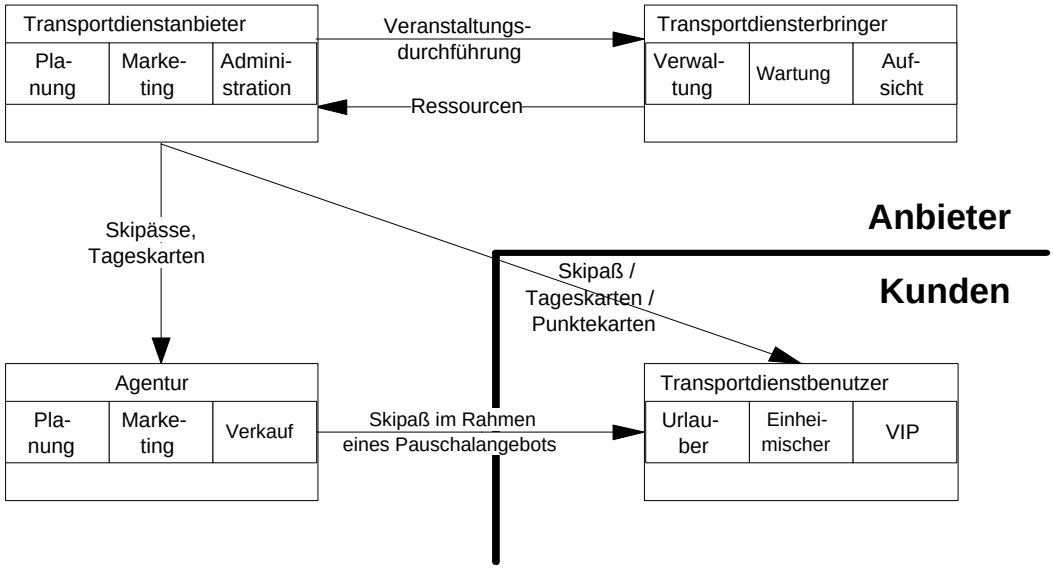
- die Transportdiensterbringer und Transportdienstanbieter einigen sich auf die Nutzung der Transporteinrichtungen.
- die Transportdiensterbringer stellen im Rahmen der Vereinbarung ihre Einrichtungen zur Verfügung.
- die Agenturen und Transportdienstanbieter einigen sich auf Tarife und Nutzungsbedingungen der Transporteinrichtungen.
- Die Transportdienstbenutzer können Nutzungslegitimationen im Rahmen von Pauschalangeboten von Agenturen und direkt von den Transportdienstanbietern erhalten.

Analog zu den Messeveranstaltungen zeigt Abbildung 2.4 Parteien und Hierarchie der gegenseitigen Rechtevergabe bei den Skigebieten. In dem gegenseitigen Beziehungsschema sind neben den Hauptakteuren auch deren denkbare Untergruppen angedeutet.

Ähnlich wie schon zum Thema Messeveranstaltungen ausgeführt, muß auch bei den Skigebieten das Zugangskontrollsystem anhand von Berechtigungsidentifizierungen Zugang gewähren oder verweigern.

Transportdienstbenutzer

Wie der Messebesucher muß auch der Transportdienstbenutzer (Kunden) entsprechend seiner Skikarte oder seines Skipasses Lifte, Bergbahnen und Skibusse *sofort nach Erwerb benutzen können*; weiterhin soll er Zugang zu Informationsterminals haben und weitere Dienstleistungen (wie Skikurse, Tourenführer, Ausleihen von Sportausrüstungen usw.) in Anspruch nehmen können. Skipässe, Tageskarten, Punktekarten erhä lt er entweder direkt vom Transportdienstanbieter oder von Agenturen, die in der Regel Sondertarife oder Paketangebote offerieren.



Abbildung~2.4: Hierarchie der Rechtevergabe bei Skigebieten

Agenturen

In Absprache mit den Transportdienstanbietern vertreiben sie Skipässe oder Tageskarten in Kombination mit weiteren Dienstleistungen (An- und Abreise, Unterbringung, Skikurse, Tourenführerer, Skitests, usw.).

Transportdiensterbringer

Die Transportdiensterbringer stellen die Transportinfrastruktur zur Verfügung. Sie erwarten vom Zugangskontrollsystem, daß sie mit dessen Hilfe die Kontrollstationen und Beförderungsmaschinenanlagen überwachen und gegebenenfalls steuern können. Im Falle hoher Nutzungsdichten kann es beispielsweise notwendig werden, auf die Maschinenanlagen und Kontrollstationen direkt Einfluß zu nehmen. Die Auswertung momentaner Daten mit statistischen Methoden unter Einbeziehung von bereits erstellten Bewegungsprofilen ermöglicht es, vorausschauend Steuerungsaufgaben zu optimieren und bei entsprechenden Prämissen einzusetzen. Daher sind Daten über folgende Bereiche von Interesse:

- Beförderungszahlen
- Erstzutritte pro Skigebiet
- Bewegungsdaten
- Kartentyp und Ausgabestelle
- Transportdienstanbieter
- Störungs- und Sicherheitsverletzungsereignisse

- Maschinenanlagenzustandsdaten

Diese Daten werden — entsprechend gefiltert — an die betreffenden Transportdienstanbieter weitergeleitet. Die Kontrolleinrichtungen müssen in der Lage sein, getrennt von dem Restsystem (offline) aktive Bedrohungen wie z.B. Ticketfälschungen zu erkennen und abzuwehren. Bei Ausfall von Komponenten durch physikalische Einwirkungen wie Blitz oder Energieversorgungsausfall müssen die Daten in einem konsistenten Zustand wiederzubeschaffen sein.

Transportdienstanbieter

Transportdienstanbieter können einzelne Lift- und Bergbahngesellschaften sowie Pools sein. Sie unterhalten Verkaufsautomaten und Verkaufsstellen, an denen Karten und Skipässe an die Kunden verkauft werden. An diesen Verkaufsstellen sollen auch signifikante Daten der Kunden zur Überprüfung der Überlassungsbedingungen und statistischen Auswertung erfaßt werden. Es sollen berührungsfreie CHIP-Karten, Magnetstreifenkarten und Barcodekarten eingesetzt werden. Diese müssen folgende Tickettypen ermöglichen:

- Einzelfahrt-Karte
- Tages-, Halbtageskarten
- Skipässe, Mehrtageskarten
- Saisonkarten und Jahreskarten
- Wahltageskarten: 5 aus 15; 10 aus 30
- Punktekarten : 60, 120
- VIP-Karten
- Freikarten
- Gruppenkarten

Die Transportdienstanbieter einigen sich mit den Transportdiensterbringern auf Nutzungsmodi und Abbrechnungsverfahren für erbrachte Transporte. Sie müssen in der Lage sein, an grafischen Benutzeroberflächen selbständig Tarife eingeben und an die Verkaufsstellen übermitteln zu können. Zur Unterstützung bei der Tarifentwicklung und der Abrechnung mit den beteiligten Partnern muß das Zugangskontrollsystem in der Lage sein, Daten von den Transportgesellschaften und Verkaufsstellen zu beschaffen sowie statistisch und grafisch aufzubereiten. Dies soll nach folgenden Kriterien möglich sein:

- Typ des Käufers: Agentur, Urlauber, Einheimischer, usw.
- Kartentyp
- Verkaufsstelle

- Einzelgäste, die Pooltickets gekauft haben.
- Einzelgäste, die Tickets von Transportdienstanbietern gekauft haben, die keine Pooltickets sind.
- Bewegungsdaten
- Transportdienstbenutzerarten (Snowboarder, Skifahrer, Wanderer, usw.)
- Gästeverhalten pro Person

2.3.3 Banken

Die Anforderungsprofile der bisher dargestellten Einsatzszenarios beschreiben Systeme, die in erster Linie Bereitstellung, Betrieb und Verwaltung von Dienstleistungen zum Ziel haben. Im letzten Beispiel sollen Zugangskontrollsysteme betrachtet werden, bei denen der Schutz und die Sicherheit von Objekten im Vordergrund stehen, wie dies typischerweise auf Banken zutrifft. Sie sind Repräsentanten für Systeminstallationen, die in verschiedenen Bereichen ein unterschiedlich hohes Maß an Sicherheitsvorkehrungen benötigen. Die Spanne reicht vom Einsatz weniger Geräte und einfacher Vorgehensweisen bis hin zu einem komplizierten Regelwerk aus technischen Einrichtungen und Verhaltensvorschriften, um die Durchsetzung festgelegter Regeln sicherzustellen.

Um in der Lage zu sein, das Maß der Sicherheit solcher Systeme einstufen und verifizieren zu können, liegt diesen ein Plan zugrunde, der die Methoden, Regeln, Handlungsweisen und Eigenschaften technischer Komponenten und beteiligter Personen festlegt. Hierbei müssen alle Bereiche abgedeckt werden, die signifikante Bedeutung für die Sicherheit haben. Dieser Plan wird auch Sicherheitspolitik genannt.

Für das Zugangskontrollsystem bedeutet dies zum einen, daß seine Komponenten entsprechend der Sicherheitspolitik ausgelegt werden müssen, und zum anderen, daß das Regelwerk, welches Ereignisse sowie technische und personenbezogene Reaktionen festlegt, abgebildet werden kann. Außerdem muß das Gesamtsystem als solches und in seiner Funktion verifizierbar sein.

Zentrales Sicherheitsmanagement

Im Zuge neuer technischer Möglichkeiten bieten Banken veränderte und neue Nutzungsmöglichkeiten bereits bestehender Dienstleistungen an. Außerdem wird das bestehende Angebot durch neuartige Serviceleistungen erweitert. Diese Veränderungen, zusammen mit der allgemeinen Tendenz ansteigender Kundenzahlen und zunehmender Kriminalität insbesondere in den Bereichen bargeldloser Zahlungsmittel (Kreditkarten, Eurochequekarten, usw.) und Kundenselbstbedienung, machen den Einsatz umfassender Kontroll- und Überwachungsmaßnahmen notwendig. Um den zusätzlichen Kosten- und Verwaltungsaufwand sinnvoll begrenzen zu können, gehen einzelne Bankgesellschaften dazu über, zur Überwachung ihrer Niederlassungen zentrale Sicherheitsmanagements einzurichten. Deren Aufgabe ist:

- Zentrale Erfassung und Überprüfung von Zustandsdaten, Gefahren-, Störungs- und Überfallmeldungen

- Überprüfung der erhaltenen Meldungen und Daten durch visuelle und akustische Erfassungssysteme, Detektoren und Sensoren
- Zentrale Steuerung und Auslösung der notwendigen Reaktionen auf die erhaltenen Informationen

Die Personenkreise, von denen Bedrohungen ausgehen können, sind:

- Bankfremde Personen, wie Mitarbeiter von Dienstleistungsbetrieben (Handwerker, Reinigungspersonal, usw.), kriminelle Elemente
- Bankkunden
- Bankmitarbeiter

Aufgrund der erheblichen Datenmengen, mit denen ein zentrales Sicherheitsmanagement konfrontiert wird, muß das Zugangskontrollsystem die eingehenden Ereignisse nach Wichtigkeit und Dringlichkeit aufbereiten und die Sicherheitsmanager entsprechend informieren. Einfache und unkritische Vorgänge sollten vom System selbständig abgearbeitet werden können. In kritischen Situationen sollten die durch die Sicherheitspolitik vorgesehenen Pläne anschaulich aufgezeigt werden. Das System sollte die Sicherheitsexperten bei der schnellen und richtigen Einschätzung der Situation unterstützen, mögliche Maßnahmen aufzeigen und bei der Ausarbeitung geeigneter Lösungen helfen.

Aus dem breiten Spektrum schutz- und überwachungsbedürftiger Bankbereiche sollen hier stellvertretend nur Selbstbedienungszonen sowie Schalter-, Kassen- und Tresorräume angesprochen werden, an denen jedoch exemplarisch alle im Sicherheitssystem zu integrierenden Anforderungen demonstriert werden können.

Schalter- und Kassenräume

Schalterräume sind ein Beispiel für Bereiche, die inhomogen sicherheitsrelevante Raumzonen aufweisen, und deren Sicherheitseinstufung sich zeitlich ändert (Zeiten ohne Bankpersonal, Dienstzeiten mit und ohne Publikumsverkehr). Sie weisen in der Regel drei verschiedene Funktionseinheiten auf:

- Automaten für gängige Geldgeschäfte (Inlandsüberweisungen, Auszahlung kleinerer Geldbeträge)
- Schalter mit Personal (Informationen, spezielle Geldgeschäfte)
- Kassenraum (Auszahlung größerer Geldbeträge)

In Schalterräumen sind üblicherweise Kassenräume integriert. Die Kassenräume sind in der Regel mit durchschußhemmenden und meist durchsichtigen Elementen vom restlichen Schalterraum abgetrennt. Je nach Sicherheitspolitik müssen sich während des Publikumsverkehrs eine definierte Anzahl von bestimmten Mitarbeitern im Kassenraum aufhalten. Ein Wechsel der Beschäftigten in diesem Bereich ist nur zu bestimmten Zeiten oder bei genau definierten Ausnahmesituationen zugelassen. Dazu

muß vor dem Betreten oder Verlassen des Bereichs eine entsprechende Signalisierung gegeben werden. Dadurch wird eine Meldung an die Sicherheitszentrale abgesetzt, griffbereites Bargeld automatisch sicher verwahrt und die Barriere, die den Durchgang zum Schalterraum sichert, entriegelt.

In den Schalterräumen muß bei Publikumsverkehr — ähnlich wie in den Kassenräumen und je nach lokalen Gegebenheiten (Größe der Räume, Anzahl der Geldautomaten,...) — immer eine bestimmte Anzahl von Mitarbeitern anwesend (Mehr-Personen-Anwesenheitskontrolle) und definiert verteilt sein. Nach Beendigung des Publikumsverkehrs gelten andere Regeln. Das beliebige Wechseln in und aus dem Kassenraum ist nun möglich. Das Arbeiten mit Bargeld ist in dieser Zeit auch außerhalb des gesicherten Kassenraums zulässig; hierzu gehören Tätigkeiten wie Auffüllen oder Verwahren der Geldbestände und Bestücken der Geldautomaten. Dabei muß — etwa mittels Sichtblenden — sichergestellt werden, daß Drittpersonen diese Tätigkeiten mit Bargeld nicht beobachten können. Weitere Regelungen legen die Bedingungen und Verhaltensweisen der Mitarbeiter für das Betreten und Verlassen der Bankräumlichkeiten fest.

Eine dritte Kategorie von Verhaltensregeln gilt für Mitarbeiter, die ihre Arbeiten außerhalb der regulären Dienstzeit versehen, wie Wachpersonal, Handwerker und Reinigungsdienste.

Ausnahmeregelungen, die automatische Alarmauslösungen festlegen, sind bei besonderen Situationen wie beispielsweise bei einem Überfall vorgesehen. Auch hier muß das Zugangskontrollsystem durch automatische Bild- und Tonaufzeichnungen sowie automatische Sperren die Schadensbegrenzung unterstützen.

Selbstbedienungszonen

Die Selbstbedienungszonen zählen zu den neuartigen Nutzungsmöglichkeiten bisheriger Dienstleistungen. Sicherheitstechnisch sind diese Räumlichkeiten homogen, und es gibt nur zwei Zeitzonen mit wechselnden Sicherheitseinstufungen (Publikumsverkehr, Wartungs- und/oder Auffüllzeiten). Inhaber von Kunden-, Kredit- oder Eurochequekarten können an den Terminals in diesen Räumlichkeiten Bankgeschäfte rund um die Uhr vornehmen. Besondere Bedrohungen sind hier gegeben durch:

- Vandalismus (z.B. Verstopfen von Schlitzen, Hineinkippen von Flüssigkeiten, Zerstören der Tastatur oder Öffnen der Geldautomaten)
- Kriminelle Elemente, die im weitesten Sinne Kartenmißbrauch betreiben
- Bedrohungen bzw. das Ausrauben von Kunden
- Betrugsversuche von Kunden, die vorgeben, angefordertes Bargeld nicht erhalten zu haben

Da die Selbstbedienungszonen in der Regel unbeaufsichtigt sind, ist eine Videoüberwachung dieser Bereiche zur Beweissicherung sowie zur Abschreckung unerläßlich. Sie soll den Kunden schützen, Vandalismus frühzeitig erkennen helfen und die Überprüfbarkeit von Aussagen und Behauptungen ermöglichen. Eine weitere wichtige Funktion kommt den Zugangsbarrieren für diese Zonen zu. Sie sollen den Aufenthalt nicht autorisierter Personen in diesen Bereichen verhindern und damit zur Prävention der genannten Gefahren beitragen. Die Erkennung von Defekten sowie die mögliche Fernwartung

und Steuerung der Komponenten dieser Zonen, wie Barrieren und Geldautomaten, Video- und Akustiküberwachungseinheiten, ist die dritte wesentliche Forderung an das Zugangskontrollsystem.

Tresorräume

Tresorräume zählen nach den einleitenden Ausführungen zu den Hochsicherheitsbereichen einer Bank. Sie sollen bestimmte Gegenstände vor dem unberechtigten Zugriff von Personen schützen. Die Verwirklichung dieser Regel wird mit großem technischen Aufwand und komplizierten Vorschriften betrieben. Diese Bereiche sollen eine homogene Sicherheitseinstufung haben. Zu diesem Zweck sind Schließfach-Tresore o.ä., zu denen Bankkunden Zutritt haben, von solchen Tresorräumen getrennt, in denen die bankeigenen Werte (Geldreserven, Wertpapiere, Gold, usw.) verwahrt werden. Die Art und Weise des Zutritts zu den jeweiligen Räumen unterscheidet sich durch die Zusammensetzung des Personenkreises, Barrieren und Zeitintervalle.

Um während der Geschäftszeiten zu den Schließfächern zu gelangen, müssen die Kunden mit einer Legitimation ausgestattet sein und von einem speziell autorisierten und mit Identifikation versehenen Mitarbeiter der Bank begleitet werden. Das Zugangskontrollsystem muß sicherstellen, daß nur jeweils eine Partei den Tresorraum, der die Schließfächer beherbergt, betreten kann. Außerhalb der Schalteröffnungszeiten dürfen diese Räume nur noch durch Kontrollinstanzen betreten werden.

Wesentlich aufwendiger ist der Zugang zu den Tresorräumen, in denen die Wertbestände der Bank aufbewahrt werden. Sie können nur zu bestimmten Zeiten und von einer Gruppe betreten werden, deren Mitglieder nach Anzahl und Sicherheitseinstufung definiert sein müssen. Um dies sicherzustellen, ist der Zugang nur durch eine Mehr-Personen-Zutrittskontrolle mit einer anschließenden Mehr-Personen-Anwesenheitskontrolle möglich. Erst wenn sich alle Personen im Vorraum des Tresors befinden, und weitere durch die Sicherheitspolitik festgelegten Prämissen erfüllt sind, können die Durchgänge geöffnet oder die Schließ- und Öffnungskonfigurationen geändert werden.

Informationssysteme

Die Informationssysteme einer Bank können in gewissem Sinne als ihr Nervensystem bezeichnet werden. Sie stellen das zentrale Werkzeug für das operative Geschäft dar. Fehlerhafte oder nicht rechtmäßige Transaktionen können innerhalb kürzester Frist zum Ruin führen. Täglich muß eine gewaltige Datenmenge verarbeitet und transportiert werden. Dabei muß eine große Anzahl von Benutzern mit unterschiedlichsten Aufgaben und Nutzungsrechten "online" bedient werden. Die Spanne der Benutzer reicht vom Schalterpersonal, den Kunden an den Selbstbedienungsterminals und Nutzern des Homebanking über die Mitarbeiter der Finanzbuchhaltung und Provisionsabrechnung bis hin zu Wertpapierdisponenten die die verschiedensten Börsentransaktionen durchführen. Um diese Vorgänge kontrollieren zu können, bedarf es spezieller Systeme und Mechanismen, die auch mit Kenntnis ihrer Funktionsweise nicht sabotiert bzw. unerlaubt beeinflußt werden können. Dies betrifft technische Bereiche ebenso wie Vorgehensmethoden. Die Aufgaben eines leistungsfähigen Zugangskontrollsystems liegen auch hier in der Sicherstellung und konsequenten Umsetzung der in der Sicherheitspolitik festgelegten Regeln, indem es die Pforten zu diesen Systemen kontrolliert und

sichert.

In Tabelle 2.1 wird ein abschließender Überblick über die vorgestellten Einsatzszenarios geggeben, in dem die charakteristischen Merkmale der jeweiligen Anwendung einander gegenübergestellt werden.

Die dargestellten Beispiele zeigen, daß das neue Zugangskontrollsystem sehr flexibel konfigurierbar sein muß, um den unterschiedlichen Organisationsstrukturen und Randbedingungen gerecht zu werden. Dabei müssen neben den eigentlichen Zugangskontrollaufgaben grafisch unterstützte Konfigurations-, Informations- und Auswertungsdienste zur Verfügung gestellt werden. Die Vielfalt der Systembenutzer und der Umfang der erforderlichen Installationen machen den Einbau unumgänglicher Sicherheitsmechanismen notwendig, die unterschiedlichen Klassen von Angriffsmethoden und -verfahren widerstehen könnnen.

	Messeveranstaltungen	Skigebiete	Banken
Systemtyp	DNB	DNB	Objektschutz
Benutzergruppen	4	4	2
Benutzerkategorien (Gruppen)	2 (2:2)	2 (3:1)	2 (1:1)
Gruppenbeziehungen (G_x) innerhalb und zwischen den Kategorien (K_x)	<table><tr><th></th><th colspan="2">K_A</th><th colspan="2">K_K</th></tr><tr><th></th><th>G_V</th><th>G_M</th><th>G_A</th><th>G_B</th></tr><tr><td>G_V</td><td>*</td><td>1</td><td>0</td><td>0</td></tr><tr><td>G_M</td><td>1</td><td>*</td><td>0</td><td>1</td></tr><tr><td>G_A</td><td>1</td><td>0</td><td>*</td><td>1</td></tr></table>	<table><tr><th></th><th colspan="3">K_A</th><th>K_K</th></tr><tr><th></th><th>G_T</th><th>G_E</th><th>G_A</th><th>G_B</th></tr><tr><td>G_T</td><td>*</td><td>1</td><td>1</td><td>1</td></tr><tr><td>G_E</td><td>1</td><td>*</td><td>0</td><td>1</td></tr><tr><td>G_A</td><td>1</td><td>0</td><td>*</td><td>1</td></tr></table>	<table><tr><th></th><th>K_A G_B</th><th>K_K G_K</th></tr><tr><td>G_B</td><td>*</td><td>0</td></tr><tr><td>G_K</td><td>1</td><td>*</td></tr></table>
Umwelteinwirkungen auf Installationskomponenten	mechanische Beanspruchung; bei regulärem Betrieb; Witterungseinflüsse; Vandalismus	extreme Witterungseinflüsse; starke mechanische Beanspruchung bei regulärem Betrieb	mechanische, chemische, elektromagnetische Einwirkung durch Angreifer; Vandalismus
Raumzonen	fest und variabel	fest	fest
Komponenteninstallation	stationär und mobil	stationär	stationär
Komponentenkommunikation	ständig online, temporär online	ständig online, temporär online, offline	ständig online
Kontrollfunktionen	Zugangskontrolle, Zutrittskontrolle, Buchung und Abrechnung, Ereignisprotokollierung	Zutrittskontrolle, Buchung und Abrechnung, Ereignisprotokollierung	Zugangskontrolle, Zutrittskontrolle, Ereignisprotokollierung
mögliche Subjektverfolgung	keine / passive / aktive	keine / passive	aktive
Sicherheitsanforderungen	autonomer Komponentenbetrieb, kryptographisch gesicherte Kommunikation, ereignisorientierte Alarmierung, ereignisorientierte Benachrichtigung, ereignisorientierte Reaktionen	autonomer Komponentenbetrieb, gesicherte Kommunikation, ereignisorientierte Alarmierung, ereignisorientierte Benachrichtigung, ereignisorientierte Reaktionen	autonomer Komponentenbetrieb, kryptographische Sicherheitsprotokolle, Abbildung und Durchsetzung einer Sicherheitspolitik
mögliche Zertifikationstypen	Qualitätszertifikation	Qualitätszertifikation	Qualitäts- und Sicherheitszertifikation
erweiterte Funktionen	Veranstaltungsplanung, veranstaltungsspezifische Datenauswertung, datenspezifisches Routing, Abrechnungsfunktionen, Informations- und Kommunikationsfunktion	Tarifentwicklung und Durchsetzung, tarifnutzungsungsspezifische Datenauswertung, datenspezifisches Routing, Abrechnungsfunktionen, Maschinensteuerung	Sicherheitsmanagementsystem, datenspezifisches Routing, Sensorensteuerung, Krisenmanagementsystem

Tabelle 2.1: Charakteristische Merkmale der Einsatzszenarios

Kapitel 3

Systemanalyse

Nach einem ersten Überblick in der Einleitung zum Themenkreis Zugangskontrollsysteme sowie den Zielsetzungen und künftigen Einsatzgebieten des neuen SIPORT-Systems werden in der Systemanalyse die beteiligten Objekte und Subjekte, deren gegenseitige Beziehungen, Aufgaben sowie benötigten Funktionen dargestellt. Spezielle, das System beschreibende Begriffe werden definiert, Gemeinsamkeiten und charakterisierende Attribute der beteiligten Personen und Komponenten betrachtet. Zur Darstellung der dynamischen Abläufe werden Stellen/Transitionen-Netze, Prädikaten/Transitionen-Netze oder bei Bedarf NF^2-Relationen/Transitionen-Netze verwendet, wie sie in [Rei85] und [Obe96] beschrieben sind. Die statischen Strukturen werden durch objektorientierte Modellierungen beschrieben, die der Nomenklatur in [Boo94] und [Whi94] folgen.

3.1 Systemrelevante Subjekte und Objekte

Die Anforderungsbeschreibung für ein Zugangskontrollsystem muß neben der funktionalen Eigenschaftsanalyse eine Festlegung der Systemelemente, -strukturen sowie Abläufe im und um das System umfassen. Hierfür ist eine differenzierte Betrachtung der statischen und dynamischen Verhältnisse notwendig, die einerseits die Modellierung und Beziehungen der Systemelemente festlegen und andererseits deren wechselseitige Rollen von Subjekten (aktive Elemente) und Objekten (passive Elemente) in den unterschiedlichen Systemzuständen darstellen.

In diesem Abschnitt werden zunächst die Wirkungsprinzipien zur Akzeptanz und Nutzung von Systemelementen durch das System beschrieben, auf die nachfolgend unter dem Begriff der Legitimation Bezug genommen wird. Daran schließt sich eine allgemeine Charakterisierung der Benutzergruppen, die Beschreibung von Raum- und Gebietsobjekten, von Hardware- und Softwareelementen sowie die durch sie bereitgestellten Dienste des Zugangskontrollsystems an.

3.1.1 Legitimationen

Legitimationen spielen eine Schlüsselrolle in einem Zugangskontrollsystem. Sie sind die Repräsentanz der Systembenutzer, Systemkomponenten und Raumzonen für das Sicherheitssubsystem und ermöglichen es, effizient und sicher Anfragen von "Systemmitgliedern" zu registrieren, zu prüfen und Entscheidungen über die Gewährung oder

Ablehnung des Zugangs bzw. der Bearbeitung von Aufträgen zu berechnen.

Legitimationskarten

Die Legitimierungsvorgänge im System sowie Nutzung von Diensten sollen am Beispiel der Legitimationskarten aufgezeigt werden. Legitimationskarten zählen zu den Systemkomponenten. Damit sie verwendet werden können, müssen sie selbst vom System legitimiert worden sein. Die Karten dienen zur Aufnahme der Legitimationsdaten von Personen; außerdem wird die Legitimationskennung der Karte bei den systeminternen Legitimationsdaten der Person gespeichert.

Wie in der Einleitung beschrieben, gibt es unterschiedliche Kartentypen. Für alle gilt jedoch das in Abbildung 3.1 dargestellte Zustandsdiagramm:

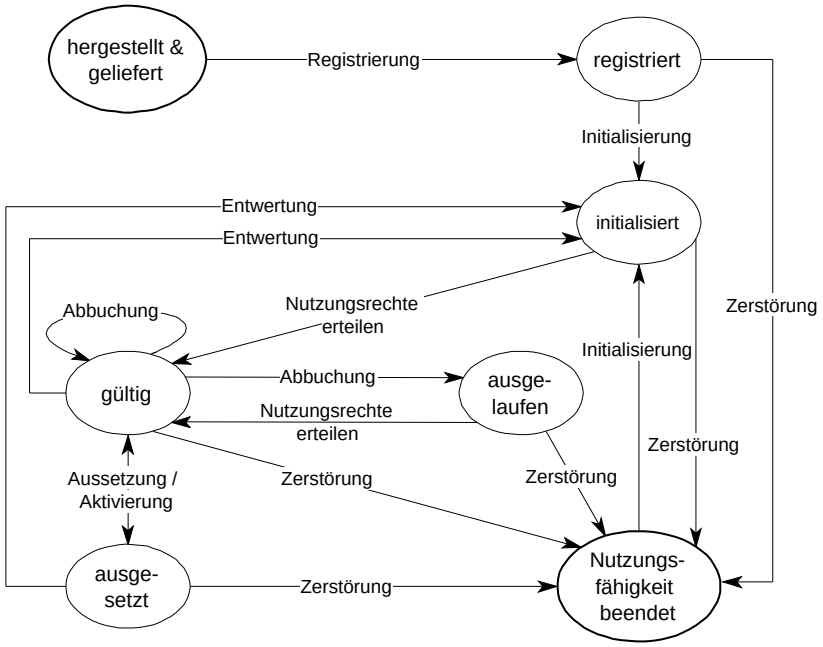
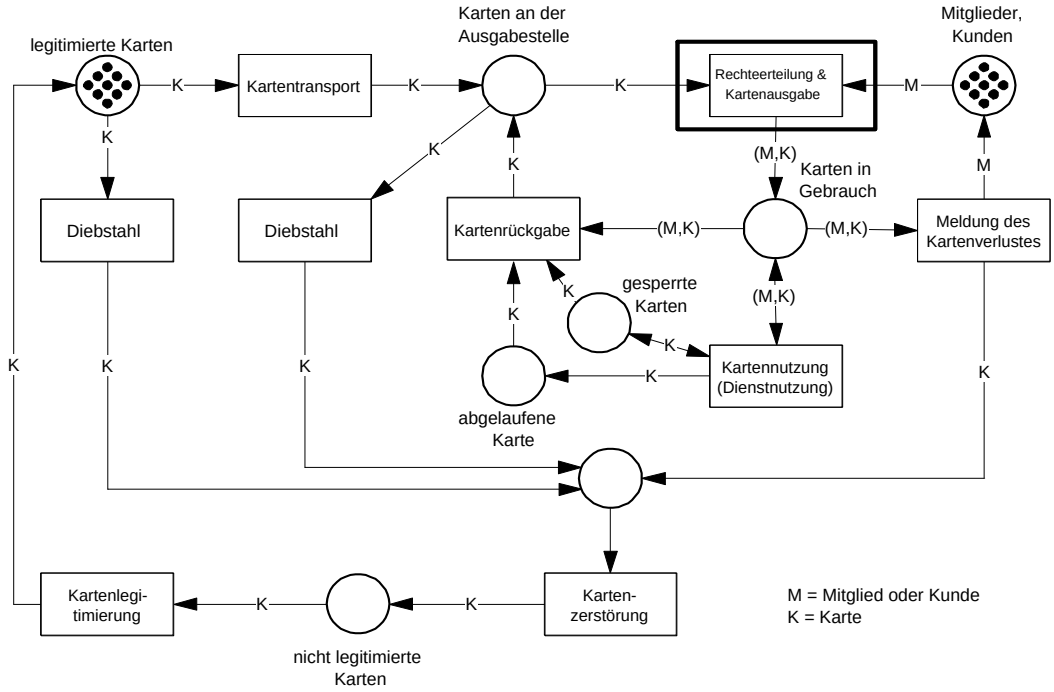


Abbildung 3.1: Zustandsübergangsdiagramm von Legitimationskarten

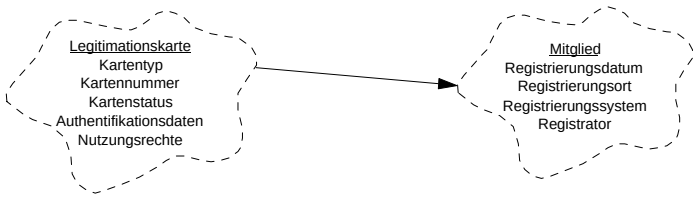
Die Initialisierung beinhaltet die Legitimierung der Karte durch die Sicherheitsabteilung. Erst wenn diese erfolgt ist, können die Karten an die Ausgabestellen verteilt werden. Bei einer weniger sicherheitskritischen Anwendung kann die Legitimation auch an den Ausgabestellen, wie z.B. Kassen des Skizirkus, erfolgen. In jedem Fall muß die Registrierung durch Mitarbeiter des Systembetriebs vorgenommen werden. Die eigentliche Aufgabe der Ausgabestelle ist die Erteilung der Nutzungsrechte, hier durch "Nutzungsrechte erteilen" gekennzeichnet, sowie die Veranlassung ihrer Durchsetzung. Bei Skipässen, Messekarten und Bankkarten erfolgt die Durchsetzung durch die Stelle selbst, also durch das Schreiben der Nutzungsrechte auf die Karte. Die Abbuchung entspricht der ständigen Nutzungsrechtekontrolle. Bei Punktekarten oder Bankkarten bedeutet dies, daß beim Abheben oder bei der Benutzung einer Dienstleistung "neue Nutzungsrechte" erteilt und durchgesetzt werden. Wird eine Karte als "verloren" gemeldet, oder wird sie von einer dritten Person abgegeben, soll die Karte logisch zerstört

werden. Damit ist gemeint, daß ihre Legitimation aus dem System entfernt wird. Um eine abgelaufene Karte wieder "auffüllen" zu lassen, muß sie an einer Ausgabestelle (z.B. Kasse, Kassenautomat, Abteilungsverwaltung, usw.) zurückgegeben und dort mit entsprechenden neuen Rechten ausgestattet werden. Verhält sich ein Karteninhaber nicht entsprechend den Nutzungsvereinbarungen, so kann die Karte gesperrt werden. Dies wird auch notwendig, wenn das Zugangskontrollsystem feststellt, daß mehrere Karten mit derselben Nummer im System verwendet werden. Außerdem kann eine Karte jederzeit vom Karteninhaber zurückgegeben werden. Diese Zusammenhänge sind im Petrinetz in Abbildung 3.2 dargestellt.



