

## Software in Videosystemen

### Allgemeines

Software ist ein essenzieller Bestandteil moderner Videoüberwachungsanlagen (VÜA): Von ihr hängt es ab, ob verschiedene Systemkomponenten zueinander kompatibel sind (d.h. ob sie problemlos und umfassend zusammenarbeiten), welche Funktionen zur Verfügung stehen und wie komfortabel (d.h. wie produktiv) sie genutzt werden können. Dies wiederum entscheidet darüber, ob die gesteckten Sicherheitsziele tatsächlich erreicht werden und welcher Personalaufwand dafür nötig ist, hat also großen Einfluss auf den Projekterfolg und die Gesamtbetriebskosten.

In der Praxis wird die Bedeutung der Software dennoch häufig unterschätzt. Das liegt zum einen daran, dass viele Marktteilnehmer von den früher üblichen analogen Systemen gewohnt sind, eine VÜA durch einfaches Zusammenstecken verschiedener Hardwarekomponenten zu realisieren. Bei vielen Geräten ist Software vorinstalliert oder beigelegt und wird mitunter verwendet, ohne dass bewusst darüber nachgedacht wird. Zum anderen ist Software sehr abstrakt und im wahrsten Sinne des Wortes schwer zu „begreifen“: Sie wiegt nichts, man kann sie nicht anfassen, ihre Qualität und ihr Wert sind ohne entsprechende Fachkenntnisse und Erfahrungen im Vorhinein schwer zu bewerten: Die Auswirkungen der Entscheidung für eine bestimmte Software werden oft erst im laufenden Betrieb oder bei späterem Erweiterungsbedarf spürbar.

Mit Software lassen sich heute weitaus leistungsfähigere und komplexere Anlagen realisieren als früher. Dafür stellt sie aber auch besondere Anforderungen an Planung, Konfiguration und Wartung. Für Planer und Errichter sind deshalb fundierte Kenntnisse der grundlegenden Software-Konzepte von großem Vorteil, damit sie ihren Kunden optimale Lösungen anbieten können.



Bild: Videoarbeitsplatz im Mehrmonitor-Betrieb, Accellence Technologies GmbH, Hannover

## Einsatzgebiete

Software kommt in vielen Komponenten einer Videoüberwachungsanlage zum Einsatz:

- 
- IP-Kameras
- Video-Encoder
- Digitale Videorecorder (DVR)
- Netzwerk-Videorecorder (NVR)
- Video-Analyse, Privacy Masking
- Client-Software (z.B. Remote-Viewer)
- Videomanagement-Software (VMS)

Bewusst wahrgenommen wird die Software über ihre Bedienschnittstellen überall dort, wo Videobilder ausgewertet und Funktionen gesteuert werden, etwa mit Client-Anwendungen auf PC und Smartphone, oder als Videomanagement-Software, wie sie in Leitstellen eingesetzt wird.

Aber auch in IP-Kameras, Video-Encodern und Bildspeichern läuft Software, die fachgerecht konfiguriert und gewartet werden muss, selbst wenn Anwender nicht direkt in Kontakt mit ihr kommen. Auch alle Lösungen im Bereich der Videoanalyse basieren auf Algorithmen, die in Software implementiert sind, auch wenn dies nicht immer offensichtlich ist, etwa wenn sie in Form geschlossener Geräte (als „Black Box“) geliefert werden. Die folgenden Abschnitte gehen näher auf diese Einsatzgebiete ein.

## IP-Kameras

In IP-Kameras wird die Software meist in einem Speicherchip ab Werk mitgeliefert und ist daher quasi fest eingebaut; sie wird deshalb auch als „Firmware“ bezeichnet. Dennoch muss auch diese Software gewartet werden, etwa um neue Funktionen zu ermöglichen, weitere Schnittstellen zu unterstützen (z.B. neue ONVIF-Versionen) oder um nachträglich erkannte Sicherheitslücken zu schließen. Das Installieren einer neuen Software-Version wird Firmware-Update genannt. Die dazu benötigte Software wird in der Regel von den Software-

Kameraherstellern zum Download von ihrer Service-Website bereitgestellt. Bitte beachten Sie dazu auch die Hinweise aus dem Abschnitt „Firmware-Updates“ weiter unten. Manche Kamerahersteller bieten Programmierschnittstellen und Entwicklungsumgebungen, mit denen man die Software in der Kamera nach Bedarf selbst oder mit Modulen von Drittanbietern erweitern kann (Plugin, Add-on). Damit können Funktionen und Eigenschaften der Kameras sehr flexibel an verschiedenste Anforderungen angepasst werden.

## Video-Encoder

Für Video-Encoder gilt das gleiche wie für IP-Kameras. Der Unterschied besteht lediglich darin, dass sie anstelle einer eigenen Optik mit Bildaufnehmer über Eingänge zum Anschließen analoger Kameras verfügen. Die Technik dahinter einschließlich der verwendeten Software ist weitgehend identisch.

## Bildspeicher

Digitale Bildspeicher arbeiten heute durchweg softwarebasiert. Digitale Videorecorder (DVR) und Netzwerk-Videorecorder (NVR) unterscheiden sich dabei prinzipiell nur hinsichtlich der anschaltbaren Kamertypen:

DVRs verfügen über Eingänge für analoge Kameras, während NVRs IP-Kameras via Netzwerk anbinden.

Die Software zur Aufzeichnung und Wiedergabe der Videos kann wieder identisch sein, was an Hybrid-Recordern besonders deutlich wird, indem sie mit der gleichen Software Videos von beiden Kameratypen gleichermaßen aufzeichnen können.

Während ein DVR zum Anschließen der analogen Kameras noch auf Spezialhardware (z.B. eine Grabberkarte) angewiesen ist, kann ein NVR als reine Softwarelösung realisiert werden, die auf beliebigen Standard-IT-Plattformen und sogar in der Cloud läuft. Auch bei DVRs und NVRs bitte die Hinweise aus dem Abschnitt „Firmware-Updates“ beachten.

## Videoanalyse

In Software implementierte Videoanalyse-Algorithmen werten Bildinhalte aus, um Bildinformationen anzureichern (z.B. Markieren und Tracken von bewegten Objekten bestimmter Größe und Bewegungsrichtung) oder (etwa zum Schutz der Privatsphäre) zu verfremden (Privacy Masking), oder um daraus Metadaten und Ereignisse abzuleiten (Video-Sensorik), die in der Videomanagement-Software angezeigt und weiterverarbeitet werden können.

Videoanalyse-Software kann sowohl eingebettet in den IP-Kameras laufen als auch auf dedizierter Hardware in einem eigenständigen Gerät, als zentrale Lösung auf einem Server, in der Cloud oder als Bestandteil der Videomanagement-Software auf den Arbeitsplätzen in der Leitstelle. Es können Live-Streams der Kamera analysiert und – zum Einsparen von Netzwerklast – nur bei Bedarf übertragen werden (Pre-Analyse), oder es kann in aufgezeichneten Video-Sequenzen nach bestimmten Merkmalen gesucht werden (Post-Analyse).

Videoanalyse-Technologien unterliegen zurzeit einer großen Entwicklungsdynamik, so dass hier das Thema Software-Pflege (siehe weiter unten) einen besonders hohen Stellenwert hat. Außerdem zeigt die Praxis, dass unerwünscht hohe Falschalarmraten nur durch eine fachkundige Auswahl und Konfiguration der Videoanalysesoftware vermieden werden können.

## Client-Software

Für einen einfachen Zugriff auf IP-Kameras oder Recorder liefern deren Hersteller meist passende Software mit. Die Bezeichnung Client-Software kommt daher, dass sie auf Seiten des Kunden (engl. Client) installiert wird, um auf das Videogerät zuzugreifen, das in diesem Kontext als Server betrachtet wird, der den Clients bestimmte Videofunktionen zur Verfügung stellt.

Je nach Hersteller und Funktionsumfang sind für Client-Software auch andere Bezeichnungen gebräuchlich: Remote-Viewer, Video-Client, Bediensoftware, Player. Allen gemeinsam ist, dass sie einen einfachen direkten Zugriff auf die Geräte ermöglichen, dass man darüber die Geräte einrichten und konfigurieren, Videobilder abrufen und anzeigen sowie Funktionen steuern kann.

