10. Schnittstellen zu anderen Systemen

10.1 Allgemeines

Durch die intelligente Verbindung der Videotechnik mit anderen Sicherheitsgewerken kann die Sicherheit entscheidend erhöht werden. Das Zusammenwirken und die Verknüpfung aller wichtigen Meldungen zwischen der Videosicherheitsanlage und anderen Systemen bildet die Basis für ein umfassendes Sicherheitskonzept zum Schutz von Personen und Sachwerten. Für die Verknüpfung der unterschiedlichen Sicherheitsgewerke stellen die Hersteller entsprechende Schnittstellen zur Verfügung.

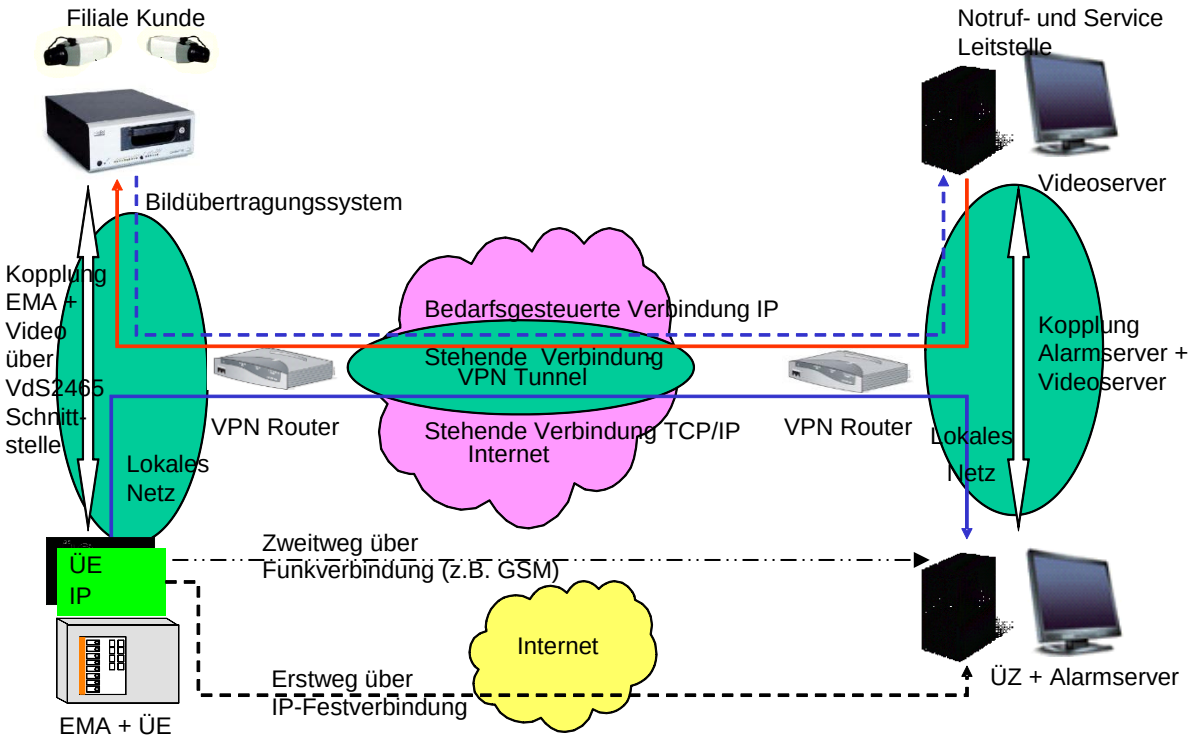
Sinnvoll und realisierbar sind je nach Anwendungsfall Kombinationen der Videosicherheitsanlage mit der Einbruchmeldetechnik, der Brandmeldetechnik, der Zutrittssteuerungstechnik, der Freigeländeüberwachungstechnik bzw. mit Systemen für Flucht- und Rettungswege.

10.2 Kombination zur Einbruchmeldetechnik

Zur Veranschaulichung der Kombination von Videosicherheit und Einbruchmeldetechnik wird nachfolgend ein konkreter Erfahrungsbericht eines Handelsunternehmens dargestellt.

Bei der Bestandsaufnahme der Sicherheitsanlagen in mehreren Filialen waren Einbruchmeldeanlagen von verschiedenen Herstellern eingebaut. Die lokal eingebauten Videosysteme wurden nur zur Warensicherung im Ladenlokal genutzt, ein Bildübertragungssystem war nicht vorhanden. Bei dem Betreiber kam es vermehrt zu Raubüberfällen beim Verlassen der Filiale, zu Einbrüchen mit Insiderwissen und zu Blitzeinbrüchen.