Abbildung~3.2: Kreislauf der Kartennutzung

Alle Kartentypen sollen durch folgende Objektklasse "Legitimationskarte" (Abbildung 3.3) dargestellt werden.



Abbildung~3.3: Die Objektklassen Legitimationskarte und Mitglied

Legitimation von Subjekten und Objekten des Systems

Alle Komponenten und Benutzer des Systems müssen eine Legitimation besitzen. Sie ist die Grundlage zur Erteilung und Durchsetzung von Nutzungsrechten, die den gegenseitigen Zugriff der Systemkomponenten aufeinander festlegen.

Um eine Legitimation zu erhalten, muß das systemfremde Objekt oder Subjekt registriert werden. Bei der Registrierung werden die Merkmale des Bewerbers erfaßt und geprüft, ob er bereits registriert ist. Ist dies der Fall, wird eine erneute Registrierung abgelehnt. Ziel dieser Vorgehensweise ist es, eine mehrfache Repräsentanz eines Subjekts oder Objekts im System zu verhindern. Das Objekt oder Subjekt ist dem System nun bekannt und wird als passives Mitglied bezeichnet. Mit dessen Sicherheitseinstufung durch das Sicherheitssubsystem wird aus ihm ein aktives Mitglied, das eine Legitimation erhalten kann. Eine Erteilung der Sicherheitseinstufung "Ausschluß" macht die Generierung einer Legitimation unmöglich. Man nennt aktive Mitglieder mit dieser Einstufung ausgeschlossene Mitglieder. Hat ein Mitglied eine Legitimation erhalten, so können ihm im Rahmen seiner Sicherheitseinstufung Nutzungsrechte erteilt und diese auch durchgesetzt werden. Ein Entzug der Legitimation ist jederzeit möglich. Dies bedeutet, daß dem Mitglied alle erteilten und durchgesetzen Nutzungsrechte nicht nur entzogen, sondern auch nicht wieder erteilt werden können. Alle Nutzungsvereinbarungen und -konfigurationen werden mit sofortiger Wirkung zerstört. Eine weniger drastische Maßnahme stellt die Aussetzung aller Nutzungsrechte dar. Während der Aussetzung können Nutzungsrechte verändert, jedoch nicht durchgesetzt werden. Die bestehenden Vereinbarungen und Konfigurationen bleiben erhalten. Abbildung 3.4 zeigt den minimalen Anfangszustand (mit einem Sicherheitssystemadministrator) eines Zugangskontrollsystems mit Legitimationen und Nutzungsrechten. Die Stellen beinhalten aus Gründen der Übersichtlichkeit nur Legitimationen mit erteilten und durchgesetzten Nutzungsrechten von Personen .

Wie sich aus der Abbildung 3.4 erkennen läßt, bildet die Durchsetzung der Nutzungsrechte eine zentrale Funktion des Systems. Sie sorgt dafür, daß die Systemkomponenten berechtigten Anfragen die jeweiligen Dienste zugänglich machen. Soll nach einer Rechteerteilung deren Umsetzung erfolgen, wird bei der Durchsetzung zunächst geprüft, ob keine Regeln der Sicherheitspolitik verletzt werden. Wenn keine Konflikte auftreten, werden diese Rechte realisiert. Eine weitere wichtige Aufgabe ist die ständige Kontrolle der Nutzungsrechte auf ihre Gültigkeit sowie auf deren Verletzungen.

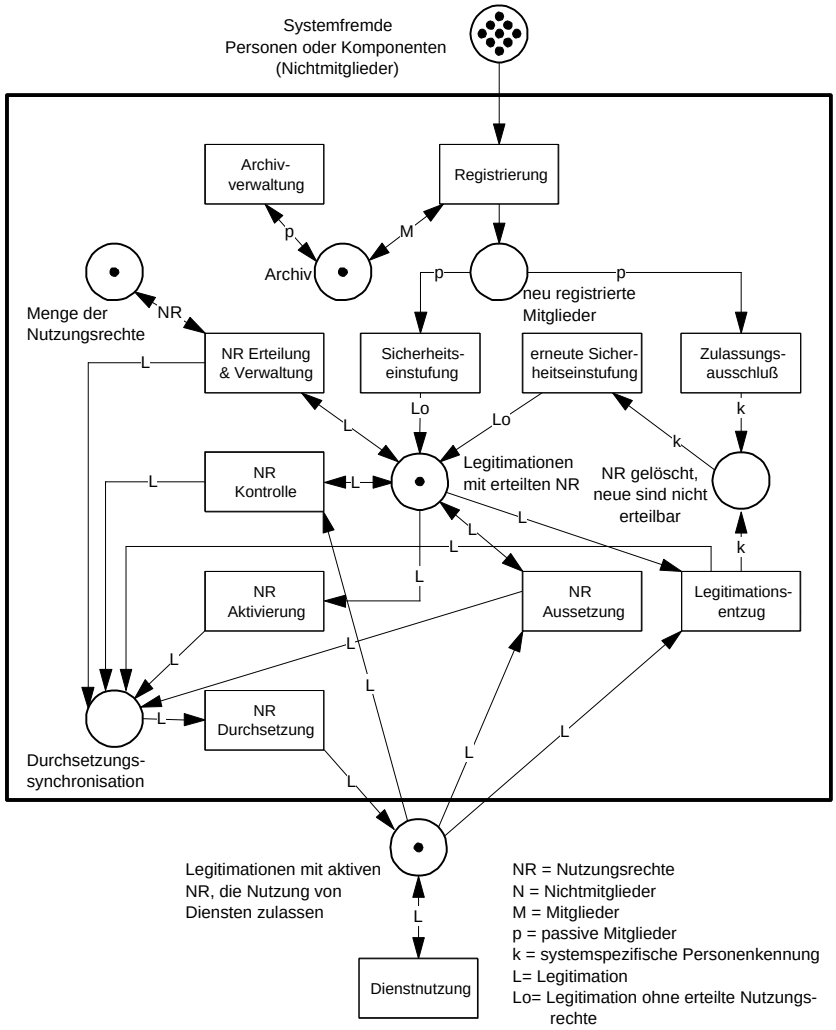
Legitimationen setzten sich aus zwei Hauptkomponenten zusammen:

1. Daten, die sich nur im Besitz des Sicherheitssubsystems befinden.

2. Daten, die sich im Besitz des Mitglieds und des Sicherheitssubsystems befinden.

Man kann sich eine Legitimation wie in Abbildung 3.5 modelliert vorstellen.

Die Daten der zweiten Hauptkomponente dienen in der Regel zur Authentifikation des Mitglieds. Eine Ausnahme bilden die Personenmitglieder in zweierlei Hinsicht. Zum einen beschreiben die sich in ihrem Besitz befindlichen Daten nicht nur ihre Identität, sondern zusätzlich deren Nutzungsrechte. Zum anderen werden diese Daten häufig auf einem oder einer Kombination aus mehreren unterschiedlichen Medien gespeichert, z.B. im Gedächtnis von Personen oder auf Karten; auch physische Merkmale (wie Finger) oder Verhaltensweisen werden als Informationsträger benutzt. Das Gedächtnis und die



Abbildung~3.4: Verwendung von Legitimationen im System

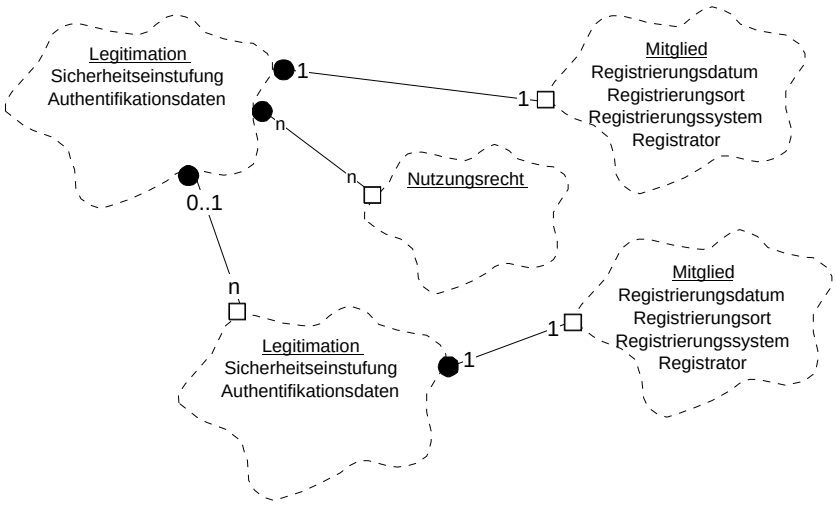
Träger der biometrischen Informationen können allerdings nur Daten zur Identifikation liefern, nicht jedoch zu Nutzungsrechten. Je sicherheitsrelevanter eine Legitimation von Personen ist, desto weniger Rechteinformationen sollten sich im Besitz des Benutzers befinden. Beispiel: Bei einem Skipaß können durchaus die Nutzungsrechte geschützt auf der Magnetstreifenkarte stehen. Bei einem Hochsicherheitssystem werden diese Daten das System nicht verlassen. Auf der Chip-Karte werden sich nur Daten und Funktionen befinden, die zu einer sicheren Identifizierung der Person beitragen.

Mit dem beschriebenen Verfahren der Legitimation ist die Verwirklichung folgender Regeln möglich:

1. Komponenten können im Zugangskontrollsystem nur genutzt werden, wenn sie überprüft sind und zum System gehören.

2. Nur Systemmitglieder können auf Systemmitglieder zugreifen.

3. Alle Zugriffsvorgänge zwischen den Mitgliedern können überprüft werden.



Abbildung~3.5: Modellierung einer Legitimation

Werden Elemente und Methoden der Legitimation derart in der Architektur des Zugangskontrollsystems verankert, daß sie eine funktionelle Notwendigkeit darstellen und nicht umgangen werden können, so ist es möglich:

- Angriffe von Personen abzuwehren, die durch:
  - ihre Person
  - Veränderung von Systemmitgliedern
  - das Einbringen systemfremder Soft- und/oder Hardwarekomponenten
  - eine Kombination dieser Methoden

  versuchen, unerlaubten Einfluß auf das System zu nehmen.
- Angriffe von Personen abzuwehren, die vom System auszuschließen sind und durch eine falsche Identität (falscher Name, verändertes Aussehen) versuchen, wieder ins System zu gelangen.
- Die Rechtmäßigkeit von Zugriffen der Systemmitglieder untereinander sicherzustellen.
- Die Vorgänge im System nachzuvollziehen.
- Eine Sicherheitspolitik durchzusetzen.

Diese Regeln und Eigenschaften sind bei Systemen zwingend notwendig, die in Bereichen zum Einsatz kommen, bei denen ein hohes Maß an Sicherheit und/oder ein Qualitätsmanagement für den Betriebsablauf erforderlich ist.

3.1.2 Personen

Alle Benutzer des SIPORT-Systems haben gemein, daß sie aufgrund von Legitimationen Dienste nutzen können. Diese Dienste werden durch das System selbst oder durch autonome Subsysteme und Maschinenanlagen erbracht.

Die Beschreibung der Einsatzszenarios zeigt zwei große Benutzergruppen für das Zugangskontrollsystem auf. Der einen gehören Firmen oder organisationsfremde Personen wie Servicemitarbeiter des Systemanbieters, Kunden und/oder Besucher an. Die andere wird durch Mitarbeiter des Systembetreibers gebildet, die sich wiederum in drei Untergruppen aufteilen. Als erstes sind die Mitarbeiter zu nennen, die Dienste des Systems nutzen, um den eigentlichen Geschäftszweck bereitzustellen und zu entwickeln sowie 'Backoffice'-Tätigkeiten zu verrichten (operativer Betrieb). Die zweite Gruppe von Mitarbeitern beschäftigt sich mit der Wartung, dem Betrieb und der Konfiguration der Infrastruktur, dem Zugangskontrollsystem und den Maschinenanlagen (Systembetrieb). Das Aufgabengebiet der dritten Gruppe ist die Aufstellung, Durchsetzung und Verbesserung der Sicherheitspolitik auf allen Systembenutzerebenen (Sicherheitsmanagement). Es kommt mitunter vor, daß eine Person verschiedenen Benutzergruppen angehört. So ist es denkbar, daß eine Person mehrere Karten mit unterschiedlichen Rechten besitzt. Meldet sie sich mit einer Karte im System an, so besitzt diese Person natürlich nur die Rechte, die durch die Daten der jeweiligen Karte erteilt sind. Werden Rechte erforderlich, die an eine andere Karte gekoppelt sind, so muß sich der Benutzer erst abmelden und mit der entsprechenden anderen Karte im System wieder anmelden.

Kunden und Gäste

Kunden und Besucher sind Systembenutzer, die nur zu ganz bestimmten Diensten Zugang erhalten können. Die Legitimation zur Nutzung dieser Dienste können an besonderen Stellen (Verkaufsstellen, Besucherbüros) erworben werden. In der Regel sind das Magnetstreifen- oder Chip-Karten. Es gibt Nutzungsrechte, die den Aufwand einer Registrierung nicht rechtfertigen oder nicht sinnvoll erscheinen lassen, wie übertragbare Tageskarten oder Punktekarten beim Skizirkus. Benutzer solcher Nutzungsrechte werden nicht unter ihren Merkmalen, sondern unter denen eines virtuellen Benutzers geführt. Diese Klasse von Nutzungsrechten kann nur dieser Benutzergruppe zugeteilt werden. Je nach Sicherheitsrelevanz gibt es weitere sehr variierende Legitimationen, die einen unterschiedlich hohen Aufwand für das System und den Benutzer implizieren.

Operativer Betrieb

Systembenutzer des operativen Betriebs beschäftigen sich mit allen Bereichen, die mit den Dienstleistungen für Kunden und Gäste sowie mit der Einhaltung administrativer Verpflichtungen mit den Geschäftspartnern zu tun haben. Die Systembenutzer des operativen Bereichs geben Legitimationen für Kunden und Gäste aus, legen im Rahmen ihrer Kompetenz Nutzungskonfigurationen fest, entwickeln neue Dienstleistungen und Tarife, sorgen für die Verteilung der Tarife und den Verkauf von Nutzungsberechtigungen, führen Abrechnungen mit den Kunden und Geschäftspartnern durch, werten Daten über die Dienstleistungen aus, usw. Die Funktionalität, die sie für sich selbst oder für die Kunden benötigen, erhalten sie von den Mitarbeitern des Systembetriebs. Nach der Registrierung, der entsprechenden Sicherheitseinstufung und Aushändigung einer

Legitimationskarte erhält ein neuer Systembenutzer des operativen Betriebs von einem entsprechend legitimierten Mitarbeiter seiner Abteilung diejenigen Nutzungsrechte, die für seine Aufgaben erforderlich sind. Benötigt ein Mitarbeiter aus arbeitstechnischen oder verhaltensbedingten Gründen eine andere Sicherheitseinstufung, so kann diese Änderung nur durch das Sicherheitsmanagement vorgenommen werden.

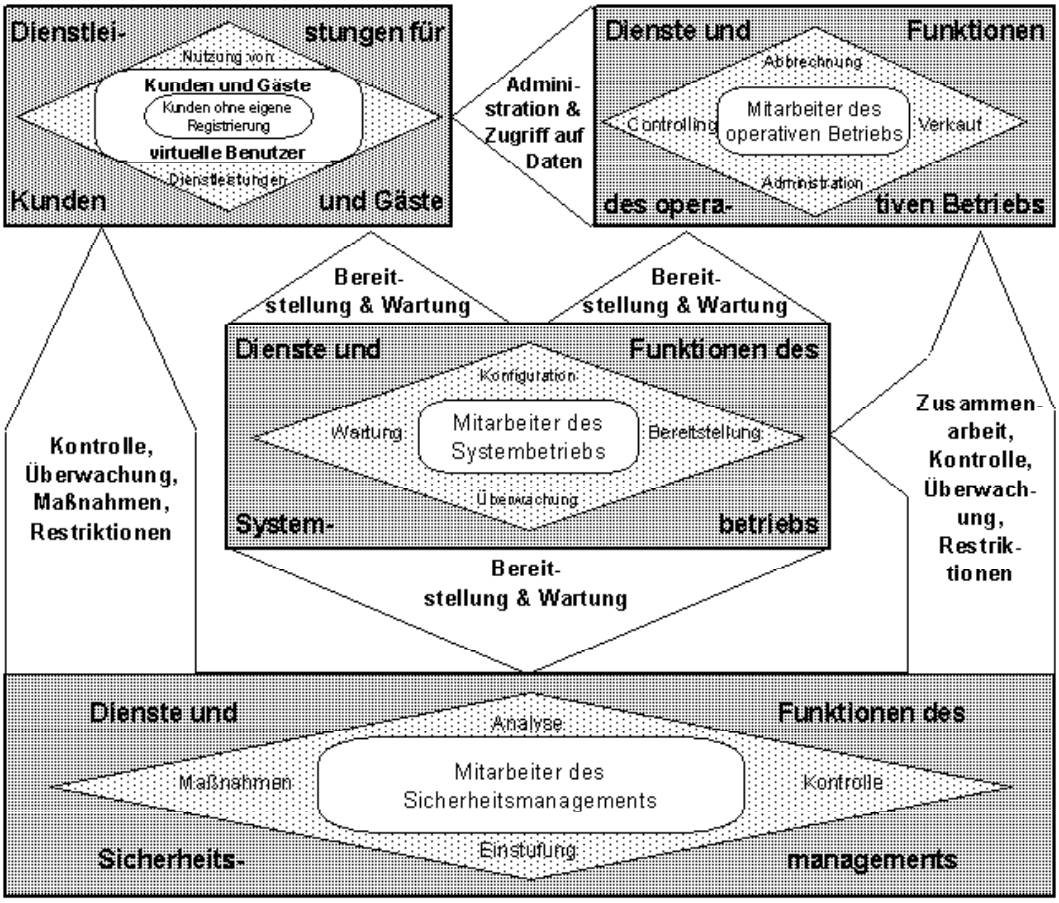
Systembetrieb

Die Mitarbeiter des Systembetriebs haben die Aufgabe, Maschinenanlagen, autonome Subsysteme, Zugangskontrollstationen und Rechnersysteme zu warten, zu überwachen, sie zu konfigurieren und Schäden zu beseitigen. Sie müssen zum einen in Zusammenarbeit mit dem operativen Betrieb und dem Sicherheitsmanagement Informationsdienste und Funktionen erarbeiten und implementieren. Zum anderen müssen diese neuen Funktionen ins Zugangskontrollsystem eingebaut und den betreffenden Benutzergruppen zu Verfügung gestellt werden. Der Aufgabenbereich der Mitarbeiter reicht vom Techniker, der Rechner und Maschinenanlagen installiert, wartet und repariert, über die Mitarbeiter der Betriebsüberwachung, welche die Rechnerleistungs-, Netzlast- und Maschinendaten kontrollieren und gegebenenfalls Maßnahmen einleiten, bis hin zu Programmierern und Technikern, die neue Funktionen oder Teile einbauen. Bei Problemen, die die Mitarbeiter des Systembetriebs nicht lösen können, werden Experten und/oder Servicemitarbeiter des Systemanbieters zugezogen, die sie bei der Problembewältigung unterstützten.

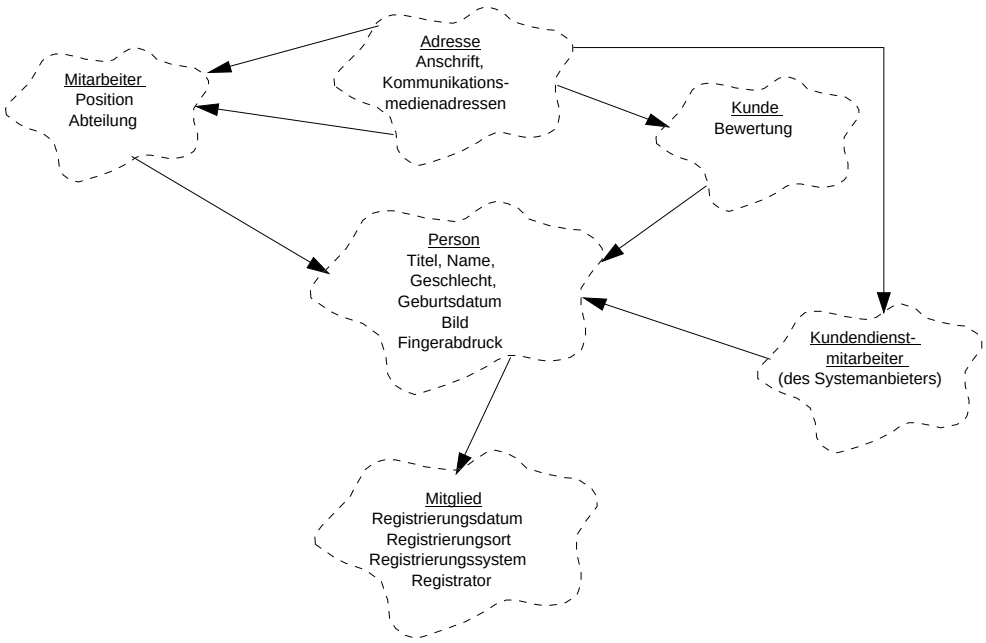
Sicherheitsmanagement

Das Sicherheitsmanagement ist für die Belange der Systemsicherheit zuständig. Die Mitarbeiter dieses Aufgabenbereichs arbeiten sehr eng mit den anderen Bereichen zusammen, um ein homogenes Sicherheitssystem aufbauen zu können, welches alle Bereiche der Systemsicherheit abdeckt. Sie erstellen eine Sicherheitspolitik und versuchen, diese durch administrative und überwachende Tätigkeiten umzusetzen. So übernimmt das Sicherheitsmanagement die Sicherheitseinstufung der Mitarbeiter, Dienste und Funktionen des Systems sowie der Maschinen. Es legt fest, wo, wann, wie, was aus sicherheitstechnischer Sicht funktionieren muß. Aus den laufenden Betriebsdaten werden Auswertungen zur Kontrolle der Umsetzung sowie Qualitätsprüfung der Sicherheitspolitik vorgenommen. Das System wird laufend überwacht, um entstehende Ausnahmesituationen frühzeitig erkennen und geeignete Gegenmaßnahmen in Zusammenarbeit mit dem Systembetrieb ergreifen zu können. Die Abbildung 3.6 zeigt zusammenfassend die Beziehungen und Rollen der einzelnen Benutzergruppen im System.

Bei der Modellierung der Personenmitglieder sollen, wie in Abbildung 3.7 dargestellt, aus Gründen der Übersichtlichkeit nur die Hauptkategorien Kunden, Kundendienstmitarbeiter des Systemanbieters und Mitarbeiter berücksichtigt werden. Eine feinere Unterteilung dieser Kategorien kann aber jederzeit ohne Beeinträchtigung der prinzipiellen Funktionsweise aufsetzender Strukturen eingefügt werden.



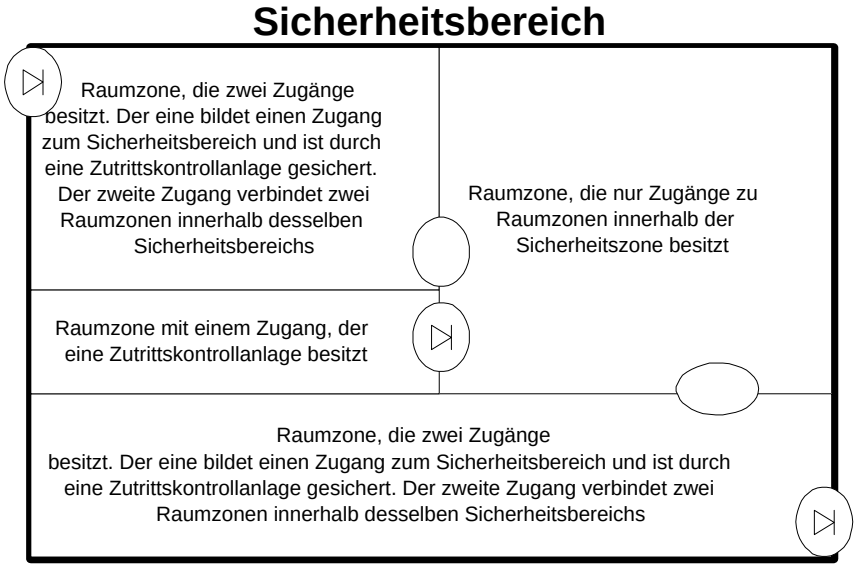
Abbildung~3.6: Beziehungen und Rollen der Systembenutzer



Abbildung~3.7: Objektmodellierung für Mitarbeiter und Kunden

3.1.3 Raumzonen und Sicherheitsbereiche

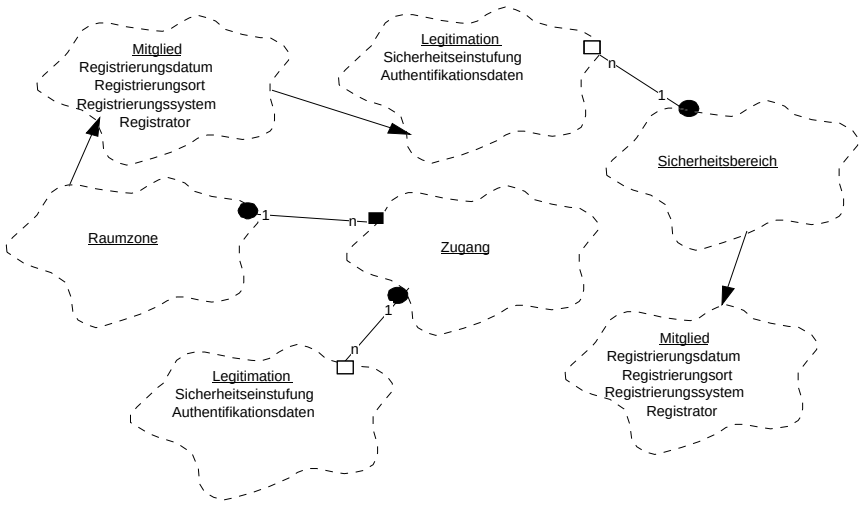
Räume, Plätze und Durchgänge, die miteinander verbunden sind, können zu einer Raumzone erklärt werden. Eine Raumzone besitzt einen oder mehrere Zugänge, Raumzugänge genannt; nur durch diese können die Mitglieder in die Raumzonen gelangen. Raumzonen sind durch Lage, Umfang und Zugänge charakterisiert. Besitzen die Zugänge einer Raumzone Zutrittskontrolleinrichtungen, so müssen diese legitimiert sein, bevor die Raumzone legitimiert werden kann. Sicherheitsbereiche können eine oder mehrere Raumzonen umfassen, die gleiche oder unterschiedliche Sicherheitseinstufungen besitzen. Sie können nur über legitimierte Raumzonen definiert werden und besitzen selbst eine Legitimation. Genau wie Raumzonen besitzen sie Zugänge. Die Menge ihrer Zugänge ist eine Untermenge der Zugänge ihrer Raumzonen. Raumzonen selbst stellen homogene Sicherheitsbereiche dar. Von einem homogenen Sicherheitsbereich redet man, wenn alle seine Raumzonen eine gleiche Sicherheitseinstufung besitzen. Abbildung 3.8 veranschaulicht die Zusammenhänge und Abbildung 3.9 zeigt die Objektmodellierung.



Abbildung~3.8: Raumzonen, Raumzugänge und Sicherheitsbereich

3.1.4 Hardwaresystemkomponenten und autonome systemfremde Subsysteme

Die zweite große Gruppe von Mitgliedern im Zugangskontrollsystem stellen Hardwarekomponenten und autonome Subsysteme dar. Zu den Hardwarekomponenten zählen ganze Systeme und deren Baugruppen, die aus elektronischen, elektrischen und mechanischen Bauelementen oder einer Kombination derselben bestehen. Die Systeme benötigen zu ihrem Betrieb eine spezielle Software (Betriebssystem). Eine besondere Klasse stellen die autonomen systemfremden Subsysteme dar. Sie können aus einer



Abbildung~3.9: Objekte der Raumzonen und Sicherheitsbereiche

Mischung von unterschiedlichster Hardware und aufwendiger Software bestehen. Die wesentlichen Unterscheidungsmerkmale zu anderen Hardwarekomponenten sind:

- Auf Parameter, Einstellungen und Konfigurationen kann nicht direkt, sondern nur indirekt über definierte Interfaces zugegriffen werden, durch mitgelieferte Treiber, mitgelieferte Programmierbibliotheken, Konfigurationsprogramme, Handbücher, usw.
- Sie erbringen eigenständig die Funktionalität, die ein Aufgabengebiet abdeckt.
- Ihre Konzeptionsstruktur entspricht nicht der des Zugangskontrollsystems.

Man kann die systemfremden Subsysteme daher jeweils als eine Blackbox betrachten , die eine ihrer Natur nach unveränderliche Funktionalität besitzt, Eingabedaten entsprechend den Steuerparametern umformt und als Ausgabedaten zur Verfügung stellt, ähnlich einer fest verdrahteten Schaltung. Aus diesem Grund werden sie in die Klasse der Hardwarekomponenten eingeordnet.

Wie alle Mitglieder des Zugangskontrollsystems, so müssen auch die Hardwarekomponenten bzw. autonomen Subsysteme eine Legitimation besitzen, bevor sie im System eingesetzt werden können. Neben den sicherheitstechnischen Gründen soll die Beschreibung dieser Komponenten die Konfiguration, Wartung, Optimierung und Überwachung des Systems ermöglichen und/oder unterstützen. Dabei werden nicht nur Daten erfaßt, die die Komponenten charakterisieren und identifizieren, sondern auch deren aktuelle Zustände und Beziehungen beschrieben. Diese Daten und deren Aktualität bilden eine Landkarte des physikalischen Systems und sind eine tragende Säule für komplexe Systeme zur Analyse oder zur Unterstützung des Krisenmanagements.