Um es dem Anwender möglichst einfach zu machen, bieten viele Geräte inzwischen einen Zugriff mit dem Web-Browser via HTTP (Hyper Text Transfer Protocol). Die Client-Software wird dann oft automatisch im Browser als Add-On installiert, sobald man sich das erste Mal mit dem Videogerät verbindet.

Seit einiger Zeit sind auch Client-Anwendungen (Apps) für Smartphones und Tablet-Computer verfügbar, die einen mobilen Zugriff auf die Videogeräte ermöglichen, damit auch Einsatzkräfte vor Ort aktuelle Bilder sehen und Kameras steuern können, etwa durch Schwenken und Neigen des Smartphones.

## Videomanagement

Die Vorstellungen, was mit Videomanagement gemeint ist, können sehr unterschiedlich sein und müssen konkretisiert werden, um Missverständnisse zwischen Kunden, Planern und Errichtern zu vermeiden. Das Spektrum reicht von einem NVR mit einer einfachen grafischen Benutzerschnittstelle bis hin zu einer mandantenfähigen über mehrere Standorte verteilten redundanten und gewerkeübergreifenden Sicherheitsarchitektur mit Single Sign-on, hierarchischer Strukturierung und normierten Datenformaten.

Die Rolle des Videomanagements wird an der Struktur einer umfassenden Sicherheitslösung deutlich:

Gesamt-Management				
Gefahren-Management, Gebäude-Management, Einsatzleitzentrale, Prozessteuerung, ...				
Videomanagement				andere Gewerke
Konfiguration, Verwaltung, Schnittstellen, Steuerung, Abläufe, Visualisierung				
Bildquellen	Bildspeicher	Bildverarbeitung	Bildanzeige	
IP-Kameras Video-Encoder	DVR NVR	Videoanalyse Privacy masking	Remote-Clients Monitore Video-Walls	EMA BMZ Zutritt ELA Intercom ...

Elementare Aufgaben:

- Video-Komponenten zu einem funktionierenden Videosystem verbinden
- Konfiguration und Verwaltung dieser Komponenten unterstützen
- Ausgewählte aufgezeichnete oder Live-Videobilder anzeigen
- Zentrale Steuerung aller Funktionen der Komponenten ermöglichen

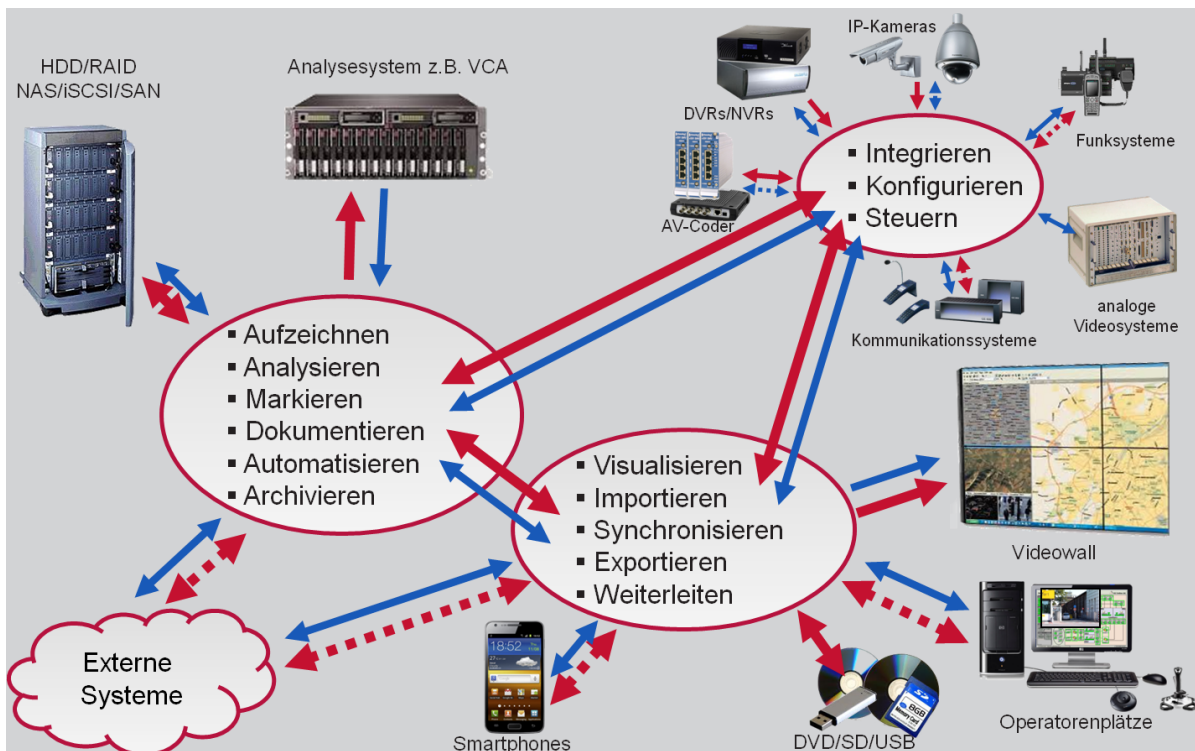


Bild: Aufgaben eines Video-Management-Systems, Accellence Technologies GmbH, Hannover

Bei den weiteren Funktionen unterscheiden sich verschiedene Lösungen. Je nach konkreten Projektanforderungen können unterschiedliche Produkte geeignet sein. Damit bei der Auswahl keine wichtige Funktion vergessen wird, kann folgende Liste zusammen mit dem Kunden durchgegangen werden:

- **Metadaten** zu allen überwachten Objekten, Kameras und zu jedem Bild erfassen und auswerten
- Kameras aus **Lageplänen** auswählbar und steuerbar bereitstellen, Kamerapositionen und aktuelle Ausrichtung (Blickwinkel, Sichtfeld) in Lageplänen sichtbar machen
- Kameras und Videoaufzeichnungen anhand **Metadaten** strukturiert in Listen zur Auswahl anbieten
- Auslesen und Übernehmen in der Bildquelle konfigurierter **Kamerabezeichnungen**
- PTZ-Steuerung der Kameras (schwenken, neigen, zoomen) über Joystick, Bedienpult oder mit der Maus ermöglichen, absolutes Positionieren auf Mausposition, Focus und Irissteuerung (Blende), Wischersteuerung, Konfigurieren und Anfahren von **Presetpositionen**
- **Bildauflösung** und **Split-Darstellung** von Videostreams je nach Erfordernissen anpassbar machen:  
Kleine Auflösung in hoher Bildfrequenz für eine schnelle Live-Vorschau etwa zur Kamerasteuerung, Einzelbilder in hoher Auflösung für eine Detailauswertung etwa von Gesichtern oder Kennzeichen
- Auswahl verschiedener **Skalierungsoptionen**, um eintreffende Bildformate je nach Anforderungen in die verfügbare Anzeigefläche einzupassen: Formatfüllend, Seitenverhältnisse beibehaltend mit Balken, Aufzoomen bis Balken verschwinden, ...
- **Digital-Zoom** zur Darstellung von Details in Megapixel-Bildern mit automatischer Mausnachführung
- Nachträgliche PTZ-Steuerung in aufgezeichneten Weitwinkel-Aufnahmen („360°-Kameras“): Entzerrung hemisphärischer Bilder durch **Morphing**.
- **Flip-Option**: Drehen der angezeigten Videobilder bei über Kopf montierten Kameras
- **Video-Recherche**: Abruf gespeicherter Bilder von DVRs und NVRs
- Auswahl der Videobilder wahlweise über eine **zoombare Timeline**, durch Auswahl eines Zeitpunkts über Datum und Uhrzeit (Analoguhrsymbol mit steuerbaren Zeigern) oder mit einem Jog-Dial verzögerungsfrei mit einzelbildgenauer Positionierung vorwärts und rückwärts
- **Synchronansicht** aufgezeichneter Videos aus verschiedenen Kameraperspektiven, etwa zur umfassenden Auswertung komplexer Tathergänge über mehrere Räume
- **Video-Loop**: Abspielen wichtiger Bildfolgen (z.B. Alarmsequenz) als Schleife
- **Sequenzbildansicht** zur schnellen und gezielten Auswahl des am besten passenden Bildes aus einer Bildfolge
- **Referenzbilder** von zutrittsberechtigten Personen oder für einen direkten Soll-Ist-Vergleich
- Konfigurierbare **Ringspeicher**, bei denen Videos nach definierter Zeit sukzessive ausgedünnt oder gelöscht werden, um Speicherplatz zu sparen und um **Datenschutzauflagen** zu erfüllen

