Sebastian Welzbacher

Planung eines Videoüberwachungssystems

Gängige Standards in Analog- und IP-Technologie

Diplomica Verlag

Sebastian Welzbacher
Planung eines Videoüberwachungssystems: Gängige Standards in Analog- und IP-Technologie

ISBN: 978-3-8428-2781-3
Herstellung: Diplomica® Verlag GmbH, Hamburg, 2012

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Im Jahr 2008 wurde in Deutschland durchschnittlich alle zwei Minuten eingebrochen, sowohl in gewerblichen als auch in privaten Objekten („Einbrüche“, 2009). Mehr als ein Drittel dieser Einbruchsversuche scheiterte jedoch an vorhandener Sicherheitstechnik. Auch die Videoüberwachung trägt durch die Abschreckung möglicher Täter und die nachträgliche Aufklärung von Straftaten zur Sicherheit bei. Hierzu bedarf es allerdings einer gründlichen Planung und fachgerechten Zusammenstellung des Videoüberwachungssystems, wie auch das Beispiel von Landolt (2010) zeigt: Ein unbekannter bewaffneter Mann dringt in die Hirslanden-Klinik in der Schweiz ein, um die Herausgabe von Morphium zu erzwingen. Trotz vorhandenem und in Betrieb befindlichem Videoüberwachungssystem existieren keine brauchbaren Bilder für die Fahndung. In diesem Fall waren wahrscheinlich die folgenden Gründe ausschlaggebend für den Misserfolg: Zum einen wurden teilweise Kameraattrappen eingesetzt, die nur zur Abschreckung dienen. Zum anderen waren die funktionierenden Kameras veraltet und lieferten qualitativ schlechtes Bildmaterial mit zu niedriger Auflösung für eine Identifikation des Täters. Zudem wurden die Bilder nur live übertragen, jedoch nicht gespeichert. Somit fehlt der Polizei eine realistische Chance auf einen Fahndungserfolg.

So stellt auch Niecke (2009a) in seinem Artikel fest, dass zunächst die örtlichen Gegebenheiten sowie der Bedarf festgestellt werden müssen. Denn erst durch die richtige Planung kann der gewünschte Effekt erzielt und eine Erhöhung der Sicherheit erreicht werden. Die eingesetzten Komponenten müssen auf die Anforderungen der Überwachungsaufgabe abgestimmt sein: „Die Überwachung und Verfolgung von

Objekten mit einer Kamera ist bei Tag eine einfache Sache. Aber bei Nacht könnten wir nichts mit unseren Tageslichtkameras sehen.“ (Maras, 2007, S. 63).
Dieser Problemstellung widmet sich das vorliegende Buch, wie anschließend in Kapitel 2 noch ausführlicher erläutert wird.

2 Zielsetzung und Zielgruppe des Buchs

Ziel dieses Buchs ist es einerseits, eine Einführung in das Themengebiet Anforderungen und Komponenten in der Videoüberwachung sowie eine Übersicht über den aktuellen Stand in diesem Bereich anzubieten. Andererseits kann es auch als praktische Arbeitshilfe zur Planung oder Bewertung eines Videoüberwachungssystems und der Auswahl geeigneter Komponenten genutzt werden.
Hierzu werden zunächst einige ausgewählte Anforderungen erörtert, die für ein Videoüberwachungssystem relevant sind (Kapitel 3). Daraus können entsprechend der Gegebenheiten vor Ort und der eigenen Zielsetzung die passenden Anforderungen ausgewählt und bei Bedarf priorisiert werden. Im Anschluss werden aktuell gängige Unterscheidungskriterien für Komponenten eines Videoüberwachungssystems aufgeführt, kurz erläutert, auf ihre Kompatibilität untersucht und im Hinblick auf die Erfüllung der ausgewählten Anforderungen bewertet (Kapitel 4).
Das Buch richtet sich hierbei an Personen, die zwar über grundlegende Kenntnisse im Bereich der Sicherheitstechnik verfügen, sich bisher aber nicht oder zumindest nicht ausführlicher mit Videoüberwachungssystemen im Allgemeinen und ihrer Planung und der Auswahl von Komponenten im Speziellen beschäftigt haben.

3 Anforderungen an Videoüberwachungssysteme

3.1 Einführung

Abhängig vom Einsatzbereich kann eine Vielzahl von Anforderungen an ein Videoüberwachungssystem gestellt werden. Bei der Planung muss zunächst eine Auswahl und Priorisierung der Anforderungen an das System auf Grundlage der Bewertung der bestehenden Situation und den selbst definierten Zielen stattfinden. Darauf basierend können anschließend die Kriterien und technischen Anforderungen an die einzelnen zu verwendenden Komponenten ermittelt werden. Im Folgenden werden häufig gestellte Anforderungen thematisch in neun Bereiche zusammengefasst und anhand der zugrunde liegenden Problemstellung erläutert.

Hierbei werden nur direkt auf die Überwachungsaufgabe an sich ausgerichtete Anforderungen betrachtet. Weitergehende Anforderungen an Beschaffung, Einrichtung und Betrieb, z.B. niedrige Anschaffungs- und Betriebskosten oder geringer Speicherplatzbedarf, sind nicht Bestandteil dieses Buchs. An einigen relevanten Stellen finden sich jedoch auch entsprechende Hinweise dazu.

Behandelt werden die folgenden Anforderungen:

- Identifikation/Erkennbarkeit
- Analyse/Auswertung/Intelligenz

- Integration/Zusammenarbeit mit anderen Systemen
- Schwierige Sichtverhältnisse
- Widrige Umgebungsbedingungen
- Schutz vor Vandalismus/Sabotage
- Hohe Verfügbarkeit
- Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit
- Integrität/Überprüfbarkeit/Beweiskraft

3.2 Übersicht und Beschreibung ausgewählter Anforderungen

3.2.1 Identifikation/Erkennbarkeit

Eines der vorrangigen Ziele der Videoüberwachung stellt sicherlich das Erkennen und die Identifikation dar. Dies kann sich, je nach Einsatzbereich, auf Personen, Gegenstände, Vorgänge, Fahrzeug-Kennzeichen oder ähnliches beziehen. So etwa zur Überwachung unbesetzter Zugänge zu Gebäuden (Kraheck et al., 1999, S. 33). Einerseits soll hierdurch die möglichst schnelle und exakte Bewertung während des Auftretens eines Ereignisses durch die überwachenden Personen ermöglicht werden, andererseits sollen aber auch im Anschluss „[...]die Voraussetzungen für das polizeiliche Handeln (z.B. Gefahrenabwehr, Fahndung) verbessert werden“ (VdS 2366, 2004, S. 3).

Die VdS-Richtlinie 2366 (2004) definiert hierzu den Begriff Verifizieren als das „Bewerten einer (bildlich dargestellten) Situation“, was je nach Einsatzbereich und gewünschtem Ziel das

- Wahrnehmen: „Feststellen eines Ereignisses (Abweichung vom Normalzustand) mit dem Ziel, die Sicherungsrelevanz zu bewerten.“
- Erkennen: „Erkennen von eindeutig zuordenbaren spezifischen Merkmalen, deren Details die Identität einer bekannten Sache oder Person feststellen lassen.“
- Identifizieren: „Erkennen von eindeutig zuordenbaren spezifischen Merkmalen, deren Details die Identität einer unbekannten Sache oder Person feststellen lassen.“

voraussetzen kann.

Um diese Anforderungen zu erfüllen, legt die Richtlinie konkrete Relationen zwischen dem Auflösungsvermögen und dem überwachten Bereich fest, die folgendermaßen lauten:

- Wahrnehmen: Ein Bildpunkt (Pixel) deckt 20mm des überwachten Bereichs ab.
- Erkennen: Ein Bildpunkt (Pixel) deckt 5mm des überwachten Bereichs ab.
- Identifizieren: Ein Bildpunkt (Pixel) deckt 1mm des überwachten Bereichs ab.

Somit stehen dem Anwender im Bereich der Erkennbarkeit und Identifikation, abhängig von gewünschter Verwendung, Anforderungen an die technische Leistungsfähigkeit des Videoüberwachungssystems zur Verfügung, mit denen die gesetzten Überwachungsziele erreicht werden können.

3.2.2 Analyse/Auswertung/Intelligenz

Aktuell stark nachgefragt und im Fokus stehend ist die Fähigkeit einer Videoüberwachungsanlage zu intelligenter Bildanalyse und -auswertung. Diese Art von Funktionen entlastet den Menschen und erhöhen die Effektivität und Zuverlässigkeit des Gesamt-Systems um ein Vielfaches. Weinzierl (2008) führt aus, dass die menschliche

Aufnahmefähigkeit nur sehr begrenzt ist. So nimmt etwa ein Beobachter zweier unterschiedlicher Situationen an zwei Bildschirmen nach 12 min nur noch die Hälfte, nach 22 min bereits nur noch fünf Prozent war. Die Analyse- und Auswertungsfunktionen können dem entgegen wirken, indem sie Bilder nur übertragen und/oder speichern, wenn eine sicherheitsrelevante Situation erkannt wird und die Beurteilung und Entscheidung durch einen menschlichen Beobachter erforderlich wird. Hierdurch entfällt das ermüdende ständige Beobachten von Bildschirmen, ohne dass jedoch mögliche kritische Ereignisse unbemerkt bleiben.

Mittlerweile gehen die Möglichkeiten über die bereits seit längerer Zeit bekannte einfache Bewegungserkennung weit hinaus. Beispielsweise können mit Hilfe mathematischer Algorithmen entwendete oder liegen gelassene Gegenstände gemeldet, Rauchentwicklung oder verdächtiges Verhalten von Personen detektiert werden. Dabei existieren neben den reinen Sicherheitsanwendungen zahlreiche weitere Einsatzbereiche. Als Beispiele sei hier die statistische Auswertung von Kundenbewegung und -Frequentierung im Einzelhandel genannt (Weinzierl, 2008). Für nahezu jede denkbare Aufgabe existieren inzwischen die technischen Möglichkeiten zur erfolgreichen Umsetzung. Wie Bodell (2010) es formuliert: „Die Möglichkeiten sind fast unbegrenzt. Man denke an Kameras die nur aufnehmen, wenn sie ein Gesicht sehen oder Videodaten nur dann sendet [sic], wenn es [sic] ein Kfz-Kennzeichen erkennt [sic].“

Die Anforderung an ein Videoüberwachungssystem, solche Funktionen zu beherrschen, kann somit in vielen Einsatzbereichen sinnvoll gestellt werden.

3.2.3 Integration/Zusammenspiel mit anderen Systemen

Wie auf den Präsentations-Ständen auf einschlägigen Fachmessen, sowie aus aktuellen Produktübersichten gängiger Hersteller und Anbieter von Videoüberwachungstechnik ersichtlich ist, geht der Trend klar in Richtung vernetzter Systeme. Die unterschiedlichen Gewerke, wie Videoüberwachungsanlage, Zutrittskontrollsystem, Brandmeldeanlage oder auch IT-Verbund, werden immer öfter als Gesamtsystem

betrachtet und zusammen geschaltet. So wird bereits von der Messe Security 2008 berichtet:

> *„Im diesjährigen thematischen Fokus steht: Interoperabilität der Systeme für Gebäudetechnik. Dabei werden Zutrittskontrolle, Videoüberwachung und Einbruchmeldung mit den übrigen Gewerken der Gebäudeinfrastruktur unter Nutzung der vorhandenen Gebäude-IT-Infrastruktur kombiniert.“ (Kräußlich, 2008a)*

Hieraus ergeben sich zahlreiche Synergien und Vorteile. Beispielsweise kann bei Zugriff auf Zutrittskontroll- oder IT-System (etwa bei Betreten eines Gebäudes oder Einloggen an einem PC-Arbeitsplatz) automatisch ein Standbild derjenigen Person mit dem jeweiligen Ereignis verknüpft abgespeichert werden. So lassen sich beinahe lückenlos die Wege und Tätigkeiten aller Personen im überwachten Bereich rekonstruieren und bei Unstimmigkeiten überprüfen. Auch die Nutzung von Überwachungskameras als Branddetektoren mit Aufschaltung auf die Brandmeldeanlage ist mittlerweile möglich.

Es ist daher nicht verwunderlich, dass bei der Neuplanung oder Aufrüstung von Videoüberwachungssystemen eine oft gestellte Anforderung die Vernetzbarkeit mit bestehenden oder ebenfalls in Planung befindlichen weiteren Systemen ist.

3.2.4 Schwierige Sichtverhältnisse

Vor allem bei der Überwachung im Außenbereich treten mitunter sehr schwierige und sich häufig ändernde Sichtverhältnisse auf. Wie von Hilpert (2009) festgestellt, teilweise innerhalb von Zeiträumen im Minutenbereich und noch darunter. Nicht zu vergessen natürlich die grundsätzlich gegensätzlichen Sichtbedingungen bei Tag und Nacht generell. Hinzu kommen können Einflüsse wie Nebel, Regen oder Schneefall, welche die Sicht behindern. Darüber hinaus können bei Fahrzeugverkehr im Bildausschnitt, z.B. bei Zufahrten oder auf Parkplätzen, kurzzeitige Beleuchtungsspitzen durch Fahrzeugscheinwerfer auftreten.

Dennoch ist in einigen Anwendungsfällen die Beobachtung solcher Bereiche unabd-

ingbar. Neben der klassischen Perimeter-Sicherung der Wirtschaftsunternehmen sind hier vor allem Grenzschutzanwendungen und weitläufige sicherheitskritische Areale wie Häfen und Flughäfen zu nennen. Die Problematik wird sehr anschaulich durch die Worte von Frank Christensen deutlich gemacht, dem Abteilungsleiter des Sicherheitsbetriebszentrums des Flughafens Kopenhagen:

> *„Die Überwachung und Verfolgung von Objekten mit einer Kamera ist bei Tag eine feine Sache. Aber bei Nacht könnten wir nichts mit unseren Tageslichtkameras sehen. Es ist unmöglich, den gesamten CSRA [der kritische Teil des Sicherheitsbereichs, Anm. d. Verfassers] zu beleuchten, da wir nicht überall Lichtmasten aufstellen können. Das würde den Verkehr der Flugzeuge zu und von den Start- und Landebahnen behindern. Wenn jedoch ein Alarm ausgelöst wird, wollen wir sehen können, was den Alarm verursacht hat, bevor wir Sicherheitsmitarbeiter zum Überprüfen der Situation vor Ort schicken.“ (Maras, 2007, S. 63)*

Somit wird klar, dass unter bestimmten Umständen die Funktion des Videoüberwachungssystems auch unter schwierigen Sichtverhältnissen eine notwendige Anforderung darstellen kann.

3.2.5 Widrige Umgebungsbedingungen

Ebenfalls erschwerend bei der Überwachung im Außenbereich wirken sich die Umgebungsbedingungen aus. Hilpert (2009) beschreibt neben Wind, Niederschlag, sehr hohen oder niedrigen Temperaturen und Temperaturschwankungen auch Faktoren wie Feuchtigkeit, Staub und Erschütterungen. Je nach geographischer Lage des Standortes und Aufstellungsort der Kameras können diese Bedingungen bis ins Extreme reichen.

Dennoch muss in manchen Anwendungsbereichen auch unter widrigsten Umständen die Videoüberwachung einwandfrei funktionsfähig bleiben.

3.2.6 Schutz vor Vandalismus/Sabotage

„Wer bei seinen Taten nicht gerne beobachtet wird, versucht Überwachungskameras auszuschalten“, macht Hilpert (2009) in ihrem Artikel deutlich. Dies kann unter anderem durch folgende Methoden erreicht werden:

- Beschädigung, Zerstörung
- Wegnahme
- Abdecken/Besprühen
- Verdrehen
- Defokussieren
- Trennen von der Übertragungseinrichtung oder Stromversorgung
- Vernichten oder Entwenden der aufgezeichneten Videobilder

Besonders gefährdet sind Kameras und andere Teile des Videoüberwachungssystems, die sich im von der VdS 2366 (2004) definierten Handbereich befinden. Dieser bezeichnet den „Bereich, der sich bis 3 m oberhalb einer frei zugänglichen Fläche befindet“ (S. 7). Aber auch die Möglichkeiten der Erreichbarkeit durch vorhandene oder mitgeführte Aufstiegshilfen müssen bedacht werden.

Werden Komponenten eines Videoüberwachungssystems in einem solchen oder einem anderen zugänglichen Bereich angebracht, und besteht Grund zu der Annahme einer Gefährdung durch Vandalismus/Sabotage, so müssen entsprechende Schutzmaßnahmen ergriffen werden.

3.2.7 Hohe Verfügbarkeit

In den allermeisten Einsatzbereichen ist die ständige Verfügbarkeit der übertragenen Bilder sowie der Aufzeichnung gewünscht oder sogar notwendig. Andernfalls können durch Ausfälle wirtschaftliche Schäden entstehen, etwa in Spielcasinos: „In

den meisten Casinos führen Ausfälle von Videoüberwachungssystemen zu verlorenen Spielzeiten und Gewinneinbußen.“ (Lahr, 2010, S. 45). Aber auch in vielen anderen sicherheitskritischen Anwendungen ist eine hohe Verfügbarkeit wichtige Voraussetzung, etwa bei der Überwachung von Flughäfen: „wir müssen sicher sein, dass die Kameras 24 Stunden am Tag arbeiten, und das an 365 Tagen im Jahr“ (Maras, 2007, S. 63). Im ungünstigsten Fall können darüber hinaus sicherheitsrelevante Ereignisse unbemerkt bleiben und/oder wertvolles Fahndungs- und Beweismaterial nicht zur Verfügung stehen. Gerade im Bereich der Sicherheitstechnik können, anders als beispielsweise in der Netzwerktechnik, auch nur kurzzeitige Unterbrechungen zu ernsthaften Folgen führen: „Ein Netzwerk, das regelmäßig für einige wenige Sekunden ausfällt oder stockt, mag für IT-Anwendungen noch ausreichend sein, für eine Videoüberwachung kann dies fatal sein.“ (Fourmont, 2009, S. 28).

Daher sollte eine möglichst lückenlose Übertragung und Speicherung der Videobilder garantiert werden. Davon betroffen sind hauptsächlich die Komponenten Stromversorgung, Aufzeichnungssystem sowie Übertragungsweg. So fordert beispielsweise die BGI 819-2 (2008), welche Anforderungen an die sicherheitstechnische Ausrüstung von Kredit- und Finanzinstituten beschreibt: „Bei einem Stromausfall dürfen die bis dahin bereits aufgezeichneten Bilder nicht verloren gehen. Außerdem hat die Anlage nach Beendigung des Stromausfalls selbstständig wieder in Betrieb zu gehen.“ (S. 33)

3.2.8 Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit

Im Sinne der Wirtschaftlichkeit, Investitionssicherheit und des Bestandserhaltes ist es auch im Falle von Videoüberwachungssystemen wünschenswert, dass diese sich in ihrem Umfang an die Bedürfnisse des beabsichtigten Einsatzes anpassen, mit geringem Aufwand beliebig erweitern und entsprechend dem aktuellen technischen Stand aufrüsten lassen. Zusätzliche Kameras, Überwachungsplätze und Speicherkapazitäten sollten sich ebenso problemlos wie neue Technologien in das vorhandene

System integrieren lassen. Dies kann beim Bau eines zusätzlichen Gebäudes, der Änderung von Vorgaben und Regelwerken oder auch geänderter Situation vor Ort (z.B. Umgebung oder Nutzung) der Fall sein. In besonderem Maße trifft dies beispielsweise auf Einrichtungen wie den Industriepark Frankfurt-Höchst zu: „Der attraktive Standort führt dazu, dass sich immer neue Unternehmen ansiedeln, so dass das System für künftige Erweiterungen flexibel sein muss. Zudem sollte eine problemlose Integration in bereits bestehende Systeme möglich sein.“ (Niehus, 2008, S. 55f.)

3.2.9 Integrität/Überprüfbarkeit/Beweiskraft

Um Manipulationen am Bildmaterial ausschließen und somit die Echtheit und Beweiskraft sicherstellen zu können, bedarf es eines wirksamen Kontrollmechanismus. Vor allem im digitalen Bereich ist diese Forderung mitunter nicht ganz einfach zu erfüllen: „Die Aufzeichnungen lassen sich mit geringem Aufwand mit Multimedia-Videobearbeitungssoftware manipulieren [...]“ (Lahr, 2010). Unter anderem kann dies jedoch durch eine wie von der BGI 819-2 (2008) geforderten Abspeicherung von Datum und Uhrzeit zusammen mit dem Bild erreicht werden. Weitere in dieser Vorschrift festgelegte Schutzmechanismen sind Sicherungen gegen unberechtigtes Wiedergeben, Ändern und Kopieren der Bilddaten. Hier kommt es also vor allem auf den Weg der Bilddaten von der Aufnahme bis zu Empfang/Aufzeichnung und den anschließenden Verbleib an.

4 Auswahlkriterien für Videoüberwachungssysteme

In diesem Kapitel werden aktuell gängige Unterscheidungskriterien in der Videoüberwachung behandelt. Die Auswahl erfolgte dabei auf Basis der derzeitigen Marktsituation sowie der Entwicklung innerhalb der letzten Jahre. Die Recherche hierzu umfasste Produktübersichten und -beschreibungen bekannter Anbieter und Hersteller von Videoüberwachungstechnik, Artikel in verschiedenen Fachzeitschriften sowie Informationen und persönliche Gespräche auf der Messe it-sa 2010 in Nürnberg.

Hierzu werden zunächst jeweils die einzelnen Technologien, Verfahren und Standards erläutert. Dabei werden auch, soweit möglich, ihre in Bezug auf das Thema relevanten Vor- und Nachteile mit einbezogen.

Im Anschluss wird die Kompatibilität untereinander untersucht. Das daraus resultierende Ergebnis wird dann noch einmal übersichtlich in Tabellenform dargestellt. Hierbei werden innerhalb der Tabellen jeweils vier Symbole zur Repräsentation benutzt:

+ Voll/uneingeschränkt kompatibel.

o Teilweise/unter bestimmten Voraussetzungen kompatibel.

- Nicht kompatibel.

x Keine Aussage möglich, Zuordnung nicht sinnvoll.

Daraus wird ersichtlich, welche verschiedenen Komponenten mit welchen Eigenschaften in einem Videoüberwachungssystem zusammen eingesetzt werden können. Zu lesen ist die Tabelle von oben nach unten, d.h. in einer Spalte findet sich die Kompatibilität des Spalteneintrags jeweils zu den einzelnen Zeileneinträgen.

Zuletzt wird jeweils die Eignung zur Erfüllung der einzelnen in Kapitel 3 aufgeführten Anforderungen überprüft. Auch dieses Ergebnis wird anschließend noch in Tabellenform zusammengefasst. Dabei kommt eine ganzzahlige Punkteskala zum Einsatz: Von Null (Erfüllt die Anforderung gar nicht) bis Fünf (Erfüllt die Anforderung vollkommen/optimal). Wo notwendig, wird auch in diesen Tabellen das Symbol 'x' mit der äquivalenten Bedeutung wie in den Kompatibilitätstabellen (Keine Aussage möglich, Bewertung nicht sinnvoll.) verwendet. Diese Übersicht zeigt, in wie weit die jeweiligen Technologien, Verfahren und Standards die einzelnen formulierten Anforderungen erfüllen können.