Rechnersysteme und Netzwerk

Um in der Lage zu sein, ein Rechnersystem im Zugangskontrollsystem einzusetzen, müßte dieses identifizierbar sein, bevor es eine Legitimation erhalten kann. Da jeder

Computer aus Baugruppen besteht und ein Betriebssystem benötigt, wäre ein möglicher Ansatz, zunächst alle Baugruppen, signifikanten Bauelemente (wie z.B. Prozessoren) und den eingesetzten Betriebssystemcode zu legitimieren, und aus ihnen die Identität des Rechners zu generieren. Da diese Baugruppen und der Code in der Regel alle eindeutig identifizierbar sind (Hersteller, Typ, Seriennummer, Lizenznummer, usw.), wäre die Legitimation der einzelnen Baugruppen, -elemente und der Codekopie kein Problem. Ein solches Vorgehen hätte folgende Konsequenzen:

1. Eine Legitimation kann dem Rechnersystem nur erteilt werden, wenn alle seine Baugruppen und speziellen Bauelemente eine Legitimation besitzen.

2. Die Sicherheitseinstufung des Rechnersystems kann nicht höher sein als die niedrigste seiner Komponenten.

3. Wird eine Komponente ausgetauscht oder neu eingebaut, muß eine neue Legitimation erteilt werden.

Diese Methode der Rechnerbeschreibung und Legitimation hat zwei wesentliche Nachteile. Zum einen entsteht ein erheblicher administrativer und verwaltungstechnischer Aufwand, der eine Flut von Daten mit sich bringt. Zum anderen ist dieses Verfahren alles andere als sicher, denn ein wesentlicher Punkt, nämlich der des Standortes, wird nicht in Betracht gezogen. Hat ein Rechnersystem eine hohe Sicherheitseinstufung, und wird sein Standort verändert, nicht jedoch seine Komponentenkonfiguration, so behält er seine Sicherheitseinstufung bei. Auf diese Weise könnten sicherheitsrelevante Daten und Prozesse in Raumzonen betrachtet, geändert bzw. angestoßen werden, die nicht der Sicherheitseinstufung des Rechnersystems entsprechen; sicherheitstechnisch ist dies ein nicht akzeptierbarer Mangel. Rechnersysteme sollen daher durch ihre Komponenten und ihren Standort — Raumzone, in der sie installiert wurden — beschrieben werden. Zur Legitimation des Computers müssen die Raumzonen eine Legitimation besitzen, und je nach deren Sicherheitseinstufung erhalten die einzelnen Komponenten eine entsprechende Legitimation. Diese Methode ermöglicht eine freie Sicherheitsskalierbarkeit bei einem vertretbaren Verwaltungsaufwand.

Genau wie Rechnersysteme bestehen Netzwerke aus Komponenten. Die Komponenten sind in Gruppen einzuteilen:

- Komponenten, die das Netzwerk benutzen (z.B. angeschlossene Rechnersysteme, deren Dienste Kommunikation benötigen)

- Komponenten, die den Netzwerkbetrieb ermöglichen (z.B. Bridges, Router, Gateways)

Eine Spezifikation des Rechnernetzes soll aufgrund des Adressraumes des TCP/IP-Protokolls der angeschlossenen Komponenten vorgenommen werden. Mitunter gehören Komponenten beiden Gruppen an, z.B. nondedicated Server. Sie sind aber eher in kleineren Anlagen zu finden, bei denen der Rechenaufwand für Netzdienste gering ist. Eine neue Legitimation des Netzwerks muß vorgenommen werden, wenn eine Komponente angeschlossen werden soll, deren Sicherheitseinstufung unter der niedrigsten der bereits angeschlossenen Komponenten liegt. Je nach Sicherheitseinstufung müssen die Netzwerke spezielle Dienste und Netzstrukturen aufweisen, um die Regeln der Sicherheitspolitik durchsetzten zu können.

Legitimationskartenausgabestationen

Die Aufgabe der Legitimationskartenausgabestationen ist es, den legitimierten Personenmitgliedern Rechte im System zu erteilen, die Legitimationskarten den Personen zuzuordnen und auf ihnen die Authentifikationsdaten zu speichern. Je nach Anwendung werden mitunter auch Nutzungsrechtdaten sowie Kontrolldaten zur Kartenverifikation auf die Karten geschrieben. Die Legitimationskartenausgabestationen bestehen aus einem Rechner, einem Gerät zum Beschreiben bzw. Programmieren der Legitimationskarten und teilweise einem Spezialdrucker zum Bedrucken der Legitimationskarten. Kassen beim Skizirkus oder bei Messen besitzen außerdem ein "Point of Sale Terminal" zur Verarbeitung von Eurocheck- und Kreditkarten, eine Geldschublade und einen Belegdrucker. Alle drei werden durch den Rechner angesteuert. Eine weitere Version der Kassen sind Kassenautomaten. Sie besitzen statt der einfachen Geldschublade eine Kassiereinrichtung, die das Geld entgegennimmt, kontrolliert, verwahrt und das Wechselgeld dem Kunden zurückgibt.

Die einzelnen Komponenten der Legitimationskartenausgabestationen müssen vom System erfaßt sein, bevor sie zu einer Systemkomponente Legitimationskartenausgabestation gruppiert werden können. Zusammen mit einem legitimierten Standort kann eine Legitimationskartenausgabestation selbst legitimiert werden.

Zugangskontrolleinrichtungen

Zugangskontrolleinrichtungen besitzen zwei Hauptgruppen :

1. Zugangskontrollstationen
2. Zutrittskontrollstationen

Zugangskontrollstationen kontrollieren den Zugang zu Funktionen und Diensten des Zugangskontrollsystems oder zu anderen Informationssystemen, die nicht eigentlicher Teil des Zugangskontrollsystems sind. Die Zugangskontrollstation wird in der Regel von einem Front-end-Rechner gebildet, der mit unterschiedlichen Methoden die Identität der Benutzer prüft. Bei einfachen Konfigurationen wird nur eine Paßwortüberprüfung vorgenommen. Bei aufwendigeren Konfigurationen wird mit Hilfe von Kartenleser und/oder Fingerprintscanner die Identität des Benutzers festgestellt. Nach der erfolgreichen Benutzererkennung stellt der Rechner entsprechend den Rechten und Anfragen des Anwenders den Zugang zu den Diensten zur Verfügung.

Zutrittskontrollstationen kontrollieren genau wie die Zugangskontrollstationen die Identität und/oder Nutzungsberechtigung der Benutzer. Fällt die Identifikation positiv aus, so werden Barrieren angesteuert, die den Zutritt zu Raumzonen oder Dienstleistungen freigeben oder Zugriff auf Gegenstände ermöglichen (Shoppingautomaten, Schließfächer, usw.). Je nach Erfordernissen sind diese Stationen einfach aufgebaut oder besitzen — vergleichbar mit den Kassenautomaten — aufwendige Kassiereinrichtungen. Die Legitimation der Zugangskontrolleinrichtungen wird genau wie die der Legitimationskartenausgabestationen vollzogen. Erst wenn alle Teilkomponenten erfaßt, zu einer Systemkomponente gruppiert und an einem legitimierten Standort installiert sind, können sie von Personenmitgliedern genutzt werden.

Informations- und Serviceterminals

Informations- und Serviceterminals sind spezielle Zugangskontrollstationen, die von Kunden und Gästen genutzt werden. Sie stehen in Raumzonen, zu denen der genannte Personenkreis Zutritt hat. Die Bedienung der Terminals ist durch grafische Benutzeroberflächen und Touchscreens sowie Sound-Unterstützung einfach und komfortabel. Serviceterminals bieten neben Informationen erweiterte Dienstleistungen wie Buchungen, Überweisungen, Anforderung von Informationsmaterial, welches postalisch zugestellt werden soll, usw. Eine Identifikation des Terminalbenutzer ist von den angeforderten Diensten abhängig. Die Terminals sind in der Regel an ein Netzwerk angeschlossen und können ferngesteuert konfiguriert und überwacht werden.

Überwachungs- und Steuereinrichtungen

Das Einsatzgebiet der Überwachungs- und Steuereinrichtungen ist ebenso vielfältig wie deren mögliche Konfigurationen. Gemeinsam ist allen, daß sie einen oder mehrere Rechner mit aktiven oder passiven Baugruppen besitzen, die

- Ist-Wert Daten unterschiedlichster Art über Sensoren, Detektoren, visuellen oder akustischen Einrichtungen erfassen und digital aufbereiten,
- Parameter von technischen Einrichtungen und Anlagen abfragen und ändern können.

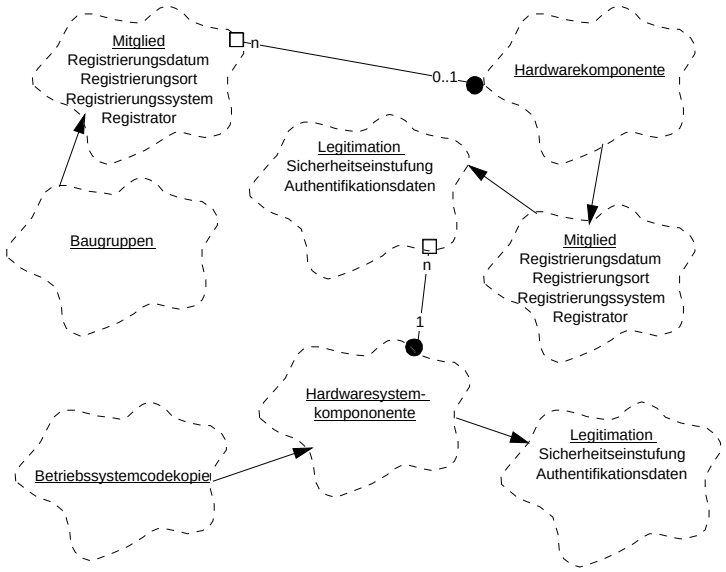
Der Rechner kann die gelieferten Daten auswerten, weiter aufbereiten und Maßnahmen einleiten wie z.B. Ändern von Betriebsparametern, Absetzen einer Meldung an das Betriebspersonal usw. Er kann jedoch auch dazu dienen, die Anlage fernzusteuern oder Fernwartungen vorzunehmen, soweit dies möglich ist.

Die dargestellten Hardwaresystemkomponenten können selbst Teilkomponenten einer anderen, übergeordneten Systemkomponente sein. Sie stellen Bausteine dar, aus denen komplexe Systemkomponenten entstehen, die nach Bedarf auch autonom arbeiten können. Solche zusammengesetzte Systemkomponenten müssen dann auch eine Systemlegitimation besitzen. Sie können diese erhalten, wenn alle ihre Teilsysteme legitimiert sind. Abbildung 3.10 zeigt die Modellierung der Hardwaresystemkomponenten.

3.1.5 Softwaresysteme, Dienstleistungen

Die letzte große Gruppe von Mitgliedern im Zugangskontrollsystem bilden die Softwaresysteme und deren Dienstleistungen. Ihre Registrierung und Legitimation soll das unkontrollierte Einbringen von Programmcodes ins Zugangskontrollsystem verhindern, eine Basis zur Vereinfachung und Automatisierung von Wartungsarbeiten (Installation von Updates, Einbringen neuer Funktionen) bilden und eine Überwachung und Beeinflussung des ausgeführten Codes ermöglichen.

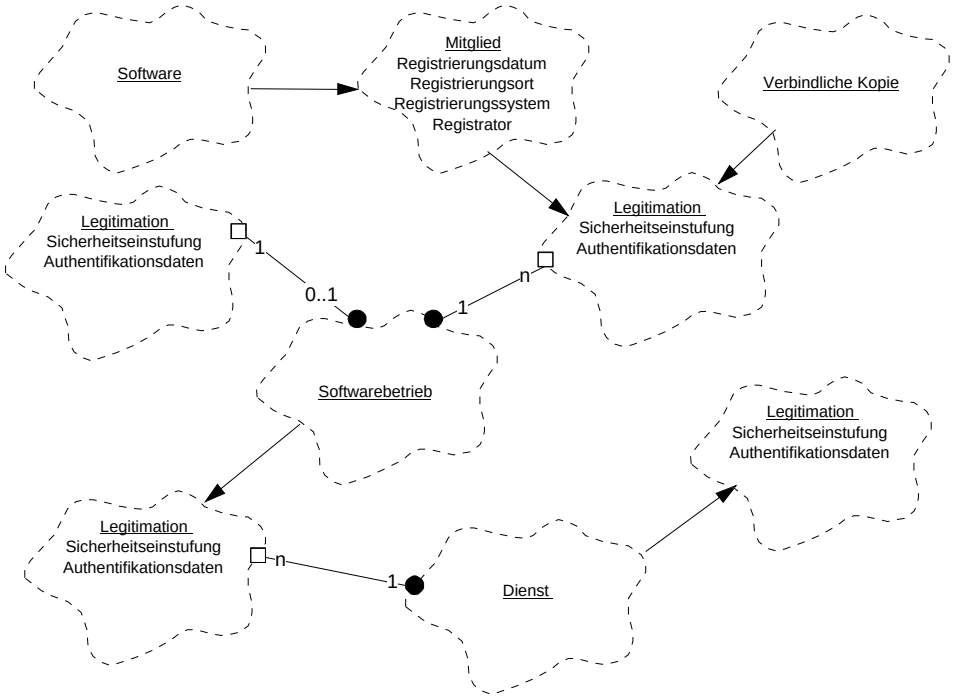
Programmcodes werden durch die Archivierung ihrer Binär- und/oder Quellendarstellung, Zusatzcharakterisierung (z.B. Name, Versionsnummer, Buildnummer, usw.)



Abbildung~3.10: Baugruppen, Hardwarekomponenten und Hardwaresystemkomponenten

und Zusatzinformationen (Dokumentationen, systemeigene Typ- und Funktionsbeschreibung) registriert. Nach der Registrierung können sie durch ihre Sicherheitseinstufung und der Fixierung ihres Wesens (Binär- und Quellcodes), durch Prüfsummen und eine elektronische Unterschrift legitimiert werden. Zur Code-Installation wird eine Kopie des fixierten Codes in einen exklusiven Zugriffsbereich des Installationsrechners gebracht, der mit einem entsprechenden Schlüssel die Datei bzw. Dateien dechiffriert und deren Inhalt anhand mitgelieferter Prüfsummen überprüft. Erst nach der erfolgreichen Installation können die Dienste dieser Codes durch eine Nutzungslegitimierung von anderen Systemmitgliedern genutzt werden.

Um eine bessere Leistungsausnutzung der vorhandenen Hardwareressourcen zu erreichen, sollen im neuen Zugangskontrollsystem nicht nur Programme mit statischem Ausführungsverhalten, sondern auch Programmsysteme mit dynamischem Verhalten eingesetzt werden. Sie sollen in der Lage sein, sich entsprechend der an sie gestellten Leistungsanforderungen und der freien Prozessorkapazitäten im System dynamisch auszubreiten oder zurückzuziehen. Diese dynamischen Programmsysteme erhalten eine eigene Sicherheitsidentität und besitzen eine eigene Sicherheitsinstanz, die ihren Funktionen bzw. Diensten eine eigene Sicherheitseinstufung vergibt. Dienste sind sehr mächtige Funktionen, die durch unterschiedlichste Einbeziehung von Softwarekomponenten des Softwaresystems selbst und/oder anderer Komponenten des Zugangskontrollsystems erbracht werden. Soll der Funktionsumfang eines Programmsystems geändert werden, so erhält es genau wie die Hardwaresysteme eine fixierte Codekopie; diese wird bei Akkumulation im Programmsystem und bei jedem Ersteinsatz auf einer Verarbeitungseinheit von der eigenen Sicherheitsinstanz des Programmsystems überprüft. Abbildung 3.11 zeigt die Modellierung der registrierten, zur Installation und zum Einsatz legitimierten Softwarekomponenten und Dienste.



Abbildung~3.11: Zur Installation und zum Betrieb registrierte und legitimierte Software und Dienste

3.2 Funktionalität

Die Zielsetzung, ein frei konfigurierbares Zugangskontrollsystem zu bauen, das auf die Ansprüche des Einsatzgebietes angepaßt werden kann, macht es notwendig, neben den eigentlichen Zugangskontrollfunktionen erweiterte, unterschiedliche Dienste und Funktionen ins System zu integrieren. Darüber hinaus variieren aber auch Umfang und Art der Zugangskontrollfunktionen durch die unterschiedlichen Installationsgrößen und Sicherheitsansprüche. Alle Systeminstallationen benötigen jedoch einen elementaren Befehls- und Funktionsumfang, der den Aufbau und die Verwaltung eines laufenden Systems bereitstellt. Diese Funktionen sollen Basisfunktionen genannt werden. Die darüberhinaus benötigten Dienste und Funktionen setzen entweder auf diese Basisfunktionen auf, indem sie diese Funktionen erweitern und ausbauen bzw. indem diese Dienste und Funktionen die Basisfunktionen für ihre eigenen Zwecke benötigen; oder sie bilden eine eigene Funktionshierarchie, in der sie Aufgaben erfüllen, welche nicht unmittelbar zu denen der Zugangskontrolle zu zählen sind.

3.2.1 Basisfunktionalität

Abbildung und Durchsetzung einer Sicherheitspolitik

Die Erstellung und Durchsetzung einer Sicherheitspolitik ist insbesondere bei Systeminstallationen, denen eine hohe Sicherheitsrelevanz zugemessen wird, ein wesentliches Kernstück. Zentrale Punkte einer Sicherheitspolitik sind:

- Definition und Beschreibung von Sicherheitseinstufungen:
  - Festlegung des prinzipiellen Aufbaus der Sicherheitseinstufungen (Sensitivity Labels) der Mitglieder des Systems
  - Festlegung und Bedeutungsbeschreibung der Attributmengen der Strukturelemente der Sicherheitseinstufungsnomenklatur
- Bewertungsregeln der Sicherheitseinstufungen, die den prinzipiellen Umgang der Systemmitglieder miteinander festlegen
- Definitionen und Bewertungen von Ereignissen und Alarmen
- Definition von Ausnahmesituationen und entsprechenden Reaktionsanweisungen
- Festlegung von Richtlinien und Vorgehensstrategien zur Sicherheitseinstufung von Systemmitgliedern
- Festlegung von Überwachungsmaßnahmen
- Regeln zur Registrierung von Systemkomponenten
- Regeln zur Erteilung und Durchsetzung von Nutzungsrechten

Das Zugangskontrollsystem muß Funktionen und Mechanismen besitzen, die das Sicherheitsmanagement bei der Definition, Bewertung und Überarbeitung der aufgestellten Sicherheitspolitik unterstützen und die Durchsetzung der aufgestellten Regeln garantieren.

Ur-Installation

Die Erstinstallation bzw. Ur-Installation stellt aus sicherheitstechnischer Sicht einen äußerst gefährdeten Vorgang im Betrieb eines Zugangskontrollsystems dar. Der Grund liegt darin, daß noch nicht alle Sicherheitsmechanismen aufgebaut und in Funktion gesetzt sind. Dadurch ist es Angreifern möglich, unzulässige Änderungen vorzunehmen, die sich möglicherweise im gesamten System fortpflanzen und dadurch nur schwer oder gar nicht mehr rückgängig zu machen sind.

Es müssen deshalb spezielle Mechanismen und Vorgehensweisen bei der Installation vorgesehen werden, die potentiellen Angreifern keine Möglichkeiten einräumen, in dieser Phase auf das System in irgendeiner Art und Weise einwirken zu können. Die Kette dieser Mechanismen wird spätestens bei der Auslieferung der Anlage — also bereits beim Hersteller — beginnen müssen und endet bei der vollständigen Aktivierung der Sicherheitsmechanismen des Systems.

Registrierung

Voraussetzung zum Betreiben eines Sicherheitsmanagements ist, daß alle Systemkomponenten identifizierbar sind. Die Registrierung soll, wie bereits beschrieben, die charakterisierenden Merkmale der Systemkomponenten erfassen, diese archivieren und den

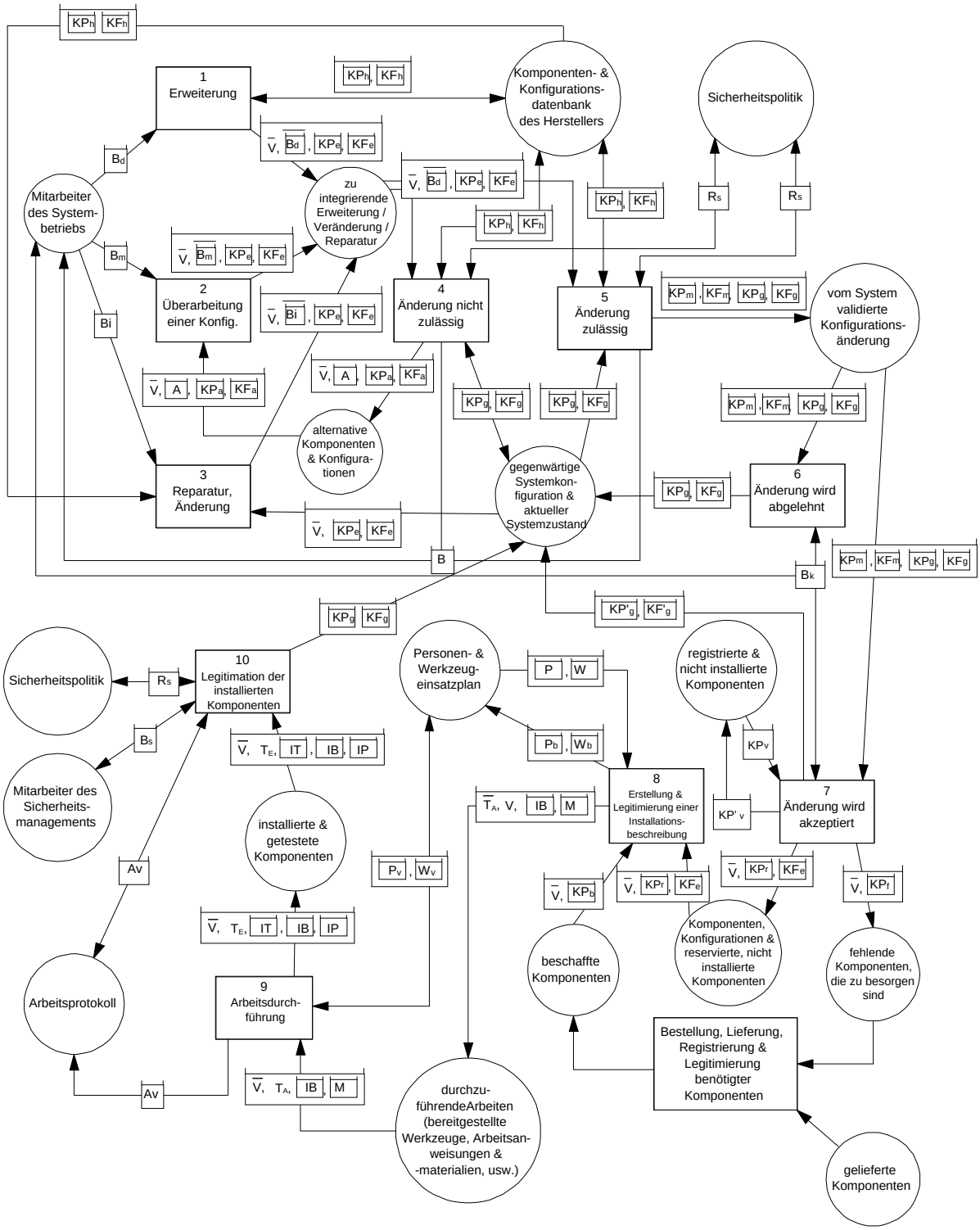
Komponenten eine systemweit eindeutige Kennung zuordnen. Die erfaßten Daten unterstützen die Aufgaben der Installation und Wartung. Die Gesamtheit der Daten aus der Registrierung bilden somit eine Art Inventarliste des Systems. Für die Erfassung und Archivierung der Daten müssen geeignete Funktionen und Methoden vom Zugangskontrollsystem bereitgestellt werden.

Installation und Wartung

Auch die Installation und Wartung eines Zugangskontrollsystems muß in die Sicherheitspolitik einbezogen werden, um ein homogenes Sicherheitssystem bereitstellen zu können. Das Zugangskontrollsystem soll durch ein Konfigurations- und Arbeitsmanagementsystem die Betriebssicherheit erhöhen und die Reaktionszeit auf Ausfälle von Systemkomponenten möglichst gering halten. Beide Managementsysteme bilden zusammen mit einem Regelwerk, welches kontinuierliche Kontrollen, Protokollierung der durchgeführten Arbeiten und regelmäßige Weiterbildungen der Mitarbeiter festlegt, Grundlage für ein Qualitätsmanagementsystem. Bei Hochsicherheitssystemen ist das Regelwerk durch die Sicherheitspolitik festgelegt. Das SIPORT-Zugangskontrollsystem muß daher in der Lage sein, dieses Regelwerk abzubilden und durch ein Überwachungssystem sicherzustellen, daß Wartungsintervalle eingehalten und Mitarbeiter regelmäßig weitergebildet werden.

Das Konfigurationsmanagement besteht aus einem Informationssystem, das die vom Zugangskontrollsystem unterstützten Komponenten- und Systemkonfigurationen sowie die registrierten und bereits installierten Komponenten bereitstellt; außerdem unterstützt es bei der Konfigurierung neu einzubauender oder zu ersetzender Komponenten. Ist eine sinnvolle Konfiguration gefunden und vom Systembenutzer akzeptiert worden, werden die Daten dem Arbeitsmanagementsystem übermittelt.

Anhand der übermittelten Daten bestimmt das Arbeitsmanagement die benötigten Komponenten, reserviert diejenigen, die verfügbar (registriert und noch nicht installiert) sind und veranlaßt die Beschaffung der übrigen. Sind die fehlenden Komponenten geliefert, registriert und legitimiert, wird eine Installationsbeschreibung angefertigt, die die notwendigen Arbeitsschritte und deren zeitlichen Ablauf, die Dokumentationspflichten und Fortschrittsmeldungen, die benötigten Arbeitsmittel und Qualifikation der Mitarbeiter beschreibt. Anschließend werden Personen und Arbeitsmittel gebucht, und vom Sicherheitsmanagement eine Durchführungslegitimation für die Installationsbeschreibung eingeholt. Ist diese erteilt, können die Installationsarbeiten entsprechend den Festlegungen in der Installationsbeschreibung durchgeführt werden. Dabei überwachen Sicherheitsmanagement und Systembetrieb die Erstellung von Dokumentation und Fortschrittsberichten. Ist die Installation abgeschlossen und die korrekte technische Funktion festgestellt, legitimiert das Sicherheitsmanagement die neuen Komponenten unter Einbeziehung der Installationsdokumentation. Mit der Legitimierung werden sie Teil der gegenwärtigen Systemkonfiguration. Abbildung 3.12 verdeutlicht den geschilderten Sachverhalt in Form eines NF^2-Relationen/Transitionen-Netzes.



Abbildung~3.12: Abläufe beim Konfigurations- und Arbeitsmanagement

Funktionsbeschreibungsergänzung der Transitionen in Abbildung 3.12:

Nr	Beschreibung
	Funktion
1	Erweiterung
	$KP_e = ks(B_d, KP_h)$ $KF_e = \cup_{i,j}^{n} kre(B_{d,}(ke(K_i, p_{i1}, ..., p_{ir}), ke(K_j, p_{j1}, ..., p_{js})), v_{ij1}, ..., v_{ijt})$ mit $i, j = 1, ..., n;\ n = card(KP_e);\ i \neq t;\ r, s, t \in \mathbb{N}_0$
2	Überarbeitung einer Konfiguration
	$KP_e = ks\ddot{u}(B_d, KP_h)$ $KF_e = \cup_{i,j}^{n} kr\ddot{u}(B_{d,}(k\ddot{u}(K_i, p_{i1}, ..., p_{ir}), k\ddot{u}(K_j, p_{j1}, ..., p_{js})), v_{ij1}, ..., v_{ijt})$ mit $i, j = 1, ..., n;\ n = card(KP_e);\ i \neq t;\ r, s, t \in \mathbb{N}_0$
3	Reparatur, Veränderung
	$KP_e = ksv(B_d, KP_h)$ $KF_e = \cup_{i,j}^{n} krv(B_{d,}(kv(K_i, p_{i1}, ..., p_{ir}), kv(K_j, p_{j1}, ..., p_{js})), v_{ij1}, ..., v_{ijt})$ mit $i, j = 1, ..., n;\ n = card(KP_e);\ i \neq t;\ r, s, t \in \mathbb{N}_0$
4	Änderung nicht zulässig
	$VEP = kpv(KP_e, KP_g, KP_h)$ $VEK = kfv(KF_e, KF_g, KF_h, R_s)$ $\overline{VEB(VEP, VEK)} \rightarrow (AB(A, KP_a, KF_a) \mid A = (V, VEP, VEK))$
5	Änderung zulässig
	$VEP = kpv(KP_e, KP_g, KP_h)$ $VEK = kfv(KF_e, KF_g, KF_h, R_s)$ $VEB(VEP, VEK) \rightarrow NSB(VEP, VEK, KP_m, KF_m)$
6	Änderung wird abgelehnt
	$\overline{SMA(B_k, KP_g, KF_g, KP_m, KF_m)} \rightarrow KV(SMA(B_k, KP_g, KF_g)$
7	Änderung wird akzeptiert
	$SMA(B_k, KP_g, KF_g, KP_m, KF_m)$ $\rightarrow (KVB(KP_g^{'}, KF_g^{'}, KP_m, KF_m, KP_g, KF_g)$ $\wedge KBV(KP_r, KP_f, KP_v^{'}, KP_v, KP_m) \wedge IEV(V, KP_r, KF_e))$
8	Erstellen & Legitimation einer Installationsbeschreibung
	$(KV(V, KP_b, KP_r) \wedge PWV(P_b, W_b, P, W))$ $\rightarrow (EIL(IB, M, KF_e, KP_m) \wedge IAE(T_a, V, IB, M))$
9	Arbeitsdurchführung
	$AO(V, T_a) \rightarrow AD(A_v, T_e, IT, V, IB)$
10	Legitimation der installierten Komponenten
	$L(A_v, T_e, IT, IP, V, IB, R_s, B_s) \rightarrow AK(KP_g, KF_g, V, IP)$

Rechteverwaltung und -durchsetzung

Die einzelnen Abteilungen des Systembetreibers müssen in der Lage sein, selbständig über die Nutzung der ihnen vom Systembetrieb zugeteilten Systemressourcen im Rahmen der Sicherheitspolitik und entsprechend den Richtlinien des Betriebs zu verfügen. Wichtig ist, daß sie auf der einen Seite die einzigen sind, die über ihre Ressourcen verfügen können, und auf der anderen Seite prinzipiell nicht in Lage sind, Rechte in ihrem Bereich zu erteilen und/oder durchzusetzen, die nicht der Sicherheitspolitik entsprechen. Außerdem dürfen sie keine Nutzungsrechte erhalten, mit denen sie zur Nutzung von nicht zugeteilten Ressourcen befähigt würden. Sollen einer Abteilung weitere Ressourcen zugeteilt werden, so muß dieser Vorgang von entsprechend autorisierten Mitarbeitern akzeptiert werden. Dasselbe gilt für die Zuteilung von Nutzungsrechten an Mitarbeiter der Abteilung.

Überwachung und Fernsteuerung

Eine mehrschichtige Überwachung und Fernsteuerung der Systemkomponenten und Vorgänge im System soll ein effizientes Handeln für die Aufgaben des Systembetriebs und des Sicherheitsmanagements ermöglichen. So erscheint es wenig sinnvoll, die Mitarbeitern des Sicherheitsmanagements in einer Krisensituation eine technisch komplizierte Maschinenanlage steuern zu lassen. Andererseits würde die Datenflut, die vom Sicherheitsmanagement laufend zur Einschätzung des momentanen Zustandes benötigt wird, die Mitarbeiter des Systembetriebes bei ihrer Arbeit eher behindern.

