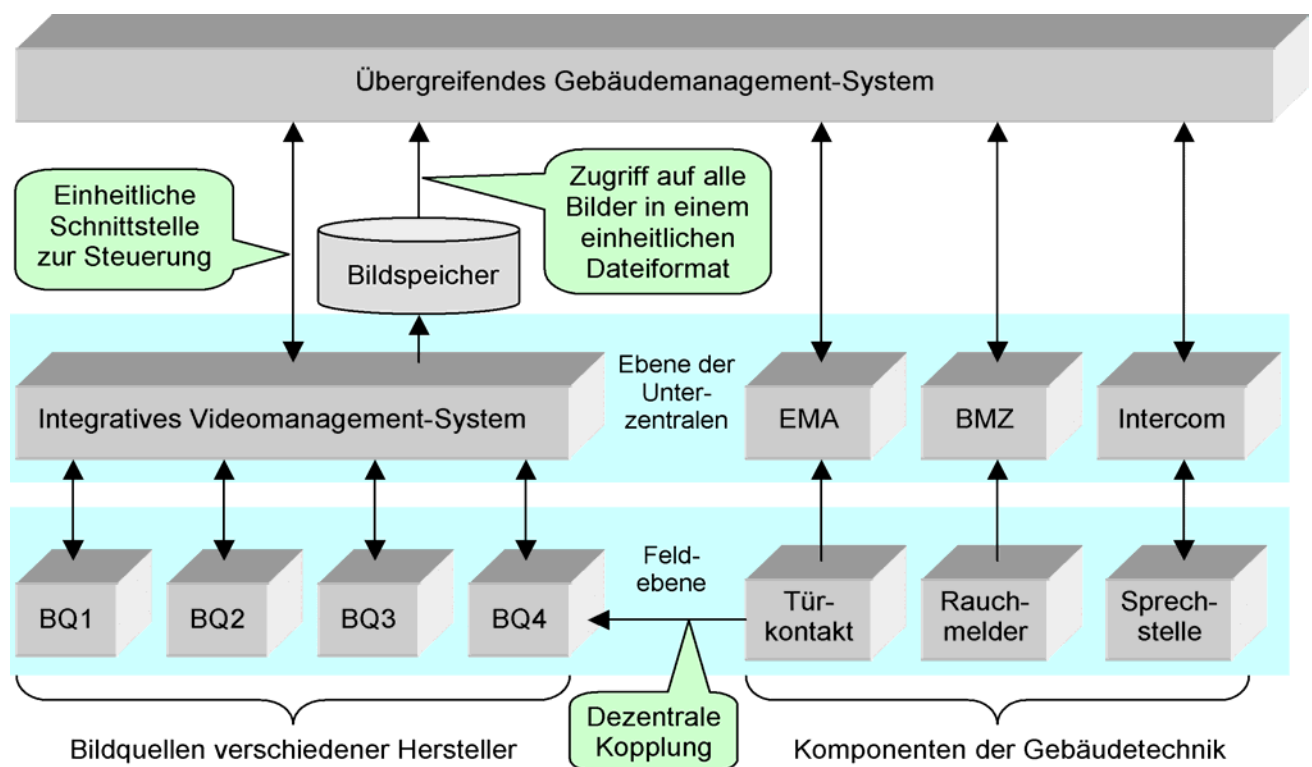


Grundlagen der Video- Integration



**Heterogene Videosysteme
planen, errichten und betreiben**

Vorwort

Dieser Fachartikel zum Thema "**Grundlagen der Video-Integration**" richtet sich an alle, die digital vernetzte heterogene Videoüberwachungssysteme planen, errichten oder betreiben wollen und sich einen fundierten Überblick über die dabei zu berücksichtigenden Aspekte verschaffen wollen.

Um auch den "klassischen" Videoerrichter "mitzunehmen", beginnt der Artikel bewusst bei analogen Systemen und führt schrittweise weiter zu digitalen, vernetzten und heterogenen Systemen.

Dabei werden alle Begriffe und Abkürzungen, die im Artikel verwendet werden, jeweils vorher erläutert, damit ein möglichst breiter Kreis von Lesern den Ausführungen folgen kann und einen Nutzen für sich daraus zieht.

Der Artikel wurde mit dem Ziel verfasst, in möglichst kompakter Form die grundlegenden Konzepte heterogener Videosysteme anschaulich und in der nötigen Tiefe darzustellen, um dem Leser ein echtes Verständnis der Zusammenhänge zu ermöglichen.

Garbsen, 07. Juli 2011

Dipl.-Ing. Hardo Naumann
Accellence Technologies GmbH

Verzeichnis der verwendeten Abkürzungen

ASCII	American Standard Code for Information Interchange: Weit verbreiteter Standard mit dem Texte digital gespeichert werden
CAPI	Common Application Programming Interface: Programmierschnittstelle für Anwendungen, die ISDN nutzen wollen
CCTV	Closed Circuit Television: Fernsehen für geschlossene Benutzergruppen; heute meist synonym verwendet für Videoüberwachungsanlagen
DFÜ	Daten Fern-Übertragung per Modem oder ISDN
DSL	Digital Subscriber Line: Digitaler Teilnehmeranschluss für das Internet
DVR	Digitaler Video Recorder
EDGE	Enhanced Data Rates for GSM Evolution: Gegenüber GPRS verbesserte Datenübertragung in GSM-Mobilfunknetzen
FTP	File Transfer Protocol: Ermöglicht Speichern und Abrufen von Dateien
GPRS	Paketorientierte Datenübertragung in GSM-Mobilfunknetzen
GPS	Global Positioning System: Satellitensystem zur Positions- und Zeitmessung
GSM	Global System for Mobile Communication: Mobilfunkstandard der 2. Generation
GUI	Grafical User Interface: Grafische Bedienschnittstelle
HDMI	High Definition Multimedia Interface: Schnittstelle zur digitalen Übertragung von Audio und Video bei Geräten der Unterhaltungselektronik
HSDPA	High Speed Downlink Packet Access: Hochgeschwindigkeits-Datenübertragung beim Empfang von Daten über UMTS
HSUPA	High Speed Uplink Packet Access: Hochgeschwindigkeits-Datenübertragung beim Versenden von Daten über UMTS
IP	Internet Protocol: Basis für eine Vielzahl weiterer Protokolle
ISDN	Integrated Services Digital Network: Dienstintegrierendes digitales Telekommunikationsnetz, vor allem in Deutschland verbreitet
JFIF	JPEG File Interchange Format: Weit verbreiteter Standard zum Speichern von Bildern
JPEG	Joint Photographic Experts Group: Standard zur Kompression von Einzelbildern
LAN	Local Area Network: Netzwerk im Nahbereich
MPEG	Moving Pictures Experts Group: Standards zur Kompression von Bewegtbildern
NTSC	In den USA übliche Norm für analoges Farbfernsehen
NVR	Netzwerk Video Recorder
PC	Personal Computer: Arbeitsplatzrechner
PAL	In Deutschland übliche Norm für analoges Farbfernsehen
QCIF	Quarter Common Intermediate Format: Digitales Bildformat mit 176x144 Bildpunkten
RGB	Rot - Grün - Blau: Übliche Abkürzung für die 3 Grundfarben bei der Darstellung von Videobildern auf Monitoren
RS232	Standard für einfache serielle Schnittstelle
RS485	Standard für serielle Schnittstelle mit erhöhter Störsicherheit
TTL	Transistor-Transistor-Logik: Definiert Spannungspegel für digitale Signale
UMTS	Universal Mobile Telecommunications System: Mobilfunkstandard der 3. Generation
VLAN	Virtual Local Area Network
VMS	Video-Management-System
VPN	Virtual Private Network: Verschlüsselte Datenübertragung
WAN	Wide Area Network: Weitverkehrs-Netzwerk
WLAN	Wireless Local Area Network: Drahtloses Netzwerk für den Nahbereich

Heterogene Videosysteme planen, errichten und betreiben

Grundlagen der Video-Integration

In vielen Anwendungsfällen ist es von großem Nutzen, Videosysteme verschiedener Hersteller untereinander und mit anderen Gewerken verbinden zu können. Auf diese Weise können Daten schneller und einfacher ausgetauscht und somit Arbeitsabläufe effizienter gestaltet werden. Dem steht entgegen, dass viele Videosysteme zueinander inkompatibel sind. Dies betrifft nicht nur die häufig diskutierte Video-Kompressionsverfahren, sondern auch Steuerprotokolle, Datenformate, Bedienkonzepte und Abläufe. Mögliche Lösungsansätze müssen daher eine Vielzahl von Aspekten berücksichtigen.

Ausgangslage

Die ersten Videoüberwachungsanlagen waren in sich abgeschlossene Systeme, in denen eine Anzahl Kameras auf einen oder mehrere Monitore aufgeschaltet werden konnten. Die Zuordnung der Kameras zu den Monitoren erfolgte über analoge Video-Kreuzschienen. Mit Video-Recordern konnten bei Bedarf Bilder aufgezeichnet und später wieder abgerufen werden. Verschiedene Hersteller haben in dieser Zeit unabhängig voneinander mit der Entwicklung ihrer Produkte für diesen Markt begonnen.

Dank der Standards aus der Fernsehtechnik (PAL, NTSC) war zumindest das eigentliche Videosignal weitgehend normiert. Aber schon bei den Steuerprotokollen für die Kameras und den Formaten und der Systematik zum Speichern der Bilder entwickelte sich eine große Vielfalt. Dies erschwerte es Errichten solcher Anlagen, Produkte verschiedener Hersteller zu kombinieren. Das war auch nicht zwingend nötig, denn jede Anlage war in sich geschlossen. Die Errichter tendierten deshalb dazu, so genannte homogene Anlagen aufzubauen, in denen nur die Produkte eines Herstellers zum Einsatz kamen.

In dieser Zeit hat sich der Begriff CCTV als Synonym für Videoüberwachungsanlagen etabliert: CCTV steht als Abkürzung für „Closed Circuit TeleVision“ und bedeutet sinngemäß „Fernsehen für geschlossene Benutzergruppen“, denn im Gegensatz zum öffentlichen Fernsehen (broadcast, Rundfunk) darf hier nicht jeder sehen, sondern nur ausgewählte Personen haben Zugriff auf die Bilder.

Trend: Digitale Vernetzung

Mittlerweile sind diese Anlagen nicht mehr geschlossen, denn auch in der Videoüberwachung schreiten

Digitalisierung und Vernetzung voran. Diese Technologien sind in anderen Anwendungsbereichen entstanden, öffnen aber auch für CCTV ganz neue Möglichkeiten.

Besonders wenn es darum geht, Videobilder kostengünstig über große Entfernungen zu transportieren oder flexibel zwischen verschiedenen Standorten oder Organisationen auszutauschen, sind die Vorteile der digitalen Netzwerktechnik erheblich. Dennoch sollten Nachteile wie beispielsweise systembedingte Verzögerungszeiten bei der Übertragung der Bilder über digitale Netze (so genannte Latenz) oder durch die verfügbare Netzwerk-Bandbreite begrenzte Bildqualität und Bildfrequenz nicht außer Acht gelassen werden. Außerdem weisen die Produkte der digitalen Videotechnik aufgrund der hohen Innovationsgeschwindigkeit häufig noch nicht den Reifegrad hinsichtlich optischer und mechanischer Qualität auf, wie er sich in der analogen Technik über viel längere Zeiträume herausbilden konnte.

Die digitale Vernetzung führt dazu, dass die bisherigen „Insellösungen“ miteinander verbunden werden. Dadurch werden aus einfachen homogenen Videoanlagen komplexe heterogene Systeme. Dies bringt große Herausforderungen für Planer, Hersteller, Errichter und Betreiber der CCTV-Anlagen mit sich.

Anwendungsbeispiele

Der Antrieb für diese Entwicklung resultiert aus dem Bedarf, Videobilder koordiniert mit anderen Daten flexibel verarbeiten, speichern und weiterleiten zu können. Einige Anwendungsbeispiele zeigen, was das in der Praxis bedeutet:

Große Parkhausbetreiber verwalten heute hunderte von Parkhäusern. Längst befindet sich nicht mehr in jedem einzelnen Parkhaus eine

Leitstelle, sondern wie in vielen anderen Bereichen wurde auch hier aus Kostengründen zentralisiert. Das heißt, von einer zentralen Leitstelle aus werden eine ganze Reihe von Parkhäusern überwacht und gesteuert. Nun wechselt aber häufig die Zuordnung, welches Parkhaus von welchem Betreiber verwaltet wird. Da nicht jedes Mal die komplette Videotechnik des Parkhauses ausgetauscht und an den Standard des jeweiligen Betreibers angepasst werden kann, müssen in diesen Leitstellen Videobilder von vielen verschiedenen Systemen verarbeitet werden können. Synchron zu den Videobildern sollen auch Schranken gesteuert und Sprechverbindungen geschaltet werden, um etwa im Bedarfsfall bei der Bedienung der Kassenautomaten helfen zu können. Es müssen also nicht nur verschiedene Videosysteme miteinander kombiniert, sondern diese als Gesamtsystem wiederum mit anderen Gewerken (Schrankensteuerung, Sprechanlagen) logisch verknüpft werden.