Betrachtet und bewertet werden die folgenden Unterscheidungskriterien:

- Technologie/Videosignal
- Bildgebungsverfahren/Kameratyp
- Bild-Sensoren
- Auflösung
- Videodatenkompression
- Übertragung
- Aufzeichnung/Speicherung
- Protokolle und Schnittstellen
- Stromversorgung
- Schutz vor Einflüssen aus der Umgebung
- Prüfung/Zertifizierung

Diese Auswahl ist selbstverständlich nicht als vollständig und abschließend zu verstehen. Es existieren noch viele weitere Unterscheidungskriterien, welche aber unmöglich alle behandelt werden können und aus bestimmten Gründen nicht in die Auswahl aufgenommen wurden. Hierzu zählen beispielsweise die Objektive, da diese ausschließlich aufgrund des gewählten Beobachtungsbereiches, der Verhältnisse vor Ort und der Kameraleistung ausgewählt werden müssen. Ebenso die Beleuchtung, welche gleichfalls an die vorhandenen Bedingungen und gesetzten Ziele individuell angepasst werden muss.

4.1 Technologie/Videosignal

4.1.1 Übersicht und Beschreibung der Technologien

Grundsätzlich ist zwischen der ehemals ausschließlich vorherrschenden analogen und der neueren digitalen/IP-basierten Videoüberwachungstechnik zu unterscheiden. Wie von Wittmann (2009) festgestellt, geht der Trend der letzten Jahre klar in Richtung Digitaltechnologie. Hier werden jährliche Zuwachsraten von 30 bis 40 Prozent verzeichnet. Der Übergang vollzieht sich jedoch, auch dank der Möglichkeit hybrider Systeme, eher sanft und allmählich als sprunghaft. Während mittlerweile zum Beispiel im Bereich der Aufzeichnung nahezu ausschließlich digitale Technik den Markt bestimmt, wurden bei den Kameras im Jahr 2008 noch zu 80 Prozent analoge Geräte verkauft. Daher gilt es, die Vor- und Nachteile beider Technologien genauer zu betrachten.

Analog

Der Bildsensor (siehe Abschnitt 4.3) liefert ein elektrisches Signal. In der Analog-Technologie besteht dieses aus „potentiell unendlich vielen Zustandsmöglichkeiten bei potentiell unendlich kleinen kontinuierlichen Übergängen“ (Brauner, Raible-

Besten & Weigert, 1998, S. 14). Höhere Helligkeit in einem bestimmten Bildausschnitt erzeugt einen höheren Lichteinfall und somit auch ein entsprechend stärkeres elektrisches Signal. Nach Beisel et al. (2004) wird dieses Signal anschließend in mehreren Stufen auf einen Normwert verstärkt und es werden Signale zur horizontalen und vertikalen Austastung (zur Steuerung des Elektronenstrahls im Anzeigegerät) beigemischt. Dieses sogenannte BAS-Signal (Bild-Austast-Synchronsignal) kann dann am Kameraausgang abgegriffen, über analoge Übertragungswege (siehe Abschnitt 4.6) weitergeleitet und mit entsprechenden Geräten betrachtet und/oder aufgezeichnet werden.

Viele vorhandene Videoüberwachungssysteme sind noch vollständig analog oder nutzen zumindest teilweise analoge Kameras, sodass diese Technologie in der Videoüberwachung noch recht weit verbreitet ist. Wie bereits beschrieben, finden sich derzeit auch auf dem Markt weiterhin zahlreiche Analogkameras. Diese weisen momentan noch einige Vorteile unter schwierigen Bedingungen, wie unter Wasser oder bei starkem Gegenlicht, auf (Niecke, 2009a). Darüber hinaus sind qualitativ gleichwertige digitale Kameras in der Regel noch vergleichsweise größer und teurer. Die Nachteile rein analoger Systeme liegen in der niedrigeren Bildqualität sowie der zeit- und platzintensiven Aufzeichnung (siehe Abschnitt 4.7). Daneben wird eine komplett eigene Infrastruktur benötigt, was sich sowohl positiv als auch negativ auf die Erfüllung mancher Anforderungen auswirken kann, wie im weiteren Text noch erläutert wird (Ekerot, 2008).

Digital/IP

Im Gegensatz zum analogen kann das digitale Signal nur zwei unterschiedliche Zustände annehmen. Damit ist es zur Übertragung von Bits (binary digit, die kleinste Informationseinheit) geeignet (Brauner, Raible-Besten &Weigert, 1998, S. 44 und 97) und kann mittels Informationstechnik empfangen und weiterverarbeitet werden. Wie bei Kraheck et al. (2004) beschrieben, wird hierbei das vom Bildsensor

(siehe Abschnitt 4.3) kommende Signal direkt digitalisiert (d.h. in ein digitales Signal umgewandelt), und steht dann am Kameraausgang digital zur Verfügung. Durch einen direkt in der Kamera integrierten Server können die Bilddaten anschließend in einem auf dem Standardprotokoll TCP/IP basierenden Netzwerk (z.B. LAN, WLAN, Internet) genutzt werden, wobei dem Kameraserver eine eigene IP-Adresse zugeordnet wird (Beisel et al., 2004). Daher werden die Begriffe Digitaltechnologie und IP-Technologie bzw. Digitalkamera und Netzwerkkamera in der Videoüberwachung weitestgehend synonym als Abgrenzung zur Analogtechnologie gebraucht.

Prinzipiell können mittlerweile bis auf wenige Sonderfälle (siehe vorhergehenden Abschnitt über Analogtechnologie) alle Überwachungsaufgaben mit einem digitalen Videoüberwachungssystem durchgeführt werden (Fourmont, 2009). Drei der Hauptargumente für die Digitaltechnologie sind die deutlich höhere Auflösung, die erreicht werden kann, die Möglichkeit der Nutzung bereits vorhandener Netzwerke als Übertragungsweg, sowie die direkte Nutzbarkeit der Daten mittels Informationstechnik. Diese Faktoren müssen jedoch immer im Kontext gesehen werden, da sie sich je nach Anwendungsbereich sowohl positiv, als auch negativ auswirken können.

4.1.2 Kompatibilität der Technologien untereinander

Bei der Frage nach der Kompatibilität stößt man immer wieder auf die sinngemäße Aussage: Wenn Sie wirkliche Kompatibilität wollen, nutzen Sie Analogtechnologie. Denn die Komponenten analoger Videoüberwachungssysteme lassen sich nahezu problemlos beliebig kombinieren und zusammenschalten. Bei digitalen Systemen sieht es dagegen etwas anders aus: „Während die analogen Signale der früheren Kameragenerationen elektrisch weitgehend kompatibel waren, arbeiten die heutigen Kameras mit unterschiedlichen digitalen Kompressions- und Übertragungsverfahren [...]“ (Klitsch, 2010). Somit kann die Kompatibilität analoger Komponenten untereinander generell als vorhanden angesehen werden, bei digitalen Komponenten hingegen ist dies derzeit (noch) nicht der Fall (siehe hierzu auch die Abschnitte 4.5 und 4.8).

Aufgrund der unterschiedlichen Signale ist es grundsätzlich nicht möglich, analoge und digitale Komponenten zusammen zu verwenden. Jedoch existieren zwei Möglichkeiten, wie dies dennoch erreicht werden kann. Einerseits können wie von Niecke (2009b) beschrieben zur gemeinsamen Nutzung analoger und digitaler Kameras sogenannte hybride Rekorder (siehe Abschnitt 4.7) eingesetzt werden. Diese können sowohl analoge als auch digitale Signale verarbeiten, die Bilddaten darstellen und aufzeichnen.
Die zweite Möglichkeit ist der Video-Encoder. Nach Ekerot (2008) lassen sich damit die analogen Signale problemlos in digitale konvertieren und in ein TCP/IP-Netzwerk einspeisen. So können alle Arten von Analogkameras praktisch genau wie eine Netzwerkkamera eingesetzt werden. Zu beachten ist hierbei jedoch, wie auch bei den Digitalkameras, die Kompatibilität der digitalen Komponenten untereinander. Darüber hinaus ist zu betonen, dass zwar, wie fest gestellt wurde, analoge Kameras in einem digitalen System eingesetzt werden können. Der umgekehrte Weg ist jedoch nicht möglich.

Tabelle 4.1: Kompatibilität der Technologien untereinander.

	Analog	Digital
Analog	+	-
Digital	o	o

(+) Voll/uneingeschränkt kompatibel
(o) Teilweise/unter bestimmten Voraussetzungen kompatibel
(-) Nicht kompatibel
(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.1.3 Erfüllung der Anforderungen durch die Technologien

Die gewählte Technologie beeinflusst die Erfüllung der Anforderungen Analyse/Auswertung/Intelligenz, Integration/Zusammenarbeit mit anderen Systemen, Skalierbarkeit/-Erweiterbarkeit/Aufrüstbarkeit und Integrität/Überprüfbarkeit/Beweiskraft.

Hinsichtlich der Anforderung **Analyse/Auswertung/Intelligenz** zeigen sich große Unterschiede, wie bei Kraheck et al. (2004) dargestellt wird. Bei analogen Systemen ist maximal eine einfache Bewegungserkennung möglich. In einigen Fällen kann der bewegungssensible Bereich noch auf ein paar Felder des Bildausschnittes begrenzt werden. Darüber hinausgehende Funktionen stehen jedoch nicht zur Verfügung. Außerdem ist hierzu eine möglichst gleichmäßige und ausreichende Beleuchtung notwendig. Daher eignen sich analoge Systeme nur sehr begrenzt zur Erfüllung dieser Anforderung, beispielsweise zur Überwachung eines gut ausgeleuchteten Innenraums auf Betreten durch Personen. Hieraus folgt eine Bewertung mit einem Punkt.
Anders sieht es bei der Digitaltechnologie aus. Da das Bildmaterial digital vorliegt, kann es mittels Informationstechnik umfangreich ausgewertet werden. Die Möglichkeiten reichen hierbei von einer richtungsabhängigen Bewegungserkennung über das Erkennen und Verfolgen von Objekten (Personen, Gesichter, Fahrzeuge, ...) bis hin zu statistischen Auswertungsfunktionen, beispielsweise zu Besucherströmen. Folglich ist die Digitaltechnologie zur Erfüllung dieser Anforderung optimal geeignet und wird mit fünf Punkten bewertet.

Ähnlich sieht es bei der **Integration in andere Systeme** aus. Bei analogen Systemen ist es zwar möglich, einfache Gefahrenmelder (z.B. Zaunsensoren oder Türkontakte) über ein Alarmgerät und eine Videokreuzschiene zu integrieren (Beisel et al., 2004). Hier enden aber bereits die Möglichkeiten, sodass die mäßige Erfüllung der Anforderung mit zwei Punkten bewertet wird.
Die Digitaltechnologie bietet hier deutlich größeren Spielraum. Dank der Nutzbarkeit durch Informationstechnik und die Anbindung an Netzwerke können digital vorliegende Daten anderer Systeme mit genutzt oder die digitalen Bilddaten und Auswertungsergebnisse diesen zur Verfügung gestellt werden. Auch eine gegenseitige Ansteuerung kann demnach realisiert werden. Beachtet werden muss in diesem Fall aber die Kompatibilität der Schnittstellen und Daten, was nicht in allen Fällen ohne weitere Hilfsmittel oder Maßnahmen gegeben ist. Daher erfolgt die Vergabe von vier

Punkten.

Im Falle der **Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit** bietet ein Analogsystem nahezu alle Möglichkeiten. So können bei „einem analogen Videonetz [...] beliebig viele Kameras angekoppelt sein." (Kraheck et al., 2004, S. 25). Wie in Abschnitt 4.1.2 erläutert, stellt auch die Aufrüstung auf ein digitales System kein Problem dar. Die Anforderung ist damit optimal erfüllt und zieht eine Bewertung mit fünf Punkten nach sich.
Auch ein digitales System ist grundsätzlich beliebig skalier- und erweiterbar. Jedoch stellt sich hier wieder die Frage der Kompatibilität: „Je größer die Videoanlage jedoch wird, vor allem wenn auch Aufzeichnungssysteme und Systeme unterschiedlicher Hersteller ins Spiel kommen, desto problematischer wird das Zusammenspiel." (Klitsch, 2010). Daher kann im Falle der Digitaltechnologie diese Anforderung nur als unter bestimmten Bedingungen erfüllt angesehen werden und wird mit drei Punkten bewertet.

Die **Integrität/Überprüfbarkeit/Beweiskraft** des Bildmaterials ist in analogen Systemen generell gegeben. Dieser Umstand rechtfertigt eine Bewertung mit fünf Punkten.
Bei digitalen System kann davon im Allgemeinen nicht ausgegangen werden. Da durch die Möglichkeit der Nachbearbeitung Manipulationen nicht ausgeschlossen werden können, steht die Beweiskraft zunächst in Frage, wie von Beisel et al. (2004) dargelegt wird. Hier bedarf es zusätzlicher Maßnahmen, um die Integrität sicherstellen und belegen zu können. Da die Anforderung generell durchaus erfüllt werden kann, dazu aber explizit Handlungsbedarf besteht, erfolgt die Bewertung mit einem Punkt.

Tabelle 4.2: Erfüllung der Anforderungen durch die Technologien.

	Analog	Digital
Identifikation	x	x
Analyse	1	5
Integration	2	4
Sicht	x	x
Umgebung	x	x
Vandalismus	x	x
Verfügbarkeit	x	x
Skalierbarkeit	5	3
Integrität	5	1

Von 0: Erüllt die Anforderung garnicht
bis 5: Erüllt die Anforderung optimal
(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.2 Bildgebungsverfahren/Kamera-Typ

4.2.1 Übersicht und Beschreibung der Bildgebungsverfahren

Im Wesentlichen kommen drei Bildgebungsverfahren zum Einsatz: Schwarz/Weiß (S/W), Farbe und Infrarot(IR)/Wärmebild. Diese haben unterschiedliche Vor- und Nachteile, und eignen sich damit auch unterschiedlich gut zur Erfüllung der Anforderungen. Dies soll im weiteren Verlauf näher betrachtet werden. Es existieren zwar darüber hinaus auch Kombinationen, beispielsweise sogenannte Tag/Nacht-Kameras (Kombination von S/W oder Farbe mit IR) oder Duokameras (Kombination S/W und Farbe). Von der Bewertung her stellen sie jedoch einfach eine Kombination der Vorteile bzw. zu einem gewissen Grad einen Ausgleich der Nachteile der einzelnen Verfahren dar. Daher werden sie hier nicht als eigenständige Kategorie behandelt.

Schwarz/Weiß

Während dieses Bildgebungsverfahren im Bereich der Fotografie, Amateur-Videotechnik und Unterhaltungselektronik kaum noch anzutreffen ist, findet es in der Videoüberwachung auch heute des öfteren noch Anwendung. Der Hauptgrund hierfür liegt in der höheren Lichtempfindlichkeit von Schwarz/Weiß-Kameras. Diese ist im Vergleich zu Farbkameras um den Faktor zwei bis fünf höher (Beisel et al., 2004), d.h. mit ihnen lassen sich Überwachungsaufgaben auch bei teilweise deutlich schlechteren Lichtverhältnissen als mit Farbkameras durchführen. Dies liegt an der Technik der Bild-Sensoren (siehe Abschnitt 4.3). Diese können grundsätzlich nur Helligkeitswerte detektieren. Um auch Farbinformationen zu erhalten, müssen ihnen Farbfilter vorgeschaltet werden, welche die anschließend noch auf den Sensor treffende Lichtmenge verringern (Kräußlich, 2009). Darüber hinaus ist durch das Fehlen der Farbinformation folglich auch die notwendige Übertragungsbandbreite und der Speicherplatzbedarf geringer. Aus den genannten Gründen erlaubt auch die VdS 2366 (2004) in bestimmten Fällen den Einsatz von Schwarz/Weiß-Kameras: „Bieten Schwarz-Weiß-Kameras (z.B. Nachts) Vorteile das Schutzziel zu erreichen, dürfen diese eingesetzt werden.“ (S. 16).

Farbe

Mit Ausnahme der zuvor genannten Bereiche ist generell der Einsatz von Farbkameras anzuraten. Durch Beisel et al. (2004) wird dies einerseits durch die Farbinformation als zusätzliches, wichtiges Identifikationsmerkmal begründet, wodurch eine Situation durch einen menschlichen Beobachter auch schneller eingeschätzt werden kann. Andererseits bewirkt das Betrachten farbigen Bildmaterials geringere Ermüdungserscheinungen als Schwarz/Weiß-Bilder. Daher sieht die VdS 2366 (2004) nachvollziehbarerweise grundsätzlich den Einsatz von Farbkameras vor, in Bank- und Kreditinstituten sind diese durch die BGI 819-2 (2008) sowie in den Richtlinien der DGUV Test zur Zertifizierung nach der UVV Kassen (2010) sogar zwingend

vorgeschrieben.

Infrarot/Wärmebild

Im Gegensatz zu Schwarz/Weiß- und Farbkameras arbeiten Infrarot- oder Wärmebildkameras nicht im für das menschliche Auge sichtbaren Bereich des elektromagnetischen Spektrums, sondern machen sich, wie es der Name vermuten lässt, die Wärmeabstrahlung im infraroten Bereich zunutze. Nach Völckers & Liebelt (2008) werden hierbei kleinste Temperaturunterschiede in der Umgebung detektiert und in ein für den Menschen sichtbares Echtzeit-Videobild umgewandelt, das auf einem handelsüblichen Monitor dargestellt werden kann. Daher sind sie, anders als die beiden erstgenannten Kameratypen, in keinster Weise auf natürliches oder künstliches Licht angewiesen, funktionieren also auch bei völliger Dunkelheit oder Nebel. Daneben können, wie bei Maras (2007) erwähnt, teilweise auch zusätzliche Erkenntnisse aus dem Wärmebild gewonnen werden. Etwa, ob ein Fahrzeug vor kurzem noch bewegt wurde oder bereits längere Zeit steht, erkennbar am Temperaturunterschied zwischen Motor und Umgebung.

Zu beachten gibt es bei diesem Bildgebungsverfahren, dass zwei unterschiedliche Systeme erhältlich sind: Ungekühlte und gekühlte. Völckers und Liebelt (2008) stellen in ihrem Artikel einen Vergleich her: Gekühlte Kamerasysteme besitzen eine deutlich größere Empfindlichkeit, verursachen aber durch verschleißende bewegliche Teile und mit der Zeit entweichendem Gas kürzere Wartungsintervalle und höhere Betriebskosten. Während jedoch aufgrund ihrer höheren Leistungsfähigkeit die Kosten auch bei weiten Beobachtungsentfernungen annähernd gleich bleiben, weisen ungekühlte Systeme einen signifikanten Anstieg der Kosten auf. Dies liegt an der Notwendigkeit vergleichsweise sperriger und teurer Objektive mit einer ähnlichen Leistung wie diejenigen der gekühlten Systeme. So können sich ab einer Beobachtungsentfernung von etwa 5 km gekühlte Systeme als kostengünstiger erweisen.

4.2.2 Kompatibilität der Bildgebungsverfahren untereinander

Da die Art der Bilddatenerfassung für das daraus erzeugte Signal nicht relevant ist, zeigen die verschiedenen Kameratypen hinsichtlich der Kompatibilität keine Unterschiede. Alle drei Typen sowie deren Kombinationen lassen sich problemlos in jedem Videoüberwachungssystem einsetzen, sind frei austauschbar und lassen sich nebeneinander im selben System betreiben. Entscheidend ist hier lediglich die Frage nach Analog- oder Digitaltechnologie (siehe hierzu Abschnitt 4.1). Von daher können alle Bildgebungsverfahren als voll kompatibel betrachtet werden.

Tabelle 4.3: Kompatibilität der Bildgebungsverfahren untereinander.

	S/W	Farbe	IR
S/W	+	+	+
Farbe	+	+	+
IR	+	+	+

(+) Voll/uneingeschränkt kompatibel
(o) Teilweise/unter bestimmten Voraussetzungen kompatibel
(-) Nicht kompatibel
(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.2.3 Erfüllung der Anforderungen durch die Bildgebungsverfahren

Die drei Bildgebungsverfahren unterschieden sich bei der Erfüllung der Anforderungen Identifikation/Erkennbarkeit, schwierige Sichtverhältnisse sowie hohe Verfügbarkeit.

Bei der **Identifikation/Erkennbarkeit** zeigt das Schwarz/Weiß-Bild eine große Schwäche, da hier definitionsgemäß die für den menschlichen Seheindruck wichtige Farbinformation nicht mit erfasst wird. Diese kann aber, wie bei Kraheck et al. (2004) dargelegt, gerade bei Personenbeschreibungen von hoher Bedeutung sein.

Daher wird diese Anforderung hier nur mäßig erfüllt, was eine Bewertung mit drei Punkten nach sich zieht.
Noch schwieriger gestaltet sich dies bei der Wärmebildtechnik. Hier zeigen sich zwar minimale Temperatur-Unterschiede, diese sind jedoch zur Identifikation einer Person oder eines Objektes durch einen Menschen kaum brauchbar. Hingegen sind verwertbare Details wie Gesichtsmerkmale oder, ähnlich wie im Schwarz/Weiß-Bereich, die Farbinformationen gar nicht sichtbar. Gut erkennbar sind jedoch Vorgänge, wie Bewegungen von Fahrzeugen und Handlungen von Personen, meist sogar deutlicher als bei den anderen beiden Bildgebungsverfahren. Somit kann die Erfüllung dieser Anforderung mit zwei Punkten bewertet werden.
Eine optimale Erfüllung ist dagegen durch Farbkameras möglich. In der Kategorie der Bildgebungsverfahren liefert das Farbbild die besten Ergebnisse. Da das dargestellte Bild dem menschlichen Sehen entspricht und alle relevanten für das Auge verwertbaren Informationen enthält, besteht hier die höchste Wahrscheinlichkeit auf eine erfolgreiche Identifikation. Diese Tatsache begründet eine Bewertung mit fünf Punkten.

Ein anderes Bild zeigt sich beim Einsatz unter **schwierigen Sichtverhältnissen**. Hier bildet die Farbkamera das Schlusslicht, da sie im Vergleich zu den anderen beiden Typen relativ lichtschwach ist und keine nennenswerten Vorteile für den Einsatz unter schwierigen Sichtverhältnissen bietet. Ohne zusätzliche Maßnahmen kann daher nur eine Bewertung von einem Punkt erzielt werden.
Schwarz/Weiß-Kameras erzielen hier ein etwas besseres Ergebnis durch ihre höhere Lichtempfindlichkeit. Sie können somit unter schlechteren Lichtverhältnissen als Farbkameras noch wirksam eingesetzt werden. Jedoch versagen auch sie bei völliger Dunkelheit, Nebel und anderen Sichtbehinderungen. Daraus ergibt sich eine Bewertung von zwei Punkten.
Die Wärmebildkamera ist im Gegensatz dazu für den Einsatz unter schwierigen Sichtverhältnissen prädestiniert. Begründet ist dies durch den anderen Erfassungsbereich im elektromagnetischen Spektrum. Da der sichtbare Teil des Lichts für dieses

System nicht relevant ist, schränken weder völlige Dunkelheit, noch starkes Gegenlicht oder Wettereinflüsse wie Nebel oder Niederschlag die Sicht maßgeblich ein. Demnach erfolgt eine Bewertung mit fünf Punkten.

In der Kategorie der Bildgebungsverfahren hängt die **Verfügbarkeit** eines verwertbaren Videobildes direkt mit der Leistungsfähigkeit unter verschiedenen Sichtverhältnissen zusammen. Nur durch Sichterschwernisse kann hier die Qualität des empfangenen Bildmaterials eingeschränkt werden. Ist diese zu niedrig, so kann das Videoüberwachungssystem nicht mehr als verfügbar angesehen werden. Daher erfolgt hier, der Argumentation beim Einsatz unter schwierigen Sichtverhältnissen folgend, die selbe Einstufung: Ein Punkt bei Farbkameras, zwei Punkte bei Schwarz/Weiß-Kameras und fünf Punkte bei Wärmebildkameras.

Tabelle 4.4: Erfüllung der Anforderungen durch die Bildgebungsverfahren.

