Universelles Videomanagementsystem von Accellence Technologies GmbH

Eigenschaften

Impressum

Herausgeber

Gesellschaft:	Accellence Technologies GmbH
Handelsregister:	HRB 110799 Hannover
Geschäftsführer:	Dr. Heinz Stephanblome
Redaktion:	Torsten Heinrich
Tel:	+49 (0)511 277 2400
Fax:	+49 (0)511 277 2499
E-Mail:	info@accellence.de
Internet:	http://www.accellence.de
Anschrift:	Accellence Technologies GmbH Garbsener Landstrasse 10, 30419 Hannover, Deutschland

 Datum: 29.10.2013

Inhaltsverzeichnis

Abkürzungsverzeichnis

ASCII	American Standard Code for Information Interchange
AAC	Advanced Audio Coding
AES	Advanced Encryption Standard
CA	Certificate Authority oder Certification Authority
CCTV	Closed Circuit Television
DB	Datenbank
DCOM	Distributed Component Object Model
DVR	Digital Video Recorder
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
GUI	Graphical User Interface
GOP	Group Of Pictures
HID	Human Interface Device
LDAP	Lightweight Directory Access Protocol
MMI	Man Machine Interface
NAS	Network Attached Storage
NFR	Non-functional Requirement
NTP	Network Time Protocol
NVR	Network Video Recorder
OPC	OLE for Process Control
RFC	Request For Comments
RTSP	RealTime Streaming Protocol
PTZ	Pan Tilt Zoom
PKCS	Public Key Cryptography Standards

PKI	Public-Key-Infrastruktur
SAN	Storage-Area-Network
SAS	Serial Attached SCSI
SDP	Session Description Protocol (see RFC 4566)
SHA	Secure Hash Algorithm
SQL	Structured / Sequential / System Query Language
SRTP	Secure Real-Time Transport Protocol
SSB	Schnittstellenbeschreibung
SSD	Solid-State-Drive
SSL	Secure Sockets Layer
SW	Software
TCP	Transmission Control Protocol
vimacc	Video Management System von Accellence Technologies GmbH
MMS	Übergeordnetes Management System

1 Einleitung

1.1 Zweck des Dokumentes

Das vorliegende Dokument ist ein Teildokument der System Dokumentation für das Produkt **vimacc** der Accellence Technologies GmbH.

vimacc ist eine universelle Videomanagementsoftware zur Übertragung, Anzeige, Auswertung und Archivierung von Video-, Audiodaten und zugehörigen Metadaten sowie zur Steuerung der Video- und Audiotechnik wie z.B. Kameras und Schaltkontakten eines digital vernetzten CCTV-Systems.

Dieses Dokument liefert eine umfassende technische Leistungsbeschreibung der **vimacc** Videomanagementsoftware.

1.2 Aufbau der Dokumentation

Die **vimacc** System Dokumentation besteht aus einer Reihe von Dokumenten, die jeweils einen Teilaspekt behandeln und in sich abgeschlossen sind.

Die folgende Aufstellung beschreibt kurz die zur Verfügung stehenden Dokumente, die in ihrer Gesamtheit die **vimacc** Videomanagementsoftware beschreiben:

- vimacc Systemdokumentation: Einführung
  Dieses Dokument skizziert zunächst die Problemstellung eines heutigen digitalen Videoüberwachungssystems und leitet daraus die Notwendigkeit einer universellen Videomanagementsoftware her. Anschließend gibt es einen Überblick über die allgemeinen Eigenschaften von **vimacc** und zeigt einige sich daraus ergebenen möglichen Einsatzgebiete.

- **vimacc Systemdokumentation: Eigenschaften**
  Dieses Dokument.

- vimacc Systemdokumentation: Architektur
  Dieses Dokument gibt einen detaillierten Einblick in die Architektur von **vimacc** und stellt die zur Verfügung stehenden Software Komponenten und ihre Funktionen vor.

- vimacc Systemdokumentation: Schnittstellen
  Dieses Dokument beschreibt die externen Schnittstellen eines **vimacc** Systems. Über diese Schnittstellen kann ein **vimacc** System in übergeordnete Managementsysteme integriert werden, um beispielsweise

Videostreams abzurufen, Kameraaufschaltungen durchzuführen oder das gesamte **vimacc** Subsystem fernzusteuern.

- vimacc Systemdokumentation: Systemvoraussetzungen
  Dieses Dokument beschreibt die Minimalanforderungen an Hardware und Betriebssystem-Software, die erfüllt sein müssen, damit **vimacc** auf einer Hardware-Komponente installiert werden kann.

- vimacc Systemdokumentation: Systemplanung
  Dieses Dokument beschreibt die besonderen Randbedingungen, die bei der Planung eines modernen und vernetzten Videosystems zu berücksichtigen sind und kann somit einem Systemplaner als Hilfestellung dienen, ein **vimacc** System zu dimensionieren und zu planen.
  Darüber hinaus stellt es die zur Verfügung stehenden Software Editionen und deren Einsatzgebiete vor.

2 Eigenschaften

2.1 Allgemeine Eigenschaften

vimacc bietet Video- und Audiostreaming in höchster Qualität und nutzt Rechnerressourcen optimal aus.

Alle Basisdienste für die **vimacc** Funktionseinheiten *Framework*, *Integration* und *Recording* (→ *vimacc Systemdokumentation: Einführung*) sind plattformunabhängig implementiert, so dass sie auf 64-bit und 32-bit Editionen der Windows und Linux Betriebssysteme lauffähig sind.

Alle Anwendungen mit Benutzerschnittstelle der **vimacc** Software sind auf Standard-PC-Hardware mit den 64-bit und 32-bit Editionen der verschiedenen Windows Betriebssysteme lauffähig (→ *vimacc Systemdokumentation: Installation und Voraussetzungen*).

Alle zentralen **vimacc** Software-Komponenten können redundant betrieben werden, so dass beim Ausfall einer zentralen Komponente die zentralen Dienste ohne Einschränkungen weiter genutzt werden können.

vimacc ist in der Lage, sowohl Audio- als auch Videoquellen zu integrieren. Die digitalen Nutzdaten können unabhängig voneinander aufgezeichnet werden, dauerhaft in einem Ringspeicher oder ereignisgesteuert. Audio- und Videodaten können unabhängig voneinander, oder einander zugeordnet und synchron wiedergegeben werden.

vimacc erhöht für die Videoausgabe die Latenzzeit der Gesamtübertragungsstrecke (Streamübernahme von der integrierten Hardware bis zur Bildausgabe) um im Mittel nicht mehr als 80 Millisekunden.

Alle Aufschaltzeiten für Streaming-Verbindungen von den Audio- und Videoquellen oder von den Aufzeichnungsservern sind im Mittel kleiner als 500 Millisekunden, sofern dies die herstellerspezifischen Audio- und Videoquellen ermöglichen.
Bei großen Intraframe-Abständen in interframe-kodierten Videostreams wird zur Reduzierung der Aufschaltzeit bei der Aufschaltung explizit ein Intraframe angefordert, sofern die Videoquelle diese Funktion unterstützt.

Bei Stromausfall bzw. nach Stromwiederkehr stellt **vimacc** sicher, dass das System alle Verbindungen automatisch wieder herstellt und den Anlagenstatus aktualisiert.

vimacc unterstützt für die Videostream-Übertragung, die Livebildanzeige, die Aufzeichnung und deren Wiedergabe die Videostandards H.264, MPEG-4, MPEG-2 und MJPEG.
vimacc unterstützt momentan die Audio-Codecs G.711 und AAC (Advanced Audio Coding).

2.2 Livestream Übertragung

Mit **vimacc** können Livestreams von Videoquellen unterschiedlicher Hersteller über LAN- und/oder über WAN-Verbindungen aufgeschaltet und über die Bedienoberfläche auf einem **vimacc**-Arbeitsplatz, einem Videomonitor oder einer Großbildanzeige dargestellt werden.

vimacc ist in der Lage, unterschiedliche Standard-Audio- und Videoformate an seinen Schnittstellen zu übernehmen, intern zu speichern und erneut zur Wiedergabe bereitzustellen.

Mit **vimacc** können ebenso analoge Videokomponenten (Videokameras und Videomonitore) miteinander verschaltet werden. Hierzu kann **vimacc** analoge Koppelfelder mittels der entsprechenden Kontrollschnittstellen (z.B. via RS 485) steuern und die entsprechenden Endpunkte miteinander verbinden (→ Beispiele in *vimacc Systemdokumentation: Einführung*).

Derartige Aufschaltungen einer Kamera in einer Zentrale können entweder manuell durch Anklicken des entsprechenden Symbols auf einer Bedienoberfläche, ereignisgesteuert durch ein übergeordnetes Alarm-, Gefahren- oder Gebäudemanagementsystem oder automatisch nach einem vorher festgelegten Zeitplan erfolgen.

Für die Auswahl der Streaming-Quellen wird in der Bedienoberfläche des **vimacc** Arbeitsplatzes ein Auswahlbaum angezeigt, so dass der Benutzer ihm zugewiesene und freigeschaltete Datenquellen wählen und aufschalten kann. Die Anordnung der Datenquellen im Auswahlbaum entspricht einer konfigurierbaren hierarchischen Struktur. Diese Anordnung kann von den Administratoren des Systems jederzeit geändert werden.
Mit der freien Anordnung der Datenquellen im Auswahlbaum ist eine Zusammenfassung entsprechend verschiedener Ansichten möglich, wie z.B. eine Ansicht der geografischen Struktur, so dass Elemente nach Räumen, Gebäuden, Liegenschaften geordnet werden können, oder eine Ansicht entsprechend der technischen Topologie, so dass z.B. Elemente aktiven Netzwerkkomponenten zugeordnet werden können.

Um den Netzwerk-Ressourcenbedarf zu begrenzen, werden die Videodaten nur einmal von einer Videokamera abgerufen um sie live (ggfs. auch auf mehreren Monitoren) darzustellen und ebenso bedarfsgesteuert parallel aufzuzeichnen (siehe Kapitel 2.3).

Für die Datenübertragung von den Videoquellen zu den entsprechenden Empfängern können unterschiedliche Netzwerkprotokolle verwendet werden. Hier können wahlweise UDP-Multicast, UDP-Unicast oder TCP-Verbindungen genutzt werden.

vimacc unterstützt eine Vielzahl von möglichen Bildauflösungen und Bildformaten, wie etwa CIF, 4CIF, PAL, NTSC, usw.

2.2.1 Steuerung von PTZ-Kameras

vimacc ist in der Lage, PTZ Kameras (Schwenk-, Neige-, Zoom-Kameras) von verschiedenen Herstellern über die entsprechenden Kontrollschnittstellen zu steuern. Hierbei können sowohl digitale Netzwerkkameras als auch analoge Videokameras gesteuert werden.

Bei entsprechender Berechtigung des Benutzers sind am **vimacc** Arbeitsplatz Bedienelemente für das Schwenken, Neigen, Zoomen und Fokussieren der PTZ Kameras verfügbar.
PTZ-Kameras können alternativ auch mit einem am **vimacc** Arbeitsplatz angeschlossenen Drei-Achsen-Joystick gesteuert werden.

Die folgenden PTZ-Funktionen werden von **vimacc** unterstützt:

- Schwenken, Neigen, Zoomen,
- Anfahren von vordefinierten Kamerapositionen (sog. Presets),
- Programmieren von Presets.
- Fokus,
- Iris,
- Vorgabe von verschiedenen Geschwindigkeiten,
- OSD-Menü-Navigation,
- Programmieren von privaten Zonen,
- Mouse-Tracking (Zentrieren des Videobildes um die Position des Mauszeigers).