Vor ähnlichen Herausforderungen stehen Werkschutzorganisationen großer Unternehmen: Auch hier sollen aus Rationalisierungsgründen verschiedene Firmenstandorte von einer zentralen Leitstelle der Werksicherheit überwacht und eventuelle Notfalleinsätze koordiniert werden. Besitzerwechsel und technischer Fortschritt führen auch hier zwangsläufig zu einer heterogenen Landschaft: Selbst wenn im Unternehmen ein bestimmtes Videosystem bevorzugt eingesetzt wird, wäre es unwirtschaftlich, eventuell schon vorhandene Videotechnik einzelner Standorte komplett auszutauschen.

Im Anwendungsfall Werksicherheit ist die Verknüpfung der Videosysteme mit dem Zutrittskontrollsystem essentiell, damit alle Zu- und Abgänge bei Bedarf überprüft und dokumentiert werden können.

Ein weiterer Anwendungsfall, der digitale Vernetzung erfordert, ist die Tag-Nacht-Umschaltung: Während tagsüber der eigene Pförtner die Videoanlage bedient und die Bilder auswertet, wird bei Betriebsschluss mit dem Scharfschalten der Alarmanlage automatisch auch das Videosystem zur nächsten Notruf- und Service-Leitstelle weitergeleitet. So kann im Bedarfsfall weiterhin schnell reagiert werden, ohne dass jeder Standort rund um die Uhr besetzt sein muss.

Die Notruf- und Service-Leitstellen wiederum wollen die Videobilder an die so genannten Blaulichtorganisationen weiterleiten können, um ihren Kunden mehr Sicherheit und schnellere Reaktionen bieten zu können: Wenn der Zentralist mittels Videoüberwachung einen Unfall oder eine Straftat beobachtet, sollen die Bilder zusammen mit allen nötigen Zusatzinformationen (Objektdaten, Lageplan, Maßnahmentexte) möglichst schnell und vollständig zur zuständigen Stelle weitergeleitet werden.

Videobilder können im Ernstfall helfen, Gefahren schneller richtig zu bewerten und die Einsatzkräfte gezielter zu führen. Dazu wäre es aber nötig, dass Rettungsdienste und Polizei potenziell Videobilder von allen am Markt relevanten Videosystemen empfangen und verarbeiten können.

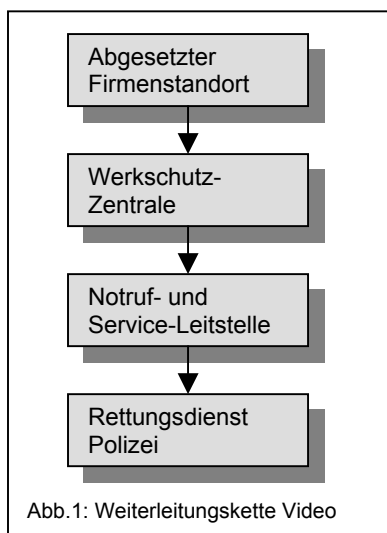


Abb. 1: Weiterleitungskette Video

Spätestens hier ist der Leidensdruck durch die vielen unterschiedlichen Videoformate und Systemeigenschaften so groß, dass folgerichtig die Initiative zum Koordinierungs-Ausschuss Bildübertragung (kurz KA Bild) entstand, der sich genau dieser Problematik widmete

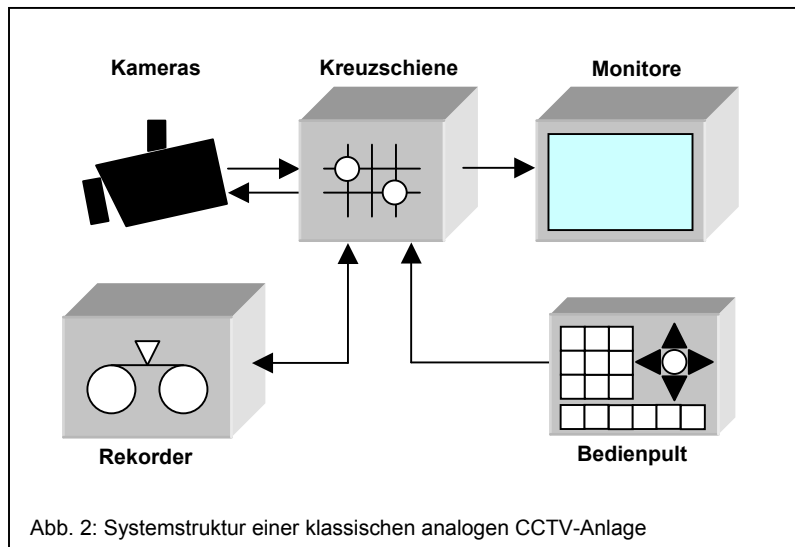


Abb. 2: Systemstruktur einer klassischen analogen CCTV-Anlage

und Empfehlungen dazu erarbeitet hat.

Wie die Beispiele zeigen, sind moderne Videoüberwachungsanlagen heute keineswegs mehr in sich abgeschlossene homogene Anlagen. Vielmehr besteht die Herausforderung darin, bedarfsgerecht Videobilder auch über verschiedene Organisationen und Standorte hinweg austauschen und mit anderen Systemen und Daten verknüpfen zu können.

Systemstruktur (analog)

Bevor die einzelnen Aspekte der Video-Integration behandelt werden, soll zunächst ein Überblick über die Teilkomponenten eines Videoüberwachungssystems gegeben werden. Das klassische analoge CCTV-System besteht aus folgenden aktiven Komponenten:

- Kameras
- Kreuzschiene (Koppelmatrix)
- Monitore
- Rekorder
- Bedienpult

Hinzu kommen passive Teile (Geräteschränke, Verkabelung, Adapter) und Hilfsfunktionen (Signalverstärker und -umsetzer, Bildteiler, Stromversorgung, Beleuchtung, Klimatisierung), auf die nicht näher eingegangen wird.

Als erster Zwischenschritt zum digitalen Videosystem wurden analoge Videorecorder, die in der Regel auf ein Magnetband aufzeichnen, durch digitale Videorecorder (DVR) ersetzt, bei denen die Bilder auf Festplatten gespeichert werden. Dadurch werden auch nonlineare Zugriffe möglich. Das heißt, dass

nicht ein Band der Länge nach durchgespult werden muss, um ein bestimmtes Bild finden und anzeigen zu können, sondern auf jedes Bild kann jederzeit wahlfrei zugegriffen werden.

Wenn der DVR mit einem Netzwerkanschluss ausgestattet wird und es einen passenden Video-Client gibt, also eine PC-Anwendung zur Steuerung des Recorders und zur Auswertung der Bilder, ist ein weiterer Schritt in Richtung Digitalisierung und Vernetzung getan. Ein DVR weist aber immer noch analoge Eingänge zum Anschließen der Kameras auf.

Die Videosignale der Kameras werden in der Regel als Farb-Bild-Austast-Synchron-Signal (FBAS) im PAL-Format über Koaxialkabel übertragen. Bei sehr billigen Geräten sind die Kabel via Cinch-Stecker, bei besseren Geräten mit BNC-Steckern am Gerät angeschlossen, die mittels Verriegelung gegen unbeabsichtigtes Herausziehen gesichert sind.

Zusätzlich bieten viele Kameras Steuereingänge, in einfachen Ausführungen via RS232 etwa zum direkten Anschluss an die serielle Schnittstelle eines PC, in professionellen Umgebungen meist in Form einer RS485-Schnittstelle. Beide Schnittstellen definieren die Signalpegel und den zeitlichen Ablauf der Übertragung elementarer digitaler Daten (Bytes), nicht aber die Bedeutung der übertragenen Daten. Dazu existiert eine Vielzahl herstellerspezifischer Protokolle. Alle Geräte, die Kameras eines bestimmten Herstellers steuern sollen, müssen das jeweilige Protokoll beherrschen.

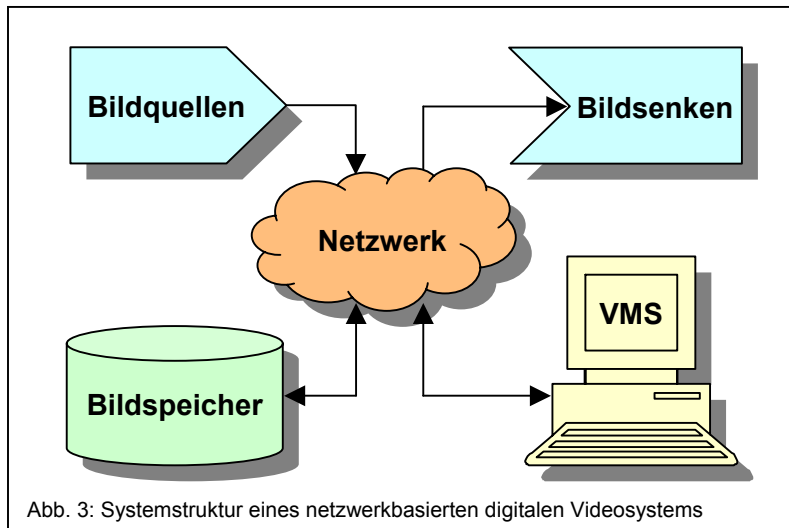


Abb. 3: Systemstruktur eines netzwerkbasierenden digitalen Videosystems

Systemstruktur (digital)

Die Systemstruktur eines modernen digitalen Videosystems weist einige Ähnlichkeiten zum analogen CCTV-System auf, es gibt aber auch wichtige Unterschiede:

An die Stelle der Kameras treten in dieser Struktur die so genannten **Bildquellen**: Damit werden alle Geräte bezeichnet, die Videobilder in das digitale Netzwerk einspeisen. Das können Netzwerk-Kameras sein, aber auch digitale Videorecorder, die über einen Netzwerkanschluss die Bilder mehrerer Kameras gleichzeitig zur Verfügung stellen, oder so genannte Video-Encoder, die analoge Videosignale digitalisieren, komprimieren und im Netzwerk verfügbar machen.

Das Gegenstück zur Bildquelle ist die **Bildsenke**: Dies ist der abstrakte Oberbegriff für alle Geräte, an denen die Videobilder das digitale Netzwerk wieder verlassen. Konkret sind damit alle Geräte gemeint, die digitale Videoströme aus dem Netzwerk so umwandeln, dass sie beispielsweise auf einem Monitor dargestellt werden können (Video-Decoder), oder auch so genannte Video-Clients, Programme, die auf einem PC laufen und die Videobilder dort per Software anzeigen, drucken oder exportieren können.

Der dritte wichtige Funktionsbereich eines digitalen Videosystems ist der **Bildspeicher**. Er kann aktiv als Netzwerk-Videorecorder (NVR) ausgeführt sein: Ein NVR stellt von sich aus Verbindungen zu den Bildquellen her, holt deren Bilder ab und speichert sie. Alternativ kann der Bildspeicher passiv als File-Server etwa in Form eines Network Attached Storage (NAS) oder als

FTP-Server realisiert sein, in den die Bildquellen von sich aus ihre Bilder hineinschreiben. Im Gegensatz zu einem DVR benötigt ein digitaler Bildspeicher keine Videoeingänge mehr, sondern lediglich einen Netzwerkanschluss, der aber ausreichend leistungsstark ausgelegt sein muss (Stichwort Gigabit-Ethernet), da je nach Anwendungsfall sehr viele Zugriffe von verschiedenen Bildquellen und Bildsenken gleichzeitig erfolgen können.

Der letzte und entscheidende Funktionsbereich ist das **Video-Management-System (VMS)**: Von hier aus wird die gesamte Anlage konfiguriert, überwacht und gesteuert. Die grafische Bedienschnittstelle (englisch graphical user interface, kurz GUI) des VMS tritt die Nachfolge des mechanischen Bedienpultes analoger CCTV-Anlagen an. Um die Akzeptanz der Anwender zu gewinnen, ist es vorteilhaft, wenn die GUI möglichst intuitiv zu bedienen ist und die Charakteristik der vertrauten Bedienpulte nachbildet. Insbesondere tief verschachtelte Menü- und Fensterstrukturen, wie sie in PC-Anwendungen beliebt sind, sollten vermieden werden.

Das VMS nutzt die Eigenschaften digitaler Netzwerke, um daraus eine „virtuelle Kreuzschiene“ zu machen: Das VMS steuert, welche Bildquelle ihre Daten zu welcher Bildsenke sendet, welche Bilder aufgezeichnet und welche vom Bildspeicher abgerufen werden. Der Datentransport wird dabei über handelsübliche, in großen Stückzahlen hergestellte und damit preisgünstig verfügbare Netzwerkkomponenten realisiert. Das „Spezialwissen“ über die Erfordernisse und Abläufe im Anwendungsgebiet Videoüberwachung,

also die eigentliche Systemlogik, steckt jedoch vollständig im VMS.