	S/W	Farbe	IR
Identifikation	3	5	2
Analyse	x	x	x
Integration	x	x	x
Sicht	2	1	5
Umgebung	x	x	x
Vandalismus	x	x	x
Verfügbarkeit	2	1	5
Skalierbarkeit	x	x	x
Integrität	x	x	x

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.3 Bild-Sensoren

4.3.1 Übersicht und Beschreibung der Bild-Sensoren

Zur Umwandlung des einfallenden Lichts aus dem Beobachtungsbereich in elektrische Signale werden bereits seit einigen Jahrzehnten mit großem Erfolg Bild-Sensoren eingesetzt. Auch in der Videoüberwachung hat sich diese Technik bewährt, wobei derzeit hauptsächlich zwei Sensor-Typen zum Einsatz kommen: CCD-Sensoren und CMOS-Sensoren (Kräußlich, 2009a). Daher werden diese beiden Typen im Folgenden vorgestellt.

CCD-Sensor

Ein CCD-Sensor (Charge Coupled Device) ist ein „ladungsgekoppelter Halbleiterbaustein, ein Bauteil aus miteinander verbundenen Mini-Dioden (ladungsgekoppelten Halbleitern), die analog zum Lichteinfall Spannung erzeugen.“ (Brauner, Raible-Besten & Weigert, 1998, S. 60). Wie von Kräußlich (2009a) erläutert, beruht die Technik auf dem inneren fotoelektrischen Effekt. Je mehr Licht einfällt, desto höher ist auch die erzeugte Spannung. Dabei sammeln die einzelnen Zellen des CCD-Sensors über einen bestimmten Zeitraum das einfallende Licht und werden anschließend ausgelesen. Durch die Proportionalität von Helligkeit und erzeugter Spannung kann, zunächst jedoch nur in Graustufen, ein Abbild des Beobachtungsbereichs erzeugt werden. Um auch Farbinformationen zu erhalten müssen, wie bereits im Unter-Abschnitt über das Schwarz/Weiß-Bildgebungsverfahren (4.2.1) beschrieben, dem Sensor Farbfilter vorgeschaltet werden.

In seinem Artikel stellt Kräußlich (2009a) die Stärken und Schwächen des CCD-Sensors im Vergleich zum CMOS-Sensor dar: Er liefert generell gute Bilder und ist lichtempfindlicher. Jedoch zeigt er Schwächen bei Beleuchtungsspitzen und starkem Gegenlicht, was sich in der Überstrahlung (sogenanntes Blooming) benachbarter Bildbereiche zeigt. Des weiteren sind oft mehrere Versorgungsspannungen notwendig,

und der Chip hat eine höhere Leistungsaufnahme. Er bewirkt also einen höheren Energieverbrauch. Mittlerweile sind jedoch auch Techniken entwickelt worden, mit denen das Ergebnis bei schwierigen Lichtverhältnissen verbessert werden kann, etwa durch den gleichzeitigen Einsatz von je zwei lichtempfindlichen Elementen pro Bildpunkt: Einem mit hoher, und einem mit niedriger Lichtempfindlichkeit.

CMOS-Sensor

Auch der CMOS-Sensor (Complementary Metal Oxide Semiconductor) nutzt nach Kräußlich (2009a) wie der CCD-Sensor den inneren fotoelektrischen Effekt, und wandelt einfallendes Licht proportional in elektrische Spannung um. Im Gegensatz zu letzt genanntem wird hier jedoch nicht über einen bestimmten Zeitraum angesammelt und anschließend ausgelesen, sondern es findet eine kontinuierliche Induktion eines elektrischen Stromes statt.

Auch der CMOS-Sensor bietet, wie Kräußlich (2009a) schreibt, einige Vor- und Nachteile: Er zeigt generell stärkeres Rauschen („farbliche oder geometrische Verzerrungen im Bild“, nach Brauner, Raible-Besten & Weigert (1998), S. 283) und öfter Fehlstellen. Auch ist er weniger lichtempfindlich als der CCD-Sensor. Dagegen stellen Beleuchtungsspitzen und starkes Gegenlicht kein Problem dar, eine Überstrahlung tritt praktisch nicht auf. Auch die Notwendigkeit oft nur einer Versorgungsspannung und die geringe Leistungsaufnahme wirken sich positiv aus. Zudem lässt sich beim CMOS-Sensor eine weitere Schaltung oder Logik zur Signalverarbeitung direkt in den Schaltkreis integrieren, mit der auf die einzelnen Fotozellen zugegriffen werden kann. Dadurch lassen sich Kameras mit geringeren Ausmaßen herstellen. Und nicht zuletzt ist der CMOS-Sensor kostengünstiger als der CCD-Sensor.

4.3.2 Kompatibilität der Bild-Sensoren untereinander

Da in Videoüberwachungskameras grundsätzlich nur ein Chip verbaut wird (Kräußlich, 2009a), ist die Frage der Kompatibilität innerhalb der Kamera hinfällig. Dies ist jedoch auch nicht Gegenstand der Betrachtung. Entscheidend ist die Kompatibilität des gesamt betrachteten Videoüberwachungssystems hinsichtlich seiner einzelnen Komponenten. Daher gleicht die Situation derjenigen bei den Bildgebungsverfahren (Abschnitt 4.2): Da die Art der Umwandlung von einfallendem Licht in elektrische Signale nicht entscheidend ist, sondern die Gestalt des Signals an sich (also Analog- oder Digitaltechnologie sowie evtl. Videodatenkompression etc.), sind die Kameras unabhängig vom Sensor-Typ als austauschbar und kompatibel anzusehen. Für den Einsatz innerhalb eines Videoüberwachungssystems spielt es keine Rolle, ob ein CCD-Sensor oder ein CMOS-Sensor verbaut wurde.

Tabelle 4.5: Kompatibilität der Bild-Sensoren untereinander.

	CCD	CMOS
CCD	+	+
CMOS	+	+

(+) Voll/uneingeschränkt kompatibel
(o) Teilweise/unter bestimmten Voraussetzungen kompatibel
(-) Nicht kompatibel
(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.3.3 Erfüllung der Anforderungen durch die Bild-Sensoren

Die Wahl des Sensors zeigt prinzipiell nur Auswirkungen auf die Anforderungen Einsatz unter schwierigen Sichtverhältnissen sowie geringe Auswirkungen bei der Identifikation/Erkennbarkeit. Wie bereits im Unter-Abschnitt über die Erfüllung von Anforderungen durch die Bildgebungsverfahren (4.2.3) dargestellt, hat die Leistungsfähigkeit beim Einsatz unter schwierigen Sichtverhältnissen im Allgemeinen

auch Auswirkungen auf die Anforderung der hohen Verfügbarkeit. Zwar sind solche Unterschiede zwischen den beiden Sensor-Typen zunächst einmal vorhanden, diese wirken sich aber im Zusammenspiel mit den anderen Komponenten eines Videoüberwachungssystem kaum merkbar aus, sodass diese hier als vernachlässigbar angesehen werden.

Hinsichtlich des **Einsatzes unter schwierigen Sichtverhältnissen** zeigen beide Sensor-Typen Vor- und Nachteile. Wie in der Beschreibung festgestellt, ist der CCD-Sensor grundsätzlich deutlich lichtempfindlicher, kann also auch unter schlechteren Lichtverhältnissen noch wirksam eingesetzt werden. Jedoch zeigt er aufgrund der Überstrahlungs-Effekte bei starkem Gegenlicht und Beleuchtungsspitzen Schwächen. Gegenüber diesen Effekten ist der CMOS-Sensor praktisch unempfindlich, besitzt aber eine geringere Lichtempfindlichkeit. Auf weitere Sichtbehinderung wie z.B. Nebel hat keiner der beiden Sensor-Typen eine Auswirkung. Sie sind durch ihre Nachteile nicht optimal zur Erfüllung dieser Anforderung geeignet, gleichen sich aber durch die verschiedene Vorteile gegenseitig aus. Dies führt bei beiden zu einer Bewertung mit drei Punkten.

Im Falle der **Identifikation/Erkennbarkeit** ist der CCD-Sensor grundsätzlich etwas im Vorteil. Zum einen liefert er generell ein gutes Bild. Zum anderen besitzt der CMOS-Sensor mit dem stärkeren Rauschen und häufigeren Fehlstellen Eigenschaften, die sich negativ auf die Bildqualität auswirken. In Folge dessen wird der CCD-Sensor mit fünf, der CMOS-Sensor mit vier Punkten bewertet.

Anzumerken ist in dieser Kategorie noch, dass die Beurteilung nur einen allgemeinen Anhaltspunkt darstellt. Durch bereits vorhandene und noch in der Entwicklung befindliche Techniken kann sich die Leistung der Bild-Sensoren durchaus verändern. Beispielsweise durch einen CCD-Sensor mit geringerer Empfindlichkeit gegenüber Überstrahlungs-Effekten. Dies sollte in jedem Einzelfall gesondert Beachtung finden.

Tabelle 4.6: Erfüllung der Anforderungen durch die Bild-Sensoren.

	CCD	CMOS
Identifikation	5	4
Analyse	x	x
Integration	x	x
Sicht	3	3
Umgebung	x	x
Vandalismus	x	x
Verfügbarkeit	x	x
Skalierbarkeit	x	x
Integrität	x	x

Von 0: Erüllt die Anforderung garnicht
bis 5: Erüllt die Anforderung optimal
(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.4 Auflösung

4.4.1 Übersicht und Beschreibung der Auflösungen

Es existiert eine Vielzahl an unterschiedlichen Videoauflösungen. In diesem Abschnitt werden die derzeit gängigsten Formate im Bereich der Videoüberwachung aufgelistet.

CIF-Auflösungen

CIF (Common Intermediate Formate) ist ein von der Internationalen Fernmeldeunion (International Telecommunication Union, ITU) definierter Auflösungsstandard, ursprünglich zur Verwendung in der Bildtelefonie vorgesehen (Brauner, Raible-Besten & Weigert, 1998, S. 66).

CIF sowie die Variante QCIF sind in der ITU-T Recommendation H.261 (1994) festgelegt. Auf diesen Formaten basierend existieren unter anderem folgende gängige Auflösungen (nicht abschließende Aufzählung):

- QCIF (Quarter CIF): 176 x 144 Pixel
- CIF: 352 x 288 Pixel
- 2CIF (2 x 1 CIF): 704 x 288 Pixel
- 4CIF (2 x 2 CIF): 704 x 576 Pixel
- 9CIF (3 x 3 CIF): 1 056 x 864 Pixel
- 16CIF (4 x 4 CIF): 1 408 x 1 152 Pixel

VGA-Auflösungen

Aus dem Computer- bzw. Computer nahen Bereich stammen die bei Poynton (2003) und Niehus (2008) genannten Auflösungsstandards VGA und darauf basierende. Durch den Einzug der Digitaltechnologie in der Videoüberwachung und somit der Nutzbarkeit der Daten mittels Informationstechnik finden auch diese Auflösungen Verwendung. Hier können unter anderem zum Einsatz kommen (nicht abschließende Aufzählung):

- VGA (Video Graphics Array): 640 x 480 Pixel
- SVGA (Super VGA): 800 x 600 Pixel
- XGA (Extended Graphics Array): 1 024 x 768 Pixel
- SXGA (Super XGA): 1 280 x 1 024 Pixel
- SXGA+ (SXGA Plus): 1 400 x 1 050 Pixel
- UXGA (Ultra XGA): 1 600 x 1 200 Pixel
- QXGA (Quad XGA): 2 048 x 1 536 Pixel

HDTV

Nach der Unterhaltungselektronik folgt auch die Videoüberwachung dem Trend zu HDTV, so schreibt Rech (2010) in seinem Artikel. HDTV (High Definition Television) ist ein Sammelbegriff für bestimmte Bildauflösungen und -wiederholungsraten. Die Benennung und Einordnung erfolgt hierbei anhand von drei Faktoren:

1. Anzahl der Bildzeilen (720 oder 1080)
2. Bildaufbauverfahren (Vollbilder, engl. *Progressive Scan*, abgekürzt 'p', oder Zeilensprungverfahren, engl. *Interlaced*, abgekürzt 'i')
3. Bildwiederholrate (24, 25, 30, 50 oder 60 Bilder pro Sekunde)

So bieten HDTV-fähige Digitalkameras beispielsweise 720p25/30 (eine Auflösung von 1 280 x 710 Pixel bei einer Bildwiederholrate von 25 oder 30 Bildern pro Sekunde im Vollbildverfahren) oder 1080i25/30 (eine Auflösung von 1 920 x 1 080 Pixel bei einer Bildwiederholrate von 25 oder 30 Bildern pro Sekunde im Zeilensprungverfahren).

Zu erwähnen sind hier noch die Standards der SMPTE (Society of Motion Picture and Television Engineers), die eine für die Videoüberwachung wichtige Bildwiederholrate von mindestens 25 oder 30 Bildern pro Sekunde garantieren. Hierbei steht der Standard SMPTE 296M für 720p, der Standard SMPTE 274M für 1080i oder 1080p.

Megapixel

Als Megapixel-Auflösungen werden alle Auflösungen bezeichnet, die mehr als ein Megapixel (also eine Million Bildpunkte) aufweisen. Dieser Begriff umfasst also beispielsweise Auflösungs-Standards wie SXGA (1 310 720 Bildpunkte), 16CIF (1 622 016 Bildpunkte) oder aus dem HDTV-Bereich 1080i25/30 (2 073 600 Bildpunkte). Es finden sich aber auch gerade unter dieser Bezeichnung zahlreiche weitere nicht stan-

dardisierte Auflösungen. Der Ausdruck wird hauptsächlich als Sammelbegriff für alle unterschiedlichen hochauflösenden Formate, die bei Digitalkameras möglich sind, verwendet, in Abgrenzung zu den vergleichsweise niedrigen Auflösungen in der Analogtechnologie.

Generell besteht in der Videoüberwachung keine derart große Ausrichtung auf und Nachfrage nach extrem hohen (Mega-)Pixelzahlen wie beispielsweise in der Digitalfotografie im Consumer-Bereich. Der Hauptgrund hierfür liegt in den sehr viel höheren Datenmengen, welche eine deutlich stärkere Belastung von Übertragungswegen und Speichermedien bedeuten. Daneben ist die Verwendung sehr hoher Auflösungen auch nur bedingt sinnvoll, wie im Unter-Abschnitt 4.4.3 erläutert wird. Formate wie SXGA+ oder andere mit vergleichbaren oder höheren Pixelzahlen werden hauptsächlich dort eingesetzt, wo räumlich große Bereiche in der Übersicht und im Bedarfsfall auch im Detail überwacht werden sollen, oder zur Verwendung auf großen Videoleinwänden und -bildschirmen, beispielsweise in Überwachungszentralen und Leitstellen.

4.4.2 Kompatibilität der Auflösungen untereinander

In dieser Kategorie bezieht sich die Frage nach der Kompatibilität auf das Zusammenspiel zwischen der Kamera einerseits und der Empfangsstelle (also Bildschirm, evtl. Videomanagementsoftware und Aufzeichnungssystem) andererseits. Da die Kameras an sich nicht direkt untereinander in Wechselwirkung treten, ist die Auflösung einer Kamera für alle anderen auch nicht von Belang. Folglich kommt es darauf an, ob die von der jeweiligen Kamera gebotene Auflösung in der Empfangsstelle auch unterstützt wird.

Die Anpassung an unterschiedliche empfangene Auflösungen funktioniert bei Röhrenmonitoren grundsätzlich etwas besser als bei Flachbildschirmen. Die hierfür relevanten Gründe werden von Schnitzler (2006) genannt: Die Röhrenmonitore sind dank der zugrunde liegenden Technik des Elektronenstrahls nicht an eine feste Auflösung gebunden und können sich daher auch ohne größeren Qualitätsverlust an

unterschiedliche Formate anpassen. Bei deutlich höheren als der empfohlenen Auflösung beginnt allerdings die Bildwiederholrate stark zu sinken, sodass es auch hier eine Obergrenze für noch verwertbare Auflösungen gibt.
Bei den Flachbildschirmen existiert hingegen durch das gegebene physikalische Bildpunktmuster eine sogenannte native Auflösung, auf welche die Geräte ausgelegt sind. Kleinere Auflösungen als diese können entweder eins zu eins nur auf Teilen der Bildfläche oder durch Streckung mit Qualitätseinbußen als Vollbild angezeigt werden. Höhere Auflösungen sind dagegen nicht möglich.

Daraus lässt sich schlussfolgern, dass Auflösungen untereinander zunächst einmal grundsätzlich kompatibel sind und aneinander angepasst werden können. So kann ein Monitor durchaus die Bilder verschiedener Kameras mit unterschiedlichen Auflösungen problemlos darstellen. Jedoch hängt dies stark vom Anzeigegerät und dessen Verhältnis zur Auflösung des gesendeten Bildmaterials ab. In der Systematik und Einstufung dieses Buchs müssen die verschiedenen Auflösungen daher untereinander generell als teilweise/unter bestimmten Voraussetzungen kompatibel (Tabellensymbol 'o') angesehen werden.

Auf die Darstellung in Tabellenform soll in dieser Kategorie verzichtet werden. Dies liegt einerseits in der beschriebenen starken Abhängigkeit der Kompatibilität von mehreren anderen Komponenten begründet, und andererseits in der Vielzahl an möglichen Auflösungen, sodass eine Auflistung hier nicht sinnvoll erscheint.

4.4.3 Erfüllung der Anforderungen durch die Auflösungen

Prinzipiell hat die Auflösung nur auf die Anforderung **Identifikation/Erkennbarkeit** direkte Auswirkungen. Hier lassen sich jedoch keine allgemein gültigen Eignungen formulieren. Wie in der Beschreibung der Anforderung (Abschnitt 3.2.1) dargestellt, hängt die Erfüllung von dem Verhältnis zwischen Anzahl der Bildpunkte und den räumlichen Ausmaßen des überwachten Bereichs ab. Diese Größe ist aber nur durch die Kameraleistung in Kombination mit den Montagebedingungen (Aufstellungsort,

Blickfeld, Umgebung) zu ermitteln.

So können Megapixel-Auflösungen zur Überwachung weitläufiger räumlicher Bereiche, wobei auch Details von Bedeutung sind, wie etwa auf größeren Parkplätzen, durchaus sinnvoll und angebracht sein. Dabei ist sowohl der Überblick über die Gesamtsituation gewährleistet, als auch die Erkennbarkeit von einzelnen Fahrzeugen, Kennzeichen und Personen, wenn notwendig. In vielen Fällen sind jedoch auch Kameras mit geringerer Auflösung vollkommen ausreichend. Beispielsweise wie von Wittmann (2009) angeführt bei einer Türüberwachung. Hier genügt auch eine Auflösung unterhalb des Megapixel-Bereichs, um einen möglichen Täter sicher zu identifizieren.

Aus den genannten Gründen ist eine Bewertung der Auflösungen zur Erfüllung der Anforderung, trotz ihrer Bedeutung hierfür, in losgelöster Form grundsätzlich nicht sinnvoll (Tabellensymbol 'x'). Auch in diesem Unter-Abschnitt wird, wie bei der Kompatibilität, aufgrund der Vielzahl an möglichen Auflösungen von einer Darstellung in Tabellenform abgesehen.

4.5 Videodatenkompression

4.5.1 Übersicht und Beschreibung der Videodatenkompressionen

Bei allen Vorteilen bringt die Digitaltechnologie in der Videoüberwachung aber auch eine nicht zu vernachlässigende Schwierigkeit mit sich: Die extrem hohe Menge an Daten, die gehandhabt werden muss. Ein einfaches Rechenbeispiel aus dem Artikel von Kräußlich (2009b) führt dies deutlich vor Augen: Bei farbigen Bildern schlagen die Farb- und Helligkeitsinformationen mit je 24 Bit (entspricht 3 Byte) pro Bildpunkt zu Buche. Bei einer VGA-Auflösung (siehe Abschnitt 4.4) mit 640 x 480 = 307 200 Bildpunkten sind dies 921 600 Byte pro Einzelbild. Dies ergibt bei einer Bildwiederholrate von 25 Bildern pro Sekunde, um eine flüssige Videoübertragung

zu erhalten, eine Datenlast von ca. 23 Megabyte pro Sekunde. Folglich wären für eine Stunde Aufzeichnung schon knapp 83 Gigabyte an Bildmaterial zu speichern, was bereits mehrere DVDs füllen würde. Bei höheren Auflösungen, z.B. im Megapixel-Bereich, und mehreren Kameras vervielfacht sich das Ganze noch entsprechend.

Um also die Belastung von Übertragungsweg und Speichersystem möglichst gering zu halten ist eine Komprimierung der gewonnenen Bilddaten notwendig. Es werden die folgenden gängigen Verfahren beleuchtet: M-JPEG, MPEG-2 / H.262, MPEG-4, H.264 sowie Beispiele für spezielle Videokompressionsverfahren in der Videoüberwachungstechnik.

M-JPEG

M-JPEG (Motion-JPEG) basiert, wie der Name bereits vermuten lässt, auf dem JPEG-Kompressionsverfahren für digitale Einzelbilder. Wie von Kräußlich (2009b) beschrieben, werden hierbei nicht alle einzelnen Bildpunkte getrennt betrachtet. Stattdessen werden solche, die neben einander liegen und ähnliche oder gleiche Farbwerte aufweisen in Blöcken zusammengefasst. Da die meisten Bilder solche gleichmäßigen Farbflächen enthalten, kann so beispielsweise bei mittlerer gewählter Kompressionsstärke die Datenmenge um den Faktor 30 reduziert werden.

Beim M-JPEG-Verfahren werden alle Einzelbilder separat mittels JPEG komprimiert und aneinandergereiht. Dabei weist das Bildmaterial, eine nicht allzu extreme Kompressionsstärke vorausgesetzt, noch eine relativ gute Qualität im Verhältnis zum unkomprimierten Bild auf.

MPEG-2 / H.262

MPEG ist sowohl die Abkürzung für die *Motion Pictures Experts Group*, einem ISO-Gremium für Audio- und Videonormen, als auch Bezeichnung für die von diesem entwickelten Kompressionsverfahren (Brauner, Raible-Besten & Weigert, 1998, S. 231).

Wie Kräußlich (2009b) schreibt, basiert der 1994 entwickelte Standard MPEG-2 auf folgender Methode: Im Gegensatz zu M-JPEG wird hier nicht jedes Einzelbild komplett übertragen oder gespeichert, sondern nur die sich im Vergleich zum vorhergehenden Bild geänderten Teile. Somit wird umso weniger Bandbreite und/oder Speicherplatz benötigt, je weniger Bewegung im überwachten Bereich stattfindet. Daher sind eher unruhige Hintergründe, wie vom Wind bewegte Pflanzen oder passierende Fahrzeuge ungünstig für dieses Kompressionsverfahren.

Der von der ITU (siehe 4.4.1) entwickelte Standard H.262 ist nach Strutz (2005) mit MPEG-2 identisch.

MPEG-4

MPEG-4, so Kräußlich (2009b), ist der direkte Nachfolger von MPEG-2, da MPEG-3 aufgegeben wurde. Ziel waren qualitativ gute Ergebnisse bei, im Hinblick auf die Bandbreite des zu dieser Zeit üblichen ISDN, Datenraten unter 64 kBit pro Sekunde. Bei MPEG-4 „[. . .] wird das Bild in statische und bewegte Elemente sowie räumliche Ebenen aufgelöst. Die Objekte werden auf getrennten Kanälen digital verarbeitet und zeitgleich komprimiert“ (Kräußlich, 2009b, S. 24). Es ergibt sich eine deutlich höheren Kompressionsrate als bei MPEG-2.

