# Systeme für die automatische Verkehrskontrolle mit digitaler Bildtechnik

im Auftrag des

## Bundesamt für Strassen ASTRA

Forschungsauftrag 1999/301

**Datum**: 10. September 2002 **Bericht-Nr.:** 23.058.0/001 **Status:** Endbericht

Mitglieder der Begleitkommission:
**Pascal Blanc (ASTRA)** (Präsident)

| | | | | | |
|---|---|---|---|---|---|
| **Roland Aellen (ASTRA)** | **Erich Burkhalter (OZD/LSVA)** | **Walter Fasel (metas)** | **Hans Peter Oehrli (mobiletix)** | **Beat Schüpbach (Kapo BL)** | **Beat Zumsteg (R.Brüninger AG)** |

Projektleitung:
**Bernhard Oehry** Leiter Abt. Verkehrstelematik
Verfasser:
**Simon Benz** Abt. Verkehrstelematik
Mitarbeit:
**Christian Egeler** Abt. Verkehrstelematik
**Urban Kaiser** Abt. Verkehrstelematik

RAPP INGENIEURE + PLANER

**RAPP AG Ingenieure und Planer, Hochstrasse 100, 4018 Basel, Tel. + 41 61 335 77 77, http://www.rapp.ch**

# Zusammenfassung

## Gegenstand

Die Durchsetzung des Strassenverkehrsrechts und die Erhöhung der Verkehrssicherheit erfordern eine hohe Kontrolldichte, um deutliche Wirkungen zu zeigen. Aus diesem Grund ist man bestrebt, **Kontrollvorgänge zu automatisieren**. Im Gegensatz zu mobilen Verkehrskontrollen begleitet bei der automatischen Verkehrskontrolle keine vereidigte Person den Kontrollvorgang. Durch das Fehlen eines vereidigten Zeugen wachsen die Anforderungen an den automatisch und unbeobachtet erstellten Beweisdatensatz, da dieser alleine - d.h. ohne weitere Beweismittel - gerichtsfest sein muss.

Zur Zeit werden im Bereich automatischer Verkehrskontrollen praktisch ausschliesslich Kameras mit chemisch zu entwickelnden Filmen (sogenannte Nass-Filme oder Wet-Filme) eingesetzt. Die ergänzenden Daten (Datum/Zeit, Kontrollort, usw.) werden dabei direkt in das Bild eingeblendet und mitfotografiert. Der Einsatz von Wet-Film Kameras zieht jedoch eine Reihe von Nachteilen mit sich:

- Die Filme müssen physisch an der Station abgeholt werden.
- Die Filme müssen vor der Verarbeitung des Bildinhaltes entwickelt werden.
- Das Filmmaterial muss manuell archiviert werden.

Aus diesen und weiteren Gründen besteht der Wunsch, die herkömmlichen Wet-Film Kameras durch elektronische Bilderfassungsgeräte, insbesondere durch **digitale Kameras**, zu ersetzen.

Der Einsatz digitaler Kameras wirft jedoch eine Reihe von Fragen auf. So kann beispielsweise die **Authentizität eines Beweisbildes** nicht mehr durch die Tatsache belegt werden, dass es Teil einer ganzen Filmrolle ist. Aber auch Fragen rund um die Manipulation von digitalen Bildern, Verschlüsselung bei der Übertragung, usw. gilt es zu untersuchen. Dabei ist zudem zu berücksichtigen, dass durch den Einsatz digitaler Kameras auch neue Kontrollverfahren ermöglicht werden, die wiederum neue Fragestellungen erzeugen.

Wie oben festgestellt sind an automatisch generierte Beweisdatensätze erhöhte Anforderungen zu stellen. Der Einsatz digitaler Verfahren eröffnet zudem erweiterte Anwendungsmöglichkeiten, was jedoch die Anforderungen weiter erhöht, um zweifelsfrei nachweisen zu können, dass der Beweisdatensatz intakt ist und das originale Geschehen unverändert wiedergibt. Die Forschungsarbeit soll deshalb als ein wesentliches Ergebnis einen **Normentwurf** enthalten, der Anforderungen an Systeme für die automatische Verkehrskontrolle mit digitaler Bildtechnik vorgibt.

# Vorgehen

Die Forschungsarbeit untersucht in einem ersten Schritt den **Ist-Zustand** bezüglich bestehenden Anwendungen und Forschungsarbeiten sowie bezüglich den gesetzlichen Grundlagen auf dem Gebiet der automatischen Verkehrskontrolle. Dabei werden Aspekte und Informationen aus dem Inland und dem europäischen Ausland berücksichtigt.

In einem nächsten Schritt erfolgt eine kurze allgemeine Darstellung der **technischen Methoden** und Verfahren zu den Themen:

- Digitale Bilderfassung (digitale Standbildkameras sowie Videokameras)
- Datensicherheit (Verschlüsselung, Signatur, elektronisches Wasserzeichen, usw.)
- Bearbeitung von digitalen Daten, insbesondere von Bilddaten
- Komprimierungsverfahren

Als wesentliche Grundlage für den Normentwurf wird ein **funktionales Modell** für Systeme zur automatischen Verkehrskontrolle entwickelt. Das funktionale Modell soll so einfach und allgemeingültig wie möglich die Grundelemente und grundsätzlichen Abläufe solcher Kontrolleinrichtungen darstellen, damit die Anforderungen an diese Subsysteme klar definiert werden können. Dabei liegt besonderes Augenmerk darauf, dass das Modell sowohl auf alle bestehenden als auch auf denkbare zukünftigen Verfahren anwendbar ist.

Anhand des erstellten Modells wird dann der **Normierungsbedarf abgegrenzt**. Zusätzlich wird abgeklärt, ob durch den Einsatz der neuen digitalen Bilderfassungsverfahren Anpassungsbedarf an bestehenden rechtlichen Grundlagen besteht.

Aufbauend auf der Analyse des Normierungsbedarfs werden die Anforderungen an die digitalen Datensätze erstellt. Aus diesen Anforderungen wird dann der **Normentwurf** gebildet.

# Ergebnisse

### Gesetzliche Grundlagen

Die beiden bestehenden technischen Weisungen zum Thema automatische Kontrollanlagen sind sehr funktional gehalten. Beschrieben werden insbesondere der Kontrollablauf, die Rahmenbedingungen sowie die Anforderungen an das Beweisbild (inkl. eingeblendeten Zusatzdaten). Der Einsatz von digitalen Bilderfassungsmitteln wurde bei der Erstellung zwar nicht berücksichtigt, wird aber auch nicht explizit ausgeschlossen.

### Funktionales Modell

Der Gesamtvorgang einer Verkehrskontrolle lässt sich in drei Teilfunktionen unterteilen:

- **Detektion**: Umfasst alle Einzelschritte anhand welcher festgestellt wird, ob und in welchem Masse sich ein Verkehrsteilnehmer gegen bestehende Gesetze verhält.
- **Dokumentation**: Umfasst sämtliche Einzelschritte welche notwendig sind, um den Verstoss ausreichend zu dokumentieren. Ausserdem fallen in diesen Bereich die Übertragung der Daten an eine zentrale Stelle sowie die Aufbewahrung.
- **Verarbeitung**: Umfasst sämtliche Tätigkeiten nach der Übertragung des Beweisdatensatzes an die nachbearbeitende Stelle (exkl. Aufbewahrung). Darunter fällt beispielsweise das (manuelle oder automatische) Herauslesen eines Kontrollschildes, oder die Verifizierung des funktionalen Bildinhalts.

### Physikalische Struktur

Analog dem funktionalen Modell kann auch das physische Gesamtsystem einer Verkehrskontrolleinrichtung (Enforcementanlage) in mehrere Systemteile gegliedert werden. Es bietet sich eine Gliederung in folgende drei Teile an:

- **Strassenseitige Kontrolleinrichtung**: Dieser Teil beinhaltet sämtliche Kontrolleinrichtungen vor Ort an der Strasse. Dazu gehören insbesondere die Bilderfassungsanlage, die Messeinrichtung(en), sowie allenfalls vorhandene Auswertungselektronik.
- **Übertragungskanal**: Primär gemeint ist der Übertragungskanal zwischen der strassenseitigen Kontrolleinrichtung und dem Hintergrundsystem. Weitere Übertragungsstrecken sind jedoch nicht ausgeschlossen. Denkbar sind beispielsweise längere Verbindungen zwischen einzelnen Anlagekomponenten wie beispielsweise beim Verfahren der Abschnittsgeschwindigkeitskontrolle.
- **Hintergrundsystem**: Hier erfolgen die weitere Bearbeitung eines Datensatzes wie beispielsweise die manuelle Bestätigung des LPR/OCR Resultates oder die Kontrolle des Klassifizierungsresultats. Im weiteren werden hier die Daten archiviert bzw. verwaltet.

### Normierungsbedarf

Der ursprüngliche Titel der Forschungsarbeit *„Systeme für die automatische Verkehrskontrolle (Enforcement) mit digitaler Bildverarbeitung und automatischer Kontrollschilderkennung“* suggerierte, dass die zentrale Problematik digitaler Bildverfahren bei automatischen Verkehrskontrollanlagen in der Bildverarbeitung und hier besonders in der automatischen Kontrollschilderkennung liegt.

Die Analyse des Normierungsbedarfs hat jedoch klar ergeben, dass die zwei explizit angeführten Schlüsselbegriffe des ursprünglichen Titels, nämlich „digitale Bildverarbeitung“ und „automatische Kontrollschilderkennung“ keine entscheidenden Prozesse bei der automatischen Kontrolle mit digitalen Bilderfassungsmitteln sind. Bei beiden Verfahren handelt es sich im Grunde nur um Hilfsmittel für die Verarbeitung, welche jedoch aus rechtlicher Sicht für die Beweiskraft eines Kontrolldatensatzes bedeutungslos sind. Entscheidend ist die Entstehung und der unveränderte und eindeutige Inhalt des Beweisdatensatzes. So konzentriert sich dann auch der Norm-Entwurf ausschliesslich auf die Teilfunktion *Dokumentation* und lässt die Funktionen *Detektion* und *Verarbeitung* ausser Betracht.

Um dieser Erkenntnis Rechnung zu tragen wurde auch der Titel der Arbeit angepasst und der Fokus auf die Schlüsselworte „automatische Verkehrskontrolle“ und „digitale Bildtechnik“ gelegt.

### Anforderungen an Daten und Abläufe

Die Analyse zeigt, dass der Normierungsbedarf sich im wesentlichen auf den Beweisdatensatz beschränkt. Umgelegt auf das funktionale Modell bedeutet das, dass die normativen Anforderungen an die Teilfunktion *Dokumentation* gestellt werden. Die verschiedenen Anforderungen können in einzelne Bereiche unterteilt werden:

- **Funktionale Anforderungen an die Beweisdatensätze**: Die Integrität sowie die Authentikation müssen nachweisbar sein. Ausserdem muss der Datensatz den Tatbestand vollständig dokumentieren.

- **Anforderungen bezüglich Datenschutz und Datensicherheit**: Dazu gehört einerseits der Zugriffsschutz/Überwachung für strassenseitige Anlagekomponenten. Andererseits müssen die Daten bei der Übertragung ausreichend geschützt sein. Kann dies nicht durch die Beschaffenheit des Übertragungskanals gewährleistet werden, so müssen die Daten verschlüsselt werden. Auch bei der Aufbewahrung der Daten im Hintergrundsystem müssen die Daten so geschützt sein, dass der Zugriff nur für berechtigte Personen möglich ist.
- **Anforderungen bezüglich Integrität & Authentizität**: Um die Integrität und Authentizität des Datensatzes prüfen und nachweisen zu können, muss der Datensatz noch in der gesicherten Umgebung der Kontrollanlage signiert werden. Je nach Architektur der Anlage ist es allenfalls nötig, einzelne Teile des Datensatzes zusätzlich separat zu signieren.
- **Anforderung an die Nachbearbeitung**: Der Original-Beweisdatensatz muss in jedem Fall in unveränderter Form gespeichert werden. Ansonsten bestehen keine Einschränkungen.
- **Anforderung an die Aufbewahrung & Verwaltung**: Der Zugriff auf Enforcementdaten muss jederzeit möglich sein. Ausserdem müssen die Daten in geeigneter Form dargestellt und ausgegeben werden können. Die Integrität und Authentizität muss erhalten bleiben und jederzeit nachgewiesen werden können. Die dafür nötigen Schlüssel müssen dementsprechend sicher und langfristig verwaltet werden.
- **Anforderungen an die Bildqualität**: Die Anforderungen an die Bildqualität eines Beweisbildes können funktional wie folgt definiert werden: Das Bild muss den Tatbestand zweifelsfrei dokumentieren. In den meisten Fällen heisst das konkret, dass das Kontrollschild sowie der Lenker zweifelsfrei erkannt werden können müssen. Mit dieser Definition ergeben sich gewisse Mindestanforderungen an die Anzahl der Bildpunkte sowie Restriktionen hinsichtlich dem zulässigen Datenkompressionsgrad (beim Einsatz von verlustbehafteten Komprimierungsalgorithmen).

## Kernresultate

- Der **Norm-Entwurf** gibt eine Grundlage für eine schweizerische Norm für automatische Kontrollanlagen mit digitaler Bildtechnik.
- Die für den Einsatz automatischer Verkehrskontrollsysteme mit digitaler Bildtechnik **notwendigen Anpassungen an den bestehenden technischen Weisungen sind gering**.
- Dem Einsatz von automatischen Kontrollanlagen mit digitaler Bildtechnik steht – bei Beachtung der erarbeiteten Anforderungen - grundsätzlich nichts im Weg.

# Inhalt

(Leerseite)

# 1. Problemstellung

## 1.1. Ausgangslage

Vielerorts in der Schweiz stösst der Strassenverkehr an die Grenzen seiner Leistungsfähigkeit. Mit der Zunahme des Verkehrs ist ein effektives Verkehrsmanagement unter Berücksichtigung eines günstigen Kosten-Leistungsverhältnisses nötig.

Die Verkehrssicherheit ist ein wichtiges Ziel des Verkehrsmanagements. Zur Erhöhung der Sicherheit und zur Durchsetzung des Strassenverkehrsrechts ist eine hohe Kontrolldichte erforderlich, um deutliche Wirkungen zu zeigen. Eine hohe Kontrolldichte erfordert derzeit jedoch grossen Personaleinsatz sowohl in der Durchführung der Kontrollen (Aufnahme von Verstössen) als auch in der Ahndung.

Seit den fünfziger Jahren kommen Fotoapparate zum Einsatz, um kosten- und arbeitsintensive Überwachungsmethoden abzubauen. Mit der weiteren Entwicklung der Verkehrstelematik kann eine noch wesentlich höhere Effizienz erreicht werden. Der Einsatz von digitalen Bilderfassungsmitteln sowie die elektronische Bildverarbeitung ermöglichen einerseits neue Kontrollverfahren, und können andererseits zu einer effizienteren Gestaltung der Kontrollvorgänge beitragen.

## 1.2. Aufgabe

Im Rahmen der Forschungsarbeit soll untersucht werden, unter welchen Voraussetzungen automatische Kontrollen unter Anwendung von elektronischen Hilfsmitteln, insbesondere Geräte und Verfahren der digitalen Bildtechnik, wie digitale Kameras, Daten(fern)übertragung, digitale Bildverarbeitung oder automatische Kontrollschild-erkennung zum Einsatz kommen können. Anhand einer Grundlagenstudie soll der Normierungsbedarf ermittelt werden.

## 1.3. Forschungsziele

Ziel der Forschungsarbeit ist die Erstellung eines Entwurfs für eine Norm, welche die Anforderungen an eine Enforcementanlage mit digitaler Bilderfassung definiert. Es gilt insbesondere Anforderungen an:

- die Ausrüstung
- die Abläufe
- und gesetzlichen Voraussetzungen

abzuklären und bei Bedarf neu festzulegen. Im weiteren gilt es eine Referenz-Architektur für derartige Systeme festzulegen.

Es ist die Frage zu klären, in wie weit es erforderlich ist, Qualitätsansprüche für die Detektion von Vorgängen zum einen und für die automatische Kontrollschilderkennung zum anderen zu definieren. Anforderungen an nötige Bildinhalte, Bildformate und deren Sicherung zur Dokumentation von Vorgängen müssen so definiert werden, dass sie einer gerichtlichen Prüfung standhalten.

## 1.4. Vorgehen und Methoden

*1. Projektvorbereitung*

Im Rahmen der Projektvorbereitung wurden ergänzende Grundlagen (Literatur, Normen) beschafft und die Koordinationsabläufe mit anderen relevanten Projekten festgelegt.

*2. Aufarbeitung der Grundlagen*

Bereits bestehende Anwendungen mit digitalen Bildern sowie Unterlagen und Berichte über digitales Enforcement geben eine fundierte Grundlage zur Thematik. Zum Beispiel wurde im Rahmen des EU-Forschungsprojektes VERA (Video Enforcement for Road Authorities) schon einmal eine allgemeine Betrachtung des Einsatzes von digitalen Video- oder Bildaufnahmen getätigt. Allerdings ging es dabei mehr um eine Harmonisierung der Abläufe des Enforcements in den europäischen Staaten.

Im weiteren werden die für diese Untersuchung benötigten Begriffe definiert. Eine Zusammenstellung der gesetzlichen Grundlagen hilft einen Überblick darüber zu gewinnen, welche Konsequenzen die Untersuchung auf spätere Gesetzesanpassungen haben kann.

3. *Digitale Bildverarbeitung*

Es ist wichtig, dass insbesondere die Technologie der digitalen Bildverarbeitung, welche im Rahmen dieser Arbeit eine zentrale Rolle einnimmt, aufgearbeitet wird, so dass eine klare Grundlage geschaffen ist. Hierzu gilt es grob die Entstehung und die Möglichkeiten von digitalen Bildern aufzuzeigen.

4. *Systemarchitektur*

Um die geforderte Referenz-Architektur festzulegen, bedarf es der Ausarbeitung eines Modells. Dies soll anhand einer Analyse bestehender Enforcementvorgänge erfolgen. Das Modell muss sowohl auf der physischen als auch der funktionalen Ebene erstellt werden. Die Modellierung gibt einen generellen Überblick über das System und ist Grundlage einer einheitlichen Betrachtung.

5. *Der Umgang mit Daten*

Wenn Widerhandlungen ausschliesslich in digitaler Form dokumentiert werden, wirft dies Fragen bezüglich Datenschutz auf. Aus diesem Grunde müssen zwingend die Anforderungen an

- Datenschutz und -sicherheit
- Integrität und Authentikation
- Nachbearbeitung von Daten
- Aufbewahrung und Verwaltung
- Bildqualität

aufgezeigt werden.

6. *Normenentwurf*

Die vorangegangenen Schritte sollten es möglich machen, den geforderten Entwurf des Normierungsbedarf für das digitale Enforcement festzulegen.

# 2. Begriffsdefinitionen

In der Verkehrstelematik sind noch nicht alle Begriffe vollständig geklärt. Grundlagen bestehen bereits in der Schweizer Norm SN 671832-875 „Verkehrstelematik“. Das folgende Kapitel beschreibt die wichtigsten Begriffe und schafft eine einheitliche Grundlage für den weiteren Bericht.

## 2.1. Enforcement im Strassenverkehr

Unter Enforcement versteht man, die Einhaltung von Bestimmungen und Gesetzen – in diesem Fall rund um die Benützung von Strassen – durchzusetzen. Verkehrsüberwachung z.B. in Form von Stauerkennung, aktive Verkehrsbeeinflussung u.ä. fallen nicht unter den Bereich des Enforcement, sondern werden unter dem Begriff Monitoring zusammengefasst. Beim Monitoring wird der Gesamtbetrieb „Strasse“ überwacht, wobei die Anonymität des einzelnen Fahrzeuges bzw. dessen Fahrers unbedingt gewahrt werden muss. Im Gegensatz dazu geht es beim Enforcement explizit darum, den einzelnen Verkehrsteilnehmer zu kontrollieren und das Fahrzeug und dessen Lenker bei Bedarf zu identifizieren.

## 2.2. Video Enforcement

Die vorliegende Forschungsarbeit beschäftigt sich mit einem spezifischen Teilaspekt des Enforcements, den Video Enforcement Systemen (VES). Hierbei werden Bilder als Beweis einer festgestellten Zuwiderhandlung erstellt, wobei die Bilder mit zusätzlichen Informationen (Zeit, Ort, Geschwindigkeit usw.) ergänzt werden.

Bisher wurden bei solchen Enforcementanlagen ausschliesslich herkömmliche Kameras („Wet-Film“) eingesetzt. Diese haben aber entscheidende Nachteile. So müssen die Bilder physisch an der Anlage abgeholt und anschliessend entwickelt werden, damit eine Verarbeitung erfolgen kann. Zudem ist eine automatisierte Verarbeitung schwierig.

In den letzten Jahren hat sich der Einsatz von digitalen Bildern in allen Bereichen stark verbreitet. Es ist deshalb naheliegend, die zahlreichen Vorteile digitaler Technologien auch im Bereich Video-Enforcement zu nutzen.

## 2.3. Anwendungen von Video Enforcement

Bisher wurden Bilder im Bereich automatische Verkehrskontrollen für folgende Anwendungen verwendet:

- Überwachung von Rotlichtanlagen
- Geschwindigkeits-Überwachungsanlagen

Diese beiden aufgeführten Anwendungen sind auch in entsprechenden technischen Weisungen des UVEK definiert. Insbesondere durch den Einsatz von digitalen Systemen ist eine ganze Reihe von weiteren Anwendungen denkbar, wie Abschnittsgeschwindigkeits-kontrollen, Busstreifenüberwachung, Zufahrtsberechtigungsüberwachung, usw.

## 2.4. Definition automatische Verkehrskontrolle

Eine automatische Verkehrskontrollanlage ist ein System, welches Fahrzeuge ohne die Anwesenheit von vereidigten Personen überwachen kann. Das System ist fähig, ein Widerhandlung automatisch zu detektieren und so zu dokumentieren, dass das daraus entstandene Material als Sachbeweis gerichtsfähig ist.

# 3. Situation und Grundlagen

## 3.1. Bestehende Anwendungen mit digitalen Bildern

### 3.1.1. LSVA

Am Südportal des Belchentunnels wird seit Anfang 2001 eine Enforcement Anlage mit digitaler Bilderfassung für die Leistungsabhängige Schwerverkehrsabgabe LSVA betrieben:

**Abbildung 1: LSVA Enforcement-Anlage am Belchen**

Der Aufbau der Anlage präsentiert sich wie folgt:

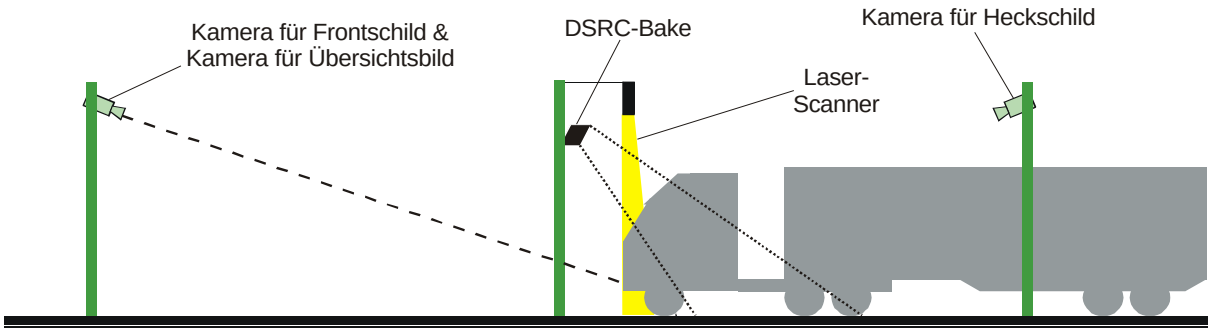



**Abbildung 2: Aufbau der LSVA Enforcementanlage**

Grundsätzlich wird jedes Fahrzeug an der Anlage erfasst und klassifiziert (wobei die Daten von nicht pflichtigen Fahrzeugen umgehend gelöscht werden). Zusätzlich wird – falls vorhanden – das Erfassungsgerät (TRIPON) ausgelesen. Damit stehen dem System folgende Daten zur Verfügung:

- Detektierte Fahrzeugklasse (inkl. Anhängerinformation)
- Kennzeichen des Fahrzeugs und (falls vorhanden) des Anhängers
- Daten aus dem Erfassungsgerät (insbesondere der aktuelle Status, d.h. der Betriebszustand des Gerätes und der Deklarationszustand)

Bei Fahrzeugen mit Erfassungsgerät werden die Messdaten mit den im Gerät deklarierten Daten verglichen. Diese werden an der Kontrollanlage über Funk (DSRC) ausgelesen.

Handelt es sich um ein nicht ausgerüstetes Fahrzeug, so werden die Messdaten mit den vom Fahrer bei der Einfahrt in die Schweiz am Selbstbedienungsterminal deklarierten Daten verglichen. Daraus kann ermittelt werden, ob ein Verstoss vermutet werden muss oder nicht.

Die erfassten Bilder werden von den Kameras direkt mit einer kryptografischen Signatur versehen, so dass nachträgliche Veränderungen am Bildinhalt erkannt werden können (vgl. Kapitel 4.5.2). Auch die automatische Kontrollschilderkennung (LPR/OCR) geschieht direkt in der Kamera. Im Stationsrechner laufen die Datenelemente (Scanner-Rohdaten, DSRC-Daten, Resultat der automatischen Kontrollschild-Erkennung und die drei Bilder) zusammen. Dieser Datensatz wird anschliessend als Gesamtes signiert und so gegen unbemerkte Veränderungen geschützt.

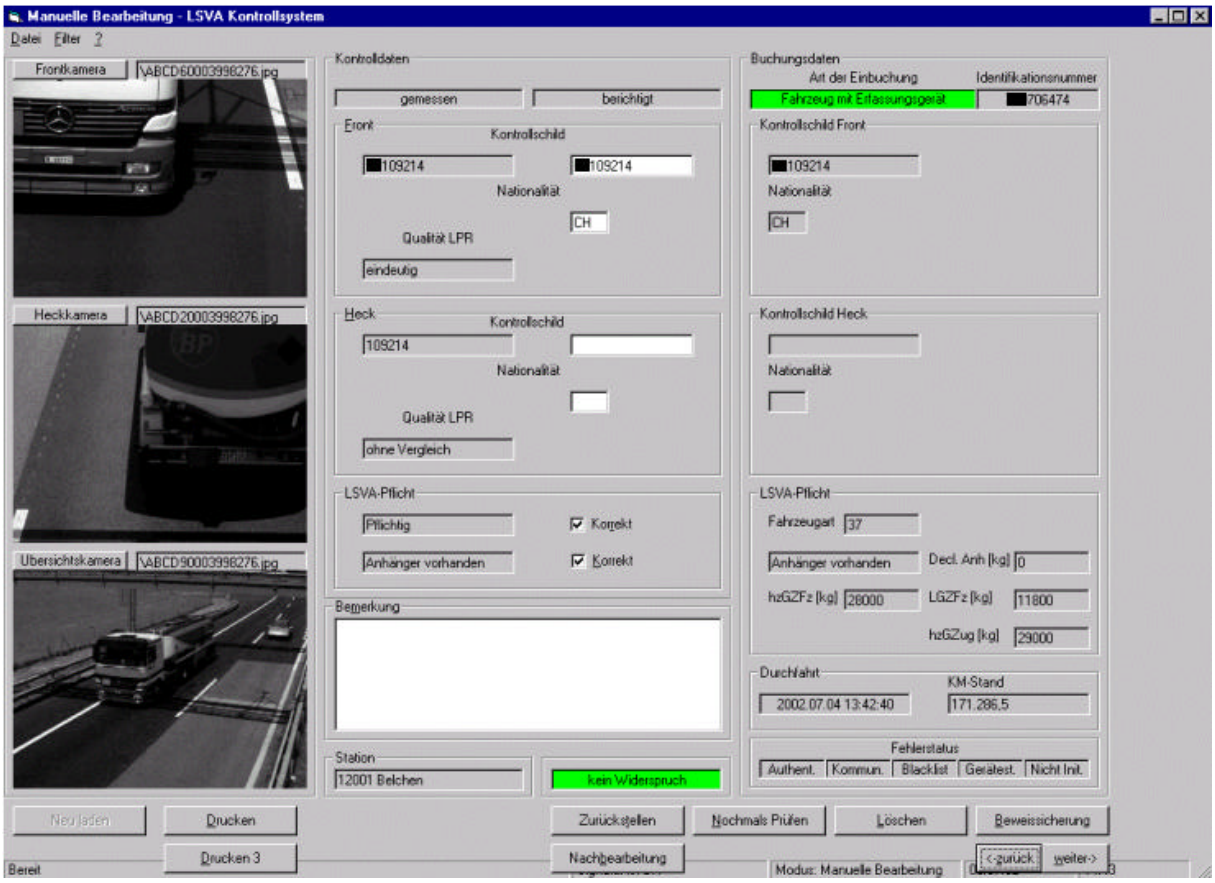



**Abbildung 3: Bildschirmdarstellung bei der Bearbeitung eines Falles in der LSVA Enforcement Zentrale**

Die Kontrollanlage am Belchen ist die einzige uns derzeit bekannte Anwendung im Bereich Strassen[1] in der Schweiz, bei welcher digitale Bilder als Beweismittel eingesetzt werden. Die Erfahrungen und Resultate aus dem bisherigen Betrieb sind sehr wertvoll für das Forschungsprojekt *Digitales Enforcement*, insbesondere auch weil bei der LSVA Enforcementstation Datensätze mit mehreren verschiedenen Teilkomponenten entstehen.