Der Verdrahtungsaufwand digitaler Videosysteme kann bei geschickter Planung gegenüber analogen CCTV-Anlagen erheblich reduziert werden, weil sehr kostengünstig öffentliche Infrastruktur genutzt und viele Videokanäle auf einem Medium gebündelt werden können.

Außerdem ist bei digitalen Systemen die Verdrahtung besser von der Anwendung entkoppelt: Ein digitales Netz kann je nach Bedarf alle nur denkbaren Arten von Daten übertragen, beispielsweise auch Videoformate, die es heute noch gar nicht gibt. Damit sind digitale Systeme zukunftssicherer.

Darüber hinaus zeichnet sich das digitale Netzwerk als verteiltes System durch eine sehr gute Skalierbarkeit aus. Dies meint, dass Umfang und Leistungsfähigkeit der Anlage jederzeit je nach Erfordernis weiter ausgebaut werden können: An jedem Ort, der über einen geeigneten Netzwerkanschluss verfügt, können nachträglich oder temporär zusätzliche Bildquellen oder Bildsenken angeschlossen werden. Damit wird ein Grad von Flexibilität erreicht, wie er bei analogen Videoanlagen undenkbar war.

Viele Bildquellen verfügen nicht nur über Videoeingänge, mit denen Bilder der realen Welt in das Netzwerk eingespeist werden können, sondern auch über zusätzliche Anschlüsse und Funktionen

- zur Kamerasteuerung (Schwenken, Neigen, Zoomen)
- zur Bildanalyse (Videosensorik, Motion-Detection)
- zur ereignisgesteuerten Bildübertragung (Alarmbild)
- für Telemetrie und Fernsteuerung (Licht, Türöffner, Scharfschaltung)
- für Audio (Hören, Sprechen)

sowie über diverse herstellerspezifische Sonderfunktionen.

Auch diese Funktionen müssen im VMS abgebildet werden und darüber bedienbar sein. Bei Auswahl des VMS muss darauf geachtet werden, ob es alle aktuell und möglicherweise künftig an diesem Videosystem angeschlossenen Komponenten der verschiedenen in Frage kommenden Hersteller unterstützt und ob es alle benötigten Funktionen in der zur gewählten Systemstruktur passenden Form bietet.

Systemstruktur (hybrid)

Mindestens für eine Übergangszeit von einigen Jahren werden analoge und digitale Videokomponenten nebeneinander und miteinander Verwendung finden. Auch bei der Erweiterung bereits existierender Video-Anlagen wird es oft wirtschaftlicher sein, vorhandene analoge Komponenten zu integrieren, statt sämtliche Videotechnik auf einen Schlag auszutauschen. Videosysteme, die sowohl analoge als auch digitale Komponenten enthalten, werden als „hybrid“ bezeichnet.

Hybride Videosysteme stellen einen guten Migrationsweg dar, wenn ein vorhandenes analoges Videosystem schrittweise digitalisiert werden soll.

Man spricht beispielsweise von „hybriden Recordern“, wenn Geräte Eigenschaften eines DVR und eines NVR in sich vereinigen, also sowohl FBAS-Eingänge zum direkten Anschließen analoger Kameras vorhanden sind als auch die Bilder von Netzwerkkameras gespeichert werden können. Zahlreiche Hersteller klassischer DVRs bieten mittlerweile diese Kombination an.

Analoge Kameras können auch mittels passender Analog-Digital-Wandler (englisch analog digital converter, kurz ADC) in digitalen Videosystemen weiter verwendet werden. Wenn im ADC neben der reinen Digitalisierung auch noch eine Datenreduktion mittels eines

der vielen Video-Kompressionsverfahren erfolgt, spricht man von einem Video-Encoder. Viele dieser Geräte bieten neben einem oder mehreren FBAS-Eingängen auch Schnittstellen (typisch RS232 oder RS485), mit denen die angeschlossenen Kameras gesteuert werden können. Damit das Gesamtsystem funktioniert, ist darauf zu achten, ob in dem gewählten Video-Encoder bereits das passende Protokoll der daran angeschlossenen Kamera implementiert ist, oder ob die serielle Schnittstelle nur transparent im Netzwerk zur Verfügung gestellt wird; in letzterem Fall müssen die für den speziellen Kameratyp nötigen Protokolle im VMS implementiert werden.

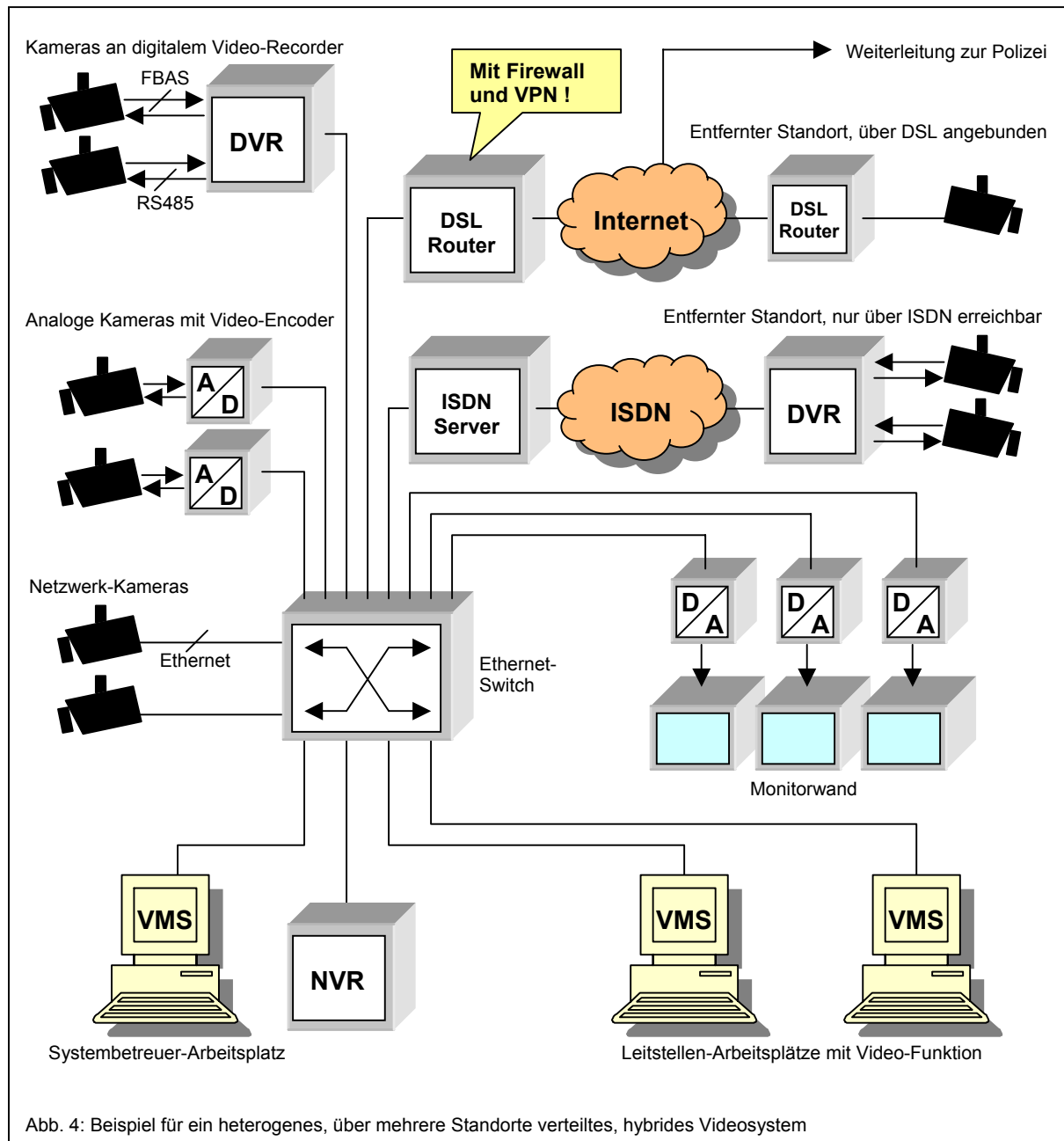


Abb. 4: Beispiel für ein heterogenes, über mehrere Standorte verteiltes, hybrides Videosystem

Datenmengen und Zeitverhalten

Bei der Planung und Realisierung digitaler Videosysteme ist die richtige Auswahl und Konfiguration des Netzwerks von entscheidender Bedeutung, denn die Videoübertragung stellt hohe Anforderungen an das Netzwerk: Große Datenmengen sollen möglichst ohne Zeitverzug übertragen werden.

Um die Problematik anschaulich zu machen: Ein Text im Umfang von einer DIN-A4-Seite erfordert zu seiner digitalen Übertragung ein Datenvolumen von weniger als 5 kByte, ein Videobild in PAL-Auflösung dagegen mehr als 1200 kByte, also mehr als das 250-fache.

für einen Videostream mit 25 PAL-Bildern pro Sekunde in guter Qualität ist immer noch anspruchsvoll für die Auslegung des Netzwerks, denn eine Livebild-Übertragung erfordert nicht nur große Datenmengen, sondern auch ein gutes Zeitverhalten.

Die Kompression und die paketorientierte Datenübertragung, wie sie bei IP-Netzen praktiziert wird, bewirken prinzipbedingt immer einen Zeitversatz zwischen dem Absenden und dem Empfangen der Daten. Dieser Zeitversatz wird als Latenz bezeichnet und sollte idealerweise unter 150ms liegen, damit der Anwender keine Verzögerung etwa bei der Steuerung von

gemacht werden. Das kann dann zu den Videoanlagen führen, von denen die Anwender sagen, die frühere Analogtechnik sei doch viel besser gewesen. Daher sollte man besser schon bei der Planung eines digitalen Videosystems auf die passende Dimensionierung des Netzwerks achten und über geeignete Konzepte zur Eindämmung der Datenflut nachdenken.

Eine Möglichkeit dazu bietet „Intelligenz“ in den Bildquellen: Um die Netze nicht zu überlasten, sollen nur dann Bilder übertragen werden, wenn sie relevante Informationen enthalten. Die Bewertung, wann Bilder relevant sind, ist eine anspruchsvolle Aufgabe, die ausgefeilte Algorithmen und viel Rechenleistung erfordern. Verschiedene Hersteller arbeiten an solchen Lösungen; es ist je nach Anwendungsfall zu prüfen, welche dieser Ansätze passen und ob sie schon ausgereift genug sind, um in der Alltagspraxis einen echten Nutzen zu bringen.

Eine weitere Eindämmung der Datenflut gelingt durch immer ausgefeiltere Kompressionsverfahren, die aber prinzipbedingt auch unerwünschte Eigenschaften bezüglich des Zeitverhaltens oder der Bildqualität mit sich bringen können.

Eine aktuelle Entwicklung ist Scaleable Video Coding (SVC): Dabei werden die Videodaten im Netzwerk in mehreren Teilstreams übertragen, die jeder für sich dekodierbar sind. Durch Kombination der Teilstreams wird die Bildqualität verbessert. Damit kann je nach verfügbarer Bandbreite die bestmögliche Bildqualität erreicht werden.

Es gibt Hersteller von Videosystemen, die eine besondere Kompetenz bei der Übertragung von Video über schmalbandige Netze (ISDN mit 64 kBit/s oder - bei Kanalbündelung mit 2 B-Kanälen - 128 kBit/s, oder Mobilfunk wie GPRS, EDGE, UMTS) entwickelt haben und selbst über solche Netze noch brauchbare Resultate liefern. Andere Hersteller haben sich von vornherein auf breitbandige IP-Netze eingestellt und erzielen damit unter Umständen bessere Ergebnisse als die auf Schmalbandübertragung spezialisierten Hersteller, versagen jedoch, wenn die verfügbare Bandbreite knapp wird. All dies ist bei der Planung eines verteilten Videosystems zu beachten.