Jedoch ist MPEG-4 nach Strutz (2005) weit mehr als nur ein Kompressionsverfahren. Alle Möglichkeiten der Digitaltechnologie werden ausgeschöpft, wobei im Gegensatz zu den statischen Bilddaten in MPEG-2 hier alle enthaltenen Informationen dynamisch gestaltet werden können, beispielsweise die Kombination und Mitcodierung des Videomaterials zusammen mit Text oder grafischen Elementen.

Wie bei Kräußlich (2009b) erwähnt, existieren jedoch verschiedene sogenannte Profile für MPEG-4 in Abhängigkeit vom Codec (Encoder/Decoder, ein Software-Element zur Kompression und Dekompression der Daten). Diese können unterschiedliche Kompressionsstärken und Qualitätsstufen bieten.

H.264

Das bei Strutz (2005) beschriebene Kompressionssystem H.264 ist eine dem MPEG-4-Standard entstammende Gemeinschaftsentwicklung der MPEG-Gruppe und der ITU. Es liefert eine deutlich gesteigerte Kompressionsrate im Vergleich zu MPEG-4 bei etwa gleich bleibender Qualität. Im Vergleich zu MPEG-2 verringert sich die resultierende Datenmenge um den Faktor drei, wie Kräußlich (2008a) schreibt. Die Verbesserungen resultieren hierbei nicht aus einer einzigen Innovation, sondern aus vielen kleineren Änderungen. Jedoch ergibt sich laut Kräußlich (2009b) auch eine merkbar höhere Anforderung an die Rechenleistung beim Codieren des Signals. Auch von H.264 existieren wie bei MPEG-4 mehrere verschiedene Variationen.

Wie von Korkin (2009) prognostiziert, wird H.264 aufgrund seiner Vorteile und seiner Leistungsfähigkeit im Bereich der Videoüberwachung eine vorherrschende Stellung einnehmen, was bereits jetzt anhand der häufigen Verwendung in aktuellen Produkten absehbar ist. Auch ONVIF (Open Network Video Interface Forum, siehe Abschnitt 4.8) setzt auf diesen Standard.

Spezielle Verfahren

In seinem Artikel spricht Kräußlich (2009b) einen grundlegenden Nachteil aller MPEG-Verfahren (also die hier behandelten MPEG-2 / H.262, MPEG-4 und H.264) an: Da sie nicht speziell für die Videoüberwachung, sondern für Film und Fernsehen generell entwickelt wurden, zeigen sie starke Qualitätseinbußen bei bewegten Bildern. Während es im Allgemeinen nicht relevant ist, Einzelheiten von bewegten Objekten zu erkennen, ist dies in der Videoüberwachung hingegen von hoher Bedeutung.

Einige Hersteller von Videoüberwachungsprodukten haben daher eigene spezielle Kompressionsverfahren entwickelt, die an die besonderen Bedürfnisse in diesem Bereich angepasst sind. Kräußlich (2009b) nennt hierfür zwei Beispiele: MxPEG von

Mobotix, welches auf M-JPEG basiert, und MPEG4CCTV von Geutebrück, das auf MPEG-4 basiert. In beiden Fällen erzielen auch bewegte Bilder eine ähnlich hohe Qualität wie M-JPEG, weisen aber eine um den Faktor drei bis fünf höhere Kompressionsrate auf.

4.5.2 Kompatibilität der Videodatenkompressionen untereinander

Die Videokompressionsverfahren sind generell nicht gegenseitig kompatibel, da sie auf völlig unterschiedlichen Techniken und Methoden basieren. M-JPEG und MPEG-2 / H.262 sind zu sich selbst voll kompatibel, was bei MPEG-4 und H.264 nicht automatisch der Fall ist, da von den beiden, wie zuvor beschrieben, verschiedene Variationen existieren. Hier müssen der Encoder in der Kamera und der Decoder in der Empfangsstelle das selbe Profil benutzen. Diese beiden Verfahren sind also zu sich selbst eingeschränkt kompatibel. Auch die speziellen Verfahren wie MxPEG oder MPEG4CCTV sind zwar zu sich selbst kompatibel, untereinander jedoch nicht. Daher wird diese Gruppe als Gesamtheit zu sich selbst als teilweise kompatibel bewertet.

Tabelle 4.7: Kompatibilität der Videodatenkompressionen untereinander.

	M-JPEG	MPEG-2 / H.262	MPEG-4	H.264	Speziell
M-JPEG	+	-	-	-	-
MPEG-2 / H.262	-	+	-	-	-
MPEG-4	-	-	o	-	-
H.264	-	-	-	o	-
Speziell	-	-	-	-	o

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.5.3 Erfüllung der Anforderungen durch die Videodatenkompressionen

Die Kompressionsverfahren wirken sich auf die Anforderungen Identifikation/Erkennbarkeit und Integrität/Überprüfbarkeit/Beweiskraft aus. Ein wichtiges Auswahlkriterium in dieser Kategorie ist sicherlich auch die Kompressionsrate, um eine möglichst geringe Auslastung des Übertragungssystems und des Speichermediums zu erreichen. Dies ist jedoch, wie Anfangs erwähnt, nicht Gegenstand dieses Buchs und muss daher bei Bedarf separat in die Bewertung miteinbezogen werden.

Bei der **Identifikation/Erkennbarkeit** zeigen sich Unterschiede bei bewegten Objekten: Während die nicht auf die Videoüberwachung ausgerichteten Verfahren MPEG-2 / H.262, MPEG-4 und H.264 hier deutliche Schwächen zeigen, liefern das von Haus aus qualitativ hochwertige M-JPEG und die speziell aus diesem Grund entwickelten Kompressionsverfahren (z.B. MxPEG oder MPEG4CCTV) auch in solchen Fällen gut verwertbares Bildmaterial. Daher werden die drei erst genannten Verfahren jeweils mit drei Punkten, die anderen beiden mit je fünf Punkten bewertet.

Die Verfahren M-JPEG und MPEG-4 weisen keine Merkmale auf, die zur Erhöhung der **Integrität/Überprüfbarkeit/Beweiskraft** beitragen. Die damit übertragenen Bilddaten können im Nachhinein problemlos verändert werden. Da auch H.264 und die speziellen Kompressionssysteme auf einem dieser beiden Verfahren aufbauen, verhält es sich mit ihnen genauso. Ohne weiterführende Maßnahmen kann diese Anforderung durch sie nicht erfüllt werden, sodass eine Bewertung aller genannten Verfahren mit null Punkten erfolgt. Lediglich MPEG-2 erzeugt Strutz (2005) zufolge statische Daten, sodass eine Texteinblendung wie z.B. eine Datums- und Zeitangabe nicht entfernbar ist. Diese Tatsache schützt zwar nicht vor Manipulation des Bildmaterials an sich, kann jedoch zumindest die zeitliche Integrität garantieren. Daher wird die Erfüllung dieser Anforderung durch MPEG-2 bzw. H.262 mit drei Punkten bewertet.

Tabelle 4.8: Erfüllung der Anforderungen durch die Videodatenkompressionen.

	M-JPEG	MPEG-2 / H.262	MPEG-4	H.264	Speziell
Identifikation	5	3	3	3	5
Analyse	x	x	x	x	x
Integration	x	x	x	x	x
Sicht	x	x	x	x	x
Umgebung	x	x	x	x	x
Vandalismus	x	x	x	x	x
Verfügbarkeit	x	x	x	x	x
Skalierbarkeit	x	x	x	x	x
Integrität	0	3	0	0	0

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.6 Übertragung

4.6.1 Übersicht und Beschreibung der Übertragungsarten

Im Anschluss an die Videodatenkompression muss das Signal zur Empfangsstelle, also einem Monitor- und/oder Aufzeichnungssystem übertragen werden. Im analogen Bereich können klassischerweise die Zwei-Draht-Übertragung, das Koaxialkabel, oder eine Funkverbindung genutzt werden. In der Digitaltechnologie werden dagegen primär Netzwerke (LAN, Internet) oder Drahtlos-Netzwerke (WLAN) eingesetzt. Aber auch eine Lichtwellenleiter- oder Infrarot-Verbindung ist in beiden Fällen möglich. Diese unterschiedlichen Arten sollen mit ihren jeweils spezifischen Vor- und Nachteilen in diesem Abschnitt genauer betrachtet werden.

Zwei-Draht-Verbindung

Eine der einfachsten Möglichkeiten der Übertragung von Videosignalen stellt die Zwei-Draht-Verbindung dar. Nach Kraheck et al. (2004) besteht diese aus einem verdrillten Paar eines handelsüblichen Fernmeldekupferkabels. Da diese Übertra-

gungsart anfällig für Störungen ist, sollten einige Maßnahmen getroffen werden, etwa eine gute Abschirmung des Kabels sowie die Nutzung möglichst weniger Aderpaare und die Übertragung nur weniger Signale innerhalb eins Kabels. Es können allerdings laut Niecke (2009a) hohe Reichweiten von bis zu zwei Kilometern erzielt werden.

Koaxialkabel

Eine der am häufigsten anzutreffenden Übertragungsarten im Bereich der analogen Videoüberwachung ist das von Kraheck et al. (2004) genannte Koaxialkabel. Bei diesem Kabeltyp müssen an beiden Leitungsenden jeweils Abschluss-Widerstände von 75 Ohm vorhanden sein, um eine störungsfreie Übertragung zu erhalten. Diese Widerstände sind in den verschiedenen Komponenten einer Videoüberwachungsanlage entweder bereits fest integriert oder können geschaltet werden. Vorteilhaft ist laut Niecke (2009a) die bei diesem Kabel verwendete BNC-Steckverbindung, welche bei der Großzahl der Geräten vorhanden ist. ein Nachteil hingegen ist die relativ geringe Reichweite von nur etwa 150 Metern. Wie von Kraheck et al. (2004) beschrieben, kann diese durch das Zwischenschalten von Entzerrverstärkern noch in begrenztem Rahmen erhöht werden. Zu beachten ist jedoch, dass dann nur noch Signale in eine Richtung übertragen werden können, also beispielsweise das Senden von Steuerbefehlen an eine Kamera nicht mehr möglich ist.

Lichtwellenleiter

Eine weitere kabelgebundene Möglichkeit der Übertragung stellt der Lichtwellenleiter (Abkürzung: LWL), auch Glasfaser (Niecke, 2009b, S. 50) genannt, dar. Nach Kraheck et al. (2004) wird hierbei das elektrische Videosignal in optische Impulse umgewandelt und übertragen. Diese Übertragungsart bietet viele Vorteile, z.B. große Reichweite (mehrere Kilometer), Unempfindlichkeit gegenüber elektromagnetischen Störeinflüssen und die Möglichkeit, praktisch beliebig viele Signale über ein Kabel

zu übertragen. Nachteilig wirken sich jedoch die bisher noch vergleichsweise hohen Kosten für Anschaffung und Installation aus.

Funk

Auch kabellos über Funk können die Videosignale übertragen werden. Ähnlich wie beim Lichtwellenleiter sind hier, wie Niecke (2009a) schreibt, teilweise hohe Reichweiten möglich. Daneben entfallen die Kosten und der Aufwand einer Kabelverlegung. Zu berücksichtigen ist aber die höhere Störanfälligkeit und eingeschränkte Anzahl an möglichen Kameras. Zudem weisen Kraheck et al. (2004) auf den Sicherheitsaspekt hin: Da es keine räumlich begrenzte und abgeschirmte Übertragungsstrecke gibt, ist ein relativ einfacher Zugriff von außen auf die gesendeten Daten möglich.

Optischer Richtfunk

Neben der Funkverbindung steht der optische Richtfunk in Form der Infrarot- (Abkürzung: IR) oder Laser-Verbindung als kabellose Alternative zur Verfügung. Anders als beim Funk werden hier die Daten, wie von Kraheck et al. (2004) dargestellt, in einem einzigen zielgerichteten optischen Lichtstrahl versendet. Der Übertragungsweg ist also ähnlich wie der eines Kabels räumlich begrenzt, allerdings wie auch beim Funk nicht räumlich abgetrennt. In jedem Fall ist bei der Laser-/IR-Verbindung eine direkte Sichtverbindung zwischen Sender und Empfänger notwendig.

LAN

Niecke (2009a) und Fourmont (2009) stellen in ihren Artikeln die drei großen Vorteile der Übertragung über ein lokales Netzwerk (LAN) dar:

1. Die Nutzung als einheitliche gemeinsame Infrastruktur für Videoüberwachung, IT, Gebäudetechnik und weitere Systeme bei einer Neuinstallation.

2. Bei der Aufrüstung, Erweiterung oder Umstellung des Videoüberwachungssystem die Mitbenutzung bereits vorhandener Netzwerke, was Installationsaufwand und -kosten drastisch verringern kann.

3. Durch den Anschluss des Netzwerkes an das Internet weltweiter Zugriff auf die Videodaten. Eine räumliche Nähe der Empfangsstelle zur Kamera ist nicht mehr erforderlich.

Allerdings gilt es bei einer Mehrfachnutzung des Netzwerkes die maximal mögliche Auslastung und benötigte Bandbreite zu beachten. Laut Fourmont (2009) ist dies in modernen Netzen jedoch kein großes Problem mehr. So lassen sich in der Praxis etwa 30 Kameras über ein Netzwerk betreiben, bei Vorhandensein einer Gigabit-Ethernet-Anbindung folglich sogar die zehnfache Anzahl.

WLAN

Ein Drahtlos-Netzwerk (WLAN) stellt die kabellose Alternative für Digitalkameras dar. Prinzipiell weist es die selben Vor- und Nachteile wie die Funkübertragung aus dem analogen Bereich kombiniert mit der Funktionalität eines Netzwerkes auf. Nach Stiewe (2010) eignet sich diese Übertragungsart vor allem für Outdoor- und mobile Anwendungen, sowie für schwer zugängliche Gebiete.

4.6.2 Kompatibilität der Übertragungsarten untereinander

Zwei-Draht-Verbindungen lassen sich, von den Reichweiten-Beschränkungen abgesehen, beliebig miteinander verbinden, sind also uneingeschränkt kompatibel. Dies trifft ebenso auf das Koaxialkabel zu. Auch untereinander können die beiden, allerdings nur mit Hilfe von Adaptern, zusammengeschlossen werden.
Bei der Funkübertragung gibt es, wie bei Kraheck et al. (2004) erwähnt, verschiedene Frequenzbereiche. Sender und Empfänger sind also nur kompatibel, sofern sie die selben Frequenzen unterstützen. Erhältlich sind auch Konverter zum Anschluss an

analoge Kabelübertragungswege, was damit die Kompatibilität zu Zwei-Draht-Verbindungen und Koaxialkabeln unter bestimmten Voraussetzungen ermöglicht.
Alle kabelgebundenen und kabellosen IP-basierten Netzwerke sind zu sich selbst jeweils praktisch uneingeschränkt kompatibel. So können beispielsweise Netzwerkkameras hinsichtlich des Netzwerkes (nicht aber des Signales) herstellerunabhängig kombiniert und hinzugefügt werden. Auch lassen sie sich mit entsprechenden handelsüblichen Komponenten wie z.B. Router / WLAN-Router oder Switch untereinander zusammenschließen und kombinieren.
Beim optischen Richtfunk wird das Signal laut Kraheck et al. (2004) üblicherweise digitalisiert, sodass Sender und Empfänger nicht wahllos kombiniert werden können, sondern ein gleichartiges Signal nutzen müssen, womit sie nur teilweise kompatibel sind. Mit entsprechenden Sendern und Empfängern können alle anderen Übertragungsarten mit dem optischen Richtfunk kombiniert werden. Üblicherweise sind dies digitale Netzwerk-Signale (Graf-Jahnke, 2004), durch Digitalisierung im Sender und Rückwandlung im Empfänger sind aber auch analoge Signale möglich (BHE CCTV 1.1, 2007).
Grundsätzlich lassen sich alle analogen Übertragungswege (Zwei-Draht, Koaxialkabel, Funk), wie bereits im Unter-Abschnitt zur Kompatibilität von Analog- und Digitaltechnologie (4.1.2) erörtert, mittels Video-Encoder an ein Netzwerk anschließen. Sie sind also zu LAN / WLAN unter bestimmten Voraussetzungen kompatibel. Wie bei Bemmel (2010) dargestellt, können umgekehrt auch Netzwerk-Signale aus LAN oder WLAN mittels spezieller IP-Router streckenweise über Koaxialkabel oder Zweidrahtverbindungen übertragen werden.
Lichtwellenleiter-Verbindungen können, wie Kraheck et al. (2004) schreiben, auch mit bereits bestehenden verbunden werden. Sie sind also zu sich selbst uneingeschränkt kompatibel. Nach Schnabel (1997 - 2010) können mit Hilfe entsprechender Komponenten sowohl digitale als auch analoge Signale per LWL-Technik übertragen werden. Lichtwellenleiter sind somit also zu allen anderen Übertragungsarten unter Voraussetzung des Vorhandenseins der notwendigen technischen Ausstattung kompatibel.

Tabelle 4.9: Kompatibilität der Übertragungsarten untereinander.

	Zweidraht	Koax	Funk	IR/Laser	LWL	LAN	WLAN
Zweidraht	+	o	o	o	o	o	o
Koax	o	+	o	o	o	o	o
Funk	o	o	o	o	o	o	o
IR/Laser	o	o	o	o	o	o	o
LWL	o	o	o	o	+	o	o
LAN	o	o	o	o	o	+	o
WLAN	o	o	o	o	o	o	+

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.6.3 Erfüllung der Anforderungen durch die Übertragungsarten

Die verschiedenen Übertragungsarten zeigen Unterschiede in der Erfüllung der Anforderungen Integration/Zusammenspiel mit anderen Systemen, widrige Umgebungsbedingungen, Schutz vor Vandalismus/Sabotage, hohe Verfügbarkeit, Skalierbarkeit/ Erweiterbarkeit/Aufrüstbarkeit und Integrität/Überprüfbarkeit/Beweiskraft. Bei der Betrachtung der Übertragungsarten sind sicherlich auch weitere Kriterien interessant, so etwa Installationsaufwand und -kosten, die mögliche Bandbreite und Übertragungsreichweite. Diese stehen jedoch, wie anfangs erwähnt, nicht im Fokus dieses Buchs. Allerdings spielen sie teilweise auch eine Rolle bei der Erfüllung der formulierten Anforderungen und werden entsprechend berücksichtigt. Darüber hinaus spielen gerade im Bereich der Übertragung viele individuelle Faktoren der Installation vor Ort eine Rolle. Daher können die hier ermittelten Punktwerte nur als erster Richtwert gelten und müssen jeweils noch mittels einer eigenen Beurteilung angepasst werden.

Um eine gute **Integration/Zusammenspiel mit anderen Systemen** zu gewährleisten, muss die Übertragungsart von möglichst vielen anderen Systemen genutzt oder unterstützt werden. Wie schon im Unterabschnitt über die Erfüllung der An-

forderungen durch die Technologien (4.1.3) erörtert, ist dies bei der digitalen Übertragung per LAN oder WLAN am besten möglich, sodass diese beiden Übertragungsarten hier mit fünf Punkten bewertet werden.
Weniger weit verbreitet und etwas komplizierter zu handhaben sind die Systeme Lichtwellenleiter und optischer Richtfunk. Durch ihre relativ gutes Zusammenspiel mit Netzwerken und die Nutzung digitaler Signale ist jedoch noch eine Bewertung mit vier Punkten angemessen.
Die analogen Übertragungswege Zweidraht-Verbindung, Koaxialkabel und Funk sind am wenigstens gut zur Integration geeignet, können jedoch mit Hilfe spezieller Konverter/Adapter in den meisten Fällen auch mit anderen Systemen zusammenarbeiten. Entsprechend erfolgt die Bewertung dieser drei Systeme mit jeweils drei Punkten.

Widrige Umgebungsbedingungen, in diesem Fall die Wetterverhältnisse, beeinflussen vor allem die kabellosen Übertragungsarten, also Funk, optischen Richtfunk und WLAN. Die kabelgebundenen Übertragungsarten werden hiervon gar nicht oder nur kaum beeinflusst, insbesondere Verlegung unter der Erde, innerhalb Wänden oder ähnliches. Diese sind folglich für den Einsatz unter widrigen Umgebungsbedingungen voll tauglich und werden mit fünf Punkten bewertet.
Wie von Gilke (2008) dargestellt, können die auf nicht-optischen elektromagnetischen Wellen basierenden Systeme Funk und WLAN durch Wettereinflüsse gestört werden. Relevante Auswirkungen sind jedoch nur in stärkeren Wetterlagen zu erwarten. Auch sind mittlerweile für den Außeneinsatz geeignete Funksender und Wetterschutzgehäuse erhältlich, sodass Funk und WLAN diese Anforderung mit vier Punkten erfüllen können.
Beim optischen Richtfunk hingegen zeigen sich größere Schwierigkeiten. Der räumlich eng fokussierte optische Strahl kann durch jegliche Hindernisse innerhalb der Übertragungsstrecke gestört oder komplett abgeschirmt werden. Dies kann beispielsweise bei Niederschlag, durch Wind bewegte Gegenstände oder auch wie von Kraheck et al. (2004) erwähnt bei Nebel der Fall sein. Aber auch Rauche, Gase, Stäube oder Luft-

turbulenzen durch Temperaturschwankungen und ähnliches beeinflussen die Übertragung negativ, so Graf-Jahnke (2004). Diese Übertragungsart ist also deutlich anfälliger gegenüber Wettereinflüssen und somit schlechter zum Einsatz unter widrigen Umgebungsbedingungen geeignet, was eine Bewertung mit zwei Punkten nach sich zieht.

Der **Schutz vor Vandalismus/Sabotage** meint in Bezug auf die Übertragungsart den Schutz vor einem Trennen der Verbindung zwischen Kamera und Empfangsstelle. Auch hier bestehen Unterschiede zwischen den kabelgebundenen und den kabellosen Übertragungsarten. Bei ersteren hängt dies stark von der Art der Verlegung ab. Während beispielsweise ein offenes, frei zugängliches Kabelstück zwischen Kamera und Wand bereits mit einfachsten Werkzeugen oder auch nur körperlicher Gewalt zu durchtrennen ist, gestaltet sich das Unterfangen bei innerhalb von robusten Kameramasten oder Wänden verlegten Kabeln deutlich schwieriger. Eine generell gültige Aussage über die Sicherheit vor Vandalismus oder Sabotage der kabelgebundenen Übertragungsarten ohne Betrachtung der Installation vor Ort ist daher als nicht sinnvoll zu erachten.
Anders sieht es bei den drei kabellosen Verfahren aus. Hier kommt es nicht allzu sehr auf die genaue Positionierung der Komponenten an, als vielmehr auf die Sende-Eigenschaften. Bei Funk und WLAN breiten sich die Signale über einen größeren räumlichen Bereich aus. Eine gezielte Störung oder Unterbrechung des kompletten Signals ist somit nur sehr bedingt möglich. Beim optischen Richtfunk hingegen kann der optische Strahl mit jedem beliebigen Gegenstand, etwa wie von Kraheck et al. (2004) erwähnt einem gasgefüllten Ballon, oder auch einem Stück Klebeband vollständig abgeschnitten werden. Hier spielt wieder die räumliche Platzierung und Art der Installation eine größere Rolle. Die Bewertung dieser Anforderung erfolgt dementsprechend bei Funk und WLAN mit vier, bei optischem Richtfunk mit zwei Punkten.