- **Weiterleitung** von Videos und Metadaten zu anderen Arbeitsplätzen, ggf. an anderen Standorten
- **Audio** Wechselsprechen (push to talk), Gegensprechen, nur live oder auch mit Aufzeichnung Software
- **Telemetrie, Fernwirken:** Auswerten und Schalten von **I/O-Kontakten** an den Videogeräten
- **Meldungen** und **Alarmbilder** von den Videogeräten empfangen und verarbeiten
- **Ablaufsteuerung:** Zeit- oder ereignisgesteuert Aktivitäten nach konfigurierbaren Maßnahmenplänen ausführen, etwa zur Alarmbearbeitung, incl. Aufschalten bestimmter Kameras auf bestimmte Monitore und Anfahren definierter Presetpositionen, z.B. durch einen skriptbasierten Event-Manager
- **Digitale Video-Kreuzschiene, Video-Wall:** Kamerabilder wahlfrei auf Monitore schalten
- Ein **Sequencer** schaltet in vorgegebenen Zeitabständen verschiedene Kamerabilder auf Monitore
- **Virtueller Wächterrundgang:** Zu festgelegten Zeitpunkten werden Überwachungsaufträge anhand konfigurierbarer Maßnahmenpläne abgearbeitet und quittiert
- Integrierte **Überwachung** der nötigen Ressourcen, z.B. Netzwerkverbindungen, Festplattenspeicher
- Anzeige der Betriebszustände, Hinweise auf Fehler mit Maßnahmen zur Störungsbehebung
- Verwaltung der Benutzer mit ihren Zugriffsrechten auf das Videosystem
- **Exportieren** und **Importieren** von Videosequenzen in allen benötigten Formaten
- Auslagerung von Videos zum **Archivieren** auf externe Datenträger
- **Protokollierung** zur lückenlosen Dokumentation und Rekonstruktion aller Vorgänge mit Auswertung, z.B. Statistik gemäß EN 50518 und Verbindungsnachweis zur Abrechnung gegenüber Kunden
- Einfache Übernahme von Videobildern über die **Zwischenablage** (Clipboard) in E-Mail-Programme, Office-Anwendungen und Bildbearbeitungssoftware
- **Shortcuts, Hotkeys:** Aufruf wichtiger Funktionen auf Tastendruck

Eng verwandt mit Videomanagement ist **Video-Asset-Management**, bei dem im Vordergrund steht, große Bestände von Videoaufzeichnungen zu verwalten und anhand Schlagworten gezielt abrufen zu können.

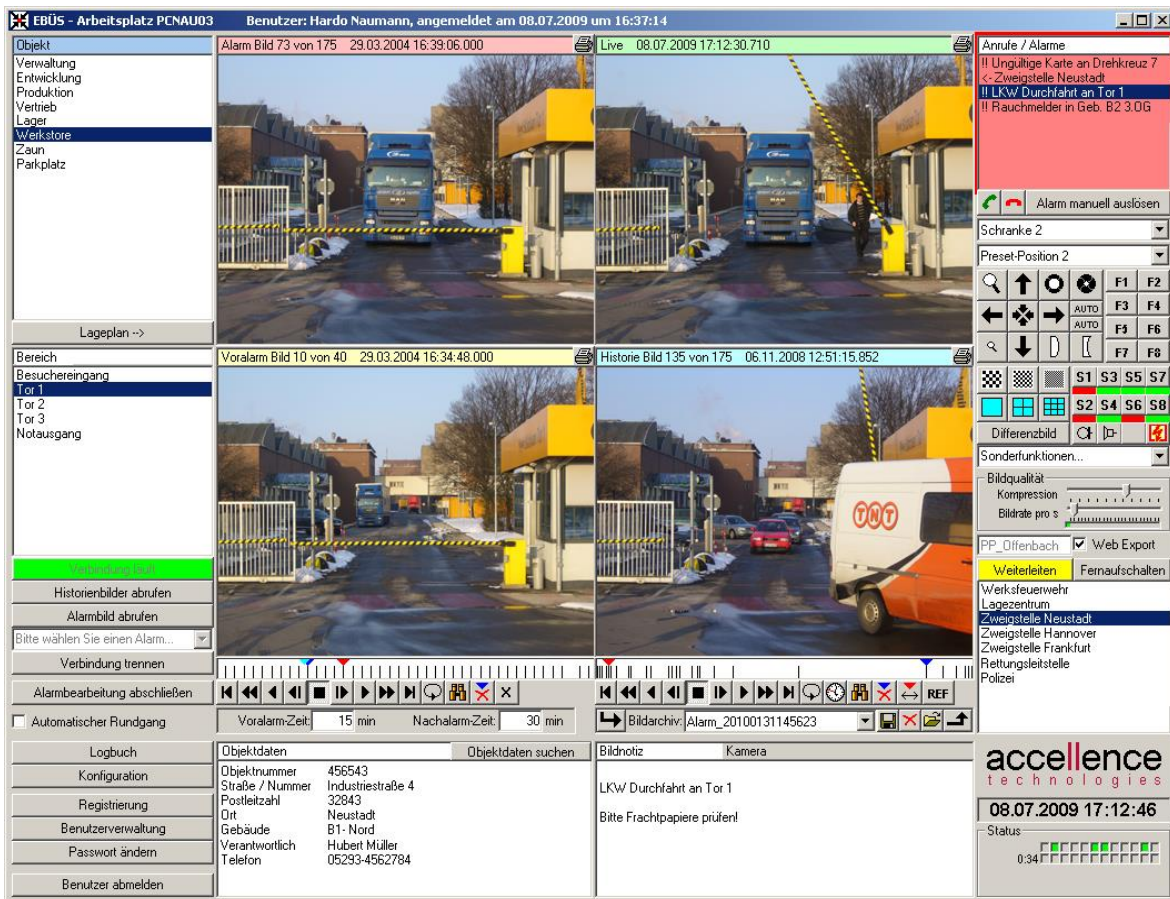


Bild: Schrankensteuerung mit Video-Management, Accellence Technologies GmbH, Hannover

## Stand-Alone oder voll integriert

Videomanagement kann **Stand-Alone** als eigenständige Insellösung betrieben oder als **Video-Subsystem** nahtlos in eine Gesamt-Sicherheitsarchitektur eingebettet werden. Beim Betrieb als Subsystem kommt es vor allem auf die Schnittstelle zum übergeordneten Management-System (ÜMS) und die Möglichkeiten an, die es zur Integration der Videoanzeigen und Video-Bedienelemente in das ÜMS bereitstellt, während sich eine Stand-Alone-Lösung vor allem durch ihre eigene **grafische Benutzerschnittstelle** (graphical user interface, GUI) auszeichnet. Wenn eine voll integrierbare Software auch als **Rückfallebene** bei eventuellem Ausfall des übergeordneten Systems dienen soll, muss sie beides bieten.

Als ÜMS kommen u.a. in Frage:

- Gefahrenmanagement-Systeme, Gebäudemanagement-Systeme (GMS)
- Software in Lagezentren, Einsatzleitstellen (ELS), Betriebszentralen, Verkehrsleitstellen
- Leitstellen- oder Alarmbearbeitungssoftware, Alarm Management Software (AMS)
- Physical Security Information Management (PSIM)
- Prozesssteuerungssoftware, Leitwarten, Supervisory Control and Data Acquisition (SCADA)

Eine voll integrierte Lösung sollte auch ihre Konfigurationsdaten aus der zentralen Datenhaltung der Sicherheitsarchitektur übernehmen, um doppelte Dateneingabe zu vermeiden; die Software muss dazu über entsprechende Import-Funktionen verfügen, während eine Stand-Alone-Lösung stets eine eigene Konfigurationsdatenbank und zugehörige Eingabemasken benötigt.