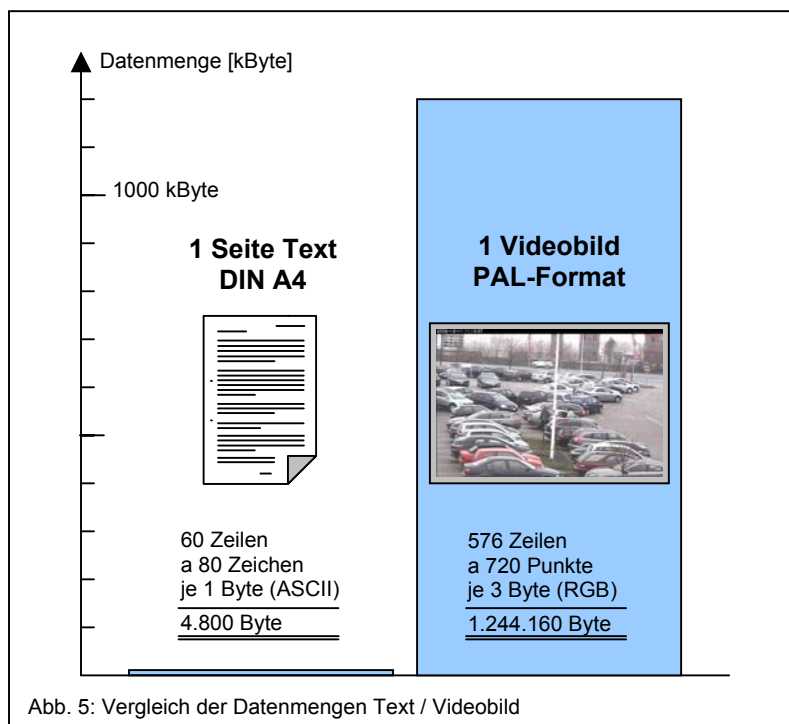


Abb. 5: Vergleich der Datenmengen Text / Videobild

Diese große Datenmenge fällt bei einer Live-Übertragung 25 mal pro Sekunde an. Dies multipliziert mit der Anzahl Kamerabilder, die parallel in eine Leitstelle übertragen werden sollen, ergibt die Gesamtbelastung des Netzwerks mit Videodaten. So etwas würde selbst mit neuesten Netzwerktechnologien schnell an Grenzen stoßen. Deshalb ist die Reduktion der zu übertragenden Datenmenge mittels geeigneter Video-Kompressionsverfahren unerlässlich. Dadurch wird bei Inkaufnahme von mehr oder weniger starken Qualitätseinbußen (Artefakte, verringerte Auflösung oder Bildfrequenz) eine Datenreduktion von 50:1 bis zu 200:1 erreicht.

Der daraus resultierende Datenstrom von beispielsweise 2 MBit/s

Kameras „spürt“. Solche geringen Latenzzeiten erfordern jedoch einen hohen technischen Aufwand und bedingen damit hohe Kosten. Billige Lösungen weisen dagegen meist höhere Latenzzeiten auf. Je nach Anwendungsfall sind daher verschiedene Lösungen wirtschaftlich optimal. Kritisch bezüglich Latenz ist beispielsweise die Verfolgung von Personen mittels Schwenk-Neige-Zoom-Steuerung, Audio bidirektional (Gegensprechen) oder das Betätigen von Schranken und Rolltoren aus der Ferne.

Bei der Datenrate, die ein Netzwerk übertragen kann, spricht man auch von der Bandbreite des Netzwerks. Wenn nicht genügend Bandbreite zur Verfügung steht, müssen Abstriche an Bildqualität und Bildfrequenz

Stichwort Megapixel

Bei analogen Kameras orientiert sich die Bildauflösung (Anzahl der maximal unterscheidbaren Bildpunkte in horizontaler und vertikaler Richtung) meist an den Fernsehstandards PAL (in Deutschland) bzw. NTSC (in den USA). Rein digitale Systeme sind jedoch nicht mehr an diese Formate gebunden. Mit JPEG (genauer JFIF) können beispielsweise alle Bildauflösungen bis maximal 65.536x65.536 Bildpunkte übertragen und gespeichert werden. Einige Hersteller unterstützen Full-HD und HDMI, also Technologien, die aus dem Bereich der Unterhaltungselektronik kommen, andere Hersteller bieten nahezu beliebige andere Auflösungen, von QCIF bis hin zu aktuell 16 Megapixeln (Millionen Bildpunkten).

Welche Bildauflösung optimal ist, muss im Einzelfall geprüft werden, denn hohe Auflösungen erfordern viel Rechenleistung und belasten die Netzwerke - die Bilder kommen dann nicht mehr flüssig, und das Übertragen, Speichern und Nachbearbeiten wird unnötig teuer und langsam. Auch die Lichtempfindlichkeit ist bei Multi-Megapixel-Kameras ein kritisches Thema, weil jeder Bildpunkt ("Pixel") bei gleicher Chipgröße mit einer kleineren Lichtmenge auskommen muss. Außerdem ist eine hohe Megapixelzahl nur dann sinnvoll, wenn Optik und Mechanik darauf abgestimmt sind: Bei vibrierendem Kameramast, minderwertigen Linsen oder ungenauer Brennweite bringt eine hohe Megapixelzahl keinen Vorteil.

Im Gegensatz zum Anwendungsfall "Fernsehen", wo viele Konsumenten im "Broadcast"-Verfahren das gleiche Bildmaterial im gleichen Format auf weitgehend standardisierten Geräten empfangen und es nur darauf ankommt, bei Anzeige des Gesamtbildes eine für das Auge angenehme Darstellung zu erreichen, ist es bei digitalen CCTV-Systemen möglich und je nach Anwendungsfall sinnvoll, mit unterschiedlichen Auflösungen zu arbeiten: Um vor dem Schließen eines Rollltores zu prüfen, ob da eventuell noch ein Kinderwagen steht, genügt eine Festkamera mit geringer Auflösung. Bei der Überwachung eines Kriminalitätsschwerpunktes (beispielsweise Bahnhofsvorplatz) kann dagegen eine hochauflösende Weitwinkel-Kamera durchaus sinnvoll sein, wenn dadurch nachträglich aus den aufgezeichneten Videobildern noch Gesichter oder Kennzeichen herausvergrößert werden können, um einen Täter identifizieren zu können.

Die für solche Anwendungsfälle benötigten Auflösungen liegen deutlich über dem "HD-Format" aus dem Consumer-Bereich, weil hier nicht nur das Gesamtbild betrachtet wird, sondern Ausschnittsvergrößerungen zusätzliche Details liefern sollen. Außerdem bewirkt der technische Fortschritt, dass künftig immer höhere Auflösungen möglich sein werden: Die verfügbare Rechenleistung, der Speicherplatz und die Netzwerkkapazitäten werden voraussichtlich weiterhin exponentiell wachsen. Aber auch dann müssen noch alte Bestandsgeräte mit entsprechend geringeren Auflösungen aufgeschaltet werden können. In der Praxis sind daher Systeme von Vorteil, die variable Bildauflösungen unterstützen und idealerweise dynamisch den jeweiligen Erfordernissen angepasst werden können, beispielsweise mit einer niedrigen Auflösung bei entsprechend hoher Bildfrequenz für schnelle Bewegungen und Kameraschwenks oder mit einer hohen Auflösung unter Inkaufnahme einer langsameren Bildfolge, wenn man Details erkennen will.

Stichwort Unicast - Broadcast - Multicast

Das Internet-Protokoll (IP) kennt 3 mögliche Varianten der Datenzustellung:

Unicast Die Daten eines Senders werden genau einem Empfänger zugestellt. Dies ist die häufigste Form der Datenzustellung. Wollen mehrere Empfänger die gleichen Daten desselben Senders über Unicast empfangen, muss der Sender die Daten mehrfach absenden, was bei einer großen Anzahl von Empfängern sehr ineffizient wird und gegebenenfalls den Sender überlasten kann.

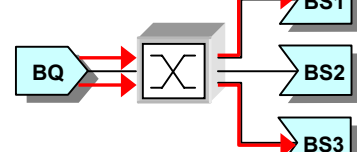
Broadcast Die Daten eines Senders werden allen Empfängern eines Netzwerksegmentes zugestellt, unabhängig davon ob ein Empfänger die Daten benötigt oder nicht. Damit können Daten im Netzwerksegment verteilt werden, ohne dass der Absender die einzelnen Empfänger kennen muss. Anwendungsbeispiel: Ein VMS will alle im Netzwerksegment verfügbaren Bildquellen abfragen, um Kontakt zu ihnen aufnehmen zu können. Broadcast ist nur innerhalb eines Netzwerksegmentes zulässig und möglich, weil sonst das Gesamtnetzwerk von solchen Daten überschwemmt würde. Broadcast ist quasi die Verteilung mit der Gießkanne und eignet sich nicht für eine effiziente Übertragung von Videodaten.

Multicast Die Daten eines Senders werden einer Empfängergruppe zugestellt. Jedes Mitglied der Empfängergruppe abonniert die Daten eines Senders, indem es sich als Gruppenmitglied mit einer speziellen Gruppenkennung per IGMP (Internet Group Management Protocol) beim Netzwerk registriert. Der Sender muss die Daten nur ein Mal senden, die Verteilung an die Abonnennten erfolgt durch die aktiven Netzwerkkomponenten (Switche, Router). Die per Multicast versendeten Daten können auch über Netzwerksegmentgrenzen geroutet werden, sofern multicastfähige Router die Netzwerksegmente koppeln.

Zur Nutzung von Multicast in einem Videonetzwerk müssen Layer-2-Switches, die das Feature "IGMP Snooping" beherrschen, zusammen mit multicastfähigen Routern beziehungsweise multicastfähigen Layer-3-Switches kombiniert werden. Da das Multicasting häufig nicht in jedem Infrastrukturabschnitt zur Verfügung gestellt werden kann, kombinieren moderne digitale Videosysteme geschickt das Unicasting und das Multicasting. Die Daten eines Senders werden dann beispielsweise durch einen RTP-Proxy über Unicast in die Zentrale übertragen und dort per Multicast effizient weiterverteilt.

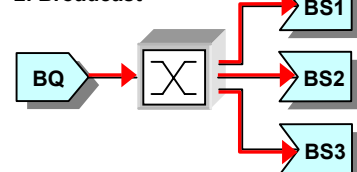
Ob der mit Multicast verbundene Mehraufwand für Infrastruktur und Konfiguration wirtschaftlich ist, hängt vom Anwendungsfall ab: Multicast lohnt sich nur, wenn viele Empfänger exakt zur gleichen Zeit den absolut identischen Datenstrom empfangen wollen.

1. Unicast



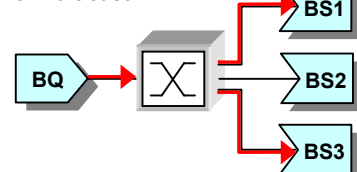
Bildquelle (BQ) muss alle Videobilder 2x senden, wenn sie auf 2 Bildsenken (BS1, BS3) angezeigt werden sollen

2. Broadcast



Bildquelle muss Videobilder nur 1x senden, dafür werden sie auch an Bildsenken gesendet, die sie nicht anzeigen sollen

3. Multicast



Daten werden vom Switch gezielt zu den Bildsenken gesendet, die sich für diese Daten angemeldet haben

Abb. 10: Varianten der Datenzustellung

Aspekte der Video-Integration

Damit Videosysteme verschiedener Hersteller zusammen funktionieren, müssen sie entweder kompatibel sein oder mittels einer geeigneten Software, die Schnittstellen und Datenformate konvertiert, kompatibel gemacht werden.

Wenn im Videobereich von Kompatibilität die Rede ist, wird oft nur über Kompressionsverfahren wie MPEG oder H.264 gesprochen. Daneben gibt es aber eine Vielzahl weiterer Aspekte, die für den reibungslosen Betrieb eines heterogenen Videosystems mindestens genauso wichtig sind:

- Netzwerkverbindung, Protokolle
- Datensicherheit, Authentifizierung
- Bildübertragung, Datenreduktion
- Zeitsynchronisation, Timecodes
- Metadaten
- Kamerasteuerung
- Fernwirken, Telemetrie
- Audio (Hören, Sprechen)
- Aufzeichnung, Recherche
- Ereignis-Übertragung
- Sonderfunktionen

Netzwerkverbindung, Protokolle

Schon beim Netzwerkanschluss und den verwendeten Protokollen unterscheiden sich die angebotenen Videogeräte erheblich. Am weitesten verbreitet ist als Netzwerkanschluss **Ethernet**; weit verbreitet sind 100 MBit/s Datenrate, bei alten Geräten teils nur 10 MBit/s. Die Länge der Netzkabel bis zum nächsten Switch oder Hub ist beim üblichen 100Base-T-Anschluss auf 100 Meter begrenzt, über Lichtwellenleiter (LWL) sind mehrere Kilometer möglich.

Daneben gibt es auch Geräte, die mittels eingebauter **WLAN**-Antenne drahtlos vernetzt werden können. Allerdings muss sich dann in Reichweite (abhängig von den Ausbreitungsbedingungen für die Funksignale etwa 5-300 Meter) ein passender WLAN-Access-Point befinden. Ab da geht es dann meistens mit Ethernet weiter.

