Thomas Noack, Dipl.-Ing. (FH), Rücker + Schindele Beratende Ingenieure GmbH, Berlin (D)
Walter Jäger, Autobahndirektion Nordbayern, Nürnberg (D)

Digitale Videotechnik zur Überwachung von Straßentunneln: Datenschutz und IT-Sicherheit, zukünftige Entwicklungen

Zur Überwachung von Straßentunneln wurden bisher analoge Videokameras eingesetzt. Die von der Kamera aufgenommenen Video-Streams mussten mehrfach analog/digital umgewandelt werden, um sie zu Tunnelleitzentralen übertragen und auswerten zu können. Dabei gab es erhebliche Qualitätsverluste. Mit Einzug von IP-Kameras ist vieles einfacher geworden; diverse Punkte sind jedoch zu beachten. Mit der Weiterentwicklung der Videotechnik und den daraus resultierenden hochauflösenden Videobildern geht eine verbesserte Erkennbarkeit von Objekten und Personen einher. Trotz hoher Auflösung müssen die Anforderungen des Datenschutzes erfüllt werden. Darüber hinaus muss das IT-Sicherheitsgesetz, das zum Schutz kritischer Infrastrukturen – wozu auch Tunnel gehören – eingeführt wurde, bei der Konzeption von Videosystemen beachtet werden. Ein Ausblick auf zukünftig nutzbare Technologien lenkt den Blick auf die nächste Generation der Videotechnik und die damit einhergehenden Herausforderungen.

1 Einleitung

Videotechnik spielt eine immer größere Rolle bei der Überwachung von Prozessen und beim Management von unvorhergesehenen Ereignissen oder Störfällen (Bild 1). Dabei ersetzt diese Technik zunehmend den Faktor Mensch, durch das automatisierte Erkennen von Standardsituationen und daraus abgeleitete Reaktionen. Auch zur Überwachung des Tunnelraums von Straßentunneln werden gemäß den Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT) spätestens ab einer Länge von 400 m Kameras eingesetzt. Um die eintönigen Überwachungsprozesse zu automatisieren, werden zunehmend softwarebasierte Bildauswertungen verwendet, die Störungen, z. B. Falschfahrer oder stehende Fahrzeuge, erkennen.

2 Übergang von der analogen zur digitalen Videotechnik

In der analogen Videowelt hatten verschiedene Anbieter diverse proprietäre Standards entwickelt, die zunehmend an ihre Grenzen stoßen. Dies betrifft zum einen physikalische Grenzen, die aufgrund der großen Länge von Straßentunneln erreicht werden, zum anderen die fehlende Kompatibilität der verschiedenen Herstellerstandards.

Digital Video Technology for the Surveillance of Road Tunnels: Data Protection and IT Security, Future Developments

Until now, analog video cameras have been used for the surveillance of road tunnels. The video streams recorded by the cameras have to be analog/digital converted many times in order to be able to transmit them to the tunnel control centre for evaluation, resulting in a considerable loss of quality. With the introduction of IP cameras, this has become much simpler although various points have to be noted. The continued development of video technology and the resulting high-resolution images is associated with better ability to recognise objects and people. In addition, the data safety law, which has been introduced for the protection of critical infrastructure including tunnels, has to be observed in the design of video systems. An outlook to the technology that will be available in the future switches attention to the next generation of video technology and the associated challenges.

Für die Übertragung der Video-Streams zur entfernten Kreuzschiene, die sich meistens im Betriebsgebäude bzw. der Betriebsstation befindet, musste eine mehrfache Wandlung (analog – digital – analog) erfolgen, womit erhebliche Qualitätsverluste der Bildinformationen verbunden sind. Weiterhin war es ohne Konvertierungsaufwand nicht möglich, digitalisierte Streams von einem Kamerahersteller auf die Videokreuzschiene eines anderen Herstellers aufzuschalten. Bei der zeitlich versetzten Fertigstellung von mehreren Tunneln war man daher auf die im ersten der errichteten Tunnelbauwerke ausgewählten Fabrikate und Typen angewiesen, wenn nicht weitere Encoder/Decoder und damit weitere Schnittstellen integriert werden sollten.