2.2.2 Aufschaltung von Sequenzen

Unter einer Sequenz wird in diesem Zusammenhang das zeitgesteuerte Aufschalten von einer festgelegten Anzahl von Kameras auf einen Videomonitor verstanden.
Hierbei können vordefinierten Kamerapositionen und auch ganze Szenarien (vgl. Kapitel 2.2.3) programmiert werden.

vimacc ist in der Lage, in jedem einzelnen Videodialog eine separate Sequenz ablaufen zu lassen.

Die Programmierung von Sequenzen kann dabei je nach Rechtevergabe im Gesamtsystem durch den Operator am **vimacc** Arbeitsplatz oder durch einen Administrator erfolgen.

2.2.3 Aufschaltung von Szenarien

Unter einem Szenario wird in diesem Zusammenhang das gleichzeitige Aufschalten von beliebig vielen Kamera auf die verschiedenen Videomonitore des Systems verstanden.

vimacc unterscheidet hier zwischen lokal am Arbeitsplatz konfigurierten und global oder für eine bestimmte Gruppe zentral bereit gestellten Szenarien.
Damit wird eine optimale Unterstützung der Geschäftsprozesse gewährleistet

Durch die sehr geringen Aufschaltzeiten, die mit **vimacc** realisiert sind, ist es damit möglich, viele Live-Verbindungen quasi gleichzeitig zu schalten.

Die Programmierung von Szenarien kann dabei je nach Rechtevergabe im Gesamtsystem durch den Operator am **vimacc** Arbeitsplatz oder durch einen Administrator erfolgen.

2.2.4 Zeitgesteuerte Aufschaltungen

vimacc ist in der Lage, zeitgesteuert konfigurierte Aktionen durchzuführen, so dass nach einem vorgegebenen Zeitplan z.B. Kameras auf bestimmte Monitore/Videodialoge aufgeschaltet werden können.

In einem komplexeren Fall könnte beispielsweise ein virtueller Wächterrundgang realisiert werden, bei dem zeitgesteuert Kameras in einer vorgegebenen Reihenfolge auf einen oder mehrere Monitore aufgeschaltet werden.

2.2.5 Alarmaufschaltungen

vimacc ist in der Lage, Ereignisse bzw. Alarme von verschiedenen Ereignisquellen zu erkennen und selbständig mit konfigurierten Aktionen zu reagieren.
Derartige Ereignisse können beispielsweise sein:

- Ein Notruf wurde ausgelöst
- Ein Schaltkontakt wurde betätigt
- Ein Schaltkontakt an einer Kamera wurde betätigt.
- Ein unbefugter Eingriff an der Bildquelle (Kamera verdreht, Gehäuse geöffnet, Rüttelkontakt, usw.) wurde erkannt.
- Eine Bewegung vor einer Kamera erkannt (Videosensorik) wurde erkannt.
- Es wurde ein Geräusch erkannt
- Eine technische Störung an der Bildquelle (z.B. Kamerasignal ausgefallen, Festplatte voll, u.s.w.) wurde erkannt
- Ein Routineruf zur Überwachung der Funktionsfähigkeit der Ereignisübertragung von der Bildquelle zur Leitstelle wurde ausgelöst.

Jedem Ereignis können dabei bestimmte Aktionen zugeordnet werden, die **vimacc** automatisch nach Erkennung des Ereignisses durchführen kann. Derartige Aktionen können z.B. Aufschaltungen von Videokameras auf bestimmte Videomonitore, das Starten von vorkonfigurierten Sequenzen oder das Versenden einer Email sein.

Darüber hinaus stellt **vimacc** sicher, dass alle erkannten Ereignisse und alle durchgeführten Aktionen vollständig und kontextbezogen protokolliert werden (siehe Kapitel 2.11). Eine kontextbezogene Dokumentation bedeutet in diesem Zusammenhang, dass die zu einem bestimmten Ereignis gehörenden Protokollmeldungen des Systems jederzeit abgerufen werden können, so dass eine lückenlose Verfolgung aller automatisch durchgeführten oder von einem Benutzer initiierten Aktionen möglich ist.

vimacc ist dadurch in der Lage, ein Alarm-Management vollständig innerhalb des **vimacc** Teilsegmentes durchzuführen.

Durch die externen Schnittstellen von **vimacc** (→ *vimacc Systemdokumentation: Schnittstellen*) ist es allerdings auch möglich, die erkannten Ereignisse an übergeordnete Systeme weiterzuleiten und auf entsprechende Steuerkommandos zu warten, um ereignisbezogene Aktionen im **vimacc** System durchzuführen.
Somit ist ein **vimacc** Subsystem auch in einem Verbund mit einem übergeordneten Managementsystem vollständig fernsteuerbar und kann in dessen Alarm-Management eingebunden werden.

2.3 Aufzeichnung und Wiedergabe

2.3.1 Allgemein

Mit **vimacc** können Livestreams von Videoquellen unterschiedlicher Hersteller über LAN- und/oder über WAN-Verbindungen zentral gespeichert und wiedergegeben werden.

Neben Videodaten unterstützt **vimacc** auch die Aufzeichnung und Wiedergabe von Audiodaten. Momentan unterstützt **vimacc** die Audio-Codecs G.711 und AAC (vgl. Kapitel 2.1).

Die Software-Komponente, die die Aufzeichnung und die Wiedergabe von Audio- und Video-Streamingdaten realisiert, wird im Folgenden mit **vimacc** Streaming-Server bezeichnet.
Der von **vimacc** realisierte Streaming-Server ist ein vom Betriebssystem unabhängiger Streaming-Server und erlaubt eine bildquellenunabhängige Aufzeichnung.

Der **vimacc** Streaming-Server zeichnet die Audio-/Videostreams aller Videoquellen in zentralen oder in verteilten Archiven auf. Der Streaming-Server kooperiert mit allen gängigen Massenspeichertechnologien (NAS - Network Attached Storage, SAS – Server Attached Storage, SAN – Storage Area Network, etc.), ist

plattformunabhängig und offen und lässt sich ebenfalls in virtualisierten Umgebungen (Cloud Computing) betreiben (siehe Kapitel 2.8).

Der Streaming-Server kann einfach mit Bildanalysesoftware gekoppelt werden, um auf dem Datenbestand Prozesse zur Analyse des Inhaltes durchzuführen, z.B. zur forensischen Suche oder zur Informationsverdichtung für eine leistungsfähige Objektsuche, wie z.B. für eine Kennzeichensuche.

2.3.2 Aufzeichnung

Die digitalen Video- und Audiodaten der an ein **vimacc** System angeschlossenen Video- bzw. Audioquellen können vom **vimacc** Streaming-Server nach verschiedenen Verfahren aufgezeichnet werden:

- **Linearaufzeichnung**:
  Die Aufzeichnungsdauer wird durch die Kapazität des Datenspeichers begrenzt. Ist die Kapazitätsgrenze erreicht, wird die Aufzeichnung beendet.
- **Ringaufzeichnung**:
  Die Aufzeichnung erfolgt im Ring. Ältere Teile werden nach X Tagen gelöscht, oder wenn die Speicherkapazität erschöpft ist.
- **Voralarmaufzeichnung**:
  Die Aufzeichnung wird X Minuten vorgehalten. Streaming-Daten älter als X-Minuten werden gelöscht. Wird in den Alarmaufzeichnungsmodus gewechselt, werden die X Minuten vorgehaltener Streaming -Daten gespeichert.
- **Alarmaufzeichnung**:
  Die Aufzeichnung erfolgt linear, wird aber nach X Minuten automatisch beendet (Wird verwendet im Zusammenhang mit der Voralarmaufzeichnung).
- **Standby Aufzeichnung**:
  Alle Verbindungen zu redundanten Servern sind Standby geschaltet, der Ring wird mit allen notwendigen Metadaten versorgt, aber es werden keine Streaming-Daten übertragen. Dieser Modus kommt zum Einsatz, wenn ein Server Aufzeichnungskanäle temporär übernimmt um z.B. einen Ausfall eines anderen Servers zu überbrücken.

Die Video-Bildraten (frames per seconds = fps) und die Bildauflösungen für die Aufzeichnung können unabhängig von den Bildraten und Bildauflösungen der Live-Verbindungen (siehe Kapitel 2.2) konfiguriert werden. So ist beispielsweise eine Livestream Übertragung mit 25 Bildern pro Sekunde (fps) und eine Aufzeichnung mit 4 fps möglich, wobei die Umschaltung der Framerate ereignisgesteuert im laufenden Betrieb erfolgen kann.

Die maximale Aufzeichnungsdauer ist ausschließlich abhängig von der Speicherkapazität der eingesetzten Speichersysteme. Die Ausführung des Datenspeichers kann flexibel auf die quantitativen und sicherheitsrelevanten Anforderungen abgestimmt werden. So können z.B. einfache Festplatten, RAID-

Arrays, iSCSI Geräte (Internet Small Computer System Interface) oder NAS Speichersysteme eingesetzt werden.

Die maximale Anzahl gleichzeitig aufzuzeichnender Streams (Audio, Video) ist nur durch die Leistung der eingesetzten Hardware, durch das Netzwerk oder durch Lizenzvorgaben begrenzt.

Audio- und Videodaten werden getrennt voneinander abgespeichert. Auf der Anwendungsebene können von einer Videoquelle stammende Audiodaten der Videoquelle zugeordnet werden, so dass eine gleichzeitige Wiedergabe der zusammengehörenden Daten möglich ist.
Audiodaten können auch völlig unabhängig von einer Videoquelle aufgezeichnet werden, so dass z.B. die Aufzeichnung von Gesprächen über angeschlossene Kommunikationssysteme möglich ist (→ *vimacc Systemdokumentation: Einführung*).

Die Anzahl der in einem Verbund betriebenen **vimacc** Streaming-Server ist nicht begrenzt.

Der Streaming-Server kann aufgezeichnete Streaming-Daten ganz oder teilweise vor dem Löschen bzw. Überschreiben schützen. Dieser Schutz kann jederzeit auch wieder aufgehoben werden.

Der Streaming-Server erlaubt das Löschen ganzer Spuren (die Streaming-Daten einer Streaming-Quelle) oder Spurteilabschnitte.

Der Streaming-Server ist bzgl. der Anbindung von Streaming-Quellen unabhängig vom Kodierungsverfahren und unabhängig vom Hersteller.

Der Streaming-Server kann die Videostreams der angeschlossenen Streaming-Quellen im eingestellten Ursprungsformat unverschlüsselt oder optional verschlüsselt aufzeichnen.

Der Streaming-Server verfügt über eine offene Schnittstelle zur Aufzeichnung von beliebigen Streaming-Daten, so dass zukünftig herstellerunabhängig weitere Streaming-Quellen zur Aufzeichnung angebunden werden können.

Der Streaming-Server kann Auskunft über die aktuelle Lastsituation geben, d.h. über die aktuelle Aufzeichnungs-Streamleistung, die Playback-Streamleistung und Kapazitätsangaben des von ihm verwalteten Datenspeichers.

Ein Streaming-Server kann Stream-Daten anderer Streaming-Server ohne Einschränkung übernehmen, sofern die Kapazität ausreicht. Zusammen mit dem **vimacc**-Framework kann über diese Funktion der Server-Abgleich durchgeführt werden, wenn bei redundanter Aufzeichnung, auf einem der beteiligten Server Daten verloren gegangen sind.

2.3.2.1Daueraufzeichnung

Für jede Audio- und Videoquelle ist die Art der Daueraufzeichnung (linear oder im Ring – siehe Kapitel 2.3.2) getrennt konfigurierbar.

Die Größe der Speicherbereiche für die Daueraufzeichnung ist für jede Videoquelle frei konfigurierbar oder auch ganz abschaltbar.