[1] Die Anwendung ist zwar im Bereich Strassen, bewegt sich aber in Rahmen der LSVA-Gesetze und nicht des Strassenverkehrsgesetzes.

### 3.1.2. Fahrzeugfahndung

Ein Anwendungsbeispiel für Fahrzeugfahndung mit digitaler Bildtechnik betreibt die Stadtpolizei Zürich. Dabei handelt es sich um eine Anlage zur Auffindung von gesuchten Fahrzeugen aus dem fliessenden Verkehr. Die Anlage arbeitet mit elektronischen Bildern und LPR/OCR. Bei dem Vorgang werden die elektronischen Bilder aber nicht als Beweismittel eingesetzt. Sie dienen lediglich zur Selektion der Fahrzeuge, welche nach einer Ausleitung untersucht werden sollen. Der Nutzen für das Forschungsprojekt „Digitales Enforcement“ beschränken sich damit auf die allenfalls gegebene Frage des Datenschutzes bei der Aufzeichnung von Daten resp. Bildern.

### 3.1.3. C.A.S.E. (Continuous Applied Speed Enforcement)

Bei dieser Anwendung wird – im Gegensatz zu herkömmlichen Geschwindigkeits-Kontrolleinrichtungen – ein ganzer Streckenabschnitt (Länge: einige 100m bis einige km) kontrolliert. Zu diesem Zweck werden zu Beginn und Ende der zu kontrollierenden Strecke die Fahrzeuge mittels digitalen Kameras erfasst. Mit eigens für diese Anwendung entwickelten Algorithmen werden Fahrzeuge am Ende des Abschnitts wiedererkannt, die Durchfahrtszeit berechnet und die Durchschnittsgeschwindigkeit für den Abschnitt ermittelt.

Dieses Konzept wurde in Holland entwickelt und erstmals erprobt. Die Erfahrungen und Erkenntnisse aus dem holländischen Projekt sind im Zusammenhang mit digitalem Enforcement grundsätzlich als sehr wertvoll einzustufen. Neu an dieser Anlage ist in erster Linie das angewendete Messverfahren und weniger die Verwendung digitaler Bilder. So sank die Anzahl der zu schnell fahrenden Fahrzeuge von 6% auf 1% des gesamten Verkehrs (Vor der Installation wurde der Abschnitt bereits deutlich verstärkt mit traditionellen, nicht automatischen Methoden kontrolliert und eine Tafel mit Hinweis auf mögliche Kontrollen war ebenfalls bereits montiert. Zuvor betrug die Übertretungsrate 35% (Vortrag Jan Malenstein, KLPD, 27.5.99). Die durchschnittliche Geschwindigkeit sank von 116 km/h auf 106 km/h bei einer Tempolimite von 100 km/h. Ein gleichmässigerer Verkehrsfluss (geringere Geschwindigkeitsunterschiede) als vor Inbetriebnahme der Anlage sowie deutlich geringere Unfallzahlen und Stauereignisse wurden festgestellt.

Für die Forschungsarbeit liegt der Fokus auf den Einsatz von digitalen Bildern, und nicht auf der Ereignisdetektion, wie es bei C.A.S.E realisiert ist.


**Abbildung 4: C.A.S.E Anlage in Holland**

### 3.1.4. Geschwindigkeitsüberwachungsanlage mit digitaler Bilderfassung

Zur Zeit (Mitte 2002) ist eine provisorische Zulassung für die erste Geschwindigkeitsüberwachungsanlage mit digitaler Bilderfassung in der Schweiz in Bearbeitung. Das Verfahren wird voraussichtlich in den nächsten Monaten abgeschlossen, so dass ein Pilotbetrieb begonnen werden kann. Die Anlage arbeitet mit Piezosensoren zur Detektion, und kann wahlweise mit einer herkömmlichen oder einer digitalen Kamera ausgerüstet werden. Die Anlage kann sowohl zur Geschwindigkeitsüberwachung als auch zur Rotlichtüberwachung eingesetzt werden und verfügt über eine Schnittstelle zur Fernwartung und zur Parametrisierung. Da die Zugriffsverwaltung noch ungenügend geklärt ist, ist die Schnittstelle zur Zeit jedoch noch nicht freigegeben. Eine spätere Freigabe ist aber unter bestimmten Auflagen denkbar. Die erste Anwendung dieser Anlage wird eine Geschwindigkeitsüberwachung sein.

Der Zulassungsprozess dieser Anlage ist für das vorliegende Forschungsprojekt als sehr wichtig einzustufen. Es handelt sich um die erste Zulassung einer Enforcementanlage mit digitaler Bilderfassung im Rahmen des Strassenverkehrsgesetzes in der Schweiz. Der Zulassungsprozess gibt wichtige Anhaltspunkte über den sinnvollen Detailierungsgrad der zu erstellenden Norm. Es gilt einen Mittelweg zwischen nötigen Rahmenbedingungen und behindernden Vorschriften zu finden.

**Anmerkung:** Bei der oben erwähnten Abnahme wird die Anlage zusammen mit der Datenübertragungsstrecke als Gesamtsystem abgenommen.

## 3.2. Unterlagen und Berichte zum Thema „digitales Enforcement“

### 3.2.1. Italienische Norm UNI – E14C8005

Die von UNINFO – einer Unterstelle der italienischen Normierungsbehörde UNI (Ente Nationale Italiano di Unificazione) – erarbeitete Norm E14C8005 befasst sich mit der Struktur und den Anforderungen an automatische Kontrolleinrichtungen, wobei besonderes Augenmerk auf die automatische Kontrollschilderkennung via OCR gelegt wird. Die Norm ist sehr unterschiedlich detailliert was die einzelnen Systemteile angeht. Während Themen wie Systemarchitektur, Security und Authentizität der Datensätze oder Bildformate nur sehr allgemein gehalten sind, wird das Thema LPR/OCR sehr ausführlich und präzise beschrieben. Insbesondere werden Laboraufbauten und Testverfahren zur Bestimmung der LPR/OCR Erfolgsrate sehr detailliert dargestellt. Dies verwundert deshalb etwas, weil es sich beim Systemteil OCR im Prinzip um ein reines Hilfssystem handelt. Dementsprechend sind auch die Anforderungen stark von der jeweiligen Anwendung abhängig. Ausserdem sind Labortests für den Praxisbetrieb nur beschränkt aussagekräftig (was in der Norm auch ausdrücklich erwähnt wird). Eine genaue Beschreibung der Abnahmetests für LPR/OCR Systeme dient letztlich lediglich der Vergleichbarkeit der Anlagen verschiedener Hersteller.

Die UNI Norm ist aufgrund der ungleichen Gewichtung nur begrenzt anwendbar für die vorliegende Forschungsarbeit. Trotzdem liefert sie gewisse Anhaltspunkte für die grobe Strukturierung einer Norm.

### 3.2.2. Forschungsprojekt VERA

Das EU-Forschungsprojekt VERA (**V**ideo **E**nforcement for **R**oad **A**uthorities) befasste sich mit dem Thema der Verkehrskontrolle und deren Vollzug auf Autobahnen und Strassen durch die dafür zuständigen Behörden. Es wurden die technischen, rechtlichen und institutionellen Gesichtspunkte untersucht und ausgewertet. Das geplante Nachfolgeprojekt VERA II befasst sich im Kern mit der Problematik der grenzüberschreitenden Verfolgung von Verkehrsvergehen. Es ist geplant Richtlinien, Abläufe und Schnittstellen zu definieren, die ein cross-border Enforcement ermöglicht respektive vereinfacht.

Die Erfahrungen und Ergebnisse aus VERA sind für diese Forschungsarbeit als sehr wichtig einzustufen. Insbesondere die Resultate im Bereich des funktionalen Modells sind sehr wertvoll.

### 3.2.3. Forschungsprojekt ADVICE

Das im Zuge des 4. Rahmenprogramms der Europäischen Kommission durchgeführte Forschungsprojekt ADVICE (Advanced Vehicle Classification and Enforcement) befasste sich ausführlich mit neuen Technologien zur Fahrzeugklassifizierung und -überwachung. Das Ziel von ADVICE war die Schliessung von Forschungslücken betreffend Vollzugssicherheit bei elektronischen Gebührenerhebungssystemen.

Aufgrund des spezifischen Fokus auf Enforcement in Gebührenerhebungssystemen ist diese Arbeit für das Projekt *Digitales Enforcement* nur beschränkt von Bedeutung.

## 3.3. Bestehende gesetzliche Grundlagen

### 3.3.1. Anwendungen im Rahmen des Strassenverkehrsgesetzes

**Strassenverkehrsrecht**

Die Durchführung von automatischen Verkehrskontrollen ist im **Strassenverkehrsrecht** SR 741.51 geregelt.

In Art. 130 Absatz 4 heisst es dort:

*„Das Bundesamt erlässt Weisungen über die Durchführung automatischer Verkehrskontrollen ohne Anhalteposten und regelt das Verfahren.“*

Weiter heisst es in Art. 133 zum Thema Geschwindigkeitskontrollen:

*„Das Bundesamt erlässt Weisungen über die Durchführung der polizeilichen Geschwindigkeitskontrollen und über die Messverfahren. Es regelt die Verwendung automatischer Geschwindigkeitsmessgeräte.“*

**Technische Weisungen**

In den Anhängen ***A/4.3 Technische Weisungen über Geschwindigkeitskontrollen im Strassenverkehr des UVEK vom 10. August 1998*** und ***A/4.4 Weisungen über den Einsatz fotografischer Rotlicht Überwachungsgeräte vom 14. April 1988*** werden Richtlinien und Weisungen für Kontrollen dieser Art beschrieben.

Die Technische Weisung regelt auch die Frage der Zulassung von Enforcementanlagen:

*„Geräte für amtliche Geschwindigkeitsmessungen unterliegen der Typengenehmigung und der Zulassung durch das Eidg. Amt für Messwesen (EAM).Sie dürfen nur verwendet werden, wenn sie nach den Vorschriften der Verordnung über die Qualifizierung von Messmitteln (Eichverordnung) typengenehmigt und mit einem amtlichen Zulassungszeichen versehen sind.“*(Ziffer 3.1 der Technischen Weisungen über Geschwindigkeitskontrollen im Strassenverkehr des UVEK vom 10. August 1998.)

**Anmerkung:** Das ehemalige Amt für Messwesen nennt sich mittlerweile Bundesamt für Metrologie und Akkreditierung (metas).

Die Anforderungen für die Zulassung durch das metas sind in der **Verordnung über die Qualifizierung von Messmitteln (Eichverordnung)** SR 941.210 festgehalten.

**Abbildung 5: metas Logo**

### 3.3.2. Anwendungen ausserhalb des Strassenverkehrsgesetzes

Bis jetzt ist die LSVA die einzige Anwendungen rund um den Strassenverkehr, welche nicht unter das Strassenverkehrsgesetz fällt. Die LSVA stützt sich rechtlich auf:

Das **Schwerverkehrsabgabegesetz (SVAG)** SR 641.81 vom 19.12.1997. Dort steht unter Artikel 22:

*„[1]Die Strafverfolgung und Beurteilung von Widerhandlungen, die inländische Fahrzeuge betreffen, ist Sache der Kantone.*

*[2]Widerhandlungen, die ausländische Fahrzeuge betreffen, werden nach dem Bundesgesetz vom 22. März 1974 über das Verwaltungsstrafrecht durch die Eidgenössische Zollverwaltung verfolgt und beurteilt.“*

Die **Schwerverkehrsabgabeverordnung (SVAV)** SR 641.811 vom 6.3.2000. Dort steht unter Kapitel 8, Artikel 42, Kontrolleinrichtungen:

*„Die Zollverwaltung kann ortsfeste und mobile Kontrollstationen betreiben. Sie beschafft die Spezialausrüstung für mobile Kontrollequipen und kann diese den Kantonen zur Verfügung stellen.“*

## 3.4. Zulassung und Betrieb einer automatischen Kontrollanlage

Automatische Kontrollanlagen dürfen nicht ohne weiteres in der Schweiz eingesetzt werden. Neben den nötigen Zulassungspapieren, muss die Anlage geeicht und somit für den Betrieb zugelassen werden. Zusammengefasst werden folgende Schritte durchlaufen:

| **1. Schriftlicher Antrag** |
|---|
| Ein Hersteller möchte ein Messmittel, welches zur amtlichen Feststellung von physikalischen Grössen verwendet wird, in der Schweiz verkaufen. Da solche Messmittel zulassungspflichtig sind, beantragt er beim Bundesamt für Metrologie und Akkreditierung (metas) eine Zulassung für diesen Messmitteltyp. |
| **2. Bauartprüfung/Typenprüfung** |
| Beim metas wird daraufhin eine Bauartprüfung vorgenommen. Diese beinhaltet eine ganze Reihe von Einzelprüfungen: Überprüfung der Messgenauigkeit, EMV-Prüfung, Temperaturtests, Mechanische Belastungstests (z.B. Vibration), Speisespannungstests, usw.. Genügt die Messgenauigkeit und Zuverlässigkeit des Messmitteltyps der vorgesehenen Anwendung, wird eine Zulassung erteilt. Damit kann der Hersteller das Messmittel für diese Einsatzzwecke verkaufen.<br>**Anmerkung:** Ausländische Zulassungen werden anerkannt, sofern diese den schweizerischen Anforderungen entsprechen und die Gegenseitigkeit gewährleistet ist. |
| **3. Eichprüfung** |
| Kauft beispielsweise eine kantonale Polizeistelle ein solches Messmittel, so muss dieses vor Inbetriebnahme noch einer Eichprüfung bei einer vom Bundesrat ermächtigten Eichstelle unterzogen werden. Das Bundesamt für Metrologie und Akkreditierung (metas) legt die Eichvorschriften fest.<br>Die regelmässige Eichung gewährleistet, dass jedes einzelne Messmittel den gesetzlichen Vorschriften entspricht. Anschliessend an die Eichprüfung kann die Kontrollanlage in den Normalbetrieb übergehen.<br>**Wichtig:** Nur Messergebnisse von Anlagen mit gültiger Eichung sind gerichtsfest. |
| **4. Betrieb/Nacheichung** |
| Messmittel, welche sich im Betrieb befinden, müssen in vorgegebenen Zeitintervallen nachgeeicht werden. Die Eichfrist beträgt in der Regel 1 Jahr. Die Nacheichung erfolgt durch Eichstellen oder das metas. |

**Tabelle 1: Beschreibung Antrag/Zulassung/Eichung von Kontrollanlagen**

**Quelle: Beschreibung gem. Auskunft von Herrn Walter Fasel, Leiter Labor Verkehr beim metas**

# 4. Digitale Bilder und digitale Bildverarbeitung

Das folgende Kapitel gibt einen kurzen Einblick in die digitale Bildtechnik. Es dient lediglich als Grundlage für die folgenden Kapitel, und geht somit nur sehr bedingt auf die konkrete Anwendung im Enforcementbereich ein.

## 4.1. Entstehung von digitalen Bildern

Im Folgenden werden die Funktionsweisen sowie die Bestandteile von digitalen Standbildkameras und von Videokameras beschrieben. Nicht zuletzt soll das Kapitel auch zu einem einheitlichen Verständnis hinsichtlich des Begriffs Video(kamera) beitragen. Dieser wird - abhängig vom jeweiligen Zusammenhang - recht unterschiedlich verwendet.

### 4.1.1. Aufbau von digitalen Standbildkameras

Digitale Fotokameras halten im Gegensatz zu analogen Kameras das Aufnahmemotiv nicht auf einem Filmstreifen sondern auf einem elektronischen Speichermedium fest. Solche digitalen Geräte benötigen (ebenso wie „analoge“ Standbildkameras) ein Objektiv zur Abbildung des Motivs, ein Verschlusssystem (mechanisch oder elektronisch), ein Suchersystem (oft durch ein Display ergänzt oder ersetzt), einen Bildsensor, einen A/D-Wandler sowie einen Bildspeicher. Während in herkömmlichen Kameras das Licht selbst für die Informationsübertragung und –speicherung sorgt, kommen Digitalkameras nicht ohne Zusatzelektronik (z.B. A/D-Wandler) aus. Deshalb ist eine Stromversorgung zwingend notwendig. Die folgende Abbildung zeigt den groben Aufbau einer digitalen Standbildkamera:

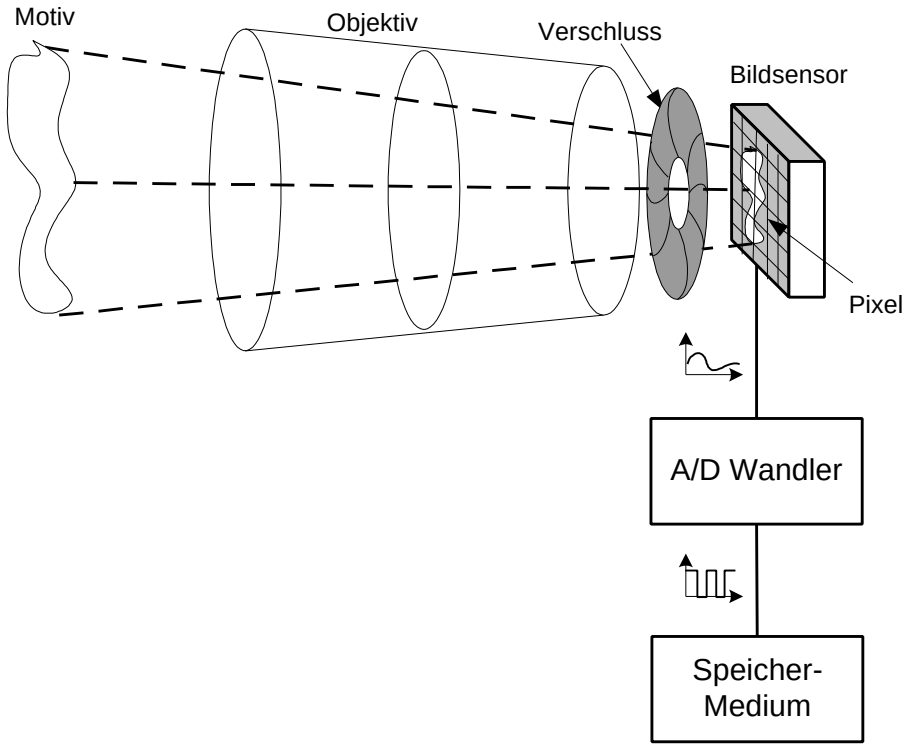



**Abbildung 6: Funktionaler Aufbau einer digitalen Standbildkamera**

Der Output einer digitalen Standbildkamera sind Datenpakete, welche jeweils die Informationen zu einem Bild beinhalten.

### 4.1.2. Aufbau von Videokameras

Im Gegensatz zu einer Standbildkamera wird der Bildsensor bei einer Videokamera ständig neu ausgelesen. Bei dem ausgelesenen Signal handelt es sich um ein analoges Signal. Erst durch einen nachgeschalteten A/D-Wandler entsteht ein digitaler Datenstrom. Der Output einer Videokamera ist somit eine dynamische Grösse.

Es ist aber auch möglich, aus einem (analogen) Videosignal Standbilder zu gewinnen. Dazu wird ein Framegrabber benötigt. Dieser ist in der Lage, einzelne Bildpakete aus dem Datenstrom herauszupicken und in eine digitales Datenpaket umzuwandeln. Damit kann eine Videokamera quasi als Standbildkamera eingesetzt werden. Ausserdem können Bilder kurzfristig zwischengespeichert und – das ist besonders interessant für Enforcementanwendungen – im Nachhinein herausgepickt werden. Der Entscheid, ob ein Bild erfasst, d.h. dauerhaft gespeichert werden soll, muss somit nicht zum Zeitpunkt, an dem ein Fahrzeug den Bildbereich passiert, gefällt werden.

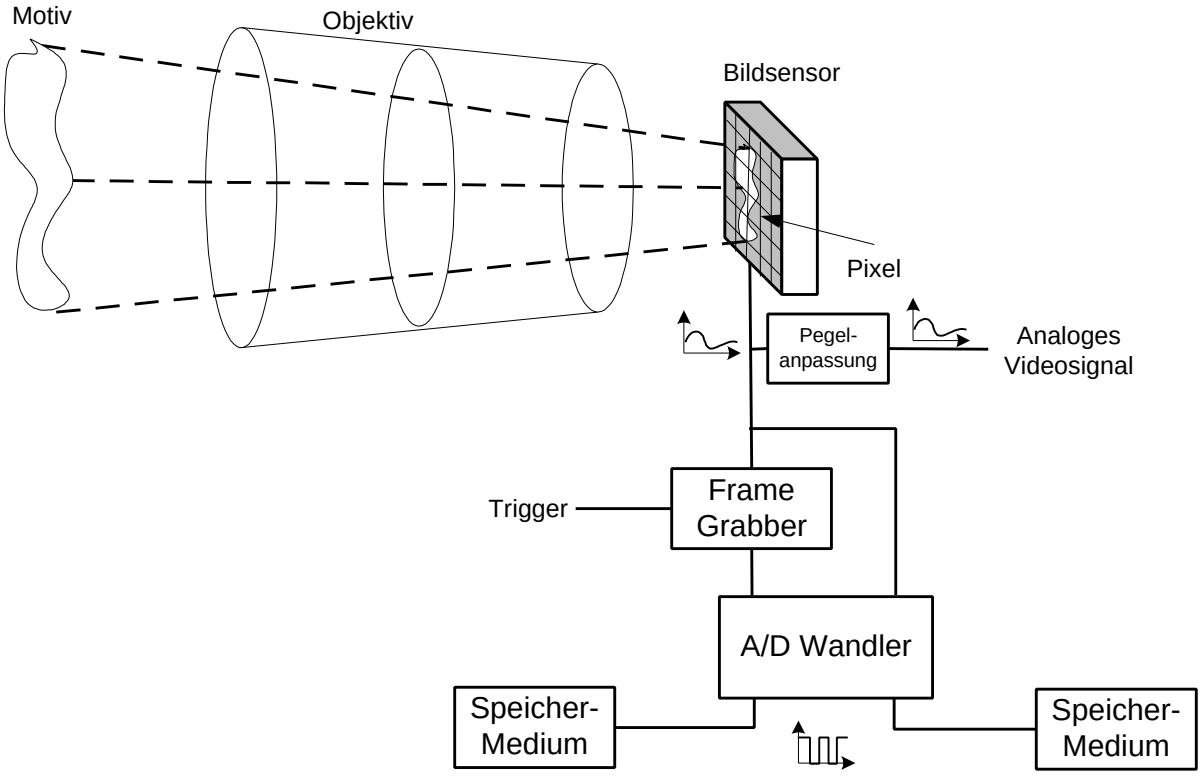



**Abbildung 7: Funktionaler Aufbau einer digitalen Videokamera mit Standbildfunktion**

Der Output einer Videokamera kann entweder:

- ein dynamisches, analoges Signal (Signal vom Bildsensor), oder
- ein dynamisches, digitales Signal (bei Einsatz eines A/D-Wandlers), oder
- ein statisches digitales Signal (bei Einsatz eines Framegrabbers) sein.

### 4.1.3. Komponenten

**Bildsensor**

Der Bildsensor ist das Herzstück der digitalen Kamera. Seine Qualität entscheidet letztlich über die Qualität der Bilder. Zu den wichtigsten Charakteristika zählen die Anzahl der Sensorzellen (Pixelauflösung) und die Empfindlichkeit des Bildsensors. Die Empfindlichkeit einer Digitalkamera ist – im Gegensatz zu einer herkömmlichen Wet-Film Kamera - ein konstanter Wert. Professionelle Kameras variieren die Empfindlichkeit, indem mehrere Pixel zu einem Bildpunkt zusammengefasst und damit die Fläche und letztlich die Empfindlichkeit pro Bildpunkt erhöht werden. Natürlich verringert sich durch diese Massnahme die Auflösung. Analog ist dies übrigens auch bei Wet-Filmen der Fall. Je grösser die Empfindlichkeit, desto höher die Korngrösse des Films.

Ein Bildsensor ist in viele Sensorelemente aufgeteilt. Diese wiederum bestehen aus einer lichtempfindlichen Fotozelle und einer Speicherzelle. Fotozellen wandeln Licht in elektrische Spannung um. Je grösser die Anzahl der Fotozellen, desto grösser wird die Bild- bzw. Pixelauflösung.

**A/D-Wandler**

Das vom Bildsensor gelieferte Signal ist analog. Um es auf einem digitalen Speichermedium ablegen zu können, muss das Signal zuvor digitalisiert werden. Diese Aufgabe übernimmt ein sogenannter Analog/Digital kurz, A/D-Wandler. Er quantifiziert das analoge Signal jedes Bildpunktes und macht so aus Analogwerten Bits und Bytes.

**Framegrabber**

Ein Framegrabber ist in der Lage aus einem dynamischen Videosignal einzelne Bilder herauszupicken. Anschliessend werden die Daten mit Hilfe eines A/D-Wandlers digitalisiert. Das so gewonnene digitale Standbild kann auf einem geeigneten Speichermedium abgelegt werden.

**Verschluss**

Genau gleich wie Wet-Film Kameras benötigen auch digitale Kameras einen Bildverschluss. Dieser steuert die Zeit, während welcher Licht (vom Motiv) auf den Bildsensor gelangt. Diese Verschlusszeit zusammen mit der Lichtstärke des Motivs ergeben den Wert, welcher vom Bildsensor letztlich gespeichert wird.

Im Gegensatz zu Wet-Film Kameras benötigen digitale Kameras nicht zwingend einen mechanischen Bildverschluss. Die Abdunklung des Bildsensors kann auch elektronisch erfolgen. Kameras auf dem professionellen Sektor sind jedoch nach wie vor mit einem mechanischen Verschluss ausgerüstet, da ein elektronischer Verschluss unerwünschte Restlichtwerte aufweist, welche das Bild verfälschen.