Mit Einsatz von IP-Technik werden die beschriebenen Nachteile der analogen Videokameras weitgehend beseitigt.

3 Digitale Videotechnik im Straßentunnel „State of the Art"

IP-Kameras für den Industriebereich unterscheiden sich in der Qualität kaum noch von analogen Kameras. Inzwischen sind früher vorhandene Nachteile, die Anwahlzeiten, Lichtempfindlich-

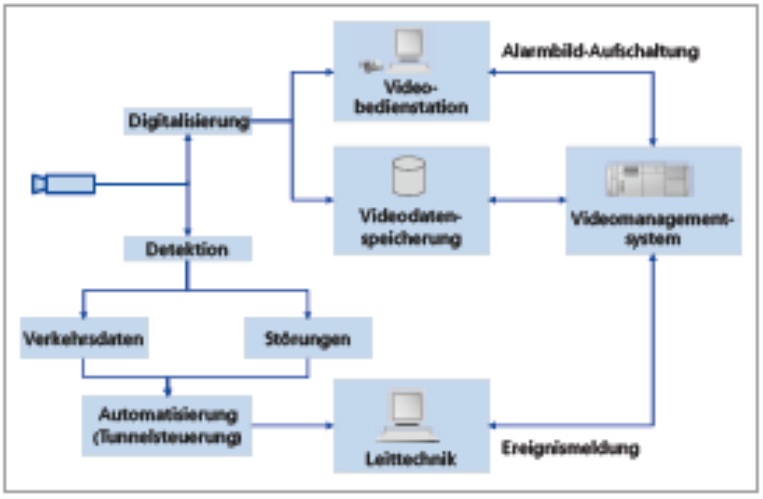

Bild 1 Grundsätzlicher Aufbau von Videosystemen in Straßentunneln

keit, Gegenlichtkompensation und Dynamikverhalten (Wide Dynamic Range – WDR) betroffen haben, kaum noch messbar.

Die Vorteile der IP-Videotechnik liegen auf der Hand:

- Der Zugriff auf jeden beliebigen Video-Stream ist jederzeit und überall möglich, wenn das zugehörige IP-Netzwerk erreichbar ist (Notfallkonzept).
- Die hohe Auflösung, derzeit in HD-Technologie (1.920 × 1.080 Pixel).
- Die Möglichkeit der Fernkonfiguration über die bestehende Verkabelung.
- Die Möglichkeit, die Funktionsfähigkeit der Kamera jederzeit und von überall im Netzwerk zu überprüfen (alive bit).
- Die Einsatzmöglichkeiten von Power over Ethernet (PoE), lediglich mit der Einschränkung, dass die Heizleistung der Frostsicherung gewisse Grenzen nicht überschreiten darf.
- Ein sehr viel geringerer Verkabelungsaufwand, insbesondere beim Einsatz von Ringstrukturen und eines Customer Edge Switches (CE).

In der Übertragung kann auf bewährte Technik aus dem Office- bzw. dem Telekommunikationsbereich zurückgegriffen werden. Es wird Switch-Technologie mit Transmission Control Protocol (TCP) bzw. User Datagram Protocol (UDP) eingesetzt. Die Verkabelung erfolgt über die sogenannte strukturierte Verkabelung oder direkt über Lichtwellenleiter.

Damit wird der Transfer zu Videomanagementsystemen, Beobachtungsgeräten, Speichereinheiten und Videodetektion über die sogenannte digitale Kreuzschiene wesentlich vereinfacht. Ein weiterer Vorteil ist die Verwendung von offenen Bildformaten, die unabhängig von spezieller Hardware, Betriebssystemen oder Lizenzierung zur Übertragung der Bildinformationen zwischen Quelle und Senke genutzt werden können. Dazu zählen vor allem das Real Time Streaming Protocol (RTSP) oder das Open Network Video Interface Forum (ONVIF) [1].

IP-Videotechnologie reduziert die Abhängigkeit zu bestehenden Lieferanten aus den genannten Gründen erheblich.