Wieder andere Videogeräte arbeiten mit **Mobilfunk** (GSM, UMTS), um auch über größere Entfernungen

Stichwort LAN - WAN

Von einem „Local Area Network“ (LAN) spricht man, wenn es nur um kurze Entfernungen geht, in der Regel innerhalb eines Grundstücks. Typische Übertragungstechnologien im LAN sind:

- Ethernet
- WLAN

„Wide Area Network“ (WAN) steht für Datennetze, die große Entfernungen überbrücken. Das WAN wird in der Regel von „Providern“ (beispielsweise der Deutschen Telekom AG) bereitgestellt. Technologien für WAN sind

- ISDN
- DSL
- GSM (GPRS, EDGE)
- UMTS (HSDPA, HSUPA)

Die Verbindung zwischen LAN und WAN wird über „Router“ hergestellt: Kann eine Adresse innerhalb eines Netzes nicht gefunden werden, so vermittelt der Router die Verbindung automatisch in das nächste Netz.

und bei mobilen Anwendungen drahtlose Verbindungen zu ermöglichen. Allerdings ist bei diesen Übertragungstechnologien die verfügbare Netzwerkbandbreite vergleichsweise gering und schwankt abhängig von der Anzahl der Teilnehmer in der Funkzelle und den Ausbreitungsbedingungen für die Funkwellen. Neben unabsichtlichen Störungen durch andere elektrische Geräte muss beim Sicherheitskonzept auch damit gerechnet werden, dass Funkverbindungen absichtlich gestört werden können, um eine Beobachtung zu verhindern. Hinzu kommen vergleichsweise hohe Kosten für den Datentransfer.

Ebenfalls mit kleinen Bandbreiten (64 kBit/s bzw. 128 kBit/s bei Kanalbündelung) müssen Videogeräte auskommen, die ihre Bilder über **ISDN** übertragen. ISDN wird zwar nach und nach abgelöst, spielt bei Bestandsanlagen aber immer noch eine Rolle. Es sind grundsätzlich zwei Arten zu unterscheiden, wie Video über ISDN übertragen werden kann:

1. IP über ISDN: Wie bei allen vorgenannten Verfahren wird auch hier IP (Internet Protocol) als grundlegendes Protokoll genutzt. Damit können Daten in den höheren Protokollschichten immer in gleicher Weise übertragen werden, unabhängig von der Art der physikalischen Verbindung (Ethernet, WLAN, DSL, UMTS oder eben ISDN). Um IP-Datenpakete über ISDN zu übertragen, müssen sie ins PPP (Point to Point Protocol) „einge-



Abb. 6: Eine kleine Auswahl von Videogeräten, die typischerweise vom VMS integriert werden müssen...

packt“ werden. Dies kann ein ISDN-Router erledigen; dafür müssen alle benötigten Verbindungen im Router konfiguriert werden. Komfortabler geht es mit DFÜ-Verbindungen, die direkt auf dem PC konfiguriert werden können, auf dem auch das VMS läuft. Bei Anlagen mit mehreren Bedienplätzen setzt das einen ISDN-Server mit Remote-CAPI voraus. CAPI steht als Abkürzung für „Common Application Programming Interface“ und ist die Standard-Programmierschnittstelle für ISDN-Anwendungen. Aktuell ist die Version CAPI 2.0. Mittels Remote Access Service (RAS) kann ein VMS die DFÜ-Verbindungen dynamisch verwalten, also je nach Bedarf anlegen, so dass die Verbindungsdaten zentral gepflegt werden können. Soll dies auch für eingehende Verbindungen oder für mehrere Verbindungen von einem PC aus möglich sein, um beispielsweise gleichzeitig die Videobilder verschiedener ISDN-Gegenstellen auf einem Bedienplatz empfangen zu können, wird ein CAPI-WAN-Treiber benötigt, der vom VMS konfiguriert und gesteuert werden kann und auf Anforderung mehrere PPP-Verbindungen über ISDN bereitstellt. All dies ist bei der Auswahl des VMS zu beachten.

2. Native ISDN: Durch direkten Zugriff auf die CAPI-Schnittstelle kann der Datenfluss besser kontrolliert und eine geringere Latenz erreicht werden. Deshalb versenden einige Videogeräte die Bilder mittels proprietärer Protokolle direkt über ISDN. Der Preis dafür ist, dass die entsprechenden Schnittstellen und Protokolle im VMS verfügbar sein müssen. Dies ist vor dem Einsatz solcher Geräte zu prüfen.

Datensicherheit

Eng verbunden mit dem Thema Netzwerk ist das Thema Datensicherheit: Sollen über WAN entfernte Bildquellen aufgeschaltet werden, sind Verbindungen nach außen nötig; damit besteht aber prinzipiell auch das Risiko von unberechtigten Zugriffen. Dieses Risiko muss durch geeignete Maßnahmen eingegrenzt werden.

Planung, Installation und Administration eines Netzwerks erfordert daher ein hohes Maß an Kompetenz und Zuverlässigkeit. Mögliche Sicherheitslücken müssen rechtzeitig erkannt und geschlossen werden. Grundlegende Regeln und Empfehlungen zur Sicherheit in digi-

talenen Netzen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter www.bsi.de.

Eine erste Maßnahme zur Erhöhung der Datensicherheit kann sein, für die Videoüberwachung ein separates Netzwerk einzurichten. Dies erfordert nicht unbedingt ein eigenes Leitungsnetz, sondern kann auch in Form eines Virtual Local Area Network (VLAN) realisiert werden: Video und Geschäftsdaten bleiben dann sauber getrennt, selbst wenn sie über die gleichen Leitungen übertragen werden.

Bei Verbindungen über das Internet ist ein Virtual Private Network (VPN) empfehlenswert: Die Daten werden dabei verschlüsselt übertragen und können somit auf ihrem Weg durch das Internet nicht von Unbefugten abgegriffen oder unbemerkt manipuliert werden.

An jedem Netzwerkzugang sollte eine Firewall selbstverständlich sein, die nur solche Verbindungen zulässt, die vom Betreiber der Anlage ausdrücklich erwünscht sind.

Das VMS und die Bildquellen sollten Zugriffe nur nach **Authentifizierung** zulassen, also wenn ein gültiger Benutzername und das zugehörige Passwort eingegeben wurden. Unter Datenschutzgesichtspunkten kann auch das 4-Augen-Prinzip zum Tragen kommen, bei dem zwei verschiedene Passwörter abgefragt werden, bevor man Zugang zu vertraulichen Daten erhält. Die Authentifizierungsverfahren der Bildquellen unterscheiden sich zum Teil sowohl im Ablauf als auch im Sicherheitsniveau erheblich.

Bildübertragung, Datenreduktion

Wie bereits erläutert, müssen die Videobilder zum effizienten Übertragen und Speichern komprimiert werden. Eines der ältesten und am weitesten verbreiteten Kompressionsverfahren für Videobilder ist JPEG. Bilder in diesem Format können auf allen PCs und von sehr vielen Programmen direkt angezeigt und verarbeitet werden.

Im Laufe der Zeit wurde eine Vielzahl weiterer Kompressionsverfahren entwickelt, die vor allem eine höhere Datenreduktion zum Ziel hatten. Die Hersteller stehen im Wettbewerb darum, wer mit seinen Geräten bei begrenzter Bandbreite die bestmögliche Bildqualität und Bildfrequenz erzielt. Daher bringen sie immer neue Verfahren auf den Markt.

Es gibt nur wenige Video-Management-Systeme, die Bilder in allen marktüblichen Verfahren empfangen und weiterverarbeiten können, denn es ist ein erheblicher Entwicklungsaufwand nötig, um alle diese Verfahren zu berücksichtigen, und es kommen laufend neue hinzu.

Einige Hersteller haben eigene Kompressionsverfahren speziell für die Videoüberwachung entwickelt, die meisten Hersteller übernehmen jedoch Kompressionsverfahren aus anderen Anwendungsbereichen. Da bei der Videoüberwachung aber andere Anforderungen bestehen als etwa beim Fernsehen oder bei Spielfilmen, müssen diese Verfahren gegebenenfalls angepasst oder zumindest geeignet parametrisiert werden.

Stichwort CBR - VBR

Wenn Kompressionsverfahren aus anderen Branchen für die Videoüberwachung genutzt werden sollen, sind einige Besonderheiten zu beachten:

Bei digitalem Fernsehen wird eine konstante Datenübertragungsrate (constant bit rate: CBR) angestrebt, da der Übertragungskanal (TV-Sender) eine fest definierte Bandbreite hat, die vollständig zur Übertragung der Bilder genutzt werden soll. Die Bilder des Fernsehprogramms ändern sich häufig, und die Zuschauer akzeptieren meist, dass bei besonders schnellen Bewegungen das Bild kurzzeitig etwas unschärfer wird.

Bei Videoüberwachung passiert dagegen in der meisten Zeit nichts; man könnte also zur Übertragung der sich kaum verändernden Bilder, die wenig neue Informationen enthalten, mit einer weit geringeren Übertragungsrate auskommen. Nur genau dann, wenn der Täter für kurze Zeit durch das Bild läuft, in der Szene also viel Bewegung stattfindet und die Informationsmenge, die für eine detaillierte Darstellung dieser Bilder nötig ist, sehr groß wird, soll die Übertragungsrate sprunghaft ansteigen: Die Bilder, auf denen sich der Täter durch das Objekt bewegt, sollen mit der größtmöglichen Detailtreue (also mit erhöhter Datenrate) übertragen werden. Bei Videoüberwachungsanlagen, bei denen sich die Videoströme mehrerer Kameras die verfügbare Bandbreite eines Netzes teilen, ist also nicht CBR, sondern VBR (variable bit rate) optimal.

Bei modernen Videokompressionsverfahren wie MPEG4 und H.264 kann konfiguriert werden, ob sie mit CBR oder VBR arbeiten. Der Errichter muss nur darauf achten, dass die von ihm verwendeten Geräte VBR unterstützen und dass er dies korrekt konfiguriert, weil die Anlage sonst ausgerechnet in den kritischen Momenten nur unscharfe Bilder liefert: dann gibt es kein brauchbares Fahndungsbild...

Stichwort GOP-Struktur

Im Consumer-Bereich geht es darum, Spielfilme mit möglichst wenig Daten zu speichern. Dazu wird ausgenutzt, dass zeitlich aufeinander folgende Bilder sich oft sehr ähnlich sind. Man kann viel Speicherplatz sparen, indem man nur die Differenz der Bildinformation zu vorangegangenen oder nachfolgenden Bildern speichert.

Die zu komprimierenden Einzelbilder können dazu in folgenden „Frame“-Typen gespeichert werden:

- **I:** enthält 1 Bild vollständig
- **P:** enthält nur die Differenz zum vorangehenden I- oder P-Frame.
- **B:** Differenz zu vorangehendem und nachfolgendem I- oder P-Frame.

Die sich wiederholende Abfolge dieser Frames wird als GOP-Struktur bezeichnet. GOP steht als Abkürzung für englisch „group of pictures“. Sie bestimmt maßgeblich die Eigenschaften eines Kompressionsverfahrens.

Bei JPEG gibt es nur I-Frames: Jeder Frame enthält die volle Bildinformation und kann auch dann korrekt dargestellt werden, wenn vorangegangene Frames gelöscht oder gestört wurden.

Bei Videokompression im Consumer-Bereich werden auch B-Frames intensiv genutzt, denn damit lassen sich die höchsten Kompressionsraten erzielen. Dies bewirkt allerdings auch eine prinzipielle Latenz, weil erst alle Bilder bis zum nächsten I- oder P-Frame abgewartet werden müssen, bevor die dazwischen liegenden B-Frames berechnet werden können.

Bei CCTV-Anwendungen mit Echtzeitanforderungen sollten daher keine B-Frames verwendet werden.

Bei begrenzter Netzwerkbandbreite ist es außerdem von Vorteil, wenn die Bildquelle je nach Anforderung verschiedene Bildfrequenzen und Bildauflösungen liefern kann: Bei Kameraschwenks oder schnellen Bewegungen wird auf eine reduzierte Auflösung umgeschaltet, um eine schnellere Bildfolge zu erreichen; wenn es auf Details ankommt (Kennzeichen, Gesichter), wird zugunsten einer besseren Auflösung die Frequenz reduziert.

Viele der neuen Kompressions-Verfahren geben nur einen Rahmen vor, innerhalb dessen unterschiedliche Umsetzungen (Implementierungen) möglich sind: So können sich, wo MPEG-4 draufsteht, in der Praxis durchaus je nach Hersteller abhängig von der verfügbaren Rechenleistung und den konkret implementierten Algorithmen sehr unterschiedliche Eigenschaften hinsichtlich Bildqualität, Kompressionsrate und Bildfrequenz ergeben. Das macht es dem Errichter und Betreiber nicht gerade leicht, die jeweils passende Auswahl zu treffen.

Zeitsynchronisation, Timecodes

Sehr viel überschaubarer sind die empfohlenen Verfahren zur Zeitsynchronisation; dennoch wird dieses Thema leider oft vernachlässigt.

Nur wenn alle an einem Videosystem beteiligten Komponenten mit der gleichen Zeitbasis arbeiten, ist eine zeitrichtige Auswertung der Bilder möglich. In der Praxis wird aber beispielsweise bei DVRs in manchen Geldautomaten über Monate die Systemzeit nicht justiert; da können Abweichungen in der Größenordnung von vielen Stunden auflaufen.