**Bildspeicher**

Die elektrischen Informationen auf dem Bildsensor werden ausgelesen und nachfolgend auf dem Bildspeicher abgespeichert. Als Bildspeicher einer kompakten digitalen Standbild-kamera können verschiedene Medien verwendet werden. Einige Beispiele:

- PC-Card (mini HD), Speicherkapazität: 200MB-1GB
- CompactFlash, Speicherkapazität: 2-512MB
- MiniatureCard, Speicherkapazität: 2-64MB
- SmartMediaCard, Speicherkapazität: 2-128MB
- MemoryStick, Speicherkapazität: 4-128MB

Bei fest installierten Kamerasystemen kann selbstverständlich der Bildspeicher direkt in einem Rechner untergebracht sein. Der Vorteil dabei ist, dass die Speicherkapazität um einiges grösser ist als bei den oben aufgelisteten Datenträgern.

→ Beim Video Enforcement werden praktisch ausschliesslich Videokameras mit Framegrabbing Funktion eingesetzt.

## 4.2. Kenngrössen

Der Informationsinhalt eines digitalen Bildes wird durch zwei Grössen gegeben:

- Anzahl der Pixel (Bildpunkte) pro Bildfläche
- Farbtiefe (Graustufen bei s/w Bildern)

Die folgende Abbildung zeigt, wie ein digitales Bild aus einzelnen Pixeln in verschiedenen Farbstufen aufgebaut ist.

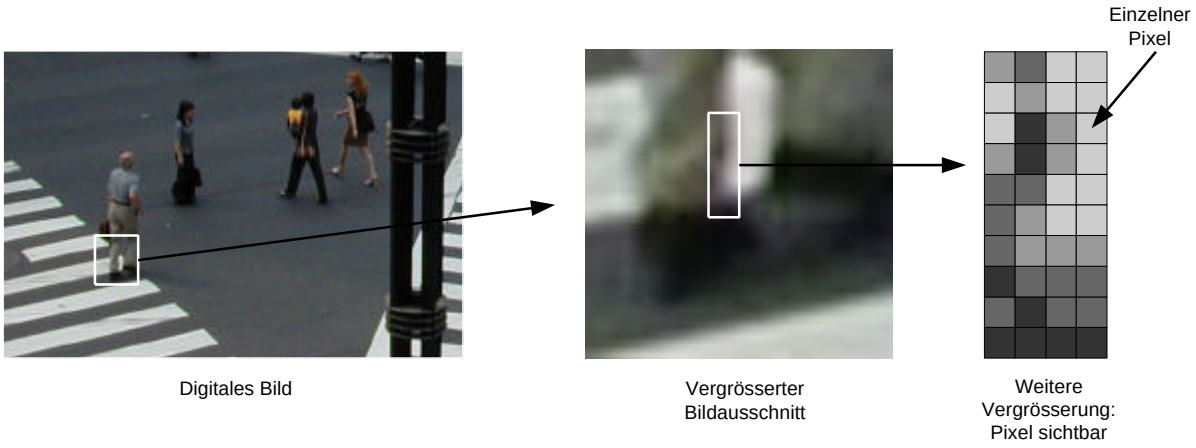



**Abbildung 8: Digitales Bild in Pixeln**

Beide Kenngrössen haben einen direkten Einfluss auf die Speichergrösse eines Bildes. Grundsätzlich gilt: Je grösser die Auflösung und die Farbtiefe, desto besser die Qualität des Bildes und desto grösser der Speicherbedarf. Durch geeignete Methoden kann der Speicherbedarf reduziert werden. So kann beispielsweise mit Strichbildern die Farbtiefe auf 1 bit reduziert werden. D.h. ein Bildpunkt kann nur entweder schwarz oder weiss sein. Eine andere, weniger drastische Massnahme ist die Verwendung von Farbpaletten. Dabei wird einem Byte nicht 256 Helligkeitsstufen einer einzigen Farbe, sondern 256 Farben zugeordnet. Bei diesem Verfahren müssen aber die Farbpaletten immer bekannt sein (Standardpaletten sind z.B. bekannt aus vielen Computeranwendungen). Geeignet ist dieses Verfahren vor allem für Bilder, welche ohnehin nur wenige verschiedene Farben enthalten.

Natürlich haben alle diese Verfahren eine Einbusse an Bildqualität zur Folge. Für die Verwendung im Bereich *Digitales Enforcement* dürften daher nur Graustufen- bzw. (RGB-) Farbbilder in Frage kommen.

Gängig bei der Bildauflösung sind im Moment Werte um 2 Mio Pixel. Bei der Farbtiefe sind 8-16 Bit gängig. Die Auflösung von Videokameras sind in der Regel schlechter als die von Standbildkameras. An der LSVA Pilotanlage werden beispielsweise Videokameras mit einer Auflösung von 1.2 Mio Pixeln und einer Farbtiefe von 8 Bit eingesetzt. Die Qualität der marktüblichen Geräte nimmt jedoch ständig zu (vgl. Home Elektronik Geräte).

→ Die Auflösung und die Farbtiefe sind die wichtigsten technischen Kenngrössen für ein digitales (Beweis-)Bild.

## 4.3. Speicherformate

Wie üblich in der Computerbranche gibt es auch für Grafiken und Bilder eine Vielzahl an verschiedenen Dateiformaten. Die folgende Auflistung beschränkt sich deshalb auf die derzeit am meisten verbreiteten Formate und erhebt keinen Anspruch auf Vollständigkeit.

| **Format** | **Beschreibung** |
|---|---|
| **Bildformate** | |
| JFIF<br>(Bekannt unter dem Namen JPEG) | JPEG steht für *Joint Photographic Expert Group*, ist also nicht der Name des Grafikformats, sondern der Name der Korporation, die das Format entwickelt hat. Das JPEG-Verfahren ist ein Kompressions-Algorithmus für Datenströme, der auf dem Algorithmus DCT (Diskrete Cosinus Transformation) in Verbindung mit der Huffman-Kodierung basiert. Das gleichnamige Dateiformat für Grafiken ist einfach eine Anwendung dieses Algorithmus auf Pixelgrafiken. Mittlerweile wird der JPEG-Algorithmus auch auf Videos angewendet und hat das beliebte Video-Format MPEG hervorgebracht. Das JPEG-Grafikformat komprimiert wie das GIF-Format ebenfalls sehr gut und hat gegenüber dem GIF-Format den Vorteil, dass es pro Bild bis zu 16,7 Millionen Farben speichern kann. Es arbeitet nicht wie das GIF-Format mit Farbpaletten bestimmter Farben, sondern mit dem gesamten Farbspektrum. Der Nachteil bei JPEG ist, dass es **mit Verlust komprimiert**. Je höher der Kompressionsfaktor, desto schlechter wird die Qualität der Grafik. Es sind Kompressionsraten von 20:1 und mehr möglich. Neben den reinen Bildinformationen können JPEG-Files auch Zusatzinformationen beigefügt werden, wobei der Inhalt von der jeweiligen Anwendung abhängig ist. |
| TIFF | Das *Tagged Image File Format* kurz TIFF ist ein häufig verwendetes Format im Bereich Desk Top Publishing um Dateien möglichst informationsreich zur be- und verarbeiten zu speichern oder weiterzugeben.<br>Das Format ist zu einem Format für alle Zwecke geworden. Es ist extrem flexibel und ermöglicht es so für praktisch jede Anwendung ein geeignetes Format zu generieren. Die Flexibilität macht das Format aber auch sehr komplex. Alleine die Originalspezifikation (TIFF Revision 6.0 vom 3. Juni 1992) umfasst 121 Seiten. Es ist dadurch leicht möglich, Fehler zu begehen, die zu Fehlinterpretationen führen. Selbst namhafte Hersteller von Grafikprogrammen sind kaum in der Lage, dieses Format in der ganzen Vielfalt zu überblicken.<br>Die Bildgrösse ist im TIFF Format auf ca. 4 Milliarden Bildzeilen beschränkt (sofern man dabei von einer Beschränkung sprechen kann). |
| GIF | GIF steht für *Graphics Interchange Format* und wurde schon vor vielen Jahren vom Online-Anbieter CompuServe eingeführt. Es zeichnet sich durch eine hohe Kompression aus. Deshalb hat es sich im Online-Bereich, wo die Übertragung von Daten Geld und Zeit kostet, schnell durchgesetzt. Der heute weit verbreitete Standard des GIF-Formats ist das so genannte „89er-Format“. Ein Nachteil des GIF-Formats ist die beschränkte Farbtiefe. Ein Pluspunkt ist dagegen, dass GIF-Grafiken verlustfrei komprimiert werden können. Aufgrund dieser Charakteristika ist das GIF-Format für hoch auflösende Grafiken wie Fotos nicht so sehr geeignet.<br>GIF-Dateien haben eine maximale Grösse von 16‘000 x 16‘000 Bildpunkten und eine Farbtiefe von 8bit (256 Farben). Es ist sowohl verlustfreie Komprimierung als auch verlustbehaftete Komprimierung nach JPEG-Standart möglich (ab Standart 6.0). |
| BMP | BMP wurde von Microsoft entwickelt und eingeführt (für die Benutzeroberfläche Windows 3.x). Da die wenigsten Programme die Komprimierung von BMP-Dateien zulassen, verliert das Format zunehmend an Bedeutung (zumindest für Windows unabhängige Anwendungen). |

| **Videoformate** | |
|---|---|
| MPEG | MPEG ist das zur Zeit wohl am meisten verbreitete Format für komprimierte Film(sequenz) Dateien. Um die riesige Datenmenge von Filmen (90 Minuten Spielfilm, 25 Einzel-Bilder pro Sekunde, hohe Auflösung, viele Farben ergeben ca. 120 GByte) mit "normalen" Computern verarbeiten und transportieren zu können, werden z.B. neben dem JPEG-Kompressions-Verfahren nur die Veränderungen zum Vorgängerbild abgespeichert (im Gegensatz zu M-JPEG): Das MPEG-Format speichert aber in regelmäßigen Abständen von typischerweise zwölf Bildern sogenannte Intra-Frames (I-Frames) ab; das sind JPEG-komprimierte Einzelbilder. Die Bilder zwischen diesen I-Frames werden nach Möglichkeit nicht komplett abgelegt. Vielmehr speichert MPEG, wie man sie durch Verschieben von Teilen aus vorangehenden oder nachfolgenden Bildern zurückgewinnen kann. Dazu werden auch vorausschauende "Predicted Frames" und "B-Frames" (Bi-directionale Frame) verwendet. Da das aber nie perfekt klappt, werden zusätzlich pro Bild die verbleibende Abweichung noch JPEG-kodiert abgespeichert. Mit dieser Methode lässt sich der Datenaufwand für einen Video-Film um etwa 99% verringern . Die mögliche Kompression geht bis 200:1.[2] |
| AVI | "Audio Video Interleave" bedeutet, dass Audio- und Videodaten ineinander verzahnt, also "interleaved" abgespeichert werden. Das AVI Format wurde von Microsoft als einheitliche Lösung für die Wiedergabe von kurzen Videoclips geschaffen, und basiert ursprünglich (1993) auf den Leistungsmerkmalen:<br>15 Bilder pro Sekunde bei einer maximalen Auflösung von 160 x 120 Pixeln.<br>Im Gegensatz zu anderen damals üblichen Animationsformaten wurde bei AVI die sogenannte Keyframe-Technik eingesetzt. Dabei wird lediglich jedes 12. bis 17. Bild (abhängig vom Bildinhalt) als Vollbild gespeichert. Für die dazwischen liegenden Frames werden nur die Unterschiede zum jeweils vorhergehenden Bild angegeben. Auch wenn diese ersten Definitionen alles andere als zukunftsträchtig klingen, gelang dem AVI-Format doch sehr schnell ein beachtlicher Siegeszug. Ein Grund dafür ist sicherlich die Tatsache, dass AVI als Bestandteil von "Video für Windows" bald fest mit Windows verknüpft war. Die entsprechenden Treiber standen und stehen für Endbenutzer kostenlos zur Verfügung. |

**Tabelle 2: Auflistung der gängigsten Bildformate**

→ Im Bereich Verkehrskontrollanlagen werden – sowohl beim Bildformat als auch bei Komprimierungsverfahren - primär proprietäre Formate eingesetzt. Diese stellen aber keine grundlegend neuen Verfahren dar, sondern bauen meist auf bekannten Verfahren auf. Nachteil von proprietären Systemen und Formaten ist die fehlende Portierbarkeit und die damit gegebene Abhängigkeit vom jeweiligen Hersteller.

## 4.4. Komprimierungsverfahren

Um die notwendige Speicherkapazität sowie die zur Übertragung benötigte Bandbreite zu reduzieren, werden Komprimierungsverfahren eingesetzt. Grundsätzlich können diese Verfahren in zwei Gruppen unterteilt werden:

- Reversible Algorithmen
- Irreversible Algorithmen

[2] Quelle: http://www.glossar.de

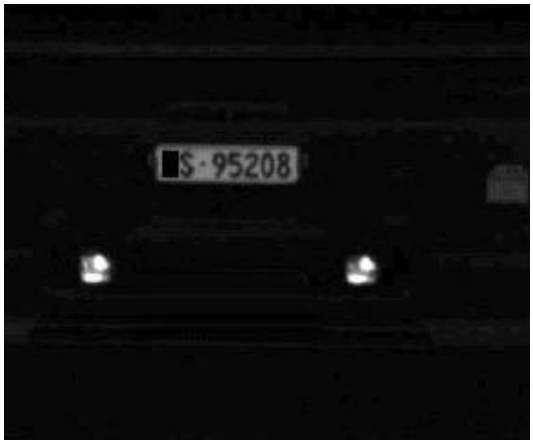
### 4.4.1. Reversible Algorithmen

Bei reversiblen Algorithmen können aus den komprimierten Daten die Ursprungsdaten wieder zurückgewonnen werden. Es handelt sich um eine sogenannte verlustfreie Komprimierung. Dabei wird die unveränderte Bildinformation in einem platzoptimierten Format abgespeichert. Besonders effektiv ist dieses Verfahren bei Bildern, wo grosse Farbflächen enthalten sind. Bei digitalen Fotografien ist der Nutzen gering, da u.a. aufgrund des Farbrauschens selten grössere Flächen mit exakt der selben Farbe vorkommen. Ein Bild, welches mit einem reversiblen Verfahren komprimiert wurde, kann immer wieder in den ursprünglichen Originalzustand gebracht werden. Die Komprimierung hinterlässt keine „Spuren“ im Bild.

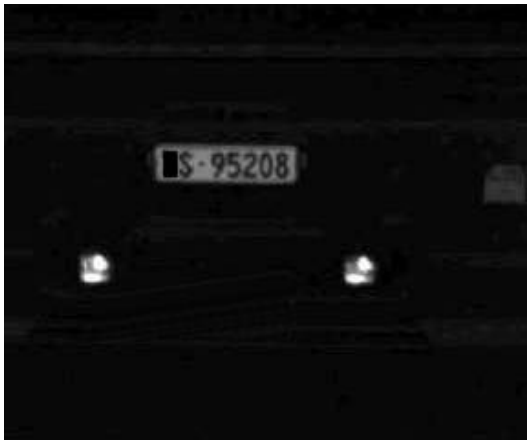
**Abbildung 9: Beispiel einer Fläche mit leichten Farbunterschieden**

### 4.4.2. Irreversible Algorithmen

Bei der Gruppe der irreversiblen Verfahren nutzt man die Schwächen der menschlichen Wahrnehmung aus und lässt Bildinformationen weg, welche durch unser Auge nicht oder nur schwer registriert werden können. Je stärker der Komprimierungsgrad (grosser Komprimierungsgrad = kleiner Speicherbedarf), desto eher sind die Eingriffe am Bild sichtbar. Beim Komprimierungsvorgang gehen Bildinformationen verloren. Nach der Anwendung eines irreversiblen Komprimierungsverfahrens können folglich die Originalbilddaten nicht mehr zurückgewonnen werden.




Komprimierung: 0%  Grösse: 24kByte




Komprimierung: 50% Grösse: 4kByte

Komprimierung: 90% Grösse 3kByte

Komprimierung: 95% Grösse: 2kByte

**Abbildung 10: Beispiel für den Komprimierungsgrad in JPEG**

Wie in Abbildung 10 ersichtlich ist, sind die Eingriffe am Bild je nach Komprimierungsgrad besser oder schlechter zu sehen. Sie können wie unten rechts zu sehen sogar zu Ziffernverfälschung (8 → 0) im Kontrollschild führen. Es gilt deshalb ein für die jeweilige Anwendung sinnvolles Mass an Komprimierung zu finden.

→ Komprimierung kann je nach Verfahren und Komprimierungsgrad den Inhalt verfälschen oder unkenntlich machen. Damit ergeben sich Einschränkungen für die Komprimierung von digitalen Bildern für die automatische Verkehrskontrolle.

## 4.5. Schutzmechanismen für digitale Daten

### 4.5.1. Das elektronische Wasserzeichen

Wasserzeichen sind in ein Bild eingebettete Signaturen, welche (meist von Auge nicht sichtbar) Aufschluss über Urheberrechtsdaten des Bildes geben.

Ein Wasserzeichen hat – ganz im Gegensatz zur Signatur – die Aufgabe, auch bei (unerlaubten) Eingriffen möglichst unverändert erhalten zu bleiben. Nur so lässt sich die Herkunft z.B. eines mit einem Wasserzeichen versehenen Bildes zweifelsfrei nachweisen. Im Bereich digitaler Bilder sind elektronische Wasserzeichen weit verbreitet. Sie werden insbesondere auch zur Verfolgung illegaler Kopien im Internet eingesetzt. Das am meisten verbreitete System in diesem Zusammenhang ist PictureMarc der Firma Digimarc (http://www.digimarc.com). Es findet beispielsweise auch in MS-Applikationen Verwendung.

Da beim digitalen Enforcement der Urheberrechtsaspekt wesentlich weniger wichtig ist als die Integrität der Daten, wird hier nicht weiter auf digitale Wasserzeichen eingegangen.

**Ziel des elektronischen Wasserzeichens: Urhebernachweis**

### 4.5.2. Signaturen

Signaturen werden überall dort eingesetzt, wo Daten vor unbemerkter Veränderung geschützt werden sollen. Sie dienen also der Authentisierung von Dokumenten bzw. Datensätzen. Mit Hilfe von Signaturen lässt sich zweifelsfrei nachweisen, dass sich ein Dokument oder Datensatz noch im ursprünglichen Zustand befindet. Zudem kann mit einer Signatur eindeutig nachgewiesen werden, wer (welche Person bzw. Anlage) die Signatur erzeugt hat.

Im Zusammenhang mit digitalen Bildern für die automatische Verkehrskontrolle sind Signaturen das ideale Werkzeug um die Authentizität der Datensätze zu beweisen. Dazu werden Bilder, Zusatzinformationen aber auch ganze Datensätze (mehrere Bilder +

Zusatzinformationen) mit Signaturen versehen, und sind so nachträglich als ein zusammenhängender Datensatz verifizierbar. Allerdings wirkt dieser Schutz erst nachdem die Signatur erzeugt wurde. Verwechslungen von Daten vor der Signierung sind somit nicht abgedeckt.

Eine Signatur entsteht, indem man zuerst einen Hash (=excerpt) über die zu signierenden Daten erstellt, und diesen Hash anschliessend verschlüsselt. Möchte man zu einem späteren Zeitpunkt die Authentizität überprüfen, so rechnet man den Hash über die Daten erneut. Anschliessend entschlüsselt man die Signatur und vergleicht den HashWert aus der Signatur mit dem selber errechneten. Sind beide Werte identisch, kann von der Authentizität der Daten ausgegangen werden.

**Wichtig:** Eine Signatur schützt einen Datensatz nicht vor unbefugter Einsicht, die Daten sind weiterhin in einem unverschlüsselten Zustand (Plain)! Die Signatur ist ein zusätzliches Informationselement, welches an den signierten Datensatz angehängt wird. Die Signatur schützt auch nicht vor einer Manipulation. Letztere kann aber mit Hilfe einer Signatur verifiziert werden. Die Signatur ist ein Hilfsmittel, mit welchem man die Unversehrtheit der signierten Daten nachweisen kann.

**Ziel der Signatur: Prüfbarkeit der Authentizität**

### 4.5.3. Verschlüsselung

Um Daten (insbesondere während der Übertragung) vor Einsicht durch Dritte zu schützen, werden sie verschlüsselt. Der Empfänger entschlüsselt die Daten anschliessend und erhält so den Klartext wieder. Massgeblich für den Grad an Sicherheit ist (neben dem Algorithmus) die verwendete Schlüssellänge. Dadurch wird bestimmt, wie viele mögliche Kombinationen für den Schlüssel in Frage kommen. Je länger der Schlüssel, desto schwieriger wird es für nicht Systemberechtigte die Nachricht zu entschlüsseln. Allerdings steigt mit der Schlüssellänge auch der Rechenaufwand bei der Ver- und Entschlüsselung.

Die folgende Abbildung zeigt das Prinzip der elektronischen Verschlüsselung. Dabei wird eine Nachricht mit einem Verschlüsselungsverfahren (kryptografischer Algorithmus) unter Verwedung eines Schlüssels so verändert, dass der Inhalt für Dritte nicht interpretierbar ist (Verschlüsselung). In dieser Form wird die Nachricht übermittelt. Der Empfänger kann dann mit Hilfe eines passenden Schlüssels die ursprüngliche Nachricht wieder zurückgewinnen (Entschlüsselung).

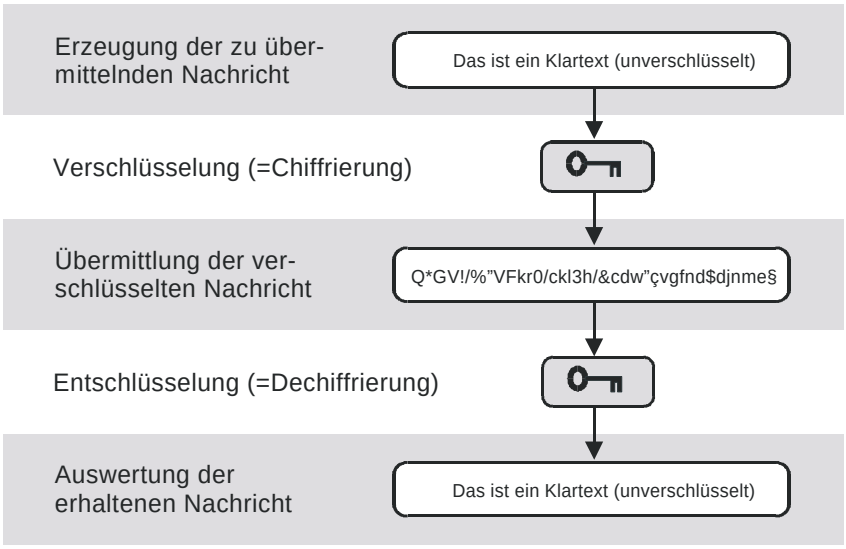



**Abbildung 11: Prinzipbild der Verschlüsselung**

Grundsätzlich kann zwischen zwei Arten der Verschlüsselung unterschieden werden:

**Symmetrische Verschlüsselung**

Von symmetrischer Verschlüsselung redet man, wenn sowohl für die Ver- als auch für die Entschlüsselung der gleiche Schlüssel verwendet wird. Dies bedingt, dass alle beteiligten Stellen im Besitz ein und desselben Schlüssels sind. Der Austausch muss dabei über einen sicheren Kanal geschehen, was in der Praxis ein Problem darstellt. Der Vorteil dieser Verfahren ist hingegen, dass sie relativ einfach zu handhaben sind. Die Algorithmen benötigen einen verhältnismässig kleinen Rechenaufwand.

DES und 3DES (gesprochen *Triple-Des*) sind die am meist verbreiteten symmetrischen Verschlüsselungsverfahren, wobei der 3DES lediglich eine dreifache DES-Anwendung mit zwei verschiedenen Schlüsseln ist.

**Asymmetrische Verschlüsselung**

Anders als bei symmetrischen existieren bei asymmetrischen Verfahren immer Schlüsselpaare: ein Private Key und ein Public Key. Dabei ist es nicht möglich, vom einen auf den anderen Schlüssel zu schliessen. Der Ablauf einer Übertragung mit asymmetrischer Verschlüsselung sieht folgendermassen aus:

1. Der Absender nimmt die zu versendende Nachricht und verschlüsselt sie mit dem Public Key des Empfängers. Dieser ist jedermann zugänglich.
2. Die verschlüsselte Nachricht wird übermittelt.
3. Der Empfänger entschlüsselt die Nachricht mit dem nur ihm bekannten Private Key.

Der Vorteil bei diesem Verfahren ist, dass der eigentlich wichtige Schlüssel (der Private Key) nach der Systeminitialisierung nie übergeben werden muss, da ihn nur eine Person benötigt. Ausserdem ist es mit Hilfe von asymmetrischen Verfahren möglich die Echtheit (Authentikation) eines Empfängers zu überprüfen, denn das Verfahren funktioniert in beide Richtungen. Also sowohl Verschlüsselung mit Private Key / Entschlüsselung mit Public Key als auch Verschlüsselung mit Public Key / Entschlüsselung mit Private Key. Hat nun ein Absender mit seinem Private Key verschlüsselt, und der Empfänger ist in der Lage die Nachricht mit dem Public Key des Senders zu entschlüsseln, kann der Empfänger sicher sein, dass die Nachricht vom angenommenen Absender stammt. Nur er bleibt im Besitz des Private Keys.

Der grosse Nachteil asymmetrischer Verfahren liegt im benötigten Rechenaufwand. Deshalb werden nur selten gesamte Dokumente, sondern vielmehr wichtige Teile wie Hash-Werte mit einem asymmetrischen Verfahren verschlüsselt.

Am meisten verbreitet bei den asymmetrischen Verfahren ist der RSA-Algorithmus.

Oft angewendet wird auch eine Vermischung von symmetrischen und asymmetrischen Verfahren. So wird die eigentliche Nachricht mittels eines symmetrischen Verfahrens verschlüsselt und verschickt. Der zur Entschlüsselung nötige symmetrische Schlüssel wird mit einem asymmetrischen Verfahren verschlüsselt und ebenfalls verschickt. Der Empfänger erhält durch Anwendung seines Private Keys den symmetrischen Schlüssel, mit welchem er das eigentliche Dokument entschlüsseln kann.

**Anmerkung:** Theoretisch kann jede Verschlüsselung durch Ausprobieren aller möglichen Schlüssel geknackt werden. Allerdings wächst der dafür notwendige Aufwand mit zunehmender Schlüssellänge drastisch an. Gleichzeitig wird mit steigender Schlüssellänge aber auch der Aufwand für Ver- und Entschlüsselung grösser. Es gilt ein für die jeweilige Anwendung optimalen Kompromiss zwischen Sicherheit und Aufwand zu finden.

**Ziel der Verschlüsselung: Schutz vor Dateneinsicht**

→ Security-Mechanismen sind wichtige Werkzeuge zum Schutz digitaler Daten. Insbesondere die Signatur (Integrität/Authentizität) sowie die Verschlüsselung (Schutz vor Einsicht) werden für die digitalen Datensätze in der automatischen Verkehrskontrolle Verwendung finden.

## 4.6. Bild-Nachbearbeitung

Im Gegensatz zu herkömmlichem Bildmaterial kann ein digitales Bild sehr einfach umfangreichen Nachbearbeitungen unterzogen werden. Im Zusammenhang mit digitalen Bildern für die automatische Verkehrskontrolle ist eine Nachbearbeitung aber allenfalls dann denkbar, wenn dadurch der Bildinhalt besser erkennbar wird. Konkret kann beispielsweise am Terminal der Enforcement Anlage des LSVA-Systems die Helligkeit, der Kontrast sowie der Gammawert der Bilder verändert werden. Dabei werden nicht die Originalbilddaten verändert, sondern lediglich die Darstellung am Bildschirm, damit eine bessere Lesbarkeit für den Bearbeiter entsteht. Es handelt sich folglich um eine reine „Anzeige-Hilfsfunktion".