Aus diesem Grund soll der Systembetrieb über Zustandsdaten und Steuereinrichtungen verfügen, die zur Überwachung und Steuerung des rein technischen Betriebs erforderlich sind. Dazu zählen neben der allgemeinen Ausfalldetektion die Suche nach deren Ursachen sowie nach den defekten Komponenten, die Behebung des Schadens und nicht zuletzt auch die Konditionierung und Optimierung des Gesamtsystems. Es können Zustandsdaten von Maschinenanlagen und anderen technischen Betriebseinrichtungen abgefragt und verändert werden, womit unmittelbar auf den Betrieb dieser Systemkomponenten Einfluß genommen wird. Das Sicherheitsmanagement auf der anderen Seite analysiert laufend Daten von sicherheitstechnischer Bedeutung, um in der Lage zu sein, sich anbahnende Krisensituationen prognostizieren, entsprechende Gegenmaßnahmen einleiten und Sicherheitslücken des Systems erkennen und beheben zu können. Zu diesem Zweck haben sie die Möglichkeit, über Daten von Barrieren und zugehörigen Systemen (z.B. Vereinzelungsanlagen), Kontrolleinrichtungen sowie visuelle und akustische Überwachungssysteme (Sensoren/Detektoren) online zu verfügen; ebenso können sie diese sicherheitstechnischen Einrichtungen konfigurieren und fernsteuern.

Bei Situationen und Systemzuständen, zu deren Bewältigung das Wissen und die Erfahrung beider Abteilungen benötigt werden, einigen sich die Abteilungen, wer bei den gemeinsam fortzuführenden Arbeiten die Leitung übernimmt. Der Datenfluß wird an die führende Abteilung umgelenkt, selbst wenn diese für einen Teil der nun eintreffenden Daten keine Zugangsberechtigung hat. Sie ist von diesem Moment an für die weitere Kanalisierung der sie erreichenden Daten zuständig und verantwortlich.

Zugangskontrolle

Wie bereits in der Einleitung beschrieben, muß das System in der Lage sein, den rechtmäßigen Zugang von Subjekten zu Objekten sicherzustellen. Die beteiligten Subjekte und Objekte müssen dem System bekannt sein, soll ihnen ein Zugangsrecht eingeräumt bzw. soll der Zugang zu ihnen geschützt werden. Zur Gewährung des Zugangs von Subjekten zu Objekten müssen die Subjekte ihre Identität dem System nachweisen.

3.2.2 Erweiterte Funktionalität

Statistische Verarbeitung vorgefallener Ereignisse

Die Mitarbeiter des operativen Betriebs der Systembetreiber von DNB-Systemen benötigen Informationen über Merkmale ihrer Kunden und deren Verhalten im System. Diese Informationen werden aus den Ereignissen im System generiert und müssen zum Teil online zur Verfügung stehen. Typische online- und offline-Auswertungen sind in Abschnitt 2.3 (geplante Einsatzszenarios) beschrieben.

Weiterleitung von Ereignissen

Über die im voranstehenden Abschnitt genannten Forderungen hinaus verlangen die Betreiber von Liftanlagen bei der Bildung eines Pools, daß Informationen, die über Inhaber von Pooltickets bei den einzelnen Liftgesellschaften generiert wurden, an die Poolzentrale online übermittelt werden.

Abrechnung von Dienstleistungen

Die von den einzelnen Geschäftspartnern erbrachten Leistungen werden nach Übermittlung der entsprechenden Ereignisdaten und deren Validierung durch das System aufgrund der geltenden Übereinkünfte abgerechnet. Die sich daraus ergebenden Vergütungen bzw. Belastungen werden berechnet, mit den Einnahmen abgeglichen und entsprechende Kontobewegungen vorgenommen.

Erstellung von Tarifen und deren Verteilung

Ein wichtiges Werkzeug, das von den Mitarbeitern des operativen Betriebs benötigt wird, ist ein Generator für Tarife. Diese Tarife können auf Basis der bei der Ereignisauswertung gewonnenen Informationen als am Bedarf des Kunden orientierte Produkte generiert werden. Entsprechend den Vertriebsstrategien des DNB-Betreibers werden diese Tarife an die eigenen Verkaufsstellen und die der Geschäftspartner übermittelt.

Spezielle Funktionen für Kassen und Informationsterminals

Das neue SIPORT-Zugangskontrollsystem soll bei seiner Verwendung als DNB-System Kassen und Informationsterminals betreiben und entsprechend erweiterte Funktionen im Rahmen der Systemintegration bereitstellen. So sollen auch die Zustandsdaten von Verkaufsstellen (wie z.B. verkaufte Produkte [Kartentypen, Erzeugnisse, Leistungen], besetzte Verkaufsstellen, Umsatz, Zahlungsart, usw.) oder Informationsterminals (z.B.

häufig nachgefragte Informationen, zeitlicher Ablauf der Anfragen) mit in die statistische Auswertung einbezogen werden; diese Daten geben eine umfassendere und exaktere Analyse der Ereignisse und sind damit insbesondere bei der Erstellung und Planung von speziellen Veranstaltungen und neuen Produkten von Interesse. Neben den Abfragen von Daten soll auch eine Neukonfigurierung der Kassen und Informationsterminals mit neuen Tarifen bzw. aktualisierten Informationen möglich sein.

Steuerung von Maschinenanlagen

Die Steuerung von Maschinenanlagen ist ein weiterer Aspket der Systemintegration, die durch das neue SIPORT-Zugangskontrollsystem ermöglicht werden soll. Neben den reinen Steuerungsaufgaben sollen Daten über Auslastung, Systemausfälle und andere Ereignisse erfaßt, protokolliert, statistisch aufbereitet und für die strategische und betriebswirtschaftliche Produktplanung bereitgestellt werden. Eine zentrale Systembetriebsüberwachung, die gezielt die Betriebsdaten sammelt und auswertet und so bei außergewöhnlichen Ergebnissen reagieren kann, soll einen optimierten, kosteneffizienten Betrieb ermöglichen.

Kapitel 4

Systementwurf

Plattformunabhängigkeit und der Betrieb in heterogenen Plattformumgebungen, Integration systemfremder Teilsysteme und die Bereitstellung von Diensten beliebiger Funktionskomplexität, die alle Systemkomponenten als ein geschlossenes Gesamtsystem erscheinen lassen, sowie Verfügbarkeit spezieller sicherheitstechnischer Verfahren sind die wesentlichen technischen Herausforderungen, die an die Architektur des neuen SIPORT Zugangskontrollsystems gestellt werden. Es wird daher eine Zwischenschicht benötigt, die die heterogenen Systemplattformen unifiziert und die Einrichtung und Ausführung von Diensten ermöglicht. Diese Zwischenschicht begründet den Einsatz einer Organisationsform von eigenständigen und abgeschlossenen Teilsystemen, die einander zugeordnet sind und nach außen als eine geschlossene Einheit auftreten. Jedes dieser Teilsysteme kann als ein Anbieter und Ausführungskoordinator von Diensten betrachtet werden, die nicht nur von ihm selbst, sondern auch durch die Dienste anderer Teilsysteme seiner Gruppe oder anderer Gruppen erbracht werden. Sie sind damit in der Lage, sich bei Bedarf dynamisch auf weitere Systemteile auszubreiten bzw. wieder zurückzuziehen. Die Mitglieder einer Gruppe kommunizieren und arbeiten miteinander nach gruppenspezifischen Regeln, deren Einhaltung durch ein bestimmtes Mitglied sichergestellt wird. Benötigt ein Mitglied Funktionen oder Dienste, die es selbst nicht erbringen kann, so fragt es bei den anderen Gruppenmitgliedern um diesen Dienst nach. Bewerben sich ein oder mehrere Mitglieder um diesen Auftrag, prüft das nachfragende Mitglied die Angebote. Es tritt mit demjenigen Bewerber in Verhandlung, der mit dem attraktivsten Angebot geantwortet hat. In der Verhandlung einigen sich die Parteien auf Nutzungsbedingungen, die in einer Nutzungsvereinbarung festgeschrieben werden. Antwortet kein Mitglied der Gruppe auf die Anfrage, so können spezielle Mitglieder, die Kommunikationsaufgaben abdecken, mit der Nachfrage bei anderen Gruppen beauftragt werden.

4.1 Module

Die Kernelemente der oben beschriebenen Zwischenschicht, die Teilsysteme, sollen Module genannt werden. Module sind Softwaresysteme, die eine eigene Systemidentität besitzen, und deren zentrales Ziel es ist, Dienste unter definierten Voraussetzungen auf Anfrage zu erbringen. Diese Voraussetzungen sind in sogenannten Nutzungsvereinbarungen, die auch Verträge genannt werden, festgelegt. Bei der Aushandlung dieser Nut-

zungsvereinbarungen verfolgen die Module eigene Strategien, die jedoch nicht zur Verletzung von Regeln ihrer Modulgemeinschaft führen dürfen. Die Erteilung der Systemidentität eines Moduls nach seiner Installierung in einer Modulgemeinschaft beinhaltet die Übergabe seiner Strategie. Strategien sind Leitlinien und/oder Handlungsvorgaben für Module. Die Strategien definieren eine Sicherheitspolitik und behandeln den Umgang mit anderen Modulen; sie geben Bewertungsmaßstäbe und Optimierungsziele der Arbeitsorganisation und Einheiten des Moduls vor und beschreiben nicht zuletzt Bedingungen und Methoden zur Änderung der Strategie selbst.

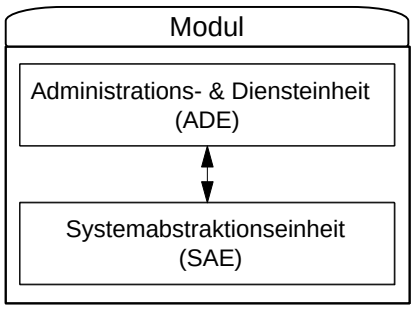
Dienste sind Funktionen, die von Modulen bereitgestellt und erbracht werden; sie werden von ihnen selbst oder von anderen Modulen genutzt. Die Komplexität dieser Dienste kann von einfachen Berechnungen bis hin zu komplizierten und vielschichtigen Anwendungen wie komplexen Regelungsaufgaben, Simulationen, Krisenmanagementsystemen usw. reichen. Die Module erbringen Dienste, indem sie Programmcodes unter ihrer Kontrolle auf ihnen zugeteilten Verarbeitungseinheiten ausführen lassen und/oder Dienste anderer Module nutzen.

Module können über mehrere Rechnersysteme verteilt sein und diese Systeme gemeinsam mit anderen Modulen nutzen. Je nach Komplexität und Entwicklungsgrad ihrer Strategien sind sie in der Lage, sich dynamisch auf Hardwareressourcen der Modulgemeinschaft zu verteilen oder sich wieder zurückzuziehen.

Alle Ereignisse und Fortschritte, die mit Diensten zu tun haben, alle Vorgänge im Modul sowie die Kommunikation mit anderen Modulen werden vom Modul protokolliert und nach definierten Kriterien in der Modulstrategie weiterverarbeitet oder vernichtet. Die gesammelten Daten können je nach Auslegung der Strategie zur Umkonfiguration der Dienste, der Moduleinheiten oder der Akquirierung bzw. Freigabe von Prozessorressourcen führen. Sie sind Grundlage zur Abrechnung erbrachter Dienste mit den dienstnehmenden Modulen.

4.1.1 Aufbau eines Moduls

Die Bandbreite des Aufgabenbereichs eines Moduls ist recht vielschichtig und reicht von administrativen, kontrollierenden, organisierenden bis hin zu systemplattformnahen Tätigkeiten. Damit die Module diese Aufgaben bewältigen können, besitzen sie zwei Basiseinheiten, die Systemabstraktionseinheit sowie die Administrations- und Diensteinheit. Abbildung 4.1 zeigt die Einheiten des Moduls.



Abbildung˜4.1: Einheiten eines Moduls

Systemabstraktionseinheit (SAE)

Die SAE kann als Vollstreckungsorgan der ADE (siehe unten) betrachtet werden. Sie organisiert, kontrolliert und verwaltet alle Programmcodes und deren Ausführung. Außerdem ist die SAE für die Bereitstellung der Kommunikation innerhalb des Moduls und mit anderen Modulen verantwortlich. Auf Anweisung der ADE führt die SAE die Verteilung eines Moduls auf weitere Verarbeitungseinheiten durch und synchronisiert die Programmabarbeitungen auf diesen Systemkomponenten. Sie stellt Verwaltungs- und Archivierungsfunktionen bereit für die Handhabung von Verträgen, Dienstskeletten, Programmcodes, Logdaten und weiteren Daten, die die ADE benötigt. Die Protokollierung aller Vorgänge im Modul und in den Schedulingfunktionen werden ebenfalls von der SAE durchgeführt.

Der Aufbau einer Systemabstraktionseinheit ist in Schichten organisiert. Die unterste Schicht wird durch einen Mikrokern gebildet. Dieser Mikrokern besitzt folgende Basisfunktionalität:

- Aufbau und Unterhaltung elementarer Organisationsstrukturen, die zum Betrieb der SAE auf einem Rechnersystem benötigt werden
- Starten, Ausführungskontrolle und Steuerung von Programmcodes
- Bereitstellung einer einfachen Kommunikation mit Filtern und Synchronisation mit anderen SAE-Teilen

Wichtige Merkmale des Mikrokerns sind:

1. Er besitzt eine Struktur, die leicht auf unterschiedliche Rechnersysteme portiert werden kann.
2. Er darf für seinen eigenen Betrieb möglichst wenig Ressourcen verbrauchen.
3. Er muß auch auf "kleinsten" Mikrorechnersystemen effizient arbeiten können.

Mehrere Codekopien des Mikrokerns eines Moduls dürfen nicht gleichzeitig auf einer Verarbeitungseinheit ausgeführt werden. Der ausgeführte Code repräsentiert die Präsenz des Moduls auf dem jeweiligen Rechner und besitzt neben der Systemkennung des Moduls eine modulinterne Kennung und Sicherheitseinstufung.

Auf dem Mikrokern setzt eine Programmcodeausführungskontrolle[1] und eine Vermittlungseinheit[2] auf. Die Programmcodeausführungskontrolle koordiniert und kontrolliert gemeinsam mit den anderen Ausführungskontrollen des Moduls die Ausführung von Programmcodes. Durch die Mikrokerne auf den Computersystemen erhält die Programmcodeausführungskontrolle Informationen über Prozessorauslastung, Systemtyp usw. Sie kann dadurch gezielt die verfügbaren Ressourcen nutzen und bei Über- oder Unterkapazitäten die ADE benachrichtigen. Die Vermittlungseinheit erhält Nachrichtenpakete von der Kommunikationseinheit oder von lokal ausgeführten Programmcodes. Sie filtert diese Pakete und leitet sie an diejenigen laufenden Programme weiter, an die die Pakete gerichtet sind. Zur Adressierung werden sogenannte

[1] Im weiteren Text wird PAK abkürzend für Programmcodeausführungskontrolle verwendet

[2] Im weiteren Text wird VE abkürzend für Vermittlungseinheit verwendet

Ports benutzt, die durch Portnummern identifiziert werden. Jede dieser Portnummern ist im Modul eindeutig. Ein Port besteht aus Puffern, in die Daten geschrieben oder aus denen Daten gelesen werden können. Jede Art des Zugriffs auf einen Port kann ganz nach Bedarf mit einem Programmcode assoziiert werden, so daß dieser Code vor und/oder nach dem Zugriff ausgeführt wird. Damit diese Ports von Plattformkomponenten beschrieben oder gelesen werden können, besitzt der Mikrokern Filter, die die jeweils benötigten Umsetzungen beschreiben und/oder durchführen.

Die dritte Schicht der SAE besteht aus modulinternen Funktionen wie Protokollierung aller Vorgänge, Fixierung und Aufbewahrung von Programmcodes, Verwahrung von Verträgen, Dienstskeletten, der Strategie, usw.

Abbildung 4.2 zeigt den Aufbau der SAE mit ihren drei Schichten.

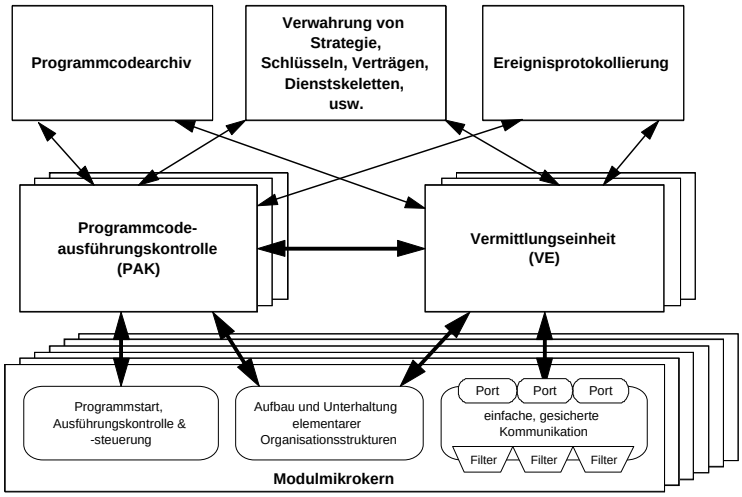


Abbildung 4.2: Aufbau der Systemabstraktionseinheit eines Moduls

Administrations- und Diensteinheit (ADE)

Der "Kopf" eines Moduls ist die ADE. Sie organisiert das Modul und gestaltet dessen Verhalten gegenüber den anderen Modulen in der Modulgemeinde. Die Hauptaufgaben der ADE sind:

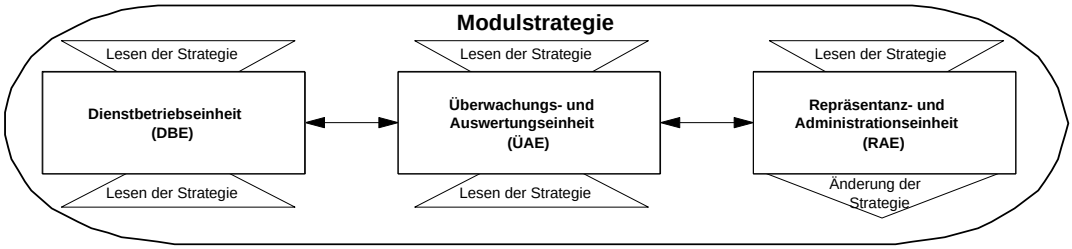
- Durchsetzung der Ziele, die in der Modulstrategie festgelegt sind, unter Beachtung der Regeln der Modulgemeinde (Modulgemeinderegeln)
- Optimierung der Modulorganisation und -arbeitsweise mit Hilfe der Ereignis- bzw. Zustandsmeldungen sowie den Log-Daten der SAE
- Einrichtung, Vermarktung und Erbringung von Diensten für andere Module

Die Verwirklichung ihrer Aufgaben bewältigt sie durch drei Funktionseinheiten:

1. Dienstbetriebseinheit (DBE)
2. Repräsentanz- und Administrationseinheit (RAE)

3. Überwachungs- und Auswertungseinheit (ÜAE)

Abbildung 4.3 zeigt die Einheiten der ADE und die Modulstrategie.



Abbildung~4.3: Modulstrategie und Einheiten der Administrations - und Diensteinheit

Dienstbetriebseinheit (DBE): Installation und Durchführung der Dienste eines Moduls werden von der DBE durchgeführt. Bei der Installation eines Dienstes wird ein sogenanntes Dienstskelett angelegt. Ein Dienstskelett beschreibt den Dienst eines Moduls vollständig. Wichtige Datenkategorien des Dienstskeletts sind:

- Identifikation und Sicherheitseinstufung des Dienstes
- Modulinterne Typ- und Sicherheitsbeschreibung des Dienstes
- Daten, die den Leistungsumfang und die Art des Dienstes beschreiben. Sie werden bei der Nachfrageauswertung und Angebotserstellung verwendet.
- Daten, die die Nutzungsmöglichkeiten, Kosten sowie Abrechnungs- und Zahlungsbedingungen für den Dienst beschreiben. Sie werden für die Verhandlungen und den Vertragsabschluß benötigt.
- Umgebungsbeschreibung: Die Voraussetzungen und benötigten Systemressourcen werden durch die Daten der Umgebungsbeschreibung festgelegt.
- Durchführungsbeschreibung: Die Daten dieser Kategorie bilden ein Durchführungsskript, in dem die Ausführungsfäden und einzelnen Schritte der Dienstbearbeitung festgelegt sind.

Alle notwendigen Daten werden in das Dienstskelett eingetragen. Zuvor müssen jedoch alle benötigten Programmcodes archiviert sein und Dienste durch entsprechende Nutzungsabkommen zur Verfügung stehen. Der Dienst wird durch die ÜAE auf seine Korrektheit überprüft und erhält dann von der RAE eine Sicherheitseinstufung. Die Installation wird mit dem Eintrag der Skelettreferenz in das Dienstverzeichnis der RAE abgeschlossen.

Fordert ein Vertragspartner bei einem Modul einen Dienst an, so bestimmt die DBE anhand der Vertrags- und Abonnentennummer die Nutzungsbedingungen und prüft deren Übereinstimmung mit den Momentanbedingungen. Erbringt die Prüfung

ein positives Resultat, wird die Verfügbarkeit der benötigten Ressourcen und Korrektheit der vom Dienstnehmer übergebenen Daten sichergestellt und mit der Bearbeitung des Dienstes begonnen. Nachdem die notwendigen Bearbeitungsschritte erfolgreich durchgeführt sind, wird die Dienstleistung entsprechend den Bestimmungen im Nutzungsvertrag abgerechnet. Alle Vorgänge der Dienstbearbeitung — beginnend bei der Dienstanforderung über die Zwischenergebnisse der einzelnen Bearbeitungsschritte bis hin zur Abrechnung — werden von der SAE protokolliert.

Treten während der Durchführung des Dienstes Zustände ein, die im Skript nicht behandelt werden, so wird die ÜAE über den Ausnahmezustand informiert. Die ÜAE berechnet dann mit Hilfe der Modulstrategie und weiteren Zustandsdaten von RAE und SAE die notwendigen Maßnahmen zur Behandlung der Situation und setzt diese durch DBE und SAE um.

Repräsentanz- und Administrationseinheit (RAE): Die RAE bildet gewissermaßen das "Wesen" des Moduls. Ihre Hauptaufgabe ist es, das Modul entsprechend der Modulstrategie zu organisieren und optimieren, das Modul gegenüber den anderen Modulen zu vertreten sowie Einstiegspunkte in das Modul für die Systemadministration bereitzustellen. Diese Aufgabe nimmt sie wahr durch:

- Auswertung von Dienstnachfragen sowie anschließende Erstellung und Abgabe von Dienstnutzungsangeboten
- Ermittlung von benötigten Diensten, Erstellung und Versendung entsprechender Dienstnachfragen bei anderen Modulen
- Verhandlungen über Nutzungsbedingungen und Abschluß von Nutzungsübereinkünften (Verträge)
- Vertragsverwaltung
- Dienstinstallation und -konfiguration durch die Funktionen der DBE
- Codearchivierung mit Hilfe der ÜAE
- Dienstbewertung
- Optimierung und Konfiguration der Einheiten des Moduls
- Funktionen zur Kommunikation mit der Systemadministration

Die RAE zieht zur Dienstbewertung sowie Optimierung und Konfiguration der Moduleinheiten — wozu sie selbst auch zählt — die Protokolldaten der SAE heran, die mit den Auswertungsfunktionen der ÜAE aufbereitet werden. Ihr Handeln wird dabei immer von der ÜAE überwacht, die kritische bzw. weitreichende Änderungsversuche gar nicht oder erst nach Zustimmung von Mitarbeitern des Systembetriebs zuläßt. Die Änderung der Modulstrategie kann prinzipiell nicht vom Modul selbst, sondern nur vom Systembetrieb bzw. dem Systemhersteller vorgenommen werden. Die Bedingungen, Methodik und Personen, die die Modifikationen der Strategie durch die Funktionen der RAE zulassen, sind in der Strategie festgelegt.

Je nach Entwicklungsgrad der Strategie und der RAE wird die Dienstinstallation und -konfiguration sowie die Bewertung durch das Modul selbst oder durch Systemadministratoren über die RAE vorgenommen. Sowohl die Mitarbeiter als auch die RAE müssen die SBE mit den entsprechenden Daten, Programmcodes und Dienstvertragsreferenzen versorgen. Programmcodes werden mit der ÜAE überprüft und durch eine elektronische Unterschrift der ÜAE fixiert, bevor sie ins Codearchiv der SAE aufgenommen werden und so dem Modul zur Ausführung zur Verfügung stehen.

Die Auswertung von Dienstnachfragen und die Erstellung von Dienstnutzungsangeboten erfolgt nach Signaturen und Interpretationen, die durch die Modulgemeinde festgelegt werden. Zwar kann jedes Modul die Bewertung und Charakterisierung seiner Dienste in den Skeletten nach eigenen Nomenklaturen vornehmen, es muß sich jedoch bei Dienstnachfragen und Dienstangeboten an die gemeindeweit geltenden Regeln halten.

Kann ein dienstnachfragendes Modul unter den Offerten der sich bewerbenden Module ein akzeptables Angebot ausmachen, so tritt es mit dem entsprechenden Dienstanbieter über die Nutzungsbedingungen des oder der angebotenen Dienste in Verhandlung. Zunächst einigen sich die Partner über Verhandlungsvorsitz und -modus. Die Verhandlung beginnt, und der Vorsitzende arbeitet die Liste seiner Verhandlungspunkte ab, indem er die Stichpunkte und möglichen Optionen übermittelt. Sein Verhandlungspartner wählt die von ihm benötigten Optionen aus und schickt diese Selektion zurück. Der Verhandlungsvorsitzende prüft die erhaltene Nutzungskonfiguration und bestätigt sie oder fordert eine Nachverhandlung an. Kann er die Nutzungskonfiguration bestätigen, bietet er seinem Partner den Vorsitz an, der dann über noch nicht behandelte Punkte und benötigte Optionen die Verhandlung weiterführt. Einigen sich die Partner, legen sie die vereinbarten Punkte in einem Nutzungsvertrag fest. Ein Vertrag besitzt und berücksichtigt in der Regel folgende Punkte:

- Vertragsidentität
  - Daten des Vertragsabschlusses (Ort, Zeit, Partner, Partnerrollen, usw.)
  - Vertragsnummer
- Vereinbarungen
  - Dauer des Vertrages und mögliche Auflösungsbedingungen
  - Dienstidentifizierungen und Nutzungsbedingungen (Zeit, Port, usw.)
  - Dienstdurchführungsanforderungen (Antwortzeiten, wie, wo, wann Ergebnisse abzuliefern sind, usw.)
  - Festlegung, wann Dienste als erbracht gelten
  - Regelungen bei Nichterfüllung von Diensten
  - Festlegung von Abonnentennummern
  - Preise und Abrechnungsbedingungen
  - Nachverhandlungsoptionen (Vertragsverlängerungen, Preisänderungen, neue Abonnenten usw.)

– sicherheitstechnische Regelungen

Der Vertrag wird von beiden Seiten durch eine elektronische Unterschrift unterzeichnet und an ein vertrautes Modul (vertraute Instanz, siehe unter Modulgemeinden) geschickt. Dieses prüft die Vertragsgültigkeit und übermittelt den Vertragspartnern eine Bestätigung über den gültigen Vertragsabschluß. Die vereinbarten Regelungen treten in Kraft.

Überwachungs- und Auswertungseinheit (ÜAE): Als das "Gewissen" eines Moduls könnte man die ÜAE bezeichnen. Ihre Aufgabe ist es, die Tätigkeit der anderen Moduleinheiten zu kontrollieren, in Ausnahmesituationen einzugreifen, die RAE durch ihre statistischen Auswertungsfunktionen zu unterstützen, durch Aufbewahrung, Weiterverarbeitung und Bereitstellung von Auswertungsergebnissen eine Wissensrepräsentanz des Moduls zu bilden sowie die Log-Dateien der SAE zu bereinigen.

Mit Hilfe der Modulstrategie, den Modulgemeinderegeln und dem aus den statistischen Auswertungen der Daten der SAE gewonnenen Erfahrungen bewertet die ÜAE Ausnahmesituationen und versucht, eine angemessene Behandlung zu berechnen. Entsprechend der Schwere und Komplexität der Ausnahmesituation und des Entwicklungsgrades der ÜAE wird die Situation bewältigt, oder es wird die Unterstützung der Systemadministration angefordert.

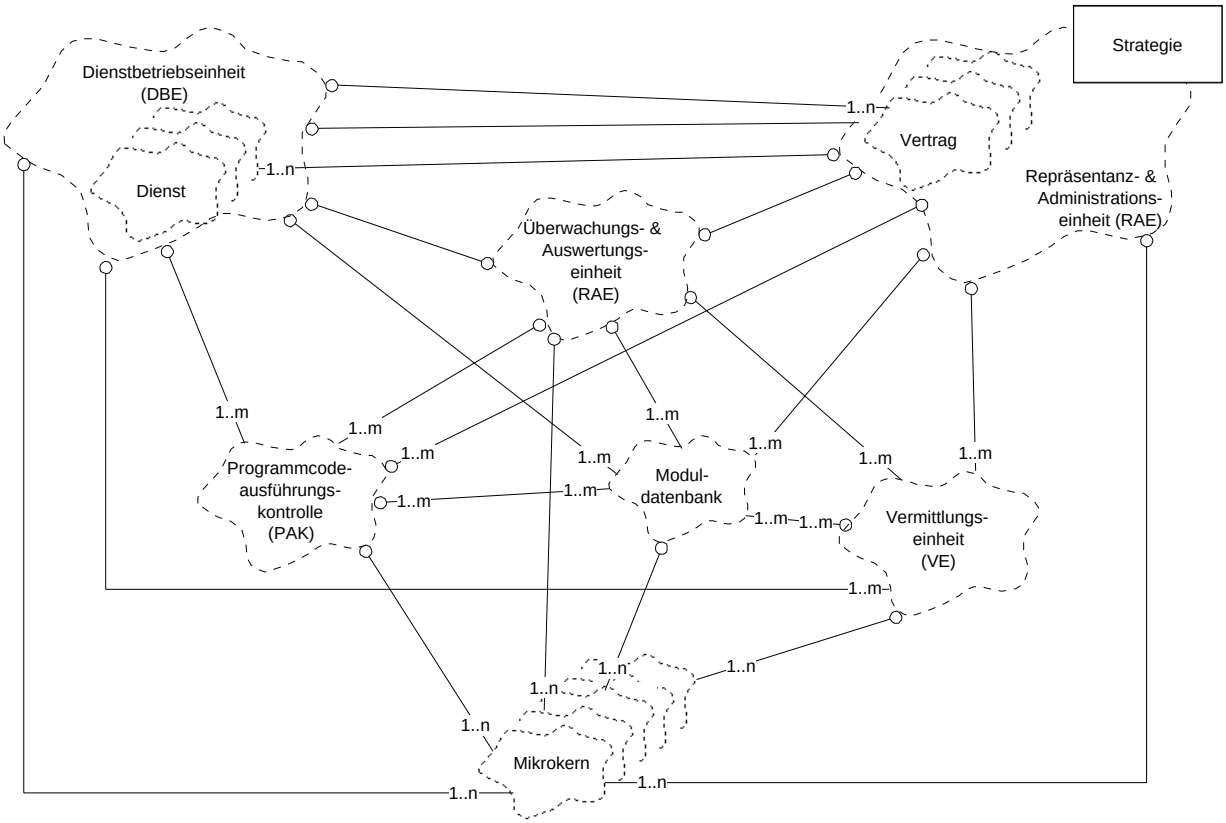
Neben den Aufgaben des "Modulkrisenmanagements" muß die ÜAE die Sicherheitspolitik des Moduls verwirklichen. Sie nimmt dazu folgende Aufgaben wahr:

- Erstellung und Durchsetzung verbindlicher Mindestvorgaben :
  - zur Sicherheitseinstufungen von Diensten
  - zum Einsatz sicherheitstechnischer Methoden bei der Diensterbringung
- Verwaltung, Berechnung und Bereitstellung kryptographischer Schlüssel
- Generierung eindeutiger Kennungen für Mikrokernkopien
- Prüfung und Fixierung von Programmcodes vor deren Archivierung oder Ausführung auf Verarbeitungseinheiten
- Erzwingung der einzuhaltenden Vorgaben bei Strategieänderung durch Mitarbeiter

Alle Meldungen der SAE an die Einheiten der ADE und umgekehrt laufen über die ÜAE. Die ÜAE filtert diese Meldungen und prüft dabei, ob sie reagieren und/oder die Nachricht an die anderen Einheiten der ADE weiterleiten muß. Ziel dieser Verfahrensweise ist die Möglichkeit für die ÜAE, jede Aktivität zu beobachten und — sofern nötig — Einfluß zu nehmen. Dabei nimmt sie nicht nur überwachende, sondern auch unterstützende Tätigkeiten wahr. Sie informiert zum Beispiel die RAE, wenn Vertragsbestätigungen eintreffen, und schaltet die entsprechenden Dienste des Vertrages zur Nutzung frei. Verträge, die nicht innerhalb einer im Vertrag definierten Zeit bestätigt werden oder bei deren Nutzung sich wiederholende und/oder schwerwiegende Vertragsverletzungen ereignen, werden von der ÜAE gesperrt; außerdem werden

entsprechende Meldungen an die RAE und DBE abgesetzt. RAE und DBE können dann entsprechend reagieren. So kann die RAE beispielsweise dem Vertragspartner eine Vertragsaufkündigung mitteilen. Wann, wie und wo reagiert wird, beschreibt die Modulstrategie.