2.3.2.2Ereignisgesteuerte Alarmaufzeichnung

vimacc ist in der Lage, zur ereignisgesteuerten Alarmaufzeichnung die Triggersignale über systeminterne Events oder über eine offene Schnittstelle von einem übergeordneten Managementsystem zu empfangen. Nach Empfang der entsprechenden Steuerkommandos kann **vimacc** die konfigurierte Aufzeichnungsart der zugehörige Audio- oder Videoquelle aktivieren bzw. wieder beenden.

Für jede Audio- und Videoquelle ist Alarmaufzeichnung getrennt konfigurierbar.

Die Größe der Speicherbereiche für die Alarmaufzeichnung ist für jede Videoquelle frei konfigurierbar.

2.3.2.3Speicherung von Metadaten

Der **vimacc** Streaming-Server ist in der Lage, zusätzlich zu den eigentlichen Streaming-Daten auch Metadaten zu speichern. Darunter werden in diesem Kontext alle Arten von Zusatzinformationen verstanden, die sich auf die Streaming-Daten (wie z.B. die Videobilder) beziehen.

Neben den genauen Zeitinformationen (Timecodes), die auch schon eine Form von Metadaten darstellen, können dem **vimacc** Streaming-Server auch von außen Zusatzinformationen übergeben werden, die zusammen mit den Streaming-Daten gespeichert werden können.

Diese Zusatzinformationen können z.B. Transaktions-Nummern von Bankautomaten und Kassensystemen, Paketnummern von Logistik-Systemen oder Alarm-Identifikationsnummern sein.
Metadaten können aber auch manuell eingegeben werden. So ist z.B. der Benutzer an einem **vimacc** Arbeitsplatz in der Lage, bei der Recherche des aufgezeichneten Materials einer bestimmten Kamera für einen beliebigen Zeitpunkt eine Notiz abzuspeichern, die den beobachteten Vorgang näher beschreibt.

Metadaten können auch über eine der offenen Schnittstellen des **vimacc** Systems von einem übergeordneten Managementsystem übernommen werden, was die Verknüpfung verschiedener Gewerke und der Automatisierung von Arbeitsabläufen erleichtert. So kann z.B. ein Alarm aus einem anderen Untersystem eine ereignisgesteuerte Alarmaufzeichnung im **vimacc** System auslösen und die ebenfalls übergebenen Metadaten können unmittelbar mit abgespeichert werden.

Durch die manuelle oder automatisierte Anreicherung der Streaming-Daten mit Metadaten wird die spätere Suche nach einem bestimmten Inhalt über einen großen Zeitraum erheblich erleichtert. In heutigen Überwachungssystemen sind Ringspeicher aller angeschlossenen Kameras in der Größe von 15 bis 30 Tagen durchaus üblich, was ein Volumen von einigen Terabytes an Videodaten bedeuten kann. Ohne die zusätzlich abgespeicherten Metadaten wäre es ungleich schwieriger, einen bestimmten Vorgang für eine weitere Analyse schnell wiederzufinden.

Systeme zur sogenannten Video-Content-Analyse (VCA) könne eine Quelle darstellen, über die das **vimacc** System automatisiert mit Metainformationen versorgt werden kann. **vimacc** kann einem VCA-System die Streaming-Daten einer Datenquelle zur Analyse übergeben und etwaige Analyseergebnisse übernehmen, um diese dann in Form von Metadaten zusammen mit dem Stream abzuspeichern.

Details, in welcher Form die Metadaten abgespeichert werden, sind in dem Dokument *vimacc Systemdokumentation: Architektur* zu finden.

2.3.3 Wiedergabe von aufgezeichneten Daten

Aufgezeichnete Daten können jederzeit z.B. über die Bedienoberfläche des **vimacc** Arbeitsplatzes vom **vimacc** Streaming-Server abgerufen und wiedergegeben werden.

Der Streaming-Server kann für das Playback gleichzeitig mehrere Streams ausgeben, so dass zeitlich zusammengehörige Streams, die von mehreren Kameras aufgenommen wurden, parallel wiedergegeben werden können.
Basierend auf der von NTP-Servern vorgegebenen Zeit stellt **vimacc** dazu für alle aufgezeichneten Streams die absoluten Zeitbezüge her, so dass beim Abspielen von mehreren Streams dieses zeitlich synchronisiert wiedergegeben werden kann.

Die Anzahl der gleichzeitig abrufbaren Streams ist nur durch die Stream-Leistung des Streaming-Servers begrenzt. Die laufenden Aufzeichnungen werden durch die gleichzeitigen Playbacks nicht gefährdet.

Für den transparenten Zugriff auf den gesamten Aufzeichnungsserververbund von einem externen System (z.B. von einem Video-Content Analyse-System) stellt **vimacc** eine offene Schnittstelle zur Verfügung.

Der Streaming-Server verfügt über eine offene Schnittstelle zur Wiedergabe von aufgezeichneten Streaming-Daten, so dass herstellerunabhängig Module zur Anzeige oder zur Verarbeitung der Streams in einem anderen System angebunden werden können (→ *vimacc Systemdokumentation: Architektur*).

Aufgezeichnete Daten können auf dem **vimacc** Arbeitsplatz oder dem **vimacc** Anzeigeplatz ausgegeben werden. Über die jeweiligen Benutzerschnittstellen kann in allen Wiedergabestreams unabhängig voneinander positioniert werden.

Die maximale Anzahl der gleichzeitig aufgeschalteten Wiedergabesstreams orientiert sich an der Leistungsfähigkeit des **vimacc** Arbeitsplatzes bzw. des **vimacc** Anzeigeplatzes.

Die Steuerung einer Video-Wiedergabe am **vimacc** Arbeitsplatz kann sowohl über die Bedienelemente der Benutzerschnittstelle, als auch über ein Jog /Shuttle erfolgen. Die exakten Wiedergabegeschwindigkeitsstufen sind in weiten Bereichen frei definierbar.
Der **vimacc** Arbeitsplatz ist in der Lage, mehrere Playback-Streams gleichzeitig über die Bedienelemente der Benutzerschnittstelle (z.B. über eine sogenannte Timeline) zu synchronisieren. Die maximale Anzahl der Playback-Streams für eine synchronisierte Wiedergabe orientiert sich an der Leistungsfähigkeit des **vimacc** Arbeitsplatzes.

Wurden von einer Videoquelle stammende Audiodaten mit den Videodaten abgespeichert, so können diese zusammen mit den Videodaten zeitlich synchronisiert wiedergegeben werden.
Audiodaten können aber auch unabhängig von einer Videoquelle wiedergegeben werden, so dass z.B. die Wiedergabe von aufgezeichneten Gesprächen angeschlossener Kommunikationssysteme möglich ist.

Anhand von zusätzlichen gespeicherten Metadaten kann gezielt der zu einem bestimmten Vorgang gehörende Inhalt von den **vimacc** Streaming-Servern abgerufen werden (siehe Kapitel 2.3.2.3).

2.3.4 Analyse

Der **vimacc** Streaming-Server verfügt über eine offene Schnittstelle zur Wiedergabe von aufgezeichneten Streaming-Daten, so dass herstellerunabhängig Module zur Verarbeitung von Streaming-Daten angebunden werden können

Der Streaming-Server kann für Prozesse zur Content-Analyse gleichzeitig mehrere Streams ausgeben.

Die Anzahl der gleichzeitig abrufbaren Streams ist nur durch die Stream-Leistung des Servers begrenzt. Die laufenden Aufzeichnungen werden durch die gleichzeitigen Playbacks nicht gefährdet.

2.3.5 Archivierung

Der **vimacc** Streaming-Server verfügt über Schnittstellen für den Export der aufgezeichneten Stream-Daten.
Über die Bedienoberfläche des **vimacc** Arbeitsplatzes kann der Benutzer in einer Timeline bildgenau Bereiche markieren und für diese Bereiche einen Export der Daten auf ein speziellen Massenspeicher oder ein permanentes Speichermedium, wie z.B. eine DVD oder USB-Sticks starten.

Dabei werden die zu exportierenden Daten zunächst auf der lokalen Festplatte des **vimacc** Arbeitsplatzes zwischengespeichert, um sie dann auf den Zieldatenträger zu übertragen.

Die exportierten Inhalte können auf den Export-Medien verschlüsselt (siehe Kapitel 2.15) oder unverschlüsselt abgelegt werden.

Für die Wiedergabe des exportierten Inhaltes wird eine lizenzfreie Wiedergabe Software mitgeliefert, die vor der Wiedergabe die Authentifizierungsdaten abfragt.

2.4 Videodekodierung und Videoausgabe

vimacc verwendet hoch optimierte und modernste Dekodierungs- und Rendering-Algorithmen, wodurch es einige besondere Leistungsmerkmale besitzt:

- Uneingeschränkte Unterstützung von HD-Video mit voller Auflösung und Bildrate.
- Nahezu verzugslose Bildaufschaltung,
  vergleichbar mit der Aufschaltgeschwindigkeit analoger Systeme
- Bei der Videoausgabe erhöht **vimacc** die Latenzzeit der Gesamtübertragungsstrecke (Übernahme des Streams von der integrierten Hardware bis zur Bildausgabe) um im Mittel nicht mehr als 80 Millisekunden.
- Bei der Wiedergabe von aufgezeichneten Videodaten ist mit **vimacc** eine bildgenaue Positionierung möglich, selbst wenn die Videodaten unter Verwendung der Standards H.264 oder MPEG-4 von den Bildquellen kodiert wurden.
- Bei der gleichzeitigen Wiedergabe von aufgezeichneten Videodaten mehrerer Kameras ist **vimacc** in der Lage, diese zeitlich synchron wiederzugeben (bis auf die eine Millisekunde genau). Dadurch können Ereignisse, die von mehreren Kameras gleichzeitig aufgenommen wurden, gleichzeitig wiedergeben werden.

2.5 Audioübertragung (ab vimacc 2.0)

2.5.1 Allgemein

vimacc ist in der Lage, Audioquellen und Audiosenken über dieselben Mechanismen zu verschalten, wie dies bei der Verschaltung von Videoquellen und Videosenken erfolgt.
Dadurch ist es möglich, neben der Vielzahl der möglichen Videoquellen auch Audioquellen an ein **vimacc** System anzuschließen, diese mit entsprechenden Audio-Ausgabegeräten zu verbinden und auch die zugehörigen Daten mittels des **vimacc** Streaming-Servers aufzuzeichnen bzw. von dort wieder abzurufen.

vimacc ermöglicht bei gleichzeitigem Abruf eines zugehörigen Videostreams ist die synchrone Wiedergabe von Audio und Video.

2.5.2 Ton von Audioquellen übernehmen

Viele Bildquellen enthalten neben den optischen Komponenten auch ein zusätzliches Mikrofon, um ein Objekt nicht nur optisch, sondern auch akustisch überwachen zu können und so einen schnelleren und umfassenderen Überblick über die Gefahrenlage zu erhalten.

Mittels einer einfachen Audio-Content-Analyse ist es **vimacc** beispielsweise möglich, Änderungen an dem von einem Mikrofon gelieferten Audio-Datenstrom zu erkennen, um damit z.B. einen akustischen Alarm auszulösen (vergleichbar mit dem Bewegungsalarm bei einer Videokamera).

vimacc ist in der Lage, auch Audiodaten von angeschlossenen Audioquellen zu übernehmen und aufzuzeichnen (siehe Kapitel 2.3), wodurch z.B. die über die Mikrofone von Videokameras aufgenommenen Signale zusammen mit den Videodaten gespeichert werden können.

vimacc arbeitet in allen Fällen transparent und datenschutz-konform. **vimacc** stellt die Funktionalität bereit und es liegt in der Verantwortung des Anwenders bzw. des Administrators, diese Funktionalität per Konfiguration zu aktivieren.