## Permanente oder bedarfsgesteuerte Verbindungen

Bei kleinen Videoanlagen ist es üblich, dass – selbst wenn gerade keine Videobilder angezeigt werden – die Videomanagement-Software **permanent Verbindungen** zu allen konfigurierten Kameras hält, etwa um die Videos zentral aufzuzeichnen. Bei großen, hierarchisch strukturierten Anlagen mit mehreren verteilten Standorten und erst recht bei Leitstellenverbänden und großen Notruf- und Service-Leitstellen ist es aber unrealistisch, zu mehreren zehntausend Kameras permanent Netzwerk-Verbindungen zu unterhalten. In solchen Fällen muss die Videomanagement-Software **bedarfsgesteuerte Verbindungen** und ein ausgefeiltes Verbindungs-Management mit konfigurierbarer automatischer Verbindungstrennung zum Senken der Verbindungskosten unterstützen. Mit einer in die VMS integrierten **Proxy-Funktionalität** kann weitere Netzwerkbandbreite gespart werden, indem jeder Datenstrom auf dem Netzwerk nur einmal übertragen wird, auch wenn er an mehreren Stellen benötigt wird (Multicast-Betrieb auf Applikationsebene).

Bedienplatz	V	B	Geladen
EBUES-BP1-XP			38%
EBUES-BP2-W7-64			0%
EBUES-BP3-XP			
EBUES-BP4-XP			5%
EBUES-BP5-AMWIN			19%
EBUES-BP6-W7-32			28%
EBUES-BP7-W7-64			25%
PCNAU04			0%
PCNAU04-VIRTXP			
LAPNAU04			

Info

- Auf Bedienplatz EBUES-BP7-W7-64 wurden 5 Einträge in der Datei EBÜS\_EBUES-BP7-W7-64\_20130905.log gefunden!
- Auf Bedienplatz EBUES-BP6-W7-32 wurden 0 Einträge in der Datei EBÜS\_EBUES-BP6-W7-32\_20130903.log gefunden!
- Auf Bedienplatz EBUES-BP6-W7-32 wurden 0 Einträge in der Datei EBÜS\_EBUES-BP6-W7-32\_20130903.log gefunden!
- Auf Bedienplatz EBUES-BP5-AMWIN wurden 0 Einträge in der Datei EBÜS\_EBUES-BP5-AMWIN\_20130904.log gefunden!
- Auf Bedienplatz EBUES-BP1-XP wurden 0 Einträge in der Datei EBÜS\_EBUES-BP1-XP\_20130923.log gefunden!
- Auf Bedienplatz EBUES-BP6-W7-32 wurden 0 Einträge in der Datei EBÜS\_EBUES-BP6-W7-32\_20130904.log gefunden!
- Auf Bedienplatz EBUES-BP7-W7-64 wurden 0 Einträge in der Datei EBÜS\_EBUES-BP7-W7-64\_20130906.log gefunden!
- Auf Bedienplatz EBUES-BP1-XP wurden 0 Einträge in der Datei EBÜS\_EBUES-BP1-XP\_20130924.log gefunden!
- Auf Bedienplatz EBUES-BP5-AMWIN wurden 0 Einträge in der Datei EBÜS\_EBUES-BP5-AMWIN\_20130905.log gefunden!
- Auf Bedienplatz EBUES-BP6-W7-32 wurden 2 Einträge in der Datei EBÜS\_EBUES-BP6-W7-32\_20130905.log gefunden!
- Auf Bedienplatz EBUES-BP1-XP wurden 0 Einträge in der Datei EBÜS\_EBUES-BP1-XP\_20130925.log gefunden!

Bild: Verbindungsnachweis ruft Daten von den Videoarbeitsplätzen ab, Accellence Technologies GmbH, Hannover

## Proprietäre oder universelle Software

Ein weiteres wichtiges Auswahl-Kriterium: Genügt eine **herstellerspezifische** (proprietäre) Software, oder soll eine **herstellerübergreifende** Lösung geschaffen werden? Die meisten Hersteller von Kameras, Encodern oder Recordern bieten kostenlos oder zu einem sehr günstigen Preis passende Software zu ihren Geräten an. Proprietäre Software hat den Vorteil, dass sie optimal auf die Geräte des jeweiligen Herstellers ausgerichtet ist und deren spezielle Eigenschaften gut zur Geltung bringt.

Außerdem kalkulieren viele Gerätehersteller so, dass sie ihren Gewinn über den Absatz der Kameras oder Recorder erzielen und die Software quasi als nötige Beigabe dazu quersubventionieren. Deshalb ist proprietäre Software meist günstiger in der Anschaffung. Diese Preisgestaltung erfolgt aber nicht ganz uneigennützig: Der von den Herstellern gewünschte Lock-in-Effekt besteht darin, dass der Kunde auch bei künftigen Erweiterungen der Anlage um weitere Kameras oder Recorder beim gleichen Hersteller bleiben muss, weil nur seine Geräte mit dieser Software kompatibel sind. Sind erst einmal alle Prozesse auf die proprietäre Software ausgerichtet und alle Mit-



arbeiter darauf geschult, dann ist ein Wechsel zu einem anderen Anbieter mit großem Aufwand verbunden. Die Praxis zeigt viele Beispiele, bei denen sich vermeintlich günstige Lösungen bei später erforderlichen Erweiterungen als sehr teuer erwiesen haben, weil Hersteller die Abhängigkeit von ihren Produkten bei der Preisgestaltung gezielt ausnutzen.

Eine herstellerübergreifende Lösung bewirkt, dass

- vorhandene Videosysteme weiter genutzt werden können: Das spart nicht nur Kosten für neue Geräte, sondern vor allem Installationsaufwand.
- verschiedene Systeme mit ihren speziellen Eigenschaften für eine besonders wirtschaftliche Lösung miteinander kombiniert werden können.
- bei künftigen Erweiterungen nicht nur ein Anbieter in Frage kommt: Günstigere Verhandlungsposition beim Nachkauf; mögliche Engpässe bei Ersatz- oder Erweiterungsbeschaffungen werden von vornherein vermieden.

Bei kleinen Anlagen ist eine proprietäre Lösung in der Regel einfacher und günstiger, bei anspruchsvolleren Aufgaben kann jedoch die Möglichkeit, Produkte verschiedener Hersteller zu kombinieren, viel mehr Geld sparen als die dazu erforderliche Software kostet. Das sollte vor einer Kaufentscheidung sorgfältig geprüft und bedacht werden. Auch in allen Anwendungsfällen, in denen noch nicht absehbar ist, welche Gerätetypen künftig aufgeschaltet werden sollen (etwa bei Notruf- und Service-Leitstellen), sollte auf eine möglichst universelle Lösung mit breiter Unterstützung vieler Hersteller geachtet werden.

### **Transparente oder normierte Datenübertragung**

Bei herstellerübergreifender Software ist wiederum zu unterscheiden, ob sie die von den verschiedenen Geräten gelieferten Daten transparent unverändert in dem Format verarbeitet und weiterleitet, in dem sie von den Quellen geliefert wurden, oder ob sie alle Daten zum Zwecke der einheitlichen Weiterverarbeitung normiert, d.h. in ein einheitliches Format übersetzt (transcodiert). Letzteres erfordert deutlich mehr Rechenaufwand, bringt aber den Vorteil, dass bei allen nachfolgenden Arbeitsschritten nur noch mit dem vereinheitlichten Format gearbeitet werden muss. Dies erleichtert den Einsatz von weiteren Softwareprodukten für die Auswertung, Nachbearbeitung und Archivierung der Videos erheblich.