Eine weitere wesentliche Aufgabe ist der Aufbau und die Pflege einer Wissensbasis des Moduls. Module sollen lernfähig sein. Dazu muß die ÜAE aus den Daten der SAE eine Datenbank aufbauen, in der Prämissen und entsprechende Folgerungen gespeichert werden. Neben dem Aufbau und der Pflege der Datenbank muß sie Funktionen zur Verfügung stellen, mit der die RAE dieses "Wissen" in Verbindung mit den Leitlinien der Strategie für ihre Aufgaben nutzen kann.
Abbildung 4.4 zeigt die Modellierung eines Moduls.



Abbildung˜4.4: Objektmodellierung eines Moduls, wobei gilt: $m \leq n$

4.1.2 Weitere Eigenschaften und Funktionsmechanismen von Modulen

Die Beschreibung des Aufbaus von Modulen hat bereits wichtige Strukturen und Vorgänge in Modulen behandelt. In diesem Abschnitt werden weitere wesentliche Eigenschaften und Funktionsmechanismen von Modulen charakterisiert, die bisher noch unerwähnt blieben oder aus Gründen übersichtlicher Darstellung nicht entsprechend ihrer Bedeutung vertieft wurden.

Abgeschlossenheit eines Moduls: Eine wichtige, wenn nicht die zentrale Eigenschaft eines Moduls ist dessen Abgeschlossenheit gegenüber anderen Programmen und Modulen, die auf den Rechnersystemen und Rechnernetzen arbeiten. Mit der Abgeschlossenheit soll sichergestellt werden, daß modulfremde Einrichtungen nur mit Erlaubnis auf Programme und Daten des Moduls zugreifen, direkt auf Vorgänge im Modul Einfluß nehmen oder über verdeckte Kanäle Informationen gewinnen können. Das hat konkrete Konsequenzen sowohl auf die Implementierung der Module als auch auf die Anforderungen in Bezug auf die Eigenschaften der eingesetzten Systemplattformen:

- Daten des Moduls, die sich auf Massenspeichern befinden, dürfen nur vom Modul gelesen, verändert oder gelöscht werden. Bei absichtlicher oder unabsichtlicher Beeinflussung der Datenbestände des Moduls muß zumindest deren Persistenz sichergestellt sein. Wünschenswert ist allerdings deren Integrität. Die Zugriffe des Moduls auf diese Medien dürfen von dritter Seite nicht ohne Erlaubnis eineindeutig dem Modul zugeordnet werden können.

- Daten und Programme, die sich im Systemspeicher des Rechnersystems befinden, dürfen nur vom Modul oder mit dessen Einverständnis gelesen oder verändert werden. Notwendige Steuerungsmaßnahmen von dritter Seite, die die Verarbeitung von Programmcodes des Moduls außerhalb seiner Kontrolle beeinflussen, müssen dem Modul angekündigt sein.

- Daten bzw. Nachrichten, die bei der Kommunikation zwischen den

  - Einheiten eines Moduls,
  - unterschiedlichen Modulen derselben Gemeinde,
  - Modulen unterschiedlicher Gemeinden

  auf denselben Rechnern oder auf unterschiedlichen Rechnersystemen ausgetauscht werden, stellen einen verallgemeinerten Fall von Anforderungen an den Umgang mit den Daten auf den Massenspeichern dar. Die Daten werden von einer Einheit bzw. einem Modul geschrieben und von einer definierten anderen Einheit bzw. anderem Modul gelesen. Neben den bereits beschriebenen Anforderungen zum Umgang mit diesen Daten muß zusätzlich sichergestellt werden, daß die Daten in einem definierten Zeitintervall für die Nachrichtensenke verfügbar sind. Eine Besonderheit gibt es bei der Intermodulkommunikation. Die Nachrichten müssen hier von einer vertrauten Modulinstanz innerhalb der Modulgemeinde der Form nach überprüfbar sein — allerdings nur von dieser vertrauten Instanz.

Für den Betrieb der Module bedeutet dies, daß

- auf einem Rechnersystem, das eine parallele Prozeßverarbeitung zur Verfügung stellt, die Forderungen bei der Interprozeßkommunikation und bei der Ablage von Daten auf Massenspeichern durch entsprechende Mechanismen des Betriebssystems abgedeckt werden müssen.

- auf einem Rechnersystem mit einer sehr elementaren Prozeßverwaltung ausschließlich die Programmcodes von maximal zwei Modulen derselben Gemeinde zur Ausführung kommen. Dabei muß das eine Modul ein Vertrauensmodul der Gemeinde sein. Zusätzlich sind die Daten, die auf Massenspeichern abgelegt werden, durch kryptographische Mechanismen zu schützen.
- zum Transport über Computernetzwerke die Daten prinzipiell durch kryptographische Verfahren geschützt werden müssen. Diese stellen sicher, daß
  - die Verfälschung der Daten erkennbar ist,
  - die Informationen der transportierten Daten nur durch die Nachrichtensenke zugänglich sind.

Kommunikation: Zur Kommunikation der Module untereinander soll eine Technik zum Einsatz kommen, wie sie im Netzwerkmanagement bei Agentensystemen verwendet wird. Wünscht ein Modul einen Dienst, so setzt es ein entsprechendes Nachrichtenpaket ins Netzwerk ab. Die anderen Module lauschen und nehmen die Nachricht, sofern diese für sie bestimmt ist, vom Netz und quittieren deren Erhalt. Aus den von ihnen geschlossenen Verträgen wissen die anfordernden Module, daß es im Netz irgendwo einen Vertragspartner gibt, der ihre Anforderung bearbeitet. Bei Angebotsnachfragen sind dementsprechend alle Gemeindemitglieder die "Vertragspartner". Bei zeitkritischen Diensten können sich die Vertragspartner in Ausnahmefällen auf eine Punkt-zu-Punkt-Kommunikation einigen.

Was bei der Intermodulkommunikation eher eine Ausnahme ist, die Punkt-zu-Punkt-Kommunikation, ist bei der Kommunikation zwischen den Einheiten eines Moduls die Regel. Ein Modul kennt sich selbst, und die Mehrzahl der Nachrichten sind zeitkritisch (z.B. laufende Synchronisationen der Moduleinheiten auf unterschiedlichen Rechnersystemen). Außerdem muß die Kommunikation zwischen den Einheiten — im Gegensatz zu derjenigen zwischen den Modulen — der Form nach nicht von einer dritten Modulinstanz der Modulgemeinde überprüfbar sein.

Abläufe bei der Kommunikation: Dreh- und Angelpunkt bei der Kommunikation zwischen Modulen und/oder den Einheiten eines Moduls ist die Vermittlungseinheit. Sie stellt sicher, daß die Nachrichtenpakete in die entsprechenden Nachrichtenkanäle des Mikrokerns gelangen. Bei Anforderungen von Diensten erledigt die Vermittlungseinheit die entsprechenden Umsetzungen der Daten- und Parameterformate, wie sie in den Verträgen festgeschrieben sind. So ist es den unterschiedlichen Modulen und den Einheiten eines Moduls möglich, die für sie sinnvollen und passenden Formate zu benutzen. Die Vermittlungseinheit bewältigt diese Aufgabe durch den Einsatz von Ports, die sie konfiguriert und verwaltet. Physikalisch sitzen diese Ports in den Mikrokernen. Erhält die Vermittlungseinheit eine Dienst- oder Funktionsanforderung, prüft sie zunächst, ob dieser Dienst ein moduleigener ist (Funktionen sind immer moduleigen). Stellt sie fest, daß es sich um den Dienst eines anderen Moduls handelt, sucht sie den entsprechenden Vertrag heraus und erstellt ein Nachrichtenpaket. Darin sind die entsprechenden Anfrage- und Dienstparameter in der vom Vertrag und den Gemeinderegeln vorgeschriebenen Darstellung aufbereitet. Daraufhin wird das Paket

zur Kommunikationseinheit des Mikrokerns geschickt. Dieser weiß durch Zusatzinformationen zum Paket, wie er es zu verschlüsseln hat und durch welches Medium es verschickt werden soll.

Bei moduleigenen Diensten, Funktionen oder Programmcodes wird zunächst mit Hilfe der Programmcodeausführungskontrolle ermittelt, auf welchem Rechnersystem sich die jeweiligen Nachrichtensenken befinden. Entsprechend der eingerichteten Ports wird das Nachrichtenpaket aufbereitet und durch den Mikrokern verschickt.

Erhält ein Modul über einen entsprechenden Port eine Dienstanforderung eines anderen Moduls, so prüft die Vermittlungseinheit, wo der entsprechende Dienst im Modul zur Verfügung steht, bereitet das Datenpaket der Dienstanforderung für die entsprechende DBE vor und schickt die Anforderung über einen Port an die DBE.

Abläufe bei der Diensterbringung: Erhält die DBE über einen Port eine Dienstanforderung, so prüft sie mit Hilfe der Vertrags-, Abonnenten- und Dienstidentifikationsnummer, ob die Anforderung eine Erbringungsgrundlage besitzt. Ist dies der Fall, eröffnet die DBE ein Diensterbringungsdokument, das durch eine modulweit eindeutige Dienstbearbeitungsnummer identifizierbar ist. In diesem Dokument werden der aktuelle Bearbeitungszustand sowie alle Vorgänge und Zwischenergebnisse bis zum Abschluß der Diensterbringung beschrieben. Den ersten Eintrag in das Diensterbringungsdokument[3] bilden die Referenzen auf das Nachfrageereignis der SAE-Log Daten, die Vertrags-, Abonnenten- und Dienstidentifikationsnummer sowie die erhaltenen Steuerungs- und Bearbeitungsparameter. Nach dieser Dokumenteneröffnung fordert die DBE eine Buchung der notwendigen Ressourcen bei der Programmcodeausführungskontrolle mit den gebotenen Prioritäten an. Die PAK prüft die Verfügbarkeit. Dazu verwendet sie den aktuellen Ressourceneinsatzplan, der bei Bedarf entsprechend modifiziert wird. Können die angeforderten Mittel mit Sicherheit oder hoher Wahrscheinlichkeit zu den gewünschten Bedingungen der Reservierung bereit gestellt werden, so wird die Buchung bestätigt. Ist die Reservierung nicht mit den zur Verfügung stehenden Ressourcen möglich, und erzwingt die Anforderungspriorität der DBE eine unbedingte Bereitstellung, so meldet die PAK diesen Mangel an die ADE, die daraufhin weitere Maßnahmen entsprechend der Modulstrategie ergreifen muß. Sind die Ressourcen gebucht und bestätigt, wird der erste Bearbeitungsschritt des Diensterbringungsskripts begonnen. Dabei werden die für den ersten Schritt benötigten Ressourcen abgerufen, der Programmcode gestartet bzw. der Dienst angefordert und eine entsprechende Referenz auf die Log-Daten der SAE ins DED eingetragen, die diesen Vorgang dokumentieren. Nachdem der Programmcode abgearbeitet ist bzw. der angeforderte Dienst erbracht wurde, werden die Zwischenergebnisse und der Ergebnisstatus im DED festgehalten und bewertet. Der erste Bearbeitungsschritt ist nun abgeschlossen. Entsprechend der Bewertung wird der nächste Bearbeitungsschritt aus dem Skript bestimmt und mit dessen Bearbeitung begonnen. Aus dem Zwischenergebnis des vorhergehenden Bearbeitungsschritts werden Parameter generiert und der entsprechende Programmcode gestartet bzw. Dienst angefordert. Genau wie beim ersten Schritt wird die entsprechende Ereignisreferenz auf die SAE Log-Daten ins DED eingetragen. Dieses Vorgehen der Abarbeitung des Skriptes wiederholt sich so lange, bis der Dienst erbracht ist. Bei einem Bearbeitungsschritt können mehrere Programmcodes gestartet

[3] Im weiteren Text wird DED abkürzend für Diensterbringungsdokument verwendet

und/oder Dienstanforderungen abgesetzt werden, oder auch eine Kombinationen aus beiden. Das Ergebnis und/oder der Ergebnisstatus wird an den Dienstnehmer, wie im Vertrag festgelegt, übergeben und die erbrachte Dienstleistung abgerechnet.

Treten Ausnahmesituationen bei der Skriptbearbeitung auf — das bedeutet Ergebnisstatus oder Zwischenergebnisse, die nicht durch das Skript beschrieben sind —, so wird die Bearbeitung ausgesetzt und das DED der ÜAE übergeben. Entsprechend den Gemeinderegeln und der Modulstrategie wird eine Ausnahmebehandlung berechnet und in Zusammenarbeit mit der DBE durchgeführt. Je nach Art und Komplexität dieser Ausnahmesituation und dem Verlauf der Ausnahmebehandlung kann die Bearbeitung des Dienstes fortgesetzt oder als gescheitert eingestuft werden.

Entsprechend den Festlegungen im Vertrag werden Ergebnisstatus und gegebenfalls Ergebnisse an den Dienstnehmer übermittelt und die erbrachte Leistung in Rechnung gestellt. Die Diensterbringung ist damit abgeschlossen. Das DED wird mit der Bezahlung des erbrachten Dienstes geschlossen und archiviert.

Abläufe beim Start eines Moduls: Nachdem durch ein spezielles Modul (Gemeindeverwaltungsmodul) ein Mikrokern mit einer vorläufigen Modulkennung des neuen Moduls auf einem Rechnersystem gestartet wurde, werden zunächst elementare Organisationsstrukturen aufgebaut und eine PAK gestartet. Die PAK baut die von ihr benötigten Datenstrukturen auf und initialisiert diese. Anschließend wird der Start einer VE eingeleitet. Ist die VE einsatzbereit, beginnt der eigentliche Aufbau des Moduls mit der Ausführung eines Modulstartskripts durch die PAK. In diesem Skript sind alle erforderlichen Programmcodes, Dienstskelette, Basisverträge und andere notwendige Daten enthalten, um ein funktionsfähiges Modul aufzubauen und in Betrieb zu setzen. Entsprechend dem Skript werden, sofern vorgesehen, auf weiteren Ressourcen Mikrokerne sowie PAK, VE und Datenbanksysteme gestartet, eingerichtet und synchronisiert. Ist die SAE des neuen Moduls voll in Funktion getreten, werden die Einheiten der ADE in Betrieb genommen. Als erste Einheit der ADE nimmt die RAE ihre Arbeit auf, gefolgt von der ÜAE und DBE. Haben sich die Einheiten der ADE eingerichtet, synchronisiert und sind abschließende Validierungen und Funktionstests erfolgreich verlaufen, meldet die RAE die Einsatzbereitschaft bei dem Gemeindeverwaltungsmodul durch Übergabe der Ergebnisse der Funktionstests und Validierungsdaten. Das Gemeindeverwaltungsmodul überprüft diese Daten und übergibt der RAE die Modulstrategie, Sicherheitseinstufung und endgültige Modulidentität. Das Modul kann nun seine Arbeit aufnehmen.

4.2 Modulgemeinde

Die Sicherstellung der Abgeschlossenheit eines Moduls benötigt eine erhebliche Zahl an Diensten und Funktionen, soll jegliche Art von Angriffen abgewehrt werden können. Je höher die Sicherheitsrelevanz eines Moduls ist, desto aufwendigere und ausgeklügeltere Mechanismen werden notwendig, um diese Eigenschaft sicherzustellen. Das kann dazu führen, daß das Modul für sich und seine Schutzmechanismen erheblich mehr Ressourcen benötigt als für seine eigentlichen Aufgaben, die darin bestehen, Dienste für andere Module zu erbringen. Entschließt man sich, unterschiedliche Funktionsgruppen eines Zugangskontrollsystems auf verschiedene Module zu verteilen, müßte jedes dieser Mo-

dule einen aufwendigen Eigenschutz aufbauen und unterhalten. Mit steigender Zahl von Modulen in einem System würde der Ressourcenverbrauch erheblich ansteigen. Aufgrund der individuellen "Lernfähigkeit" wäre außerdem nicht unbedingt sichergestellt, daß Module derselben Sicherheitsklasse ein homogenes Niveau an Selbstschutz besitzen. Es könnte lediglich ein Mindestniveau sichergestellt werden.

Anstatt jedes Modul für sich "kämpfen" zu lassen, erscheint es sinnvoller, eine Gemeinschaft von Modulen aufzubauen, die durch spezielle Mechanismen und Modultypen den Mitgliedern der Gemeinschaft eine wohldefinierte und integre Arbeitsumgebung bereitstellt und gewährleistet. Dabei verwenden die Module weiterhin elementare Sicherheitsmechanismen, die ihre Abgeschlossenheit in der Gemeinschaft sicherstellt (z.B. Einsatz von Verschlüsselungs- und Authentifikationsalgorithmen zur Innermodulkommunikation, Schlüsselverwaltung und Schlüsselerzeugung, Verwaltung und Erstellung von Prüfsummen, usw.).

Eine Gemeinschaft von mindestens zwei Modulen, die durch spezielle Mechanismen und Regeln ihre Mitglieder kapselt und ihnen eine wohldefinierte und integre Arbeitsumgebung bereitstellt, heißt Modulgemeinde. Ein Modul gehört immer genau einer Modulgemeinde an. Module, die einer Modulgemeinde angehören, heißen Modulgemeindemitglieder oder Gemeindemitglieder. Abbildung 4.5 zeigt eine Modulgemeinde mit Modulgemeindemitgliedern, die sich aus typischen sowie anwendungsspezifischen Gemeidemitgliedern zusammensetzt. Dabei erfüllen die sog. typischen Gemeidemitglieder üblicherweise die für die Infrastruktur einer Gemeinde benötigten Funktionen, während die anwendungsspezifischen Gemeidemitglieder die vorhandenen Strukturen lediglich für ihre eigenen, anwendungsorientierten Zwecke nutzen. Die Modulgemeinderessourcen (Rechnersysteme mit Kennung 1 bis 8) werden von den Modulgemeindemitgliedern teilweise gemeinsam verwendet.

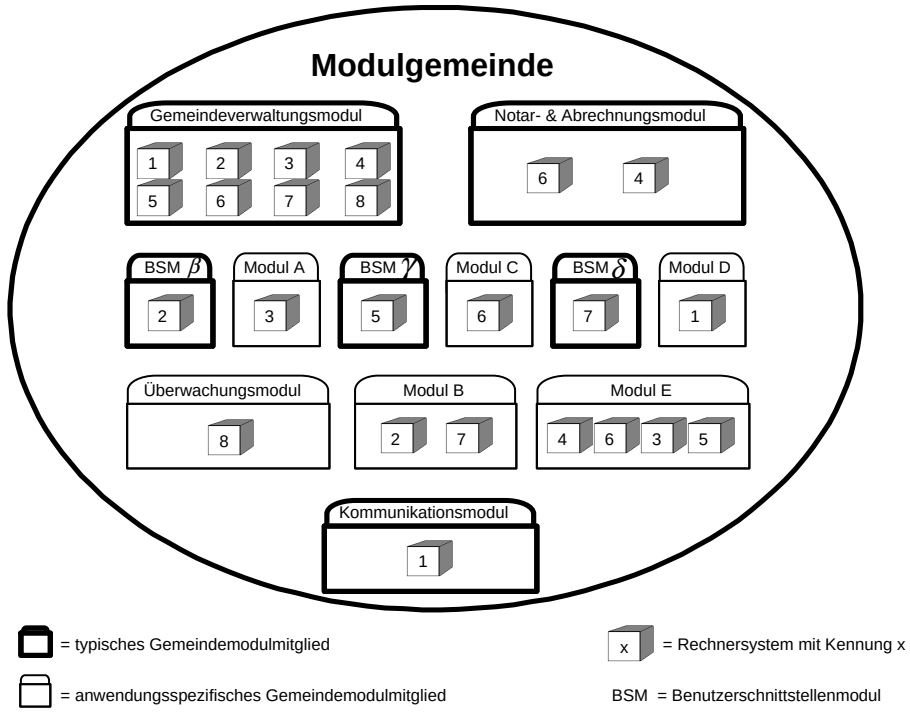
Die Strategie der Modulgemeinde ist es, durch

1. Modulauthentifikation,
2. laufende Überwachung des Betriebs der Gemeinde sowie Kontrollen der Ressourcen, Gemeindemitglieder und Personenbenutzer,
3. gezielte Gegenmaßnahmen spezialisierter Instanzen

eine für die Gemeindemitglieder sichere und effiziente Umgebung bereitzustellen und potentielle Angriffe von den Objekten der Gemeinde fernzuhalten. Zum Aufbau und zur Unterhaltung einer wohldefinierten und integren Arbeitsumgebung verwenden Modulgemeinden ein Regelwerk bestehend aus:

- Verhaltensvorschriften für Gemeindemitglieder
- Gemeindestandards
- einer Gemeindesicherheitspolitik

Weiterhin sind spezielle Module erforderlich, die eine entsprechende Funktionsinfrastruktur bereitstellen, mit der das Regelwerk abgebildet und durchgesetzt werden kann.



Abbildung~4.5: Modulgemeinde mit typischen und anwendungsspezifischen Gemeindemodulen, die die Gemeinderessourcen gemeinsam nutzen

Dieses Regelwerk ist gewissermaßen das "Gesetzbuch" der Modulgemeinde und wird als Modulgemeinderegeln bezeichnet. Modulgemeinderegeln behandeln mindestens folgende Punkte:

- Beschreibung einer Sicherheitspolitik für die Gemeinde:
  - Definition und Beschreibung von Sicherheitseinstufungen von Gemeindemitgliedern und Ressourcen:
    - Festlegung des prinzipiellen Aufbaus der Sicherheitseinstufungen (Sensitivity Labels)
    - Festlegung und Bedeutungsbeschreibung der zur Sicherheitseinstufungsnomenklatur gehörenden Strukturelemente und Attributmengen
  - Bewertungsregeln der Sicherheitseinstufungen
  - welche Sicherheitsmechanismen wann, wie und durch wen verwendet werden
  - wie und wann Schlüssel erzeugt, verteilt, verwahrt und eingesetzt werden
  - wie, auf was und wodurch gemeidefremde Module Zugriff in der Gemeinde erhalten
  - Festlegung von Modulklassen (z.B. welche Gemeindemitglieder auf welchen Gebieten vertraute Instanzen sind.)
  - Definitionen und Bewertungen von Ereignissen und Alarmen

  - Überwachungsstrategie der Vorgänge, Ressourcen und Mitglieder der Gemeinde
    * Algorithmen und Daten, die zur Überprüfung der Integrität dienen
    * Überwachungsmodi und -zeitintervalle
  - Definition von Ausnahmesituationen und entsprechenden Behandlungsmechanismen
  - Festlegung von Notstandsplänen
  - Festlegung der Registrierung, Überprüfung, Legitimierung von neuen oder veränderten Ressourcen
  - Festlegung der Registrierung und Legitimierung von Personen, die Dienste von Modulen der Gemeinden nutzen dürfen.
  - Festlegung, wie neue Module installiert und in die Gemeinde aufgenommen werden.
  - Sanktionsmaßnahmen gegen Mitglieder, die sich nicht an Gemeinderegeln oder geschlossene Verträge halten.

- Festlegung von Interpretationen und Signaturen für Dienstnachfragen und Dienstnutzungsangebote
- Festlegung des formalen Ablaufs von Vertragsverhandlungen und -abschlüssen
- Festlegung der Kommunikationsmodi zwischen den Modulgemeindemitgliedern
- Festlegung unverbindlicher Gemeindestandards (z.B. Abrechnungsintervalle für erbrachte Dienste, usw.)
- weitere Festlegungen

4.2.1 Gemeindeverwaltungsmodul (GVM)

Das Instrument zur Abbildung und Durchsetzung der Gemeinderegeln ist das Gemeindeverwaltungsmodul, kurz GVM. Es ist sozusagen die "Regierung" der Gemeinde und leitet den Aufbau und die Unterhaltung der wohldefinierten und integren Arbeitsumgebung. Dazu besitzt es folgende Funktionen und Dienste:

- Möglichkeit zur Erstellung, Wartung und Verwahrung von Gemeinderegeln
- Bereitstellung einer Nachrichtenübermittlung über Speichervermittlung für Personen und Modulgemeindemitglieder
- Bereitstellung von Diensten zum Einrichten und Verwalten von Interessengruppen, die aus Personen und/oder Modulen bestehen.
- Zustandsbeschreibung der Modulgemeinde und Zustandsübergangsdurchsetzung
- Unterstützung und Auswertung bei Situationssimulation in der Modulgemeinde

- Schaffung spezieller (event. temporärer) Installationen von speziellen Simulationsmodulen zur Datenerfassung und Situationsgenerierung
- Verwaltung von Ressourcen der Modulgemeinde durch :
  - ein Installations- und Wartungsmanagement, wie in der Funktionsanalyse beschrieben.
  - ein Sicherheitsmanagement, mit dem die Ressourcen entsprechend der Sicherheitspolitik legitimiert werden, und regelmäßig deren Integrität geprüft werden kann.
  - ein Ressourceneinsatzmanagement, das die Ressourcenauslastung überwacht und optimiert. Unter Berücksichtigung des Momentanzustandes der Gemeinde und der Ressourcen werden den Gemeindemitgliedern Gemeinderessourcen zur Verfügung gestellt oder entzogen.
- Gewährleistung der Sicherheit der Modulgemeinde durch:
  - ein Personenmanagement, das Personen registriert, legitimiert, deren Nutzungsrechteerteilung verwaltet und mit MAC Labels sowie SRL durchsetzt. Siehe auch Systemanalyse, 2.1.1.
  - ein Modulmanagement, das Module in der Gemeinde installiert, registriert, legitimiert, deren Nutzungsrechte verwaltet und mit MAC Labels sowie SRL durchsetzt. Siehe auch Systemanalyse, 2.1.1.
  - ein Ereignisüberwachungssystem, mit dem Ausnahmesituationen erkannt und entsprechend den Vorgaben der Gemeindesicherheitspolitik behandelt werden (in Zusammenarbeit mit dem Ressourceneinsatzmanagement).
  - ein Kryptographiesystem, das Kryptoengines und Schlüssel bereitstellt und wartet.
  - Deklaration von bestimmten Modulen zu vertrauten Instanzen sowie deren besondere Überwachung.

Damit das GVM in der Lage ist, die von der Gemeinde genutzten Rechnersysteme administrieren und überwachen zu können, jederzeit für die Gemeindemitglieder erreichbar zu sein und alle Vorgänge in der Gemeinde mitverfolgen zu können, befinden sich auf allen Computersystemen, auf denen Codes von Gemeindemitgliedern ablaufen, zumindest ein Mikrokern des GVM. Darüberhinaus können auch Teile oder ganze Einheiten dieses Moduls vorhanden sein. Wie sich leicht erkennen läßt, sind eine Vielzahl der benötigten Funktionen und Dienste bereits durch die Struktur eines Moduls manifestiert. Die Modulgemeinderegeln stellen die Strategie des GVM dar.

Ausfallerkennung und -behandlung von Gemeinderessourcen

Das GVM setzt auf zwei Methoden zur Erkennung von Beeinträchtigungen oder Ausfällen von Gemeinderessourcen. Die eine ist eine passive Methode. Kann ein Gemeindemitglied seine Einheit oder seinen Mikrokern auf einem Rechnersystem nicht mehr erreichen, so wird es beim GVM nachfragen, ob irgendwelche Störungen vorliegen.

Ist dem GVM kein Ereignis bekannt, so wird es mit Hilfe seines Mikrokerns auf dem betreffenden und den benachbarten Rechnern eine Situationsanalyse durchführen.

Die andere ist eine aktive Methode. Bei regelmäßigen Überprüfungen des GVM, deren Umfang und Art in den Gemeinderegeln festgelegt sind, werden Funktionstests durchgeführt und Auslastungsdaten der Ressourcen erfaßt. Je nach Komplexität dieser Tests werden die Überprüfungen selbständig vom Mikrokern des GVM auf den einzelnen Rechnern durchgeführt, oder sie werden durch eine PAK des GVM veranlaßt. Die Ergebnisse können jederzeit von einer PAK abgerufen oder bei kritischen Werten unaufgefordert von dem betreffenden Mikrokern an eine PAK übermittelt werden.

Konnten Auffälligkeiten oder Mängel im System festgestellt werden, versucht das GVM durch unterschiedliche Methoden die Ursachen und/oder das Ausmaß der Mängel festzustellen; dies kann etwa durch den Mikrokern auf der Ressource und/oder den Mikrokernen auf benachbarten Rechnersystemen sowie auch durch den Einsatz von möglicherweise vorhandenen Detektoren/Sensoren geschehen. Entsprechend dem Analyseergebnis ergreift das GVM Maßnahmen, die aus Benachrichtigungen an die betroffenen Module, Informierung der Mitarbeiter des Systembetriebs und/oder des Sicherheitsmanagements (z.B. bei Sabotage usw.) oder in der selbständigen Behebung des Mangels durch das GVM bestehen können.

Belegung von Hardwareressourcen und Optimierung der Ressourcennutzung

Neben der Bereitstellung einer sicheren Umgebung soll das GVM den Einsatz der Gemeinderessourcen effizient gestalten. Dazu besitzt es ein Ressourceneinsatzmanagement, welches das Leistungsverhalten der einzelnen Rechnersysteme, des Rechnernetzes und anderer Gemeinderessourcen laufend analysiert und durch entsprechende Kennwerte beschreibt. Stellt ein Modul fest, daß die ihm zur Verfügung stehenden Ressourcen nicht ausreichen oder nicht voll genutzt werden, so wird es weitere belegen oder sich von den nicht benötigten zurückziehen. Treten extreme Ausnahmesituationen (z.B. Ausfall von Ressourcen, Nutzungsaussetzung aufgrund sicherheitstechnischer Probleme, usw.) in der Gemeinde auf, müssen Ressourcen umverteilt werden. All diese Anforderungen sollen mit Hilfe eines zentralen Ressourceneinsatzmanagements bewältigt werden, das eine optimale Auslastung der unterschiedlichen Gemeindebetriebsmittel gewährleistet. Deshalb können die Modulgemeindemitglieder nicht nach Belieben Ressourcen akquirieren und wieder freigeben, sondern müssen sich die Betriebsmittel vom GVM zuteilen oder gegebenenfalls auch entziehen lassen.