2.5.3 Ton zu Audioempfängern senden

vimacc ist in der Lage, z.B. über die Bedienoberfläche eines **vimacc** Arbeitsplatzes Audio (wie z.B. Durchsagen) zu einem audiofähigen Gerät zu senden, sodass z.B. Durchsagen auf im System angeschlossenen Lautsprechersystemen getätigt werden können.

Die Auswahl der entsprechenden Audioempfänger erfolgt dabei über dieselbe intuitive Bedienung wie bei der Kameraauswahl zur Livestream-Überwachung, d.h. hier werden dieselben Bedienelemente (Auswahl über hierarchische Darstellung in einer Baumansicht, Auswahl über Lagepläne etc) verwendet.

Ebenso sind auch Durchsagen zu Lautsprechergruppen möglich, so dass z.B. Durchsagen über mehrere Lautsprecher eines Bahnsteiges oder einer Haltestelle gleichzeitig getätigt werden können.

2.5.4 Bidirektionale Audioübertragung

vimacc ist in der Lage, auch Audioverbindungen zu angeschlossenen Kommunikationssystemen aufzubauen, so dass z.B. Wechsel- oder Gegensprechanlagen einfach in ein **vimacc** System integriert werden können.

In diesem Fall wird eine bidirektionale Audioverbindung zwischen dem **vimacc** Arbeitsplatz zu dem angeschlossenen Kommunikationssystem aufgebaut. Je nach Anwendungsfall können die geführten Gespräche zur späteren Nachverfolgung auch dem **vimacc** Streaming-Server aufgezeichnet werden.

vimacc unterstützt hier sowohl die wechselseitige Datenübermittlung (Halbduplex), wie sie z.B. in Wechselsprechanlagen oder Funksystemen angewendet wird, als auch die beidseitige Datenübermittlung (Vollduplex).

2.6 Integration von Datenquellen und -Senken

Die Integration der unterschiedlichen Datenquellen erfolgt innerhalb eines **vimacc** Systems über sogenannte **vimacc** Interfaces.

Diese **vimacc** Interfaces integrieren die unterschiedlichste Audio- und Videotechnik verschiedener Hersteller und stellen die empfangenen Daten über normierte Schnittstellen dem **vimacc** System zur weiteren Verarbeitung zur Verfügung.
Das Spezialwissen über hersteller-spezifische Protokolle, Formate etc liegt ausschließlich in den **vimacc** Interfaces, so dass z.B. PTZ Kameras von verschiedenen Herstellern, die üblicherweise auch über verschiedene Protokolle angesprochen werden müssen, innerhalb eines **vimacc** Systems über eine normierte Schnittstelle bedient werden können.

Diese Normierung verringert zum einen die Komplexität derjenigen Software Komponenten, die die eingesetzte Audio- und Videotechnik verwenden, erheblich, da diese völlig frei von hersteller-spezifischen Protokollen und Formaten implementiert werden können. Geringere Komplexität der Software bedeutet automatisch auch bessere Wartbarkeit und Stabilität und damit bessere Qualität der Software.

Darüber hinaus werden durch diese Normierung die Flexibilität und die Erweiterbarkeit eines **vimacc** Systems erheblich verbessert, denn die Anbindung einer neuen Komponente eines weiteren Herstellers erfordert lediglich Anpassungen an einem **vimacc** Interface. Sobald diese Änderung vorgenommen wurde, stehen die neuen Komponenten automatisch dem gesamten **vimacc** System zur Verfügung, so dass z.B. eine neue Kamera automatisch auf den **vimacc** Arbeitsplätzen angezeigt und ggf. gesteuert werden können und gleichzeitig die Aufzeichnung der Streaming Daten auf den Streaming-Servern erfolgen kann.

Auf diese Weise integrieren die **vimacc** Interfaces beispielsweise die am Markt gängige digitale Videotechnik mit ihrem üblichen Funktionsumfang, wie z.B. Videokameras, Video-Decoder, Netzwerkkameras, digitale Videorekorder usw.
Die aktuelle Liste der bereits integrierten Videotechnik sollte immer direkt angefragt werden (Kontaktdaten siehe Kapitel *Support*).

Für die Videostream-Übertragung, die Livebildanzeige, die Aufzeichnung und deren Wiedergabe überstützen die **vimacc** Interface die Videostandards

- H.264,
- MPEG-4,
- MPEG-2,
- MJPEG.

Für die Audiostream-Übertragung, die Aufzeichnung und deren Wiedergabe überstützen die **vimacc** Interface die Audio Kodierungsverfahren

- G.711,
- AAC.

Alle Komponenten eines **vimacc** Systems, für die zeitliche Bezüge essentiell sind (Videoquellen, Audioquellen, Schnittstellenumsetzer etc.), müssen über das NTP-Protokoll mit einem Zeitserver synchronisiert werden muss. Üblicherweise werden dazu der oder die **vimacc** Streaming-Server als NTP-Server und alle weiteren Komponenten als NTP-Clients konfiguriert.

Können die angeschlossenen Komponenten nicht zeitlich synchronisiert werden, so ist ein **vimacc** Interface in der Lage, den empfangenen digitalen Datenstrom mit dem aktuellen Zeitstempel des eigenen Rechners zu versehen.

2.7 Topologie Ansichten

vimacc verfügt über die Fähigkeit, verschiedene Ansichten auf die Topologie der angeschlossenen Peripheriegeräte bereitzustellen.
In großen **vimacc** Systemen ist es unverzichtbar, die Vielzahl von Peripheriegeräten hierarchisch zu strukturieren, damit der Bediener einer graphischen Oberfläche auf einfache Weise in der Lage ist, die angezeigten Daten zuzuordnen oder zu einer bestimmten Datenquelle zu navigieren, um eine Aufschaltung vorzunehmen.

Da auf Grund der Vielzahl der verschiedenen Anwendungsfälle keine feste Topologie vorgegeben werden kann, stellt **vimacc** die Möglichkeit bereit, verschiedene Ansichten auf die Topologie der Peripheriegeräte zu erstellen. Dadurch ist es möglich eine Standort-zentrierten Sicht, aber auch eine Gerätetyp-spezifische oder auch Netzwerk-zentrierte Sicht unterschiedlich darzustellen.

Einem Bediener an einem **vimacc** Arbeitsplatz würde dann beispielsweise die Standort-zentrierte Sicht präsentiert werden, durch die der Benutzer von Ebene zu Ebene zu einer bestimmten Netzwerkkamera gelangen kann. Einem Netzwerkadministrator dagegen könnte in einem bestimmten Anwendungsfall eher die Netzwerk-zentrierte Sicht präsentiert werden, damit z.B. zu erkennen ist, an welcher aktiven Netzwerkkomponente ein Gerät physikalisch angeschlossen ist.

Bei der Systemplanung können kundenspezifische Anforderungen bzgl. der gewünschten Topologie berücksichtigt werden. Handelt es sich um eine Topologie, die bereits in **vimacc** enthalten ist, so wird diese über das

AccVimaccConfigurationCenter wählbar sein. Ist die spezifische Topologieansicht noch nicht Bestandteil von **vimacc**, so kann ein projektspezifischer Topologie-Manager implementiert werden.

2.8 Virtualisierung

vimacc kann in virtuellen Umgebungen betrieben werden.
Die Darstellung von Videos unterliegt bei Linux-basierten Systemen durch die Nutzung von XVideo ggf. Einschränkungen. Der Streamtransport sowie die Speicherung und Weiterleitung der Daten unterliegt keinen Einschränkungen.

Virtualisierung bedeutet, dass Ressourcen vorhandener IT-Infrastrukturen (wie CPU, RAM, Netzwerk und Massenspeicher) nicht ausschließlich den **vimacc** Softwarekomponenten zur Verfügung stehen, sondern dass diese durch das eingesetzte Virtualisierungssystem mehreren Anwendungen gleichzeitig bereitgestellt werden. Dies hat den Vorteil, dass bereits getätigte und ebenso zukünftige Investitionen in hochverfügbare Server- und Speichersysteme auch dem Videomanagementsystem unmittelbar zu Gute kommen.

Bei dem Einsatz von **vimacc** in einer virtuellen Umgebung sind die besonderen Eigenschaften wie Echtzeitdatenübertragung, hohe Datentransferraten und hohe Speichervolumenanforderungen eines Video-Managementsystems zu beachten. Die Anwendungsfälle Video-Aufzeichnung, Video-Live-Streaming und Video-Playback müssen bei der Systemplanung genauer analysiert werden, da in einigen Konstellationen spezielle Konfigurationseingriffe an der virtuellen Umgebung notwendig werden können bzw. einzelne Komponenten des Videomanagementsystems aufgrund von speziellen Anforderungen außerhalb der virtuellen Umgebung betrieben werden müssen.

Anhand des Beispiels "Live-Streaming" soll dies etwas detaillierter erläutert werden:
Live-Streaming wird in der Regel als RTP/UDP Echtzeitdatentransfer über Unicast- bzw. Multicast-Verbindungen realisiert. Erreicht der Datenstrom den Video-Decoder, so wird er dekodiert. Die dekodierten Daten haben je nach Ausgabe-Farbraum (z.B. RGB => 3 Byte pro Pixel) ein Volumen von bis zu 1,2 MByte pro Bild (4CIF => 704x576 Pixel). Damit wird z.B. bei 25 Bildern pro Sekunde eine Datentransferleistung zur Bildausgabe von mindestens 232 Mbps pro Videokanal benötigt.
Nun sollen die Videokanäle auf einer virtuellen Workstation aufgeschaltet werden, zu der eine Remote-Desktop-Verbindung (RDP) besteht. Dann beansprucht die Datenrate von 232 Mbps pro Videokanal die RDP-Verbindung erheblich, weil die Videokanäle auf der virtuellen Workstation dekodiert werden und dann über die RDP-Verbindung als hochfrequente Bitmaps transportiert werden müssen. Sobald mehrere Videokanäle gleichzeitig angezeigt werden sollen, steigt die Datenrate auf der RDP-Verbindung in Regionen, bei denen der Bildfluss einbricht und die Latenzzeit stark ansteigt.
Wenn aber eine geringe Latenzzeit und eine hohe Bildrate zwingend notwendig ist, z.B. weil eine Schranke ferngesteuert werden soll und demzufolge die Forderung nach einer sehr geringen Verzögerung zwischen Bilderfassung und Bildausgabe

besteht, wird man die Dekodierung der Videodaten auf einer Workstation durchführen müssen, die nicht teil der virtuellen Umgebung ist.

Dies macht die Besonderheiten eines Video-Managementsystems deutlich und erklärt, warum es nicht ganz so problemlos in einer virtuellen Umgebung eingesetzt werden kann, wie etwa die üblichen Büro-Anwendungen.

Nichtsdestotrotz ist **vimacc** für den Einsatz in virtuellen Umgebungen optimiert. Generell kann man die folgenden Regeln anwenden:

1. Es lassen sich alle Prozesse des **vimacc** Videomanagementsystems virtualisieren.
2. Videoausgabeintensive Anwendungen mit Mehrquadrantendarstellungen sollten auf separaten Rechnern außerhalb einer virtuellen Umgebung ablaufen, wenn hohe Bildraten und geringe Latenzzeiten gefordert sind.
3. Der Einsatz von virtuellem Massenspeicher, z.B. ausgeführt als Storage-Area-Network (SAN), ist ohne Risiko für die Videoaufzeichnung möglich, sofern die geforderten Datentransferraten und die geforderten Ein-/Ausgabe-Operationen pro Sekunde für Aufzeichnung und Wiedergabe kontinuierlich zugesichert werden können.