Die **hohe Verfügbarkeit** des Videosignals hinsichtlich des Übertragungsweges hängt im Prinzip von der Verfügbarkeit unter widrigen Umgebungsbedingungen sowie

dem Schutz vor Vandalismus/Sabotage ab, sodass die zu diesen Anforderungen ermittelten Bewertungen als Basis dienen können. Die kabelgebundenen Übertragungsarten weisen sehr gute Leistungen unter widrigen Umgebungsbedingungen auf, beim Schutz vor Vandalismus/Sabotage kommt es jedoch ganz auf die Installation vor Ort an. Insgesamt können sie im Allgemeinen eine recht hohe Verfügbarkeit garantieren, insbesondere im Vergleich zu den kabellosen Verfahren, sodass sie mit vier Punkten bewertet werden.
Davon abweichend schneidet das LAN etwas schlechter ab, da es hier (vor allem bei der Nutzung durch mehrere Systeme, z.B. Videoüberwachung und IT) öfters zu kurzzeitigen Unterbrechungen kommen kann: „Die Installation einer Netzwerk basierten Videoüberwachung offenbart häufig Schwächen des Netzes, die vorher unbemerkt blieben oder einfach stillschweigend toleriert wurden.“ (Fourmont, 2009, S. 28). Folglich fällt hier die Bewertung mit drei Punkten etwas niedriger aus.
Bei den kabellosen Übertragungsarten gilt es neben den bereits genannten Faktoren noch verschiedene weitere negative Einflüsse zu berücksichtigen, z.B. bei Funk und WLAN Störungen durch metallische Gebäudeteile und Objekte, oder Vogel-/Insektenflug bei IR/Laser. Gesamt betrachtet erfolgt daher eine Bewertung mit jeweils zwei Punkten.

Bei der **Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit** ist der deutlich geringere Installationsaufwand und ein leichter Umbau ein genereller Vorteil der kabellosen Übertragungsverfahren. Überlegungen zur örtlichen Positionierung bei der Umsetzung oder dem Hinzukommen von Kameras spielen sind deutlich nachrangiger. Hindernisse für kabelgebundene Verfahren, wie Gewässer oder Straßen, spielen kaum eine Rolle.
Die beste Leistung zeigt hier der optische Richtfunk. Durch den räumlich stark begrenzten Sendebereich können praktisch beliebig viele IR-/Laser-Verbindungen auch in direkter Nachbarschaft aufgebaut werden. Positiv sind auch die Reichweiten von bis zu fünf Kilometern und die hohe Bandbreite, so Graf-Jahnke (2004). Daraus folgt eine Bewertung mit 4 Punkten.

Beim WLAN sind nicht ganz so hohe Bandbreiten und Reichweiten möglich. Jedoch ist grundsätzlich durch die Vergabe individueller IP-Adressen eine hohe Anzahl an Kameras und anderen Komponenten möglich. Es ergibt sich eine Bewertung mit drei Punkten.
Bei der Funkübertragung sind, wie Kraheck et al. (2004) schreiben, die möglichen nutzbaren Frequenzen begrenzt, womit ein funkbasiertes Videoüberwachungssystem recht schnell eine quantitative Grenze erreicht. Dies zieht eine Bewertung mit zwei Punkten nach sich.
Wie bereits dargelegt wurde, weisen die kabelgebundenen Übertragungsarten den Nachteil einer aufwändigen und somit meist auch kostspieligen Verlegung auf. Allerdings sind auch verschiedene positive Eigenschaften vorhanden. So weist etwa der Lichtwellenleiter nach Schnabel (1997 - 2010) sehr hohe Übertragungsraten und die Möglichkeit sehr vieler Parallelübertragungen auf. Daneben ermöglicht er größere Reichweiten als alle anderen Übertragungsarten und ist zu sich selbst uneingeschräkt kompatibel. Dementsprechend können mit LWL-Verbindungen auch ausgedehnte und anspruchsvolle Systeme realisiert werden, sodass dieser insgesamt mit vier Punkten bewertet wird.
Das LAN ist dem Lichtwellenleiter in vielerlei Hinsicht, vor allem der Bandbreite und möglichen Paralellübertragungen, unterlegen. Es bietet aber den Vorteil, die in den meisten Fällen bereits vorhandene Netzwerk-Infrastruktur mitnutzen zu können. Dadurch werden Aufwand und Kosten für eine Verlegung oftmals hinfällig. LAN wird folglich mit drei Punkten bewertet.
Die Zweidrahtverbindung und das Koaxialkabel können die Nachteile der kabelgebundenen Übertragungsarten nicht signifikant relativieren. Sie werden speziell für die Videoüberwachung geplant und verlegt. Eine Änderung oder Erweiterung ist anschließend nur mit hohem Aufwand möglich. Da sie aber dennoch eine höhere Anzahl an möglichen Kameras als die Funk-Verbindung bieten können, werden sie insgesamt ebenfalls mit zwei Punkten bewertet.

Die Anforderung **Integrität/Überprüfbarkeit/Beweiskraft** bedeutet bei den

Übertragungsarten die Möglichkeit, respektive Unmöglichkeit des Abgreifens des Signals entlang der Übertragungsstrecke. Folglich also, wie in der Beschreibung der Anforderung formuliert, das unberechtigte Mitsehen, Kopieren oder sogar Manipulation der Bilddaten. Auch in diesem Fall können durch die örtlichen Gegebenheiten und die Art der Installation die Bewertungen teilweise noch deutlich variieren. Die hier ermittelten Punktwerte stellen allgemeine Richtwerte im Hinblick auf das verwendete Verfahren dar. Je nach eigener Beurteilung der tatsächlichen Situation vor Ort können oder müssen diese dann noch entsprechend angepasst werden.
Die Übertragungsarten Zweidraht-Verbindung, Koaxialkabel und Lichtwellenleiter können, bei entsprechender Verlegung, einen sehr hohen Schutz gegen das unberechtigte Abgreifen von Daten bieten. Sie werden daher mit fünf Punkten bewertet.
Das LAN als weitere kabelgebundene Möglichkeit bietet als größten Vorzug die Nutzbarkeit bereits vorhandener und auch neuer Netzwerk-Infrastruktur durch mehrere Systeme. Dadurch entstehen an vielen Stellen Zugriffsmöglichkeiten auf den Datenstrom außerhalb des eigentlichen Videoüberwachungssystems. Dem kann jedoch durch ein exklusiv für die Videoüberwachung verlegtes Netz oder technische Maßnahmen, z.B. Verschlüsselung oder Nutzung eines virtuellen privaten Netzwerks, entgegengewirkt werden. Gesamt betrachtet kann das LAN ebenso sicher wie die anderen kabelgebundenen Übertragungsarten sein, aber auch deutlich unsicherer. Somit erfolgt als Richtwert eine Bewertung mit vier Punkten.
Ähnlich sieht es beim WLAN aus. Zwar ist durch den Sendebereich theoretisch auch ein Zugriff auf die Daten von außerhalb des Betriebsgeländes möglich. Dies hängt jedoch entscheidend von der Verschlüsselung ab. So bieten etwa laut Stiewe (2010) die Verschlüsselungsverfahren WPA2, WPA2-PSK oder RADIUS einen hohen Sicherheitsstandard, während hingegen WEP, WPA oder sogar unverschlüsselte kabellose Netzwerke keinen Schutz gewährleisten und die Integrität stark gefährden. Ähnlich wie beim LAN ist also durchaus eine sichere Nutzung möglich, aber nicht von vornherein garantiert. Für das WLAN werden ebenfalls als Richtwert vier Punkte vergeben.

Auch der optische Richtfunk bietet, trotz kabellosen Übertragens, eine recht hohe Sicherheit gegen das Abgreifen der Videodaten, wie auch Kraheck et al. (2004) deutlich machen. Zum einen müsste dazu ein Empfänger in den räumlich eng begrenzten Übertragungsstrahl gebracht werden, was sich je nach Position sehr schwierig gestalten kann. Zum anderen sind bei weitem nicht alle Sender und Empfänger untereinander kompatibel, sodass dazu eine genaue Kenntnis der vorhandenen Modelle und verwendeten Signale notwendig ist. Daher werden für IR/Laser ebenfalls vier Punkte vergeben.
Das schlechteste Ergebnis in Bezug auf diese Anforderung erzielt die Funk-Verbindung. Dies liegt einerseits in dem, ähnlich dem WLAN, großen räumlichen Sendebereich begründet, was ein Abgreifen der Daten erheblich erleichtert. Daneben sind laut Kraheck et al. (2004) die wenigstens Systeme auf dem Markt kodiert, was die Daten für jeden im Sendebereich zugänglich macht. Durch den zusätzlichen Umstand nur weniger zugelassener, also möglicher Frequenzen reichen bereits einfache technische Mittel und ein geringer Aufwand zum Abgreifen des Signals aus. Auch hier kann die Sicherheit natürlich noch erhöht werden, etwa durch einen nicht über das (gesicherte) Betriebsgelände hinaus gehenden Sendebereich oder eine Kodierung des Signals. Dennoch bietet die Funkverbindung im Allgemeinen keinen hohen Schutz und wird mit zwei Punkten bewertet.

4.7 Aufzeichnung/Speicherung

4.7.1 Übersicht und Beschreibung der Aufzeichnungs-/Speichermedien

Neben der abschreckenden Wirkung und dem Erkennen möglicher sicherheitsrelevanter Ereignisse in Echtzeit ist eine Hauptaufgabe eines Videoüberwachungssystem das nachträgliche zur Verfügung Stellen von Bildmaterial beim Eintritt sicherheitsrelevanter Ereignisse, um den Vorgang rekonstruieren und mögliche Täter identifizieren

Tabelle 4.10: Erfüllung der Anforderungen durch die Übertragungsarten.

	Zweidraht	Koax	Funk	IR/Laser	LWL	LAN	WLAN
Identifikation	x	x	x	x	x	x	x
Analyse	x	x	x	x	x	x	x
Integration	3	3	3	4	4	5	5
Sicht	x	x	x	x	x	x	x
Umgebung	5	5	4	2	5	5	4
Vandalismus	x	x	4	2	x	x	4
Verfügbarkeit	4	4	2	2	4	3	2
Skalierbarkeit	2	2	2	4	4	3	3
Integrität	5	5	2	4	5	4	4

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

zu können. Hierzu bedarf es einer zuverlässigen Aufzeichnung oder Speicherung, wofür es viele unterschiedliche Möglichkeiten gibt. Betrachtet werden die folgenden gebräuchlichen Systeme:

- DVD
- SD-Karte
- Interner Kameraspeicher
- Video-Drucker
- Digital Video Recorder (DVR)
- Network Video Recorder (NVR)
- Network Attached Storage (NAS)
- Storage Area Network (SAN)

Die BGI 819-2 (2008) fordert den Einsatz möglichst weit verbreiteter Systeme, um die Bilddaten der Polizei und anderen Behörden zur Verfügung stellen zu können, was auch durch alle genannten Möglichkeiten erfüllt wird. Entweder durch diese selbst (bei SD-Karte, DVD und Drucker), oder durch Anschluss und Übertragung

der Bilddaten auf ein gefordertes System (z.B. CD, DVD, SD-Karte, USB-Stick oder externe Festplatte).

Auch in der Kategorie der Aufzeichnungs-/Speichersysteme gibt es einige mögliche Anforderungen, die bei der Auswahl von Interesse sein können, aber aufgrund des Fokus dieses Buchs nicht näher betrachtet werden. So etwa die Kosten und die mögliche Speichergröße.

DVD

Die Digital Versatile Disk, kurz DVD, ist der Nachfolger der CD. Nach Brauner, Raible-Besten & Weigert (1998) können die Datenträger in zwei Schichten jeweils beidseitig beschrieben werden, womit Speicherkapazitäten bis zu über 18 Gigabyte erreicht werden. Es sind sowohl nur einfach- als auch wiederbeschreibbare Versionen erhältlich. Aus Qualitäts- und Sicherheitsgründen sollten in der Videoüberwachung jedoch nur einfach beschreibbare DVDs verwendet werden. Daher werden in diesem Buch auch nur diese betrachtet. Insofern besteht in der nur einmaligen Beschreibbarkeit und somit auch Unabänderlichkeit der Daten eines der hervorstechendsten Merkmale der DVD innerhalb der betrachteten Systeme.

SD-Karte

SD-Karten (Secure Digital Memory Card, zu deutsch Sichere Digitale Speicherkarte) sind nach Brauner, Raible-Besten & Weigert (1998) Speicherkarten, die aus schnell und elektrisch beschreibbaren EEPROM-Bausteinen bestehen. Sie sind löschbar, wiederbe- und überschreibbar. Aufgrund ihrer geringen geometrischen Ausmaße und im Vergleich zu anderen Systemen auch geringeren Speicherkapazität werden sie vorrangig zur direkten Aufzeichnung innerhalb einer Kamera eingesetzt. In diesem Sinne werden sie auch in diesem Buch betrachtet.

Interner Kameraspeicher

Interner Kameraspeicher meint in diesem Zusammenhang einen fest in die Kamera integrierten Festplatten-Speicher. Dieser entspricht somit in den für dieses Buch relevanten Eigenschaften der SD-Karte mit der Abweichung, dass diese ohne größeren Aufwand herausnehmbar und austauschbar ist, während der interne Kameraspeicher fester Bestandteil ist.

Video-Drucker

Ein Video-Drucker ist dazu geeignet, „ [...] Livebilder oder Aufzeichnungen, zu Beweiszwecken oder als Dokumentation auszudrucken [...] “ (Kraheck et al., 2004, S. 19). Dabei wird das empfangene Videobild direkt in einem internen Zwischenspeicher abgelegt und als unverändertes Originalbild auf geeignetem Fotopapier ausgedruckt. Möglich, und preiswerter, ist dies zwar auch mittels PC und einem handelsüblichen Drucker, jedoch können dann Manipulationen des Bildmaterials nicht ausgeschlossen werden.

Digital Video Recorder

Ein Digital Video Recorder (Abkürzung: DVR), zu deutsch Digitaler Videorekorder, „ [...] ist ein Aufzeichnungsgerät, das Video in einem Digitalformat auf einer Festplatte oder Solid State Disk (SSD) aufzeichnet.“ („DVR“, 2010). Er ist im Prinzip die Weiterentwicklung des VHS-Videorekorders. Die empfangenen digitalen Daten werden hierbei jedoch per Videodatenkompression komprimiert und anschließend auf einem digitalen Datenträger gespeichert, im Gegensatz zum analogen Videosignal und der Speicherung auf Videokassetten beim VHS-Videorekorder. Dabei sind Speicherkapazitäten von mehreren Giga- oder Terabyte möglich. Durch den Empfang unkomprimierter Daten wird allerdings auch eine hohe Belastung in der Übertragungsstrecke erzeugt.

Als sogenannter Hybrid-Rekorder oder Hybrid-DVR können, wie von Kühlewind (2009) erwähnt, auch die Signale analoger Kameras empfangen, digitalisiert, komprimiert und gespeichert werden. Dabei können, so schreiben Kraheck et al. (2004), mehrere Videosignale gleichzeitig empfangen und aufgezeichnet werden.

Network Video Recorder

Ein Network Video Recorder (Abkürzung: NVR), zu deutsch Netzwerk Videorekorder, zeichnet wie in „NVR“ (2010) beschrieben digitale Videosignale aus IP-Netzen auf. Im Gegensatz zum DVR werden hierbei die Daten bereits vor der Übertragung in der Kamera komprimiert und im NVR nur gespeichert. Durch die Nutzung von Netzwerken können NVR, anders als DVR, standortunabhängig von den Kameras aufgestellt und betrieben werden. Auch hier ist die parallele Aufzeichnung mehrerer Videosignale möglich. Speichergrößen von mehreren Terabyte sind gängig.

Network Attached Storage

Wie Troppens, Erkens & Müller (2008) schreiben, werden als Network Attached Storage (Abkürzung: NAS), zu deutsch ans Netzwerk angeschlossener Speicher, vorkonfigurierte Fileserver mit mehreren Datenträgern und speziellem Betriebssystem bezeichnet. Durch die Vorkonfiguration sind sie sehr einfach in Betrieb zu nehmen und zu verwalten. Sie werden an das Netzwerk angeschlossen und stellen im Falle der Videoüberwachung ihre Speicherkapazität unabhängig allen Kameras und zugriffsberechtigten Bedienerplätzen zur Verfügung.

Storage Area Network

Ein Storage Area Network (Abkürzung: SAN), zu deutsch Speichernetzwerk, ist ein „[...] Hochgeschwindigkeitsnetzwerk zwischen Servern (Hosts) und Speichersubsys-

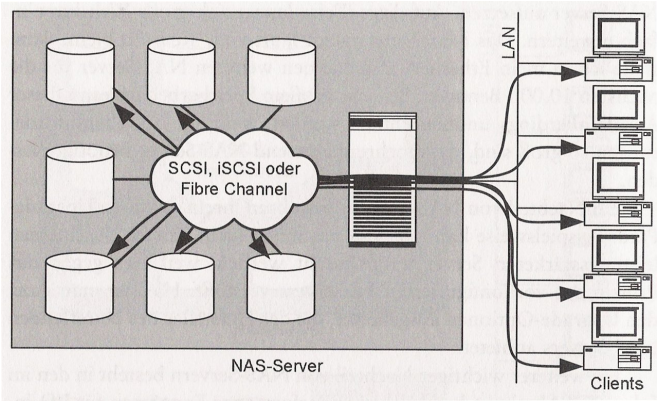


Abbildung 4.1: Funktionsprinzip eines NAS
Quelle: Troppens, Erkens & Müller, 2008, S. 148

temen.“ (Robbe, 2001). Es können auch große Datenmengen mit hoher Geschwindigkeit ausgetauscht werden. Hierbei sind alle Verbindungen flexibel und unabhängig untereinander möglich: Server zu Server, Server zu Speichersubsystem, Speichersubsystem zu Speichersubsystem. Zudem ist es einfach und sicher zu verwalten.

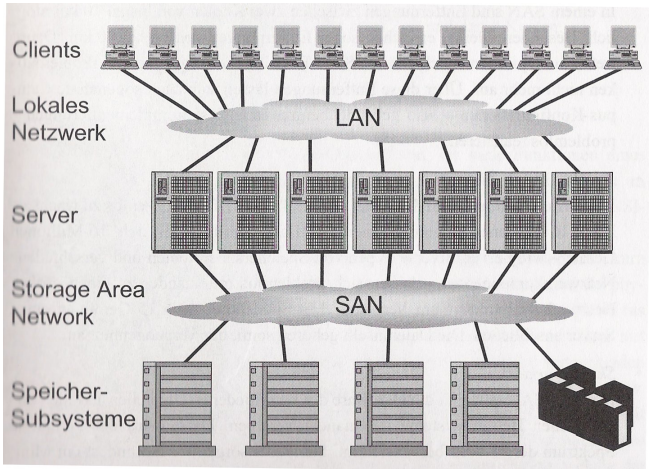


Abbildung 4.2: Aufbau eines SAN
Quelle: Robbe, 2001, S. 29

Im Falle der Videoüberwachung setzen sich die Clients in der Abbildung aus den Kameras, welche das Bildmaterial zur Verfügung stellen und im SAN abspeichern, sowie Bedienplätzen, die auf die gespeicherten Aufzeichnungen zugreifen können, zusammen.

4.7.2 Kompatibilität der Aufzeichnungs-/Speichermedien untereinander

Prinzipiell können die aufgeführten Speichersysteme frei miteinander kombiniert werden. Natürlich gilt es dabei, ein sinnvolles Maß an Aufwand zu betreiben. Ein Videoüberwachungssystem mit internem Speicher und SD-Karte in jeder Kamera, das die Videodaten sowohl an jeweils einen Digitalrekorder als auch ein Speichernetz überträgt, wobei die dort abgelegten Daten zusätzlich auf DVD gesichert werden, ist zwar durchaus realisierbar, der Kosten/Nutzen-Faktor allerdings sehr fragwürdig. Da alle hier beschriebenen Systeme mit digitalen Videodaten arbeiten, können diese darüber hinaus auch untereinander übertragen und genutzt werden.

Lediglich die Rückübertragung ausgedruckter Videobilder vom Videodrucker in ein anders Speichermedium funktioniert nicht. Der Videodrucker kann zwar durchaus auch mit allen anderen Speichermedien parallel eingesetzt werden, der Datenaustausch ist aber nur bedingt (nämlich nur in eine Richtung) möglich.

Tabelle 4.11: Kompatibilität der Speicher-/Aufzeichnungssysteme untereinander.

	DVD	SD	Intern	V-Drucker	DVR	NVR	NAS	SAN
DVD	+	+	+	o	+	+	+	+
SD	+	+	+	o	+	+	+	+
Intern	+	+	+	o	+	+	+	+
V-Drucker	+	+	+	o	+	+	+	+
DVR	+	+	+	o	+	+	+	+
NVR	+	+	+	o	+	+	+	+
NAS	+	+	+	o	+	+	+	+
SAN	+	+	+	o	+	+	+	+

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.7.3 Erfüllung der Anforderungen durch die Aufzeichnungs-/Speichermedien

Das genutzte Speichermedium wirkt sich unterschiedlich auf die Anforderungen Schutz vor Vandalismus/Sabotage, hohe Verfügbarkeit, Skalierbarkeit/Erweiterbarkeit/-Aufrüstbarkeit und Integrität/Überprüfbarkeit/Beweiskraft aus.

Den niedrigsten **Schutz vor Vandalismus/Sabotage** unter den Speichermedien bietet die SD-Karte. Sie ist direkt in der entsprechenden Kamera enthalten und per Definition leicht herausnehmbar, auch wenn sie möglicherweise durch eine verschlossene Klappe oder ähnliches geschützt wird. Sie wird daher mit einem Punkt bewertet.
Ein interner Kameraspeicher ist bereits etwas schwieriger unbrauchbar zu machen. Dies gelingt meist nur durch die Zerstörung oder Wegnahme der kompletten Kamera. Es erfolgt eine Bewertung mit zwei Punkten.
Eine DVD und ein Ausdruck eines Videodruckers sind frei bewegliche Objekte von relativ geringen Ausmaßen. Sie werden in der Regel nicht in unmittelbarer Nähe der Kamera, sondern in der Empfangsstelle erstellt und entweder auch dort oder an speziell dafür vorgesehenen Orten aufbewahrt. Dennoch können sie mit vergleichsweise geringem Aufwand entwendet und/oder zerstört werden und erhalten somit drei Punkte.
Ein Digitaler Videorekorder wird sich in den meisten Fällen ebenfalls in der Empfangsstelle befinden. Eine Wegnahme oder Zerstörung ist aber schon mit höherem Aufwand verbunden als bei der DVD oder einem Ausdruck und wird mit deutlich niedrigerer Wahrscheinlichkeit unbemerkt durchgeführt werden können. Daraus resultiert eine Bewertung mit vier Punkten.
Den besten Schutz bieten Netzwerk Videorekorder, Network Attached Storage und Storage Area Network. Da sie alle über das Netzwerk mit Kameradaten gespeist werden und diese auch wieder über das Netzwerk zur Verfügung stellen, ist eine räumliche Nähe weder zu den Kameras noch zur Empfangsstelle notwendig. Demzu-

folge ist ein physischer Kontakt mit dem mutmaßlichen Täter eher unwahrscheinlich, was eine Bewertung mit fünf Punkten bedingt.