Solange der DVR nur als abgeschlossenes System betrachtet wird, stimmt wenigstens die zeitliche Reihenfolge der Bilder. Spätestens bei der Verknüpfung mit anderen Videosystemen passt aber nichts mehr zusammen: Wenn man einen komplexen Tathergang rekonstruieren will und dazu nicht nur Bilder des Geldautomaten, sondern auch der Foyer- und Kassenkameras oder sogar aus dem Außenbereich (Fußgängerzone, Parkhaus) hinzuziehen will, um beispielsweise das Kennzeichen des Fahrzeugs zu ermitteln, das der Täter benutzt, wird die Auswertung massiv erschwert, wenn die Bilder der verschiedenen Kameras nicht mit der gleichen Zeitbasis gespeichert wurden.

Dabei ist es eigentlich ganz einfach: In Deutschland gilt die „Gesetzliche Normalzeit“, die von der Physikalisch Technischen Bundesanstalt (PTB) in Braunschweig zur Verfügung gestellt wird (www.ptb.de).

Sofern eine Netzwerk-Verbindung besteht, kann die Zeitbasis mittels Network Time Protocol (NTP) empfangen und weitergegeben werden. Alle Videokomponenten sollten deshalb NTP unterstützen und müssen fachgerecht konfiguriert werden, damit sie jederzeit mit der Normalzeit synchron laufen.

An Standorten ohne Online-Zugang kann die Uhrzeit über das Funkuhrsignal DCF-77 oder das Satellitensignal des GPS (Global Positioning System) empfangen werden; passende Empfänger für PCs sind am Markt erhältlich. Von da aus kann die Zeit mittels NTP an weitere im LAN angeschlossene Geräte weitergegeben werden: Ein PC mit Funkuhr-Empfänger dient dann als lokaler Zeitserver.

Damit kann die Zeitabweichung der beteiligten Systeme dauerhaft unter einer Sekunde gehalten werden; das ist für die typischen Anwendungsfälle im Sicherheitsbereich vollkommen ausreichend.

Sofern Bildquellen verwendet werden, die kein NTP beherrschen und an die auch kein Funkuhrempfänger angeschlossen werden kann, muss geklärt werden, wie hier die Zeit synchronisiert werden kann. Einige Bildquellen sehen andere Möglichkeiten zur Zeitsynchronisation vor, die dann aber auch vom VMS unterstützt werden müssen (siehe Abschnitt „Sonderfunktionen“).

Nun ist noch auf die Problematik der verschiedenen **Zeitzone**n und der **Sommerzeitumstellung** zu achten: Da Leitstellen heute mittels

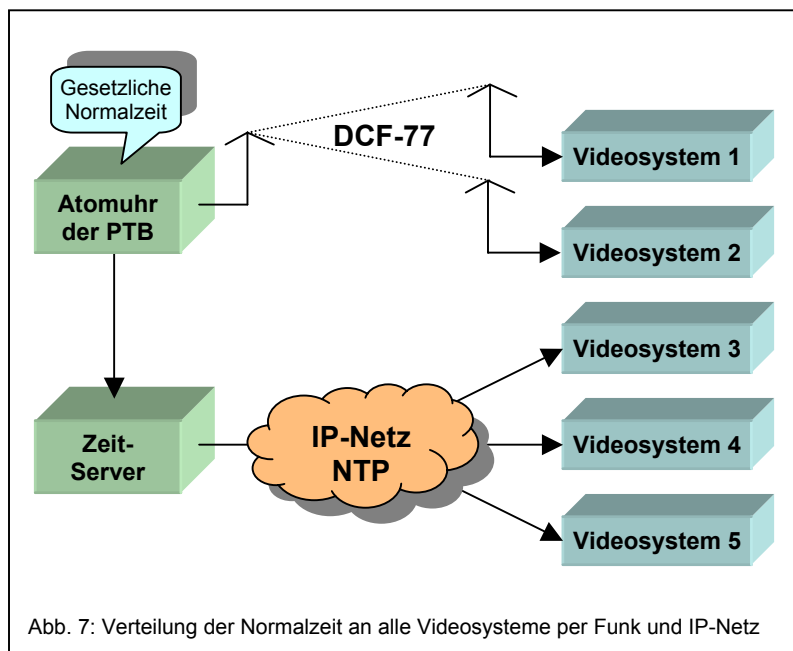


Abb. 7: Verteilung der Normalzeit an alle Videosysteme per Funk und IP-Netz

IP-Technik oft auch Überwachungsaufgaben in entfernten Regionen wahrnehmen (zum Beispiel das Ferienhaus eines Kunden in Spanien), laufen die angeschlossenen Bildquellen eventuell in verschiedenen Zeitzonen. Damit die Zeitangaben dennoch einheitlich und eindeutig sind, sollten sie systemintern auf jeden Fall in „Koordinierter Weltzeit“ (UTC) übertragen und gespeichert werden und erst bei der Anzeige in die jeweils passende Zeitzone (Lokalzeit) umgerechnet werden. Damit vermeidet man auch die Probleme, die sich sonst im Zuge der Sommerzeitumstellung ergeben würden: Wenn im Herbst die Uhr eine Stunde zurückgestellt wird, ist die Lokalzeit nicht eindeutig; nur die Weltzeit bietet eine kontinuierliche eindeutige Zeit. Es empfiehlt sich daher zu prüfen, ob ein Videosystem UTC beherrscht und wie es für die benötigten Zeitzonen konfiguriert werden kann.

Damit die einzelnen Bilder bei der Anzeige und späteren Auswertung richtig zugeordnet werden können, erhält jedes Bild einen Zeitstempel (engl. timecode), der zusammen mit dem Bild übertragen und gespeichert werden sollte. Auch hier empfiehlt sich UTC als Zeitbasis, um von Zeitzonen oder Sommerzeitumstellungen unabhängig zu bleiben. Die Timecodes spielen eine wichtige Rolle für die Auswertung, denn nur anhand der Timecodes kann jedes Bild auf der Zeitleiste (timeline) korrekt eingeordnet werden. Ob und in welcher Form Bildquellen Timecodes zur Verfügung stellen, unterscheidet sich sehr und muss im Rahmen des Systemkonzepts berücksichtigt werden.

Metadaten

Ein erstes Beispiel für Metadaten liefern bereits die eben besprochenen Timecodes. Allgemein werden im Kontext von CCTV unter Metadaten alle Arten von Zusatzinformationen verstanden, die sich auf die Videobilder beziehen.

Metadaten können in separaten Textdateien, in Datenbanken, in speziellen Abschnitten innerhalb der Videodateien oder im Dateinamen der Videodaten gespeichert werden. Die beiden letztgenannten Möglichkeiten haben den Vorteil, dass die Metadaten fest mit den Videodaten verbunden sind und auch beim Verschieben oder Kopieren von Videodateien nicht verloren gehen. Timecodes werden daher oft direkt

in den Dateinamen der jeweiligen Videodatei eincodiert. Dann kann man schon am Dateinamen erkennen, von welchem Zeitpunkt die Bilder stammen.

Weitere Beispiele für Metadaten sind Transaktions-Nummern von Bankautomaten und Kassensystemen oder Paketnummern in der Logistik: Sie dienen dazu, später gezielt die zu einem bestimmten Vorgang gehörenden Videobilder abrufen zu können.

Die Bildquellen unterscheiden sich erheblich, in welchem Umfang und in welcher Form sie Metadaten liefern. Dies hängt davon ab, für welche Zielgruppen und Branchen sie entwickelt wurden. Im einfachsten Fall werden die Metadaten direkt in das Videobild eingeblendet.

Metadaten können aber auch unabhängig von der Bildquelle nachträglich erzeugt werden: Vom VMS einheitlich gespeicherte Bilder werden dazu mittels Bildanalyse-Software nach Texten oder bestimmten Objekten durchsucht, die als Metadaten gespeichert werden. Weitere Metadaten können vom VMS aus anderen Management-Systemen übernommen und den Bildern hinzugefügt werden.

Metadaten können auch manuell eingegeben werden. Als Beispiel dafür seien Bildnotizen genannt: Die Sicherheitsfachkraft kann zu jedem Bild ihre Beobachtungen eintragen. Anhand dieser Texte kann später ein bestimmtes Bild schnell wieder aufgefunden werden, indem nach Textfragmenten gesucht wird. Die Bildnotizen werden zusammen mit dem Bild ausgedruckt und exportiert, so dass sie auch bei weiteren Verarbeitungsschritten zur Verfügung stehen.

Metadaten spielen eine große Rolle bei der Verknüpfung verschiedener Gewerke und der Automatisierung von Arbeitsabläufen. Daher sollte diesem Thema beim Systemkonzept ausreichend Aufmerksamkeit gewidmet werden.

Kamerasteuerung

Die Grundfunktionen der Kamerasteuerung sind

- **Schwenken**
- **Neigen**
- **Zoomen**

abgekürzt mit SNZ, oder auf englisch pan - tilt - zoom (PTZ). Es ist darauf zu achten, ob jeweils nur

in festen Schrittweiten (steps) oder kontinuierlich geschwenkt und gezoomt werden kann, eventuell sogar mit einstellbarer oder automatisch angepasster Geschwindigkeit. Manche neuere Bildquellen bieten auch Auto-Tracking: Ein einmal ins Visier genommenes Objekt wird von der Kamera automatisch verfolgt.

Bei Steuerung mit der Maus sind Kameras nützlich, die „absolut“ positioniert werden können: Der interessante Bildausschnitt wird im Videobild mit der Maus angeklickt, worauf die Kamera exakt auf diese Position hin zentriert wird; durch Drehen am Mausekranz kann dieser Bildausschnitt vergrößert werden, um Details (ein Kennzeichen, ein Gesicht) genauer erkennen zu können. Bei digitalen CCTV-Anlagen mit ihrer systembedingten Latenz ist diese Art der Steuerung wesentlich schneller und präziser als beispielsweise eine Steuerung über Joystick.

Unter Presets versteht man vordefinierte Positionen, die nach Auswahl aus einer Liste von der Kamera angefahren werden. Bei CCTV-Anlagen mit großer Latenz ist dies das Mittel der Wahl, um überhaupt eine praktikable Kamerasteuerung zu ermöglichen.

Manche Kameras erlauben zusätzlich die Steuerung von

- **Iris:** Blende, steuert die Lichtmenge und damit die Helligkeit
- **Focus:** Brennweite, beeinflusst die Schärfe des Bildes.

In den meisten Fällen werden jedoch automatische Blenden und Autofocus zum Einsatz kommen, weil das Leitstellenpersonal mehr mit anderen Aufgaben beschäftigt ist, als dass es diese Parameter in aller Feinheit regeln könnte. Bei billigen Produkten sind Iris und Focus ohnehin fest, was aber unter- oder überbelichtete sowie unscharfe Bilder zur Folge haben kann.

Weitere mögliche Funktionen aus dem Bereich Kamerasteuerung sind bei hochwertigen Kameras im Außenbereich Wischer und Heizung, eventuell kann für die Nachtsicht auch eine Infrarot-Beleuchtung und ein Infrarot-Filter geschaltet werden.

Bei Auswahl der Bildquellen und des VMS ist darauf zu achten, dass alle benötigten Funktionen durchgängig unterstützt werden: Es nützt wenig, hochwertige Kameras einzusetzen, wenn deren Funktionen nicht angesteuert werden können.

Fernwirken (Fernsteuerung)

Fernwirken meint, dass von der Leitstelle aus über die Kamera hinaus weitere Funktionen im überwachten Objekt gesteuert werden können. Dazu bieten viele Bildquellen einen oder mehrere digitale Schaltausgänge, mit denen

- Licht
- Türöffner
- Schranken, Rolltore
- Alarmanlage (Scharfschaltung)
- Sirenen, Blitzlampen
- Vernebelungsanlagen

und weitere Funktionen im überwachten Objekt geschaltet werden können. Damit kann die Leitstelle ihren Kunden über die Video-Beobachtung hinaus weitere Dienstleistungen bieten.

Es gibt verschiedene elektrische Ausführungen der Schaltausgänge. Üblich sind

- TTL-Pegel
- Open-Collector-Ausgänge
- Opto-Koppler
- Relais (öffnend oder schließend)

Beim Anschließen der zu steuernden Geräte durch den Errichter muss deshalb genau auf passende Anschlusswerte geachtet werden.

Auch für die Steuerungslogik gibt es je Hersteller und Anwendungsfall unterschiedliche Konzepte:

- bistabil: Ausgang kann wahlweise an oder aus geschaltet werden
- togelnd: Jede Betätigung wechselt den Zustand des Ausgangs
- monostabil: Eine gewisse Zeit nach der Betätigung wechselt der Schaltausgang automatisch wieder in die Ruhestellung.