Gamma-Wert = 1 Gamma-Wert = 2

**Abbildung 12: Beispiel für Bildnachbearbeitung**

Bei zukünftigen Anwendungen wäre es allenfalls denkbar, Teile aus dem Bild unkenntlich zu machen. Dies könnte insbesondere im Zusammenhang mit grenzübergreifendem Enforcement von Bedeutung sein.

→ Die Nachbearbeitung von digitalen Bildern kann verschiedenste Schritte beinhalten. Im Enforcementbereich dürften aber primär Verfahren im Anzeigebereich zur Anwendung kommen, welche die Analyse des Bildinhaltes vereinfachen.

# 5. Systemarchitektur

In diesem Kapitel geht es darum, den Enforcementvorgang durch ein geeignetes Modell zu beschreiben. Ziel ist eine Unterteilung das Gesamtprozesses in funktionale Teilblöcke. Das Modell soll einerseits eine Fokussierung auf die Kernpunkte ermöglichen, und andererseits die Grundlage für eine einheitliche Betrachtung schaffen.

## 5.1. Beschreibung und Analyse von beispielhaften Systemen

Eine Analyse von bereits bestehenden Enforcementsystemen soll Auskunft über deren Aufbau geben. Es gilt Parallelitäten der verschiedenen Systeme zu finden, um diese auf die Modellbildung zu übertragen.

### 5.1.1. Automatische Rotlichtüberwachungsanlage mit induktiven Schleifen


**Abbildung 13: Automatische Rotlichtüberwachung mit einer Induktivschleife hinter dem Haltebalken**

Automatische Rotlichtüberwachungsanlagen des im folgenden beschriebenen Typs werden in der Schweiz schon seit geraumer Zeit eingesetzt. Die Anlage ist ein typisches Beispiel einer Wet-Film Anwendung.

**Aufbau der Anlage**

Die Anlage besteht aus den folgenden Komponenten:

- Zwei induktive Schleifen
- Kamera zur Beweisbild-Aufnahme
- Logik zur Signalverarbeitung, Kamerasteuerung, Systemzeit, usw.

Die beiden induktiven Schleifen sind in einem definierten Abstand nach der Haltelinie angebracht. Die Schleifen geben ihr Signal an eine Kontrolleinheit weiter, welche sämtliche übrigen Komponenten beherbergt. Diese Einheit ist ausserdem mit der Steuerungseinheit des zu überwachenden Rotlichts verbunden. Von dort erhält die Überwachungsanlage die Information, in welchem Zustand (Rot, Orange, Grün) sich die Anlage jeweils befindet.

**Kontrollablauf**

Die Schleifen erkennen ein Fahrzeug, das die Haltelinie überfährt. Gleichzeitig wird die Geschwindigkeit des Fahrzeuges ermittelt. Die Kontrolleinheit erhält die Messwerte von den Schleifen und übernimmt dann die Auswertung. Die Anlage erstellt ein Bild, wenn:

- die Ampel Rot zeigt, und das Fahrzeug die Schleifen mit einer Geschwindigkeit von >8km/h passiert (die zweite Bedingung schützt vor ungewollten Aufnahmen in Stausituationen) → Widerhandlung = Missachtung des Rotlichts.
- die Ampel Grün zeigt, und das Fahrzeug die Schleifen mit einer Geschwindigkeit > der maximal zulässigen Geschwindigkeit passiert → Widerhandlung = Überschreitung der zulässigen Höchstgeschwindigkeit.

Nach einer definierten Zeit (typisch 0.5 oder 1 Sekunde) wird automatisch ein zweites Bild erstellt. Dieses wird benötigt, um die Bedingung einer zweiten unabhängigen Messmethode erfüllen zu können.

Alle wichtigen Messdaten und Informationen (Uhrzeit, Vorhaltezeit usw.) werden direkt in das Bild eingeblendet und mitfotografiert. Dieses Vorgehen verunmöglicht eine Verwechslung bei der Zusammenführung von Mess- und Bilddaten. Um auch den Anzeigezustand der Ampel nachträglich verifizieren zu können, wird die Ampel – per Lichtleiter - ebenfalls ins Beweisbild integriert.

Periodisch werden die (Wet-)Filmrollen bei der Station abgeholt und entwickelt. Dabei befinden sich jeweils eine grosse Anzahl von Bildern auf einer zusammenhängenden Rolle. Dieser Zusammenhalt wird als Nachweis für die Integrität und Authentizität des Beweisbildes verwendet und akzeptiert. Die Originalrolle wird deshalb am Stück für eine eventuell nötige spätere Beweisführung archiviert.

→ Die physische Verkettung der Bilder auf dem (Wet-)Film ist ein wichtiger Teilaspekt für den späteren Beweis der Echtheit der Bilder.

**Verarbeitung der Enforcementdaten**

In der Nachbearbeitung erfolgen grundsätzlich zwei Tätigkeiten:

- Manuelle Überprüfung bzw. Beurteilung des dokumentierten Vorganges.
- Ermittlung des Kontrollschildes aus den Bildern.

Bei der manuellen Überprüfung bzw. Beurteilung wird ermittelt, ob es sich tatsächlich um ein Missachten des Rotlichtes handelt, und ob der Verstoss durch die Beweisbilder eindeutig dokumentiert ist.

Wurde der Verstoss durch die manuelle Beurteilung bestätigt, so wird das Kontrollschild aus den Bildern gelesen. Dies kann manuell oder über automatische Kontrollschilderkennung erfolgen. Im letzteren Fall muss das Bild aber vorgängig digitalisiert (eingescannt) werden. Anschliessend wird der zugehörige Halter des Fahrzeuges ermittelt. Nun können die weiteren Verfahrensschritte eingeleitet werden.

### 5.1.2. Automatische Abschnittsgeschwindigkeitskontrolle

Die automatische Abschnittsgeschwindigkeitskontrolle ist eine typische Enforcement Anwendung, welche erst durch den Einsatz digitaler Bildtechnik möglich wird. Sie ist ein gutes Beispiel für die veränderten Abläufe gegenüber herkömmlichen Anlagen.

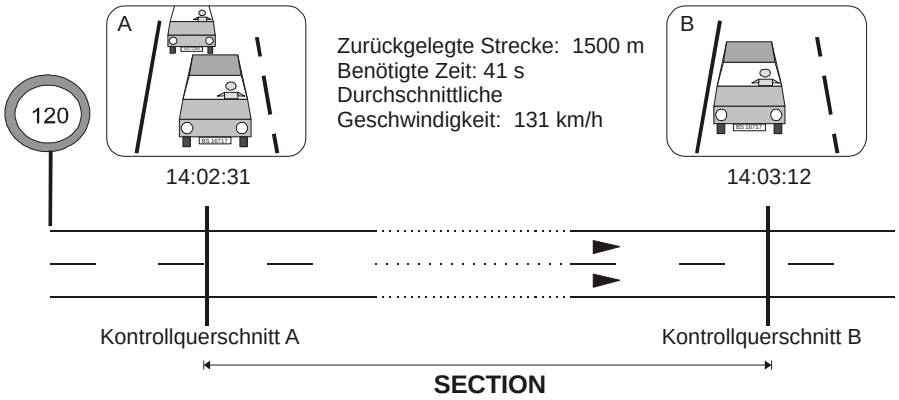



**Abbildung 14: Abschnittsgeschwindigkeitskontrolle**

**Aufbau der Anlage**

Die Anlage zur Abschnittsgeschwindigkeitskontrolle (AGK) besteht aus zwei Kontrollstellen, welche jeweils mit Kameras plus zugehöriger Beleuchtung und Triggerung ausgerüstet sind. Die beiden Stationen sind über eine Datenleitung miteinander verbunden. Eine der beiden Stationen verfügt zusätzlich über Auswertesoftware, mit welcher Bilder bzw. die darauf abgebildeten Fahrzeuge verglichen werden können. Eine Zentrale ermöglicht die Verwaltung und Verarbeitung der gesammelten Kontrolldaten.

**Kontrollablauf**

Ein Fahrzeug passiert die erste Kontrollstelle. Unabhängig von Geschwindigkeit und Art des Fahrzeuges wird ein Bild erstellt und die Durchfahrtszeit gespeichert. Der so erstellte Datensatz (Bild+Durchfahrtszeit) wird zur zweiten Kontrollstelle übermittelt, wo er temporär gespeichert wird. Auch hier wird von jedem Fahrzeug ein Bild erstellt sowie die Durchfahrtszeit gespeichert. Nun werden mit Hilfe einer Auswertelogik zusammengehörige Datensatzpaare gesucht. Der Vergleich erfolgt nicht anhand von Kontrollschildern, sondern anhand einem direkten Vergleich von Fahrzeugmerkmalen. Ist ein solches Datensatzpaar gefunden, wird anhand der Zeitdifferenz und der bekannten Distanz zwischen den beiden Stationen die Durchschnittsgeschwindigkeit des Fahrzeuges für den kontrollierten Abschnitt ermittelt. Ist diese innerhalb der erlaubten Limite, werden die Datensätze umgehend gelöscht. Wurde eine Übertretung erkannt, so werden die Daten an die Zentrale übermittelt.

**Verarbeitung der Kontrolldaten**

In der Kontrollzentrale erfolgt die Verarbeitung der Kontrolldaten. Überprüft wird insbesondere, ob die Zuordnung der beiden Bilder korrekt ist d.h. ob es sich tatsächlich auf beiden Bildern um dasselbe Fahrzeug handelt. Ausserdem muss überprüft werden, ob die Bilder den Anforderungen an die Beweiskraft gerecht werden (ist der Fahrer sowie das Fahrzeug eindeutig erkennbar?). Danach muss das Kontrollschild ermittelt werden. Dies kann entweder durch automatische Kontrollschilderkennung oder aber manuell erfolgen. Anschliessend können die weiteren Verfahrensschritte eingeleitet werden.

→ Die einzelnen Ablaufschritte können je nach Anwendung stark variieren.

## 5.2. Funktionales Modell

Das Ziel ist es nun, ein funktionales Modell für den gesamten Enforcementvorgang zu erstellen. Ein allgemein anwendbares Modell für *Digitales Enforcement* muss für alle technischen Realisierungen der drei Grundfunktionen geeignet sein. Das Modell darf, insbesondere was die chronologische Abfolge der Teilfunktionen angeht, keinesfalls einschränkend sein.

Bei Betrachtung der in Kapitel 5.1.1 und 5.1.2 beschriebenen Enforcementanwendungen lassen sich klare gemeinsame Funktionen erkennen. Diese Gemeinsamkeiten zeigen sich besonders deutlich, wenn die Abläufe in die drei folgenden Teilschritte unterteilt werden:

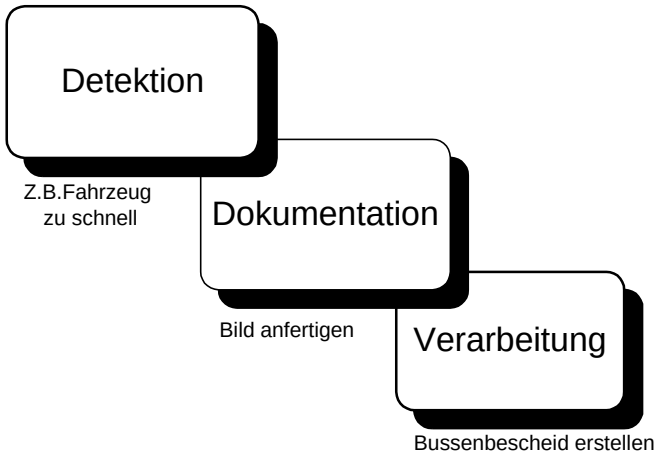



**Abbildung 15: Teilschritte im Enforcementvorgang**

Mit diesen drei Teilschritten kann das funktionale Modell beschrieben werden. Zur Verdeutlichung werden sie auf die zwei Enforcementbeispiele angewendet:

| **Teilfunktion** | **Autom. Rotlichtüberwachung** | **Abschnittsgeschw.kontrolle** |
|---|---|---|
| **Ereignisdetektion** | • Zustand: Ampel="rot" UND v>8km/h | • Zeitdifferenz zwischen Kontrollpkt.1 und Kontrollpkt.2 kleiner als zulässig |
| **Dokumentation** | **Erstellen**<br>• Beweisbilder (mit eingeblendeten Zusatzdaten) | **Erstellen**<br>• Beweisbild 1 (Kontrollpkt.1)<br>• Beweisbild 2 (Kontrollpkt.2)<br>• Zusatzdaten (errechnete Geschw., Datum/Zeit, Ort, usw.) |
| | **Übertragung**<br>• Abholen der Filmrolle | **Übertragung**<br>• Datenübertragung (z.B. über WAN) |
| | **Aufbewahrung**<br>• Lagerung der Filmrollen | **Aufbewahrung**<br>• Speichern der Daten auf geeignetem Medium. |
| **Verarbeitung** | • Manuelle Analyse des dokumentierten Vorganges.<br>• Ermittlung des Kontrollschildes aus den Beweisbildern | |

**Tabelle 3: Anwendung des Modells auf Enforcementbeispiele**

### 5.2.1. Ereignis-Detektion

Mit der Funktion Ereignis-Detektion wird festgestellt, ob und wenn ja in welchem Masse sich ein Verkehrsteilnehmer gegen bestehende Gesetze und Regelungen verhält (Widerhandlung).

Oft ist die Funktion Ereignis-Detektion nicht ein einzelner Schritt, sondern lässt sich in mehrere Einzelschritte unterteilen. Während im Beispiel unter 5.1.1. die Detektion aus einem einzigen Schritt besteht, ist im Beispiel 5.1.2. die Detektion in mehrere einzelne Teilschritte gegliedert. Um dieser Tatsache gerecht zu werden, muss der Begriff Ereignis-Detektion weiter aufgegliedert werden:

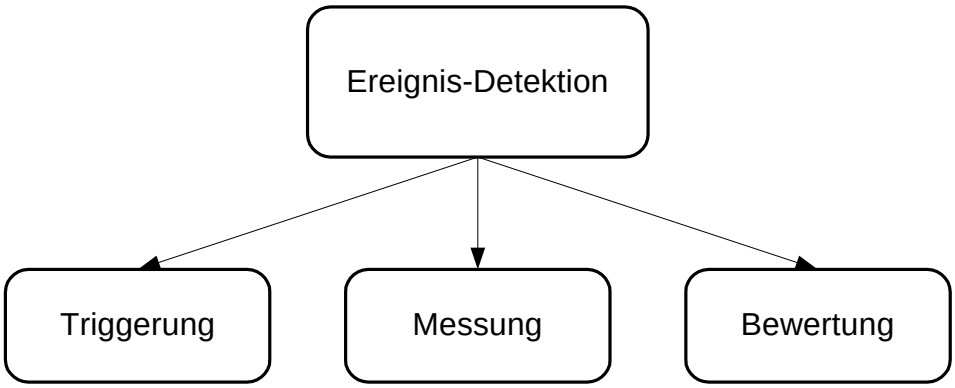



**Abbildung 16: Teilbereiche der Ereignis-Detektion**

Erklärung zu den Begriffen:

| Begriff | Erklärung |
|---|---|
| Ereignis-Detektion | Beschreibt den Gesamtvorgang bei welchem eine Widerhandlung festgestellt wird. |
| Triggerung | Auslösender Vorgang innerhalb des Enforcementvorgangs wie z.B. der Impuls zur Aufnahme eines Bildes. |
| Messung | Vorgang der lediglich einen Wert zurück liefert, aber für sich alleine noch keine Aktion auslöst. |
| Bewertung | Logischer Prozess zur Bewertung von Messergebnissen. |

**Tabelle 4: Begriffe Ereignis-Detektion/Triggerung/Messung/Bewertung**

### 5.2.2. Dokumentation

Bei der Dokumentation geht es darum, den detektierter Verstoss anhand von geeigneten Beweisdaten protokollieren. Die Teilfunktion Dokumentation kann in die drei folgenden Unterfunktionen unterteilt werden:

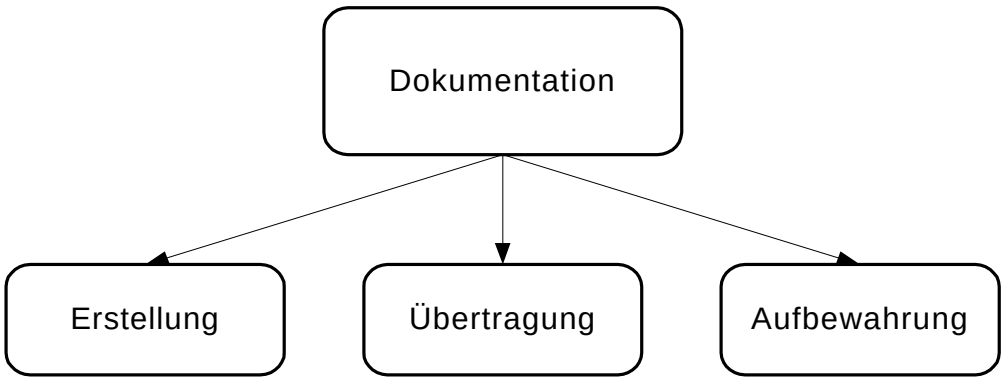



**Abbildung 17: Teilbereiche Dokumentation**

Erklärung zu den Begriffen:

| Begriff | Erklärung |
|---|---|
| Erstellung | Da es sich um eine automatische Kontrolle handelt - d.h. es bestehen keine ergänzenden Protokolle von vereidigten Personen o.ä. -, muss der erstellte Datensatz für sich den Verstoss zweifelsfrei dokumentieren. Im Fall des *Digitalen Enforcement* ist der Hauptbestandteil der Dokumentation das Beweisbild. Dieses kann bzw. muss jedoch durch weitere Angaben ergänzt werden wie: Messwerte, Parameter, Standort, Uhrzeit, usw. Unter Erstellen wird der Vorgang verstanden, bei welchem die Gruppierung der Daten erfolgt. |
| Übertragung | Der erstellte (Beweis-)Datensatz muss von der Kontrollanlage an den Ort der weiteren Behandlung (z.B. Kontrollzentrale) übermittelt werden. Dabei können die verschiedensten Übertragungsmedien eingesetzt werden: leitungsgebundene Übertragung, Funkübertragung, portable Speichermedien, usw. |
| Aufbewahrung | Am Bestimmungsort angelangt müssen die Datensätze in geeigneter Form abgespeichert/archiviert werden, so dass die nachgelagerte Verarbeitung sowie alle weiteren Bearbeitungsschritte erfolgen können. Darüber hinaus muss sichergestellt werden, dass sämtliche relevanten kryptografischen Schlüssel für die Zeitdauer der Aufbewahrung verfügbar bleiben. |

**Tabelle 5: Begriffe Erstellung/Übertragung/Aufbewahrung**

### 5.2.3. Verarbeitung

Die Verarbeitung beinhaltet sämtliche Bearbeitungsschritte nach der Übermittlung der Datensätze von der Kontrollanlage und kann folgendes umfassen:

- Überprüfung der von der Kontrollanlage gelieferten Resultate
- Ermittlung von Daten für die weitere Behandlung (z.B. Kontrollschild oder Fz-Halter)
- Nachbearbeitung von Bildmaterial
- Weitergehende Auswertung der Messdaten

Die Art und der Umfang der Verarbeitung hängt wesentlich vom jeweiligen Verfahren sowie von der Kontrollanlage ab. Eine eindeutige und umfassende Auflistung ist deshalb nicht möglich.

## 5.3. Datenstruktur

Systeme mit digitaler Bildverarbeitung müssen eine grosse Menge an Daten verarbeiten. Der korrekte Umgang mit dieser elektronischen Form von Beweismitteln ist folglich sehr entscheidend. Deshalb ist es bei der Betrachtung der Systemarchitektur eines Enforcement-systems unabdingbar, den Datensätzen eine klare und einheitliche Struktur zu geben.

Vergleicht man die in Kapitel 5.1.1 und 5.1.2 beschriebenen Enforcementanwendungen, so findet man auch in der Datenstruktur Parallelen. Ähnlich wie bei den einzelnen Schritten in der Beschreibung des Ablaufes ist auch bei den einzelnen Datenteilen eine Definition erforderlich. Im Folgenden werden die in Tabelle 6 aufgeführten Begriffe verwendet:

| **Begriff** | **Definition** |
|---|---|
| Datensatz | Dokumentationsdaten, welche einen Kontrollfall beschreiben. Der Inhalt des Datensatzes besteht seinerseits wieder aus einzelnen Datenbereichen s. 5.4. |
| Fall | Ein Fall beschreibt (auf administrativer Ebene) einen zu behandelnden Verstoss. Dieser kann allenfalls auch durch mehrere Datensätze beschrieben werden. |

**Tabelle 6: Definition Datensatz / Fall**

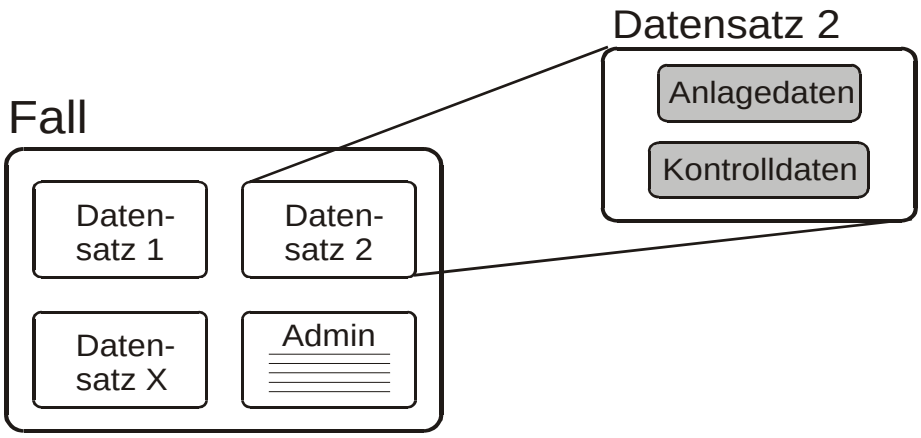



**Abbildung 18: Inhalt Fall / Datensatz**

Der Datensatz seinerseits besteht aus einzelnen Datenelementen. Die Elemente können in zwei Gruppen unterteilt werden:

| **Gruppe** | **Beschreibung** |
|---|---|
| Anlagedaten | Angaben zur Kontrolleinrichtung wie Anlagetyp, Version, Gerätenummer, Einstellungen, Status, usw. Diese Angaben sind unabhängig vom kontrollierten Fahrzeug. |
| Kontrolldaten | Angaben über oder vom kontrollierten Fahrzeug wie Geschwindigkeit, Deklarationsdaten, Kategorie, LPR/OCR-Resultat usw. Diese Daten werden für jedes kontrollierte Fahrzeug neu ermittelt. Zu den Kontrolldaten gehören auch digitale Bilddaten wie Einzelbild(er) und/oder Videosequenzen. |

**Tabelle 7: Gruppierung der Daten innerhalb eines Datensatzes**

## 5.4. Physische Struktur

Analog dem funktionalen Modell, kann auch das (physische) Gesamtsystem einer Enforcementanlage in mehrere Systemteile gegliedert werden. Es bietet sich eine Gliederung in folgender drei Teile an:

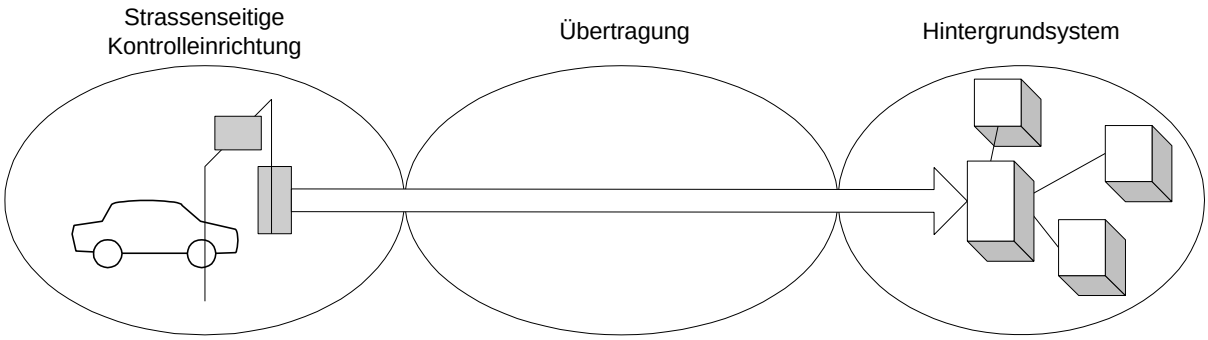



**Abbildung 19: Teilbereiche eines Enforcementsystems**

**Strassenseitige Kontrolleinrichtung**

Dieser Teil beinhaltet sämtliche Kontrolleinrichtungen vor Ort. Dazu gehören insbesondere die Bilderfassungsanlage, die Messeinrichtung(en) sowie allenfalls vorhandene Auswerteelektronik.

**Übertragungskanal**

Primär gemeint ist der Übertragungskanal zwischen der strassenseitigen Kontrolleinrichtung und dem Hintergrundsystem. Weitere Übertragungsstrecken sind jedoch nicht ausgeschlossen. Denkbar sind beispielsweise Verbindungen zwischen einzelnen Anlagekomponenten wie beispielsweise bei der Abschnittsgeschwindigkeitskontrolle.

**Hintergrundsystem**

Hier erfolgen die weitere Bearbeitung eines Datensatzes wie beispielsweise die manuelle Bestätigung des LPR/OCR Resultates, oder die Kontrolle des Klassifizierungsresultats. Weiter werden hier die Daten aufbewahrt bzw. verwaltet.

# 6. Analyse des Normierungsbedarfs

## 6.1. Abgrenzung des Normierungsbedarfs

Für die zu entwickelnde Norm stellt sich die Frage, welche Bereiche überhaupt von einer Norm beschrieben werden können bzw. sollten. Die in Kapitel 5.2 definierten drei Teilfunktionen:

- Detektion
- Dokumentation
- Verarbeitung

gilt es hinsichtlich Normierungsbedarf zu analysieren. Dabei muss die Betrachtung aus allen drei Blickwinkeln – Funktionaler Aufbau / Datenstruktur / Physischer Aufbau – erfolgen.

**Thema der Forschungsarbeit**

Gemäss Forschungsauftrag lautet der Titel dieser Arbeit „*Systeme für die automatische Verkehrskontrolle (Enforcement) mit digitaler Bildverarbeitung und automatischer Kontrollschilderkennung*“. Betrachtet man diesen Titel so würde man erwarten, dass die Norm zumindest die digitale Bildverarbeitung sowie die automatische Kontrollschilderkennung (LPR/OCR) beinhaltet bzw. behandelt. Betrachtet man andererseits das funktionale Modell, ist dies nicht mehr ganz so selbstverständlich.

**Was ist neu?**

Was ist das eigentlich neue an den hier behandelten Systemen? Es ist weniger die digitale Bildverarbeitung und der LPR/OCR Prozess, sondern der Einsatz von digitalen Bildern an automatischen Kontrolleinrichtungen. LPR/OCR kann (und wird) auch bei herkömmlichen Wet-Film Anlagen eingesetzt. Als einziger Unterschied muss das Bild zuvor eingescannt /digitalisiert werden. An dieser Stelle (Verarbeitung im Hintergrundsystem) ist aber der zentrale und wesentliche Vorgang schon abgelaufen. Das Beweisbild, welches alle wichtigen Informationen enthält, ist nämlich bereits in einer gerichtsfesten Form vorhanden. Die nachfolgende elektronische Bearbeitung ist folglich ein reines Hilfsmittel, welches aus rechtlicher Sicht eigentlich belanglos ist. Ob eine Person oder eine Maschine das Kontrollschild aus dem Beweisbild ermittelt, hat für den Verfahrensprozess nur beiläufigen Charakter. Entscheidend ist vielmehr, was auf dem Beweisbild bzw. mit dem Beweisdatensatz tatsächlich dokumentiert ist.