Im Zuge der Überarbeitung der Sicherheitskonzeption wurden mehrere Maßnahmen ergriffen.
Die nachfolgende Grafik zeigt eine Systemskizze der kombinierten Anlage:



Sämtliche Standorte wurden mit Bildübertragungssystemen ausgestattet und die Übertragungsgeräte ersetzt, um eine Leitungsüberwachung zu ermöglichen (über das kundeneigene VPN). Es folgte die Kopplung der Bildübertragungs- und Aufzeichnungssysteme mit der vorhandenen EMA Technik. Zusätzlich wurden zeitkritische Zustände überwacht (Scharfschaltung fehlt, Unscharf außerhalb Zeitfenster, Unscharf nach Scharfschaltung).

Nach der Inbetriebnahme konnten durch die kombinierte Anlage mehrere bestätigte Einbruchereignisse und Sabotageangriffe auf die Außenkameras detektiert werden. In zwei Fällen führte dies zur Festnahme der Täter durch die Polizei.

10.3 Kombination zur Brandmeldetechnik

Zur Kombination von Videosicherheit mit Brandmeldetechnik wird in der Praxis die Brandfrüherkennung durch Videobildauswertung betrieben.

Die Videokamera wird dank modernen Bildauswertemethoden immer häufiger zum Sensor für verschiedene Ereignisse. Neben dem Erkennen und Vergleichen von Personen, Fahrzeugen und Bewegungen, ist es naheliegend, die digitale Bildauswertung auch zum Detektieren von Rauch und Feuer einzusetzen, als sogenanntes Videobranderkennungssystem. Bei dieser Form der Brandfrüherkennung muss im Gegensatz zur Objekterkennung jede Art von Feuer und Rauch im Bild erkannt werden. Bei den am Markt verfügbaren Produkten gibt es Lösungen, die mit Spezialkameras, optischen Filtern oder speziellen Beleuchtungen arbeiten und solche, die Bilder von Standard-Überwachungskameras auswerten.

10.4 Kombination zur Zutrittssteuerung

Die Zutrittssteuerung ist darauf angewiesen, dass sich ihre Nutzer kooperativ verhalten und ihre PIN eingeben, ihren Ausweis vor das Zutrittsterminal halten oder den Sensor eines biometrischen Erkennungssystems benutzen. Aber sie kann üblicherweise nicht die Situation überschauen, die sich vor, während oder nach der Buchung abspielt.

Hier verspricht eine integrierte und koordinierte Anwendung von Zutrittssteuerung und Videosicherheit Abhilfe. Mit entsprechender Software und den Kameras als Sensor können Gesichter auf Distanz erkannt, das Verhalten von Personen beurteilt und bei Verletzung virtuell aufgebauter Bildbereiche Alarme ausgeben werden. Außerdem ist per Kamera und virtueller Vereinzelungsräume festzustellen, ob sich der Benutzer allein vor dem Zutrittsterminal befindet oder ob er z.B. einer Bedrohung ausgesetzt ist. Diese Technik ist aber auch einsetzbar, wenn der Berechtigte schon frühzeitig erkannt werden soll und ihm bereits die Tür offensteht.

Alle diese Möglichkeiten sind heute schon realisierbar. Sie liefern den Sicherheitsverantwortlichen des Unternehmens Informationen für ihre Entscheidungen zur Abwehr einer Gefahrenlage meist schon bevor sich die Situation zugespitzt hat.

Ein Zutrittssteuerungssystem bietet zudem die Möglichkeit, Lieferanten- und Personalmanipulationen zu verhindern bzw. zu erschweren. In Verbindung mit Videosicherheitsanlagen lassen sich hiermit auch sehr erfolgreich "Austrittsüberwachungen" vornehmen.

Mithilfe von LPR/Kennzeichenerkennung lässt sich die Videosicherheitsanlage ebenfalls gut in die Zutrittssteuerung von Einfahrten implementieren.

Deshalb werden Zutrittssteuerung und Videosicherheit in Zukunft noch stärker integriert und ihre Stärken für die Bereiche Organisation und Sicherheit zur Anwendung in die Unternehmen einbringen.

10.5 Kombination zur Freigeländeüberwachungstechnik

Die ganzheitliche Sicherheit von Objekten beginnt bereits an der Grundstücksgrenze. Hierfür werden auch für Außenanlagen bedarfsgerechte Freigeländeüberwachungssysteme am Markt angeboten. Der entscheidende Vorteil dieser Systeme liegt darin, dass durch eine sehr frühzeitige Detektion im Außenbereich eine Verlängerung der Reaktionszeit für Interventionsmaßnahmen gewonnen wird.