Es gibt viele Gründe, aus denen aufgezeichnetes Datenmaterial verloren gehen kann. Beispiele hierfür sind technische Defekte eines Speichermediums, der Ausfall von Stromversorgung oder Übertragungseinrichtung, die Zerstörung oder Entwendung von Datenträgern oder gar Zerstörung der beherbergenden Räumlichkeiten durch Brand, Wassereinbruch oder ähnliches. Bei der Absicherung des Datenbestandes an Videomaterial geht es darum hauptsächlich um redundante Speicherhaltung. Es spielt also nicht vordergründig das verwendete Medium, sondern die Anzahl an parallel eingesetzten gleich- oder besser noch verschiedenartigen Medien eine Rolle.
Daher werden, mit drei Ausnahmen, alle Speichermedien mit drei Punkten bewertet. Die Erfüllung der Anforderung **Hohe Verfügbarkeit** ergibt sich dann aus der Addition der Punktzahlen aller zur parallelen Aufzeichnung eingesetzten Speichermedien. So kann beispielsweise das von Kühlewind (2009) beschriebene ANR-Verfahren zum Einsatz kommen: Verwendet werden können hierbei etwa ein NAS sowie SD-Karten direkt in den Kameras. Die Aufzeichnung erfolgt grundsätzlich im NAS. Sollte das Netzwerk einmal unterbrochen werden oder der NAS ausfallen, wird die SD-Karte zur Zwischenspeicherung genutzt. Nach Wiederherstellung wird der NAS mit den Videodaten aus den SD-Karten aufgefüllt. Umgekehrt stehen bei Zerstörung oder Diebstahl der SD-Karte oder der kompletten Kamera die Daten im NAS weiterhin zur Verfügung.
Die erwähnten drei Ausnahmen mit anderer Bewertung sind SAN, NAS und der Videodrucker. SAN und NAS können Dey (2006) zufolge aufgrund redundanter Konfiguration bzw. optimaler Abbildbarkeit von Hochverfügbarkeitsstrukturen bereits von sich aus eine hohe Verfügbarkeit garantieren. Zudem können sie auch über weite räumliche Entfernungen untereinander sowie zu Kameras und Empfangsstelle operieren, was eine zusätzliche Sicherheit bietet. Daher werden diese beiden Speichermedien mit 5 Punkten bewertet. Ein Videodrucker hingegen kann nur stellenweise einzelne bedeutsame Bilder zusätzlich redundant abbilden, jedoch keine dauerhaft

hohe Verfügbarkeit garantieren. Er erhält folglich nur einen Punkt.

Auch bei der **Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit** verfügen NAS und SAN über die besten Eigenschaften. Nach Robbe (2001) können in einem SAN bis zu 16 Millionen Komponenten miteinander verbunden werden, was nahezu grenzenloses Wachstum ermöglicht. Daneben können unterschiedlichste Hardware verschiedener Hersteller und unterschiedliche Betriebssysteme problemlos zusammen eingesetzt werden. Auch NAS kann durch unterschiedlich viele und unterschiedlich große Datenträger ebenso wie durch den Einsatz mehrerer NAS-Server in einem Netzwerk an die eigenen Bedürfnisse angepasst werden und ist, wie Troppens, Erkens & Müller (2008) beschreiben, bei Bedarf einfach erweiterbar. Genau wie SAN ist NAS laut „NAS“ (2007) Plattform übergreifend einsetzbar. Damit können die gestellten Anforderungen durch diese beiden Systeme optimal erfüllt werden, was einer Bewertung von fünf Punkten entspricht.
Die Datenträger bei DVR und NVR sind auch in verschiedenen Kapazitäten erhältlich, und die Geräte können in unterschiedlicher Stückzahl nebeneinander verwendet bzw. die Anzahl erhöht werden. Alles aber in begrenzterem Rahmen als dies bei NAS und SAN möglich ist. Ferner ist die Speicherkapazität bereits vorhandener Geräte nicht unbegrenzt aufrüstbar und nicht alle Rekorder arbeiten einwandfrei mit jeder Videomanagementsoftware zusammen, sodass hier vier Punkte vergeben werden.
Ähnlich sieht es beim internen Kameraspeicher aus, der ebenfalls nur begrenzten und kaum erweiterbaren Speicherplatz bietet. Im Gegensatz zu DVR und NVR entfällt hier aber zusätzlich die Möglichkeit des Einsatzes mehrerer Speicher bzw. die Zuschaltung neuer Speicher. Somit wird der interne Speicher mit drei Punkten bewertet.
DVDs besitzen, wie in der Beschreibung erwähnt, eine maximale Kapazität von etwas mehr als 18 Gigabyte. Es können natürlich mehrere DVDs parallel und auch nacheinander eingesetzt werden, was aber mit steigender Daten-Bandbreite und Speicherbedarf immer aufwendiger wird. Auch die Speichergröße von SD-Karten

ist je nach Version auf ein bestimmtes Maß beschränkt. Zudem sind Schnittstellen und Lesegeräte nur bis zu einer gewissen Größe kompatibel, was Aufrüstung und Neuanschaffungen erschwert. Demzufolge erfüllen diese beiden Speichermedien nur in begrenztem Maße die Anforderung und werden mit zwei Punkten bewertet.
Bei einem Videodrucker erweist sich die Frage nach Speichergröße und Erweiterbarkeit als nicht sinnvoll, sodass in der Tabelle das dafür vorgesehene Zeichen ('x') aufgeführt wird.

Die **Integrität/Überprüfbarkeit/Beweiskraft** der Videodaten können grundsätzlich nur die DVD und der Videodrucker garantieren. Durch den direkten Bezug der Daten von den Kameras ohne externe Zwischenspeicherung sind die Ausdrucke beim Videodrucker laut Kraheck et al. (2004) „absolut beweiskräftig“ (S. 20). Ebenso verhält es sich bei der DVD, wenn in selbiger Weise verfahren wird, wovon hier in diesem Buch ausgegangen wird. Durch die nur einmalige Beschreibbarkeit ist eine nachträgliche Manipulation ausgeschlossen. Daher wird jeweils mit fünf Punkten bewertet.
Bei den restlichen Systemen werden die Daten digital hinterlegt und aufbewahrt. Mit entsprechender Software können diese dann beliebig verändert werden. Um dies zu verhindern, müssen weitergehende Maßnahmen getroffen werden. Von sich aus bieten die Medien zunächst einmal keinen Schutz, werden also mit null Punkten bewertet. Dies bedeutet nicht, dass sie prinzipiell zur Speicherung beweiskräftiger Daten ungeeignet sind. Um diese Anforderung zu erfüllen besteht jedoch zusätzlicher Handlungsbedarf.

Tabelle 4.12: Erfüllung der Anforderungen durch die Speicher-/Aufzeichnugssysteme.

	DVD	SD	Intern	V-Drucker	DVR	NVR	NAS	SAN
Identifikation	x	x	x	x	x	x	x	x
Analyse	x	x	x	x	x	x	x	x
Integration	x	x	x	x	x	x	x	x
Sicht	x	x	x	x	x	x	x	x
Umgebung	x	x	x	x	x	x	x	x
Vandalismus	3	1	2	3	4	5	5	5
Verfügbarkeit	3	3	3	1	3	3	5	5
Skalierbarkeit	2	2	3	x	4	4	5	5
Integrität	5	0	0	5	0	0	0	0

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.8 Protokolle und Schnittstellen

4.8.1 Übersicht und Beschreibung der Protokolle und Schnittstellen

Wie bisher deutlich wurde, ist es nicht immer ohne weiteres möglich, verschiedenartige Produkte und Komponenten zu kombinieren, vor allem in der Digitaltechnologie (siehe 4.1.1), oder ein Videoüberwachungssystem zu erweitern/aufzurüsten und mit anderen Systemen (z.B. Zutrittskontrolle) zusammenarbeiten zu lassen (siehe hierzu die Anforderungen 3.2.3 und 3.2.8).
Zur Lösung derartiger Probleme existieren bereits einige Protokolle und Schnittstellen, welche die Kommunikation und Kompatibilität zwischen Komponenten und Systemen standardisieren.

Im Folgenden werden ausgewählte Beispiele, die derzeit in der Videoüberwachung von Bedeutung sind vorgestellt. Dies sind das Pelco-D Protokoll, die ONVIF-Schnittstelle, OPC, BACnet und der Sinteso Video Fire Controller.

Pelco-D-Protokoll

Das Pelco-D-Protokoll „ [...] ist das weitverbreiteste Protokoll für die Ansteuerung von PTZ-Kameras.“ („Pelco-D“, 2009). PTZ steht für pan/tilt/zoom, also die Schwenk-, Neige- und Vergrößerungsfunktion. Es vereinfacht Anschaffung, Zukauf und Austausch von verschiedenen Kameras und Steuerelementen, wie am Beispiel des Flughafens Kopenhagen deutlich wird: „Genau wie alle anderen Kameras, die wir verwenden, lassen sich die Flir-Wärmebildkameras über das Pelco-D-Protokoll ansteuern. So konnten sie einfach in unser bestehendes Pelco-D-Netzwerk integriert werden.“ (Maras, 2007, S. 63).

ONVIF

Das Open Network Video Interface Forum (Abkürzung: ONVIF) ist nach „ONVIF“ (2010) eine Non-Profit-Organisation, die 2008 von drei führenden Herstellern von Videoüberwachungstechnik gegründet wurde. Ziel war und ist die Schaffung einer global einheitlichen offenen Schnittstelle für Netzwerk-Videoprodukte. Die Schnittstelle basiert auf der Metasprache Web Service Description Language (Abkürzung: WSDL) und gewährleistet somit die Interoperabilität unabhängig von Produkt, Hersteller, Plattform, Protokoll und Programmiersprache.
Inzwischen sind der Initiative, wie Klitsch (2010) schreibt, bereits mehr als 100 Unternehmen beigetreten. Zusammen repräsentieren diese einen Marktanteil von 40 % im Bereich der Videoüberwachung, bei den Netzwerk-Videoprodukten sind es sogar 60 % („ONVIF“, 2010, S. 3). Demzufolge hat sich die ONVIF-Schnittstelle mittlerweile als führender de facto Standard auf dem Markt etabliert.
In Planung bzw. bereits in der Entwicklung befindlich ist die Einbindung weiterer Bereiche wie Zutrittskontrolle oder Brandmeldetechnik.

OPC

Die Schnittstelle Object Linking and Embedding for Process Control (Abkürzung: OPC) wird von Kräußlich (2008b) in seinem Artikel erläutert: Sie stammt ursprünglich aus der Automatisierungstechnik und definierte einen standardisierten Datenaustausch zwischen verschiedenen Anwendungen. Inzwischen wird der Standard vor allem in der Leitebene zur software-seitigen übergreifenden Kommunikation unterschiedlicher Subsysteme (z.B. Zutrittskontrolle und Videoüberwachung) untereinander eingesetzt.

BACnet

Das 1987 entwickelte Protokoll Building Automation and Control Networks (Abkürzung: BACnet) stammt laut Kräußlich (2008b) aus der Gebäudeautomation und ist ein Standard zur Datenkommunikation innerhalb und zwischen verschiedenen Systemen. BACnet ist gemäß DIN-EN 16484-5 genormt. Wie Schneider (2010) schreibt, lassen sich mit seiner Hilfe systemübergreifend die Gewerke verschiedener Hersteller integrieren. Damit erfüllt es ähnliche Aufgaben wie OPC.

Sinteso Video Fire Controller

Der Video Fire Controller des Brandmeldesystems Sinteso ermöglicht die Ansteuerung von Videokameras durch die Brandmeldezentrale, so Kräußlich (2008a). Mittels der Videodaten können Alarme verifiziert und die Situation geklärt werden. Dadurch können Fehlalarme und die notwendige Stärke des Sicherheitspersonals reduziert werden.

4.8.2 Kompatibilität der Protokolle und Schnittstellen untereinander

Die aufgeführten Protokolle und Schnittstellen befinden sich auf unterschiedlichen Ebenen und behandeln unterschiedliche Aufgabengebiete. Im Gegensatz zu den bisher behandelten Unterscheidungskriterien stehen sie sich nicht als mögliche Alternativen für den selben Einsatzzweck gegenüber. Daher ist eine Aussage über die Kompatibilität untereinander als nicht sinnvoll anzusehen.

Tabelle 4.13: Kompatibilität der Protokolle/Schnittstellen untereinander.

	Pelco-D	ONVIF	OPC	BACnet	SVFC
Pelco-D	x	x	x	x	x
ONVIF	x	x	x	x	x
OPC	x	x	x	x	x
BACnet	x	x	x	x	x
SVFC	x	x	x	x	x

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.8.3 Erfüllung der Anforderungen durch die Protokolle und Schnittstellen

Die Potokolle und Schnittstellen ermöglichen und/oder verbessern definitionsgemäß die Integration von und das Zusammenspiel mit anderen Systemen sowie die Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit von Videoüberwachungssystemen.

Die Anforderung **Integration/Zusammenspiel mit anderen Systemen** ist zwar nicht direkte Aufgabe des Pelco-D-Protokolls. Es kann aber durch die standardisierten Steuerbefehle für unterstützte Kameras eine Zusammenarbeit vereinfachen, indem es von einem anderen System zur Ansteuerung genutzt wird. Entsprechend wird es mit zwei Punkten bewertet.

Die ONVIF-Schnittstelle wird zwar zukünftig auch mit anderen Systemen zusammenarbeiten können, derzeit ist dies aber noch nicht der Fall. Im Moment können daher noch keine Punkte vergeben werden. Sollte sich dies zum Zeitpunkt der Nutzung dieses Buchs bereits geändert haben, sind hier entsprechende Anpassungen der Punktzahl vorzunehmen.
Sowohl OPC als auch BACnet können einen Datenaustausch zwischen Systemen gewährleisten. Da dies aber nur auf bestimmten Ebenen und bestimmte Funktionen beschränkt ist, können sie keine vollständige Integration ermöglichen. Sie stellen viel mehr eine Art Verknüpfung oder Zwischenstück dar, keine umfassende einheitliche Lösung. Darüber hinaus sind sie nicht explizit für Videoüberwachungssysteme entwickelt worden, welche im Fokus dieses Buchs stehen. Daher erfolgt eine Bewertung mit drei Punkten.
Der Sinteso Video Fire Controller gestattet die vollständige Nutzung des Videoüberwachungssystems durch die Brandmeldeanlage. Es erfüllt die Anforderung aus Sicht des Videoüberwachungssystems optimal, jedoch nur für den Bereich Brandmeldeanlagen. Andere Gewerke wie Zutrittskontrolle oder Zeiterfassung werden nicht unterstützt. Aufgrund der umfassenden, speziell auf Videoüberwachungssysteme zugeschnittene Funktion, aber des eingeschränkten Einsatzbereichs erfolgt eine Bewertung mit drei Punkten.

Das Pelco-D-Protokoll ermöglicht die problemlose **Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit** eines Videoüberwachungssystems, wie im Beispiel in 4.8.1 genannt. Dies aber nur für PTZ-Kameras und die Steuersignale. Auf das Videosignal hat es hingegen keinen Einfluss. Es umfasst also nur einen Teilaspekt und wird daher mit zwei Punkten bewertet.
Im Gegensatz dazu bietet die ONVIF-Schnittstelle eine umfassende Kompatibilität aller unterstützten Komponenten. Nach „ONVIF“ (2010) umfasst dies unter anderem auch die automatische Erkennung von Geräten, die PTZ-Steuerung und sogar Ereignishandling und Videoanalyse. Ein auf ONVIF-konformen Komponenten basierendes Videoüberwachungssystem kann ohne Einschränkungen angepasst

und erweitert werden sowie den Austausch von Komponenten ermöglichen. Demzufolge erfüllt die Schnittstelle die Anforderung in optimaler Weise.
OPC und BACnet ermöglichen den Datenaustausch zwischen Systemen, jedoch nicht zwischen den Komponenten innerhalb eines Videoüberwachungssystems. Für diese Aufgabe wurden sie nicht entwickelt und können diese Anforderung folglich nicht erfüllen.
Auch der Sinteso Video Fire Controller dient einzig dem Zweck der Interoperabilität von Videoüberwachungssystem und Brandmeldeanlage. Zur Erfüllung der Anforderung trägt er jedoch nicht bei.

Tabelle 4.14: Erfüllung der Anforderungen durch die Protokolle und Schnittstellen.

	Pelco-D	ONVIF	OPC	BACnet	Sinteso VFC
Identifikation	x	x	x	x	x
Analyse	x	x	x	x	x
Integration	2	0	3	3	3
Sicht	x	x	x	x	x
Umgebung	x	x	x	x	x
Vandalismus	x	x	x	x	x
Verfügbarkeit	x	x	x	x	x
Skalierbarkeit	2	5	0	0	0
Integrität	x	x	x	x	x

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.9 Stromversorgung

4.9.1 Übersicht und Beschreibung der Stromversorgungsarten

Eine essentielle Rolle in einem Videoüberwachungssystem spielt die Energieversorgung der Kameras und anderen Komponenten. Neben dem gewöhnlichen 230 V-Netz bietet sich in Netzwerk basierten Systeme auch Power over Ethernet sowie bei analogen Komponenten das Video-Kombi-Kabel als Alternative an. Daneben sollte

im Bereich der Sicherheitstechnik generell auch der Einsatz einer unterbrechungsfreien Stromversorgung oder einer Netzersatzanlage in Betracht gezogen werden. Die genannten Systeme werden im Folgenden näher betrachtet.

230 V-Netz

Die naheliegendste Möglichkeit stellt die direkte Versorgung über das öffentliche 230 V-Netz dar. Zu beachten ist jedoch, dass in diesem Fall auch in räumlicher Nähe aller zu versorgenden Komponenten eine Leitung bzw. ein Stromanschluss zur Verfügung stehen muss.

Power over Ethernet

Die Notwendigkeit eines separaten Stromanschlusses in direkter räumlicher Nähe der Kameras und anderen Komponenten kann bei Netzwerk basierten Videoüberwachungssystemen durch die Nutzung von Power over Ethernet (Abkürzung: PoE) umgangen werden. Wie Rech (2008) schreibt, wurde diese Erweiterung des Ethernet-Standards 2003 als IEEE-802.3af (IEEE ist die Abkürzung für Institute of Electrical and Electronics Engineers, einem weltweiten Verband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik) spezifiziert und hat sich inzwischen weithin etabliert. Bei diesem Verfahren wird neben den Daten auch eine Gleichspannung über das normale Netzwerkkabel übertragen, wobei die Datenübertragung dadurch jedoch nicht beeinflusst wird.

Video-Kombi-Kabel

Das Video-Kombi-Kabel stellt eine Art analoge Entsprechung der PoE-Technologie dar. Nach Niecke (2009a) sind hier neben dem Anschluss zur Übertragung der Videodaten zusätzlich zwei Litzen zur Stromversorgung integriert. Damit kann auch bei

analogen Systemen oder einzelnen Komponenten die Notwendigkeit von räumlich nahen Netzanschlüssen umgangen werden.

Unterbrechungsfreie Stromversorgung

Eine unterbrechungsfreie Stromversorgung (Abkürzung: USV) wird nach Brauner, Raible-Besten & Weigert (1998) zwischen Netz und zu versorgende Komponente(n) geschaltet und kann bei einem Ausfall kurzfristig die Energieversorgung weiterhin sicherstellen. Dies geschieht durch eine Batterie- bzw. Akkupufferung, wodurch die Überbrückungszeit allerdings auf kürzere Intervalle begrenzt ist: "Wenn das Stromnetz für mehrere Stunden ausfällt, helfen auch die besten Batterien nicht."(Wölpert & Baganz, 2008, S. 174).

Netzersatzanlagen

Eine Netzersatzanlage (Abkürzung: NEA) stellt eine erweiterte Form der USV dar und eignet sich zum Überbrücken auch längerer Netzausfallzeiten. In den meisten Fällen handelt es sich dabei um Dieselgeneratoren, aber auch andere Formen wie Blockheizkraftwerke oder Brennstoffzellen sind möglich, so Wölpert & Baganz (2008). Während eine USV bei einem Netzausfall ohne merkbare Verzögerung in Betrieb geht, ist bei Netzersatzanlagen zunächst eine Anlaufzeit notwendig. Um eine Unterbrechung der Energieversorgung zu verhindern, müssen NEA daher mittels USV gepuffert werden.

4.9.2 Kompatibilität der Stromversorgungsarten untereinander

Versorgung aus gewöhnlichen Anschlüssen ans 230 V-Netz, Video-Kombi-Kabel und Power over Ethernet können beliebig nebeneinander eingesetzt werden. Auch aus unterbrechungsfreier Stromversorgung und Netzersatzanlagen können alle drei Versorgungsarten bei einem Netzausfall gespeist werden. Jedoch ist die direkte Ver-

sorgung allein aus einer NEA ohne Unterbrechungen nur unter der Bedingung des Vorhandenseins einer USV möglich. Natürlich können auch mehrere USV und/oder NEA nebeneinander eingesetzt werden.

Tabelle 4.15: Kompatibilität der Stromversorgungsarten untereinander.

	230 V	PoE	Kombi-Kabel	USV	NEA
230 V	+	+	+	+	o
PoE	+	+	+	+	o
Kombi-Kabel	+	+	+	+	o
USV	+	+	+	+	+
NEA	o	o	o	+	+

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.9.3 Erfüllung der Anforderungen durch die Stromversorgungsarten

Die Art der Stromversorgung eines Videoüberwachungssystems wirkt sich auf die Anforderungen Schutz vor Vandalismus/Sabotage, hohe Verfügbarkeit und Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit aus.

Die Versorgung über das 230 V-Netz, Power over Ethernet oder Video-Kombi-Kabel leistet an sich keinen Beitrag zum **Schutz vor Vandalismus/Sabotage**. Alle drei sind auf das Kabel als Übertragungsmedium angewiesen und sind dadurch gleichermaßen vulnerabel gegenüber den Angriffen Dritter. Ein wirksamer Schutz kann nur durch die Art der Verlegung gewährleistet werden, was einen individuellen vom jeweiligen Einzelfall abhängigen Faktor darstellt, welcher nicht durch eine generelle Bewertung hier erfasst werden kann. Die Systeme an sich müssen folglich mit null Punkten bewertet werden. Abhängig von den Bedingungen im zu bewertenden Videoüberwachungssystem können die Punktezahlen eigenständig entsprechend angepasst

werden.

Ein Akt der Sabotage oder des Vandalismus führt in der Regel zur Trennung der Stromversorgung (Durchtrennen von Leitungen, Abschalten/Zerstören von Sicherungen etc.) und damit zu längerfristigen Ausfallzeiten bis zur Durchführung entsprechender Reparaturmaßnahmen. Da eine USV den Weiterbetrieb nur für kürzere Zeitabschnitte gewährleisten kann, ist sie zur Erfüllung der Anforderung nur beschränkt geeignet. Unterschieden werden muss jedoch zwischen dem kompletten Ausfall im gesamten Videoüberwachungssystem und dem Ausfall der Versorgung einzelner Komponenten (z.B. der Durchtrennung eines Versorgungskabels entlang der Übertragungsstrecke von Kamera zur Empfangsstelle). USV sind in verschiedenen Größen und Leistungsklassen erhältlich und sowohl zur Pufferung einzelner Komponenten direkt am oder neben dem Gerät, als auch zur Pufferung ganzer (Teil-)Systeme geeignet und sind damit in der Lage, beide Fälle abzudecken. Daher werden sie mit drei Punkten bewertet.

Im Gegensatz dazu ermöglicht eine Netzersatzanlage auch über längere Zeiträume hinweg eine ausreichende Stromversorgung eines kompletten Videoüberwachungssystems. Tritt hingegen der zweite Fall ein, also die Trennung der Versorgung einzelner Komponenten an einer Stelle zwischen NEA/230 V-Netz und dem Gerät, ist die NEA nutzlos. Demzufolge werden hier ebenfalls drei Punkte vergeben.

Auch anderen Ausfallgründen können die Versorgung über 230 V-Netz, PoE oder Video-Kombi-Kabel nicht entgegenwirken. Sie haben generell keine Auswirkung auf die **hohe Verfügbarkeit** der Energieversorgung, womit sie auch hier mit null Punkten bewertet werden.