Dennoch sind auch in der IP-Videotechnik Punkte zu beachten, die bisher keine Rolle gespielt haben. Mit der Analogtechnik wurden die Streams jeweils am Ausgang einer lokalen Videokreuzschiene bereitgestellt (Bild 2) und dieser Kanal permanent bis zum Videowandrechner in der Überwachungsstelle übertragen. Damit kam es bei zyklischen Bildwechseln zwischen verschiedenen Video-Streams zu keinen sichtbaren Unterbrechungen.

Mit der IP-Technologie werden die Kameras in der Überwachungsstelle direkt vom Videomanagementsystem über die IP-

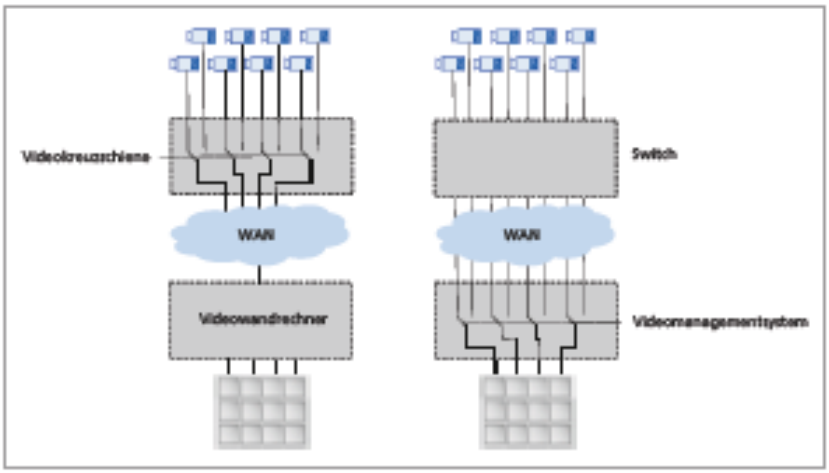

Bild 2 Unterschiedliche Ansteuerung der Streams im analogen und digitalen Videosystem