Der aktuelle Zustand eines Ausgangs sollte an die Leitstelle zurückgemeldet werden. Das ist leider nicht bei allen Geräten der Fall.

Der Errichter, der die Anlage im überwachten Objekt installiert, verbindet die Schaltausgänge der Bildquelle mit den entsprechenden Einrichtungen. Alle Verbindungen muss er an die Leitstelle melden, damit dort das Management-System entsprechend konfiguriert werden kann. Aus Sicht der Bildquelle gibt es z.B. „Schaltausgang 3“; die Bildquelle kann bei einfachen digitalen Schaltausgängen nicht wissen, was für ein Gerät an Ausgang 3 angeschlossen ist. Die Problematik wird deutlich, wenn man sich vorstellt, dass der Zentralist mangels dieser Information statt des Türöffners die Sprinkleranlage betätigt.

Telemetrie

Telemetrie meint jede Form der Übertragung von Messwerten vom überwachten Objekt in die Leitstelle. Das kann ein einfacher digitaler Eingang sein, der nur „0“ oder „1“ meldet (beispielsweise den Scharfschaltzustand der Alarmanlage oder einen Türkontakt), oder auch eine Wetterstation, die umfangreiche Daten vom überwachten Gelände liefert. In welchem Umfang und in welcher Form die Bildquellen Telemetrie unterstützen, ist sehr unterschiedlich. Weit verbreitet und sehr universell sind transparente serielle Schnittstellen, mit denen auf Seiten der Objekte eine Vielzahl verschiedener Geräte angeschlossen werden kann. Im VMS müssen die zu diesen Geräten passenden Protokolle implementiert werden.

Audio

Viele Bildquellen enthalten auch mehr oder weniger umfangreiche Audiofunktionen. In Verbindung mit einer CCTV-Anlage gibt es dafür folgende typische Gründe:

1. um das Objekt nicht nur optisch, sondern auch **akustisch überwachen** zu können und so einen schnelleren und umfassenderen Überblick über die Gefahrenlage zu erhalten,
2. um **Durchsagen** in das Objekt machen zu können, um dort befindliche Personen zu warnen oder Täter abzuschrecken,
3. um ein **Gespräch** mit der beobachteten Person aufnehmen zu können und beispielsweise Hilfestellung bei der Bedienung eines Automaten leisten zu können.

Bei Audio-Verbindungen sind aus Sicht der Leitstelle folgende Betriebsarten möglich:

- nur Hören (Überwachung)
- nur Sprechen (Durchsagen)
- vorgefertigte Ansagen
- Wechselsprechen
- Gegensprechen
- Freisprechen

Die akustische Überwachung kann auch in der Form genutzt werden, dass bei bestimmten Geräuschen Alarme ausgelöst werden.

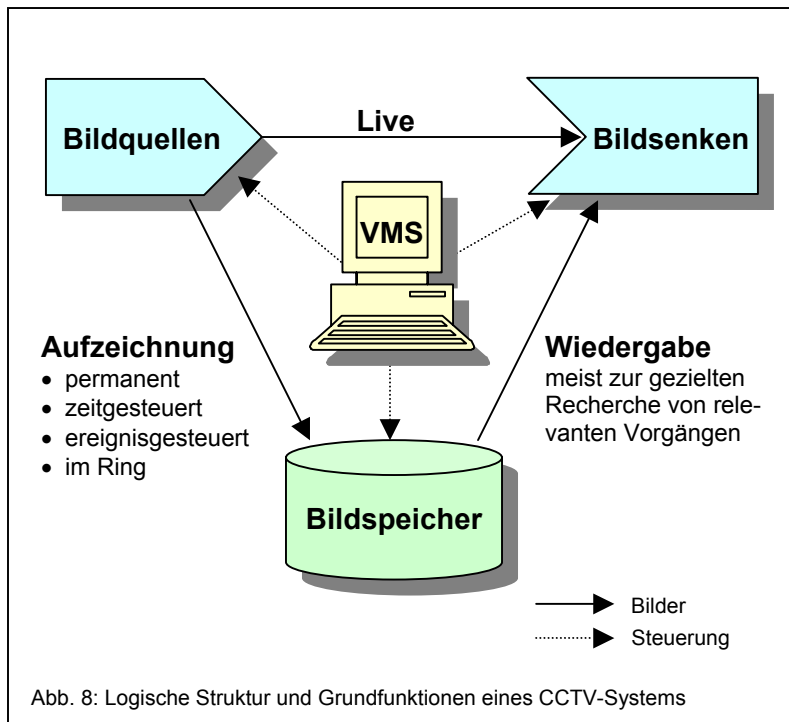
Beim **Wechselsprechen** wird abwechselnd gehört und gesprochen; das VMS muss passende Bedienelemente bieten, um dazwischen umschalten zu können. Beim **Gegensprechen** kann gleichzeitig gesprochen und gehört werden.

Dies bedeutet aber auch, dass die Leitstelle das, was sie selbst sagt, nach einer gewissen Verzögerungszeit (englisch delay), die von der Netzwerk-Latenz abhängt, als Echo hört. Dies kann die Kommunikation erheblich beeinträchtigen. Deshalb muss bei dieser Betriebsart für eine ausreichende akustische Entkopplung zwischen Mikrofon und Lautsprecher gesorgt werden. Auf Seiten der Leitstelle kann dies mit einem so genannten Headset erfolgen, einem Kopfhörer mit daran angebrachtem Mikrofon.

Das **Freisprechen** ist eine Sonderform des Gegensprechens, bei der versucht wird, ohne Kopfhörer auszukommen, um den Gesprächspartnern mehr Bewegungsfreiheit zu bieten. In diesem Fall ist keine akustische Entkopplung mehr gegeben, sondern es wird durch schaltungstechnische Maßnahmen in der Sprechstelle (Echokompensation) dafür gesorgt, dass das selbst akustisch ausgegebene Signal nicht wieder über den Mikrofonweg an die Gegenstelle zurückgesendet wird. Je nach den örtlichen akustischen Verhältnissen funktioniert das mehr oder weniger gut.

Als Sonderform der Durchsagen können auch vorgefertigte Ansagen abgespielt werden. Sofern diese in der Bildquelle gespeichert wurden, kann auf diese Weise Netzwerkbandbreite zur Übertragung der Audiosignale gespart werden. Außerdem sind diese Ansagen frei von Nebengeräuschen, die sonst bei Ansagen über das Mikrofon in einer stark frequentierten Leitstelle leicht auftreten können. Das VMS muss eine Liste der verfügbaren Ansagetexte zur Auswahl bereitstellen, aus der je nach Situation die passende Ansage gewählt werden kann.

Für die Sprachübertragung über digitale Netze (englisch: voice over internet protocol, VoIP) gibt es eine Fülle verschiedener Formate und Standards: Zur Steuerung der Verbindungen (Signalisierung) sind SIP und H.323 verbreitet, für die Kodierung der Audiodaten G.711, G.728 und andere. Einige Bildquellenhersteller verwenden auch eigene (proprietäre) Verfahren zur Audioübertragung. Es bestehen große Unterschiede bezüglich Qualität und Bandbreitenbedarf. In einem heterogenen Videosystem muss das VMS alle gängigen Formate empfangen und steuern können.



Aufzeichnung, Recherche

Zur Aufzeichnung der Videobilder dienen Bildspeicher. Diese können zentral (etwa in der Leitstelle), dezentral (in den Bildquellen) oder auch verteilt realisiert sein. Wenn alle Bildquellen permanent in der Zentrale aufzeichnen, wird das Netz von der Fülle der gleichzeitig zu übertragenden Videostreams sehr beansprucht. Daher empfiehlt es sich, Langzeit-Aufzeichnungen nahe der Bildquelle vorzunehmen, zum Beispiel mit einem DVR. Damit der Bildspeicher im Dauerbetrieb nicht überläuft, wird er oft als Ringspeicher organisiert: Nach einer konfigurierbaren Zeit werden die Bilder wieder gelöscht, um Platz für neue Bilder zu schaffen.

Eine Übertragung und Aufzeichnung in der Leitstelle erfolgt bei diesem verteilten Speicherkonzept nur im Bedarfsfall, zum Beispiel bei erkannten Bewegungen oder ausgelösten Alarmen. Wenn sich bei der Auswertung dieser Bilder herausstellen sollte, dass weitere Bilder benötigt werden, die noch nicht in der Zentrale gespeichert wurden, so können diese mittels Video-Recherche von den dezentralen Bildspeichern abgerufen werden.

Mit Recherche ist die Suche nach bestimmten Videobildern gemeint. Dies ist bei CCTV-Systemen der häufigste Anwendungsfall für die Wiedergabe von aufgezeichneten Bildern. Die Suche erfolgt entweder anhand der Timecodes nach dem

Bild einer bestimmten Kamera und eines bestimmten Zeitpunkts, nach bestimmten Bildinhalten (mittels Bildanalysesoftware) oder anhand der Metadaten beispielsweise nach einem besonderen Ereignis wie etwa einem Alarm oder einer Transaktion an einem Geldautomaten.

Die meisten Bildspeicher bieten Funktionen, mit denen ausgehend vom gefundenen Bild in verschiedenen Geschwindigkeiten vor- oder zurückgespult werden kann, um die Videoaufzeichnung eines Vorgangs effizient auswerten zu können:

- schnell (Zeitraffer)
- normal (Echtzeit)
- langsam (Zeitlupe)

Die Bedienelemente hierfür sind oft Video Cassetten Recordern (VCR) nachempfunden, um Anwendern die Bedienung möglichst leicht zu machen.

Für den gezielten Abruf von Bildern anhand der Zeit gibt es so genannte Zeitleisten (englisch timeline): Ein Mausklick an eine Stelle auf der Zeitachse führt zur Anzeige des Bildes, das diesem Zeitpunkt am nächsten liegt. Zur besseren Orientierung sind in die Zeitleisten oft weitere Informationen wie Alarme, Notizen und markierte Bereiche eingetragen. Die Zeitleisten sollten über eine Zoom-Funktion zum Dehnen bestimmter Ausschnitte verfügen, damit auch in langen Videoaufzeichnungen zu jedem einzelnen Bild navigiert werden kann. Das Mausekranz kann als Jog-

Dial zur schnellen und einfachen Bildauswahl genutzt werden: Jede Raste am Mausekranz bewirkt die Auswahl des nächsten Bildes, je nach Drehrichtung vor oder zurück.

Bei Auslegung des Gesamtsystems ist darauf zu achten, wie viele Funktionen jede Komponente gleichzeitig erfüllen soll. Videosysteme, die entweder nur Livebilder liefern oder nur aufzeichnen, werden mit **Simplex** bezeichnet. Wenn ein System gleichzeitig Bilder live anzeigen als auch aufzeichnen kann, dabei aber keine Recherche möglich ist, spricht man von **Duplex**. Ist während der Live-Übertragung und Aufzeichnung auch eine Recherche möglich, so spricht man von **Triplex**. Nach heutigem Stand der Technik sollten alle Komponenten Triplex beherrschen. Manche Hersteller verwenden Bezeichnungen wie Quadplex oder Pentaplex, um damit auszudrücken, dass weitere Funktionen gleichzeitig möglich sind. Außerdem ist wichtig, wieviele Streams gleichzeitig übertragen werden sollen.

Hinsichtlich der Speicherkonzepte und Recherche-Möglichkeiten unterscheiden sich die Systeme verschiedener Anbieter erheblich, so dass dieser Punkt vor einer Kaufentscheidung gründlich und praxisnah geprüft werden sollte.

Ereignis-Übertragung

Alle bisher besprochenen Funktionen setzen voraus, dass eine Verbindung von der Leitstelle zur Bildquelle aufgebaut wurde. Es gibt aber auch Fälle, in denen die Bildquelle von sich aus Ereignisse an die Leitstelle melden soll, etwa

- Bewegung im Kamerabild
- Objekt im Bild erkannt
- Kamerakontakt betätigt
- Geräuschpegel überschritten
- Sabotage an der Bildquelle
- Technische Störungsmeldung
- Routine-Ruf zur regelmäßigen Überprüfung der Technik

Da manche Leitstellen tausende Bildquellen betreuen, ist es nicht praktikabel, zu allen Bildquellen permanent Verbindungen zu halten. Im Falle heterogener Videosysteme sind daher herstellereigene Verfahren gefragt, mit denen Bildquellen Ereignisse an die Leitstellen melden können.