Ob die Videodekodierung und die Videodarstellung in virtuellen Umgebungen realisierbar ist, lässt sich nicht ohne Detailkenntnis des zu Grunde liegenden Virtualisierungssystems beantworten und ist stark abhängig von dem Zielsystem.

vimacc benutzt hoch optimierte und modernste Dekodierungs- und Rendering-Algorithmen. Die Leistungsfähigkeit von **vimacc** wird alleine durch die Leistungsfähigkeit der Hardware und der Leistungsfähigkeit der virtuellen Umgebung begrenzt. Es müssen die folgenden Randbedingungen berücksichtigt werden, um entscheiden zu können, welche Komponenten des **vimacc** Systems in einer virtuellen Umgebung eingesetzt werden können:

- Anzahl der geforderten, parallelen Aufzeichnungskanäle,
- Anzahl der geforderten, parallelen Live-Streaming Kanäle
- Anzahl der geforderten, parallelen Playback Kanäle
- geforderte maximale Latenzzeit.

Abhängig von diesen Anforderungen muss bei der Systemplanung entschieden werden, ob alle Komponenten, oder nur Teile des **vimacc** Systems virtuell betrieben werden.
Durch die modulare Architektur von **vimacc** (→ *vimacc Systemdokumentation: Architektur*) ist es einfach möglich, auf die jeweiligen Projektanforderungen zu reagieren. So ist es beispielsweise möglich, alle zentralen Komponenten in einem virtuellen Umfeld zu betreiben und nur die Dekodierung und die Bildausgabe auf separaten, nicht virtualisierten Standard-PCs mit leistungsstarker Grafikkarte durchzuführen.
In anderen Systemen könnte es sich dagegen als wirtschaftlicher erweisen, die Videoaufzeichnung auf einem klassischen RAID-Array als Direct Attached Storage durchzuführen, den Rest der Prozesse aber im virtuellen Umfeld ablaufen zu lassen.

2.9 Redundanz

Mit dem Begriff Redundanz wird im Allgemeinen das mehrfache Vorhandensein funktional gleicher Komponenten verstanden, die sich im Falle einer Fehlers gegenseitig ersetzen können, damit ein störungsfreier Betrieb gewährleistet werden kann.
Generell kann Redundanz auf verschiedene Weise hergestellt werden:

- Hardware-Virtualisierung
  Eine Möglichkeit ist die bereits in Kapitel 2.8 beschriebene Virtualisierung der Hardware. Hierbei werden innerhalb der virtuellen Umgebung die systemkritischen Komponenten redundant ausgelegt und die Umschaltung zwischen den fehlerhaften Komponenten von der Virtualisierungssoftware durchgeführt, was in der Regel völlig transparent für die Anwendungssoftware erfolgt.
  Der Vorteil dieser Lösung ist, dass die Virtualisierungsumgebung in großen IT-Infrastrukturumgebungen kostengünstig zu realisieren ist, wenn man von den Kosten für die IT-Infrastrukturumgebung absieht. Existiert also bereits ein großes Rechenzentrum, so kann der Betrieb von **vimacc** in einer virtuellen Umgebung schnell realisiert werden (unter der Berücksichtigung der in Kapitel 2.8 ausgeführten Randbedingungen.
  Der Nachteil dieser Lösung ist allerdings, dass ausschließlich Ausfälle von Hardware-Komponenten abgefangen werden können.

- Redundanz auch Softwareebene
  Bei dieser Lösung werden ebenfalls die systemkritischen Komponenten redundant ausgelegt, allerdings wird die Redundanz auf Softwareebene implementiert.
  Mit diesem Ansatz kann eine größere Performance erzielt werden, da keine performance- und speicherintensive Virtualisierungssoftware parallel zu der Anwendungssoftware betrieben werden muss. In kleineren Systemen und bei nicht vorhandener IT-Infrastruktur ist diese Lösung in jedem Fall wirtschaftlicher. Darüber hinaus sind damit ebenfalls kritische Fehler der Anwendungssoftware, wie etwa Programmabstürze, erkennbar, so dass die Software auch in diesem Fall eine Redundanzumschaltung durchführen kann, um den störungsfreier Betrieb zu gewährleisten.
  Der Nachteil ist sicherlich, dass sich diese Art von redundanten Systemen schlechter in eine bestehende IT-Infrastruktur integrieren lassen.

Der Betrieb von **vimacc** in einer virtuellen Umgebung wurde bereits in Kapitel 2.8 beschrieben.

Zur Realisierung eines redundanten Systems auf Anwendungsebene können alle zentralen **vimacc** Komponenten redundant betrieben werden. Auf diese Weise ist es leicht möglich, ein hochverfügbares System aufzubauen, bei dem beim Ausfall einer zentralen Komponente die zentralen Dienste ohne Einschränkungen weiterhin genutzt werden können.

Redundant betriebene **vimacc** Streaming-Server können so konfiguriert werden, dass

- die Videodaten der angeschlossenen Netzwerkkameras im Normalfall jeweils anteilig aufgezeichnet werden (sogenanntes Load-Balancing) und nur im Fehlerfall ein Streaming-Server alle Streams aufzeichnet, oder
- die Videodaten jeder einzelnen Datenquelle gleichzeitig auf mindestens zwei **vimacc** Streaming-Servern aufgezeichnet werden. In diesem Fall wird natürlich die Netzwerklast mit der Anzahl der parallelen Aufzeichnungen multipliziert.

Das **vimacc** System ist in der Lage, selbständig den Ausfall einer zentralen Komponente zu erkennen und auf die entsprechende Ersatzkomponente umzuschalten. Die Umschaltzeit bei einer Redundanzumschaltung beträgt dabei üblicherweise weniger als eine Minute.

2.10 Mandanten-Fähigkeit

Mit Hilfe von **vimacc** ist es möglich, sehr große Systeme mit einer Vielzahl von integrierten Datenquellen verschiedener Hersteller aufzubauen. **vimacc** ist in der Lage, diese Datenquellen und ebenso die auf den Streaming-Servern aufgezeichneten Daten dieser Datenquellen für verschiedene Abnehmer (Mandanten) individuell bereitzustellen (Mandanten-Fähigkeit).
Jeder Abnehmer kann dabei nur auf die Datenquellen und deren gespeicherte Inhalte zugreifen, die ihm per Konfiguration zugeordnet worden sind und kein Abnehmer hat Zugriff auf die Daten eines anderen.

Dadurch ist es möglich, sehr große Systeme zentral zu errichten, zu konfigurieren und zu verwalten und trotzdem die Nutzung des **vimacc** Systems durch die verschiedenen Mandanten zu strukturieren.

2.11 Protokollierung

vimacc ist in der Lage, eine exakte und vollständige Protokollierung aller Aktionen des Systems bzw. Benutzers, der Systemvorgänge allgemein, als auch aller Schnittstellenprozesse sowie eine Zuordnung aller Aktionen zu den jeweils angemeldeten Benutzern durchzuführen.

Alle Interaktionen für die Steuerung des Systems an den Integrationsschnittstellen zu den einzelnen Untersystemen/Komponenten werden dabei detailliert protokolliert, so dass exakt rekonstruiert werden kann, wann (Millisekunden genau) welche Telegramme zwischen welchen Systemen ausgetauscht wurden.

Alle **vimacc** Komponenten können darüber hinaus Protokoll-Dateien erstellen, die eine detaillierte Diagnose der Systemzustände zulassen (siehe Kapitel 2.17).

Alle Protokoll-Dateien werden mit Systemrechten und wahlweise verschlüsselt gespeichert, damit sie von nicht autorisierten Anwendern weder eingesehen noch geändert oder gelöscht werden können.

An allen Streaming-Schnittstellen (Aufzeichnungsverbindungen, Live-Verbindungen) werden zyklisch (ca. alle 5 Sekunden) statistische Werte über Frame-/Paketrate, Bandbreite und Paketverlustrate protokolliert. Wenn die erwarteten Raten unter einen Grenzwert sinken, wird eine Störung in der Peripherieverwaltung bzw. in den **vimacc** Client-Anwendungen angezeigt.

2.12 Datenbasis für die Systemkonfiguration

vimacc verfügt über eine zentrale Datenbasis, mit deren Hilfe die Software des gesamten **vimacc** Managementsystems konfiguriert werden kann.
In dieser Datenbasis sind neben den Parametrierungen der **vimacc** Softwarekomponenten die Parameter der eingebundenen und integrierten Videotechnik, Nutzerberechtigungen, Transaktionen, sowie detaillierte Peripherie- und Geräteparameter wie etwa Schrifteinblendungen, Kamera-Parametersätze usw. enthalten.

Die Datenbasis kann redundant betrieben werden, so dass der Ausfall einer Komponente, auf der die Datenbasis betrieben wird, nicht zum Ausfall des Gesamtsystems führen kann (→ *vimacc Systemdokumentation: Architektur*).

Die Datenbank ist gegen unbefugten Zugriff geschützt. Administratoren und Anwender mit entsprechenden Rechten haben entweder Vollzugriff oder eingeschränkten Zugriff auf Daten und Parametersätze.

Besteht das Gesamtsystem aus dem Verbund mehrerer **vimacc** Subsysteme (→ Beispiele in *vimacc Systemdokumentation: Architektur*), so kann jedes Subsystem für die Verwaltung der subsystem-spezifischen Konfigurationsdaten eine eigene Datenbasis betreiben, so dass jedes Subsystem für sich zunächst einmal auch autark arbeiten kann.
Änderungen in der Datenbasis des Gesamtsystems werden automatisch in die Subsystemdatenbasis übernommen werden, auch wenn während der Konfigurationserweiterung bzw. -änderung ein betroffenes Subsystem offline war.

Der genaue Aufbau der Datenbasis wird in dem Dokument *vimacc Systemdokumentation: Architektur* detailliert beschrieben.

vimacc verfügt über entsprechende Softwarekomponenten, die die Erstellung, Verwaltung, Sicherung und Wartung der Datenbasis ermöglichen.

2.13 Integration in übergeordnete Managementsysteme

vimacc stellt eine Reihe von unterschiedlichen, offenen Schnittstellen zur Verfügung, so dass ein **vimacc** System in ein übergeordnetes Managementsystem integriert werden kann.
Dazu gehören z.B.

- eine **RTSP-Streaming** Schnittstelle zum Abruf der aufgezeichneten Audio- und Videodaten, so dass diese auch in einer nicht zum **vimacc** System gehörenden Applikation in einen externen System dargestellt und wiedergegeben werden.
- eine **HTTP-Steuerschnittstelle** die es ermöglicht, ein **vimacc** System von einem externen System fernzusteuern. So ist es über diese Schnittstelle beispielsweise möglich, die Liste der angeschlossenen Videokameras und Monitore abzurufen und Videokameras auf Monitore aufzuschalten.
- eine **OPC-Steuerschnittstelle** die es ermöglicht, über OPC Datenelemente Ereignisse zu signalisieren, um z.B. die Aufschaltung einer bestimmten Kamera auf einen bestimmten Monitor durchzuführen, oder die Speicherung der zugehörigen Videostreams zu veranlassen.

Durch die modulare Architektur von (→ *vimacc Systemdokumentation: Architektur*) ist es darüber hinaus sehr leicht möglich, weitere Schnittstellen zu spezialisierten Gewerken zu integrieren, wie z.B. Schnittstellen zu

- Einbruchmeldeanlagen (EMA) oder
- Brandmeldeanlagen (BMA).

Ähnlich wie bei der Integration von Streaming-Quellen verschiedener Hersteller (vgl. Kapitel 2.6) wird auch bei der Integration von Steuerschnittstellen das Spezialwissen über das zu integrierende Gewerk auf diskrete Softwarekomponenten beschränkt.