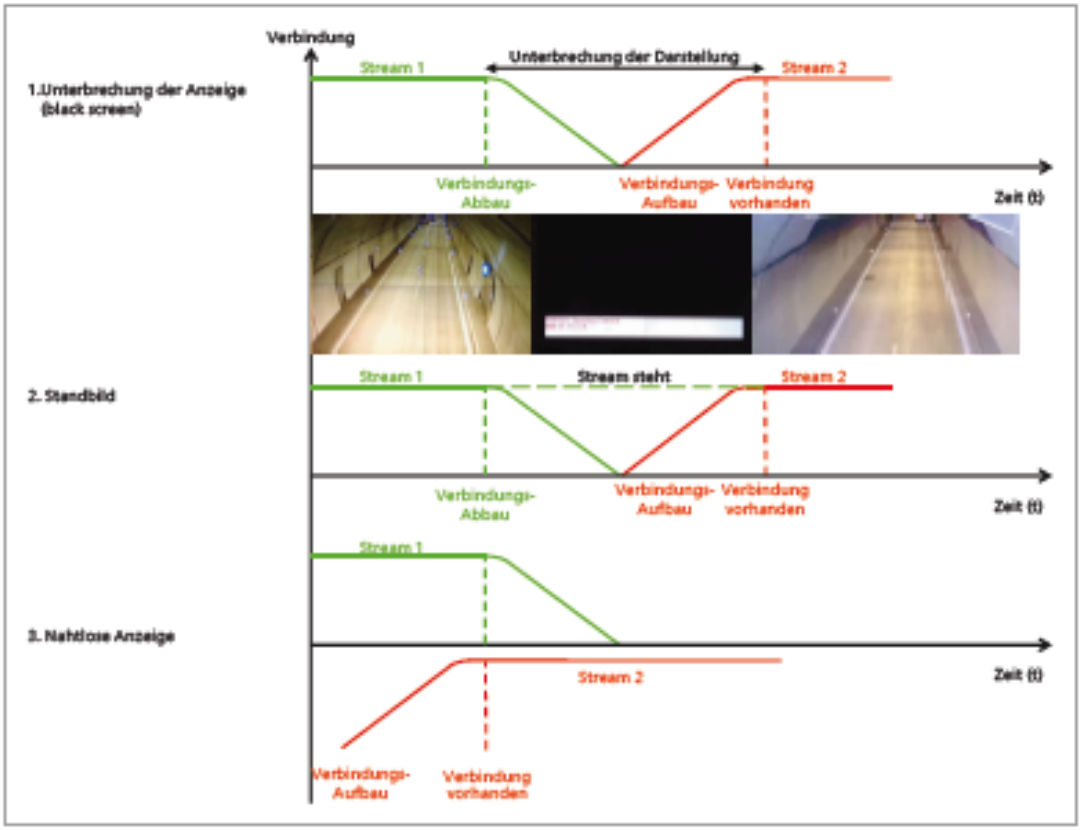

Bild 3 Verbindung des Videomanagementsystems zur Kamera

Adresse angewählt. Der Nachteil besteht darin, dass der Verbindungsweg über das WAN (Wide Area Network) bis zur Videokamera zuerst aufgebaut werden muss, bevor die Inhalte des Video-Streams übertragen werden können (Bild 3). In diesem Zeitraum hat der Operator vor dem Bildschirm keine Bildinformation, d. h., der Bildschirm bleibt schwarz. Bei einem zyklischen Wechsel der Kameras, z. B. Durchlauf der Überwachung in einer Tunnelröhre vom Einfahrts- bis zum Ausfahrtsportal, muss die Übertragungstechnik den Übertragungsweg von Kamera n abbauen und von Kamera n + 1 aufbauen. Dadurch ist die Unterbrechungszeit doppelt so groß. Um die Bildunterbrechungen für den Operator zu vermeiden, gibt es folgende Möglichkeiten:

- Möglichkeit 1, Standbild: Der Stream von Kamera n wird eingefroren, das letzte Bild im Speicher geladen und dem Operator angezeigt, bis der Stream von Kamera n + 1 anliegt und dem Operator angezeigt werden kann. Diese Möglichkeit ist allerdings für den fließenden Verkehr wenig geeignet, da kurzzeitig der Eindruck entsteht, dass der Verkehr steht.
- Möglichkeit 2, gleichzeitiger Aufbau von zwei Streams: Im zweiten Fall wird vor dem Verbindungsabbau von Stream 1 parallel der Stream 2 aufgebaut. Erst wenn die Verbindung zu Kamera n + 1 aufgebaut ist und der Stream 2 angezeigt werden kann, wird die Verbindung zu Kamera n abgebaut. Bei dieser Variante muss das Übertragungssystem so ausgelegt sein, dass es für diese Übergangszeit zwei Streams verarbeiten kann. Dies gilt sowohl für die Übertragungsstrecke (erforderliche Bandbreite) als auch für die Leistungsfähigkeit des Videomanagementsystems.

4 Datenschutz

Mit den Möglichkeiten zur Beobachtung des Verkehrs im Straßentunnel über hochauflösende IP-Videokameras stehen die Überwachungsstellen im Spannungsfeld zwischen optimal aufgelösten Bildern und dem Datenschutz. Technisch stehen für eine 24 h/7 d-Überwachung beste Bildqualitäten zur Verfügung. Oftmals wird die Auflösung wieder künstlich reduziert, um dem Datenschutz gerecht zu werden. In der Konsequenz erhält man gegebenenfalls sehr grob aufgelöste Videobilder, auf denen keine Details zu erkennen sind. Nicht nur, dass damit gegen die Vorgaben der Arbeitsstätterwerordnung [2] verstoßen wird, die fordert: „… Text- und Grafikdarstellungen auf dem Bildschirm müssen entsprechend der Arbeitsaufgabe und dem Sehabstand scharf und deutlich sowie ausreichend groß sein … Zeichen- und Zeilenabstand muss angemessen … Bild muss flimmerfrei sein."

Vielmehr steigt hiermit natürlich auch die Gefahr, dass Störungen im Betriebsablauf nicht rechtzeitig erkannt werden können und Hilfe- bzw. Rettungsmaßnahmen verzögert eingeleitet werden.