Benötigt ein Gemeindemitglied weitere Prozessorleistung oder spezielle Hardware, über die es bisher noch nicht verfügen kann, so stellt es eine Dienstanfrage an das GVM. Das GVM prüft nach den Richtlinien der Gemeinderegeln und mit Hilfe des Ressourcen- und Sicherheitmanagements, ob die spezifizierten Ressourcen zum gewünschten Zeitpunkt und zu den gewünschten Bedingungen zur Verfügung gestellt werden können. Kann den Anforderungen entsprochen werden, so antwortet das GVM mit einem Vertrag. Außerdem wird eine vom GVM unterschriebene Version des Vertrags an das Notar- und Abrechnungsmodul der Gemeinde geschickt. Akzeptiert das nachfragende Modul den Vertrag des GVM, unterschreibt es ebenfalls und läßt den Vertrag dem Notar- und Abrechnungsmodul zukommen. Das Notar- und Abrechnungsmodul prüft die elektronischen Unterschriften sowie die Inhalte der Verträge und bestätigt den Ver-

tragspartnern die Gültigkeit ihres Abkommens. Das GVM wird nun vertragskonform die Ressourcen auf die Ausbreitung des Moduls vorbereiten, indem es zum gegebenen Zeitpunkt einen Port einrichtet, durch den sein Vertragspartner einen 'eigenen' Mikrokern auf der entsprechenden Hardware zur Ausführung bringt. Hat der Mikrokern seine Arbeit aufgenommen, wird dem GVM die erfolgreiche Expansion des Moduls signalisiert, worauf dieses den Port wieder schließt. Je nachdem, welche Aufgaben auf den neu eingenommenen Ressourcen zu bearbeiten sind, werden weitere Programmcodes von der PAK des expandierenden Moduls auf die Ressource transportiert. Die Authentizität der Programmcodes wird von der ÜAE des aussendenden Moduls überprüft und anschließend zur Ausführung gebracht. Abbildung 4.6 stellt die beschriebenen Vorgänge in einem Pr/T-Netz dar.

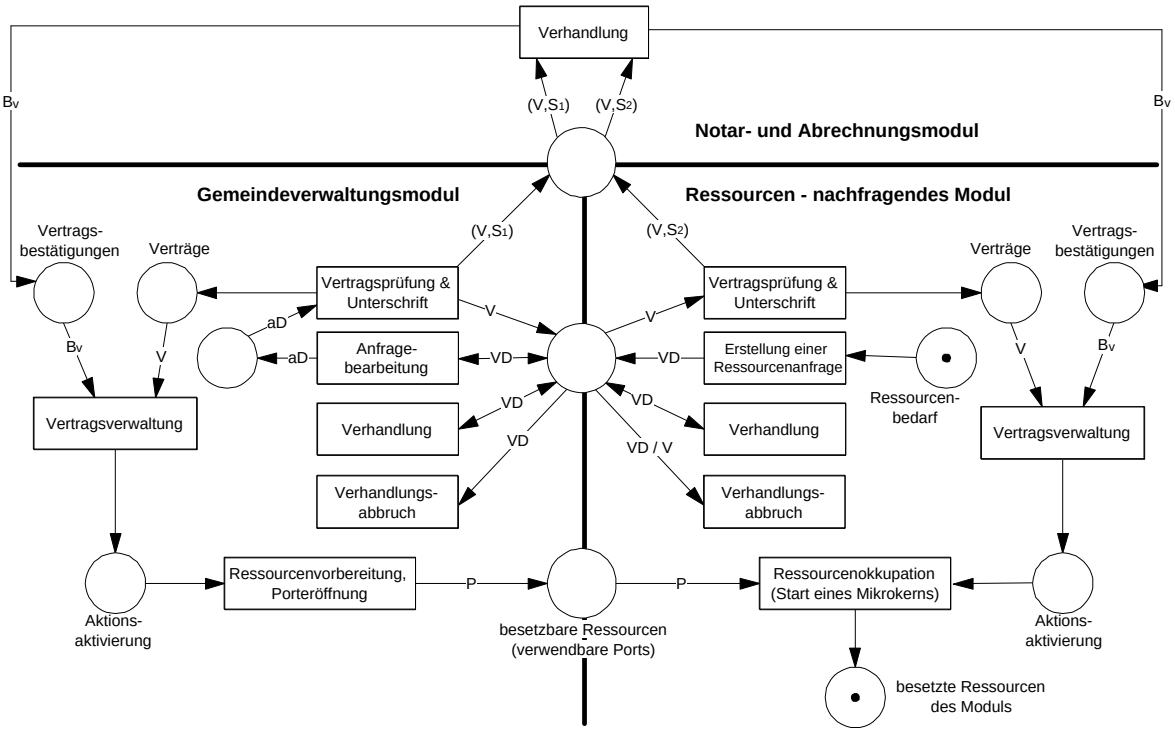


Abbildung 4.6: Vorgänge bei der Ressourcenbelegung durch ein Modul

Installation eines Moduls: Bei der eben vorgestellten Methode der Ressourcenbelegung ist das Modul Initiator dieses Vorgangs und kann die angebotenen Ressourcen und deren Nutzungsbedingungen akzeptieren oder auch nicht. Voraussetzung dafür ist, daß es bereits mindestens eine Prozessorressource nutzt, wie man aus Abbildung 4.6 entnehmen kann. Eine nicht erkennbare Voraussetzung ist, daß das Modul zur Gemeinde gehört. Um die Kette der Modulauthentifikationen nicht zu unterbrechen, können nur solche Module Mitglieder der Gemeinde sein, die durch das GVM installiert worden sind.

Soll ein neues Modul in der Gemeinde installiert werden, müssen zunächst alle benötigten Komponenten für den Betrieb des neuen Moduls registriert, wenn nötig

installiert und legitimiert sein. Je nach Art und Größe des neuen Moduls können diese Vorbereitungsarbeiten mitunter aufwendig und knifflig sein. Deshalb wird neben der eigentlichen Modulinstallierung in der Gemeinde auch die Modulplanung, Modulkonfigurierung und Vorbereitung durch das Installations- und Wartungsmanagement[4] unterstützt. Vom Hersteller werden für die jeweilige Systeminstallation bestimmte Modulgrundtypen mit Strategie und Modulstartskript vorkonfiguriert, die dann entsprechend den Lizenzen des Kunden erweitert oder umkonfiguriert werden können. Sind die Eigenschaften, Dienste und anderen Parameter bei der Modulplanung erfaßt worden, berechnet das IWM die Komponentenkonfigurationen mit den jeweiligen Einstellungen unter Berücksichtigung der bereits vorhandenen Systemkomponenten und plant den Arbeitseinsatz. Dieser Plan kann von den Mitarbeitern des Systembetriebs geprüft und bei Bedarf geändert werden. Der Plan wird erneut durchgerechnet und bei nicht behebbaren Konflikten verworfen. Das IWM weist auf die Probleme hin und gibt, sofern möglich, Vorschläge für einen alternativen Plan an. Wird der Plan von den Systemadministratoren akzeptiert, beginnt das IWM die Arbeitseinsätze so weit als möglich vorzubereiten, Listen von physikalisch bzw. logisch nicht vorhandenen Komponenten zu erstellen sowie eine Strategie und ein Modulstartskript zu generieren. Nachdem notwendige Installationsarbeiten der Komponenten durchgeführt und Legitimationen ausgesprochen worden sind, wird eine Installationskennung für das neue Modul berechnet, und das vorbereitete Installationsskript elektronisch unterschrieben. Der Mikrokern erhält die Installationskennung und wird auf dem betreffenden Rechnersystem gestartet. Während sich das neue Modul startet, werden die Vorgänge vom IWM überwacht; bei Bedarf wird eingegriffen. Erklärt das neue Modul seine Einsatzbereitschaft durch die Übermittlung seiner Funktionsüberprüfungsergebnisse und Authentifikationsdaten, die es aus der Eigenvalidierung erzeugt, wertet das IWM die Daten aus und beauftragt das Sicherheitmanagement, eine Sicherheitseinstufung und Legitimierung des neuen Moduls vorzunehmen. Ist die Legitimierung erfolgt, erhält das neue Modul seine Strategie und seine endgültige Systemidentität. Bei der Legitimierung wird das neue Modul im Modulregister des GVM aufgenommen und ein Konto mit seiner Identität beim Notar- und Abrechnungsmodul angelegt. Erst mit der Legitimierung kann das neue Modul mit anderen Gemeindemitgliedern Verträge abschließen.

4.2.2 Kommunikationsmodule (KOM)

Modulgemeinden können in Koexistenz mit anderen Gemeinden Rechnernetze und Rechnersysteme sowie andere Hardwarekomponenten nutzen. Das bedeutet, daß mehrere Gemeinden ein Rechnersystem als Gemeinderessource aufnehmen können und dieser Computer durch Module der einzelnen Gemeinden genutzt wird. Die Sicherheitspolitik der Gemeinden und der jeweiligen Module legt fest, welche Module bzw. Einheiten auf der betreffenden Verarbeitungskomponente zum Einsatz kommen.

Kommunikation zwischen Modulen verschiedener Modulgemeinden erfolgt über spezielle Kommunikationsmodule. Diese Kommunikationsmodule repräsentieren ihre Gemeinden gegenüber anderen Gemeinden, sorgen für einen integren Kommunikationsaustausch zwischen den Modulen dieser Gemeinden und nehmen Vermittlertätigkeiten

[4]Im weiteren Text wird IWM abkürzend für Installations- und Wartungsmanagement verwendet

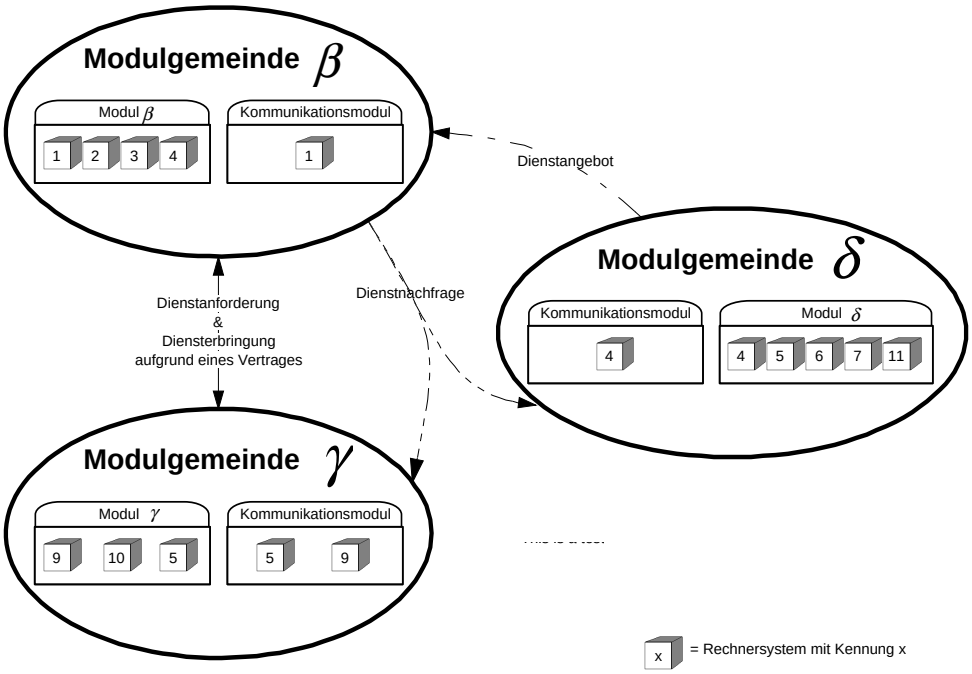
wahr. Erhält ein Modul auf seine Dienstanfrage keine oder unbefriedigende Dienstnutzungsangebote, so kann es ein oder mehrere Kommunikationsmodule, sofern vorhanden, beauftragen, bei anderen Modulgemeinden nach entsprechenden Diensten nachzufragen. Kommunikationsmodule, die solche Vermittlungsaufträge erhalten, nehmen Kontakt mit Kommunikationsmodulen anderer Gemeinden auf und übermittlen die Dienstanfrage. Die Kommunikationsmodule der fremden Gemeinden erstellen und versenden entsprechende Dienstnachfragen an die Module ihrer Gemeinden und leiten die eintreffenden Dienstangebote an das nachfragende Kommunikationsmodul der fremden Gemeinde weiter, das seinerseits die Dienstangebote seinem Auftraggeber zustellt. Kann ein akzeptables Angebot ausgemacht werden, so treten die Module der einzelnen Gemeinden über die vermittelnden Kommunikationsmodule in Vertragsverhandlungen ein. Ist ein Vertragsabschluß erzielt, so werden alle notwendigen Daten zur Dienstanforderung, Diensterbringung und Dienstabrechnung über die Kommunikationsmodule abgewickelt.

Die Beschreibung der Tätigkeit von Kommunikationsmodulen läßt schon erahnen, daß sie ein umfangreiches Spektrum unterschiedlichster Funktionsklassen benötigen. Die Qualität ihrer Funktionalität bestimmt wesentlich die Sicherheit ihrer Gemeinde. Versuchen Kommunikationsmodule Kontakt mit Kommunikationsmodulen anderer Modulgemeinden aufzunehmen, so müssen sie sich zunächst über eine gegenseitige Akzeptanz und Sicherheitsrelevanz einigen. Konnte eine Einigung erzielt werden, müssen sie Kommunikationsmodi, Sicherheitsmechanismen sowie eine Signatur und Interpretation der Nachrichteninhalte und Sicherheitskennzeichen festlegen. Nun können Daten ausgetauscht und für die Module der jeweiligen Gemeinden aufbereitet werden. Bei einem Vertragsabschluß zwischen Modulen verschiedener Gemeinden werden die vermittelnden Module und die genannten Festlegungen der Intermodulgemeindekommunikation zu Vertragsbestandteilen. Die Kommunikationsmodule speichern die Vertragsnummer und richten spezielle Ports zur Dienstanforderung und Diensterbringung ein. Abbildung 4.7 zeigt drei Modulgemeinden, die teilweise Rechnersysteme gemeinsam nutzen und miteinander kommunizieren.

4.2.3 Notar- und Abrechnungsmodule (NAM)

Notar- und Abrechnungsmodule, kurz NAM, zählen zu den vertrauten Instanzen einer Modulgemeinde. Vertraute Instanzen sind Ressourcen oder Module einer Modulgemeinde, die eine besondere Vertrauensstellung genießen. Diese Vertrauensstellung wird vom GVM ausgesprochen und gilt für ein wohldefiniertes Aufgabengebiet. Notar- und Abrechnungsmodule werden bei Vertragsabschlüssen benötigt. Sie erhalten die Verträge von den Vertragsparteien zusammen mit deren elektronischen Unterschriften. Das NAM überprüft die Übereinstimmung der Vertragsexemplare, die formale Form des Vertrages, registriert den Vertrag, die Vertragsparteien, die am Vertrag beteiligten Instanzen sowie die Abrechnungsbedingungen. Mit Hilfe des Sicherheitssystems des GVM und des NAM-eigenen Abrechnungssystems überprüft das NAM, ob die beteiligten Parteien und Instanzen integer sind, d.h. ob die Vertragsparteien zum Zeitpunkt des Abschlusses:

- legitimiert sind, und deren Sicherheitseinstufungen nicht mit den im Vertrag vereinbarten Nutzungsrechten kollidieren. Das gleiche gilt für beteiligten Instanzen



Abbildung~4.7: Modulgemeinden, die teilweise dieselben Ressourcen nutzen und miteinander kommunizieren

wie z.B. Benutzerschnittstellenmodule, Kommunikationsmodule usw.

- über entsprechnde Finanzmittel verfügen um den Vertrag erfüllen zu können.

Fällt die Überprüfung positiv aus, vergibt das Sicherheitsmanagement des GSM eine Sicherheitseinstufung für diesen Vertrag. Das NAM erklärt nun den Vertrag als abgeschlossen und setzt die Vertragsparteien davon in Kenntnis, indem es jeder Partei ein sicherheitseingestuftes und von ihm unterschriebenes Vertragsexemplar zukommen läßt.

Komplizierter sind die Vorgänge bei Verträgen zwischen Modulen unterschiedlicher Modulgemeinden. Hier erhält jedes NAM der jeweiligen Gemeinde die von den Vertragspartnern unterzeichneten Verträge. Verlaufen die Überprüfungen erfolgreich, so tauschen die NAM die Dokumente gegenseitig aus und es werden entsprechende Finanzmittel beim NAM der diensterbringenden Gemeinde hinterlegt. Wiederum setzt eine Überprüfung ein. Ist auch diese erfolgreich, so synchronisieren sich die NAM und teilen den Modulen ihrer Gemeinden die Gültigkeit des geschlossenen Vertrages mit.

Neben den Vertragsbestätigungen muß das NAM die Abrechnungen der erbrachten Dienstleistungen durchführen. Aus den Vertragsprüfungen kennt es die vereinbarten Abrechnungsmodi und läßt sich, sofern im Vertrag vorgesehen, vom Dienstnehmer Anzahl und Art der Dienstereignisse bestätigen. Stimmen diese Daten mit denen der Diensterbringer überein, so werden die entsprechenden Beträge abgebucht bzw. gutgeschrieben. Bei Abrechnungen von Diensterbringungen zwischen Modulen unterschiedlicher Gemeinden sychronisieren sich entsprechend die NAM der jeweiligen Gemeinden. Kommt es bei der Abrechnung zwischen den Modulen einer Gemeinde zu Konflikten,

so kann das Problem durch die Gemeinderegeln geklärt werden. Bei Abrechnungen zwischen zwei Modulgemeinden haben sich die NAM auf entsprechende Behandlungen beim Vertragsabschluß geeinigt.

4.2.4 Personenbenutzer einer Modulgemeinde

Genau wie die Modulgemeindemitglieder und Gemeinderessourcen werden auch die Personen, die die Funktionen und Dienste von der Modulgemeinde nutzen wollen, registriert und legitimiert; anschließend wird ihnen ein Nutzungsrecht zuerkannt. Die Registrierung und Legitimierung einer Person kann nur durch die Dienste des Personenmanagements des GVM erfolgen. Jede Person erhält mit der Legitimierung, genau wie alle anderen Mitglieder und Dokumente im System auch, eine Sicherheitseinstufung, die durch ein sogenanntes "security label" bzw. MAC Label prinzipiell festlegt, welche Rechte ihnen in welchem Bereich des Systems erteilt werden können (MAC). In Modulgemeinden gibt es drei Benutzergruppen:

1. Moduladministratoren (MA): Den Moduladministratoren kann als einziger Personenguppe der Modulgemeindebenutzer das Recht zugesprochen werden, über das GVM auf die Administrationsfunktionen der RAE der einzelnen Modulgemeindemitglieder zuzugreifen. Damit können sie in die Lage versetzt werden, die Aktivitäten der jeweiligen Module direkt zu überwachen, auf diese unmittelbaren Einfluß zu nehmen, Aktivitäten zu initiieren sowie die Strategie des Moduls zu ändern. Den Einheiten des Moduls bleibt es verborgen, ob die RAE selbständig oder unter Leitung eines MA handelt. Allerdings werden Vorgänge und Ereignisse im Modul von diesem protokolliert, so daß jederzeit nachverfolgt werden kann, welche Handlungen ein MA vorgenommen hat. Kontrolliert wird er dabei von der ÜAE des Moduls selbst und dem Sicherheitsmanagement des GVM. Zielgruppe dieser Gemeindebenutzergruppe sind ausgewählte und hoch qualifizierte Mitarbeiter des Systembetriebs und des Sicherheitsmanagements (siehe Systemanalyse, 2.1.2).

2. Modulgemeindebenutzer (MB): Die Modulgemeindebenutzer bilden in der Regel die größte Personengruppe, die Zugriff auf die Modulgemeinde erhalten kann. Bei ihrer Legitimierung erhalten sie ein Konto bei dem Notar- und Abrechnungsmodul, welches es ihnen ermöglicht, Verträge abzuschließen. Subjekte, die Verträge abgeschlossen haben, werden Vertragsinhaber genannt. Die von ihnen abgeschlossenen Verträge können, sofern dies vorgesehen war, durch Nachverhandlungen erweitert bzw. verändert werden. Auf diese Weise können sie die Nutzung der im Vertrag festgelegten Dienste durch sogenannte Subscriber-Einträge anderen Subjekten zugänglich machen, wie dies auch die Module können. Allerdings können sie als Subscriber nicht Module einsetzen, was den Modulen im umgekehrten Fall möglich ist. Ob die von Subscriber genutzten Dienste auf deren Konto oder demjenigen des Vertragsinhabers abgerechnet werden, obliegt wiederum der Festlegung durch den Vertragsinhaber. Subscriber eines Vertrages kann nur ein legitimiertes Systemmitglied werden, das ein dem Vertrag entsprechendes security label besitzt. Die Gruppe der Modulgemeindebenutzer besteht aus drei Typen:

- aktive Modulgemeindebenutzer (AMB): Sie können im Rahmen ihrer Sicherheitseinstufung selbständig Nutzungsverträge mit den Modulen der Gemeinde abschließen und Dienste im Rahmen der abgeschlossenen Verträge nutzen. Die Verträge können von ihnen selbst oder durch einen VMB für sie ausgehandelt worden sein. Zum Abschluß eines Nutzungsvertrages, egal ob er von ihnen selbst oder für sie ausgehandelt wurde, muß dieser mit einer elektronischen Unterschrift von ihnen authentifiziert worden sein.
- vertraute Modulgemeindebenutzer (VMB): Personen, die zu den VMB zählen, können genau die Rechte erhalten, die auch AMB erhalten können. Darüberhinaus können sie befugt werden, Dienste für andere MB auszuhandeln und diesen zum Vertragsabschluß vorzulegen. Außerdem kann ihnen das Recht zum Anlegen von MA und VB sowie zum Aushandeln von Verträgen für andere AMB und PMB eingeräumt werden.
- passive Modulgemeindebenutzer (PMB): Passive Gemeindemodulbenutzer sind MB, die lediglich Verträge abschließen, nicht aber aushandeln können.

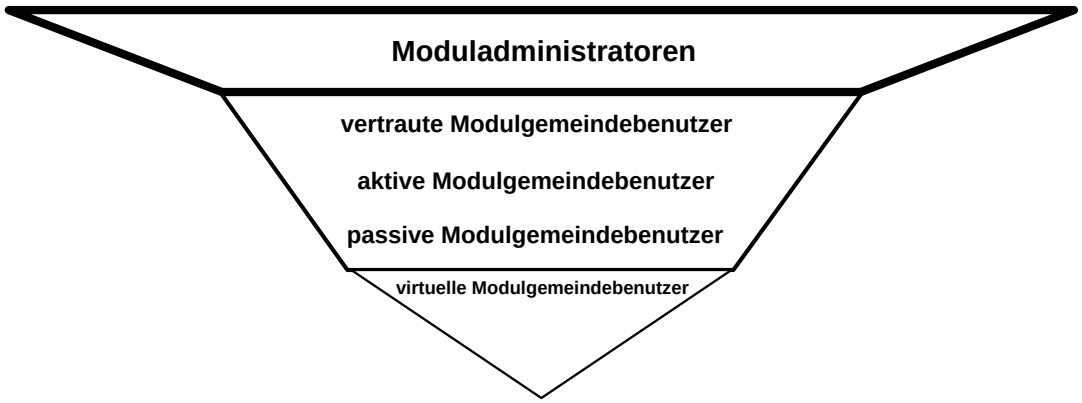
Alle MB können als "Paten" für VB eingesetzt werden und so deren Interessen wahrnehmen, allerdings nur in ihrem Rahmen als MB-Typ.

3. virtuelle Modulgemeindebenutzer (VB): stellen eine Sonderform der PMB dar. Durch sie soll es ermöglicht werden, Personen wie z.B. Besuchern, Gästen und speziellen Kunden zum System Zutritt zu gewähren, ohne sie explizit registrieren und legitimieren zu müssen. Diese Personen erhalten eineindeutige Legitimationsnachweise, mit denen sie zu den Diensten, die den VB zur Verfügung stehen sollen, Zugang erhalten. Jeder VB besitzt sogenannte Paten, die für ihn Verträge abschließen oder ändern können. Paten können AMB, VMB oder PMB sein.

Abbildung 4.8 zeigt die einzelnen Benutzertypen der Modulgemeinde und beschreibt deren sicherheitstechnische Relevanz. Die absolute Bedeutung wird durch die horizontale Ausbreitung der Einrahmungen dargestellt, während die relative Beziehung durch die vertikale Anordnung gegeben ist.

4.2.5 Interessengruppen einer Gemeinde

Interessengruppen werden durch Personentypen und/oder Module gebildet. Sie werden auf Initiative von mindestens zwei Gruppenmitgliedern beim GVM angelegt und verwaltet. Die Interessengruppen besitzen eine eigene Kommunikationsadresse und leiten eintreffende Nachrichten an die Mitglieder weiter. Ziel einer Interessengruppe ist es, die Aktivitätsergebnisse einzelner Gruppenmitglieder allen Mitgliedern zukommen zu lassen oder durch die Gesamtheit der Gruppe bestimmte Dienste zu ermöglichen oder zu verbessern. So können einzelne Module durch das Senden ihrer Alarme an eine Gruppe, die aus Krisenmanagementmodulen und Mitarbeitern des Sicherheitsmanagements besteht, deren Mitglieder geschlossen alarmieren, ohne diese einzeln verständigen zu müssen. Eine andere Interessengruppe, die nur aus in verschiedenen Gemeinden liegenden Modulen besteht, bauen eine spezielle Dienstinfrastruktur auf und vermarkten diese gemeinsam.



Abbildung~4.8: Benutzertypen der Modulgemeinde und deren sicherheitstechnische Bedeutung.

4.2.6 Benutzerschnittstellenmodule (BSM)

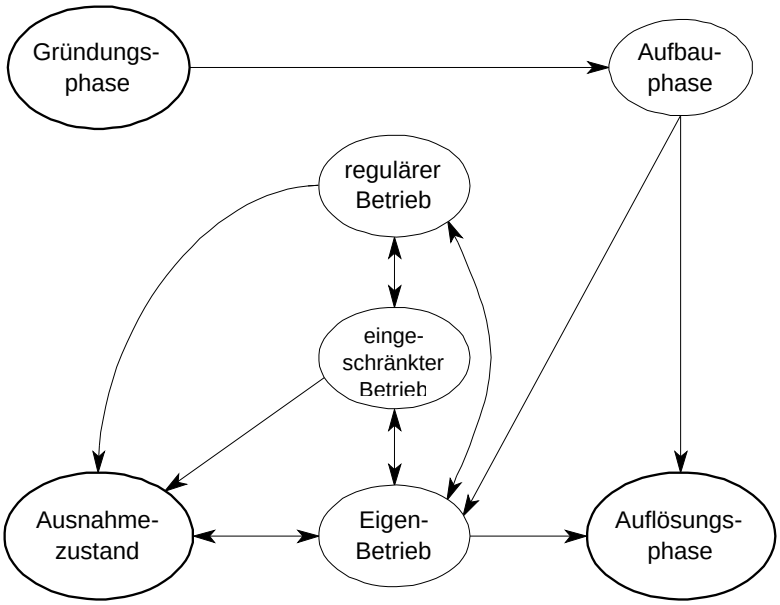
Benutzerschnittstellenmodule bilden, wie der Name schon andeutet, die Schnittstellen zwischen Modulgemeinde und Personen. Mit Hilfe dieser Module können Anwender Informationen von Modulen erfragen (Dienstnachfragen), Verträge aushandeln und abschließen sowie Dienste anfordern. Möchte ein Benutzer zu einer Modulgemeinde Zugang erhalten, so muß er sich gegenüber dem BSM authentifizieren. Kann das BSM die Authentifikation akzeptieren, so ist es dem Benutzer möglich, Kontakt zu Modulen oder anderen Benutzern der Modulgemeinde aufzunehmen. Ein BSM kann mehrere Anwender gleichzeitig bedienen.

4.2.7 Lebenszyklus einer Modulgemeinde

Der Lebenszyklus einer Modulgemeinde beginnt mit der Ur-Installation eines GVM. Während dieser Ur-Installation werden erste Rechnersysteme vollständig in Besitz genommen und das GVM wird installiert und in Betrieb genommen. Die Gemeinde befindet sich in der Gründungsphase, die mit der vollen Betriebsbereitschaft des GVM beendet wird. Mit der Akquisition weiterer Gemeinderessourcen, Registrierung und Legitimierung von Personen, Installation weiterer Basismodule und deren eigenständigen Aufbau und Ausdehnung auf die Gemeinderessourcen wird die Aufbauphase der Gemeinde begonnen. In dieser Phase wird zunächst die Infrastruktur der Gemeinde durch die Einrichtung von NAM, BSM und KOM vervollständigt. Anschließend werden system- bzw. anlagenspezifische Module installiert. Die Aufbauphase ist mit dem Abschluß der Modulinstallationen und der Einrichtung aller zum Betrieb erforderlichen Verträge abgeschlossen.

Es folgt der Betriebszustand Eigen-Betrieb. Der Eigen-Betrieb stellt einen abgesicherten Betriebszustand einer Modulgemeinde dar, in welchem definierte Zustände und Situationen in der Modulgemeinde hergestellt und durchgetestet werden können. Jegliche Zugänge von nicht speziell autorisierten und in die Tests bzw. Simulationen einbezogenen Personen zu den Modulen oder zur Gemeinde sind geschlossen. Nichts kann von draußen rein und nichts von drinnen raus. Zeigen die Tests der Modulge-

meinde, daß ein eingeschränkter oder gar regulärer Betrieb möglich scheint, so kann in diesen Betriebszustand gewechselt werden. Beim eingeschränkten Betrieb sind bestimmte Teile der Modulgemeinde in einem abgesicherten Zustand. Dieser ist vorgesehen für Wartungsarbeiten oder Erweiterungen der Modulgemeinde, die nicht eine vollständige "Schließung" der Modulgemeinde — Wechsel in den Eigen-Betrieb — erfordern. In besonders kritischen Situationen des Gemeindebetriebs kann das GVM einen Ausnahmezustand über die Gemeinde verhängen. Wird dieser Zustand erklärt, legen alle Gemeindemodulmitglieder ihren Betrieb nieder, beginnen mit der Ausführung entsprechender Notprogramme und stellen ganz spezielle Dienste zur Verfügung. Je nach Notstandsplänen der Gemeinderegeln wird — ähnlich wie beim Eigen-Betrieb — die Modulgemeinde "dicht" gemacht. Der letzte Zustand in der Existenz einer Modulgemeinde ist die Auflösungsphase. Während dieser Phase werden alle belegten Ressourcen sowie die Daten und Programmcodes der Modulgemeindemitglieder auf den Gemeinderessourcen beseitigt. Abgeschlossen wird dieser Zustand mit der Selbstzerstörung des GVM. Abbildung 4.9 zeigt den Lebenszyklus einer Modulgemeinde.



Abbildung˜4.9: Lebenszyklus einer Modulgemeinde

Ur-Installation

Eine besondere Bedeutung in der Gründungsphase kommt der Ur-Installation zu. Sie ist mitentscheidend für die spätere Abgeschlossenheit und Integrität der Modulgemeinde.

Die Strategie der Modulauthentifikation fußt auf dem Prinzip des 'secure booting'. Ziel ist es, durch eine Kette von elektronischen Unterschriften integrer Subsysteme ein integres Gesamtsystem aufzubauen. Durch die Unterschriften ist die Authentizität der Teilsysteme sichergestellt. Beim Aufbau dieser Kette initiiert ein integres Grundsystem neue Teilsysteme, deren Integrität es durch spezielle Mechanismen prüft. Diese

neuen Teilsysteme werden wiederum durch eine elektronische Unterschrift des Grundsystems fixiert und somit ihre Authentizität gewährleistet. Diese Teilsysteme können nun ihrerseits neue Systemteile aufbauen. Dabei verfahren sie wie das Grundsystem und fixieren die von ihnen initiierten Systemteile mit ihrer Unterschrift.

Die Ur-Installation muß dafür Sorge tragen, daß das Grundsystem, der Grundstein der neuen Gemeinde, integer ist. Dazu soll eine spezielle Software verwendet werden, deren Authentizität durch eine elektronische Unterschrift des Herstellers bzw. des Systemanbieters fixiert ist. Damit diese Software, genannt Ur-Installation, ihre Arbeit auf einem Digitalrechner aufnehmen kann, wird ein Schlüssel zur Generierung einer Gemeindeidentität und zum Dechiffrieren der verschiedenen Programmcodes der Ur-Installation benötigt. Schlüssel und Software erreichen den authorisierten Systemanwender auf getrennten Wegen, um die Rechtmäßigkeit der Ur-Installation sicherzustellen.