Im Falle der Stromversorgung gilt es zur Erfüllung der Anforderung hohe Verfügbarkeit die Energieversorgung bei einem Ausfall des öffentlichen Netzes sicherzustellen. Nach Merz (2008) dauert ein solcher Stromausfall in Deutschland durchschnittlich 19,3 Minuten. Zeiträume dieser Größenordnung können sowohl von USV als auch von NEA überbrückt werden. Bei statistisch zu erwartenden deutlich längeren Ausfallzeiten garantiert allerdings nur eine NEA eine durchgängige Verfügbarkeit. Daher

erfolgt eine Bewertung der USV mit vier, der NEA mit fünf Punkten.

Zur Gewährleistung der **Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit** ist eine Versorgung über direkte Anschlüsse ans 230 V-Netz kaum geeignet, da sich die Anschlüsse wie bereits in 4.9.1 beschrieben in räumlicher Nähe zu den Komponenten befinden müssen. Vor allem im Außenbereich befindet sich nur selten ein Netzanschluss am Montageort, was das aufwändige Verlegen von zusätzlichen Kabeln notwendig macht. Folglich wird hier mit einem Punkt bewertet.
Bei der Nutzung von Video-Kombi-Kabeln ist nur noch ein Kabel zur Kamera notwendig. Netzanschlüsse müssen nicht mehr direkt an jedem Montageort vorhanden sein, was vor allem den Standortwechsel und die Aufstellung zusätzlicher Kameras deutlich erleichtert. Allerdings kann es nur zur Versorgung analoger Kameras verwendet werden. Das Video-Kombi-Kabel wird daher mit drei Punkten bewertet.
Neben den selben Vorzügen wie auch das Video-Kombi-Kabel, jedoch im digitalen Bereich, kann die Versorgung über PoE darüber hinaus problemlos in bereits vorhandene Netzwerkstrukturen integriert werden, so Rech (2008). Zur Einspeisung können geeignete Hubs oder Switches, aber auch sogenannte Injektoren, die einfach an den entsprechenden Stellen zwischengeschaltet werden, benutzt werden. Da PoE-fähige Geräte automatisch erkannt und die Funktion erst dann am jeweiligen Anschluss aktiviert wird, können auch nicht PoE-fähige Geräte bedenkenlos im selben Netz eingesetzt werden. Darüber hinaus besteht auch die Möglichkeit, die Stromversorgung direkt am Anschluss mittels eines Splitters wieder vom Datensignal zu trennen. So können auch nicht PoE-fähige Geräte über nur ein Netzwerkkabel verbunden und mit Strom versorgt werden. Angesichts der hohen Funktionalität und Flexibilität aber auch der Beschränkung des Einsatzes auf Netzwerk basierte Komponenten wird PoE mit vier Punkten bewertet.
Zwar lassen sich unterbrechungsfreie Stromversorgungen laut Wölpert & Baganz (2008) einfach erweitern und nachrüsten, was auch bei Netzersatzanlagen der Fall ist. Dennoch erhöhen die beiden Systeme nicht die Skalierbarkeit/Erweiterbarkeit/-Aufrüstbarkeit des Videoüberwachungssystems an sich, sondern erfüllen die An-

forderung nur auf sich selbst bezogen. Dementsprechend ist eine Bewertung und Punktevergabe hinsichtlich des gesamten Videoüberwachungssystems nicht sinnvoll.

Tabelle 4.16: Erfüllung der Anforderungen durch die Stromversorgungsarten.

	230 V	Kombi-Kabel	PoE	USV	NEA
Identifikation	x	x	x	x	x
Analyse	x	x	x	x	x
Integration	x	x	x	x	x
Sicht	x	x	x	x	x
Umgebung	x	x	x	x	x
Vandalismus	0	0	0	3	3
Verfügbarkeit	0	0	0	4	5
Skalierbarkeit	1	4	3	x	x
Integrität	x	x	x	x	x

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.10 Schutz vor Einflüssen aus der Umgebung

4.10.1 Übersicht und Beschreibung der Schutztechniken

Vor allem im Außenbereich sind Kameras und andere Komponenten einer Vielzahl von erschwerenden Einflüssen aus ihrer Umgebung ausgesetzt. Dies können Temperatur, Sichtbedingungen und Wetter ebenso sein wie Versuche der Manipulation oder Vandalismus. Je nach Aufstellungsort muss mit derartigen Faktoren gerechnet und entsprechende Gegenmaßnahmen getroffen werden. Hierzu können die Kameras und Komponenten entsprechend einer IP-Schutzart konstruiert werden, sie können mit technischen Zusatzausstattungen sowie Manipulations- und Vandalismusschutz ausgestattet werden. Diese Möglichkeiten werden im Folgenden behandelt.

IP-Schutzart

Die IP-Schutzarten nach DIN EN 60529 geben wie bei „Schutzarten“ (2008) beschrieben den Schutz elektrischer Betriebsmittel vor Berührung/Fremdkörpern und Wasser an. Die Angabe besteht aus dem Kürzel IP und zwei Ziffern, in manchen Fällen erweitert durch zwei Kennbuchstaben, und entspricht dem Schema IP XXXX. Hierbei steht IP für International Protection, die erste Ziffer gibt den Schutz vor Berührung/Fremdkörpern an (Einteilung der Klassen wie in Tabelle 4.17), die zweite Ziffer den Schutz vor Wasser (Einteilung der Klassen wie in Tabelle 4.18). An der dritten Stelle kann ein Kennbuchstabe zum zusätzlichen Berührungsschutz und an der vierten Stelle ergänzende Buchstaben angegeben werden. In den meisten Fällen, insbesondere in der Videoüberwachung, sind nur die beiden Ziffern relevant. Daher werden ihre Bedeutungen jeweils in einer Tabelle aufgeführt, die Kennbuchstaben werden aufgrund ihrer geringen Bedeutung in der Videoüberwachung nicht behandelt.

Tabelle 4.17: Kennziffern für den Schutz vor Berührung/Fremdkörpern nach DIN EN 60529.

Kennziffer	Schutz vor Berührung & Schutz vor Fremdkörpern
IP 0X	Kein Berührungsschutz, kein Fremdkörperschutz
IP 1X	Berührung mit Handrücken, Fremdkörper mit Durchmesser ab 50 mm
IP 2X	Berührung mit Finger, Fremdkörper mit Durchmesser ab 12,5 mm
IP 3X	Berührung mit Werkzeug, Fremdkörper mit Durchmesser ab 2,5 mm
IP 4X	Berührung mit Draht, Fremdkörper mit Durchmesser ab 1 mm
IP 5X	Vollst. Berührungssch., Staubablagerungen im Innern (staubgeschützt)
IP 6X	Vollst. Berührungssch., Eindringen von Staub (staubdicht)

Durch die Auswahl von Komponenten mit entsprechender Schutzart ist auch der Einsatz unter schwierigen Bedingungen möglich.

Technische Zusatzausstattung

Neben der Verwendung von Kameras oder Wetterschutzgehäusen mit IP-Schutzart gibt es noch eine Vielzahl weiterer technischer Zusatzausstattungen zum Schutz vor

Tabelle 4.18: Kennziffern für den Schutz vor Wasser nach DIN EN 60529.

Kennziffer	Schutz vor Wasser
IP X0	Kein Wasserschutz
IP X1	Senkrecht fallendes Tropfwasser
IP X2	Schräg fallendes Tropfwasser bis zu 15 Grad gegenüber d. Senkr.
IP X3	Schräges Sprühwasser bis zu 60 Grad gegenüber der Senkrechten
IP X4	Allseitiges Sprühwasser
IP X5	Allseitiges Strahlwasser (Düse)
IP X6	Starkes Strahlwasser, kurzzeitige Überflutung
IP X7	Zeitweiliges Untertauchen
IP X8	Untertauchen für unbestimmte Zeit

Einflüssen aus der Umgebung. Einige von Kraheck et al. (2004) genannte Beispiele sind:

- Ein Heizelement für sehr tiefe oder sich schnell ändernde Umgebungstemperaturen.
- Lüfter für hohe Umgebungstemperaturen.
- Ein Schutzdach gegen Sonne und Regen.
- Ein Scheibenwischer, wenn die Beaufschlagung durch Regen nicht mittels entsprechendem Neigungswinkel oder einem Schutzdach verhindert werden kann.

Manipulationsschutz

Auch gegen Manipulationsversuche an der Kamera mit dem Ziel, die Aufzeichnung verwertbarer Bilder zu verhindern, können geeignete Maßnahmen ergriffen werden. Zum Schutz vor Verdrehen der Kamera können nach VdS 2366 (2004) mechanische plombierte Elemente oder eine Software seitige Erkennung und Meldung eingesetzt werden. Ähnlich können auch andere Manipulationsversuche wie Abdecken, Besprühen oder Defokussieren mit einer automatischen Kamerasabotageerkennung detektiert werden, so beschrieben bei ”Videosicherheitsanlage”(2010).

Vandalismusschutz/IK-Schutzklassen

Die IK-Schutzarten nach DIN EN 50102 beschreiben, wie bei „IK-Schutzarten“ (2008) dargestellt, den Schutz elektrischer Betriebsmittel gegen äußere mechanische Beanspruchung in Form von Stößen. Die Einteilung in die zehn verschiedenen Klassen erfolgt dabei, wie in Tabelle 4.19 aufgeführt, anhand der maximal möglichen Schlagenergie.

Tabelle 4.19: Kennziffern für den Schutz vor mechanischer Beanspruchung nach DIN EN 50102.

Kennziffer	Maximale Schlagenergie	Entspricht Schlag mit folgendem Gegenstand
IK 00	Keine Stoßfestigkeit	/
IK 01	0,150 Joule	0,2 Kg aus 5 cm Entfernung
IK 02	0,200 Joule	0,2 Kg aus 8 cm Entfernung
IK 03	0,350 Joule	0,2 Kg aus 14 cm Entfernung
IK 04	0,500 Joule	0,2 Kg aus 20 cm Entfernung
IK 05	0,700 Joule	0,2 Kg aus 28 cm Entfernung
IK 06	1,00 Joule	0,25 Kg aus 40 cm Entfernung
IK 07	2,00 Joule	0,5 Kg aus 40 cm Entfernung
IK 08	5,00 Joule	1,7 Kg aus 30 cm Entfernung
IK 09	10,00 Joule	5,0 Kg aus 20 cm Entfernung
IK 10	20,00 Joule	5,0 Kg aus 40 cm Entfernung

4.10.2 Kompatibilität der Schutztechniken untereinander

Die Nutzung einer Schutztechnik schließt den Einsatz einer oder auch mehrerer weiterer nicht aus, sodass sie untereinander uneingeschränkt kompatibel sind. So lässt sich beispielsweise ein mechanischer Verdrehschutz an einer IP-geschützten Kamera mit Schutzdach und einer automatische Kamerasabotageerkennung kombinieren. Die Ausstattung mit mehreren unterschiedlichen Schutztechniken stellt also kein Problem dar.

Tabelle 4.20: Kompatibilität der Schutztechniken untereinander.

	IP	Techn. Zusatzausst.	Manipulationssch.	IK
IP	+	+	+	+
Techn. Zusatzausst.	+	+	+	+
Manipulationssch.	+	+	+	+
IK	+	+	+	+

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.10.3 Erfüllung der Anforderungen durch die Schutztechniken

Wie bereits in 4.10.1 erläutert, dienen die Schutztechniken als Gegenmaßnahmen zu erschwerenden Einflüssen und Beanspruchungen aus der Umgebung. Ihr Einsatz erhöht daher die Erfüllung der Anforderungen widrige Umgebungsbedingungen oder Schutz vor Vandalismus/Sabotage. In dieser Kategorie sind die einzelnen Elemente und somit auch die vergebenen Punktzahlen entsprechend 4.10.2 nicht als sich gegenseitig ausschließend, sondern als ergänzend und kumulativ anzusehen. Das bedeutet, dass bei Vorhandensein oder Anbringung etwa von einem Heizelement und einem Regenschutzdach die Punkte für beide addiert werden (falls der Einsatz beider Techniken sinnvoll ist).

Eine Ausführung entsprechend einer IP-Schutzart und technische Zusatzausstattung ermöglichen einen Einsatz unter **widrigen Umgebungsbedingungen**. Eine hohe Klassifizierung nach DIN EN 60529 (d.h. ab etwa IP 65 aufwärts) bildet eine gute Grundlage für eine Nutzung in Bereichen mit hohen Anforderungen, etwa im Außenbereich. Dies bietet zwar keinen allumfassenden Schutz gegen jede Art von Umgebungseinfluss, gewährleistet aber eine grundlegende Robustheit und schützt vor zwei der hauptsächlichen Gefahren, dem Eindringen von Wasser/Feuchtigkeit und Staub. Daher erfolgt eine Bewertung mit drei Punkten. Zugrunde gelegt wird bei der Bewertung eine an den Einsatzort angepasst hohe Einstufung, was in jedem

Einzelfall eigenständig überprüft werden muss. Sollte dies nicht der Fall sein, sind entsprechende Punktabzüge vorzunehmen.
Die technischen Zusatzausstattungen sind sehr speziell auf bestimmte Einflüsse wie hohe oder niedrige Temperaturen oder Regen ausgerichtet. Sie decken also jeweils nur einen gewissen Teil aller möglichen Umgebungsfaktoren ab und werden somit mit zwei Punkten bewertet. Zu beachten ist hierbei, dass nur sinnvolle Ausrüstung mit technischer Zusatzausstattung auch diese Bewertung begründet. So sollte beispielsweise das Vorhandensein eines Heizelementes auch nur bei einem Einsatz in entsprechend kalter Umgebung mit zwei Punkten bewertet und ansonsten ignoriert werden.

Zum **Schutz vor Vandalismus/Sabotage** können die vorgestellten Techniken des Manipulations- und des Vandalismusschutzes eingesetzt werden. Beim Manipulationsschutz muss bei der Bewertung zwischen der mechanischen und der Software seitigen Ausführung unterschieden werden. Erstere kann zwar ein Verdrehen in einem gewissen Rahmen verhindern bzw. erschweren, bei höherer krimineller Energie und höherem betriebenem Aufwand seitens der mutmaßlichen Täter und bei anderen Manipulationsarten als dem Verdrehen ist sie jedoch nutzlos und wird folglich mit zwei Punkten bewertet. Eine Software basierte automatische Kamerasabotageerkennung detektiert und meldet hingegen jeden Versuch der Manipulation, sodass zeitnah und angemessen darauf reagiert werden kann. Sie kann Vandalismus zwar nicht verhindern, aber z.B. im Falle der Zerstörung der Kamera/Verlust der Aufnahmefähigkeit zumindest alarmieren. Daher werden hier vier Punkte vergeben.
Eine entsprechend einer IK-Schutzklasse beschaffene Kamera ist, eine dem ermittelten Risiko angemessen hohe Einstufung vorausgesetzt, zuverlässig gegen Beschädigung und Zerstörung durch Gewalt geschützt. Auch werden dadurch viele Manipulationsversuche durch die erschwerte Zugänglichkeit wirksam verhindert. Andere Möglichkeiten wie Besprühen oder Abdecken bleiben dessen ungeachtet weiterhin bestehen, sodass hier eine Bewertung mit drei Punkten erfolgt.

Tabelle 4.21: Erfüllung der Anforderungen durch die Schutztechniken.

	IP	Techn. Zus.-Ausst.	Mech. Verdrehsch.	Sabotageerk.	IK
Identifikation	x	x	x	x	x
Analyse	x	x	x	x	x
Integration	x	x	x	x	x
Sicht	x	x	x	x	x
Umgebung	3	Je 2	x	x	x
Vandalismus	x	x	2	4	3
Verfügbarkeit	x	x	x	x	x
Skalierbarkeit	x	x	x	x	x
Integrität	x	x	x	x	x

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.11 Prüfung/Zertifizierung

4.11.1 Übersicht und Beschreibung der Prüfungen/ Zertifizierungen

Um sichergehen zu können, auch passende und hochwertige Komponenten oder Systeme zu erhalten, ist der Einsatz geprüfter/zertifizierter Komponenten sinnvoll. Auch im Bereich der Videoüberwachung werden einige wenige Prüfungen/Zertifizierungen angeboten. Drei bedeutende Beispiele werden im Folgenden behandelt: Das LGC-Zertifikat, das DGUV Test-Zeichen nach BGV C9 und das Installationsattest nach VdS 3426.

LGC-Zertifikat

Das von dem britischen Unternehmen LGC Forensics, früher Kalagate, vergebene Zertifikat bescheinigt nach Biersack (2010) die Manipulations- und Fälschungssicherheit von Aufzeichnungsgeräten, beispielsweise Digitalrekordern. Die Geräte werden auf Schutz vor Fremdzugriff und Unverfälschtheit der darauf gespeicherten Bilder

geprüft.

DGUV Test-Zeichen

Das DGUV Test-Zeichen wird entsprechend DGUV Test-VW-SG3-1 (2010) von der Prüf- und Zertifizierungsstelle des Fachausschusses Verwaltung ausgestellt. Grundlage ist eine Baumusterprüfung der Komponenten auf Übereinstimmung mit den in BGV C9 und BGI 819-2 genannten und durch DGUV Test-VW-SG3-1 ergänzten und konkretisierten Anforderungen.

Installationsattest VdS 3426

Das in der VdS 3426 (2005) hinterlegte Installationsattest für Videoüberwachungsanlagen bescheinigt die Ausführung eines kompletten Videoüberwachungssystems gemäß den Anforderungen der VdS 2366.

4.11.2 Kompatibilität der Prüfungen/Zertifizierungen untereinander

Das LGC-Zertifikat hat ein grundlegend anderes Anliegen als das DGUV Test-Zeichen und das Installationsattest VdS 3426 und weist daher auch keine direkten inhaltlichen Überschneidungen in den Anforderungen auf. Eine LGC-Zertifizierung steht somit den beiden anderen Bescheinigung nicht entgegen, es herrscht also eine vollständige Kompatibilität ihnen gegenüber.
Zwar enthalten die Zertifizierung nach DGUV Test-Zeichen und das Installationsattest VdS 3426 einige inhaltliche Parallelen und ähnliche Forderungen, dies behindert jedoch nicht die erfolgreiche Zertifizierung nach beiden Prüfverfahren. Einerseits bezieht sich das DGUV Test-Zeichen auf einzelne Komponenten und das Installationsattest auf komplette Systeme, andererseits können bei ähnlichen Forderungen durch Erfüllung der jeweils härteren Vorgaben problemlos beide erfüllt werden. Im

Gegenteil bringt der Einsatz von Komponenten mit dem DGUV Test-Zeichen in einem Videoüberwachungssystem teilweise sogar Erleichterungen und Vorteile bei der Erlangung des Installationsattestes.
Demnach kann eine vollständige Kompatibilität der drei Prüfungen/Zertifizierungen geschlussfolgert werden.

Tabelle 4.22: Kompatibilität der Prüfungen/Zertifizierungen untereinander.

	LGC	DGUV	VdS 3426
LGC	+	+	+
DGUV	+	+	+
VdS 3426	+	+	+

(+) Voll/uneingeschränkt kompatibel

(o) Teilweise/unter bestimmten Voraussetzungen kompatibel

(-) Nicht kompatibel

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

4.11.3 Erfüllung der Anforderungen durch die Prüfungen/ Zertifizierungen

Im Gegensatz zu den meisten anderen Unterscheidungskriterien decken die drei vorgestellten Prüfungen/Zertifizierungen nicht die selben Anforderungen ab und zeigen deutliche Unterschiede. Es wird daher in diesem Kapitel von der bisherigen Vorgehensweise, der Bewertung aller Elemente des Kapitels geordnet nach Anforderungen, abgesehen. Stattdessen werden die Prüfungen/Zertifizierungen jeweils gesondert und direkt im Hinblick auf alle relevanten Anforderungen betrachtet.

Das **LGC-Zertifikat** wirkt sich definitionsgemäß nur auf die Integrität/Überprüfbarkeit/Beweiskraft aus. Nach Biersack (2010) kann damit zwar die Unverfälschtheit des Bildmaterials garantiert werden, aber eben nur zwischen Aufzeichnungsgerät und Polizei/Gericht. Über alle vorherigen Komponenten wie Kamera und Übertragungsweg wird hingegen keine Aussage getroffen, woraus eine Bewertung mit drei

Punkten resultiert.

Das **DGUV Test-Zeichen** bescheinigt hingegen nach DGUV Test-VW-SG3-1 (2010) die Erfüllung mehrerer Anforderungen: Zum einen wird durch die Vorgabe der Farbtauglichkeit aller Komponenten und den Abgleich mit vorgegebenen Prüftafeln ein gewisses Maß an Identifikation/Erkennbarkeit ermöglicht. Die geprüfte Beobachtungsreichweite ist aufgrund des vorgesehenen Einsatzes innerhalb von Geschäftsräumen begrenzt und somit nicht für alle, aber dennoch für einige Überwachungsaufgaben geeignet. Hier werden daher drei Punkte vergeben.
Auch die hohe Verfügbarkeit der Bilddaten wird durch Anforderungen an die Funktionssicherheit, z.B. der Verhinderung des unbeabsichtigten Löschens von Bildmaterial, der Begrenzung des Datenverlustes und der Ausfallzeit des Aufzeichnungsgerätes bei Stromausfällen sowie der Erkennung und Meldung von Störungen in den Kameras in begrenztem Umfang erhöht, sodass hier mit zwei Punkten bewertet wird. Darüber hinaus wird ein konkreter Schutz vor unbefugtem Zugriff auf Programme und Funktionen des Videoüberwachungssystems und eine mindestens sekundengenaue Zuordnung von Datum und Uhrzeit zu jedem Bild gefordert. Hierdurch kann der Schutz vor Vandalismus/Sabotage und die Integrität/Überprüfbarkeit/-Beweiskraft ebenfalls in geringem Maße gesteigert werden. Für die Erfüllung dieser beiden Anforderungen wird je ein zusätzlicher Punkt vergeben.

Das **Installationsattest VdS 3426** bezieht sich explizit auf die Zertifizierung eines kompletten bereits fertig gestellten Videoüberwachungssystems und seiner Funktionalität im Gesamten. Demzufolge können keine allgemein gültigen Aussagen über einzelne Komponenten, verwendete Verfahren und Technologien getroffen werden. Zudem bescheinigt das Attest auch keinen einheitlich hohen Standard, sondern kann in mehreren Abstufungen vergeben werden. Die Bewertung von Anforderungen durch das Installationsattest als Auswahlkriterium für Komponenten von Videoüberwachungssystemen ist daher nicht sinnvoll.

Tabelle 4.23: Erfüllung der Anforderungen durch die Prüfungen/Zertifizierungen.

	LGC	DGUV	VdS 3426
Identifikation	x	3	x
Analyse	x	x	x
Integration	x	x	x
Sicht	x	x	x
Umgebung	x	x	x
Vandalismus	x	1	x
Verfügbarkeit	x	2	x
Skalierbarkeit	x	x	x
Integrität	3	1	x

Von 0: Erüllt die Anforderung garnicht

bis 5: Erüllt die Anforderung optimal

(x) Keine Aussage möglich, Zuordnung nicht sinnvoll

5 Anwendungsbeispiele

Im Folgenden werden die beiden Möglichkeiten der praktischen Anwendung des vorliegenden Buchs anhand von fiktiven Beispielen dargestellt.
Im ersten Beispiel soll eine Videoüberwachungsanlage für eine bestimmte Überwachungsaufgabe neu geplant und zusammengestellt werden, wobei zwei unterschiedliche Systeme zur Auswahl stehen. Diese werden anhand der zuvor ermittelten Anforderungen bewertet und verglichen.
Im zweiten Beispiel wird eine bereits bestehende Videoüberwachungsanlage aufgrund einer neu hinzugekommenen Anforderung auf seine Eignung überprüft und darauf aufbauend Verbesserungsmöglichkeiten erarbeitet.