Auch die Steuerkommandos für die verschiedenen Videogeräte sollten von der Videomanagement-Software normiert werden, damit Anwender und ÜMS die Videogeräte aller Hersteller stets auf die gleiche Weise steuern können: Für den Anwender führt eine gleichbleibende Routine bei der Bedienung zu mehr Produktivität, weil er sich nicht bei jeder Aufschaltung erneut Gedanken machen muss, wie nun gerade dieser Gerätetyp bedient werden muss, und Anbieter von Management-Software sparen sich durch Rückgriff auf integrative Videomanagement-Software den Aufwand, in ihrer Software die Formate und Protokolle Hunderter unterschiedlicher Videoprodukte implementieren und laufend an den neuesten Stand anpassen zu müssen.

### **Monolithische oder offene Systemarchitektur**

Im Hinblick auf die Investitionssicherheit ist eine offene Systemarchitektur wünschenswert: Dazu sind wohldefinierte, umfassend dokumentierte und normierte Schnittstellen zwischen allen Komponenten nötig, damit je nach konkreten Anforderungen Produkte verschiedener Hersteller für eine wirtschaftlich optimale Lösung miteinander kombiniert werden können. Insbesondere ist dabei darauf zu achten, dass der Betreiber auch bei künftig notwendig werdenden Erweiterungen auf Komponenten anderer Anbieter ausweichen kann, um sich nicht von einem Lieferanten abhängig zu machen.

Dies erfordert eine saubere Trennung verschiedener Blöcke, in denen bestimmte Funktionsbereiche zur Reduzierung der Komplexität gekapselt sind, und frei verfügbare, umfassend dokumentierte und testbare (d.h. mit eindeutigen Testbedingungen als Abnahmekriterien versehene) Schnittstellen zwischen diesen Komponenten.

Von diesem Idealbild der Systemstruktur gibt es in der Praxis historisch und durch verschiedene Umstände bedingt zahlreiche Varianten und Abweichungen, meist monolithische Systeme, die im Laufe der Zeit durch schrittweise Erweiterungen aus Teilkomponenten „gewachsen“ sind und deshalb nicht der idealen Architektur entsprechen. So gibt es sowohl Bildspeicher- und Videoanalyse-Software, die um Videomanagement-Funktionen erweitert wurde, als auch Gefahrenmanagement-Systeme, die inzwischen etwas Video können.

Für bestimmte Aufgaben kann das eine günstige Lösung sein, im Hinblick auf möglichen künftigen Erweiterungsbedarf aber Probleme mit sich bringen, denn jeder Anbieter hat seine Stärken und Schwächen; es gibt kein Produkt, das in allen Bereichen am besten abschneidet. Besonders anschaulich wird dies auf dem Gebiet der Video Content Analyse (VCA): Dieser Markt differenziert sich in eine Reihe sehr unterschiedlicher Kompetenzen, z.B. Kennzeichenerkennung, Motion-Detection, Objekterkennung und -tracking, Zählen von Besuchern oder Fahrzeugen, Biometrie, Privacy Masking, Smartsearch u.v.m..

Ideal wäre daher, wenn sich jeder Anbieter auf seine Kernkompetenz konzentrieren würde und die Anwender über offene Schnittstellen die für ihre Zwecke am besten geeigneten Produkte verschiedener Hersteller frei miteinander kombinieren könnten.

Dieses Ideal wird sich in der Praxis in vielen Fällen nicht ganz erreichen lassen, man sollte es bei der Planung einer VÜA dennoch nicht aus den Augen verlieren und - soweit es wirtschaftlich vertretbar ist – auf komponentenorientierte Software achten. Eine gut durchdachte und nachhaltige Softwarearchitektur kostet zwar zunächst zusätzlichen Aufwand, wird aber immer wichtiger, je größer und komplexer eine Anlage wird.

## Konvergenz der Gewerke

Mit Konvergenz ist in diesem Zusammenhang gemeint, dass verschiedene Gewerke miteinander verknüpft werden, um aus den einzelnen Teilen ein wirkungsvolleres Ganzes zu schaffen.

Der praktische Nutzen solcher integrierter Lösungen liegt darin, dass

- alle Daten nur noch einmal eingegeben und gepflegt werden müssen und von allen Teilsystemen jederzeit auf jeweils aktuellem Stand genutzt werden können
- Benutzer sich nur noch einmal am System anmelden müssen (Single Sign-on) und ihre Berechtigungen für alle Gewerke zentral übersichtlich verwaltet werden können
- Daten, Zustände und Ereignisse automatisch von einem zum anderen Gewerk übertragen werden. Dies spart nicht nur Zeit und Arbeitsaufwand, sondern verhindert auch alle Fehler, die sonst beim manuellen Übertragen („Abschreiben“) oder durch inkonsistente Daten auftreten können, wenn verschiedene Gewerke mit unterschiedlichen Versionsständen der Datensätze arbeiten
- wichtige oder häufig wiederkehrende Abläufe weitgehend automatisiert werden
- erst die Verknüpfung verschiedener Informationen einen optimalen Gesamtüberblick verschafft
- alle benötigten Funktionen aus einer homogenen Bedienoberfläche heraus schnell und gezielt gesteuert werden können



Bild: Typische Geräte, die integriert werden sollen, Accellence Technologies GmbH, Hannover

Typische Gewerke, die mit Video verknüpft werden:

- Einbruchmeldeanlage (EMA), Brandmeldezentrale (BMZ)
- Zutrittssteuerung, Zeiterfassung, Türsteuerung, Fluchtwegemanagement
- Schrankenanlagen, Rolltore
- Sprechanlage (Intercom), Lautsprecheranlage (ELA) für Durchsagen
- Haustechnik, Gebäudeautomatisierung (Heizung, Lüftung, Klima, Licht, Verschattung, ...)
- Aufzugnotruf, Rolltreppen
- Geld- und Kassenautomaten

Damit Konvergenz gelingt, muss sorgfältig eine dafür geeignete Softwarearchitektur erarbeitet werden. Bei der Kopplung verschiedener Gewerke ist zuerst zu klären, welches das führende System ist. Es muss genau eine Stelle geben, die in letzter Instanz über Prioritäten und Maßnahmen entscheidet, damit es kein Durcheinander etwa wegen widersprüchlicher Reaktionen verschiedener Teilsysteme gibt. Nur bei Ausfall eines übergeordneten Systems darf ein Subsystem als Rückfallebene eigene Entscheidungen treffen.

Gewerke können prinzipiell auf 3 verschiedenen Ebenen gekoppelt werden:

- Management-Ebene
- Ebene der Unterzentralen
- Feldebene

Die **Feldebene** beinhaltet die Geräte im Überwachungs- und Wirkungsbereich der Sicherheitsanlage, also Kameras, Türsteuerungen, Rauchmelder etc.. Auf dieser Ebene erfolgt meist eine einfache reine Hardware-Kopplung, etwa durch I/O-Kontakte oder über eine transparente serielle Schnittstelle (RS-232/RS-485). Ein Beispiel dafür sind die in vielen Bildquellen enthaltenen Schaltkontakte, mit denen Licht, Türen, Sirenen etc. geschaltet werden können. Dies stellt für kleine, abgegrenzte Aufgaben eine einfache Lösung dar.

Allerdings sind auf Feldebene in der Regel keine Metadaten verfügbar. Das heißt, was genau z.B. mit Schaltkontakt Nr. 3 von Video-Encoder Nr. 57 geschaltet wird, weiß erst einmal nur derjenige, der die Leitung dort angeschlossen hat. Bei manchen Systemen kann der Errichter hierfür noch manuell einen Text in der Bildquelle hinterlegen wie etwa „Türöffner Gebäude 2B West EG“, aber es ist bei heutigem Stand der Technik nicht direkt ersichtlich, dass dieser Türkontakt eigentlich zum Gewerk „Zutritt“ gehört, und es gibt auch noch keinen normierten automatischen Weg, über den solche Daten wieder an die richtige Stelle in der Zutrittssteuerung eingekoppelt werden können. Wenn solche Anlagen nicht sehr diszipliniert und fachkundig gepflegt werden, entsteht im Laufe der Zeit ein unübersichtlicher Wildwuchs, der zu schwerwiegenden Problemen führen kann.