**Fazit**

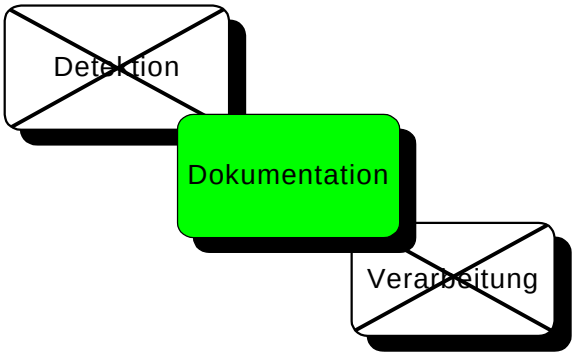
Übertragen auf die definierten Teilfunktionen heisst das, dass der entscheidende Vorgang innerhalb des Gesamt-Enforcement Prozess die Dokumentation ist. In diesem Schritt wird der entscheidende Beweisdatensatz erstellt, übertragen und abgelegt. Dabei gilt es mit geeigneten Massnahmen zu garantieren dass:

- Der Datensatz von einer autorisierten Stelle stammt.
- Die Integrität des Datensatzes garantiert ist.
- Die Daten (insbesondere bei der Übertragung) nicht von Dritten eingesehen werden können.

Dagegen besteht in der Teilfunktion Verarbeitung kein Normierungsbedarf, da sich durch den Einsatz von digitalen Beweisbildern keine bedeutenden Änderungen betreffend der Normierung ergeben.

Für die letzte verbleibende Teilfunktion – der Detektion – ist die Situation vergleichbar der Verarbeitung. Auch die Art und Weise der Detektion ist schlussendlich für die Betrachtung des Beweisdatensatzes nebensächlich. Bei der Triggerung über das Videobild handelt es sich beispielsweise um ein neues Messverfahren. Dieses hat aber mit dem digitalen (Beweis-) Bild eigentlich nichts zu tun. Natürlich müssen auch die Detektionsmittel den nötigen Anforderungen entsprechen, aber diese Anforderungen sind unabhängig von der Art und Beschaffenheit des Beweisdatensatzes, welcher hier im Mittelpunkt steht.

→ Eine Norm muss primär den Bereich Dokumentation (Erstellung/Übertragung/Aufbewahrung) abdecken.




## 6.2. Anpassungsbedarf an den bestehenden rechtlichen Grundlagen

### Verkehrszulassungsverordnung

Da in der Verordnung lediglich festgehalten wird, dass die Regelungen bezüglich automatischen Kontrollen in entsprechenden technischen Weisungen erfolgen, bedarf es keinerlei Anpassungen für die Verwendung digitaler Bildtechnik bei der automatischen Verkehrskontrolle.

### Technische Weisungen

Folgende Stellen sind im Zusammenhang mit dem möglichen Einsatz von *Digitalem Enforcement* von Bedeutung:

| **Weisung über Rotlicht-Überwachungsgeräte** |
|---|
| **Ziffer 3.5 Funktionskontrolle bei Standort- oder Filmwechsel**<br>Nach jedem Standortwechsel des Gerätes und bei jedem Filmwechsel ist das richtige Funktionieren der Anlage zu überprüfen.<br>**→ Bei digitaler Bilderfassung entfällt der Filmwechsel.** |
| **Ziffer 4.5**<br>Die auf dem Bild registrierte Zeit (seit Rotbeginn) darf nicht kürzer als die eingestellte Verzugszeit von mindestens 0.5 Sekunden sein.<br>**→ Bei digitaler Bilderfassung besteht technisch gesehen die Möglichkeit Zusatzdaten (wie die registrierte Zeit) nicht direkt ins Bild zu integrieren, sondern lediglich als (nicht visualisierten) Teil des Datensatzes zu übergeben. Bei der jetzigen Formulierung wird diese Möglichkeit nicht in Betracht gezogen.** |

**Tabelle 8: Änderungen technische Weisung Rotlicht-Überwachung**

Die technischen Weisungen gehen grundsätzlich vom Einsatz von Wet-Filmen aus - ohne dabei den Einsatz von digitalen Bildererfassungs-Verfahren auszuschliessen - und müssten entsprechend überarbeitet werden. Die obige Auflistung zeigt aber, dass sich die notwendigen Anpassungen in einem bescheidenen Rahmen bewegen werden.

**Anmerkung:** Dies gilt nicht für die Ergänzung gänzlich neuer Messverfahren wie der Abschnittsgeschwindigkeitskontrolle. Hier müsste die Weisung entsprechend ergänzt werden.

→ Die notwendigen Anpassungen sind verhältnismässig bescheiden. Insbesondere deshalb, weil die entsprechenden Verordnungen und Weisungen sehr funktional gehalten sind. Grundsätzlich genügt es, mit Hilfe einer Norm die Rahmenanforderungen an Enforcementanlagen mit digitalem Bildeinsatz zu formulieren. Wichtig dabei ist vor allem, dass alle denkbaren Anwendungen (auch ausserhalb des Strassenverkehrsgesetzes) auf diese Norm aufbauen können.

# 7. Anforderungen an Bilder und Datensätze

Nachdem der Normierungsbedarf hinsichtlich der einzelnen Teilfunktionen analysiert wurde (vgl. Kapitel 6), gilt es nun konkrete Auswirkungen und Anforderungen für den Bereich *Dokumentation* zu ermitteln.

## 7.1. Funktionale Anforderungen an die Enforcement-Datensätze

Da im Falle von automatischen Verkehrskontrollen keine vereidigten Personen anwesend sind, muss der Datensatz als alleiniges Beweismittel tauglich sein. Damit ergeben sich drei primäre funktionale Anforderungen an diesen:

**Prüfbare Authentikation**
Der Beweis-Datensatz muss prüfbar von einer autorisierten Stelle (Anlage) stammen, d.h. es muss mit geeigneten Mitteln möglich sein, den Ersteller des Datensatzes zu verifizieren. Damit soll sichergestellt werden, dass keine falschen Datensätze ins System eingebracht werden können. Ausserdem ist die Identifikation der erzeugenden Stelle unabdingbar für die spätere Nachvollziehbarkeit.

**Prüfbare Integrität**
Der Datensatz muss sich nachweislich in einem unversehrten Zustand befinden. Dazu gehören zwei Prüfungen:

- Befindet sich der Datensatz als Gesamtes in unversehrtem Zustand? D.h. wurden seit Erstellung des Datensatzes an der Kontrollanlage Datenelemente entfernt oder zugefügt?

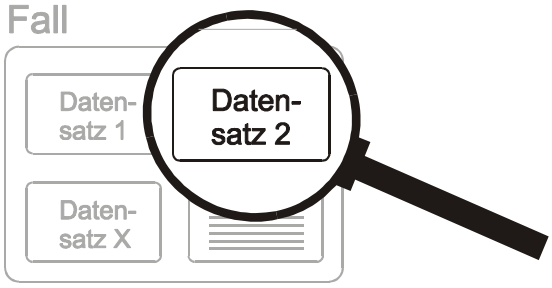



**Abbildung 20: Integrität des Datensatzes**

- Befinden sich alle einzelnen Datenelemente aus dem Datensatz (Bilddaten, Anlagedaten und Fahrzeug-Kontrolldaten) in ihrem ursprünglichen, unversehrten Zustand?

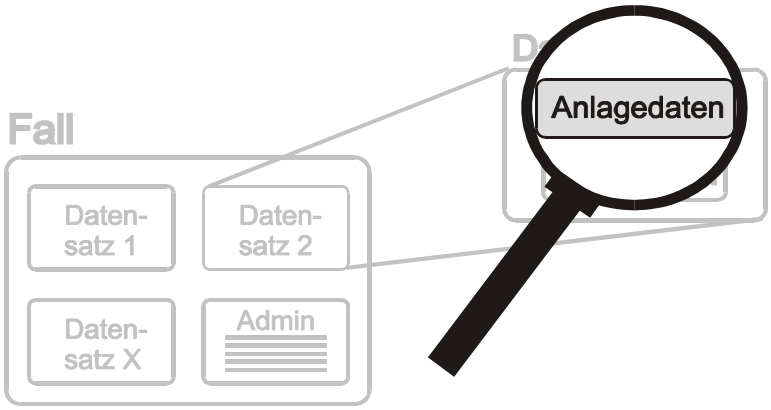



**Abbildung 21: Integrität der Datenelemente**

Die Überprüfung der Authenikation und der Integrität hat zwingend vor der Nachbearbeitung zu erfolgen. Wird bei der Überprüfung festgestellt, dass eine Verletzung der Authentikation / Integrität vorliegt, muss dies auf dem Beweisbild (bzw. den Beweisbildern) visuell sichtbar gemacht werden, z.B. durch das Einfügen eines entsprechenden Symbols in das Bild.

**Abbildung 22: Beispiel für die Kennzeichnung einer Integritätsverletzung**

**Vollständige Dokumentation der Widerhandlung**
Der Datensatz muss die erfolgte Widerhandlung vollständig dokumentieren. Dabei kommt dem (digitalen) Bild hauptsächliche Bedeutung zu. Die Anforderungen an den funktionalen Bildinhalt können je nach Anwendung variieren (Kontrollschild identifizierbar, Fahrzeuglenker identifizierbar, Fahrzeugkombination erkennbar, usw.).

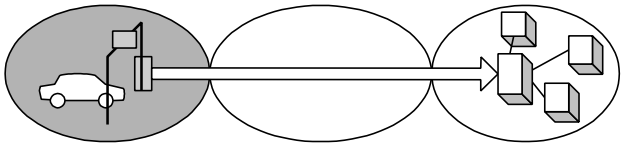
***Anmerkung:*** *Neben den funktionalen Anforderungen an die Datensätze, bestehen auch Anforderungen an die Behandlung derselben. Insbesondere zu erwähnen gilt es dabei die Anforderungen hinsichtlich Datensicherheit. Da es sich bei Enforcement Daten um persönliche und damit schützenswerte Daten handelt, müssen sie jederzeit vor Zugriff durch Dritte geschützt werden. Dies gilt insbesondere auch bei der Übertragung der Daten.*

→ Erst wenn ein Datensatz den Ansprüchen an Authentikation, Integrität und Dokumentation der Widerhandlung gerecht wird, kann er als Beweismittel verwendet werden. Des weiteren müssen Datenschutzaspekte berücksichtigt werden.

## 7.2. Anforderungen bezüglich Datenschutz und -sicherheit

Bei Enforcementdaten handelt es sich grundsätzlich um besonders schützenswerte Personendaten, welche vor Einsicht durch Dritte geschützt werden müssen. Dieser Schutz muss in allen Teilbereichen des Systems gewährleistet sein.

### 7.2.1. Zugriffsschutz der strassenseitigen Kontrolleinrichtung



Unter der strassenseitigen Kontrolleinrichtung werden sämtliche Komponenten am Kontrollort bis und mit Schnittstelle zum Übertragungskanal verstanden (Kameras, Sensoren, Beleuchtung, Lokale Speichereinheit, usw.). Die strassenseitige Kontrolleinrichtung muss folgende Anforderungen bezüglich Datenschutz erfüllen:

- Schutz vor unbefugten Eingriffen in die Systemkomponenten.
- Ausschliesslich temporäre Speicherung von Daten.

**Schutz vor unrechtmässigen Eingriffen an Systemkomponenten**

Die Komponenten der strassenseitigen Einrichtung müssen gegen unbefugten Zugriff geschützt sein. Im Minimum bedeutet dies einen mechanischen Zugriffsschutz. Allfällige Schnittstellen zu ungeschützten Netzen (vgl. Kapitel 7.2.2) müssen zudem über Schutzmechanismen für Zugriffe auf das System verfügen (Prinzip Firewall).

Neben dem Zugriffsschutz müssen die Komponenten auch über eine Zugriffsüberwachung verfügen. Diese muss einen Zugriff – insbesondere einen unberechtigten – wirkungsvoll erkennen und „dokumentieren". Je nach Art der Anlage können das sein:

- Verplombung von Gehäuseöffnungen
- Endkontakte an Gehäuseöffnungen → Alarm
- Bewegungsmelder in Anlagecontainern → Alarm
- Logfile zur Dokumentation der Systemzugriffe

Die Logfiles müssen insbesondere auch Wartungs- und Updatezugriffe dokumentieren. Als Wartung gelten Eingriffe bei welchen die Anlagesoftware bzw. deren Zertifikat erhalten bleibt (z.B. Einstellungen am Betriebstimer). Bei Updatezugriffen wird die Software verändert, was nicht mehr unter den Begriff Wartung fällt. Dieser Zugriff erfordert eine erneute Abnahme und Eichung der Anlage bzw. der Software. Sämtliche Wartungs- und Updatezugriffe müssen im entsprechenden Logfile vollständig dokumentiert werden.

Sind diese Anforderungen an Zugriffsschutz und Überwachung erfüllt, kann von einer geschützten Umgebung innerhalb einer Systemkomponente gesprochen werden.

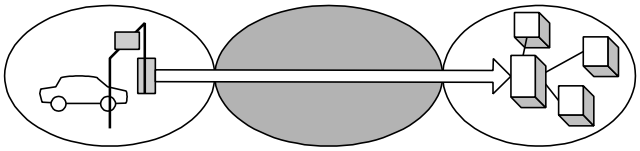
→ Strassenseitige Kontrolleinrichtungen müssen wirkungsvoll vor unbefugten Zugriffen aller Art geschützt sein. Ausserdem müssen unrechtmässige Zugriffe zuverlässig erkannt und eindeutig gegenüber rechtmässigen Zugriffen differenzierbar sein.

**Temporäre Speicherung von Daten**

Da die strassenseitige Kontrolleinrichtung nur begrenzt überwachbar ist, sollten Enforcementdaten so bald wie möglich an eine zentrale Stelle übermittelt und an der Anlage gelöscht werden. Auf keinen Fall dürfen Daten an der Station aufbewahrt werden. Mit diesem Vorgehen wird die Gefahr minimiert, dass Daten an der Kontrollstelle verloren gehen (z.B. bei Systemstörungen) oder dass ein unbefugter Zugriff/Manipulation erfolgt.

→ Enforcementdaten sollen nur so lange wie unbedingt nötig an den Kontrollanlagen gespeichert bleiben.

### 7.2.2. Zugriffsschutz bei der Datenübertragung



Mit Übertragung versteht man im Wesentlichen die Verbindung zwischen Kontrolleinrichtung und Hintergrundsystem. Es kann aber auch innerhalb der Anlage oder dem Hintergrundsystem zu Datenübertragungen kommen. Beispiel ist die Verbindung zwischen den beiden strassenseitigen Kontrolleinrichtungen bei einer Abschnittsgeschwindigkeits-kontrolle.

Es wird zwischen zwei verschiedenen Übertragungskanälen unterschieden:

- geschützter Übertragungskanal
- ungeschützter Übertragungskanal

**Geschützter Übertragungskanal**

Ein geschützter Übertragungskanal muss so gestaltet sein, dass ein Zugriff durch Dritte wirkungsvoll verhindert wird. Dabei spielt es keine Rolle, welches physikalische Übertragungsmedium verwendet wird (Kupfer/Glasfaser/Funk). Anforderung ist, dass ausschliesslich autorisierte Personen oder Stellen möglichen Zugriff auf das Netz und die darauf übertragenen Daten haben. Des weiteren muss es sich um einen geschlossenen Benutzerkreis handeln. Ein typisches Beispiel eines geschützten Übertragungskanals ist das Glasfasernetz der Stadtpolizei Zürich (physikalisch entkoppeltes Netz).

Werden solche geschützten Übertragungskanäle für die Datenübertragung eingesetzt, müssen die Enforcementdaten für die Übertragung nicht mehr zusätzlich verschlüsselt werden. Für die Anforderungen bezüglich Mechanismen zur Prüfbarkeit der Authentikation und Integrität hat das jedoch keinen Einfluss.

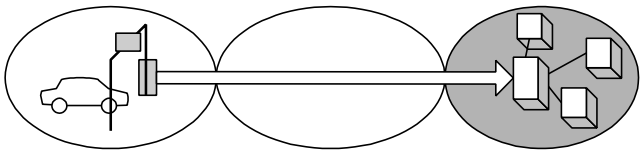
**Ungeschützter Übertragungskanal**

Unter einem ungeschützten Übertragungskanal werden Verbindungen verstanden, welche über keine speziellen Zugriffsrestriktionen verfügen. Ein typisches Beispiel für einen ungeschützten Übertragungskanal ist das Internet.

Werden ungeschützte Übertragungskanäle für die Datenübertragung eingesetzt, müssen die zu übertragenden Daten vor Einsicht geschützt werden. Zu diesem Zweck sollen die Daten verschlüsselt werden, wobei Verschlüsselungsalgorithmen eingesetzt werden sollen, welche nach Stand der Technik als sicher zu betrachten sind.

→ Werden Enforcementdaten auf einem ungeschützten Übertragungskanal übertragen, so müssen sie verschlüsselt werden. Bei Übertragung auf einem geschützten Kanal ist eine Verschlüsselung nicht zwingend erforderlich.

### 7.2.3. Zugriffsschutz im Hintergrundsystem



Im Hintergrundsystem werden die Enforcementdaten aufbewahrt. Ausserdem erfolgt hier die Nachbearbeitung und weitere Behandlung der Fälle. Auch in dieser Umgebung müssen die Daten vor unberechtigtem Zugriff geschützt sein. Auf das System und somit die Daten dürfen nur berechtigte Personen zugreifen können. Zugriffe und wichtige Nachbearbeitungsschritte sollten so dokumentiert werden, dass die Nachvollziehbarkeit jederzeit möglich ist.

→ Der unbefugte Zugriff auf Enforcementdaten muss im Hintergrundsystem wirkungsvoll unterbunden werden.

## 7.3. Anforderungen bezüglich Integrität und Authentizität

Um einen Datensatz als Beweismittel verwenden zu können, muss nachweisbar sein, dass die einzelnen Bestandteile tatsächlich zum Datensatz gehören. So muss beispielsweise sicher sein, dass die Messwerte auch tatsächlich zu dem auf den Bilddaten sichtbaren Fahrzeug gehören. Ausserdem gilt es durch geeignete Massnahmen zu verhindern, dass Daten unbemerkt verändert oder ausgetauscht werden können.

Bisher wurde (bei Video-Enforcement) diesen Anforderungen dadurch Rechnung getragen, dass die entsprechenden Daten auf dem Bild eingeblendet und mit fotografiert wurden. Dies ist zwar auch bei digitalen Bildern möglich, muss aber nicht mehr zwingend der Fall sein.

→ Der Datensatz muss mit einer elektronischen Signatur versehen werden, um dessen Integrität überprüfbar zu machen. Je nach Architektur der Anlage ist es allenfalls auch sinnvoll/nötig einzelne Teile zusätzlich separat zu signieren.

Zusätzlich müssen sämtliche Datenelemente mit Zeitstempeln versehen sein. Dies ermöglicht es zu überprüfen, ob die einzelnen Datenelemente vor der Signierung richtig zusammengefügt wurden.

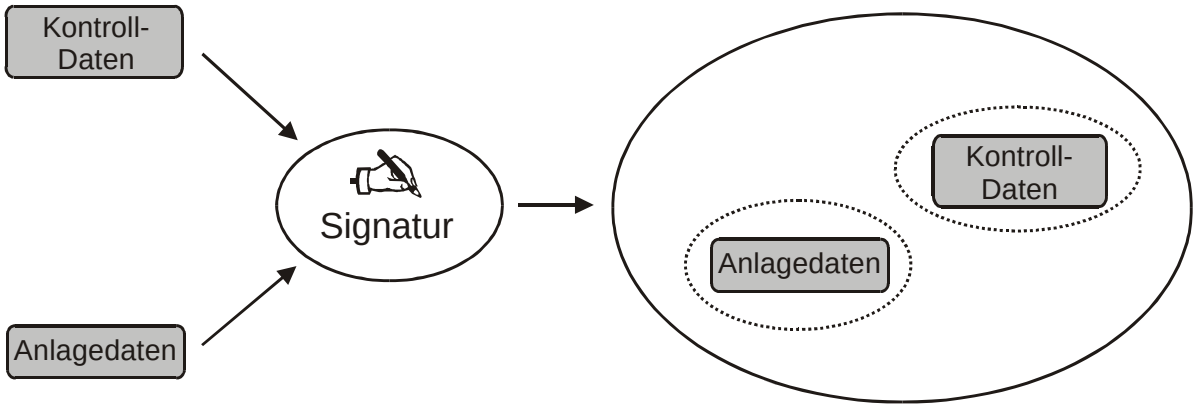



**Abbildung 23: Signierung des Datenpakets**

Im Normalfall machen die Kontrolldaten, welche auch die Bilddaten enthalten, einen Grossteil des Gesamtspeicherbedarfs eines Datensatzes aus. Daher kann es in manchen Fällen sinnvoll sein, dass ein Datensatz ohne das Bild erstellt wird. Im Datensatz enthalten ist dann lediglich ein Verweis auf die Bilddatei, welche bei Bedarf separat geladen werden kann. In diesem Fall muss sichergestellt werden, dass das Bild nicht nachträglich – d.h. nach Erstellen des Datensatzes – ausgetauscht werden kann.

Zu diesem Zweck muss der Dateiname in die Signatur mit einbezogen werden. Zuerst wird also das Bild inklusive Dateiname signiert. Anschliessend werden die Anlagedaten, die Kontrolldaten und die Signatur des Bildmaterials signiert.

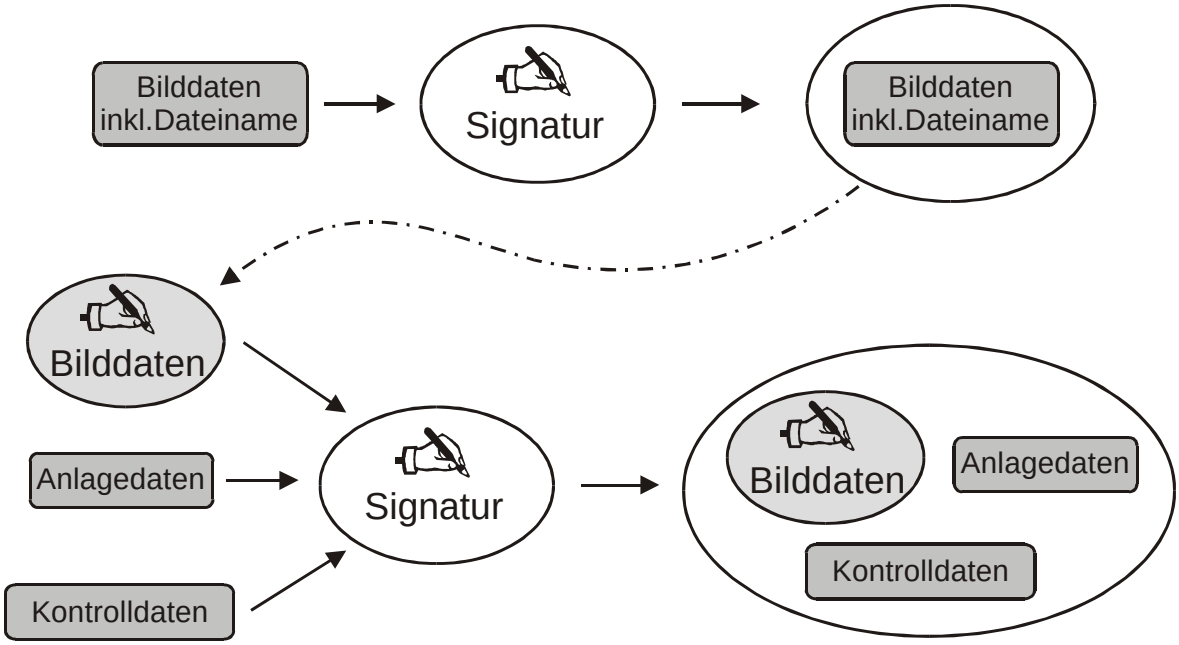



**Abbildung 24: Signierter Datensatz mit getrennten Bilddaten**

Nun können die Bilddaten separat abgelegt und verwaltet werden, ohne dabei die Integrität des Datensatzes zu gefährden. Dieses Prinzip funktioniert natürlich nicht nur bei den Bilddaten, sondern könnte beispielsweise auch für die Anlagedaten angewandt werden.

**Anmerkung:** Der Datensatz besteht auch bei einer solchen Aufsplittung weiterhin aus Anlagedaten + Kontrolldaten.

## 7.4. Anforderungen an die Nachbearbeitung

Bilddaten werden im Zuge der Verarbeitung unter Umständen gewissen Nachbearbeitungen unterzogen. Da mit jeglicher Bearbeitung des Bildes die Signatur und damit die Integrität/Authentizität verloren geht, dürfen Manipulationen in keinem Fall am Originaldatensatz vorgenommen werden. Dieser muss in jedem Fall in unveränderter Form erhalten bleiben. Nur so kann jederzeit nachgewiesen werden, dass es sich um einen „echten“ Datensatz handelt.

→ Der Original- Beweisdatensatz muss in jedem Fall unverändert gespeichert werden.

## 7.5. Anforderungen an die Aufbewahrung und Verwaltung

Bei der Erzeugung von Enforcement-Datensätzen werden oft proprietäre Verfahren und Algorithmen eingesetzt. Dies bringt natürlich eine gewisse Abhängigkeit bei den Verwaltungs- und Aufbewahrungstools. In jedem Fall müssen aber folgende Punkte für die Dauer der Aufbewahrung gewährleistet werden können:

- Der Zugriff auf Enforcementdaten muss jederzeit möglich sein. Ausserdem müssen die Daten in geeigneter Form dargestellt und bei Bedarf ausgegeben werden können.
- Die Integrität/Authentizität der Daten muss jederzeit nachgewiesen werden können. Die erforderlichen Schlüssel müssen über den geforderten Zeitraum verwaltet werden.
- Die Nachbearbeitung des Bildes muss jederzeit möglich sein (Anforderung an Verarbeitung).

## 7.6. Anforderungen an die Bildqualität

Die Anforderungen an die Bildqualität eines Beweisbildes können funktional wie folgt definiert werden: Das Bild muss den Tatbestand zweifelsfrei dokumentieren. In den meisten Fällen heisst das konkret, dass das Kontrollschild sowie der Lenker zweifelsfrei erkennbar sein müssen. Mit dieser Bedingung ergeben sich gewisse Anforderungen an die Anzahl der Bildpunkte sowie Restriktionen hinsichtlich Datenkompressionsgrad.

**Anzahl der Bildpunkte (Pixel)**

Wie in der untenstehenden Abbildung 25 zu sehen, wird mit abnehmender Anzahl der Pixel die Lesbarkeit des Kontrollschildes schlechter. Spätestens ab 4 Pixel pro Ziffernbreite ist eine einwandfreie Identifikation des Kontrollschildes nicht mehr in jedem Fall gewährleistet. Es ist dennoch schwierig eine harte Grenze für die geforderte Anzahl Pixel zu formulieren, wobei 6Pixel pro Ziffernbreite als absolute Untergrenze gelten muss.


~20 Pixel / Ziffernbreite


~10 Pixel / Ziffernbreite


~8 Pixel / Ziffernbreite


~6 Pixel / Ziffernbreite


~5 Pixel / Ziffernbreite


~4 Pixel / Ziffernbreite

**Abbildung 25: Beispiele für verschiedene Bild-Auflösungen**

Noch etwas schwieriger ist die Abgrenzung bei der Darstellung von Fahrzeuglenkern, da die Anzahl benötigter Pixel variabel ist. Abhängig von Beschaffenheit und Merkmalen eines Fahrers ist die eindeutige Identifizierung einfacher oder schwieriger. Dementsprechend kann die Anzahl benötigter Pixel nicht eindeutig definiert werden. Grundsätzlich kann aber gesagt werden, dass die eindeutige Identifizierung des Fahrers keine höhere Auflösung benötigt als die welche für die eindeutige Identifizierung des Kontrollschildes ohnehin vorgegeben wird.