Die Integration der Schnittstellen wird hierzu durch spezialisierte **vimacc** Schnittstellenadapter realisiert, die das Spezialwissen über das Gewerk kapseln und über das entsprechende Protokoll Kommandos und Ereignisse empfangen können. Auf der anderen Seite kommunizieren diese Schnittstelladapter mit dem **vimacc** System ausschließlich über dessen normierte Steuerschnittstellen, so dass alle weiteren Softwarekomponenten völlig unabhängig von den verschiedenen angeschlossenen Systemen sind.

Die momentan zur Verfügung stehenden offenen **vimacc** Schnittstellen sind ausführlich dokumentiert (→ *vimacc Systemdokumentation: Schnittstellen*).

2.14 Authentifizierung

2.14.1 Benutzerverwaltung

Die Authentifizierung von Operatoren des **vimacc** Systems kann je nach Vorgabe auf zwei verschiedene Arten erfolgen, und zwar

- über die integrierte Benutzerverwaltung, oder
- über die Anbindung an bestehende Verzeichnisdienste.

2.14.1.1 Integrierte Benutzerverwaltung

Mit der in **vimacc** integrierten **Accellence**-Benutzerverwaltung können alle verfügbaren Funktionen gezielt für einzelne Benutzer freigeschaltet werden. Dabei können für jeden Aufgabenbereich Benutzerklassen eingerichtet werden, in denen gezielt nur die Rechte freigegeben sind, die für diesen Aufgabenbereich erforderlich sind.

2.14.1.2 Anbindung an Verzeichnis-Dienste

vimacc ist ebenfalls in der Lage, objektbezogene Daten, wie zum Beispiel Benutzerdaten und Benutzerberechtigungen durch die Anbindung an eine bestehende Infrastruktur eines sogenannten Verzeichnis-Dienstes zu ermitteln.
Dadurch ist es möglich, die Authentifizierung von Operatoren des **vimacc** Systems mittels des sogenannten Single Sign-On Konzeptes durchzuführen Das bedeutet, dass sich ein Benutzer nur einmalig an einem Arbeitsplatz authentifizieren muss und **vimacc** alle notwendigen Berechtigungen diese Benutzers von einem Verzeichnis-Dienst ermittelt.

2.14.2 Authentifizierung der Komponenten untereinander

Die Authentifizierung gegenüber der angeschlossenen Peripherie, wie z.B. Netzwerkkameras, erfolgt über die gängigen Verfahren wie z.B. Digest Access Authentication oder IEEE 802.1X.

Externe Systeme authentifizieren sich gegenüber **vimacc** ebenfalls über Digest Access Authentication, wenn diese sich z.B. über die RTSP oder HTTPS Schnittstelle des **vimacc** verbinden.

Die Kommunikation der **vimacc** Komponenten untereinander wird mittels eines symmetrischen Verschlüsselungsverfahrens (AES128) verschlüsselt (siehe Kapitel 2.15.2), dessen Schlüssel nur dem **vimacc** System bekannt ist. Per Definition wird daher einer **vimacc** Kommunikationsentität vertraut, so dass keine explizite Authentifizierung durchgeführt werden muss.

2.15 Datensicherheit

2.15.1 Verschlüsselung der Streaming-Daten

2.15.1.1 Beteiligte vimacc Komponenten

Werden Streaming-Daten von Audio- und Videoquellen abgerufen und im Netzwerk zu Datensenken übertragen, so sind diese Daten ohne besondere Maßnahmen zunächst einmal im Netzwerk verfügbar und können prinzipiell unbemerkt manipuliert werden. Abbildung 2.1 verdeutlicht schematisch, an welchen Stellen der Übertragungsstrecke die Daten angreifbar sind.

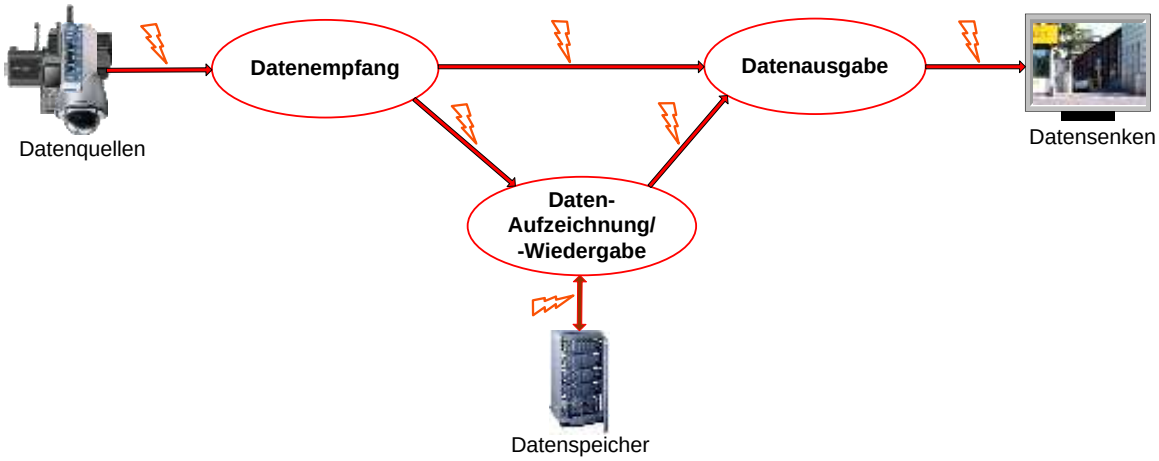

Abbildung 2.1: Unverschlüsselte Datenübertragung

In bestimmten Szenarien kann es jedoch erforderlich sein, nicht nur die Datenquellen vor unberechtigten Zugriffen zu schützen, sondern zusätzlich die Streaming-Daten vor unbemerkten Manipulationen oder Zugriffen zu schützen.

vimacc besitzt die Fähigkeit, die empfangenen Streaming-Daten zu verschlüsseln um somit die Sicherheit der Daten zu gewährleisten. Hierbei kann **vimacc** je nach Anforderung die Verschlüsselung für die unterschiedlichen Übertragungswege realisieren.

Beispielsweise kann **vimacc** derart eingesetzt werden, dass alle aufzuzeichnenden Streaming-Daten verschlüsselt werden und parallel dazu Live-Streaming-Daten unverschlüsselt übertragen werden (siehe Abbildung 2.2). Auf diese Weise ist es möglich, alle aufgezeichneten Daten vor einer unbefugten Wiedergabe zu schützen, denn nur wenn bei der Wiedergabe der entsprechende Dekodierschlüssel bekannt ist, können die aufgezeichneten Daten dekodiert und wiedergegeben werden.

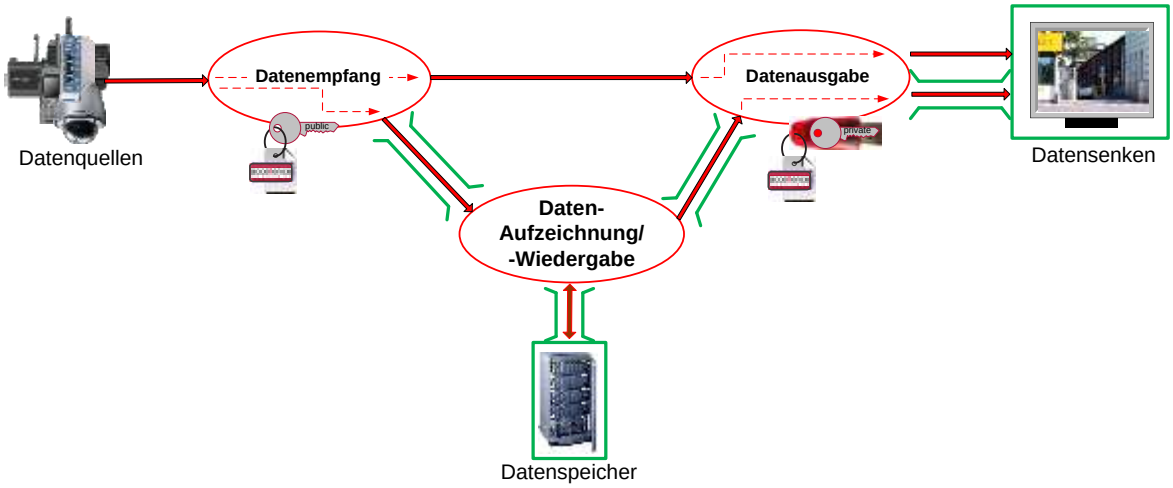

Abbildung 2.2: Mit vimacc verschlüsselte Aufzeichnung (Accellence Schließsystem)

Ebenso ist es mit **vimacc** möglich, Streaming-Quellen einzusetzen, die die Datenverschlüsselung direkt im Gerät realisieren, so dass auf allen Übertragungswegen ausschließlich verschlüsselten Daten übertragen werden und auch nur verschlüsselte Daten gespeichert werden (siehe Abbildung 2.3).

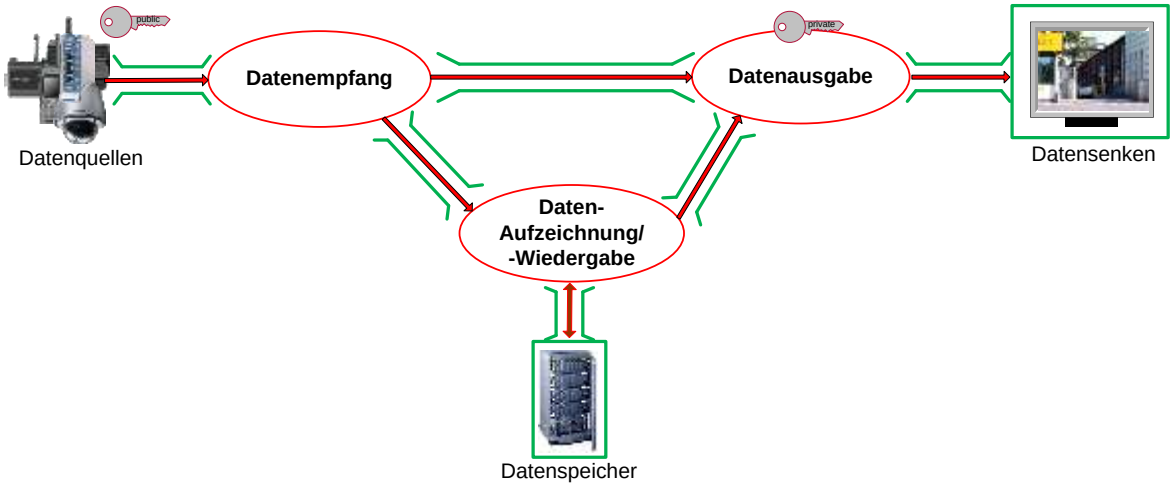

Abbildung 2.3: Datenverschlüsselung in den Streaming-Quellen

Für den Fall, dass Streaming-Quellen eingesetzt werden, die nicht über die Fähigkeit der Datenverschlüsselung verfügen, die Netzwerkverbindung zu dieser Quelle nicht genügend abgesichert werden kann, es aber trotzdem die maximale Datensicherheit gewährleistet werden soll, so kann ein spezieller Verschlüsselungsadapter eingesetzt werden, der direkt mit der Quelle verbunden ist und das Netzwerk zwischen unsicherer Quelle und dem abgesicherten Netzwerk der **vimacc** Empfangs-Komponente trennt (siehe Abbildung 2.4 und Abbildung 2.5).

Dieser Verschlüsselungsadapter ist eine dedizierte Hardware-Komponente, auf der **vimacc** direkt betrieben wird, um die Verschlüsselung der empfangenen Streaming-Daten vorzunehmen. Diese Hardware-Komponente hat die Besonderheit, dass sie über zwei getrennte Netzwerkanschlüsse verfügt, so dass sie auf der einen Seite physikalisch so nah wie möglich über ein Netzwerkkabel direkt mit der Streaming-

Quelle verbunden werden kann. Auf der anderen Seite kann sie über den zweiten Netzwerkanschluss mit einer der aktiven Netzwerkkomponenten des Streaming-Netzwerkes verbunden werden.