Mit der Ebene der **Unterzentralen** sind z.B. die BMZ, EMA oder Intercom-Anlage gemeint. Auf dieser Ebene ist auch das Videomanagement einzuordnen, indem es eine Anzahl Kameras zu einem Subsystem vereinigt. Fehlt ein ÜMS, kann eine der Unterzentralen zum führenden System gemacht werden. Eine Schneider Intercom Anlage ist beispielsweise in der Lage, die für ein Videosubsystem erforderlichen Kommandos zu generieren. Mitunter wird auch eine Videomanagement-Software erweitert, um direkt andere Gewerke zu steuern. Das ist genau dann die passende Lösung, wenn Video im Mittelpunkt steht und es kein ÜMS gibt.

Die **Management-Ebene** stellt bei anspruchsvollen komplexen Aufgaben die bevorzugte Ebene zur Kopplung der Gewerke dar. In einer klaren hierarchischen Struktur laufen hier alle Fäden zusammen: Alle Meldungen und Ereignisse aus den verschiedenen Gewerken werden an das ÜMS gemeldet, und dort werden gemäß zentral konfigurierter Prioritäten und Maßnahmenpläne die passenden Aktionen in den einzelnen Gewerken initiiert. Jedes Subsystem koordiniert dabei die Aktivitäten und Ereignisse innerhalb seiner Zuständigkeit, alle gewerkeübergreifenden Maßnahmen laufen über das ÜMS. Dies ist die sauberste und übersichtlichste Struktur, deren konsequente Umsetzung allerdings viel Sorgfalt und Ausdauer erfordert.

Ein weiteres Gewerk, mit dem eine Videoanlage gekoppelt werden kann, ist die von einem Unternehmen verwendete IT-Infrastruktur. In einer modernen vernetzten Videoanlage gibt es viele Beteiligte, und jedem sollen entsprechend seiner Aufgaben („Rolle“) die passenden Zugriffsrechte und Steuerungsmöglichkeiten zugewiesen werden. Dazu ist ein **differenziertes Rechtemanagement** nötig. Seitens der IT-Infrastruktur stehen dafür Technologien wie Active Directory (AD) und LDAP zur Verfügung. Wenn diese genutzt werden, ergibt sich der zusätzliche Vorteil des **Single Sign-on**, d.h. jeder Benutzer muss sich nur einmal am PC mit Benutzernamen und Passwort anmelden und erhält damit die Zugriffsrechte auf alle Dienste, die für ihn freigegeben wurden, auch auf die Videofunktionen. Von Seiten des Systemadministrators muss dann jeder Benutzer nur einmal im System angelegt werden, und seine Gruppenzuordnung und Berechtigungen können übersichtlich und strukturiert zentral verwaltet werden. Dies ist eine enorme Arbeitserleichterung gegenüber einer separaten Benutzerverwaltung in jedem einzelnen Gewerk. In der IT übliche Werkzeuge wie die Management-Konsole von AD verschaffen dem verantwortlichen Systembetreuer einen guten Überblick. Auch Sicherheitslücken durch „vergessene“ Benutzer werden somit vermieden: Wird ein Benutzer in der zentralen Benutzerverwaltung gesperrt, kann er auf keinen

der Dienste mehr zugreifen. Voraussetzung dafür ist, dass die Videomanagement-Software Verzeichnisdienste wie Active Directory umfassend unterstützt.

## Strukturierung und Mandantenfähigkeit

Mit dem Zusammenwachsen der bisherigen Insellösungen wird auch eine **hierarchische Strukturierung** des Videosystems nötig. Ein Beispiel soll dies veranschaulichen: Die Videoanlage in der Filiale eines Unternehmens wird tagsüber vom Empfang vor Ort („Pfortner“) bedient und ausgewertet. Mit Dienstschluss sollen alle Videobilder und Meldungen zu einer zentralen Werkschutzleitstelle umgeleitet werden („Tag-Nacht-Umschaltung“). Diese Umschaltung sollte – damit sie nicht vergessen wird – automatisiert werden, indem sie z.B. an die Scharfschaltung der Alarmanlage in der Filiale gekoppelt wird (Fehlervermeidung durch Konvergenz). Sobald Pfortner oder Werkschutzleitstelle eine kriminelle Handlung beobachten (etwa einen Einbruchversuch in eine Filiale), sollen Videobilder und bestimmte Steuerungsfunktionen an die zuständige Polizeidienststelle weitergeleitet werden. Von dort wiederum sollen ausgewählte Videobilder direkt an die Einsatzkräfte vor Ort weitergeleitet werden, damit diese schon vor Erreichen des Tatorts sehen können, wo genau gerade was passiert und die Täter gezielt auf frischer Tat überraschen und festnehmen können.

Dazu ist es nötig, dass Videomanagement-Software auch andere Videomanagement-Systeme integriert, d.h. Videobilder und Daten von ihnen übernehmen und ihre Funktionen steuern kann. Auf diese Weise entsteht eine hierarchische Struktur mehrerer miteinander gekoppelter Videosysteme.

Unter **Mandantenfähigkeit** wird verstanden, dass eine Videoanlage für verschiedene Kunden genutzt werden kann. Jeder Kunde soll nur auf seine eigenen Kameras und Videoaufzeichnungen zugreifen können, und alle über das Videosystem erbrachten Leistungen sollen gegenüber jedem Kunden detailliert abgerechnet werden können (Accounting). Auch hierzu ein Beispiel: In einem Industriepark oder großen Bürogebäude wird vom Facility Management eine gemeinsame Videoanlage für alle Mieter betrieben. Dies ist wirtschaftlicher als eine Vielzahl kleiner Anlagen, die jeder Mieter selbst betreibt, aber auch besonders sensibel, denn vertrauliche Innenansichten aus einem Unternehmen dürfen nicht in falsche Hände geraten. Ferner muss darauf geachtet werden, dass durch die gemeinsame Nutzung der Videoanlage nicht unabsichtlich die Netzwerke verschiedener Kunden miteinander gekoppelt werden und dadurch potenzielle Sicherheitslücken durch unerwünschte Querverbindungen entstehen.

## Ausschreibung und Auswahl

Je nach geplantem Anwendungsfall sind unterschiedliche Funktionen und Eigenschaften wichtig und kommen verschiedene Systemarchitekturen in Frage. Dies sollte vor Ausschreibung oder Auswahl einer Software sorgfältig analysiert werden.

Ausgangspunkt für die Ausschreibung sollten das Sicherheitskonzept und die darin definierten Schutzziele sein. Die Auswahl der Software sollte sich nach den Arbeitsabläufen und der Organisationsstruktur des Anwenders richten. Dies dient nicht nur der Sicherheit und Produktivität, sondern steigert auch die Akzeptanz durch die Anwender.

Dazu ist es sinnvoll, gemeinsam mit dem Kunden und den späteren Anwendern alle Arbeitsabläufe präzise durchzugehen und zu dokumentieren, die vom Sicherheitssystem unterstützt werden sollen (Use-Case-Analyse). Daraus können dann systematisch die funktionalen Anforderungen an die Software abgeleitet werden. Dabei ist besonders darauf zu achten, dass die Anforderungen vollständig, widerspruchsfrei und eindeutig formuliert werden - Definitionslücken und Interpretationsspielräume könnten sonst später zu teuren Nachforderungen führen.

Eine Ausschreibung sollte sich nicht auf einen bestimmten Hersteller oder ein bestimmtes Produkt beziehen, sondern die benötigten Funktionen in abstrakter Form umfassend definieren und nor-

mierte Schnittstellen vorgeben, über die verschiedene Varianten und Komponenten miteinander kombiniert werden können. Nur so kann die wirklich am besten passende Lösung gefunden werden.

Herstellerübergreifende Videomanagementsoftware mit offenen Schnittstellen ist schwieriger auszuschreiben und in der Regel teurer in der Anschaffung, bietet den Betreibern aber größere Flexibilität und Investitionssicherheit, weil bei künftigem Erweiterungsbedarf auf Produkte verschiedener Hersteller zurück gegriffen werden kann.