Im Bayerischen Datenschutzgesetz (BayDSG) [3] z. B. wird im Artikel 21a Videobeobachtung und Videoaufzeichnung (Videoüberwachung) gefordert: „(1) Mit Hilfe von optisch-elektronischen Einrichtungen sind die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist, um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die

sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen … aufhalten, zu schützen."

Hier ist klar festgelegt, dass eine Videoüberwachung und die zeitweise Speicherung erlaubt sind. Damit diese Daten durch die zunehmende IT-Durchdringung und Vernetzung nicht unerlaubt in falsche Hände gelangen können, ist ein besonderes Augenmerk auf die Informationssicherheit zu legen.

5 Informationssicherheit

Voraussetzung für eine datenschutzgerechte Videoübertragung und -speicherung für Tunnel ist eine Informationsverarbeitung, die mindestens die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen muss. Vorgaben dazu sind in verschiedenen Gesetzen und Normen erlassen worden. Wichtigste Grundlagen sind der IT-Grundschutz gemäß den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) und das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) [4]. Im § 8 wird der Sektor Transport und Verkehr und die hier als kritisch eingestuften Anlagen und Anlagenteile benannt.

Mit dem IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen (Kritis) und durch das BSI wird die Umsetzung der folgenden Anforderungen verbindlich eingefordert:

- Pflicht zur Umsetzung der IT-Sicherheit nach dem Stand der Technik,
- Pflicht zur Überprüfung der Vorgaben,
- Meldepflicht von IT-Sicherheitsvorfällen an das BSI,
- Unverzügliche Versorgung mit relevanten Informationen durch das BSI,
- Möglichkeit der Beratung und Unterstützung durch das BSI,
- Festgestellte Pflichtverstöße werden mit einem Bußgeld geahndet.

In Tabelle 1 sind den Schutzzielen einige typische Gefahren bzw. Bedrohungen zugeordnet und entsprechende Maßnahmen zur Minimierung der Risiken benannt. Bezogen auf das Thema Videotechnik muss der komplette Übertragungsweg von der Kamera bis zum Bedien-Client bzw. zur Videowand in der Überwachungsstelle betrachtet werden. So gehören dazu auch die kompletten Kabelwege sowie die Klemm-/Rangierverteiler (u. a. in Kabelhäusern, Streckenstationen), die sich auf dem Weg zwischen dem Tunnel und der Überwachungsstelle befinden und auch 100 km entfernt stehen können.

Folgende Lösungen wären für die Sicherstellung der Sicherheitsanforderungen möglich:

- Verwendung in sich geschlossener Netzwerke – Virtual Private Network (VPN),
- Keine Übertragung über das Internet,
- Begrenzung der Wartungszugänge und Absicherung mit Firewalls,
- Verschlüsselung der Video-Streams.

Um das IT-Sicherheitsniveau gegenüber Dritten nachweisen zu können, gibt es seitens des BSI ein Vorgehensmodell. Darin werden konkrete Verfahrensschritte von der IT-Strukturanalyse bis zur Umsetzung und Zertifizierung beschrieben.

Bezogen auf die Videotechnik wird somit das Risiko minimiert, dass die Video-Streams von der Quelle bis zur Senke durch Dritte verwendet oder manipuliert werden.

6 Zukünftige Entwicklungen

Mit der Migration von analogen zu digitalen Systemen haben sich eine Vielzahl von Möglichkeiten, aber auch Notwendigkeiten ergeben.