***Anmerkung:*** *Natürlich ist die Anzahl der Pixel nicht der alleinige Parameter, welcher die Darstellung beeinflusst. Auch die Anzahl der Graustufen hat einen Einfluss, ist aber bei den auf dem Markt befindlichen Produkte nicht der limitierende Faktor.*

→ Die dargestellten Zeichen müssen ohne Kenntnis der Syntax zweifelsfrei identifiziert werden können.

**Kompressionsgrad**

Wie bereits unter Kapitel 4.4 beschrieben, können Kompressionen zu Bildverfälschungen führen. Ist das Kompressionsverfahren verlustfrei, so kann beliebig komprimiert werden. Ist die Kompression allerdings verlustbehaftet, so gelten gewisse Einschränkungen was den Kompressionsgrad angeht.

Die bei der (verlustbehafteten) Kompression entstehenden Verfälschungen können in drei Kategorien unterteilt werden:

a) Verfälschungen, welche lediglich eine Qualitätseinbusse zur Folge haben, aber den funktionalen Bildinhalt nicht beeinflussen.

b) Verfälschungen, welche den funktionalen Bildinhalt zerstören → z.B. ein Kontrollschild kann infolge Kompressionsverlusten nicht mehr einwandfrei identifiziert werden.

c) Verfälschungen, welche den funktionalen Bildinhalt verändern → z.B. eine Ziffer im Kontrollschild verändert infolge Kompression ihren Wert. Unter dem funktionalen Bildeinhalt wird beispielsweise ein abgebildetes Kontrollschild gemeint. Solange das Schild einwandfrei zu identifizieren ist, ist der funktionale Bildinhalt erhalten geblieben.

Während Verfälschungen der Kategorie a) für das *Digitale Enforcement* weitgehend problemlos sind, können Verfälschungen der Kategorie b) und c) nicht akzeptiert werden. Als besonders problematisch müssen insbesondere Verfälschungen der Kategorie c) betrachtet werden, da diese unter Umständen eine Strafverfolgung von Unbeteiligten zur Folge haben können, während im b) Fall schlimmstenfalls ein Verkehrssünder „durchschlüpft".

Ähnlich wie bei der Frage der erforderlichen Auflösung ist es auch bei der Frage des zulässigen Kompressionsgrades nicht möglich, einen genauen Wert festzulegen. Dies insbesondere auch deshalb, weil verschiedene Kompressionsalgorithmen eingesetzt werden.

→ Bei verlustfreien Kompressionsverfahren bestehen keine Einschränkungen an den Kompressionsgrad. Dagegen muss beim Einsatz von verlustbehafteten Kompressionsverfahren sichergestellt sein, dass durch die Kompression keine funktionalen Bildinhalte zerstört oder verändert werden. Letzteres ist primär zu behandeln.

**Beispiel**: Das folgende Beispiel zeigt, wie sich ein Bild mit zunehmendem Komprimierungsgrad verändert. Es zeigt auch, dass sich das Kontrollschild erst ab einem gewissen Komrimierungsgrad merklich verschlechtert (in diesem Fall ab ~80%). Zuvor verschlechtert sich wohl die Bildqualität, nicht aber der funktionale Inhalt des Bildes. Die Grenze kann aber je nach Komprimierungsverfahren variieren. Im vorliegenden Fall wurde ein Bild mit 1024x768 Pixel mit JPEG komprimiert. Die Anzahl der Pixel bleibt dabei konstant:

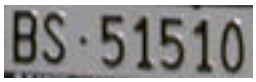
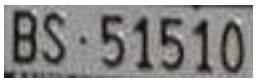
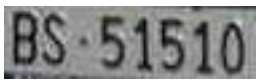
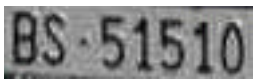
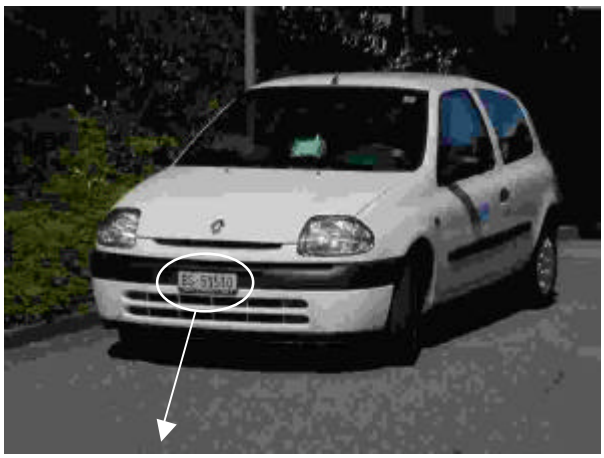
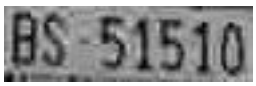
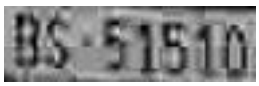
| | | | |
|---|---|---|---|
|  | |  | |
|  | Komprimierung: 0%<br>Grösse: 163kByte |  | Komprimierung: 50%<br>Grösse: 71kByte |
|  | |  | |
|  | Komprimierung: 75%<br>Grösse: 44kByte |  | Komprimierung: 80%<br>Grösse: 38kByte |
|  | |  | |
|  | Komprimierung: 90%<br>Grösse: 25kByte |  | Komprimierung: 95%<br>Grösse: 18kByte |

**Abbildung 26: Beispiel für den Komprimierungs-Einfluss beim Einsatz von JPEG**

# 8. Glossar

| Begriff | Erklärung |
|---|---|
| Datensatz | Unter einem Datensatz werden in diesem Bericht Daten verstanden, welche **einen** Kontrollfall dokumentieren. |
| DSRC | **D**edicated **S**hort **R**ange **C**ommunication. Funkschnittstelle auf einer Frequenz von 5.8GHz für Anwendungen im Bereich der elektronischen Gebührenerhebung. |
| Farbtiefe | Die Farbtiefe gibt an, wie viele Farben bzw. Graustufen dargestellt werden können. Die Farbtiefe wird angegeben durch die Anzahl Bit mit der eine Farbe beschrieben wird.<br>• 1 Bit = 2 Farben (schwarz/weiss)<br>• 4 Bit = 16 Farben/Grautöne<br>• 8 Bit = 256 Farben/Grautöne<br>• 16 Bit = 32767 oder 65'535 Farben<br>• 24 Bit = 16,7 Millionen Farben |
| Laser-Scanner | Gerät, welches mit Hilfe eines Lasers ein Profil (Höhe, Breite, Länge) von vorbeifahrenden Fahrzeugen vermessen kann. Mit Hilfe von nachgeschalteter Verarbeitungssoftware, kann der passierende Verkehr in einzelne Klassen unterteilt werden (PW, LKW, Bus, usw.). |
| LPR | **L**icence **P**late **R**eading |
| OBU | **O**n **B**oard **U**nit |
| OCR | **O**ptical **C**haracter **R**ecognition |
| TRIPON | Erfassungsgerät für die leistungsabhängige Schwerverkehrsabgabe (LSVA) der Schweiz |
| VES | **V**ideo **E**nforcement **S**ystem |
| Hash | Eine Hash-Funktion ist ein Verfahren zur Komprimierung von Daten mittels einer Einwegfunktion, so daß die ursprünglichen Daten nicht rückrechenbar sind. Die Hash-Funktion liefert für einen Eingabewert beliebiger Länge einen Ausgabewert fester Länge und ist so beschaffen, daß eine Änderung der Eingangsdaten mit sehr hoher Wahrscheinlichkeit Auswirkungen auf den berechneten Hash-Wert (d.h. den Ausgabewert) hat. Ein typischer Vertreter der Hash-Algorithmen ist der SHA-1. Das Ergebnis einer Hash-Funktion ist der Hash-Wert, der oft auch als digitaler Fingerabdruck bezeichnet wird. |
| Frame-grabber | Als Framegrabber bezeichnet man eine elektronische Einheit, welche aus einem dynamischen analogen Videosignal einzelne Standbilder herauspickt. |
| UVEK | Eidgenösisches Departement für Umwelt, Verkehr, Energie und Kommunikation |
| metas | Bundesamt für Metrologie und Akkreditierung |
| VERA | Video Enforcement for Road Authorities; EU-Forschungsprojekt |
| ADVICE | Advanced Vehicle Classification and Enforcement; EU-Forschungsprojekt |
| C.A.S.E. | Continuous Applied Speed Enforcement |
| DES | Data Encryption Standard gemäss ANSI X3.92. Meist verbreitetes symmetrisches Verschlüsselungsverfahren |
| UNI | Ente Nationale Italiano di Unificazione, Italienische Normierungsbehörde |

# Anhang A: Norm-Entwurf

# Systèmes pour les contrôles routiers automatiques avec traitement d'images numériques

pour l'

# Office Fédérale des Routes OFROU

Projet de recherche 1999/301

Date: 10. septembre 2002 **Rapport-N°:** 23.058.0/001 **Version:** Rapport final


Membres de la commission d'experts:
**Pascal Blanc (OFROU)** (président)
**Roland Aellen (OFROU)** **Erich Burkhalter (OZD/LSVA)** **Walter Fasel (metas)** **Hans Peter Oehrli (mobiletix)** **Beat Schüpbach (Kapo BL)** **Beat Zumsteg (R.Brüninger AG)**

Chef de projet:
**Bernhard Oehry** Chef de département télématique du transport
Auteur:
**Simon Benz** Département télématique du transport
Collaboration:
**Christian Egeler** Département télématique du transport
**Urban Kaiser** Departement télématique du transport

RAPP INGENIEURE + PLANER

**RAPP AG Ingenieure und Planer, Hochstrasse 100, 4018 Basel, Tel. + 41 61 335 77 77, http://www.rapp.ch**

# Résumé

## Objet

Pour améliorer la sécurité routière et pour imposer la législation routière d'une manière efficace, une haute densité de contrôles routiers est nécessaire. Pour cette raison, des efforts sont entrepris pour **automatiser les processus de surveillance**. Contrairement aux contrôles mobiles, aucune personne assermentée n'accompagne les procédures de contrôle effectuées par des systèmes automatisés. Le fait qu'aucun agent administratif ne soit présent sur les lieux de l'incident, et que le jugement s'effectue à partir d'une pièce à conviction enregistrée automatiquement, fait augmenter les exigences relatives à l'enregistrement comme élément de preuve qui doit être recevable par les tribunaux sans que d'autres pièces probatoires soient disponibles.

Actuellement, la surveillance automatisée de la circulation routière se fait pratiquement sans exception avec des caméras traditionnelles, où les films sont développés au laboratoire (technique du « Wet-film » ou à film argentique). Les données additionnelles (date/temps, lieu du contrôle etc.) y sont directement incrustées dans l'image lorsque la photo est prise. Pourtant, la technique à film argentique présente toute une série d'inconvénients :

- Il faut chercher les films manuellement au poste de contrôle.
- Il faut développer les films au laboratoire avant de pouvoir exploiter le contenu des images.
- L'archivage des films doit être fait par procédé manuel.

C'est, entre autres, pour ces raisons que des efforts sont faits pour remplacer les caméras traditionnelles à film argentique par des dispositifs électroniques de saisie d'images, plus particulièrement par des **caméras numériques.**

L'utilisation de caméras numériques soulève pourtant toute une série de questions : Par exemple, l'**authenticité d'une image** ne peut plus être prouvée par le simple fait que l'image fait partie d'une pellicule entière. Ensuite, il y a d'autres questions à étudier qui se réfèrent à la manipulation des images digitalisées, au chiffrement des données pour la transmission etc. Il faut en plus tenir compte du fait que l'utilisation de caméras numériques permettra la mise en place de nouvelles méthodes de surveillance qui, à leur tour, soulèveront encore d'autres questions.

Comme montré ci-avant, les exigences formulées en matière des enregistrements comme éléments de preuve, générés par un procédé automatique, doivent être considérables. D'ailleurs, l'application de systèmes digitalisés ouvre la voie à de plus amples applications. Ceci fera encore croître les exigences pour prouver de façon indiscutable que l'enregistrement comme élément de preuve est intact et représente l'événement original sans la moindre modification. Pour cela, le résultat principal de notre projet de recherche sera un **projet de norme** définissant des exigences en matière des systèmes pour la surveillance automatique de la circulation avec traitement d'images numériques.

# Procédure

Dans un premier temps, une analyse est faite sur l'état actuel des applications existantes et sur les projets de recherche ainsi que sur les bases juridiques dans le domaine des contrôles automatisés de la circulation. Cette analyse se repose sur les aspects et informations provenant d'origine nationale ainsi que d'autres pays européens.

La deuxième étape est une description générale des **méthodes et procédures techniques** concernant :

- La saisie d'images numériques (appareils photo numériques et caméras vidéo) ;
- La sécurité des données (chiffrement, signature, tatouage de l'image etc.) ;
- Le traitement des données numériques, en particulier les donnés-images ;
- Les méthodes de compression.

Un **modèle fonctionnel** pour les systèmes de surveillance automatique de la circulation sera développé et servira comme base principale pour le projet de norme. Le modèle fonctionnel doit présenter les éléments de base et les procédures fondamentales des installations de contrôle d'une manière aussi simple et généralement valable que possible, afin de permettre une définition précise des exigences relatives à ces systèmes subordonnés. Que le modèle soit applicable à toutes les procédures existantes ainsi qu'à toutes les méthodes concevables pour l'avenir est d'une importance particulière.

Il s'agit ensuite de déterminer les **lacunes normatives** sur la base du modèle. En plus, il sera clarifié si l'utilisation des nouveaux systèmes numériques de saisie d'image demande une adaptation des bases juridiques en vigueur.

L'analyse des lacunes normatives fournira la base sur laquelle les exigences envers les enregistrements numériques seront déterminées. Le **projet de norme** sera basé sur ces exigences**.**

# Résultats

### Bases juridiques

Les deux directives existantes sur le sujet des installations automatisées de contrôle sont rédigées de façon très fonctionnelle. Le déroulement du processus de contrôle, les conditions-cadre et les exigences en matière de l'image comme élément de preuve (y compris les données supplémentaires incrustées) y sont décrits en particulier. Bien que les directives ne considèrent pas l'application des techniques numériques de saisie d'image, elles ne les excluent pas explicitement non plus.

### Modèle fonctionnel

Le processus entier du contrôle routier peut être subdivisé en trois fonctions principales :

- **Détection** La détection comprend l'ensemble des étapes nécessaires à déterminer si, et à quel degré, un véhicule a commis une infraction à la loi en vigueur.
- **Documentation :** La documentation comprend l'ensemble des étapes nécessaires à documenter de façon exhaustive toute infraction au code routier. En outre, cette étape prévoit le transfert des données et leur stockage à un office central.
- **Traitement :** Le traitement comprend l'ensemble des actions requises après le transfert des enregistrements au service de traitement supplémentaire (sauf l'archivage) ce qui inclut, par exemple, la lecture (manuelle ou automatique) d'une plaque minéralogique ou la vérification du contenu fonctionnel de l'image.

**Structure physique**

De façon analogue au modèle fonctionnel, il est possible de subdiviser le système physique global d'une installation de contrôle-sanction (installation d' »Enforcement ») en plusieurs sous-systèmes. Une division en les trois parties suivantes parait raisonnable :

- **Dispositif de contrôle en bordure de route :** Cette partie du système représente l'ensemble des installations sur site, à proximité directe de la chaussée, et consiste en particulier des dispositifs de saisie d'image, de l'équipement de mesure et, le cas échéant, d'un système électronique d'exploitation des images.
- **Canal de transmission** Le terme désigne en première ligne le canal de transmission des données entre le dispositif routier de contrôle et le système central de fond. Pourtant, cela n'exclue pas les autres voies de transmission éventuellement existantes, telles que, par exemple, des liaisons plus longues entre les composants individuels d'un système, comme on les trouve dans les installations de contrôle de trajectoire.
- **Système central de fond:** Ce système prévoit le traitement supplémentaire des enregistrements, par exemple la confirmation manuelle des résultats LPR/OCR (reconnaissance automatique des plaques d'immatriculation/reconnaissance des chiffres et caractères) ou bien la vérification des résultats du processus de classification. En plus, le système assure l'archivage et la gestion des données.

**Lacunes normatives**

Le titre original du projet « Systèmes pour la surveillance automatique de la circulation (« Enforcement ») avec traitement d'images numériques et reconnaissance automatique des plaques d'immatriculation » a supposé que le problème central de l'application des technologies numériques dans les installations de surveillance routière réside dans le traitement de l'image et là surtout dans la reconnaissance automatique des plaques d'immatriculation.

L'analyse des lacunes normatives a cependant clairement montré que les termes-clé mentionnés de façon explicite dans le titre original, à savoir « traitement d'images numériques» et « reconnaissance automatique des plaques d'immatriculation » ne constituent pas des processus cruciaux dans la surveillance automatisée à dispositifs numériques de saisie d'images. Dans les deux cas, il s'agit en principe seulement de techniques auxiliaires pour le traitement des images qui, du point de vue juridique, n'ont aucune influence sur la force probatoire d'un enregistrement comme élément de preuve. Ce qui est décisif, c'est la façon dont les données à conviction sont saisies ainsi que l'intégrité et l'authenticité de l'enregistrement comme pièce à conviction. D'où le projet de norme se concentre exclusivement sur la fonction *Documentation*, sans prendre en considération les fonctions *Détection* et *Traitement*.

Pour tenir compte de cette conclusion, nous avons adapté le titre de notre projet de recherche et mis l'accent sur les mots-clé « surveillance automatique » et « traitement d'images numérique ».

**Exigences relatives aux données et procédés**

L'analyse révèle que les lacunes normatives à combler se limitent en principe à enregistrement comme élément de preuve. Traduit sur le modèle fonctionnel cela signifie que les exigences en matière de normalisation concernent la sous-fonction *Documentation*. Les exigences relatives à la normalisation se divisent en plusieurs catégories :

- **Exigences fonctionnelles en matière des enregistrements comme éléments de preuve :** L'intégrité et l'authenticité des données doivent être garanties. En plus, enregistrement doit fournir une documentation complète de l'évènement.
- **Exigences relatives à la protection de la personnalité et à la sécurité des données :** D'une part, il s'agit de la sécurité des fichiers/de la surveillance des composants du système en bordure de la route, d'autre part, d'une protection adéquate des données lors de leur transmission. Si l'état et la structure du canal de transmission ne garantissent pas cette sécurité, il faut transférer les données sous forme cryptée. De la même manière, le procédé de sauvegarde des données dans le système central doit garantir qu'aucune personne non autorisée ne pourra avoir accès aux données.
- **Exigences relatives à l'intégrité et l'authenticité :** Pour pouvoir garantir et vérifier l'intégrité et l'authenticité des données, c'est encore dans l'environnement sûr de l'installation que l'enregistrement doit être pourvu d'une signature numérique. Selon l'architecture du système, il peut éventuellement être nécessaire de signer séparément certaines parties de l'enregistrement
- **Exigences relatives au traitement supplémentaire :** enregistrement original servant de pièce à conviction ne doit en aucun cas pouvoir être modifiée avant la mise en mémoire. Il n'y a pas d'autres restrictions.
- **Exigences relatives à la sauvegarde et la gestion :** Les données enregistrées doivent être accessibles à tout moment. Les données doivent pouvoir être présentées sous forme appropriée et rappelées si besoin en est. L'intégrité et l'authenticité des données doivent être garanties et doivent pouvoir être vérifiables à chaque instant. En conséquence, la gestion des clés requises pour l'accès aux données doit être sûre et assurée à long terme.
- **Exigences en matière de la qualité de l'image** La définition fonctionnelle des exigences relatives à la qualité d'une image servant de pièce à conviction est la suivante : L'image doit fournir une documentation indiscutable de l'infraction. Dans la plupart des cas, cela veut dire que la plaque d'immatriculation et le conducteur doivent pouvoir être identifiés sans aucun doute possible. Cette définition donne lieu à certaines prescriptions minimales relatives au nombre de pixels et à des restrictions sur le degré de compression admissible (lors de l'utilisation d'algorithmes de compression avec une perte d'informations).

## Résultats centraux

- Le **projet de norme** fournit une base pour l'établissement d'une norme suisse sur les systèmes pour la surveillance automatique de la circulation avec traitement d'images numériques.
- **Les adaptations aux directives techniques en vigueur** requises pour l'application des systèmes automatisés de contrôle routier avec traitement d'image numérique sont peu.
- Il n'y a, en principe, aucun obstacle à la mise en œuvre de systèmes automatisés pour les contrôles routiers avec traitement d'images numériques, pourvu que les exigences présentées soient respectées.

# Sommaire

(page vide)

# 1. Problème

## 1.1. Situation de référence

En maints endroits en Suisse, la circulation routière tend vers ses limites. Avec l'accroissement des transports, gérer le trafic de façon performante devient nécessaire sans négliger pour autant le rapport coûts-service.

Un objectif central de la gestion du trafic est la sécurité routière. Pour augmenter la sécurité routière et pour imposer la législation routière d'une manière efficace, une haute densité des contrôles est nécessaire. En même temps, une densité élevée de contrôles requiert beaucoup de personnel pour les contrôles eux-mêmes (enregistrement des infractions) ainsi que pour la poursuite des infractions.

Depuis les années 50, les appareils photo ont été introduits afin de supprimer les méthodes de surveillance coûteuses en termes de financement et de travail. Grâce au développement de la télématique routière, il est possible d'atteindre une efficacité encore plus grande. L'utilisation de dispositifs digitaux de saisie d'images et le traitement électronique de l'image permettent non seulement des applications totalement nouvelles mais aussi une efficacité beaucoup plus élevée des procédés.

## 1.2. Mission

L'objectif du projet de recherche est d'établir les conditions sous lesquelles une surveillance automatique employant des systèmes électroniques, en particulier des appareils et procédés numériques, tels que caméras numériques, télétransmission, traitement d'images numériques et reconnaissance automatique des plaques d'immatriculation, est possible. Une étude fondamentale sera établie pour déterminer les lacunes normatives.

## 1.3. Objectifs de la recherche

L'objectif du travail de recherche est d'établir un projet de norme définissant les exigences relatives à une installation de contrôle-sanction avec traitement d'images numériques. Il s'y agit en particulier de préciser les exigences en matière de :

- l'équipement
- des procédés
- des bases juridiques

et de les redéfinir, si besoin en est. Ensuite, il s'agit de définir une architecture de référence pour de tels systèmes.

Il faut tirer au clair la question à savoir jusqu'à quel point il est nécessaire de définir des exigences de qualité en matière de la détection d'évènements, d'un côté, et pour la reconnaissance automatique des plaques d'immatriculation de l'autre côté. La définition des exigences relatives au contenu des images, à leur format et au procédé de sauvegarde pour la documentation des évènements doit être telle qu'ils subissent la vérification au tribunal.

## 1.4. Procédure et méthodes

*1. Préparation du projet*

Dans le cadre de la préparation du projet les bases supplémentaires (littérature, normes) ont été établies, et le déroulement du projet a été coordonné avec d'autres projets persistants.

*2. Exploitation des bases*

Les applications existantes de la technologie à images numériques ainsi que les documents et rapports sur le contrôle-sanction numérique constituent un bon fondement pour le sujet. Dans le cadre du projet de recherche européen VERA (Video Enforcement for Road Authorities), par exemple, une étude générale a été menée sur l'emploi de systèmes à saisie d'images (vidéo) numériques. Il s'y agissait, cependant, plutôt de l'harmonisation des procédures de contrôle-sanction au niveau des états européens.

Ci-après seront définis les termes utilisés dans ce projet. Le résumé des bases juridiques sert à fournir une notion des conséquences possibles que pourra avoir cette étude pour une future adaptation de la législation.

3. *Traitement d'images numériques*

Il est important de traiter surtout la technologie du traitement d'images numériques, qui occupe une place centrale dans le cadre de ce projet, pour pouvoir partir d'une base bien-définie. Il s'agit donc de donner une description rudimentaire de l'histoire et des possibilités de l'imagerie numérique.

4. *Architecture du système*

Pour pouvoir déterminer l'architecture de référence requise, un modèle doit être développé. Ceci se fera sur la base d'une analyse sur les procédés de contrôle-sanction existants. Le modèle doit être crée non seulement au niveau physique mais aussi au niveau fonctionnel. La modélisation permet de gagner une vue d'ensemble sur le système et sert comme base pour une prise en considération globale.

5. *La manipulation des données*

Lorsque des infractions sont documentées exclusivement sous forme numérique, cela soulève des questions relatives à la protection de la personnalité. Pour cette raison, il est indispensable de formuler les exigences relatives à

- la protection de la personnalité et à la sécurité des données
- l'intégrité et l'authentication
- le traitement supplémentaire des données
- la sauvegarde et la gestion
- la qualité de l'image.

6. *Projet de norme*

Les étapes précédentes devront permettre d'établir le projet requis relativement aux lacunes normatives dans le domaine du contrôle-sanction numérique.

# 2. Définition des termes techniques

Dans la télématique routière, il n'existent pas encore des définitions définitives pour tous les termes techniques. Des bases ont été établies dans la norme suisse SN 67 1832-875 «Télématique des transports». Le chapitre suivant décrit les termes principaux afin de procurer une base homogène pour le suivant rapport.

## 2.1. Contrôle-sanction dans la circulation routière

Le terme de contrôle-sanction (Enforcement) désigne l'ensemble des mesures entreprises pour faire respecter les lois et les règles de la circulation – dans ce cas tous ce qui a rapport à l'utilisation des routes. La surveillance générale du trafic, par ex. la reconnaissance de dysfonctionnements, la manipulation active des flux etc., ne sont pas comprises dans la notion de contrôle-sanction mais désignées par le terme « Monitoring ». Dans le cadre du monitoring, c'est l'ensemble des véhicules dans la circulation routière qui se trouve sous surveillance où l'anonymat individuel des véhicules et/ou des conducteurs doit impérativement être respecté. Dans le cas du contrôle-sanction, par contre, il s'agit explicitement de contrôler les véhicules individuels et d'identifier le véhicule et son conducteur en cas d'une infraction.

## 2.2. Systèmes vidéo de contrôle-sanction (Video Enforcement)

Le projet de recherche présent s'intéresse à un sous-aspect particulier du processus de contrôle-sanction, ce sont les systèmes vidéo de contrôle-sanction (Video Enforcement Systems VES). Lorsqu'une infraction est constatée, ces systèmes prennent des images comme éléments de preuve de l'infraction en y ajoutant des informations supplémentaires (heure, lieu, vitesse etc.).

Jusqu'ici, les installations de contrôle-sanction fonctionnaient exclusivement avec des caméras traditionnelles (à film argentique). Cette technologie présente cependant des inconvénients non négligeables : D'abord, il faut chercher les filmes aux sites de contrôle (procédé manuel) et ensuite les développer au laboratoire pour pouvoir procéder à leur exploitation. D'ailleurs, le traitement automatisé des films est difficile.

Au cours de ces dernières années, la technologie des images numériques s'est beaucoup répandue dans tous les domaines. Il convient donc de bénéficier des avantages multiples offerts par les technologies numériques aussi dans le domaine de la surveillance vidéo.

## 2.3. Applications des systèmes vidéo de contrôle-sanction

Jusqu'à maintenant, les applications courantes dans le domaine des contrôles automatiques de la circulation étaient les suivantes :

- Contrôle des feux rouges
- Contrôle de la vitesse.

Les directives techniques publiées par le DETEC aussi se réfèrent donc à ces deux applications. C'est en particulier l'emploi de systèmes numériques qui ouvre la voie à de nombreuses autres applications, comme par ex. le contrôle de trajectoire, contrôle des voies de bus, contrôle d'accès limité etc.

## 2.4. Définition de la surveillance automatique de la circulation

Une installation de surveillance automatique de la circulation est un système qui assure la surveillance des véhicules sans que la présence de personnes assermentées soit nécessaire. Le système est capable de détecter automatiquement une infraction et à l'enregistrer de sorte que le matériel résultant est recevable comme élément de preuve par les tribunaux.