Bei der Bewertung der Angebote sollten nicht nur die Anschaffungskosten, sondern die Gesamtbetriebskosten (total cost of ownership, TCO) betrachtet werden. Wenn mittels Prozessoptimierung und automatischer Datenübernahme Bedien- und Eingabefehler vermieden und Personalkosten reduziert werden, kann sich ein höherer Anschaffungspreis für die Software durchaus lohnen.

Die Produktivität einer Notruf- und Service-Leitstelle bemisst sich z.B. darin, wie viele Alarmvorfälle sie pro Zeiteinheit und eingesetzten Mitarbeitern erfolgreich bearbeiten kann. Eine Software, die pro Schicht mehr abrechenbare Aktivitäten erlaubt, zahlt sich schnell aus.

Eine **Marktübersicht** über Videomanagement-Software gibt es unter [www.sicherheit.info/artikel/1106573](http://www.sicherheit.info/artikel/1106573).

Neben den Punkten, die sich aus den vorangegangenen Abschnitten ergeben, sollten in Ausschreibungen von Videomanagement-Software auch folgende Anforderungen berücksichtigt werden:

- Unterstützte **Kompressionsverfahren und Bildformate** bis x Megapixel
- **Erweiterbarkeit:** Anzahl Kameras, Server und Arbeitsplätze bei Maximalausbau des Systems.
- Ideal: Lineare Skalierbarkeit, d.h. durch auf beliebig viele Ressourcen verteilbare Prozesse gibt es keine Beschränkungen hinsichtlich Anzahl Streams, Arbeitsplätzen und Speicher
- **Load Balancing:** Verteilung von Rechenlast und Speicherbedarf per statischer Konfiguration oder sogar dynamisch auf alle verfügbaren Ressource
- Hohe **Verfügbarkeit** durch Redundanz
- **Datensicherheit** (Verschlüsselung, Public Key Infrastructure (PKI), Signaturen und Wasserzeichen)
- Geringe **Latenz** (besonders wichtig bei PTZ-Steuerung, Fernwirken (z.B. Schranken und Rolltoren) sowie in Verbindung mit Audio-Kommunikation)
- **Interoperabilität** zu anderen Gewerken (Konvergenz)
- **Multilingualität:** Umschalten verschiedener Sprachen bei der Benutzeranmeldung
- Möglichkeit eines **Software-Pflegevertrages** zur Sicherstellung nötiger Updates
- Einfaches **Update-Verfahren**, bei dem bisher eingegebene Daten erhalten bleiben
- Aufstockung der **Software-Lizenzen** (mehr Kameras, zusätzliche Funktionen) ohne Neuinstallation

Schließlich sollte die Ausschreibung auch eine Liste der Videogeräte enthalten, die aktuell und in Zukunft damit aufgeschaltet werden sollen. Dabei muss auch die **Integrationsstiefe** definiert werden, also welcher Funktionsumfang auf diesen Geräten genutzt werden soll, denn es ist ein großer Unterschied, ob nur Livebilder angezeigt werden sollen, oder ob auch alle Steuerungsfunktionen und Audio genutzt und vor Ort konfigurierte Metadaten und aufgezeichnete Videos abgerufen werden sollen.

#### Checkliste Integrationstiefe:

- Anzeige Livebild
- Umschalten verschiedener Video-Auflösungen
- Split-Darstellung mehrerer Kamera-Eingänge neben- und übereinander
- Abruf Kameraliste mit Kameranamen von der Bildquelle
- Umschalten verschiedener Kamera-Eingänge
- Steuern der Kamera (Schwenken, Neigen, Zoomen, Focus, Iris (Blende), Wischer, ...)
- Abruf Presetliste, Konfigurieren und Ansteuern von Preset-Positionen
- Fernsteuern von Schaltkontakten (Türöffner, Licht, Sirene, ...)
- Fernabfrage von Schalteingängen
- Fernabruf gespeicherter Bilder von der Bildquelle
- Abruf einer Senderkennung zum eindeutigen Identifizieren der Bildquelle
- Empfang von  Alarmbildern  Vor- und Nach-Alarmbildern  Meldungen  
via  FTP  E-Mail (SMTP)  TCP/IP  ISDN  \_\_\_\_\_
- Audio:  Abspielen auf der Bildquelle vorkonfigurierter Ansagen aus einer Liste
- Nur Hören  Nur Sprechen  Wechselsprechen  Gegensprechen  Aufzeichnen
- Sonderfunktionen: \_\_\_\_\_

#### Mögliche **Bewertungskriterien**:

- Anschaffungskosten der Software
- Anschaffungskosten der zum Betrieb dieser Software nötigen Hardware
- Betriebskosten (incl. eigenem Personalaufwand)
- Effizienz (Anzahl Streams, die pro Server verarbeitet werden können)
- Wie viele Videokanäle können in welcher Auflösung und Framerate angezeigt werden?
- Reaktivität: Wie schnell reagiert die Software auf Benutzereingaben?
- Funktionalität (vgl. Punkte aus Abschnitt 10.8.8)
- Bedienungskomfort, Benutzerführung
- Produktivität: Wie gut werden die Arbeitsabläufe unterstützt?
- Mögliche Suchkriterien für Video-Recherche: Zeitpunkt, Ereignis, Metadaten, ...
- Plattformunabhängigkeit: Unterstützte Betriebssysteme
- Investitionssicherheit: Erweiterbarkeit durch Module und offene, gut dokumentierte Schnittstellen
- Zuverlässigkeit (Verfügbarkeit, Datensicherheit)
- Servicequalität (Beratung, Hotline, kundenspezifische Erweiterungen), Software-Pflege
- Einfache Installation und Netzwerkkonfiguration
- (Gibt es ein einfaches Setup? Wie viele Ports müssen an der Firewall freigegeben werden?)
- Gibt es eine Online-Hilfe? Wie umfassend und verständlich ist die Dokumentation?
- Referenzen? Beratungskompetenz? Qualität der eingereichten Dokumente?

## Betriebssysteme

Native Software, die ohne weitere Zwischenschichten direkt auf die Systemressourcen (Speicher, Netzwerk u.s.w.) zugreift, ist zwar sehr effizient, aber immer weniger Hersteller sind bereit, angesichts steigender Anforderungen des Marktes den damit verbundenen hohen Entwicklungsaufwand zu tragen.

Betriebssysteme stellen vielfältige universelle Funktionen und Protokolle in standardisierter Form bereit und entlasten damit die Anwendungsentwickler. Dies führt zu mehr Funktionsvielfalt bei geringeren Kosten und Zeitbedarf. Deshalb kommen auch auf den meisten IP-Kameras und Recordern inzwischen Betriebssysteme zum Einsatz.

Als Betriebssystem für kompakte Geräte (Kameras, Recorder) wird häufig Embedded LINUX verwendet, weil es wenig Ressourcen (CPU-Leistung, Speicherplatz) erfordert und keine Lizenzgebühren dafür anfallen.

Für den Betrieb von Servern werden sowohl LINUX als auch Windows genutzt. Auf den Anwender-PCs ist immer noch Microsoft Windows das mit Abstand meistgenutzte Betriebssystem.

Für mobile Endgeräte (Smartphones, Tablets) sind vor allem Android und iOS verbreitet. Allen Betriebssystemen ist gemeinsam, dass ihre Komplexität und weite Verbreitung viele Ansatzpunkte für mögliche Sicherheitslücken bieten. Deshalb müssen diese Systeme einer regelmäßigen Softwarepflege (Wartung) unterzogen werden, in deren Rahmen u.a. nötige Sicherheits-Updates installiert werden. Außerdem ist eine fachgerechte Konfiguration etwa der Netzwerkparameter Voraussetzung für einen sicheren Betrieb.

Von Vorteil sind Software-Lösungen, die plattformübergreifend - also sowohl unter LINUX als auch unter Windows - laufen und über Clients für Android und iOS verfügen.

## Software-Pflege (Wartung)

Für einen sicheren Betrieb der Software sind die Instandhaltungshinweise des jeweiligen Software-Herstellers zu beachten und die empfohlenen Instandhaltungsschritte sorgfältig auszuführen.