Ist die Ur-Installation auf einem Digitalrechner in Betrieb gesetzt worden, beginnt sie zunächst mit der Untersuchung dieses Computers. Dabei hält sie entscheidende Merkmale des Systems fest. Erfüllt das Computersystem die von der Ur-Installation benötigten Voraussetzungen, so beginnt sie mit der Installation des Betriebssystems auf dem Rechner. Die Codes des Betriebssystems sind ebenfalls in der Ur-Installation enthalten. Das Betriebssystem wird konfiguriert und mögliche Zugänge (wie z.B. Wechselmedienlaufwerke, Netzwerkzugänge, Konsolen usw.) verschlossen bzw. blockiert. Das Rechnersystem ist nun vorbereitet, um das Gemeindeverwaltungsmodul der neuen Gemeinde aufzubauen. Es wird zunächst dessen Mikrokern gestartet, der entsprechend der Beschreibung der Modulinstallation ein GVM initiiert, welches vorerst nur auf einem Rechnersystem arbeitet. Es werden zunächst nur Funktionen und Dienste bereitgestellt, die zur weiteren Fortführung der Ur-Installation benötigt werden. Sind die Schutzmechanismen des neuen GVM aktiviert, werden die Zugänge zum Rechnersystem angemessen geöffnet. Erste Systemadministratoren können registriert und legitimiert werden, weitere Computersysteme mit speziellen, vom GSM vorbereiteten Datenträgern werden über ein Netzwerk in Betrieb genommen, registriert und legitimiert. Sind alle notwendigen Ressourcen und Personen für die Aufbauphase erfaßt, baut sich das GVM vollkommen auf. Die Ur-Installation ist damit abgeschlossen.

4.3 SIPORT, Modulkonfiguration für ein DNB-System

Mit Hilfe von Modulen und Modulgemeinden sollen die an das neue SIPORT Zugangskontrollsystem gestellten Aufgaben effizient und universell gelöst werden. Speziellen Wünschen und Anforderungen der Kunden, die

- eine neue Anlage benötigen,
- eine bestehende Anlage erweitern oder verändern wollen,

können durch

- Installation zusätzlicher "standard SIPORT Module",

- Erweiterung bestehender durch neue Module,
- Veränderung bestehender Dienste,
- Implementierung und Installation neuer Module

entsprochen werden. Es ist somit möglich, sehr unterschiedliche Systeminstallationen aus einer relativ geringen Anzahl von Standardbausteinen zusammenzusetzen. Zu diesen Standardbausteinen sind neben den bereits beschriebenen Modulen einer Modulgemeinde die anwendungsspezifischen SIPORT Module zu zählen.

Es sollen nun einige dieser SIPORT Module vorgestellt werden, mit denen die in der Systembegründung dargestellten DNB-Systeme realisiert werden können.

4.3.1 Zutrittskontrollmodul (SiZuM)

Zutrittskontrollmodule übernehmen die lokale Zugangskontrolle. Zu ihrem Aufgabenbereich gehört:

1. die Abbildung und Durchsetzung der Regeln der Sicherheitspolitik für den Zugangskontrollbereich
2. das Validieren von Legitimationskarten
3. die Sanktion von Legitimationskarten
4. die Erzeugung und Aktualisierung der zur Kartenvalidierung verwendeten Daten auf den Karten und im System
5. die Überprüfeng von Zugangs- bzw. Nutzungsrechten
6. die Veränderung der Nutzungsrechte (Abbuchungen)
7. die Ansteuerung von Barrieren oder Öffnung von Zugängen
8. die Protokollierung der Ereignisse
9. die Bereitstellung von Zustandsdaten und der protokollierten Ereignisse
10. die Benachrichtigung oder Alarmierung der Mitarbeiter des Sicherheitsmanagements bzw. Systembetriebs entsprechend den Regeln der Sicherheitspolitik bzw. bei definierten betriebstechnischen Situationen.

Die Haupteinheiten des SiZuM sitzen auf einem Rechner, der eine Gemeinderessource der SIPORT Modulgemeinde ist.

Für die Ansteuerung der Kartenleser, Barrieren und anderen Zutrittskontrollperipherien, die durch das SIPORT OSM-Betriebssystem (das einen eigenen Rechner benötigt) verwaltet werden, besitzt das SiZuM spezielle Filter. Durch sie findet der Datenaustausch zwischen dem OSM-System und dem Modul statt. Dabei werden zum einen Konfigurationen und auf direktem Wege Maßnahmen vom Modul an das OSM-System übermittelt, das diese seinerseits durchsetzt. Zum anderen werden Alarme,

Nachrichten, Zustandsdaten und Konfigurationen vom OSM-System aktiv oder passiv dem Modul bereitgestellt.

Der Kartenleser mit eigenem PC-Mikrorechnersystem wird durch das Modul selbst mit einem Mikrokern und entsprechenden Programmcodes belegt. Damit kann das Modul selbständig die benötigten Anfragen, Konfigurationen und andere Aktionen bearbeiten und durchführen. Die Vorzüge des Moduls, wie z.B. seine Abgeschlossenheit gegenüber der Umwelt, seine Betriebssicherheit, Flexibilität usw. kommen hier voll zur Geltung.

4.3.2 Kassenmodul (SiKaM)

Die SIPORT Kassenmodule stellen Dienste für den Betrieb von Legitimationskartenausgabestationen bereit (vgl. Systemanalyse). Sie unterstützen:

1. Erfassung von Waren und Dienstleistungen durch Kassierer bzw. Kunden
2. selbständige Bestimmung des günstigsten Tarifes (Tarifoptimierer)
3. Legitimierung von Kunden
4. Initialisierung von Legitimationskarten
5. sofortige Durchsetzung von Nutzungsrechten im System
6. Freischaltung sanktionierter Legitimationskarten
7. Erstellung von Belegen und Gutscheinen
8. Unterstützung des Zahlungsvorganges (moderne Zahlungsverfahren, automatische Wechselgeldausgabe, usw.)
9. Verwahrung von Barwerten
10. Kassenabrechnung mit dem Kassenpersonal
11. Überfallmelder für Kassenpersonal bzw. Sensor für Manipulationsversuche bei Kassenautomaten
12. Protokollierung der Ereignisse
13. Bereitstellung von Zustandsdaten und der protokollierten Ereignisse
14. Benachrichtigung oder Alarmierung der Mitarbeiter des

    (a) Sicherheitsmanagements entsprechend den Regeln der Sicherheitspolitik

    (b) Systembetriebs bei definierten betriebstechnischen Situationen

    bei

    (a) Fehlverhalten des Personals bzw. der Kunden,

    (b) Ausfall von Komponenten oder Baugruppen, die das SiKaM benutzt.

Ein SiKaM befindet sich jeweils auf einem Kassenrechner bzw. Mikrorechner in einem Verkaufsautomaten, an den die Peripheriegeräte für Legitimationskartenausgabestationen angeschlossen sind. Dieses Rechnersystem ist eine Gemeinderessource der SIPORT Modulgemeinde. Für die Unterstützung der Zahlungsvorgänge mit modernen Zahlungsmitteln verfügt das SiKaM über spezielle Filter, über die der Datenaustausch mit den Point of Sale Terminals erfolgt.

4.3.3 Auswertungsmodul (SiAuM)

Hauptaufgabe eines Auswertungsmoduls ist es, die durch Kunden und Geschäftspartner verursachten Ereignisse zu sammeln und entsprechend den Anforderungen des operativen Betriebs auszuwerten. Dabei sollen Onlineauswertungen entsprechend den Beschreibungen in den Einsatzszenarios ebenso möglich sein wie aufwendige statistische Trendanalysen und Hochrechnungen. Es soll bei der Bedarfsplanung und Kostenanalyse sowie bei der Tarifgestaltung unterstützen. Damit es die für seine Tätigkeit notwendigen Daten von den Gemeindemitgliedern erhält, wird es vom GVM zu einer vertrauten Instanz erklärt; dieser Instanz werden die Ereignisdaten der einzelnen Module zu bestimmten Vertrags- und Diensttypen durch die Module selbst zu Verfügung gestellt.

4.3.4 Tarifmodul (SiTaM)

Das Tarifmodul soll eine einfache, schnelle und flexible Erstellung, Verteilung, Durchsetzung und Verwaltung der Tarife ermöglichen. Der Betreiber eines DNB-Systems soll mit Hilfe der Informationen des SiAuM ein Tarifsystem aufbauen und weiterentwickeln können, welches seinen betrieblichen Zielen entspricht. Dabei kann er nicht nur auf die eigenen Dienste und Vertriebswege zurückgreifen, sondern auch mit anderen Betreibern, die ebenfalls ein SIPORT Zugangskontrollsystem verwenden, einen Verbund bilden. Alle administrativen Tätigkeiten wie Tarifverteilung, Tarifanpassung, Abrechnung erbrachter Transportdienste, usw. wird dabei über die Infrastruktur der Modulgemeinden und das SiTaM abgewickelt.

4.3.5 Maschinenanlagesteuerungsmodul (SiMaM)

Die Integration der Steuerung von Maschinenanlagen (z.B. Skilifte) ins Gesamtsystem SIPORT soll mit dem SiMaM verwirklicht werden. Jedes installierte SiMaM ist genau einer Maschinenanlage zugeordnet, deren Parameter durch die Dienste des SiMaM abgefragt, geändert und protokolliert werden. Das SiMaM arbeitet auf einem oder mehreren Rechnersystemen, die Baugruppen besitzen und/oder an die Peripheriegeräte angeschlossen sind, durch die Anlagenparameter erfaßt und/oder verändert werden können. Der Datenaustausch zwischen Anlage und Modul erfolgt über Modulfilter, die notwendige algorithmische Transformationen und/oder Umsetzung des Datenformats vornehmen und die Daten in die bzw. aus den entsprechenden Kanälen der Hardwarekomponenten und Modulports schreiben bzw. lesen.

Entsprechend dem Anlagentyp und der Organisationsstruktur des Betriebskonzeptes übernimmt das SiMaM eines oder mehrere der folgenden Aufgaben:

- als passives Medium: Abfrage und/oder Veränderung von Parametern werden durch die Prozeßsteuerung bzw. Systembetrieb und/oder die Anlage initiiert.

- als aktives Medium: Abfragen und/oder Veränderung von Parametern zwischen Prozeßsteuerung bzw. Systembetrieb und der Anlage werden vom Modul initiiert.

- Dokumentation des Anlagenbetriebs: Betriebsdaten und Anlagenparameter werden aufgezeichnet und ausgewertet. Diese Daten werden auf Anfrage oder auf Initiative des SiMaM an autorisierte Instanzen zur Verfügung gestellt.

- aktive Steuerung, Regelung: Es werden Steuerkennwerte oder Betriebsmodi vom Systembetrieb und/oder von der Prozeßsteuerung vorgegeben bzw. abgefragt, die durch das Modul umgesetzt bzw. generiert werden. Mit Hilfe der Momentanbetriebswerte berechnet das Modul den gebotenen Verlauf der Anlagenparameter, die es mit geeigneten Steuerungs- und Regelalgorithmen umsetzt, oder aus deren Verlauf es umgekehrt Betriebskennzahlen generiert.

- eigenständiger Anlagenbetrieb: Die Anlage wird durch das SiMaM betrieben, indem es selbständig Anlagenparameter überprüft und verändert. Systembetrieb und/oder Prozeßsteuerung können die Steuerung der Anlage übernehmen und den eigenständigen Betrieb abschalten. In definierten Situationen wird das SiMaM von sich aus den Systembetrieb und/oder die Prozeßsteuerung benachrichtigen, alarmieren und/oder die Anlagensteuerung an eine entsprechend qualifizierte Instanz abgeben.

Die SiMaM sind Front-Ends zu den Maschinenanlagen, durch die diese von einem Prozeßleitsystem, z.B. in Form eines Prozeßsteuermoduls, oder durch Personen lokal oder von fern gesteuert werden können. Darüberhinaus könnten andere Module Daten von den SiMaM abfragen, um beispielsweise "online" eine Verkaufssteuerung oder Kundenlenkung durchzuführen. Damit sollen die Ziele verwirklicht werden, die im Abschnitt *Erweiterte Funktionalität* unter *Systemanalyse* dargestellt sind.

4.3.6 Kundeninformationsmodul (SiKIM)

Ein Kundeninformationsmodul ist ein Informationssystem, mit dem der DNB-Systembetreiber mit seinen Kunden und/oder die Kunden untereinander kommunizieren können, gleichsam eine "multimediale Litfaßsäule" mit erweiteter Funktionalität. Die Litfaßsäulen bilden die Service- und Informationsterminals (siehe Systemanalsyse), die durch den DNB-Systembetreiber und die Anbieter gestaltet werden.

Ziel ist es, daß der DNB-Systembetreiber bestimmten Kundengruppen ein Medium für Werbung und Informationsaustausch mit gegenwärtigen und möglichen zukünftigen Kunden zu Verfügung stellt. Der Anbieter kann selbständig seine Informationsdarstellung, Dienstpräsentation sowie Art und Umfang der Kommunikation mit dem Benutzer am Informations- bzw. Serviceterminal im Rahmen der vom DNB-Systembetreiber erworbenen Rechte gestalten und gezielt auf verschiedene Personengruppen abstimmen.

Der Kunde am Informations- und Serviceterminal kann die für ihn bestimmten Informationen und Dienste des DNB-Systembetreibers und der Anbieter abrufen. Die

Notwendigkeit der Identifikation des Terminalbenutzers ergibt sich aus Art und Informationsinteressen der Informations- bzw. Dienstanbieter.

Neben den reinen Kommunikations- und Diensterbringungsaufgaben soll das SiKIM Informationen über die Art der Benutzung der einzelnen Dienste des Moduls durch die Terminalbenutzer und die Anbieter sammeln und statistisch aufbereiten. Diese Daten sind teilweise den Kunden und/oder ausschließlich dem DNB-Systembetreiber zugänglich. Beispielsweise kann es für einen Anbieter von Interesse sein, welche Personengruppen welche Informationen von welchen Standorten aus abgerufen haben. Der SNB-Systembetreiber möchte in Hinblick auf eine eigene Bedarfsplanung wissen, wie häufig und an welchen Plätzen welche Terminalbenutzer auf die Terminals zugreifen. Weiterhin möchte er seine anbietenden Kunden beraten können, wie die Informationen und Dienste strategisch sinnvoll zu verteilen sind. Darüberhinaus benötigt der SNB-Systembetreiber Daten, die als Grundlage zur Abrechnung mit den Benutzern des SiKIM dienen.

Um ein solches Informationssystem aufbauen und betreiben zu können, stellt das SiKIM Dienste für folgende Aufgaben bereit:

- Administration des Informationssystems durch den DNB-Systembetreiber
- Bereitstellung und Konfiguration einer Entwicklungsumgebung durch den DNB-Systembetreiber zur Einrichtung und Verteilung von Informationen und Dienstleistungen durch den anbietenden Kunden im Rahmen seiner erworbenen Rechte
- Basisdienste für die Kunden zur Navigation, zum Abrufen und zur Bedienung der im SiKIM eingerichteten Dienste
- Protokollierung der kundenspezifischen Vorgänge im SiKIM und Auswertung der gesammelten Daten

4.4 Zusammenwirken der Module am Beispiel eines Skigebietes

Anhand einiger exemplarisch ausgewählter Tatigkeiten in einem DNB-System — hier am Beispiel eines Skigebietes — sollen die Wirkungsmechanismen der Module in einem realen System aufgezeigt werden.

Bei Lift- und Gondelbetreibern werden SiZuM zum Betrieb der Zutrittskontrollkomponenten eingesetzt, die in den offiziellen Besucherzugängen zu Lift- und Gondelanlagen installiert sind. Wird einem Kunden der Zugang zur Nutzung der betreffenden Anlage gewährt, so betrachtet das SiZuM dieses Ereignis als eine erbrachte Transportdienstleistung und rechnet diese mit seinem Vertragspartner ab. Dies ist in der Regel ein SiTaM.

4.4.1 Erstellung und Verbreitung von Tarifen

Tarife sind spezielle Verträge des SiTaM. Sie behandeln die Nutzungsbedingungen verschiedener Transportdienste, die durch das SiZuM erbracht werden. Soll ein Tarif erstellt werden, sendet das SiTaM an die verschiedenen SiZuM eine Dienstnachfrage ab.

Diese antworten mit entsprechenden Dienstnutzungsangeboten. Die Daten der Dienstnutzungsangebote und die der bereits unter Vertrag genommenen Transportdienste werden für die Tarifgenerierung aufbereitet und dem Anwender in entsprechender Form zur Auswahl angeboten. Er wählt die für seinen neuen Tarif benötigten Transportdienste aus. Entsprechend der Selektion werden weitere Dienste unter Vertrag genommen. Das SiTaM generiert einen Vertragsentwurf, der die ausgewählten Dienste, deren Nutzungsrechte sowie die Kosten für den neuen Tarif festlegt. Der Anwender kann nun Veränderungen an diesem Entwurf vornehmen, wobei er vom SiTaM unterstützt wird. Stellt der Anwender Werte ein, die nicht möglich oder wenig sinnvoll sind, wird er vom System darauf hingewiesen. Ist eine endgültige Version des Vertragsentwurfs festgelegt, und soll der Kunde das Angebotspaket nutzen können, aber nicht registriert und legitimiert werden, wird ein virtueller Benutzer angelegt, der Vertragsnehmer ist.

Verbreitung und Verkauf eines neu geschaffenen Tarifs (Vertragsentwurf) wird durch unter Vertrag stehende Kassenmodule realisiert. Diesen SiKaM wird der Tarif übermittelt, die daraufhin die entsprechenden Vertragsentwürfe in ihren Tarifoptimierer aufnehmen. Der Vertrag zwischen SiTaM und SiKaM legt fest, wie das Kassenmodul den Vertrag zwischen Kunde und Tarifmodul vorzubereiten und abzuschließen hat (welche Daten an das SiTaM zu übermitteln sind, welche Daten das SiTaM bereitstellt, wie welche Daten auf welchen Kartentyp zu schreiben sind, usw.).

4.4.2 Verkauf und Erteilung von Nutzungsrechten

Der Verkauf und die Erteilung von Nutzungsrechten wird durch die SiKaM vorgenommen. Hat sich der Kunde für einen Tarif entschieden, und sind alle notwendigen Daten erfaßt, so initialisiert das SiKaM eine entsprechende Legitimationskarte. Hat der Kunde einen personenbezogenen Tarif erworben, erhält er über das SiKaM eine eigene Identität und Legitimation im System. Dabei wird dem SiKaM vom Gemeindeverwaltungsmodul die Identitätsnummer und ein Schlüssel für die elektronischen Unterschriften des Kunden übermittelt. Das SiKaM übermittelt im Gegenzug dem GVM eine Legitimationskartennummer. Der Vertrag zwischen Kunde und GVM wird durch das SiKaM vorbereitet und mit der elektronischen Unterschrift abgeschlossen. Nach Abschluß des Vertrages setzt das GVM den neuen Vertragsnehmer auf die Subscriberlisten der entsprechenden Transportdienstnutzungsverträge mit den SiZuM. Mit Hilfe der Identitätsdaten des Kunden sowie seiner Nutzungsrechte wird die Legitimationskarte durch das SiKaM initialisiert und anschließend dem Kunden übergeben. Hat der Kunde einen übertragbaren Tarif erworben, so erhält er keine eigene Systemidentität. Stattdessen erhält er eine Legitimationskarte, die einem virtuellen Systembenutzer zugeordnet wird. Entsprechend dem Vertrag mit dem DTM übermittelt das SiKaM die Kartendaten an das SiTaM, das seinerseits die entsprechenden Subscribererweiterungen bei seinen Vertragspartnern vornimmt. Genau wie bei den personenbezogenen Tarifen wird die Legitimationskarte initialisiert und dem Kunden übergeben.

4.4.3 Vorgänge bei der Erbringung von Transportdiensten

Wird von einem Kunden mittels seiner Legitimationskarte ein Transportdienst an der Zugangskontrollstation einer Beförderungseinrichtung angefordert, so wird zunächst das ansteuernde SiZuM die Karte validieren. Erkennt das SiZuM die Karte an, werden

die Nutzungsrechte anhand der gültigen Verträge und der Kartendaten überprüft. Legitimieren die Rechte den Kunden zur Nutzung des Dienstes, werden entsprechend dem Typ der Legitimation, sofern erforderlich, die Nutzungsrechte geändert (Abbuchung bei Punktekarten, Wahltageskarten (5 aus 15); keine Veränderung bei Tageskarten; usw.). Das SiZuM gibt die Karte zurück und öffnet die Barriere zur Beförderungseinrichtung.

Kann das SiZuM beim Einlegen der Legitimationskarte diese identifizieren und lesen, so werden zunächst alle Daten gelesen. Das Ereignis wird registriert und protokolliert, entsprechend den Vorgängen bei der Diensterbringung eines Moduls. Alle weiteren Vorgänge werden ebenfalls protokolliert. Wird die Barriere geöffnet, so gilt der Transportdienst für das SiZuM als erbracht. Aufgrund des entsprechenden Vertrages, der die Nutzung des Transportdienstes begründet, wird mit dem Vertragspartner über die erbrachte Leistung abgerechnet.

4.5 Spezielle Sicherheitsmechanismen

Wie bereits in der Systemanalyse erwähnt, stellt die Herausgabe von sicherheitstechnisch bedeutsamen Daten aus dem System in Form von Legitimationskarten ein sicherheitstechnisches Problem dar. Je nach Kartentyp, Datenübertragungsmethode und Art der auf der Karte gespeicherten Daten können unrechtmäßige Legitimationskarten mehr oder minder leicht erstellt und unerlaubt benutzt werden. Auch die aufwendigsten Prozeßsteuerungs- und -kontrollsysteme bei Kartenherstellung und Vertrieb können eine Kartenfälschung nicht verhindern. Prinzipiell ist es nicht möglich, in einem System einzelne Karten mit genau denselben Merkmalen voneinander zu unterscheiden. Man kann allerdings feststellen, wenn zwei oder mehr solcher identischer Legitimationskarten im System benutzt werden.

4.5.1 Aktive Subjektverfolgung

Ziel der aktiven Subjektverfolgung ist es, jeden Kartenmißbrauch durch Subjekte zu verhindern. Dafür ist es erforderlich, daß sowohl die Identität und die Berechtigung des Subjektes geprüft als auch die korrekte Zuordnung der Karte zum Subjekt sichergestellt werden. Die aktive Subjektverfolgung ist ein Verfahren, das in Hochsicherheitssystemen bzw. -bereichen zur online-Validierung von Legitimationskarten verwendet wird, wie sie beispielsweise von Banken oder bei besonders sensiblen Forschungs- und Entwicklungseinrichtungen benötigt werden. Voraussetzung für dieses Verfahren ist, daß alle einbezogenen Zugangskontrolleinrichtungen miteinander vernetzt sind und jederzeit miteinander kommunizieren können.

Das Wirkungsprinzip besteht in der Voranmeldung des Subjekts und der laufenden Veränderung der Daten auf der Karte. Die Voranmeldung des Subjekts und seiner Legitimationskarte wird an allen Kontrollstationen vorgenommen, die vom Subjekt von der zuletzt besuchten Kontrollstation aus direkt erreicht werden können. Wird eine dieser Kontrollstationen vom Subjekt passiert, so werden zum einen die Daten auf der Legitimationskarte verändert; zum anderen werden alle zuvor benachrichtigten, aber nicht besuchten Kontrollstationen verständigt, die nun ihrerseits die ihnen vorliegende Anmeldung auflösen. Gleichzeitig meldet die passierte Kontrollstation das Subjekt

nun bei allen Kontrollstationen an, die von ihr aus direkt erreichbar sind. Der zuvor beschriebene Vorgang wiederholt sich.

Wird ein Sicherheitsbereich von einem Subjekt mit seiner Legitimationskarte betreten, so erhält es eine Aufenthaltskennummer, die im System gespeichert und auf die Karte geschrieben wird. Jede Anmeldung, die von Zugangskontollstationen generiert und an die entsprechenden anderen Zugangskontrolleinrichtungen versendet wird, besitzt eine systemweit eineindeutige Identifikation. Die Anmeldung besteht aus:

- Aufenthaltsnummer
- Legitimationskartennummer
- Subjektidentität
- maximale Lebenszeit der Anmeldung
- Optionen zur Validierung beim Passieren
- andere benötigte Daten

Beim Verlassen des Sicherheitsbereichs wird die Aufenthaltskennung inaktiv erklärt und kann nicht wieder verwendet werden. Sie verbleibt jedoch bis zum nächsten Eintritt des Subjekts in den Sicherheitsbereich auf der Karte. Stellt eine Zugangskontrolleinheit fest, daß ein nicht korrekt angemeldetes Subjekt versucht, Zutritt zu erhalten, wird das Sicherheitsmanagement alarmiert.

Ein Vorteil der aktiven Subjektverfolgung ist, daß sie keine Historie für ihren Algorithmus benötigt. Dies kann aus datenschutzrechtlichen Gründen von Interesse sein.

4.5.2 Passive Subjektverfolgung

Die passive Subjektverfolgung kann einen Kompromiß zwischen erreichbarem Sicherheitsniveau und verfügbarer Infrastruktur erreichen. Können die hohen Ansprüche, die die aktive Subjektverfolgung an die Infrastruktur stellt, aus technischen Gründen nicht befriedigt werden, so ist nur die passive Subjektverfolgung in der Lage, eine größere Anzahl "gleicher" Legitimationskarten im System online zu erkennnen und zu sperren. Prinzipiell kann sie jedoch auch jeden einzelnen Mißbrauch aufdecken, wobei jedoch der technische Aufwand im Vergleich zur aktiven Subjektverfolgung überproportional steigt.

Betreiber von Skiliften benötigen beispielsweise ein Kartenvalidierungssystem, das in der Lage ist, Karten auch an solchen Kontrollstationen zu validieren, die nicht vernetzt sind. Ihr Bemühen richtet sich weniger auf die individuelle Kontrolle der einzelnen Person, sondern vielmehr darauf, Fälschungen relativ teurer Skipässe "im großen Stil" uninteressant zu machen.

Die passive Subjektverfolgung arbeitet mit einer Historie, die in den Kontrollstationen und auf den Legitimationskarten gespeichert wird. Neben der eigentlichen Kartennummer besitzt jede Karte eine sogenannte Freischaltungskennzahl. Jedesmal, wenn mit einer Karte ein Transportdienst angefordert wird, vergleicht die Kontrollstation die Freischaltungskennzahl und Historie auf der Karte mit den von ihr gespeicherten Kartendaten.

Ist die Kartenfreischaltungskennzahl aktueller als die, die gespeichert ist, übernimmt die Kontrollstation diese Zahl sowie die auf der Karte gespeicherte Historie und aktualisiert die Kartenhistorie mit den Daten der Kartenpassierereignisse.

Entspricht die Kartenfreischaltungskennzahl derjenigen, die in der Kontrollstation gespeicherten ist, überprüft die Kontrollstation die von ihr gespeicherte Historie mit derjenigen auf der Karte. Erscheinen die Ereignisse der Historien plausibel, wird die Historie auf der Karte übernommen und entsprechend dem vorherigen Fall erweitert. Anschließend überprüft die Kontrollstation die Nutzungsberechtigung und gewährt oder verweigert die Nutzung des Transportsystems. Sind die Ereignisse der Historien nicht plausibel, wird die Karte in den Zustand "ausgesetzt" überführt und kann nur durch eine authorisierte Person des Liftbetreibers freigeschaltet werden. Die Freischaltung erfolgt mit der Aktualisierung der Kartenfreischaltungskennzahl auf der Karte.

Bei einer Kartenfreischaltungskennzahl, die älter ist als die lokal von der Kontrollstation gespeicherte, wird die Karte in den Zustand "ausgesetzt" überführt und von der Kontrollstation eingezogen.

Ist eine Dienstperiode beendet (nach einem Skitag), werden alle aktuellen Kartenfreischaltungskennzahlen an die Kontrollstationen verteilt.

Je größer die Anzahl der auf der Karte gespeicherten Ereignisse der Historie ist, und je häufiger dieselben Kontrollstation aufgesucht werden, desto höher wird die Güte der Kartenvalidierung sein. Es gilt, für die jeweiligen Skigebiete eine sinnvolle Historienlänge festzulegen.

Kapitel 5

Anmerkungen und Ausblicke

Die aufgezeigte Konzeption der Module und ihrer Gemeinden verwendet in der gegebenen Darstellung recht komplexe Techniken, um die Zielsetzung eines sich selbst optimierenden Systems zu verwirklichen. Damit sollen die in der Zukunft denkbaren Anforderungen und technologischen Optionen zu erfüllen sein, die von einem verteilten und hoch integrierten System gefordert werden. Es wird in der Lage sein, im Sinne einer Eigendynamik eine ständige Weiterentwicklung bestehender Strukturen zu ermöglichen. Prozessoren und andere Hardwareressourcen werden in einem bisher nicht gekannten Maß genutzt werden können, um ein wesentlich höheres Leistungspotential bereitzustellen. Mit der Möglichkeit, individuelle Sicherheitsstrategien umzusetzen, wird auch die Ausfallsicherheit der Teilsysteme eines solchen Großsystems erheblich gesteigert werden. Verfügen die Einheiten der ADE über ausgereifte Mechanismen der Wissensrepräsentanz und -anwendung, könnten solche Großsysteme eine frühe Vorstufe von Informationsagenten bilden, wie sie in [PLS92] und [BJP94] dargestellt sind.

Gleichzeitig kann aufgrund der elementaren und erprobten Funktionsmechanismen des Moduls, wie im Betriebssystembau und in der Kommunikationstechnik bereits verwendet, eine einfache Version von Modulen und deren Modulgemeinde verwirklicht werden, die in der Lage ist, die in der Systembegründung dargelegten kurz- und mittelfristigen Ziele des neuen SIPORT Systems zu verwirklichen. Insbesondere kann eine leistungsstarke Infrastruktur aufgebaut werden, die aufgrund ihres internen Verrechnungswesens den Anforderungen eines DNB-Systems in gleicher Weise gerecht werden kann wie denen eines Hochsicherheitssystems, dessen Bewertbarkeit in der Abbildung und Durchsetzung einer Sicherheitspolitik fußt. Dazu zählt die Unantastbarkeit der einzelnen Systemkomponenten untereinander und die gestattete Transparenz der Vorgänge im System für vertraute Instanzen genauso wie die Ausfallsicherheit. Die Hauptvorteile der Konzeption des neuen SIPORT Zugangskontrollsystems sind:

- Einfachheit der elementaren Funktionsmechanismen eines Moduls
- schnelle Implementierbarkeit bei Einsatz von Standardbasiskomponenten und Kryptotoolboxen (z.B. SELANE)
- Multiplattformfähigkeit
- modulare Erweiterbarkeit
- Integrierbarkeit fremder Subsysteme

- Wiederverwendbarkeit vorhandener Funktionalität im System
- Aufbau und Unterstützung beliebig komplexer Gesamtsystemstrukturen
- Überprüfbarkeit und Wartbarkeit der Teilsysteme
- Ausfallsicherheit durch:
  - Verteilbarkeit der Subsysteme auf verschiedene Systemressourcen
  - weitgehend autonome Subsysteme
  - Selbstkontroll- und Protokollmechanismen
- konfigurierbare und verifizierbare Systemsicherheit durch:
  - Abbildung und Durchsetzung unterschiedlich komplexer Sicherheitspolitiken
  - Vollständige Abschottung einzelner Gruppen von Teilsystemen des Gesamtsystems, sowohl statisch als auch dynamisch
  - Zugangskontrollsysteme: Teilsysteme mit heterogenen Sicherheitsbereichen
  - Abgeschlossenheit der Teilsysteme
  - Einrichtung eines zentralen oder eines verteilten Sicherheitssubsystems
- freie Leistungsskalierbarkeit:
  - Einsatz heterogener Rechnerplattformen
  - Einsatz spezieller Baugruppen (Kryptoboards, Grafikboards, usw.)
  - Einsatz fremder, autonomer Subsysteme
  - dynamische und statische Ressourcenzuteilung
- zukünftige Ausbaufähigkeit hin zu hoch integrierten Gesamtsystemen, die
  - sich selbst optimieren,
  - selbständig komplexe Situationen behandeln können,
  - die lernfähig sind und eine Eigendynamik entwickeln.