# 3. Situation et bases

## 3.1. Applications existantes d'imagerie numérique

### 3.1.1. RPLP

A l'entrée sud du tunnel Belchen, une installation de surveillance avec saisie d'images numériques pour la redevance des poids lourds liée aux prestations (RPLP) a été mise en service début 2001 :

**Figure 1 : Installation de contrôle-sanction RPLP au Belchen**

L'architecture de l'installation est la suivante :

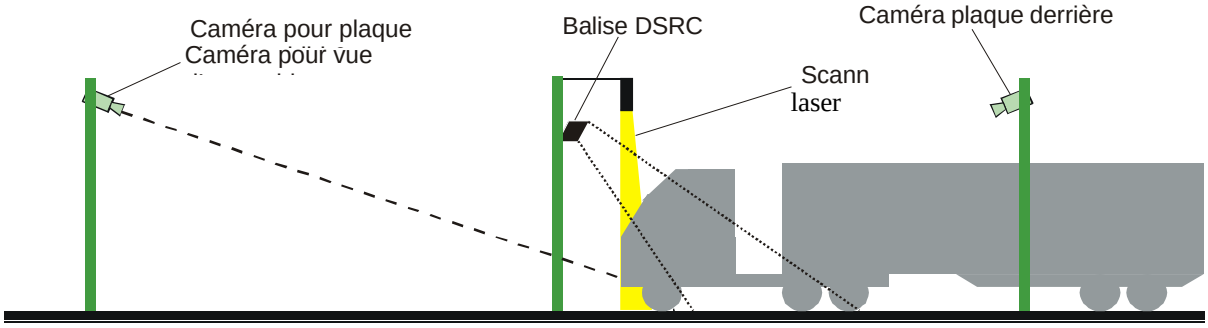



**Figure 2 : Architecture du système de contrôle-sanction RPLP**

D'une façon générale, le système enregistre et classifie tous les véhicules passant le poste de contrôle (les données des véhicules non imposables sont effacées immédiatement après). , Si le véhicule est équipé d'un dispositif de saisie RPLP (TRIPON) les données y enregistrées sont rappelées. Le système dispose alors des suivantes données :

- Classe du véhicule détecté (y compris informations sur la remorque)
- Plaque d'immatriculation du véhicule et (le cas échéant) de la remorque
- Informations de l'appareil de saisie RPLP (surtout son statut actuel, c.-à-d. l'état de fonctionnement de l'appareil et l'état de déclaration).

Pour les véhicules équipés de dispositifs de saisie les valeurs mesurées sont comparées à la déclaration donnée dans l'appareil. Ces données sont transférées par balise-radio

(DSRC) à la station de contrôle. Pour les véhicules sans système de saisie, les données mesurées sont comparées à la déclaration donnée par le conducteur au terminal « self-service » à la frontière, lors de son entrée en Suisse. A partir de ces données, le système peut relever si une infraction doit être supposée ou non.

Les images saisies sont directement pourvues d'une signature cryptographique lors de leur enregistrement par la caméra, ce qui permet d'identifier toute modification ultérieure de l'image (voir chapitre 0). La reconnaissance automatique des plaques d'immatriculation (LPR/OCR) aussi se fait directement dans la caméra. Les différentes données (données-brutes en sortie du scanneur, données DSRC, résultat de la reconnaissance automatique des plaques d'immatriculation et les trois images) sont recueillies au poste de contrôle. Cet enregistrement est ensuite signé dans son ensemble pour être protégé contre des modifications inaperçues.

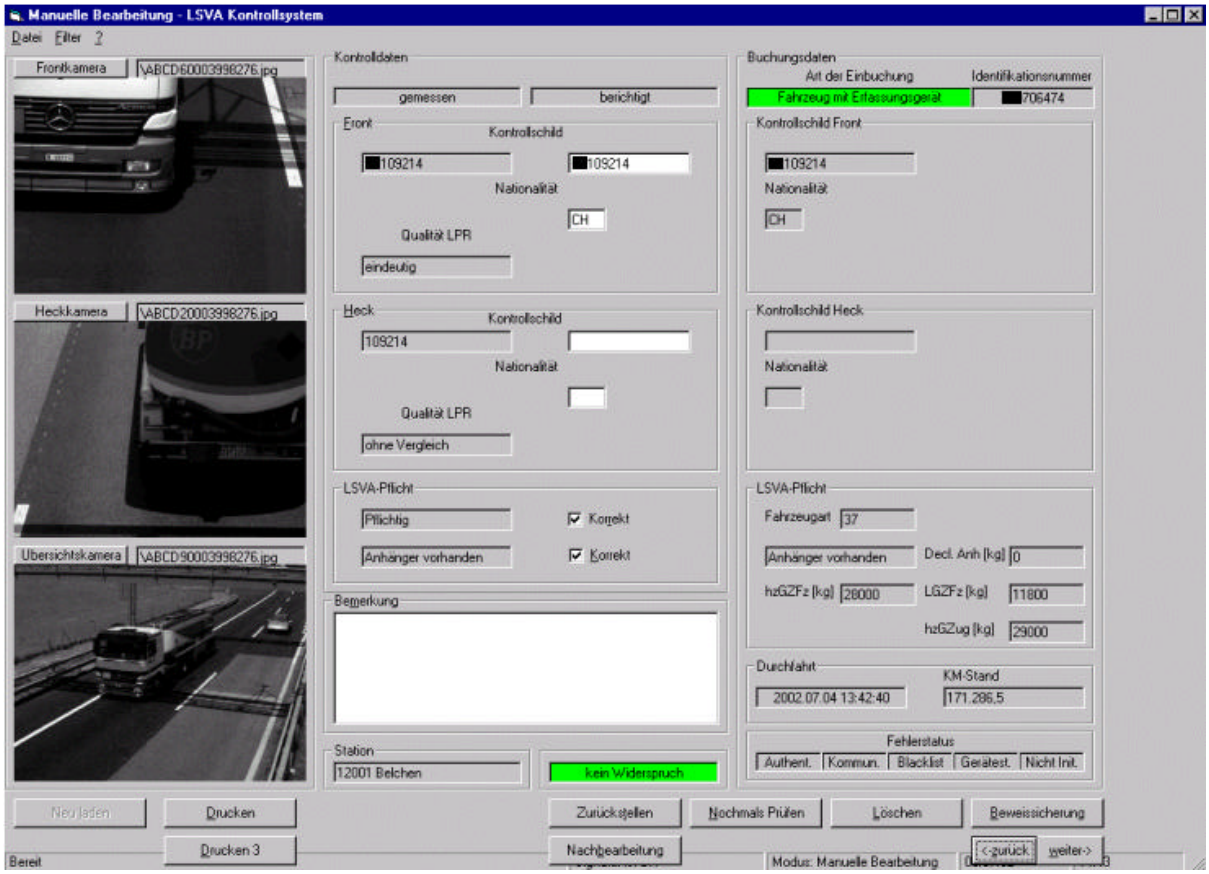



**Figure 3 : Ecran affiché pour le traitement d'un évènement au bureau central de contrôle-sanction RPLP**

Actuellement, l'installation de contrôle au Belchen est la seule application dans le domaine routier [1] en Suisse qui produit des images numériques comme éléments de preuve. Les expériences et les résultats obtenus par l'exploitation de cette installation ont une grande valeur pour le projet de recherche *Contrôle-sanction numérique*, entre autres, parce que la station de contrôle-sanction RPLP génère des enregistrements à plusieurs sous-composants différents.

[1] Bien que l'application concerne le trafic routier, elle est soumise à la réglementation RPLP et non à la législation routière.

### 3.1.2. Recherche de véhicules enregistrés sur les listes des véhicules recherchés

Un exemple pour l'emploi d'un système de contrôle-sanction fondé sur imagerie numérique dans la recherche de véhicules figurants sur les listes de véhicules recherchés est donné par la police urbaine de Zurich. Il s'agit d'un système pour la détection de voitures recherchées dans un trafic dense. Le système travaille avec des images électroniques LPR/OCR. Ce processus n'utilise cependant pas les images comme élément de preuve. Elles ne servent qu'à réaliser une présélection des véhicules à examiner après leur immobilisation. L'intérêt pour le projet de recherche "Contrôle-sanction numérique » se limite donc à la question immanente sur la protection de la personnalité lors de l'enregistrement des données, voir images.

### 3.1.3. Contrôle de trajectoire (Continuous Applied Speed Enforcement CASE)

Contrairement aux systèmes traditionnels pour le contrôle de vitesse, c'est la vitesse moyenne sur un tronçon (d'une longueur comprise entre 100m et quelques km) qui est contrôlée ici. A cette fin, deux caméras numériques sont installées au début et à la fin de la section de contrôle pour enregistrer les véhicules de passage. Des algorithmes spécialement conçus pour cette application reconnaissent les véhicules ayant passés la zone, calculent le temps de passage de la zone du véhicule et déterminent ensuite la vitesse moyenne de passage.

Ce système a été développé et testé pour la première fois aux Pays-Bas. Les expériences et les connaissances gagnées du projet néerlandais ont une très grande valeur pour la recherche dans le domaine du contrôle-sanction numérique. C'est en première ligne le procédé de mesure qui est neuf dans ce système et pas tellement la technologie d'imagerie numérique. Le nombre de véhicules roulant trop vite est passé de 6% à 1% sur l'ensemble de la circulation (avant l'installation du dispositif, la section avait déjà fait l'objet d'un contrôle renforcé avec des méthodes traditionnelles non automatiques et un tableau indiquant les contrôles potentiels avait été mis en place). Le taux d'infraction s'élevait à 35% auparavant. (Vortrag Jan Malenstein, KLPD, 27.5.99). La vitesse moyenne a baissé de 116 km\h à 106 km\h avec une limitation de la vitesse à 100 km\h. Il a été constaté que la circulation était plus régulière qu'avant la mise en activité du dispositif (avec des écarts de vitesse plus réduits) et que le nombre d'accidents et d'embouteillages s'avéraient nettement moindre.

Pour le projet de recherche l'accent est mis sur l'utilisation d'images numériques et non sur la détection des évènements, telle que réalisé dans C.A.S.E..

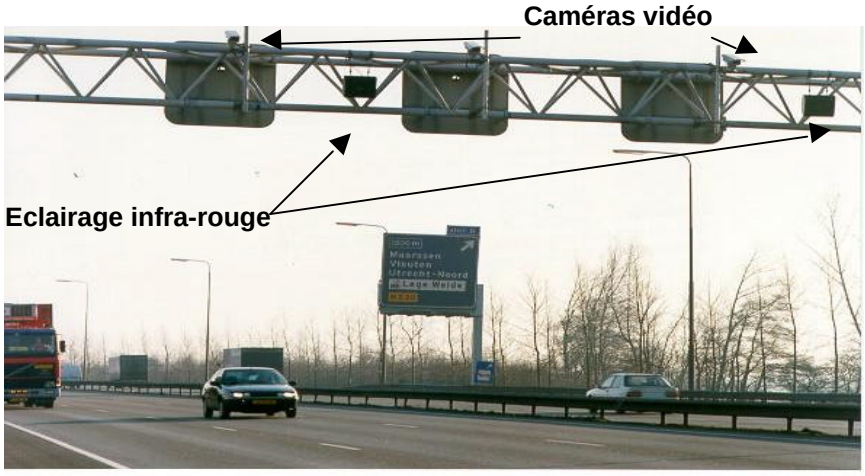



**Figure 4 : Dispositif de contôle de trajectoire (C.A.S.E.) aux Pays-Bas**

### 3.1.4. Dispositif de contrôle de vitesse avec saisie d'images numériques

Actuellement (en été 2002), l'homologation provisoire d'une première installation de contrôle de la vitesse avec saisie d'images numériques est en préparation en Suisse. Le processus sera probablement terminé dans les mois à venir et l'exploitation pilote pourra être commencée. L'installation est équipée de capteurs piézo-électriques pour la détection et peut être pourvue, au choix, d'une caméra traditionnelle ou digitale. Ce dispositif peut être utilisé pour les contrôles de vitesse aussi bien que pour les contrôles des feux rouges et dispose d'une interface pour la télémaintenance et le paramétrage. Du fait que la gestion des accès n'est pas encore suffisamment réglée, l'interface n'a pas encore été libérée. Le déblocage est pourtant envisageable si certaines conditions sont remplies. La première application de ce dispositif sera une installation de contrôle de vitesse.

Le processus d'homologation et l'autorisation à exploiter ce dispositif ont une importance considérable pour le projet de recherche. Il s'agit en effet de la première autorisation en Suisse d'exploiter une installation de contrôle-sanction fondé sur la saisie d'images numériques dans le cadre la loi sur la circulation routière.

Le processus d'homologation fournit des indications importantes sur un niveau de précision raisonnable pour la norme qui est à créer.

Il s'agit de trouver une solution intermédiaire entre des conditions-cadre nécessaires et une réglementation trop restrictive.

**Remarque :** L'homologation et l'autorisation d'exploiter l'installation décrite ci-dessus se réfèrent aux systèmes globaux, y compris la voie de transmission des données.

## 3.2. Documents et rapports au sujet du contrôle-sanction numérique

### 3.2.1. Norme italienne UNI – E14C8005

La norme E14C8005, publiée par la UNINFO – office subordonné de l'administration italienne de normalisation UNI (Ente Nazionale Italiano di Unificazione) – s'occupe de la structure et des exigences en matière de systèmes pour la surveillance automatique, avec une attention particulière sur la reconnaissance automatique des plaques d'immatriculation par procédé de reconnaissance des chiffres et caractères (OCR). Le niveau de spécification de la norme est très variable pour les différentes parties du système. Alors que les sujets tels que l'architecture du système, la sécurité et l'authenticité des enregistrements ou le format des images ne sont traités que d'une manière très générale, le procédé du LPR/OCR est décrit de façon exhaustive et précise. La norme fournit surtout une description très détaillée des installations au laboratoire et des essais mis en œuvre pour déterminer le taux de reconnaissance LPR/OCR, Ceci est un peu étonnant, puisque la partie OCR ne constitue en principe qu'un système purement auxiliaire. En conséquence, les exigences formulées sont directement liées à l'application pratique du système. D'ailleurs, la force probatoire pour l'exploitation en pratique des essais réalisés au laboratoire est assez limitée (ce qui est explicitement mentionné dans la norme). La description détaillée des essais d'homologation pour les systèmes LPR/OCR ne sert, en fin de compte, qu'à permettre une meilleure comparabilité des systèmes des différents fabricants.

Dû à l'évaluation inégale des parties du système, la norme UNI ne peut être appliquée que dans une mesure restreinte sur le présent projet de recherche. Néanmoins, elle fournit certaines indications pour la structuration générale d'une norme.

### 3.2.2. Projet de recherche VERA

Le projet de recherche européen VERA (**V**ideo **E**nforcement for **R**oad **A**uthorities) traite le thème des contrôles routiers sur les autoroutes et les routes et de leur exécution par les autorités compétentes. Les expériences vues sous l'angle technique, juridique et

institutionnel ont été étudiées et évaluées. Le sujet central qui sera traité dans le prochain projet prévu, VERA II, est la question de la poursuite transfrontalière des infractions à la réglementation de la circulation. Il est prévu de définir des directives, des procédures et des interfaces qui permettront ou simplifieront le contrôle-sanction au-delà des frontières.

Les expériences et résultats tirés de VERA sont très importants dans le cadre de ce projet de recherche, et ce sont surtout les résultats obtenus en matière du model fonctionnel qui se révèlent très précieux.

### 3.2.3. Projet de recherche ADVICE

Le projet de recherche ADVICE (Advanced Vehicle Classification and Enforcement) réalisé dans le 4ième programme cadre de la Commission européenne traite de façon exhaustive les nouvelles technologies mise au point pour la classification et la surveillance des véhicules. L'objectif d'ADVICE était de combler les lacunes dans la recherche sur la probabilité de sanction dans les applications de systèmes électroniques de péage routier.

Ce travail a une importance réduite pour le projet *contrôle-sanction numérique*, puisque l'accent y est mis sur le contrôle-sanction dans les systèmes électronique à péage.

## 3.3. Bases légales existantes

### 3.3.1. Applications dans le cadre de la loi sur la circulation routière

**Législation routière**

La **loi fédérale sur la circulation routière** RS 741.51 règle les procédures de surveillance automatique de la circulation.

L'art.130 (4) de la loi dit:

« *L'office établit des instructions sur les contrôles automatiques de la circulation sans postes d'interception et règle la procédure à suivre.* »

Sur le sujet des contrôles de vitesse l'art. 133 dit :

« *L'office établit des instructions concernant les contrôles de vitesse par la police et les méthodes de mesure. Il règle l'utilisation des appareils automatiques servant à mesurer la vitesse.* »

**Instructions techniques**

Les annexes ***A/4.3 Instructions techniques concernant les contrôles de vitesse dans la circulation routière de l'ETEC du 10 août 1998*** et ***A/4.4 Instructions concernant l'emploi de dispositifs photographiques de surveillance des feux rouges du 14 avril 1988*** décrivent les directives et instructions disponibles sur de tels contrôles.

Les instructions techniques règlent également la question de l'admission des installations de contrôle-sanction :

„Les appareils servant à mesurer de manière officielle la vitesse sont soumis à une expertise et à l'admission par l'Office fédéral de métrologie et d'accréditation (METAS). Ils ne peuvent être utilisés que s'ils sont expertisés et munis d'un signe officiel de réception. » (Chiffre 3.1 des Instructions techniques concernant les contrôles de vitesse dans la circulation routière de l'ETEC, datant du 10 août 1998.)

**Remarque :** L'ancien Office fédéral de métrologie a changé son nom en Office fédéral de la métrologie et de l'accréditions (metas).

Les exigences relatives à l'admission par le METAS sont déterminées dans l'**Ordonnance sur la qualification des instruments de mesure (ordonnance sur les vérifications)** RS 941.210.

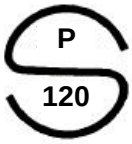



**Figure 5 : Logo METAS**

### 3.3.2. Applications en dehors de la loi fédérale sur la circulation routière

Jusqu'alors, la RPLP est la seule application dans le contexte de la circulation routière qui n'est pas réglée par la loi sur la circulation routière. La base légale de la RPLP est :

La **Loi fédérale concernant une redevance sur le trafic des poids lourds liée aux prestations (LRPL)** RS 641.81 du 19 décembre 1997, qui dit sous l'article 22 :

« [1] *La poursuite et le jugement d'infractions impliquant des véhicules suisses incombent aux autorités cantonales.*

[2]*L'Administration fédérale des douanes poursuit et juge les infractions impliquant des véhicules étrangers conformément à la loi fédérale du 22 mars 1974 sur le droit pénal administratif. »*

L'**Ordonnance concernant une redevance sur le trafic des poids lourds liée aux prestations (ORPL)** RS 641.811 du 6 mars 2000 qui dit sous chapitre 8, article 42, installations de contrôle :

*„L'Administration des douanes peut exploiter des stations de contrôle fixes ou mobiles. Elle se procure l'équipement spécial pour les équipes mobiles de contrôle et peut le mettre à la disposition des cantons. »*

## 3.4. Admission et exploitation d'une installation automatique de contrôle

La mise en service comme ça des installations automatiques de surveillance n'est pas permis en Suisse. Pour que l'exploitation de l'installation soit autorisée, les documents d'autorisation doivent être disponibles, et le dispositif doit passer la vérification officielle pour être admis à l'exploitation. En résumé, il faut passer par les étapes suivantes :

| **1. Demande écrite d'admission** |
|---|
| Un fabricant désire vendre en Suisse un instrument de mesure destiné à la détermination officielle de grandeurs physiques. Etant donné que l'autorisation officielle est requise pour exploiter de tels instruments de mesure, il dépose sa demande pour l'admission de ce type d'instrument auprès de l'Office fédéral de métrologie et d'accréditation (METAS). |
| **2. Essai de l'appareil/test typologique** |
| Le METAS réalise alors un test typologique. Ce test comprend toute une série d'essais : vérification de la précision de mesure, essai CEM, essais de température, essais en charge mécanique (par ex. vibration), essais de la tension d'alimentation etc., L'appareil est approuvé quand la précision de mesure et la fiabilité du type d'instrument de mesurage répondent aux exigences de l'application prévue. Avec cette autorisation le fabricant peut vendre le dispositif pour les applications visées.<br>**Remarque :** Les admissions étrangères sont acceptées lorsqu'elles sont conformes aux exigences suisses et à condition que la réciprocité soit garantie. |
| **3. Vérification** |
| Avant qu'un tel appareil de mesure puisse être vendu et mis en service, par ex. par un office de la police cantonale, il doit passer une procédure de vérification exécutée par un office de vérification autorisé par le Conseil fédéral. L'Office fédéral de métrologie et d'accréditation (METAS) est chargé de l'établissement des directives relatives à la vérification.<br>Le contrôle et l'étalonnage périodique des instruments de mesure assurent la conformité aux prescriptions légales de chaque dispositif de mesure. Après les examens de vérification l'installation |

| |
|---|
| de contrôle est admise à l'exploitation.<br>**Important:** Seuls les valeurs mesurées par des installations soumises à des vérifications officielles sont acceptées par les tribunaux. |
| **4. Exploitation/Vérification ultérieure** |
| Tous les instruments de mesure en service sont soumis à des procédés réguliers de contrôle et d'étalonnage obligatoire. En règle générale, le délai entre deux contrôles est d'un an. La vérification ultérieure est assurée par les offices de vérification ou par le METAS. |

**Tableau 1 : Description demande/admission/vérification des installations de contrôle**

**Source : Description d'après les renseignements donnés par M. Walter Fasel, chef du laboratoire circulation routière au METAS**

# 4. Images numériques et traitement d'images numérique

Le chapitre suivant offre un bref aperçu sur l'imagerie numérique. Comme il sert seulement de base pour les chapitres suivants, il ne traite que de façon très abrégée les applications pratiques dans le domaine du contrôle-sanction.

## 4.1. Technologie de l'imagerie numérique

Cette section décrit le fonctionnement et les composants des appareils photo numériques et des caméras vidéo numériques. En fin de compte, le chapitre devra contribuer à une compréhension homogène de la notion « (caméra) vidéo » qui, selon le contexte respectif, est utilisée de façon variée.

### 4.1.1. Structure des appareils photo numériques

Contrairement aux caméras analogiques, les appareils photographiques digitalisés enregistrent l'image sur un support électronique de stockage et non sur une pellicule. Ces appareils numériques sont équipés d'un objectif pour la représentation de l'image (comme les caméras analogiques), d'un système d'obturation (mécanique ou électronique), d'un système viseur (souvent remplacé complété par un écran numérique), d'un capteur, d'un convertisseur AN et d'un endroit de stockage des données. Alors que dans les caméras traditionnelles c'est la lumière elle-même qui assure la transmission et le stockage des informations, les caméras numériques doivent être équipées de dispositifs électroniques supplémentaires (par ex. convertisseur analogique-numérique), C'est pourquoi une alimentation en courant est indispensable pour ces dernières. La figure suivante montre de façon sommaire la structure d'un appareil photographique numérique :

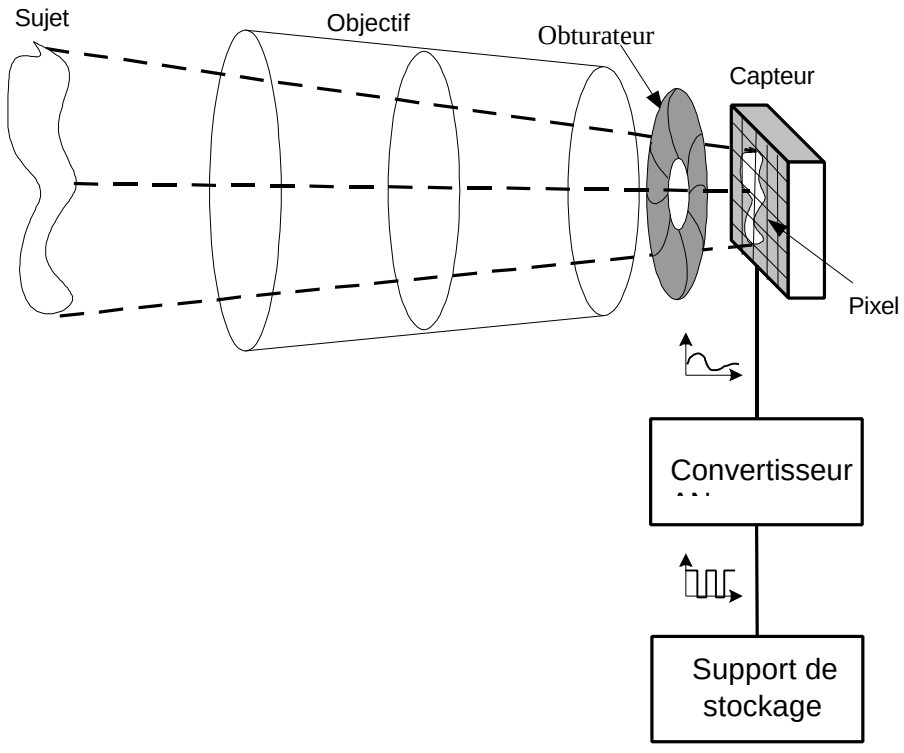



**Figure 6 : Structure fonctionnelle d'un appareil photographique numérique**

Les données émises en sortie d'un appareil photo numérique contiennent l'ensemble des informations sur l'image.

### 4.1.2. Structure des caméras vidéo

Contrairement aux appareils photographiques, les données contenues dans le détecteur d'une caméra vidéo sont rappelées en permanence. Les signaux de sortie sont des signaux analogiques. C'est seulement par le convertisseur analogique-numérique intercalé à la caméra que les informations sont converties en un flot de données numériques. La sortie d'une caméra vidéo est donc une grandeur dynamique.

Il est cependant possible de tirer des photos d'un signal (analogique) vidéo. Pour cela on utilise un logiciel de digitalisation (Framegrabber). Ce logiciel est capable de choisir certains séquences d'images dans le flot de données et de les convertir en enregistrements digitaux. Ainsi, une caméra vidéo peut quasiment être utilisée comme un appareil photographique. D'ailleurs, ce procédé permet de sauvegarder temporairement des images pour faire la sélection ultérieurement – ce qui est particulièrement intéressant pour les applications de contrôle-sanction. La décision si une image est saisie, c.-à-d. sauvegardé de façon permanente, ne doit alors pas être prise au moment du passage du véhicule dans la zone de détection.