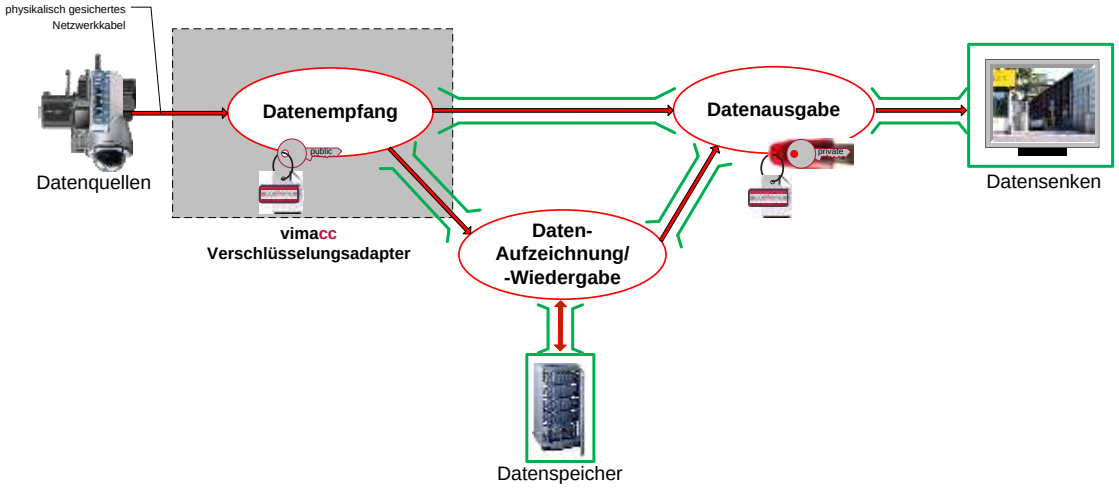

Abbildung 2.4: Datenverschlüsselung mit dem vimacc Verschlüsselungsadapter

Die unverschlüsselten Streaming-Daten gelangen auf diese Weise über die direkte Netzwerkverbindung von der Datenquelle in die **vimacc** Komponenten, werden dort verschlüsselt und anschließend über die zweite Netzwerkverbindung in das Netzwerk des Video-Managementsystems eingespeist (siehe Abbildung 2.5).
Dadurch wird erreicht, dass innerhalb des Netzwerkes des VMS ausschließlich verschlüsselte Streaming-Daten übertragen werden, obwohl Streaming-Quellen eingesetzt werden, die selbst keine Datenverschlüsselung durchführen können, d.h. das Netzwerk zu der unsicheren Streaming-Quelle wird von dem durch die Verschlüsselung gesicherten Netzwerk des VMS getrennt.

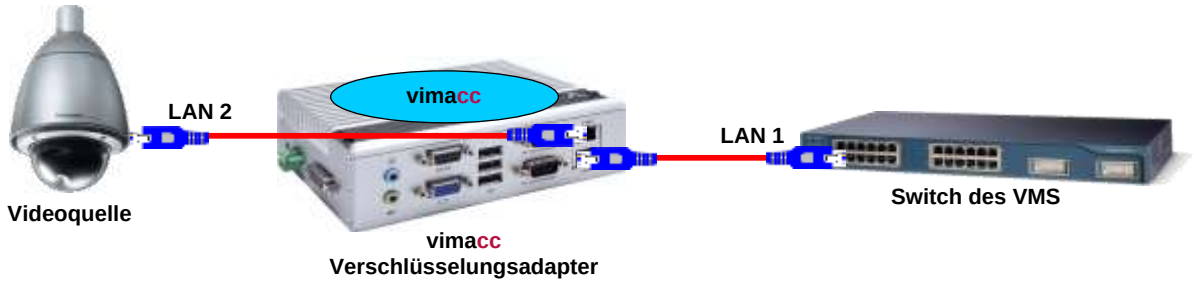

Abbildung 2.5: Verbindung eines vimacc Verschlüsselungsadapters mit einer Datenquelle

2.15.1.2 Verfahren zur Verschlüsselung der Streaming-Daten

Sofern die Datenverschlüsselung von **vimacc** aktiviert wurde, verschlüsselt **vimacc** bereits beim Datenempfang alle Streaming-Daten nach einem hybriden Verschlüsselungsverfahren.

Bei einem hybriden Verschlüsselungsverfahren werden die Verfahren der asymmetrischen Verschlüsselung und der symmetrischer Verschlüsselung kombiniert. Die zu schützenden Streaming-Daten werden zunächst mit einem

zufälligen, geheimen Schlüssel nach einem standardisierten und offengelegten Verschlüsselungsverfahren (z.B. Advanced Encryption Standard - AES) symmetrisch verschlüsselt, weil symmetrische Verschlüsselungsverfahren auch bei großen Datenmengen sehr schnell sind und nur dadurch die hohen Performance-Anforderungen an das VMS erfüllt werden können.
Symmetrische Verschlüsselungsverfahren haben allerdings den Nachteil, dass allen Kommunikationspartnern der geheimen Schlüssel bekannt sein muss, was ein großes Sicherheitsrisiko in sich birgt.
Aus diesem Grund wird der symmetrische Schlüssel wiederum mit einem asymmetrischen Verschlüsselungsverfahren verschlüsselt, denn bei asymmetrischen Verschlüsselungsverfahren wird generell zur Verschlüsselung nur der öffentliche Schlüssel gebraucht, um Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, so dass zur Übermittlung dieses Schlüssels ein authentifizierter Kanal ausreicht.
Der auf diese Weise verschlüsselte symmetrische Schlüssel wird nun mit den Streaming-Daten zu den Empfängern übertragen. Der private Schlüssel des asymmetrischen Verfahrens wird auf Seiten der Decoder-Instanzen gespeichert und dient dazu, die mit dem öffentlichen Schlüssel verschlüsselten Daten wieder zu entschlüsseln, d.h. den symmetrischen Schlüssel zur Entschlüsselung der Streaming-Daten wieder zurückzugewinnen.
Konkrete Decoder-Instanzen sind z.B. die **vimacc** Arbeitsplätze, die **vimacc** Anzeigeplätze, angeschlossene Systeme zur Video-Content-Analyse, oder auch Decoder für die Wiedergabe von einem Export-Medium.

Zur Speicherung der öffentlichen und privaten Schlüssel des asymmetrischen Verschlüsselungsverfahrens kann **vimacc** je nach Anforderung des Zielsystems unterschiedliche Verfahren anwenden:

- Verwendung des **Accellence** Schließsystems
- Verwendung einer Public-Key-Infrastructure (PKI).

Verwendung des Accellence Schließsystems:

Dieser Ansatz setzt voraus, dass **Accellence Technologies** als vertrauenswürdig angesehen wird und das von **Accellence Technologies** bereitgestellte Schlüsselpaar aus privatem und öffentlichem Schlüssel anerkannt wird.
In diesem Fall wird für das **vimacc** Zielsystem eine individualisierte Installation erstellt, bei der der öffentliche Schlüssel des asymmetrischen Verschlüsselungsverfahrens Bestandteil der Software ist und der private Schlüssel auf einem Datenzugangsschlüssel (USB-Dongle) gespeichert wird (siehe Abbildung 2.2 und Abbildung 2.3). Damit kann sichergestellt werden, dass nur die Personen, die im Besitz des Datenzugangsschlüssels sind, verschlüsselte Streaming-Daten (Live oder aufgezeichnete Daten) wiedergeben können.

Hierbei können nun verschiedene Authentifizierungsverfahren eingesetzt werden:

- Einfach:
  Verwendung eines Dongles

- Zweifach:
  Verwendung eines Dongles und zusätzlich Eingabe einer PIN erforderlich
- N-Fach:
  Verwendung von N Dongles mit oder ohne PIN Eingabe.

Verwendung einer Public-Key-Infrastructure (PKI):

Zur Umsetzung von datenschutztechnischen Anforderungen ist **vimacc** ebenfalls in der Lage, den Zugriff auf Streaming-Daten über ein PKI System benutzerbezogen abzusichern (siehe Abbildung 2.6), so dass generell die Streaming-Daten nur bei Präsenz des privaten Schlüssels einer PKI Karte entschlüsselt werden können.

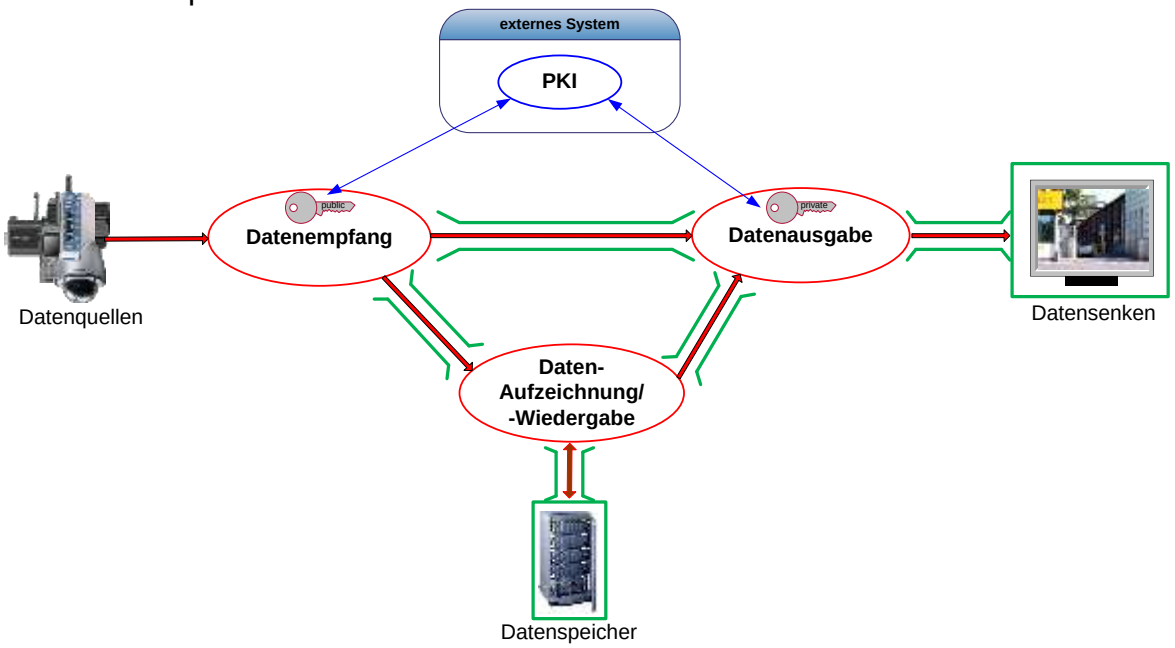

Abbildung 2.6: Mit vimacc verschlüsselte Datenübertragung (Anbindung an PKI System)

Bei diesem Verfahren werden die öffentlichen Schlüssel der zugriffsberechtigten Benutzer für das asymmetrische Verschlüsselungsverfahren ebenfalls vom PKI System bezogen. Dabei wird der symmetrische Schlüssel, mit dem die Streaming-Daten verschlüsselt werden (siehe oben) mit den öffentlichen Schlüsseln aller zugriffsberechtigten Benutzer verschlüsselt. Für die Dekodierung der Streaming-Daten wird dann der symmetrische Schlüssel mit Hilfe der Dechiffrier-Operationen auf der benutzerbezogenen Chipkarte des PKI Systems ermittelt.

Auf diese Weise wird sichergestellt, dass nur die zum Zeitpunkt der Verschlüsselung berechtigten Benutzer die verschlüsselten Streaming-Daten wiedergeben können.