Die Qualität der Sicherheit des Modulkonzeptes steht und fällt mit der Güte, die in Bezug auf die Abgeschlossenheit der einzelnen Module sowie die Schutzmechanismen der Modulgemeinden erreicht wird. Der Einsatz moderner Kryptomechanismen ist daher unerläßlich.

Anhang A

Begriffsdefinitionen

Die hier angegebenen Begriffsbestimmungen setzen sich aus allgemein gebräuchlichen und einigen in der Arbeit definierten Begriffen zusammen. Die speziellen Begriffe sind hier mit einem Ausrufungszeichen versehen und werden in der Systemanalyse oder Systemkonzeption näher definiert.

Accountability: Ist die Systemeigenschaft, Aktionen den sie initiierenden Instanzen eindeutig zuordnen zu können.

Aktive Bedrohungen (active threats): Bedrohungen bezogen auf absichtliche, unautorisierte Änderungen des Systemzustandes, wie Löschen oder Duplizieren von Nachrichten.

Aktive Mitglieder !: Durch Erteilung einer Sicherheitseinstufung werden aus passiven aktive Mitgliedern.

Alarmdaten: Informationen über Ereignisse, die gegen Regeln der Sicherheitspolitik verstoßen, sowie manuell eingegebenen Informationen für den direkten Hilferuf von Personen.

API (Application Programming Interface): Schnittstelle für die Anwendungsprogrammierung, welche den Softwareprogrammierern Routinen für die Entwicklung einer Anwendung zur Verfügung stellt.

Authentifikation: Nachweis der Echtheit der angegebenen Identifikation eines Benutzers oder Prozesses. In der Literatur wird der Begriff "Authentifikation" zusätzlich mit der Bedeutung des Begriffs "Datenintegrität" verwendet.

Authentifikationsinformationen: Daten, wie z.B. Paßworte oder krypthographische Schlüssel, die zur Authentifikation benutzt werden.

Autorisierung (authorization): Rechteerteilung auf Subjekte (z.B. Benutzer oder Instanzen) bezüglich der Benutzung von Objekten (wie Rechner oder Dateien) auf der Grundlage der festgelegten Sicherheitspolitik. Dazu zählt auch die Erteilung von Rech-

ten, die regelorientiert aufgrund des Besitzes von speziellen Token oder aufgrund der Zugehörigkeit zu Sicherheitsklassen bei Verwendung entsprechender Sicherheitsmodelle gewährt werden.

Ausgeschlossene Mitglieder !: Aktive Mitglieder, die keine Legitimation besitzen.

Barrieren: (z.B. Tor, Tür, Drehkreuz, Schranke, ...) Dienen der Verriegelung von Durchgängen, um ein unkontrolliertes Wechseln in und aus Raumzonen zu verhindern. Die Barrieren werden mittels der Stellglieder bei einem positiven Entscheid des Zugangskontrollsystems angesteuert.

Baugruppe !: Eine Baugruppe ist eine Anordnung von physikalisch fixierten elektronischen, elektrischen oder mechanischen Bauelementen, die durch ihre Anordnung eine Funktionalität erbringt.

Biometrie: Ist die Wissenschaft von der Zählung und Messung an Lebewesen. In der Computersicherheit werden ihre Methoden eingesetzt, um eindeutig quantifizierbare physiologische, morphologische oder verhaltenstypische Merkmale zu gewinnen und diese derart darzustellen, daß sie zur positiven Identifikation von Personen verwendet werden können. Beispiele solcher Merkmale sind Fingerabdrücke, Netzhautmuster, Unterschriften.

Datenintegrität (data integrity): Eigenschaft der Überprüfbarkeit der Korrektheit und Vollständigkeit von Daten.

Datenschutz: Das Recht von Individuen zu bestimmen, von wem über sie Informationen gesammelt und an wen sie weitergegeben werden dürfen.

DBMS, Database Management System (Datenbank-Managementsystem): Ist ein Programmsystem, das Dienstfunktionen zum Entgegennehmen, Abspeichern, Ändern, Löschen, Wiederauffinden und Bereitstellen von Daten in oder aus seinen Datenbeständen sowie die Verwaltung seiner Datenbestände umfaßt.

DDL, Data Definition Language (Datendefinitionssprache): Sprache, mit der ein Datenbankschema für eine Datenbasis definiert werden kann.

Detektoren/Sensoren: Dienen der technischen Überwachung der Barrieren und Stellglieder, um deren Zustand (geöffnet, geschlossen, Aufbruch, Manipulation, Personen in der Vereinzelungsanlage) an eine angeschlossene Auswerteeinheit weiterzuleiten.

Dienst !: Ein Dienst ist eine Funktionalität, die durch ein Modul erbracht wird. Die Komplexität eines Dienstes kann von einfachen Berechnungen bis hin zu komplexen Anwendungen reichen, wie Simulationen, komplizierte Regelungsanwendungen, usw.

Dienstanforderung !: Ist die durch einen Vertrag begründete und legitimierte Anforderung eines Dienstes von einem Dienstnehmer an einen Diensterbringer bzw. Dienst-

geber.

Dienstnachfrage !: Spezifikation von Eigenschaften eines Dienstes, die von einem Modul zu anderen Modulen verschickt wird. Die anderen Module werten diese Spezifikation aus und antworten entsprechend ihrer Dienste mit einem Dienstnutzungsangebot.

Dienstnutzungsangebot !: Antwort eines Moduls auf eine Dienstnachfrage eines anderen Moduls. Durch die Abgabe eines Dienstnutzungsangebots erklärt ein Modul (Dienstanbieter) seine Bereitschaft, mit einem anderen Modul (Dienstnachfrager) in Verhandlungen über Dienstnutzungsrechte zu treten, deren Eigenschaften in der Dienstnachfrage festgelegt sind. Entsprechend den Spezifikationen in der Dienstnachfrage gibt der Dienstanbieter im Dienstnutzungsangebot die Eigenschaften und Nutzungsoptionen der infragekommenden Dienste an.

Dienstskelett !: Ein Dienstskelett ist eine modulinterne Beschreibung eines Dienstes, die alle Daten umfaßt, um den Dienst anbieten und durchführen zu können.

Dienstzugangspunkt: Ort, an dem Dienste einer Instanz zur Verfügung gestellt bzw. auf Anforderung erbracht werden.

Dienstzugangspunktadresse: Die einem Dienstzugangspunkt zugeordnete Identifikation.

Digitale Unterschrift (digital signature): An eine Dateneinheit angefügte, spezielle Daten oder die kryptographische Transformation dieser Dateneinheit enthaltende Prüfsumme. Diese liefert sowohl dem Empfänger den Nachweis, daß die Dateneinheit korrekt und vollständig und vom unterschreibenden Sender abgeschickt worden ist; auch schützt es den Sender davor, daß der Empfänger nicht-nachweisbare absichtliche Datenmanipulationen vornehmen kann.

Discretionary Access Control (DAC): Zugriffssteuerungsverfahren, bei welchem die Vergabe der Rechte dem einzelnen Eigentümer des Objekts überlassen bleibt, und nicht — wie beim MAC — durch ein zentrales Regelwerk bestimmt ist. POSIX Impelementationen des DAC arbeiten mit sogenannten Zugriffskontrollisten (ACL), die eine feine Granularität bei der Vergabe von Zugriffsrechten unterstützen. Zugriffsrechte können individuell an einzelne Benutzer oder Benutzergruppen vergeben werden.

DML, Data Manipulation Language (Datenmanipulationssprache): Sprache, die Operatoren zum Umgang mit Daten einer Datenbasis bereitstellt.

Ethernet: Ist eine Netzwerkarchitektur, die auf elektrischen Leitern als Übertragungsmedien beruht. Dies können Adernpaar- (10Base-T) oder Koaxialkabel sein. Der Zugriffsmechanismus der Knoten auf das Netz wird als *Carrier Sense Multiple Access* with *Collision Detect* (CSMA/CD) bezeichnet.

FDDI (Fiber Distribution Data Interface): Token-Ring Netzwerkarchitektur, die auf Lichtwellenübertragung mit einer Wellenlänge von 1300 nm durch Glasfasermedien basiert. Es ist charakterisiert durch eine 100 Mbps Übertragungsrate mit einer maximalen Netzwerkausdehnung von 200 km Länge, wobei mindestens alle 2 km ein Repeater benötigt wird.

Flußkontrolle: Eine Funktion, die den Datenfluß innerhalb einer Schicht oder zwischen benachbarten Schichten kontrolliert.

Knoten: Ist ein System, das an ein Netzwerk angeschlossen ist.

Kryptosystem: System zur Ver- und Entschlüsselung von Daten. Es kann hardware- oder softwaremäßig realisiert sein.

Legitimation !: Ist eine Nutzungsrechterepräsentanz und ein Authentifikationsmittel sowohl für die Benutzer des Systems als auch für die Komponenten des Systems selbst. Komponenten sind Rechnersysteme, Netzwerke, autonome Teilsysteme und Dienstleistungen.

Mandatory Access Control (MAC): Zugriffskontrollsteuerungsverfahren, das mit festgelegten Regeln den Zugriff von Subjekten auf Objekte festlegt. Die Zugriffskontrolle erfolgt aus Subjekt- und Objektsicht. Die Vergabe der Zugriffsrechte obliegt nicht den einzelnen Benutzern: dieses 'Mandat' steht nur dem System zu. Dadurch wird verhindert, daß Informationen an unberechtigte Benutzer weitergegeben werden. Bei der MAC werden Attribute (MAC Labels oder security label) für Subjekte und Objekte verwendet, deren Bedeutung und gegenseitige Zugriffsrelationen durch ein Regelwerk (Teil der Sicherheitspolitik) festgelegt sind, das für alle im System befindlichen Subjekte und Objekte verbindlich ist.

Manipulationserkennung: Die Erkennung von Verletzungen der Datenintegrität oder der Verbindungsintegrität. Die Verbindungsintegrität bezieht sich nicht nur auf einzelne Nachrichten, sondern auch auf deren Reihenfolge während der Lebenszeit einer verbindungsorientierten Kommunikation.

Middleware: Einrichtungen zur Programmentwicklung auf nicht kompatiblen Rechnern, z. B. Emulatoren, Simulationsprogramme.

Mitglieder !: Unter Mitgliedern versteht man alle Subjekte und Objekte eines Zugangskontrollsystems. Siehe auch aktive sowie passive Mitglieder.

Modul !: Ein Modul ist ein Softwaresystem, das eine eigene Systemidentität besitzt und im Rahmen seiner Handlungsvorgaben (Strategie) mit anderen Modulen Nutzungsvereinbarungen (Verträge) schließt, die die Nutzung von Diensten festlegen. Der Diensterbringer ist entweder das Modul oder sein Vertragspartner. Zur Erbringung der Dienste des Moduls kommen Dienste anderer Module und/oder Programmcodes zum Einsatz, die sich im Besitz des Moduls befinden.

Modulgemeinde !: Eine Gemeinschaft von mindestens zwei Modulen, die durch spezielle Mechanismen und Regeln ihre Mitglieder kapselt und ihnen eine wohldefinierte und integre Arbeitsumgebung bereitstellt, heißt Modulgemeinde.

Modulgemeinderegeln !: Modulgemeinderegeln legen alle für eine Modulgemeinde relevanten Eigenschaften und Standards fest. Sie beschreiben das gegenseitige Verhalten von Modulgemeindemitgliedern untereinander, den Umgang mit Gemeinderessourcen, eine Gemeindesicherheitspolitik sowie verbindliche und unverbindliche Festlegungen und Standards der Modulgemeinde.

Objekt: Passive Entität, die Informationen enthält oder empfängt. Der Zugriff auf ein Objekt impliziert potentiell den Zugriff auf die Information, die es enthält. Beispiele für ein Objekt sind: Rekords, Blöcke, Seiten, Segmente, Dateien, Verzeichnisse, Videoanzeigen, Tastaturen, Uhren, Drucker, uws.

ODBC, Open Database Connectivity: Ein Treiber-Manager und ein Satz von ODBC-Treibern, mit deren Hilfe Anwendungen unter Benutzung von SQL als Standardsprache auf Daten zugreifen können.

ODBC-Treiber: Eine DLL (Dynamic-Link Library), mit der eine ODBC-fähige Anwendung Zugriff auf eine Datenquelle erhalten kann. (Jedes Datenbank-Managementsystem, wie z.B. ein SQL-Server, erfordert einen solchen Treiber.)

Partnerinstanzenauthentifikation (peer entity authentication): Die einseitige oder gegenseitige Authentifikation einer oder beider in der Kommunikation involvierten Partnerinstanzen.

Passive Bedrohungen (passive threats): Bedrohungen im Sinne unautorisierter Gewinnung von Informationen über den Systemzustand (z.B. Nachrichteninhalte), bei denen aber keine Änderungen des Systemzustands auftritt.

Passive Mitglieder !: Personen oder Systemkomponenten, die vom System registriert worden sind.

Paßwort: Vertrauliche Authentifikationsinformation, die in der Regel aus Zeichenketten besteht.

Peristenz: Nimmt bei Fehlverhalten von Operationen auf eine Datenbasis diese einen konsistenten Zustand an, der die Ergebnisse aller bis zu einem vorgegebenen Zeitpunkt erbrachter Dienstleistungen wiederspiegelt, so spricht man von Peristenz dieser Zustände.

Physikalische Sicherheit: Maßnahmen zum physikalischen Schutz von Betriebsmitteln gegen absichtliche und versehentliche Bedrohungen, wie z.B. unautorisierte Benutzung oder Zerstörung von Ressourcen.

Point of Sale Terminal: Zertifiziertes Gerät mit definierter Schnittstelle, das Kredit- und Eurocheckkarten mit Hilfe einer Telefonverbindung zu einem Bankrechner validiert, den Rechnungsbetrag von diesen Karten abbucht und dem Verkäufer gutschreibt.

Pool: Im Sinne von Skipool gebraucht: Ist eine Gemeinschaft von Bergbahn- und Skiliftgesellschaften, die Karten und Pässe zur Nutzung der Transporteinrichtungen herausgibt und die dabei entstehenden Verwaltungsaufgaben wahrnimmt.

Port !: Ein Port ist eine Ansammlung von Datenpuffern, der durch eine modulweit eindeutige Nummer identifiziert werden kann. Er dient zum Transport von Daten zwischen Programmen und Diensten eines oder mehrerer Module. Auf die Datenpuffer eines Ports kann lesend oder schreibend zugegriffen werden. Vor und/oder nach dem Zugriff werden je nach Konfiguration des Ports Programmcodes gestartet.

Raumzone: Teilbereiche eines Sicherungsbereichs, die aus einem oder mehreren Räumen mit einem oder mehreren Durchgängen bestehen. Die Summe der von einem Zutrittskontrollsystem überwachten Raumzonen bildet den Sicherungsbereich

Rechnersystem !: Digitalrechner mit einem eingerichteten Betriebssystem, welches ausführbaren Programmen die Hardwarekomponenten und Baugruppen des Rechners sowie angeschlossene Peripheriegeräte zur Verfügung stellt.

Regelorientierte Sicherheitspolitik: Eine auf globalen Regeln basierende Sicherheitspolitik in bezug auf Objekte, die Sensitivitä tsklassen zugeordnet werden, und auf Subjekte, die entsprechende Sicherheitsattribute besitzen und den globalen Regeln gehorchen.

Routing: Funktion innerhalb einer Instanz, in der Regel in der Netzwerkschicht, die den Namen oder die Dienstzugangspunktadresse einer empfangenden Instanz in einen Pfad umsetzt, über den diese Instanz erreicht werden kann.

Schlüssel (key): Bitsequenz, die die Verschlüsselungs- und Entschlüsselungsoperation kontrolliert.

Schlüsselmanagement: Generierung, Speicherung, Verteilung, Löschung, Archivierung und Verwendung von Schlüsseln gemäß der Sicherheitspolitik.

Sensitivität: Beschreibungscharakteristika für ein Betriebsmittel. Wert und Wichtigkeit der Charakteristika werden gemäß einer Sicherheitspolitik angegeben; sie bestimmen ebenfalls Grad und Umfang der Sicherheitsmaßnahmen zum Schutz des Betriebsmittels.

Sicherheitsbereich !: Gruppierung einer oder mehrerer Raumzonen, die eigene Sicherheitseinstufungen besitzen. Weisen die beteiligten Raumzonen alle die gleiche Sicherheitseinstufung auf, so wird dieser Bereich als homogener Sicherheitsbereich be-

zeichnet.

Sicherheitsdienst (security mechanism): Ein Dienst (z.B. Partnerinstanzenauthentifikation) zur Erbringung einer sicherheitsbezogenen Dienstleistung.

Sicherheitsmechanismus: Ein Mechanismus wie z.B. Verschlüsselung zu Realisierung eines Sicherheitsdienstes oder eines Bestandteils hiervon oder von Sicherheitselementen mehrerer Sicherheitsdienste.

Sicherheitspolitik: Eine Menge von (z.B. unternehmens-, benutzerspezifischer oder anwendungsbezogener) Kriterien, nach denen die Sicherheitsdienste in ihrem Umfang und ihrer Zusammensetzung zu erbringen sind. Sie können auf Regeln und/oder auf Identitäten und Attributen von Subjekten basieren.

Sicherungsbereich: Abgeschlossenes Objekt (Räume, Gebäude, Bereich, u.ä.) oder ein in sich abgeschlossener Teilbereich eines Objektes, der von einem Zutrittskontrollsystem überwacht wird.

SQL, Structured Query Language: Eine deskriptive Datendefinitions- und -anfragesprache, deren Strukturierungsregeln und Operatoren denen des relationalen Datenmodells entsprechen.

Stellglieder: Elektromechanische Sperrelemente zur Sperrung bzw. Freigabe von Barrieren.

Strategie !: besteht aus Leitlinien und/oder Handlungsvorgaben für ein Modul. Eine Strategie definiert eine Sicherheitspolitik und behandelt den Umgang mit anderen Modulen; sie gibt Bewertungsmaßstäbe und Optimierungsziele der Arbeitsorganisation und Einheiten des Moduls vor und beschreibt Bedingungen und Methoden zur Änderung der Strategie selbst.

Subject Restriction List (SRL): Zugriffssteuerungsverfahren, um aus Sicht der Subjekte Zugriffe auf Objekte zu gewähren oder zu verweigern.

Subjekt: Aktive Entität — im allgemeinen in Form einer Person, eines Prozesses oder Gerätes —, die das Fließen von Informationen zwischen Objekten verursacht oder den Systemzustand ändert.

Trigger: Ist eine Aktion, die aus Anweisungen und/oder dem Aufruf weiterer Aktionen besteht. Sie unterstützt die Durchsetzung der Konsistenzbedingungen einer Datenbasis. Diese Aktionen werden durch definierte Datenmanipulationen der Datenbasis ausgelöst und können ihrerseits Datenmanipulationen der Datenbasis verursachen.

verdeckter Kanal: Ist ein Kommunikationskanal, der es einem Prozeß erlaubt, in einer Weise Informationen zu transferieren, die die Sicherheitspolitik eines Systems verletzt.

Vereinzelungsanlage (VEA): Durchgang, der so ausgeführt ist, daß immer nur ein einzelner berechtigter Benutzer oder eine festgelegte Personenanzahl den Durchgang benutzen kann.

Verfügbarkeit (availability): Die Eigenschaft von Objekten (wie Dienste, Dateien, Rechnernetze) für autorisierte Subjekte verfügbar zu sein.

Verteiltes System: Ein System heißt verteilt, wenn sich seine Komponenten an räumlich getrennten Sellen befinden oder befinden können, hierdurch aber die Funktionalität des Gesamtsystems nicht beeinträchtigt wird.

Vertrag !: Ein Vertrag ist eine Festlegung von Nutzungsbedingungen von Diensten. Er beschreibt für einen Dienst die Nutzungsrechte sowie deren Kosten und Abrechnungsbedingungen, die zwischen den Vertragsparteien (Diensterbringer und Dienstnehmer) ausgehandelt und von jeder Partei akzeptiert wurden.

vertraute Instanz !: Ressourcen oder Module einer Modulgemeinde, die eine besondere Vertrauensstellung genießen, werden als vertraute Instanz bezeichnet.

Zugang: Ist der Zutritt oder die Einleitung der Nutzung eines Informationssystems oder Kommunikationsnetzes.

Zugangsberechtigung: Ist die für ein Identifikationsmerkmal hinterlegte Festlegung wem wann, wie und wo Zugang oder Zutritt gestattet ist.

Zutritt: Vorgang des Überschreitens der Grenze einer Raumzone (Raum, Gebäude, Bereich, Werk, Standort u.ä.)

Zutrittsberechtigung: Ist die für ein Identifikationsmerkmal hinterlegte zeitliche und/oder räumliche Berechtigung, Zutritt zu erhalten.

Zutrittswiederholkontrolle: Sie verhindert, daß innerhalb einer definierbaren Zeit ein Zutritt mit demselben Identifikationsmerkmal mehrfach in eine Richtung erfolgt.

Literaturverzeichnis

[Bau90] Bernd Baumgarten. *Petri-Netze: Grundlagen und Anwendungen.* BI Wissenschaftsverlag, Mannheim - Wien - Zürich, 1990.

[BCN95] T. Beth, J. Calmet, and H. H. Nagel. Forschung und Lehre am IKAS. Technical report, Institut für Algorithmen und Kognitive Systeme Fakultät für Informatik Universität Karlsruhe, 1995. Tätigkeitsbericht anläßlich des zehnjährigen Bestehens 1985-1995.

[Bet95] Thomas Beth. Sichere offene Datennetze. *Spektrum der Wissenschaften*, (5):46–55, mai 1995.

[BJP94] Michael Brodie, Mathias Jarke, and Michael Papazoglou. The information marketplace: Challenge of information commerce. In *Proc. of the 2nd Intl. Conference on Cooperative Information Systems*, pages 147–157, Toronto, Canada, mai 1994.

[BKSW94] Thomas Beth, H. Joachim Knoblauch, Steffen Stempel, and Peer Wichmann. Athentifikationsdienst SELANE Modularisierung und Einsatz. 1994.

[Bla95] Russ Blake. *Optimizing Windows NT.* Volume 4 of *Microsoft Windows NT Resource Kit* [Cor95a], 1995.

[BN95] Ron Ben-Natan. *CORBA: A Guide to Common Object Request Broker Architecture.* McGraw-Hill, New York, NY, 1995.

[Bon95] Pat Bonner. *Network Programming with Windows Sockets.* Prentice Hall PTR, Upper Saddle River, NJ, 1995.

[Boo94] Grady Booch. *Object Oriented Analysis and Design with Applications.* The Benjamin/Cummings Publishing Company, Inc., Redwood City, CA, 2nd edition, 1994.

[Bro95] Kraig Brockschmidt. *Inside OLE.* Microsoft Press, Redmond, WA, 2nd edition, apr 1995.

[Bun95] Bundesamt für Sicherheit in der Informationstechnik. *Anforderungen an Zutrittskontrollanlagen*, Bonn, jan 1995.

[CCC+91] Digital Equipment Corporation, Hewlett-Packard Company, NCR Corporation, Object Design Inc., and SunSoft Inc. *The Common Object Request Broker: Architecture and Specification.* John Wiley & Sons, Inc, New York, Chichester, Brisbane, Toronto, Singapore, 1991.

[Clu93] Helen Cluster. *Inside Windows NT.* Microsoft Press, Redmond, WA, 1993.

[Clu94] Helen Cluster. *Inside the Windows NT File System.* Microsoft Press, Redmond, WA, 1994.

[Com94] Dougles E. Comer. *Internetworking with TCP/IP: Principles, Protocols and Architecture*, volume 1 of *Internetworking with TCP/IP.* Prentice Hall, Englewood Cliffs, NJ, 3rd edition, 1994.

[Cor94] Microsoft Corporation. *Windows ODBC 2.0 Programmer's Reference and SDK Guide for Microsoft Windows and Windows NT.* Microsoft Press, Redmond, WA, 1994.

[Cor95a] Microsoft Corporation. *Microsoft Windows NT Resource Kit.* six volumes. Microsoft Press, Redmond, WA, 1995.

[Cor95b] Microsoft Corporation. *Version 3.51 Update.* Volume 5 of *Microsoft Windows NT Resource Kit* [Cor95a], 1995.

[Cor95c] Microsoft Corporation. *Windows NT Messages.* Volume 3 of *Microsoft Windows NT Resource Kit* [Cor95a], 1995.

[Cor95d] Microsoft Corporation. *Windows NT Networking Guide.* Volume 2 of *Microsoft Windows NT Resource Kit* [Cor95a], 1995.

[Cor95e] Microsoft Corporation. *Windows NT Resource Guide.* Volume 1 of *Microsoft Windows NT Resource Kit* [Cor95a], 1995.

[Cor96a] Microsoft Corporation. *Version 3.51 Update 2.* Volume 6 of *Microsoft Windows NT Resource Kit* [Cor95a], 1996.

[Cor96b] Microsoft Corporation. WISE: Integrating Windows solutions with UNIX and Macintosh. *TechNet*, (1-96), jan 1996.

[Cor96c] Mircosoft Corporation. MS Windows NT from a UNIX point of view. *TechNet*, (1-96), jan 1996.

[CS93a] Dougles E. Comer and David L. Stevens. *Internetworking with TCP/IP.* three volumes. Prentice Hall, Englewood Cliffs, NJ, 1993.

[CS93b] Dougles E. Comer and David L. Stevens. *Internetworking with TCP/IP: Client-Server Programming and Applications BSD Socket Version*, volume 3 of *Internetworking with TCP/IP.* Prentice Hall, Englewood Cliffs, NJ, 1st edition, 1993.

[Dav94] Ralph Davis. *Windows NT Network Programming.* Addison-Wesley Publishing Company, Inc., Wokingham, England, 1994.

[DD94] C. J. Date and Hugh Darwen. *A Guide to the SQL Standard.* Addison-Wesley Publishing Company, Inc., Wokingham, England, 3rd edition, jan 1994.

[Den95] Adam Denning. *OLE Controls Inside Out.* Microsoft Press, Redmond, WA, 1995.

[FFKK93] O. Fries, A. Fritsch, V. Kessler, and B. Klein. *Sicherheitsmechanismen: Bausteine zur Entwicklung sicherer Systeme.* R. Oldenbourg Verlag GmbH, München - Wien, 1993.

[Gal95] Bill O. Gallmeister. *POSIX.4: Programming for the Real World.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, jan 1995.

[Gas88] Morrie Gasser. *Building a Secure Computer System.* Van Nostrand Reinhold, New York, NY, 1988.

[GS88] Chris Gane and Trish Sarson. *Structured System Analysis: Tools and Techniques.* Prentice Hall, Englewood Cliffs, NJ, 1988.

[GS95] Simson Garfinkel and Gene Spafford. *Practical UNIX Security.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, jun 1995.

[HS95] Samuel P. Harbison and Guy L. Steele, Jr. *C, A Reference Manual.* Prentice Hall, Englewood Cliffs, NJ, 4th edition, 1995.

[Hu95] Wei Hu. *DCE Security Programming.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, jul 1995.

[Hun94] Craig Hunt. *TCP/IP Network Administration.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, sep 1994.

[Kri94] Gerald Kristen. *Object Orientation: The Kiss Method.* Addison-Wesley Publishing Company, Inc., Wokingham, England, 1994.

[Kru96] David J. Kruglinski. *Inside Visual C++.* Microsoft Press, Redmond, WA, 3rd edition, 1996.

[Lew94] Donald Lewine. *POSIX Programmer's Guide.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, nov 1994.

[LKK93] Peter C. Lockemann, Gerhard Krüger, and Heiko Krumm. *Telekommunikation und Datenhaltung.* Carl Hanser Verlag, München - Wien, 1993.

[LL95] Stefan M. Lang and Peter C. Lockemann. *Datenbankeinsatz.* Springer-Verlag, Berlin - Heidelberg - New York, 1995.

[Mar96] Bernd Marquardt. Microsoft Visual C++ 4.0. *Microsoft System Journal,* (1):24 – 35, jan 1996.

[MZ95] Thomas J. Mowbray and Ron Zahavi. *The Essential CORBA: Systems Integration using Distributed Objects.* John Wiley & Sons, Inc, New York, Chichester, Brisbane, Toronto, Singapore, 1995.

[NG95] Mark Nelson and Jean-Loup Gailly. *The Data Compression Book.* M&T Books, New York, NY, 2nd edition, 1995.

[Obe96] Andreas Oberweis. *Modellierung und Ausführung von Workflows mit Petri-Netzen.* B. G. Teubner Verlagsgesellschaft, Stuttgart - Leipzig, 1996.

[PLS92] Mike P. Papazoglou, Steven C. Laufman, and Timos K. Sellis. An organizational framework for cooperating intelligent information systems. *International Journal of Intelligent and Cooperative Information Systems*, (1-1):169–202, mar 1992.

[PPP96] Jim Panttaja, Mary Panttaja, and Bruce Prendergast. *The Microsoft SQL Server Survival Guide.* John Wiley & Sons, Inc., New York, Chichester, Brisbane, Toronto, Singapore, 1996.

[RBP+91] James Rumbaugh, Michael Blaha, William Premerlani, Frederick Eddy, and William Lorensen. *Object-Oriented Modelling and Design.* Prentice Hall, Englewood Cliffs, NJ, 1991.

[Rei85] Wolfgang Reisig. *Systementwurf mit Netzen.* Springer Verlag, Berlin - Heidelberg - New York - Tokyo, 1985.

[Rei91] Wolfgang Reisig. *Petrinetze, Eine Einführung.* Springer Verlag, Berlin - Heidelberg - New York - Tokyo, 2. Auflage, 1991.

[RG93] Deborah Russell and G. T. Gangemi, Sr. *Computer Security Basics.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, nov 1993.

[Ric95] Jeffrey Richter. *Advanced Windows: The Developer's Guide to the Win32 API for Windows NT 3.5 and Windows 95.* Microsoft Press, Redmond, WA, 1995.

[RT93] Ward Rosenberry and Jim Teague. *DCE and Windows NT.* O'Reilly & Associates, Inc, Sebastopol, CA, 1st edition, nov 1993.

[SC95] Joc Sanders and Eugene Curran. *Software Quality.* Addison-Wesley Publishing Company, Inc., Wokingham, England, 1995.

[Sch95] Herbert Schildt. *C++ The Complete Reference.* Osborn McGraw-Hill, Berkeley, CA, 2nd edition, 1995.

[Sch96] Bruce Scheiner. *Applied Crypthography: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, Inc, New York - Chichester - Brisbane - Toronto - Singapore, 2nd edition, 1996.

[SHM94] John Shirley, Wei Hu, and David Magid. *Guide to Writing DCE Applications.* O'Reilly & Associates, Inc, Sebastopol, CA, 2nd edition, aug 1994.

[Sin96] Alok K. Sinha. *Network Programming in Windows NT.* Addison-Wesley Publishing Company, Inc., Wokingham, England, 1996.

[SP89] Jennifer Seberry and Josef Pieprzyk. *Cryptography: An Introduction to Computer Security.* Prentice Hall, Englewood Cliffs, NJ, 1989.

[Sta90] Peter H. Starke. *Analyse von Petri-Netz-Modellen.* B. G. Teubner, Stuttgart, 1990.

[Sta94] William Stallings. *SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards.* Addison-Wesley Publishing Company, Reading, MS, apr 1994.

[Tho96] Stephen A. Thomas. *IPng and the TCP/IP Protocols: Implementing the Next Generation Internet.* John Wiley & Sons, Inc, New York - Chichester - Brisbane - Toronto - Singapore, 1996.

[VdL93] Rick F. Van der Lans. *Introduction to SQL.* Addison-Wesley Publishing Company, Inc., Wokingham, England, 2nd edition, jan 1993.

[Whi94] Iseult White. *Rational Rose Essentials: Using the Booch Method.* The Benjamin/Cummings Publishing Company, Inc., Redwood City, CA, 2nd edition, 1994.

[Zor95] Vasilios Zorkadis. *Leistungsanalyse und Optimierung sicherer Rechnernetze.* Verlag Shaker, Aachen, Dissertation, 1995.

Index