In der Regel ist jedoch bei Freigeländeüberwachungssystemen mit mehr unerwünschten Meldungen zu rechnen als bei Einbruchmeldeanlagen im Innenbereich. Eine technische Optimierung kann z.B. durch eine UND-Verknüpfung zweier Detektionssysteme mit unterschiedlichen physikalischen Wirkweisen erreicht werden. Hierbei werden Systeme kombiniert, die auf Umwelteinflüsse unterschiedlich reagieren, z.B. Zaundetektion (akustisch) mit Videodetektion (optisch).

Ein wichtiger Punkt stellt die Alarmverifikation dar. Bei großen und/oder sensiblen Überwachungsbereichen wird daher generell empfohlen, den Alarm durch ein Videosystem zu verifizieren. Der Vorteil der Kombination gegenüber einer reinen Videosicherheit liegt in der gezielten Aufschaltung der Kamera. Der Bediener betrachtet gezielt ein Kamerabild und ermüdet dadurch nicht so stark, als wenn er die durchlaufenden Kamerabilder ständig beobachten müsste.

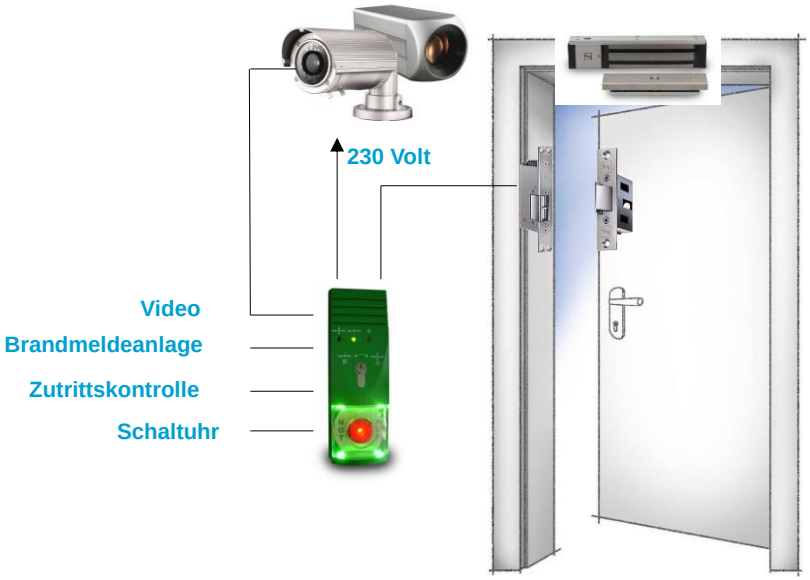
10.6 Kombination zu Systemen für Flucht- und Rettungswege

Die zwangsöffnende Nottaste ist das wichtigste Element eines Fluchttürsystems. Der Absatz 3.1.2 der EltVTR (Richtlinie über elektrische Verriegelungssysteme von Türen in Rettungswegen) enthält deshalb die prinzipielle Forderung nach einer Nottaste an der Tür. Dennoch wird im Absatz 3.1.3 die Möglichkeit zur indirekten (zentralen) Freischaltung durch eine ständig besetzte, zentrale Stelle erwähnt. Die Gesetzeslage setzt für Fluchttürverriegelungen ohne Nottaste an der Tür immer eine Genehmigung im Einzelfall voraus.

Hierbei werden meist folgende Auflagen verlangt:

- Die Stelle, an der sich die zentrale Nottaste befindet, muss ständig besetzt sein. Es sind daher mindestens 2 Mitarbeiter erforderlich.
- Darüber hinaus wird die (direkte) Einsicht auf sämtliche gesicherten Fluchttüren gefordert.
- Videosysteme können in Absprache mit der Baubehörde akzeptiert werden. Damit ergeben sich für die Betreiber solcher Objekte deutliche Einsparpotenziale durch den Videoeinsatz.

Die nachfolgende Grafik zeigt die Systemskizze der kombinierten Anlage:



10.7 Vorteile und Ziele ONVIF (Open Network Video Interface Forum)

Das offene Industrie-Forum ONVIF (Open Network Video Interface Forum) arbeitet an einem globalen Standard für die Schnittstelle von physischen, IP-basierenden Security-Produkten. Es soll weltweit die gemeinsame Kommunikation verschiedener IP-Produkte innerhalb der Videosicherheit und anderer physischer Sicherheitsbereiche sicherstellen. Die Triebfeder für ONVIF war der Wunsch nach herstellerübergreifender Kommunikation zwischen IP-Video-Produkten. Heute beinhaltet ONVIF auch Standards für Produkte der Zutrittssteuerung und einheitliche Schnittstellen für Sicherheits-Managementsysteme.