So beträgt das Seitenverhältnis der Kameras mit einer Full-HD-Auflösung (1.920 × 1.080 Pixel) 16 : 9. Die Darstellung der

Schutzziel	Typische Gefahren	Typische Maßnahmen
Vertraulichkeit	– Technisches Versagen (Ausfall, Zutrittskontrolle, fehlerhafte Anwendungsprogramme) – Vorsätzliche Handlungen (Datendiebstahl, Trojaner, Abhören von Leitungen) – Organisatorische Mängel (fehlende Sensibilisierung der Mitarbeiter, Regelungen beim Einsatz von Fremdfirmen) – Menschliche Fehlhandlungen (Fehlbedienung)	– Aufbau von Sicherheitszonen und Zutrittskontrollen für sensible Räume – Sinnvolle Segmentierung des IT-Netzes nach Schutzbedarf der Daten und Konfiguration von Schutzmechanismen (Firewalls, Gateways) – Sensibilisierung der Mitarbeiter durch Schulung
Verfügbarkeit	– Höhere Gewalt (Feuer, Wasser, Blitz) – Technisches Versagen (Ausfall von Servern, Rechnern, Energie) – Vorsätzliche Handlungen (Virenangriff, Sabotage) – Organisatorische Mängel (kein IT-Management, Planungsfehler)	– Aufbau von redundanten Systemen (Switches, Hauptserver) – Redundante Kommunikationsanbindungen (Wegeredundanz) – Vermeidung wasserführender Leitungen in Serverräumen – Klimakonzeption in Serverräumen
Integrität	– Technisches Versagen (Übertragungsfehler, fehlerhafte Anwendungsprogramme) – Vorsätzliche Handlungen (Virenangriff, Datenmanipulation) – Organisatorische Mängel (fehlende oder fehlerhafte Organisationsabläufe) – Menschliche Fehlhandlungen (Fehlbedienung)	– Verschlüsselung von Datenübertragungen – Durchführung von Datensicherungen – Definition eines Versionsmanagements für Dokumente

Tabelle 1 Gefahren der Informationsübertragung und Maßnahmen zur Minimierung von Risiken

Schritt	Leistung
IT-Strukturanalyse	Aus welchen Komponenten besteht der Bereich und wie stellt man diesen dar?
Schutzbedarfsfeststellung	Welcher Schutzbedarf besteht für die einzelnen Komponenten bezüglich der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und der örtlichen Gegebenheiten?
Modellierung	Wie wendet man die Bausteine des IT-Grundschutzes an?
Basis-Sicherheitscheck	Prüfung, ob die IT-Sicherheitsmaßnahmen umgesetzt wurden
Risikoanalyse	Durchführung einer Risikoanalyse mit Bewertung
Realisierungsplanung	In welchem Zeitraum werden fehlende Sicherheitsmaßnahmen ergänzt und umgesetzt?
Zertifizierung	Bewertung der vorhandenen IT-Sicherheitsmaßnahmen durch Dritte zum Nachweis

Tabelle 2 Vorgehensmodell des BSI

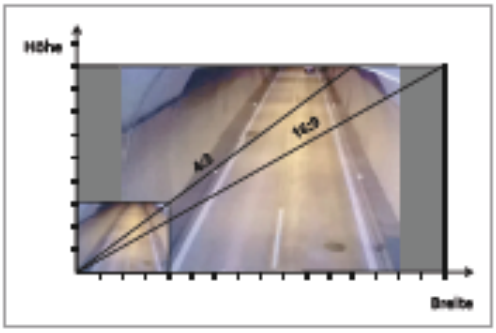

Bild 4 Seitenverhältnis von Videobildern

Videobilder auf älteren Monitoren mit einem Seitenverhältnis von 5 : 4 bzw. 4 : 3 ist somit nur möglich, indem Bildinhalte abgeschnitten oder schwarze Streifen seitlich zugelassen werden (Bild 4). Es ergibt sich die Notwendigkeit, Monitore und Videowände mit einem Seitenverhältnis von 16 : 9 einzusetzen.

Für Videowände und Bildarbeitsplätze stehen bereits Monitore mit 4K-Auflösung (3.840 × 2.160 Pixel) zur Verfügung. Damit können auch mehrere Streams, z. B. Vierer-Splits, auf einem Monitor mit voller Auflösung dargestellt werden.

Mit steigender Leistungsfähigkeit der Rechentechnik werden neue Einsatzfelder der Bildverarbeitung in der Videotechnik möglich. Bisher wird Videodetektion zur Erkennung von vergleichsweise wenig komplexen Vorgängen eingesetzt, so z. B. in der Erfassung von Falschfahrern.