Weit verbreitet ist für diesen Zweck der **FTP-Upload**. FTP steht als Abkürzung für File Transfer Protocol und ist eine seit vielen Jahren

bewährte Technik, um Dateien zwischen verschiedenen Systemen austauschen zu können. Die Bildquellen nutzen dieses Protokoll, um Bilder (meist als JPEG-Datei) und Meldungen (meist als ASCII-Text) an die Leitstelle zu übermitteln. In der Leitstelle wird ein FTP-Server betrieben, auf dem für jede Bildquelle ein eigenes Unterverzeichnis eingerichtet wird. Das VMS wertet die eintreffenden Bilder und Meldungen aus. Anhand des Unterverzeichnisses kann es alle Bilder und Meldungen der jeweiligen Bildquelle zuordnen und nach vorher festgelegten Regeln (Maßnahmenplan) darauf reagieren. Falls nötig, baut das VMS eine Verbindung zu der Bildquelle auf, die ein Ereignis gemeldet hat. Über diese Verbindung können dann alle weiteren vorgenannten Funktionen genutzt werden, um den gemeldeten Vorfall zu bearbeiten.

Ein weiteres weit verbreitetes Verfahren, mit dem Bildquellen verschiedener Hersteller Ereignisse melden können, ist **SMTP** (Simple Mail Transfer Protocol). Hier ist darauf zu achten, dass eine direkte SMTP-Verbindung von der Bildquelle zu einem eigens für diesen Zweck in der Leitstelle betriebenen SMTP-Server konfiguriert wird, weil nur dann eine schnelle Übertragung der Meldungen bis zum VMS gewährleistet ist. Mit MIME (Multipurpose Internet Mail Extensions) steht ein etabliertes Verfahren zur Verfügung, mit dem Bilder und Texte in SMTP-Meldungen eingebettet werden können.

Auch **SNMP** (Simple Network Management Protocol) bietet mit den so genannten SNMP-Traps die Möglichkeit, Ereignisse herstellerübergreifend zu melden. Bislang wird dieses Protokoll allerdings nur von wenigen Bildquellen unterstützt.

An der CAPI-Schnittstelle gemeldete **ISDN-Anrufe** können vom VMS als Ereignis einer Bildquelle ausgewertet werden. Eine aktivierte Rufnummernübertragung vorausgesetzt kann das VMS anhand der Rufnummer den Absender des Ereignisses identifizieren und eine Verbindung dorthin aufbauen, um weitere Informationen über das betreffende Ereignis zu ermitteln.

Daneben gibt es eine Vielzahl proprietärer Verfahren, die oft auf dem **TCP/IP**-Protokoll basieren. Hierfür muss im VMS das zur jeweiligen Bildquelle passende Anwendungsprotokoll implementiert sein.

Sonderfunktionen

Auch herstellerübergreifende Video-Management-Systeme können und sollten herstellereigene Sonderfunktionen berücksichtigen, sofern diese von Bedeutung für die Arbeit in der Leitstelle sind. Dies lässt sich über frei konfigurierbare Schaltflächen oder Listen in der Bedienoberfläche des VMS abbilden: Alle verfügbaren Sonderfunktionen werden beim Herstellen der Verbindung zu dem jeweiligen Bildquellentyp in eine Auswahlliste eingetragen, mit der sie vom Anwender aktiviert werden können. Der Umfang der verfügbaren Funktionen kann ggf. sogar während der Verbindung online zwischen VMS und Bildquelle „ausgehandelt“ werden:

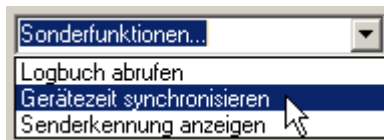


Abb. 9: Auswahlliste Sonderfunktionen

Die Sonderfunktion „Gerätezeit synchronisieren“ bietet bei einigen Bildquellen die Möglichkeit, diese trotz fehlendem NTP zumindest ab und an manuell mit der Systemzeit in der Leitstelle zu synchronisieren. Wenn das VMS diese Funktion in ausreichend kurzen Intervallen selbstständig immer wieder aufruft, ist dies sogar ein halbwegs brauchbarer Ersatz für eine Synchronisation über NTP. Voraussetzung ist in jedem Fall, dass die Bedienplätze in der Leitstelle fachgerecht synchronisiert sind.

Bei der Senderkennung handelt es sich um eine verschlüsselt übertragene Identifikation der Bildquelle, damit sich die Leitstelle vergewissern kann, dass die Bilder tatsächlich von der gemeldeten Bildquelle stammen und ihr nicht etwa von den Tätern „untergeschoben“ wurden

Wenn sich bestimmte Sonderfunktionen so weit durchsetzen, dass sie in ähnlicher Weise von mehreren Herstellern angeboten werden, sollten sie im VMS mit eigens dafür gestalteten Bedienelementen dargestellt werden, damit sie vom Leitstellenpersonal leichter gefunden und einheitlich bedient werden können. So können im Laufe der Zeit aus Sonderfunktionen etablierte Standardfunktionen werden, die den Funktionsumfang und die Einsatzmöglichkeiten des VMS sukzessive erweitern.

Lösungsansätze

Ziel der Video-Integration ist es, hinsichtlich aller vorgenannten Aspekte eine nahtlose Zusammenarbeit (Interoperabilität) der Videokomponenten verschiedener Hersteller zu erreichen. Dafür gibt es drei grundsätzlich mögliche Lösungsansätze:

1. **Standardisierung** der Bildquellen
2. **Koexistenz** verschiedener Schnittstellen und Formate
3. **Video-Interface**: Schnittstellenkonverter mit Transcodierung

Da die Umsätze im Sicherheitsbereich verglichen mit industriellen Anwendungen oder erst recht mit Consumer-Produkten relativ klein sind, dienen Verfahren, die sich in anderen Bereichen bewährt und etabliert haben, oft als Grundlage für Standardisierungsansätze auch für CCTV-Anwendungen.

Es gab schon viele Standardisierungsversuche für digitales CCTV, bislang konnte sich aber noch kein umfassender Standard durchsetzen. Erinnerung sei als Beispiel an H.323 oder OPC, die jeweils nur kleine Teilbereiche der für CCTV-Anlagen relevanten Funktionalität normierten und nur von wenigen Herstellern berücksichtigt wurden. Technisch vielversprechender sind aktuell ONVIF und PSIA, wobei noch offen ist, was sich langfristig durchsetzen wird.

Fraglich ist außerdem, ob sich überhaupt alle Hersteller einem Standard unterwerfen werden, der ihre Alleinstellungsmerkmale relativiert und ihre Produkte austauschbar macht. Einige Hersteller gehen daher sogar in die entgegengesetzte Richtung, indem sie neue proprietäre (herstellereigene) Formate entwickeln. Sie argumentieren dabei, dass die aus dem Consumer-Umfeld stammenden Verfahren nicht zu den Anforderungen der Sicherheitsbranche passen.

Selbst wenn es ab sofort einen umfassenden und allgemein akzeptierten Standard gäbe, wäre damit noch nicht das Problem gelöst, wie bereits vorhandene Bestandsgeräte integriert werden können.

Bei Lösungsansatz 2 werden alle Videos jeweils in dem Format gespeichert und weiterverarbeitet, in dem sie von der Bildquelle geliefert werden. Dies gelingt in vielen Fällen sehr gut und passt für Anlagen mit begrenztem Aufgabenumfang ohne weiteres. Es hat aber zur Folge, dass alle nachfolgenden Verarbei-

tungsstufen (etwa Auswerte- oder Archivierungssoftware) alle eventuell vorkommenden Formate und Protokolle beherrschen müssen. Zur Wiedergabe wird jeweils ein passender Decoder oder sogar die Client-Software des jeweiligen Herstellers benötigt. Eine einheitliche Weiterverarbeitung der Videodaten ist damit nicht ohne weiteres möglich.

Dies wird erst mit dem 3. Lösungsansatz erreicht: Getreu dem Motto „Kommt der Berg nicht zum Propheten, muss halt der Prophet zum Berg kommen“ wird hier nicht darauf gewartet, bis sich alle Hersteller auf einen umfassenden Standard geeinigt haben, sondern die Vielfalt der Videosysteme wird als gegeben akzeptiert; die Unterschiede werden durch Software-Anpassungen (Interfaces) im VMS ausgeglichen: Die Videobilder werden mittels Transcodierung in ein einheitliches Format übersetzt, und für die Steuerung wird ein einheitliches Protokoll bereitgestellt, das von der Interface-Software in die passenden Protokolle für die verschiedenen Bildquellen umgesetzt wird.

Die Transcodierung kann allerdings die Bildqualität mindern und die Latenz erhöhen. Um diese Nachteile möglichst gering zu halten, ist ausreichend Rechenleistung und Speicher nötig, so dass Systeme, die mit diesem Lösungsansatz geplant werden, ausreichend dimensioniert werden sollten. Der aktuelle Trend (immer mehr PC-Leistung für weniger Geld) kommt dem entgegen.

Nach der Transcodierung stehen die Bilder aller Bildquellen in einem einheitlichen Format zur Verfügung. Alle nachfolgenden Verarbeitungsstufen müssen also nur noch ein Dateiformat und ein Steuerungsprotokoll beherrschen. Insbesondere bei großen Anlagen mit einer Vielzahl weiterer Verarbeitungsschritte ist dieser Ansatz die richtige Wahl.

Ausblick

Der Trend geht klar in Richtung Digitalisierung und Vernetzung. Vorteilhaft sind Lösungen, die es schaffen, „alt“ und „neu“ miteinander zu verbinden.

Maximaler **Investitionsschutz** wird erreicht, indem eine CCTV-Anlage von vornherein als heterogenes Videosystem konzipiert wird: Die

Fähigkeit, Videokomponenten verschiedener Hersteller integrieren zu können, bewirkt dass

- vorhandene Videosysteme weiter genutzt werden können: Es werden nicht nur die Kosten für neue Geräte, sondern auch der Installationsaufwand gespart.
- man auch bei künftigen Erweiterungen nicht auf einen einzigen Hersteller angewiesen ist: Günstigere Verhandlungsposition beim Nachkauf; mögliche Engpässe bei eventuell nötigen Ersatz- oder Erweiterungsbeschaffungen werden von vornherein ausgeschlossen.

Ein weiterer Trend: Aufwändige anwendungsspezifische Hardware wird zunehmend durch flexible **Software-Lösungen** ersetzt: Software kann durch Updates jederzeit an neue Anforderungen und Technologien angepasst werden, während Hardware bei der dynamischen Entwicklung im IT-Bereich sehr schnell veraltet und an Wert verliert. Die rasante Entwicklung der Technik (immer mehr Rechenleistung und Speicher für immer weniger Geld) erschließt neue Anwendungsfelder und revolutioniert die Lösungsansätze, die zum Tragen kommen.

Um in diesem Umfeld optimale Lösungen realisieren zu können, sind Kenntnisse auf dem Gebiet der Netzwerktechnik und Software in einer Tiefe nötig, wie sie bei manchen klassischen Video-Errichtern noch nicht ausreichend vorhanden sind. Deshalb werden zunehmend IT-Systemhäuser in diesem Markt tätig. Bei diesen fehlt allerdings mitunter die nötige Erfahrung im Umgang mit Video und den speziellen Anforderungen der Sicherheitstechnik: Das Netzwerk funktioniert, aber wegen Gegenlicht, fal-

schem Öffnungswinkel oder fehlendem IR-Filter ist auf den angezeigten Bildern nichts zu erkennen, oder es gibt viel zu hohe Fehlalarmraten. Es erfordert erfahrene Spezialisten mit einem guten Systemüberblick, um die neuen technischen Möglichkeiten sinnvoll nutzen zu können.

Die wichtigste Regel lautet: Bevor Technik installiert wird, muss erst ein fundiertes Sicherheitskonzept erarbeitet werden, in dem die Ziele der geplanten Maßnahmen klar definiert und aus der Vielfalt der angebotenen Technik die jeweils passenden Komponenten fachgerecht zusammengestellt werden.

Im Rahmen des Sicherheitskonzeptes ist zu klären, welche Gewerke eine Rolle für das Erreichen der Sicherungsziele spielen (Zutrittskontrolle, Perimeter-Überwachung, Video-Sensorik, IR-Melder, Sprechanlage, Schrankensteuerung) und wie diese physikalisch und logisch miteinander verknüpft werden sollen. Dabei hilft es, wenn man gedanklich alle Arbeitsabläufe durchgeht und dokumentiert, die von dem Sicherheitssystem unterstützt werden sollen (Use-Case-Analyse). Die Verknüpfung verschiedener Gewerke automatisiert und beschleunigt nicht nur die Arbeitsabläufe, sondern vermeidet auch Bedien- und Übertragungsfehler, die sonst bei allen manuellen Bedienschritten leicht auftreten können.

Die Schlüsselrolle wird daher zunehmend der branchen- oder sogar projektspezifischen Software zufallen, mit der die gewünschte Funktionalität des Gesamtsystems erreicht wird, indem sie die Einzelkomponenten verschiedener Hersteller zu einer maßgeschneiderten Gesamtlösung verbindet.



Der Autor

Hardo Naumann ist Dipl.-Ingenieur der Elektrotechnik und Entwicklungsleiter der Accellence Technologies GmbH, einem Software-Entwicklungshaus mit dem besonderen Schwerpunkt „Video-Integration“
www.accellence.de