2.15.2 Verschlüsselung der vimacc Kommunikation

Die Software Komponenten eines **vimacc** Systems können untereinander verschiedene Kommunikationsverbindungen aufbauen, um die unterschiedlichen Anwendungsfälle zu realisieren. Damit die Kommunikation auf diesen

Netzwerkverbindungen nicht abgehört und manipuliert werden kann, können die Datentelegramme von den **vimacc** Komponenten optional ebenfalls mit einem hybriden Verschlüsselungsverfahren verschlüsselt werden. Hierbei werden die Datenpakete unter Verwendung des Secure Sockets Layer (SSL) Protokolls verschlüsselt.

2.16 Lizenzierung

Wie aus den Kapiteln 2.1 bis 2.15 hervorgeht, besitzt ein **vimacc** System eine Vielzahl von unterschiedlichen Funktionseinheiten für die unterschiedlichen Anwendungsfälle.
Da nicht alle Funktionen in jedem Zielsystem erforderlich sind, ist **vimacc** mit einem Mechanismus zur Lizenzierung von einzelnen Funktionsblöcken ausgestattet. Dadurch können tatsächlich benötigte Funktionalitäten freigegeben, bzw. nicht benötigte Funktionalitäten gesperrt werden.

Die zugehörigen Lizenzierungsschlüssel werden üblicherweise in Form von Signaturdateien auf Hardware-Dongles ausgeliefert, die zum Betrieb der **vimacc** Software-Komponenten zwingend erforderlich sind.
(Wird das **Accellence** Schließsystem zur Verschlüsselung angewendet – siehe Kapitel 2.15.1 – so befindet sich die Signaturdatei auf dem gleichen Hardware-Dongle wie der private Schlüssel des asymmetrischen Verschlüsselungsverfahrens.)

In Sonderfällen kann ein **vimacc** System aber auch vollständig ohne den Einsatz von Hardware-Dongles betrieben werden. In diesen Fällen kann eine individualisierte Installation erstellt werden, bei der die zugehörigen Signaturschlüssel Bestandteil der Software sind. Dies kann z.B. dann sinnvoll sein, wenn **vimacc** in einer virtuellen Umgebung eingesetzt werden soll, bei der die Freigabe von USB-Schnittstellen als problematisch angesehen wird, so dass der Einsatz von Hardware-Dongles dort nicht in Frage kommt.

2.17 Softwareverteilung

Bei größeren **vimacc** Systemen mit vielen Bedienplätzen, redundanten Streaming-Servern und mehreren Interfacerechnern müssen im Rahmen der Wartungsarbeiten oder im Falle von Fehlerbeseitigen oder Systemerweiterungen automatische Software-Updates durchgeführt werden. Dabei sollte immer sichergestellt werden, dass ein einheitlicher Softwarestand im System installiert ist.

Um den Installationsprozess zu automatisieren bestehen im Wesentlichen zwei Möglichkeiten:

Zum Einen kann man unter Verwendung von kommerziellen Produkten den Prozess der Softwareverteilung komplett automatisieren, z.B. mit dem Produkt *System Center*

Configuration Manager (SCCM) von Microsoft. Kommerzielle Produkte erfordern allerdings in der Regel den Einsatz einer Reihe von zusätzlichen Infrastruktur-Komponenten. Im Falle des SCCM sind das zusätzliche Rechner, die z.B. MS SQL Server, Active Directory, Certificate Authority (CA) und Internet Information Service (IIS) bereitstellen müssen. Der Vorteil dieser Lösungen ist sicherlich, dass damit vielfach auch ein Update des Betriebssystems durchgeführt werden kann, allerdings rechtfertigt sich der sehr hohe finanzielle und vor allem auch administrative Aufwand erst in sehr großen Systemen.

Die andere Möglichkeit besteht darin, den Mechanismus zur Softwareverteilung von **vimacc** zu benutzen. Damit kann innerhalb eines Systems die **vimacc** Software automatisiert auf allen Rechnern verteilt werden, ohne dass weitere Software angeschafft oder großer administrativer Aufwande betrieben werden muss.

Auf diese Weise kann geschultes Wartungspersonal sehr schnell sie gesamte **vimacc** Software innerhalb eines **vimacc** Systems aktualisieren und so den ordnungsgemäßen Betrieb mit einem einheitlichen Softwarestand sicherstellen.

2.18 Zentrale Ablaufsteuerung

vimacc verfügt über einen Mechanismus, mit dem von einer zentralen Stelle aus bestimmte Abläufe innerhalb eines **vimacc** Systems angestoßen werden können.

Diese Fähigkeit kann beispielsweise dazu benutzt werden, dass gesamte System geordnet in eine Betriebsart zu überführen, in der Wartungsarbeiten, wie z.B. die Aktualisierung der **vimacc** Software (siehe Kapitel 2.17), durchgeführt werden können.

Besonders in großen Systemen mit vielen verteilten Rechnern kann es mitunter sehr aufwändig sein, die laufende Software in einen bestimmten Zustand zu überführen, die Software zu beenden oder gar alle Rechner gezielt herunterzufahren oder neu zu starten.
Für diese Fälle hilft die zentrale Ablaufsteuerung von **vimacc**, den zeitlichen Aufwand erheblich zu reduzieren. Darüber hinaus wird sichergestellt, dass auch tatsächlich alle Rechner des **vimacc** Systems erfasst werden und nicht versehentlich ein oder mehrere Rechner vergessen werden.

2.19 Administration, Wartung und Diagnose

2.19.1 Administration

Für die Administration des gesamten **vimacc** Systems wird **vimacc** mit einer Administrations-Anwendung ausgeliefert (*AccVimaccConfigurationCenter* → *vimacc*

Systemdokumentation: Architektur), mit der die folgenden Aufgaben durchgeführt werden können:

- Peripherieverwaltung,
- Benutzerverwaltung,
- Rechteverwaltung.

Zum Starten dieser Anwendung ist auch hier die Authentifizierung über die **Accellence** Benutzerverwaltung oder über ein angeschlossenes PKI möglich, so dass sichergestellt ist, dass ausschließlich autorisierte Benutzer diese Anwendung benutzen können.

Die Peripherieverwaltung dieser Anwendung ermöglicht das Hinzufügen, Entfernen und Ändern von Peripheriegeräten wie Audio- und Videoquellen, digitalen Input/Output-Modulen, Aufzeichnungsgeräten, Anzeigeeinheiten etc.

Die Benutzerverwaltung dieser Anwendung ermöglicht das Hinzufügen, Entfernen und Ändern von Benutzerprofilen.
Über die Rechteverwaltung dieser Anwendung kann festgelegt werden, welche Operationen ein Benutzer in den Applikation ausführen darf. Berechtigungen für Operationen können z.B. kamerabezogen sowohl für einzelne Kameras als auch für Kameragruppen zugeteilt bzw. entzogen werden. Kamerabezogene Operationen sind z.B.:

- Kameranamen auflisten,
- Kameravitalitätsparameter anzeigen,
- Live-Aufschaltung,
- Kamerasteuerung,
- I/O-Kontakte schalten,
- Kamera hinzufügen und entfernen,
- Kamerakonfiguration,
- Kameraaufzeichnung im Playback aufschalten,
- Auslösung einer manuellen Alarmaufzeichnung für eine Kamera,
- Export von Videodaten einer Kamera,
- Einzelbild drucken,
- Einzelbild in die Zwischenablage kopieren.

Diese Funktionen müssen in den Fällen verwendet werden, wenn die Benutzerdaten nicht von angeschlossenen Verzeichnisdiensten ermittelt werden können (siehe 2.14.1.2).

2.19.2 Wartung und Diagnose

Für alle Anwendungen des **vimacc** Systems werden Installations-, Wartungs- und Benutzer-Handbücher geliefert.

vimacc wird mittels eines Installations-Programms ausgeliefert, so dass geschultes Wartungspersonal selbstständig in der Lage ist, ausgefallene Komponenten zu ersetzen und die SW-Installation für die ersetzten Komponenten selbständig durchzuführen.
vimacc wird mit Analyse- und Monitoring-Anwendungen ausgeliefert, die z.B. die Anzeige der Vitalitätsdaten der eingerichteten Geräte erlauben, so dass geschultes Wartungspersonal sehr schnell in der Lage ist, Fehler zu analysieren und zu beheben.

Alle Komponenten eines **vimacc** Systems erstellen darüber hinaus Protokoll-Dateien, die eine detaillierte Diagnose der Systemzustände zulassen (siehe Kapitel 2.11). Der Detaillierungsgrad der protokollieren Informationen ist dabei einstellbar. Die Protokolldateien sind in einem Ring organisiert, dessen Umfang ebenfalls einstellbar ist und je nach Anforderung mehrere Wochen umfassen kann.

Die Protokolldateien werden mit Systemrechten gespeichert und wahlweise verschlüsselt, damit sie von nicht autorisierten Anwendern weder eingesehen noch geändert oder gelöscht werden können.
Es erfolgt eine exakte und vollständige Protokollierung aller Aktionen des Systems bzw. der Benutzer, der Systemvorgänge allgemein, als auch aller Schnittstellenprozesse sowie eine Zuordnung aller Aktionen zu den jeweils angemeldeten Benutzern.

Alle Interaktionen für die Steuerung des Systems an den Integrationsschnittstellen zu den einzelnen Untersystemen/Komponenten können so detailliert protokolliert werden, dass exakt rekonstruiert werden kann, wann (millisekundengenau) welche Telegramme zwischen welchen Systemen ausgetauscht wurden.

An allen Streaming-Schnittstellen (Aufzeichnungsverbindungen, Live-Verbindungen) können zyklisch (ca. alle 5 Sekunden) statistische Werte über Frame- und Paketrate, Bandbreite und Paketverlustrate protokolliert werden. Wenn die erwarteten Raten unter einen Grenzwert sinken, kann eine Störung in den Client-Anwendungen angezeigt werden.

Um möglichen Störungen durch Festplattenüberlauf oder Laufwerksausfall vorzubeugen, ist eine Laufwerksüberwachung aller verwendeten Speicher-Laufwerke enthalten: Bei Unterschreiten eines je Laufwerk einstellbaren Rest-Speichervolumens kann eine Warnung in den Client-Anwendungen angezeigt werden.

2.19.3 Meldungen an externe Systeme

vimacc ist in der Lage, spontane Ereignisse und Fehler, die während des Betriebes innerhalb des Systems auftreten oder aufgetreten sind, an externe Systeme zu melden.
Dazu können auf den entsprechenden Komponenten die **vimacc** Report-Anwendungen installiert werden (→ *vimacc Systemdokumentation: Architektur)*, mit deren Hilfe alle Ereignisse gesammelt und über die entsprechende Reporting-Schnittstelle an externe Systeme übergeben werden können.

Hierbei können auch Ereignisse erfasst werden, die nicht von **vimacc** Software-Komponenten selbst, sondern von Software-Komponenten des Betriebssystems stammen. **vimacc** liest hierzu die in das jeweilige Betriebssystem (Windows bzw. Linux) integrierte Ereignisdatenbank aus und versendet die dort gespeicherten Einträge über die Reporting-Schnittstelle an die registrierten Empfangskomponenten. Auf diese Weise ist es möglich, Fehlerzustände der entsprechenden PC-Komponenten zu erfassen und auch nachträglich zu melden, sofern diese vom Betriebssystem erkannt und in die Ereignisdatenbank eingetragen worden sind.

3 Support / Hotline

Haben Sie noch Fragen zu **vimacc**?

Dann wenden Sie sich bitte

- per Email an **support@accellence.de**
  oder
- telefonisch unter **+49 (0)511 277 2490**

an unsere Hotline. Unsere Mitarbeiter stehen Ihnen Werktags von 9:00-17:00 Uhr gerne zur Verfügung.

Index