ONVIF ist eine Organisation, die im Jahr 2008 von Axis Communications, Bosch Sicherheitssysteme und Sony gestartet wurde. Es ist eine offizielle Non-Profit-Organisation (501 (c) 6 Delaware Corporation), deren Mitgliedschaft offen ist für Hersteller, Software-Entwickler, Berater, Systemintegratoren, Endnutzer und andere Interessengruppen, die an den Aktivitäten teilnehmen möchten.

Die Eckpfeiler von ONVIF sind:

- Standardisierung der Kommunikation zwischen Netzwerk-Sicherheitsgeräten
- Interoperabilität zwischen Herstellern von Netzwerk-Sicherheitsprodukten
- Offen für alle Unternehmen und Organisationen

Die aktuellen Profile und ihre Funktionalitäten:

- **Profil S: IP-Video-Quellen**
  Video und Audio Streaming, PTZ Funktionen und potenzialfreie Kontakte, Status-Information und Multicast
- **Profil C: IP-Zutritts-Steuerungen**
  Status-Information und Konfiguration, Event & Alarmmanagement, Türzustandsüberwachung
- **Profil G: IP-Medien-Speicher**
  Video- und Audiowiedergabe, Videoaufnahmen und Ereignissuche, Konfiguration und Steuerung der Aufnahmen
- **Profil Q: Integration von Geräten der Sicherheitstechnik**
  Standardisierte Erkennung, Einrichtung und Konfiguration konformer Geräte, Datenintegrität und -sicherheit

Motivation

Das Ziel des Forums ist die Entwicklung und Nutzung eines globalen, offenen Standards für die Schnittstelle der Netzwerk-Sicherheitsprodukte. Die Interoperabilität wird, unabhängig vom Hersteller, zwischen Netzwerk-Sicherheitsprodukten sichergestellt. Dadurch lassen sich Betreiber, Integratoren, Berater und Hersteller zunehmend von der IP-Netzwerk-Video-Technik überzeugen, was zu kostengünstigeren und flexiblen Lösungen führt.

Die ONVIF-Spezifikation definiert ein gemeinsames Protokoll für den Austausch von Informationen der Netzwerk-Video-Geräte zwischen Live-Video, Audio, Metadaten und Steuerungsinformationen. ONVIF-konforme Netzwerk-Video-Sender und Empfänger von verschiedenen Herstellern sollten in der Lage sein, störungsfrei miteinander zu kommunizieren. Die Spezifikation definiert, dass konforme Geräte im Netzwerk sowie im Video-Management-System automatisch erkannt werden.

Vorteile von ONVIF

Vorteile des offenen Standards für Netzwerk-Sicherheitsprodukte:

- Interoperabilität: Produkte verschiedener Hersteller können in einer Systemlösung in einheitlicher Sprache miteinander kommunizieren

- Flexibilität: Betreiber und Integratoren sind nicht innerhalb von proprietären Lösungen eingeschränkt
- Zukunftssicher: Standard stellt sicher, dass auf dem Markt interoperable Produkte verfügbar sind
- Qualität: Kommunikationsschnittstelle ist im Produktstandard klar definiert

Vorteile Anwender / Kunde:

- Hohe Flexibilität und Freiheit bei der Produkt-Auswahl
- Der Standard ermöglicht es, interoperable Produkte aus einer Vielzahl von Herstellern zu wählen
- Zukunftssichere Systeme und sichere Anlagen

Vorteile Integratoren:

- Zuverlässige Interoperabilität
- Interoperabilität zwischen den verschiedenen VSS-Produkt-Lieferanten
- Vereinfachte Installationen
- IP-basierte, unabhängige, physische Sicherheitsprodukte, die einfach installiert und eingesetzt werden können
- Mehr Flexibilität in den Produkten, um auf die spezifischen Bedürfnisse der Kunden einzugehen

Vorteile des offenen Standards für Netzwerk-Sicherheitsprodukte:

- Erhöhte Nachfrage der IP-basierten Security-Produkte und -Lösungen im Markt
- Sofortige Interoperabilität mit anderen Herstellern ohne Qualitätseinschränkungen
- Erweiterte Marktmöglichkeiten durch weltweiten Einsatz der IP-basierten physikalischen Sicherheitslösungen

Organisation