5.1 Beispiel 1: Planung eines neuen Videoüberwachungssystems

In diesem Beispiel liegt folgende Situation vor: Ein Werk eines Industrieunternehmens soll mit einem Videoüberwachungssystem zur Absicherung der Geländegrenzen im Außenbereich ausgestattet werden. Der Hauptgrund hierfür ist die Entlastung des Werkschutzes und die Einsparung von Wachpersonal. Die Videoüberwachungsanlage soll die Überwachung eines großen räumlichen Bereichs mit möglichst wenigen Mitarbeitern ermöglichen. Hierzu sollen mögliche sicherheitsrelevante Ereignisse automatisch erkannt und gemeldet werden. Eine genaue Identifikation von Personen ist hierbei nicht primär erforderlich. Die hauptsächliche Aufgabe besteht in der

Beobachtung und Beurteilung von Vorgängen und bei Bedarf der Alarmierung des Werkschutzes. Das System soll rund um die Uhr im Einsatz sein und die Möglichkeit bieten, in Zukunft einfach erweitert oder aufgerüstet zu werden.
Mittels der zugrunde liegenden Situation und der vorgegebenen Zielsetzung werden die folgenden Anforderungen ausgewählt:

- Analyse/Auswertung/Intelligenz [x 2] (Hauptaufgabe, daher höhere Priorität und Verdoppelung der Punkte)
- Identifikation/Erkennbarkeit (hinreichende Beurteilung von Vorgängen auf Sicherheitsrelevanz notwendig)
- Schwierige Sichtverhältnisse (Einsatz auch in der Nacht bei geringerer Beleuchtung)
- Widrige Umgebungsbedingungen (Einsatz im Außenbereich)
- Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit (zukunftssichere Investition)

Zur Auswahl stehen ein analoges System, wie es noch häufig vorzufinden ist, sowie ein modernes digitales System. Die genauen Spezifikationen sind in Tabelle 5.1 aufgeführt.

Tabelle 5.1: In Beispiel 1 zur Auswahl stehende Systeme.

	System A	System B
Technologie	Analog	Digital
Bildgebungsverfahren	Schwarz/Weiß	Farbe
Bild-Sensor	CCD	CMOS
Kompression	Keine (analog)	H.264
Übertragung	Koaxialkabel	LAN
Aufzeichnung	DVR	NAS
Protokolle	Pelco-D	ONVIF
Stromversorgung	230 V	Power over Ethernet
Schutz vor Einfl. a. d. Umgebung	Regenschutzdach	IP 67, Scheibenwischer
Zertifizierung	LGC-Zertifikat	DGUV Test-Zeichen

Für **System A** ergeben sich hinsichtlich der Erfüllung der gestellten Anforderungen folgende Punktbewertungen:

- Analyse/Auswertung/Intelligenz: 1 (Analog) = **1**
- Identifikation/Erkennbarkeit: 3 (Schwarz/Weiß) + 5(CCD) = **8**
- Schwierige Sichtverhältnisse: 2 (Schwarz/Weiß) + 3 (CCD) = **5**
- Widrige Umgebungsbedingungen: 5 (Koaxialkabel) + 2 (Regenschutzdach) = **7**
- Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit: 5 (Analog) + 2 (Koaxialkabel) + 4 (DVR) + 2 (Pelco-D) + 1 (230 V) = **14**
- **Gesamt: 2x1 + 8 + 5 + 7 + 14 = 36**

Für **System B** ergeben sich hinsichtlich der Erfüllung der gestellten Anforderungen folgende Punktbewertungen:

- Analyse/Auswertung/Intelligenz: 5 (Digital) = **5**
- Identifikation/Erkennbarkeit: 5 (Farbe) + 4 (CMOS) + 3 (H.264) + 3 (DGUV) = **15**
- Schwierige Sichtverhältnisse: 1 (Farbe) + 3 (CMOS) = **4**
- Widrige Umgebungsbedingungen: 5 (LAN) + 3 (IP 67) + 2 (Scheibenwischer) = **10**
- Skalierbarkeit/Erweiterbarkeit/Aufrüstbarkeit: 3 (Digital) + 3 (LAN) + 5 (NAS) + 5 (ONVIF) + 3 (PoE) = **19**
- **Gesamt: 2x5 + 15 + 4 + 10 + 19 = 58**

Es ergibt sich eine deutlich bessere Eignung von System B (58 Punkte) gegenüber System A (36 Punkte) für die gewünschte Zielsetzung unter den gegebenen Voraussetzungen. Die reine Zusammensetzung der Komponenten sagt jedoch noch nichts über die tatsächliche Funktionalität aus. Hier sind noch eine Reihe weiterer Faktoren zu beachten, wie die ordnungsgemäße Installation, eine ausreichende Beleuchtung in der Nacht, die Nutzung einer leistungsfähigen Videomanagement-Software und die

Schaffung eines geeigneten Überwachungsplatzes für die Werkschutzmitarbeiter.

5.2 Beispiel 2: Bewertung/Aufrüstung eines bestehenden Videoüberwachungssystems

In diesem Beispiel ist bereits ein komplettes Videoüberwachungssystem in einem Museum vorhanden. Es kam zu einem Diebstahl wertvoller Exponate. Der mutmaßliche Täter wurde beim Betreten des Gebäudes von einer Überwachungskamera erfasst. Das Gericht erkannte das Bildmaterial jedoch nicht als Beweis an, sodass es aufgrund mangelnder weiterer Beweise zu keiner Verurteilung kam. Nun soll das im Eingangsbereich installierte System auf seine Eignung hinsichtlich der Anforderung Integrität/Überprüfbarkeit/Beweiskraft untersucht und verbessert werden. Die Videoüberwachungsanlage ist wie in Tabelle 5.2 aufgebaut.

Tabelle 5.2: Das vorhandene System in Beispiel 2.

Technologie	Digital
Bildgebungsverfahren	Farbe
Bild-Sensor	CCD
Kompression	MPEG-4
Übertragung	LAN
Aufzeichnung	DVR
Protokolle	Keine
Stromversorgung	Power over Ethernet
Schutz vor Einflüssen aus der Umgebung	IK 10
Zertifizierung	DGUV Test-Zeichen

Der bisherige Punktewert für die Anforderung Integrität/Überprüfbarkeit/Beweiskraft setzt sich wie folgt zusammen: 1 (Digital) + 0 (MPEG-4) + 4 (LAN) + 0 (DVR) + 1 (DGUV) = **6 (Gesamt)**.
Um die Erfüllung der Anforderung zu erhöhen, können prinzipiell eine oder mehrere der folgenden Veränderungen vorgenommen werden (In Klammern dahinter ist jeweils die Erhöhung des Punktwerts durch die Veränderung angegeben):

- Umstellung auf ein komplett analoges System, zumindest im Eingangsbereich (+4)
- Umstellung des Kompressionsverfahrens auf MPEG-2 / H.262 (+3)
- Übertragung über Zweidraht-Verbindung, Koaxialkabel oder Lichtwellenleiter (+1)
- Speicherung der Daten auf DVD oder Ausdruck eines Standbildes (+5)
- Einsatz eines LGC-zertifizierten Aufzeichnungssystems (+2)

Es gilt zunächst natürlich noch abzuwägen, welche der genannten Veränderungen in diesem Fall sinnvoll und auch wirtschaftlich tragbar sind. So könnte die zusätzliche Speicherung der Daten auf DVD oder einem LGC-zertifizierten Aufzeichnungssystem und die Umstellung des Kompressionsverfahrens bereits eine deutliche Erhöhung bei mäßigem Aufwand ermöglichen, während hingegen der komplette Umstieg auf Analogtechnologie oder ein anderes Übertragungsverfahren unverhältnismäßig erscheint.

6 Zusammenfassung, Ergebnis und Schlussbemerkungen

Wie deutlich wurde, kann für jede denkbare Überwachungsaufgabe unter verschiedensten Bedingungen auch eine geeignete Lösung gefunden werden. Es können jedoch nicht wahllos beliebige Komponenten miteinander kombiniert werden. Und nicht jedes System ist für jede Überwachungsaufgabe gleichermaßen gut einsetzbar. Vielmehr bedarf es zunächst einer umfassenden Analyse der zu erreichenden Ziele und der vorherrschenden Bedingungen, auf dessen Grundlage dann das entsprechende Videoüberwachungssystem fachgerecht geplant, zusammengestellt, installiert und betrieben werden kann.

Wie bereits mehrfach erwähnt, sind in diesem Buch bei weitem nicht alle möglichen Anforderungen und Unterscheidungskriterien enthalten. Eine abschließende Erfassung und Aufzählung ist jedoch auch nicht das Ziel. Das Hauptaugenmerk liegt auf der Bewertungs-Systematik und der Darstellung der aktuell gängigsten Standards, Normen, Verfahren und Technologien im Vergleich. Das Punktesystem ist auch nicht als starr anzusehen, sondern kann und soll explizit im Bedarfsfall verändert und erweitert werden. So können etwa die Anforderungen wie in Beispiel 1 gewichtet/priorisiert werden, je nach Zielsetzung auch mit einem höheren Faktor als zwei. Nicht in diesem Buch enthaltende Unterscheidungskriterien und Elemente können hinzugefügt und entsprechend des Schemas eigenständig bewertet werden. Gerade bei der Punktebewertung gilt es, die hier angegebenen Richtwerte auf die Eignung im jeweiligen Anwendungsfall hin zu überprüfen und gegebenenfalls Anpas-

sungen vorzunehmen. Auch die Errechnung der Gesamtpunktzahl sollte logisch hinterfragt werden. So können beispielsweise die Punktzahlen beim parallelen Einsatz mehrerer Speichermedien hinsichtlich der hohen Verfügbarkeit ohne weiteres addiert werden, während dies beim gleichzeitigen Einsatz von Wärmebild- und Farbkameras in Bezug auf schwierige Sichtverhältnisse nicht sinnvoll ist und hier stattdessen, abhängig von den Randbedingungen, entweder der niedrigere oder der höhere Wert herangezogen werden sollte.

In Zukunft wird die Videoüberwachung voraussichtlich immer stärker von Digitalisierung und Vernetzung geprägt sein. Videoüberwachungsanlagen und andere Systeme wie die Brandmeldeanlage, Zutrittskontrolle, Zeiterfassung und Gebäudetechnik werden über kurz oder lang einheitlich auf Netzwerktechnologie basieren und als großes integriertes System zusammenarbeiten, wofür Initiativen wie ONVIF bereits jetzt die Grundsteine legen und dadurch zukünftig noch mehr an Bedeutung gewinnen werden. Bei allen sich eröffnenden interessanten Möglichkeiten und Technologien muss jedoch auch die Verhältnismäßigkeit gewahrt bleiben. So schreibt Weinzierl (2008, S. 53):

> *„Die Technologie eröffnet zwar viele neue Möglichkeiten der Vorbeugung und Aufklärung von Verbrechen, aber wie verantwortungsbewusst damit umzugehen ist, bestimmen letztendlich vor allem die rechtlichen Rahmenbedingungen.“*

Literatur- und Quellenverzeichnis

Beisel, W., Ebert, F., Foerster, W., Otto, F., Pfeiffer, W. & Wieand, H. (2004). *Lehrbuch für den Werkschutz und private Sicherheitsdienste.* Stuttgart; München; Hannover; Berlin; Weimar; Dresden: Richard Boorberg Verlag.

Bemmel, R. v. (2010). CCTV: Technologielücken schließen. *GIT Sicherheit + Management*, Oktober 2010, S. 110.

BGI 819-2 (2008). *Kredit- und Finanzdientsleistungsinstitute - Anforderungen an die sicherheitstechnische Ausrüstung von Geschäftsstellen i.V.m. §§ 5 und 6 Arbeitsschutzgesetz.* Berlin: Deutsche Gesetzliche Unfallversicherung.

BHE CCTV 1.1 (2007). *Video-(CCTV) Überwachungstechnik: Videosignalübertragung.* Brücken: Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen e.V.

Biersack, A. (2010). Unverfälschte Beweiskraft - Gerichtsverwertbarkeit von Videobildern. *Protector Special Videoüberwachung*, 2010, S. 50f.

Bodell, P. (2010). Ein Computer mit Objektiv - Was intelligente Smart-Kameras so alles drauf haben. *GIT Sicherheit + Management*, Oktober 2010, S. 114.

Brauner, D. J., Raible-Besten, R. & Weigert, M. M. (1998). *Multimedia-Lexikon.* München: R. Oldenbourg Verlag.

Dey, W. (2006). Das digitale Elefantengedächtnis. *KMU-Magazin*, Nr. 9, November 2006, S. 80 - 83.

DGUV Test-VW-SG3-1 (2010). *Anforderungen an Komponenten von optischen Raumüberwachungsanlagen für das DGUV Test-Zeichen UVV Kassen.* Hamburg: Prüf- und Zertifizierungsstelle der Deutschen Gesetzlichen Unfallversicherung, Fachausschuss Verwaltung.

„DVR“. (02. Februar 2010). DVR (digital video recorder). *ITWissen.* Zugriff am 06.01.2011 unter http://www.itwissen.info/definition/lexikon/DVR-digital-video-recorder.html

„Einbrüche“ (17. Juli 2009). *Zahlen und Fakten – Einbrüche und Einbruchschutz in*

Deutschland. Berlin: Initiative für aktiven Einbruchschutz „Nicht bei mir!“.

Ekerot, M. (2008). Analog rein, digital raus - Video-Encoder überbrücken Formatkluft und schützen Investitionen. *GIT Sicherheit + Management*, Oktober 2008, S. 79 - 81.

Fourmont, K. (2009). Der Sprung ins digitale Zeitalter. *Sicherheit & Industrie Select Videoüberwachung*, 2009, S. 26 - 29.

Gilke, S. (2008). Fernerkundung: Neue Möglichkeiten funkbasierter Videoüberwachung. *Sicherheit & Industrie Kompendium*, 2008, S. 268 - 270.

Graf-Jahnke, M. (23. März 2004). Richtfunk. *IT-Portal.* Zugriff am 05.01.2011 unter http://www.it-portal.org/netzwerk/richtfunk/richtfunk.html#2

Hilpert, T. (2009). Videoüberwachung für den Außenbereich - Hohe Bildqualität rund um Uhr und bei jedem Wetter. *GIT Sicherheit + Management*, Oktober 2009, S. 44f.

„IK-Schutzarten“ (10. August 2008). Technische Informationen: IK-Schutzarten. *GETT Gerätetechnik.* Zugriff am 19.01.2011 unter http://www.gett.de/content/infodownload/technical_info/ikprotection.html

ITU-T Recommendation H.261 (1994). *VIDEO CODEC FOR AUDIOVISUAL SERVICES AT p x 64 kbits.* Genf: International Telecommunication Union, Telecommunication Standardization Sector.

Klitsch, M. (2010). Die Schnittstellenfrage - Anbindung von Videosystemen. *GIT Sicherheit + Management*, September 2010, S. 53.

Korkin, M. (2009). Rechenleistung und Kosten für H.264-Komprimierung - Dichtung und Wahrheit. *Protector*, Juni 2009, S. 28f.

Kraheck, A., Beisel, W. G., Ehses, H., Feuerlein, H., Hirschmann, H.-P., Milkowski, G., Pfeiffer, W., Sailer, B., Sigesmund, M. & Trauboth, J. (2004). *Unternehmensschutz Praxishandbuch. - Teil D4: Video-Überwachungstechnik* Stuttgart; München; Hannover; Berlin; Weimar; Dresden: Richard Boorberg Verlag.

Kräußlich, W. (2008a). Der Markt stabilisiert sich - Video und Alarm: Branchentrends

und neue Produkte auf der Security 2008. *Sicherheit & Industrie*, Oktober 2008, S. 71 - 76.

Kräußlich, W. (2008b). Integrierte Sicherheitstechnik - Zutrittskontrolle, Sicherheitstechnik und Zeitwirtschaft wachsen zusammen. *Sicherheit & Industrie*, Oktober 2008, S. 14 - 17.

Kräußlich, W. (2009a). Auf den Chip kommt es an - Aufnahmetechnik digitaler Videokameras - ein Überblick. *Sicherheit & Industrie Select Videoüberwachung*, 2009, S. 21 - 23.

Kräußlich, W. (2009b). Daten unter Druck - Gängige Kompressionsverfahren für Videos im Überblick. *Sicherheit & Industrie Select Videoüberwachung*, 2009, S. 23f.

Kühlewind, U. (2009). IP-Kameratechnik für alle. *GIT Sicherheit + Management*, November 2009, S. 54f.

Lahr, C. (2010). Casinos: Zwölf Tipps für die Beschaffer von Sicherheitstechnik. *GIT Sicherheit + Management*, Mai 2010, S. 44f.

Landolt, C. (17. November 2010). Hirslanden-Notfall wird mit Attrappe bewacht. *Basler Zeitung online.* Zugriff am 20.01.2011 unter http://bazonline.ch/zuerich/stadtzuerich/HirslandenNotfall-wird-mit-Attrappe-bewacht/story/29344076

Maras, C. (2007). Nachtflugtauglich - Flughafen Kopenhagen installiert Wärmebildkameras. *Sicherheit & Industrie*, September 2007, S. 62f.

Merz, C. (2008). *Monetäre Bewertung der Netzzuverlässigkeit für eine effiziente Qualitätsanreizregulierung.* [Working Paper]. Energiewirtschaftliches Institut an der Universität zu Köln.

„NAS“. (27. September 2007). NAS (network attached storage). textitITWissen. Zugriff am 07.01.2011 unter http://www.itwissen.info/definition/lexikon/network-attached-storage-NAS.html

Niecke, M. (2009a). Videoüberwachung richtig planen - In elf Schritten zum fertigen Videoüberwachungssystem. *Sicherheit & Industrie Select Videoüberwachung*, 2009, S. 16 - 19.

Niecke, M. (2009b). Von Kamera bis Digitalrekorder - Die Möglichkeiten eines Videoüberwachungssystems. *GIT Sicherheit + Management*, November 2009, S. 50 - 52.

Niehus, M. (2008). Alles im Griff - Modernes Videomanagementsystem für Infraserv Höchst. *Sicherheit & Industrie*, September 2008, S. 55 - 57.

„NVR". (10. April 2010). NVR (network video recorder). *ITWissen.* Zugriff am 06.01.2011 unter http://www.itwissen.info/definition/lexikon/NVR-network-video-recorder-Netzwerkvideorecorder.html

„ONVIF" (2010). ONVIF: Der Standard? *VIEW*, Januar 2010, Zugriff am 09.01.2011 unter http://www.videor.com/cms/1/0/0/0/VIEW0110-ONVIF-Standardisierte-Schnittstelle-Netzwerk-Videoprodukte-01.html?DOCID=2794&setlanguage=de

„Pelco-D". (2009). Begriffserklärung: Pelco-D. *Silent-Secure.* Zugriff am 09.01.2011 unter http://www.silent-secure.de/content/Begriffserkl%C3%A4rung.html

Poynton, C. (2003). *Digital Video and HDTV - Algorithms and Interfaces.* San Francisco: Morgan Kaufmann Publishers.

Rech, J. (2008). *Ethernet - Technologien und Protokolle für die Computervernetzung.* Hannover: Heise Zeitschriften Verlag.

Rech, J. (2010). HDTV für bessere Bilder - Hochauflösende Bilder in der Videoüberwachung. *Sicherheit & Industrie Kompendium 2010*, S. 175f.

Robbe, B. (2001). *SAN - Storage Area Network.* München, Wien: Carl Hanser Verlag.

Schnabel, P. (1997 - 2010). Lichtwellenleiter (LWL/Glasfaser). *Elektronik-Kompendium.* Zugriff am 22.12.2010 unter http://www.elektronik-kompendium.de/sites/kom/0301282.htm

Schneider, J. (2010). Integrierte Sicherheit spart Geld - Integration von Subsystemen verschiedener Hersteller mit systemübergreifenden Funktionen. *Sicherheit & Industrie Kompendium 2010*, S. 158 - 160.

Schnitzler, B. (27. Oktober 2006). Flachbildschirm gegen Röhrenmonitor: Das letzte Gefecht. *Netzwelt.* Zugriff am 09.12.2010 unter http://www.netzwelt.de/news/

74730_2-flachbildschirm-gegen-roehrenmonitor-letzte-gefecht.html

„Schutzarten“ (11. Juli 2008). IP Schutzarten. *Elektronik-Magazin.de.* Zugriff am 16.01.2011 unter http://www.elektronik-magazin.de/page/ip-schutzklassen-25

Stiewe, C. (2010). Digitale Videoüberwachung: Auch drahtlos sicher zu managen. *WIK*, Oktober 2010, S. 118f.

Strutz, T. (2005). *Bilddatenkompression.* Wiesbaden: Vieweg & Sohn Verlag / GWV Fachverlage.

Troppens, U., Erkens, R. & Müller, W. (2008). *Speichernetze.* Heidelberg: dpunkt.verlag GmbH.

VdS 2366 (Mai 2004). *VdS-Richtlinien für Videoüberwachungsanlagen - Planung und Einbau.* Köln: VdS Schadenverhütung GmbH.

VdS 3426 (September 2005). *Installationsattest für eine Videoüberwachungsanlage (VÜA).* Köln: VdS Schadenverhütung GmbH.

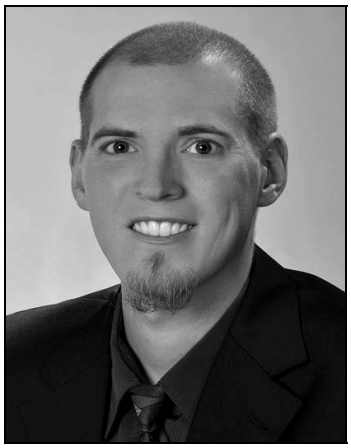
„Videosicherheitsanlage“ (30. März 2010). Hochmoderne Videosicherheitsanlage sichert Bank. *GIT Sicherheit Online Archiv.* Zugriff am 16.01.2011 unter http://www.git-sicherheit.de/topstories/security/hochmoderne-videosicherheitsanlage-sichert-bank

Völckers, B. & Liebelt, L. (2008). Feine Unterschiede - Gekühlte und ungekühlte Kameras für Überwachungen mit großer Reichweite. *Sicherheit & Industrie*, November 2008, S. 54 - 56.

Weinzierl, P. (2008). Videoüberwachung - Zwischen Prävention und Aufklärung. *Sicherheit & Industrie*, November 2008, S. 52f.

Wittmann, N. (2009). Digitale Videotechnik im Fokus. *Sicherheit & Industrie Select Videoüberwachung*, 2009, S. 8 - 10.

Wölpert, R. & Baganz, A. (2008). Sicher ist besser - Verfügbarkeit von Systemen und Daten als Grundvoraussetzung für Business Continuity. *Sicherheit & Industrie Kompendium 2008*, S. 173 - 175.



Der Autor:

Sebastian Welzbacher wurde 1986 in Aschaffenburg am Main geboren. Nach dem erfolgreichen Abschluss des Studiengangs Security & Safety Engineering (B.Sc.) an der Hochschule Furtwangen im Jahre 2011 nahm er zur weiteren Spezialisierung und Vertiefung der erworbenen Kenntnisse ein Master-Studium (Security Management) an der Hochschule für Wirtschaft und Recht in Berlin auf. Während des Studiums sammelte er bereits einige praktische Erfahrungen in verschiedenen Bereichen der Sicherheit, u.a. durch Praktika und Projekte in den Sicherheitsabteilungen bekannter Unternehmen und die Tätigkeit bei einem Sicherheitsdienstleister. Durch die Inhalte unterschiedlicher Vorlesungen, Zusatzausbildungen und praktischen Tätigkeiten kam er immer wieder mit dem Themenbereich der Sicherheitstechnik im Allgemeinen und der Videoüberwachung im Speziellen in Berührung, was auch zur Schaffung des vorliegenden Werkes führte.