Mit der Verknüpfung verschiedener Systeme, beispielsweise Video-, Automatisierungs- und Verkehrstechnik, ergeben sich weitere Möglichkeiten. So werden die Bildverarbeitungssysteme durch die rasante Entwicklung der Datenverarbeitung immer „intelligenter". Die entsprechenden Vor- und Nachteile einer Lokalisierung der Bildverarbeitungssoftware in den Kameras müssen dabei durch den Anwender, z. B. anhand einer zu definierenden Bewertungsmatrix, selbst bewertet werden. An dieser Stelle werden nur einige relevante Kriterien genannt:

- Ist das Detektionssystem unabhängig vom Kamerasystem?
- Ist ein ausreichender Einbauplatz für die Installation dezentraler Komponenten vorhanden?
- Welche Kameras mit integrierter Detektion sind am Markt verfügbar, und welche für den Nutzer relevanten Eigenschaften haben diese?
- Ist es für den Nutzer relevant, den Lebenszyklus der Kamera und den der Bildverarbeitungssoftware zu entkoppeln, da die Software schneller verändert wird als die Kamera-Hardware?

Für den Operator einer Tunnelüberwachungszentrale ist es sehr wichtig, dass er den Standort des Fahrzeugs, von dem eine Gefahr ausgeht, sofort erkennen kann. Er muss u. a. sofort unterscheiden können, ob es sich um ein brennendes Fahrzeug oder um die Auslösung der Höhenkontrolle vor einem Tunnel handelt. Bisher mussten die betreffenden Kameras manuell angewählt werden, um das Fahrzeug verfolgen zu können. Es verging wertvolle Zeit für die Suche nach der richtigen Kamera und für die Anwahl derselben. Durch die Objektverfolgung (Motion Tracking) ist dies nunmehr automatisch möglich. Das Fahrzeug wird durch verschiedene Eigenschaften wie Form, Größe, Farbe usw. und Berechnungsalgorithmen zu einem individuellen Objekt. Das Videosystem kann dem Operator eine Verfolgung dieses Objekts vorschlagen. Nach Bestätigung durch den Operator wird das Objekt dann im Videosystem immer wiedererkannt und die korrekte Kamera automatisch aufgeschaltet. Im Zusammenspiel mit der Automatisierungs- und Verkehrstechnik können dann entsprechende Verkehrsszenarien geschaltet werden, um das Fahrzeug zu stoppen oder um Hilfsmaßnahmen einzuleiten.

Da der Straßenverkehr nicht nur am Tag, sondern auch in der Nacht bei – für den Menschen – schlechteren Sichtbedingungen rollt, können zukünftig Kameras eingesetzt werden, die sowohl sichtbare als auch unsichtbare Bereiche des Lichtspektrums (Mehrbereichskamera für Infrarot- und UV-Wellenlängen) nutzen. Damit eröffnen sich noch weitere Möglichkeiten zur Identifikation und Detektion. Es kommt z. B. immer wieder vor, dass sich die Turbolader von Lastkraftwagenmotoren überhitzen und anfangen zu brennen. Anhand der Messung der Oberflächentemperatur der Fahrzeuge mit Mehrbereichs-Videokameras im Tunnelvorfeld könnte die kritische Temperatur identifiziert und das Fahrzeug an der Einfahrt in den Tunnel gehindert werden. Darüber hinaus könnten Überhitzungen von Bremsen, Reifen und Ladung per Videoüberwachung identifiziert werden.

Anhand des zugehörigen Videobilds kann der Operator die Meldung gegebenenfalls validieren und plausibilisieren.

Literatur

[1] ONVIF, www.onvif.org.
[2] Verordnung über Arbeitsstätten (Arbeitsstättenverordnung – ArbStättV), Anhang 6.1 (BGBl. I S. 2681) v. 30.11.2016, https://www.gesetze-im-internet.de.
[3] Bayerisches Datenschutzgesetz (BayDSG), Stand 22.12.2015, https://www.gesetze-bayern.de.
[4] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Erste Verordnung zur Änderung der BSI-Kritisverordnung (BGBl. I S. 1903) v. 21.06.2017, https://www.bgbl.de.