Beispiel einer Checkliste für die Software-Wartung:

- Funktion der Software noch einwandfrei vorhanden?- Statusanzeigen prüfen, Anwender nach Störungen befragen - Mit Betreiber prüfen, ob evtl. Softwarestörungen im Betriebsbuch eingetragen wurden
- Logbücher auf Fehlermeldungen und Warnungen durchsehen:- Anwendungsspezifische Protokolldateien der Management-Software - Eventlogs des Betriebssystems mit „Event-Viewer“ (Windows-Ereignisanzeige)
- Betriebssystem-Updates und insbesondere Sicherheits-Patches installieren
- Sicherheitseinstellungen und Virens Scanner auf den neuesten Stand bringen
- Verwendete Passworte von Zeit zu Zeit wechseln
- Prüfen, ob alle PCs mit der korrekten Systemzeit laufen (Vergleich mit Funkuhr)
- Reagiert der PC flüssig auf alle Eingaben, oder hakt es irgendwo?
- Systemauslastung mit Ressourcenmonitor prüfen:- Genügend Arbeitsspeicher frei?- CPU-Auslastung deutlich unter 100%?
- Prüfen, ob noch genügend freier Speicher auf den Festplatten vorhanden ist- ggf. alte Daten archivieren und Datenträger bereinigen
  - Restlebenserwartung von SSDs prüfen



- Backup anlegen und Rückspielen des Backups prüfen
- Bei redundant ausgelegten Anlagen prüfen, ob bei Ausfall einer Komponente (stromlos schalten) oder einer Verbindung (Stecker ziehen) tatsächlich der gewünschte Ersatzweg geschaltet und die Funktion aufrechterhalten wird. Diese Prüfung erfolgt selbstverständlich erst nach Rücksprache mit dem Betreiber der Anlage.

Um die Betriebssicherheit der Software zu gewährleisten, empfiehlt es sich, einen Softwarepflegevertrag abzuschließen. Die dynamische Entwicklung der Technik macht es erforderlich, dass Software stets auf dem neuesten Stand gehalten und an geänderte Umgebungsbedingungen (z.B. Updates des Betriebssystems oder neue Firmware in den Videogeräten) angepasst wird. Dabei ist zu berücksichtigen, dass eine Software während der Nutzung ständigen Verbesserungsbestrebungen unterworfen ist und daher u.U. in bestimmten Abständen ein Update erfolgen muss. Dies stellt keinen Mangel dar, sondern ist eine systemimmanente Eigenschaft von Software.

## Firmware-Updates

In der Praxis kann es vorkommen, dass sich durch ein Firmware-Update das Verhalten des betreffenden Gerätes ändert und die Kompatibilität zu anderen Systemkomponenten beeinträchtigt wird. Deshalb empfiehlt es sich, vor einem Update alle Informationen des Herstellers genau zu beachten, welche Änderungen ein Update mit sich bringt, um zu bewerten, ob das aktuelle Update überhaupt nötig und sinnvoll ist.

Ein laufendes Update darf nicht unterbrochen werden, denn ein Abbruch kann zu einem inkonsistenten Zustand des Gerätes führen, so dass es möglicherweise nicht mehr erreichbar ist und nicht mehr verwendet werden kann.

So wie jeder Eingriff in die VÜA sollte auch ein Firmware-Update vorab mit allen eventuell Betroffenen (Errichter, Betreiber, Anwender, Leitstelle) abgestimmt und anschließend im Betriebsbuch dokumentiert werden, damit eventuelle nachfolgend beobachtete Veränderungen und Störungen der richtigen Ursache zugeordnet werden können. Nach jedem Update muss die Funktionalität insbesondere im Zusammenspiel mit allen anderen Systemkomponenten der VÜA umfassend geprüft werden.

## Trends, Ausblick

Früher waren Videoüberwachungs-Systeme meist in sich geschlossene, örtlich begrenzte Anlagen. Heute wird zunehmend gewünscht, Videobilder kostengünstig über große Entfernungen transportieren, flexibel zwischen verschiedenen Standorten oder Organisationen austauschen und mit anderen Gewerken und Daten verknüpfen zu können. Dies ist nur mit modernen Softwarelösungen möglich.

Ein wichtiger Unterschied zwischen Hard- und Software besteht darin, dass Software per Update jederzeit leicht an neue Anforderungen angepasst werden kann und von der dynamischen Entwicklung im IT-Bereich (immer mehr Rechenleistung und Speicher für immer weniger Geld) profitiert, während Hardware schnell veraltet und an Wert verliert. Somit geht der Trend dahin, anwendungsspezifische Hardware durch flexible Software-Lösungen zu ersetzen.

Dies betrifft insbesondere die Video-Decoder zur Anzeige der Videos auf Monitoren oder einer Video-Wall: Sind diese an eine dedizierte Hardware gebunden, so können deren Restriktionen dazu führen, dass künftige verbesserte Videostandards oder Sonderformate damit nicht mehr dargestellt werden können. Eine Videowiedergabe mittels Software-Codecs auf Standard-IT-Plattformen ist dagegen viel flexibler und somit zukunftssicherer.

Ein weiterer wichtiger Trend geht in Richtung Digitalisierung und Vernetzung. Bisherige „Insellösungen“ verschiedener Hersteller werden dadurch miteinander verbunden; aus bisher homogenen Videoanlagen werden heterogene Systeme, die Videokomponenten verschiedener Hersteller mit-

einander kombinieren. Mit Hilfe von Video-Encodern können auch alte analoge Anlagen (Bestandssysteme) in moderne vernetzte Systeme integriert werden. Alle dazu nötigen Steuerprotokolle und Formatwandlungen können in Software implementiert werden. Einige Firmen haben sich genau darauf spezialisiert, solche Integrationsleistungen zu erbringen und können bei Bedarf jedes System anbinden. Mit neuen Technologien wie etwa VirtualEnvironment können sogar solche Systeme integriert werden, zu denen keine Schnittstellenbeschreibung vorliegt.

Weltweit werden immer mehr Kameras installiert. Es gibt aber bei weitem nicht genügend Personal, um diese Bilderflut vollständig auszuwerten. Deshalb geht ein weiterer Trend dahin, mittels immer ausgefeilterer integrativer Videomanagement-Software die Auswertung der Videobilder möglichst umfassend zu unterstützen, den Menschen von Routineaufgaben zu entlasten, Zusammenhänge herzustellen und den Blick auf das Wesentliche zu lenken.

Wichtig sind dabei realistische Erwartungen an die Software: Bei fachgerechter Planung ist es heute durchaus möglich, für bestimmte, wohldefinierte Aufgabenstellungen sehr effiziente Lösungen zu schaffen, die genau auf Organisationsstruktur und Arbeitsabläufe der Anwender abgestimmt sind - darin liegen noch erhebliche Rationalisierungspotenziale. Aber auch die modernste Software kann keine Wunder vollbringen, sondern nur Algorithmen ausführen, die Planer durchdacht und Entwickler ihr vorgegeben haben.

So beeindruckend die Fortschritte in der Software-Technologie auch sind: Der Mensch bleibt auf absehbare Zeit als letzte Entscheidungsinstanz unentbehrlich. Somit sollte sich die Software stets am Menschen (d.h. am Anwender, Operator, Pförtner, Zentralist, Alarmbearbeiter, Leitstellen-Mitarbeiter) orientieren und nicht umgekehrt. Damit das gelingen kann, kommt es auf eine intensive, offene Kommunikation und ein gutes gegenseitiges Verständnis zwischen Anwender, Planer, Errichter und Software-Lieferanten an.

© BHE; 2014/10

Diese BHE-Information wurde vom Fachausschuss für Videoüberwachungstechnik (FA-VÜT) erstellt und steht unter [www.bhe.de/software](http://www.bhe.de/software) zum Download zur Verfügung.

**BHE Bundesverband Sicherheitstechnik e.V.**

Feldstraße 28, 66904 Brücken, Tel: 06386 9214-0, Fax: 06386 9214-99

E-Mail: [info@bhe.de](mailto:info@bhe.de), Internet: [www.bhe.de](http://www.bhe.de)