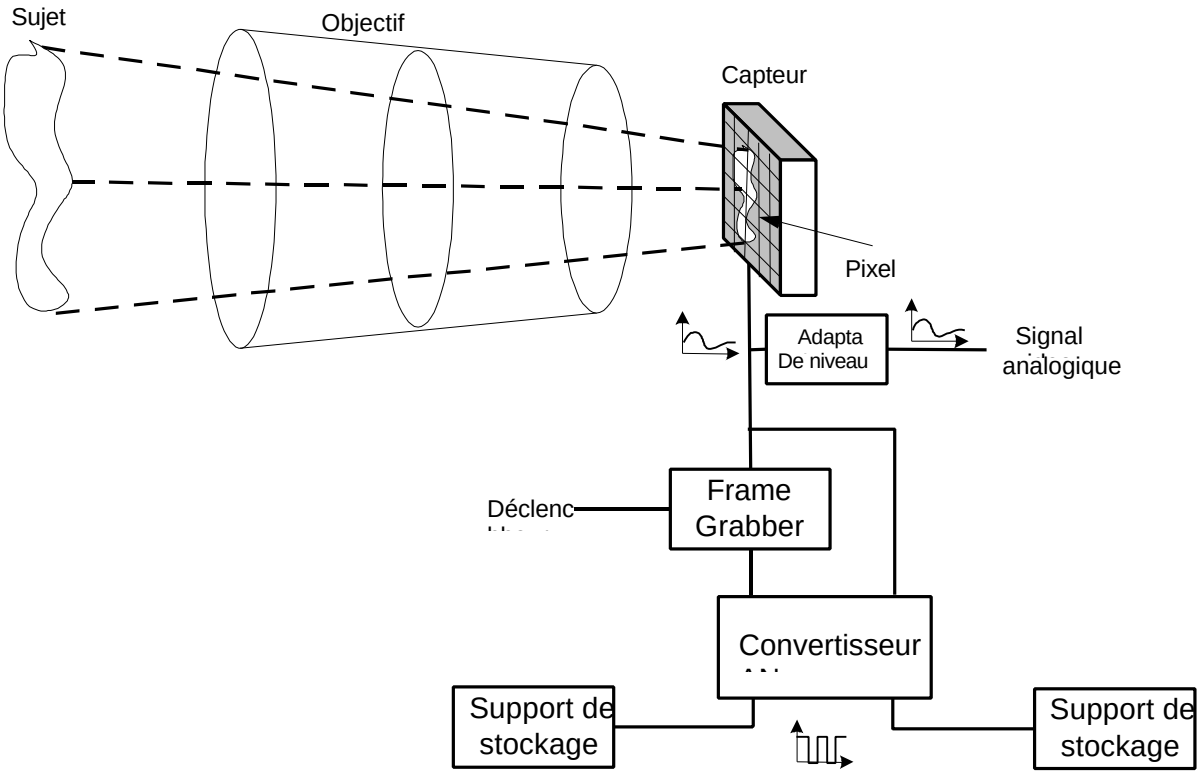



**Figure 7 : Structure fonctionnelle d'une caméra vidéo numérique avec fonction « photo »**

Les signaux obtenus à la sortie d'une caméra vidéo sont soit :

- des signaux dynamiques analogiques (signaux émis du capteur) ou
- des signaux dynamiques numériques (lors de l'utilisation d'un convertisseur AN) ou
- des signaux statiques numériques (lors de l'utilisation d'un « Framegrabber »).

### 4.1.3. Composants

**Le capteur**

Le composant central d'une caméra numérique est le capteur. C'est sa qualité qui détermine, en fin de compte, la qualité des images captées. Les principaux caractéristiques sont le nombre de photodiodes (résolution pixel) et la sensibilité du capteur. Contrairement aux caméras traditionnelles à film argentique, la sensibilité est une valeur constante des caméras numériques. Les caméras professionnelles peuvent varier la sensibilité en regroupant plusieurs pixel en un seul élément d'image pour augmenter la surface ainsi la sensibilité par pixel. Naturellement, cette mesure a pour conséquence une réduction de la résolution, ce qui d'ailleurs est aussi le cas avec les films argentiques. Plus la sensibilité est élevée, plus la résolution du film est grossière.

Le capteur se divise en de nombreux éléments dont chacun consiste enune cellule photo-électrique, sensible à la lumière, et d'une cellule mémoire. Les cellules photo-électriques transforment la lumière en tension électrique. Plus le nombre de cellules photo-électriques est élevé, plus la résolution de l'image est élevée.

**Le convertisseur analogique-numérique (CAN)**

Le capteur émet des signaux analogiques, qui doivent être digitalisés avant de pouvoir être sauvegardés sur un support de mémoire numérique. Cette tache est accomplie par un convertisseur analogique-numérique (CAN), qui quantifie le signal analogique de chaque point d'image de sorte à transformer les valeurs analogiques en bits et octets.

**Le logiciel de digitalisation (Framegrabber)**

Ce logiciel est capable de sortir des images photo d'un signal vidéo dynamique. Les données de l'image sont ensuite digitalisées à l'aide d'un convertisseur AN. La photo numérique ainsi captée peut être sauvegardée sur un support de mémoire approprié.

**L'obturateur**

De manière identique aux caméras à film argentique, les caméras numériques possèdent un obturateur pour contrôler le laps de temps pendant lequel la lumière (de la scène) peut arriver sur le capteur. La vitesse d'obturation ensemble avec la luminosité du sujet donnent la valeur qui, en fin de compte, est sauvegardée par le capteur.

Contrairement aux caméras à film argentique, les caméras numériques ne doivent pas forcément posséder d'obturateur mécanique. L'obturation du capteur se fait aussi bien de manière électronique. Toutefois, les caméras utilisées dans le domaine professionnel sont toujours équipées d'obturateurs mécaniques, car les obturateurs électroniques provoquent une luminosité résiduelle qui peut falsifier l'image.

**Le stockage des images**

Après être rappelées du capteur, les informations de l'image sont mises en mémoire. Différents supports peuvent être utilisés pour le stockage des données dans un appareil photo numérique compact. En voici des exemples:

- Carte PC (mini HD), capacité de mémoire : 200Mo-1Go
- CompactFlash, capacité de mémoire : 2-51Mo
- MiniatureCard, capacité de mémoire : 2-64Mo
- SmartMediaCard, capacité de mémoire : 2-128Mo
- MemoryStick, capacité de mémoire : 4-128Mo

Dans les systèmes à caméras fixes, il est bien sûr possible d'intégrer la mémoire directement dans un ordinateur ce qui offre l'avantage d'une capacité considérablement plus élevée que celle présentée par les supports nommés ci-avant.

→ La technologie du contrôle-sanction vidéo utilise presque sans exceptions des caméras vidéo avec une fonction « Framegrabbing ».

## 4.2. Paramètres

La teneur en informations d'une image numérique est déterminée par deux grandeurs :

- le nombre de pixels (éléments d'image) par surface
- l'intensité de la couleur (niveaux de gris pour les images NB).

La figure suivante montre comment une image numérique est formée de pixels en différents niveaux de couleur.

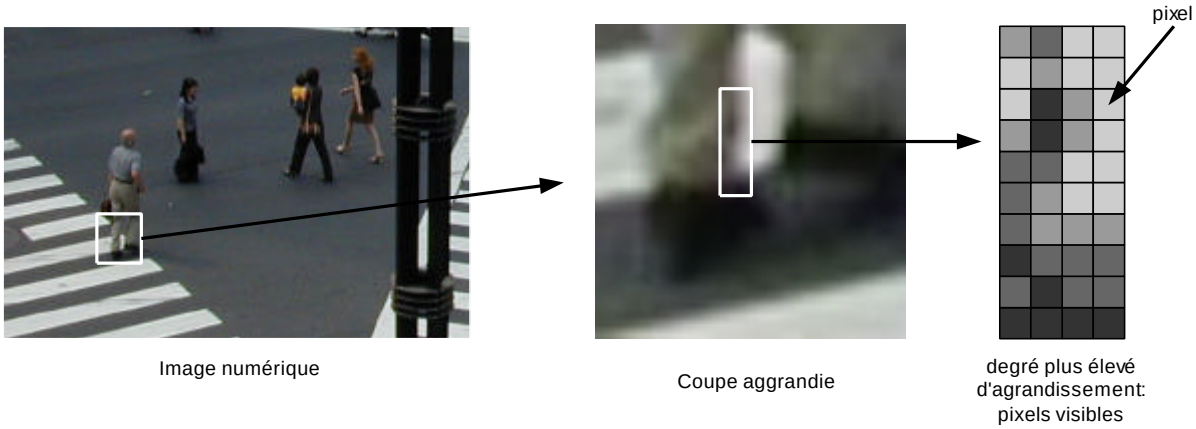



**Figure 8 : Image numérique en pixels**

Ces deux paramètres influencent directement l'encombrement de l'image dans la mémoire. De principe, il vaut : Plus la résolution et l'intensité de la couleur sont élevées, meilleure est la qualité de l'image et plus grand l'encombrement de l'image dans la mémoire. Il y a cependant des méthodes appropriées pour réduire l'encombrement. En utilisant des images à barres, on peut par ex. réduire à 1 bit l'intensité de la couleur, c.-à-d. un point peut être noir ou blanc et rien d'autre. Une autre mesure, moins rigoureuse, est l'utilisation d'une palette de couleurs. Au lieu d'attribuer 256 niveaux de luminosité d'une seule couleur à un octet, ce procédé attribue 256 couleurs à un octet. Pour cette méthode il faut toujours connaître les palettes de couleurs (les palettes standards par ex. sont connus de multiples applications PC). Cette technique est particulièrement appropriée pour les images ne contenant que peu de couleurs.

Il est évident que toutes ces méthodes de réduction d'encombrement entraînent des pertes de qualité de l'image. Les applications dans le domaine du *contrôle-sanction numérique* ne doivent donc travailler qu'avec des images à niveaux de gris ou des images couleurs RVB (RGB).

Les valeurs d'environ 2 mio. de pixels pour la résolution sont des valeurs courantes aujourd'hui. Pour l'intensité de la couleur les valeurs sont de 8-16 bits. La résolution des caméras vidéos est normalement moins élevée que la résolution des appareils photographiques. Par exemple, les caméras vidéo utilisées dans l'installation pilote RPLP possèdent une résolution de 1,2 mio. pixels et une intensité de la couleur de 8 bits. Pourtant, la qualité des appareils disponibles sur le marché augmente en permanence (comparer appareils électroniques ménagères).

→ Les deux paramètres plus importants d'une image numérique (comme élément de preuve) sont la résolution et l'intensité de la couleur.

## 4.3. Formats de stockage

Comme partout dans le domaine de l'informatique, il y a un grand nombre de formats de fichier différents aussi pour la sauvegarde d'images et de graphiques. Pour cette raison, la liste suivante se limite sur les formats les plus répandus actuellement et ne prétend pas d'être exhaustive.

| Format | Description |
|---|---|
| **Images** | |
| JFIF (Connu sous le nom JPEG) | JEPG est l'abréviation de *Joint Photographic Expert Group* – ce n'est donc pas le nom d'un format graphique mais le nom de la corporation qui a développé ce format. Le standard JPEG est un algorithme de compression de flot de données basant sur l'algorithme DCT (Discrete Cosine Transforme) et le codage de Huffman. Le format graphique du même nom est la simple application de cet algorithme à des graphiques à pixels. Entre-temps, l'algorithme JPEG s'applique aussi pour la compression de films vidéo. Le format vidéo populaire MPEG en est issue. La compression obtenue avec le format JPEG est aussi bonne que celle obtenue avec le format GIF ; de plus, le format JPEG présente l'avantage d'une capacité de stockage de 16,7 mio de couleurs par image. Le format JPEG n'utilise pas une palette de couleurs définis, comme le format GIF, mais toute la gamme de couleurs disponibles. L'inconvénient de JPEG est que la compression ne va **pas sans perte d'informations.** Plus le degré de compression est élevé, moins bonne est la qualité du graphique. JPEG permet des taux de compression 20 :1 et plus. A part les informations directement liées à l'image, il est possible d'ajouter des informations supplémentaires aux fichiers JPEG, dont le contenu dépend de l'application. |
| TIFF | Le format *Tagged Image File Format*, TIFF, est un format très répandu dans le domaine du Desk Top Publishing qui permet de traiter, de stocker et d'échanger des fichiers avec un minimum de pertes d'informations.<br>Le format est devenu un format « tous terrains ». Il est extrêmement flexible et permet de générer le format approprié pour pratiquement chaque application. En même temps c'est cette flexibilité qui rend le format très complexe. La spécification originale (TIFF révision 6.0 du 3 juin 1992) seule a 121 pages. Pour cela des fautes entraînant des interprétations fautives, sont facilement possibles Même les fabricants de logiciels graphiques ne maîtrisent presque plus ce format dans toute sa diversité.<br>La taille de l'image est limitée à env. 4 milliards de lignes sous le format TIFF (si on peut parler de limitation dans ce cas). |
| GIF | GIF est l'abréviation de *Graphics Interchange Format* qui a été mise en œuvre par Compuserve il y a beaucoup d'années. Le format GIFF est caractérisé par une forte compression. C'est la raison pour laquelle ce format s'est très vite répandu dans tout le domaine « Online » où la transmission de données est coûteuse en termes d'argent et de temps. Le standard largement répandu du format GIF est le format appelé « format 89 ». L'inconvénient inhérent au format GIF et l'intensité limitée des couleurs. L'avantage par contre réside dans la compression sans pertes des fichiers GIF. En conséquence de ces caractéristiques, le format GIF n'est pas spécialement approprié pour les graphiques à haute résolution tels que des photos.<br>Le format GIF permet une taille maximum du fichier de 16.000 x 16.000 points et une intensité des couleurs de 8 bits (256 couleurs). Le format permet soit une compression sans pertes soit une compression avec pertes selon le standard JPEG (à partir du standard 6.0). |
| BMP | BMP est un format graphique développé et introduit par Microsoft (dans Windows 3.0). Le format BMP devient de moins en moins important du fait que seulement peu de programmes permettent la compression de fichiers BMP (au moins des applications indépendantes de Windows). |
| **Formats vidéo** | |
| MPEG | MPEG est le format le plus répandu pour les fichiers comprimés de (séquences) de |

| | |
|---|---|
| | films vidéo. Afin de pouvoir traiter et transporter les quantités énormes de données de films (90 minutes, 25 images par seconde, haute résolution, nombre élevé de couleurs – cela donne env. 120 Go) avec des ordinateurs « normaux », seul les divergences par rapport à l'image précédente sont mémorisées par ex., outre le procédé de compression JPEG (contrairement au format M-JPEG). Mais le format MPEG met en mémoire dans des intervalles réguliers de typiquement douze images des « Intra-Frames » (I-Frames), qui sont des images individuelles comprimées JPEG. Les images situées entre ces « I-Frames » ne sont pas complètement sauvegardées, si possible. MPEG mémorise plutôt la façon comment les images peuvent être restaurées par décalage de parties des images précédentes ou suivantes. A cette fin s'utilisent aussi des « Predicted Frames » et des « B-Frames » (bi-directional frames) prévoyants. Comme cela ne marche jamais de manière parfaite, les variances restantes sont encore sauvegardées sous codage JPEG pour chaque image individuelle. Cette méthode permet une réduction d'env. 99% de l'encombrement des données d'un film vidéo. La compression maximale atteint jusque 200 : 1. |
| AVI | „Audio Video Interleave" (entrelacement audio vidéo) signifie que les données audio et vidéo sont stockées sous forme entrelacée (« interleaved »). A l'origine, le format AVI a été introduit par Microsoft comme solution unifiée pour la représentation de brefs clips vidéo et présentait les suivantes caractéristiques (1993) :<br>15 images par seconde avec une résolution maximale de 160 x 120 pixels.<br>Contrairement aux autres formats d'animation d'alors, le format AVI utilisait la technologie « Keyframe » (animation par scènes clés). Avec cette technologie seulement une image sur 12 à 17 (en dépendance du contenu) est sauvegardée sous forme complète. Pour les „Frames" intermédiaires seul les différences à l'image précédente sont enregistrées. Bien que ces premières définitions n'étaient pas très prometteuses, le format AVI a très vite connu un succès considérable. Une raison en est sûrement le fait que AVI soit bientôt lié à Windows comme composant de « Video for Windows ». Les logiciels pilote étaient, et le sont toujours, disponibles gratuitement pour l'utilisateur. |

**Tableau 2 : Liste des formats graphiques les plus répandus**

→ Dans le domaine des installations pour la surveillance de la circulation ce sont surtout des formats propriétaires qui sont utilisés – pour le format graphique ainsi que pour le procédé de compression. Ceux-ci ne constituent pourtant pas de technologies complètement nouvelles mais sont développés sur la base de procédures existantes. L'inconvénient de systèmes et formats propriétaires réside dans le manque de portabilité, donc dans la dépendance envers le fabricant respectif.

## 4.4. Méthodes de compression

Pour réduire la capacité nécessaire des mémoires et la largeur de bande requise pour la transmission, on se sert de procédés de compression. On peut faire la distinction entre deux groupes fondamentaux de méthodes de compression:

- les algorithmes réversibles, et
- les algorithmes irréversibles.

### 4.4.1. Algorithmes réversibles

Avec les algorithmes réversibles il est possible de restaurer les données originales à partir des données comprimées. Il s'agit d'une compression dite « sans pertes », où les informations sont comprimées sans être modifiées dans un format optimisé en terme encombrement. Cette méthode est particulièrement efficace pour les images contenant des grandes surfaces teintes. Pour les photos numériques, cependant, elle ne présente pas de grands avantages car les grandes surfaces à une seule couleur précise sont très rares dans

ce cas, ce qui est dû, entre autres, au bruit coloré. Les images comprimées à l'aide d'une procédure réversible peuvent toujours être amenées à leur état original. La compression ne laisse aucune „trace" dans l'image.

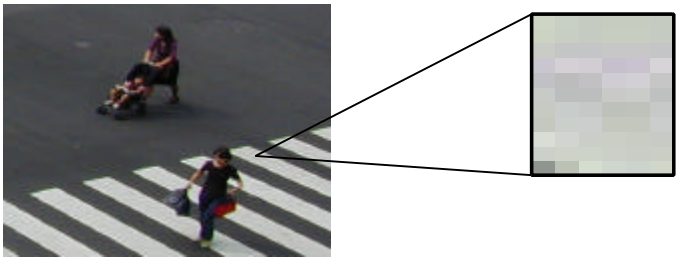
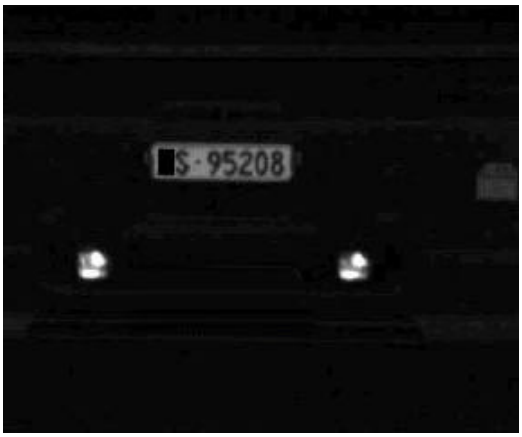


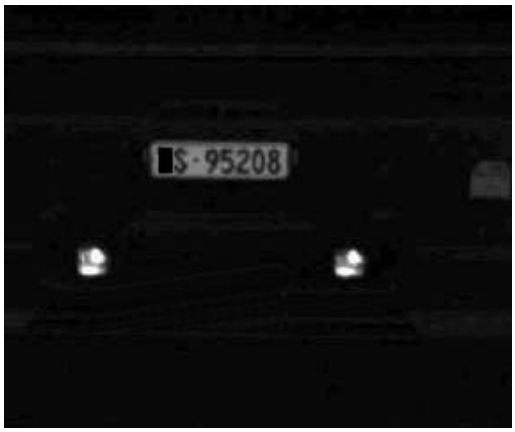
**Figure 9 : Exemple d'une surface avec des variations légères de la couleur**

### 4.4.2. Algorithmes irréversibles

Le groupe des procédures irréversibles profite des points faibles de la perception humaine et élimine les informations superflues qui ne sont pas, ou seulement à peine, visibles pour l'œil humain. Plus le degré de compression est élevé (compression forte = encombrement petit), plus les modifications de l'image deviennent visibles. Des informations sont perdues au cours de ce procédé de compression. Après être comprimées à l'aide d'une procédure irréversible de compression les données originales ne peuvent en conséquence plus être restaurées.



Compression: 0% Taille: 24Ko



Compression: 50% Taille: 4Ko

Compression: 90% Taille: 3Ko

Compression: 95% Taille: 2Ko

**Figure 10 : Exemple pour différents degrés de compression JPEG**

Comme on reconnaît dans la Figure 10, les manipulations de l'image sont plus ou moins visible, selon le degré de compression. Sur l'image droite, en bas, on voit qu'il peut même y avoir des falsifications des chiffres (8 → O) dans la plaque d'immatriculation. Il s'agit donc de trouver une mesure raisonnable de compression pour chaque application individuelle.

→ Selon la procédure et le degré de compression utilisés, la compression peut falsifier, et même rendre méconnaissable, le contenu de l'image. Il en résultent des restrictions pour la compression des images numériques captées pour les contrôles automatiques de la circulation.

## 4.5. Mécanismes de protection pour données numériques

### 4.5.1. Le tatouage électronique

On appèle tatouage des signatures numériques incorporées dans l'image qui informent sur les droits de l'auteur de l'image (normalement de façon non visible pour l'œil humain).

La fonction du tatouage – contrairement à la signature – est de rester le plus intact que possible, même en cas d'interventions (illégitimes). Comme ça seulement on peut prouver l'origine, par ex. d'une image pourvue d'un tatouage sans aucun doute possible. Dans le domaine de l'imagerie numérique, le tatouage électronique est très répandu. Il est utilisé spécialement pour la poursuite de copies illégales dans l'Internet. Le système le plus répandu dans ce contexte est PictureMarc de l'entreprise Digimarc (http://www.digimarc.com). Il est utilisé par exemple dans les applications Microsoft.

Etant donné que dans le domaine du contrôle-sanction, l'aspect des droits d'auteurs est beaucoup moins important que celui de l'intégrité des données, le tatouage numérique ne sera pas décrit plus en détail ici.

**Objectif du tatouage électronique: Vérifier les droits d'auteur**

### 4.5.2. Signatures

Les signatures électroniques s'utilisent partout où les données doivent être protégées contre une modification inaperçue. Elles servent donc à l'authentification de documents, ou mieux, d'enregistrements.

Les signatures permettent de démontrer de façon incontestable qu'un document ou un enregistrement se trouve toujours à l'état original. En plus, il est possible avec une signature numérique de démontrer clairement qui (quelle personne ou quel ordinateur) a crée la signature.

Dans le contexte de l'utilisation d'images numériques pour les contrôles automatiques de la circulation, les signatures constituent l'outil idéal pour prouver l'authenticité des enregistrements A cette fin, on ajoute des signatures aux images, aux informations supplémentaires mais aussi aux séquences complètes de données (plusieurs images + informations additionnelles) qui sont alors vérifiable comme un seul enregistrement Cette protection n'est pourtant effective qu'après la création de la signature. Il reste donc le risque de confusion des données avant la création de la signature.

Pour créer une signature, le signataire crée d'abord un « Hash » (=excerpt) sur les données à signer et code ensuite ce hash avec une clé. Si l'on veut, à un moment plus tard, vérifier l'authenticité des données, on calcule à nouveau ce « Hash » sur les données cryptées. Ensuite, on déchiffre la signature et compare la valeur « Hash » de la signature à la valeur calculée. Si ces deux valeurs sont identiques, on peut assumer que les données sont authentiques.

**Important:** Les enregistrements pourvus d'une signature restent toujours lisibles de l'extérieur, ils ne sont pas chiffrés (Plain) ! La signature est un élément informatif supplémentaire qui est ajouté aux données. Mais la signature ne protège pas contre les

manipulations qui, toutefois, deviennent vérifiables à l'aide d'une signature. La signature est un outil qui permet de certifier l'authenticité des données signées.

**Objectif de la signature: Vérifiabilité de l'authenticité**

### 4.5.3. Cryptage

Pour protéger les données (en particulier au cours de la transmission) contre la lecture non autorisée par de tiers, elles sont échangées sous forme cryptée. Le récipient des données les déchiffre ensuite et récupère le texte original. Le niveau de sécurité du cryptage est déterminé par la longueur de la clé utilisée (à part de l'algorithme). La longueur indique combien de combinaisons sont possibles pour la clé. Plus la clé est longue, plus il devient difficile pour les personnes non autorisées au système de déchiffrer le message. Seulement, qu'avec une longueur croissante de la clé les opérations deviennent plus complexes pour le chiffrement et le déchiffrement de celle-ci.

La figure suivante montre le principe du chiffrement électronique. Le procédé de cryptage (algorithme cryptographique) est utilisé pour modifier un message à l'aide d'une clé de sorte que son contenu ne peut être interprété par de tiers (cryptage). Et sous cette forme chiffrée le message est transféré. Le récipient peut restaurer le message original seulement à condition qu'il dispose de la clé appropriée (déchiffrement).

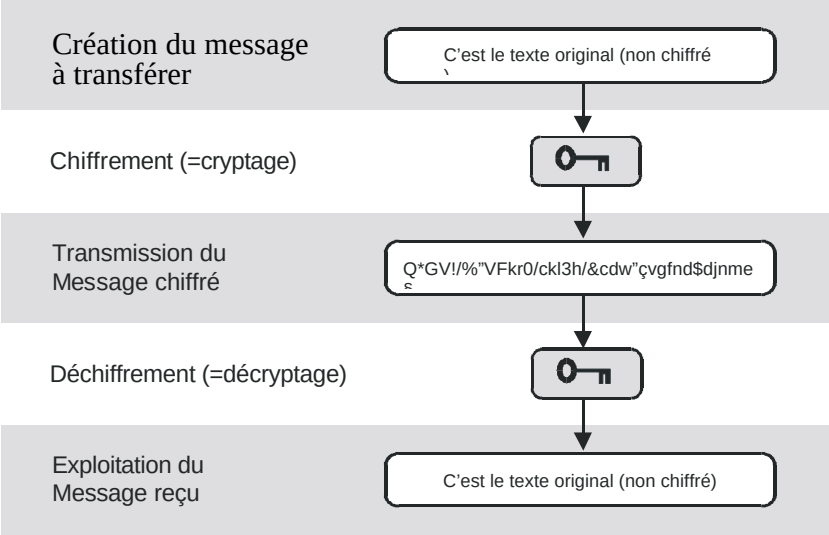



**Figure 11 : Le principe du procédé de cryptage**

La distinction est faite entre deux types fondamentaux de cryptage :

**Cryptage symétrique**

On parle de cryptage symétrique lorsque la même clé est utilisée pour le chiffrement et pour le déchiffrement. La condition en est que toutes les personnes concernées possèdent la même clé. Il faut donc que l'échange de la clé se fasse par voie d'un canal sûr, ce qui constitue un problème dans les applications pratiques. L'avantage de cette méthode est qu'elle est relativement facile à maîtriser. Les algorithmes demandent relativement peu d'opérations.

DES et 3DES (prononcé « triple-des ») sont les deux méthodes de chiffrement symétrique les plus répandues, 3DES n'étant cependant que la triple application DES avec deux clés différentes.

**Cryptage asymétrique**

Contrairement aux procédures symétriques, les méthodes asymétrique de cryptage utilisent toujours une paire de clés : une clé privée (Private Key) et une clé publique (Public Key). Il n'est absolument pas possible de conclure une clé à partir de l'autre. La transmission de données cryptées par un procédé asymétrique de chiffrement se déroule comme suit :

1. L'expéditeur prend le message qu'il veut envoyer et le chiffre avec la clé publique du récipient. Cette clé est accessible pour tout le monde.
2. Le message chiffré est transmis.
3. Le récipient déchiffre alors le message avec la clé privée que lui seul connaît.

L'avantage de cette méthode est que la clé vraiment importante (la clé privée) ne doit jamais être transmise après l'initialisation du système, car seulement une personne en a besoin. D'ailleurs, le cryptage asymétrique permet de vérifier l'authentication du récipient car il fonctionne dans les deux sens : chiffrement avec clé privée/déchiffrement avec clé publique, mais aussi chiffrement avec clé publique/déchiffrement avec clé privée. Si alors l'expéditeur a chiffré son message à l'aide de la clé privée et le récipient est capable de le déchiffrer à l'aide de la clé publique, ce dernier peut être sûr que le message provient de l'expéditeur supposé, parce que c'est lui seul qui possède la clé privée.

Un grand inconvénient de cette méthode asymétrique est pourtant que les opérations nécessaires pour le calcul sont très complexes. Pour cette raison, il est très rare que des documents entiers soient cryptés à l'aide du procédé asymétrique de cryptage. Dans la plupart des cas, ce sont plutôt les parties les plus importantes du document telles que les valeurs « Hash » qui sont cryptées par cette méthode.

L'algorithme le plus utilisé pour le chiffrement asymétrique est l'algorithme RSA.

Souvent, on utilise un mélange de procédés symétriques et asymétriques de chiffrement, où le message est chiffré avec une méthode symétrique avant d'être transmis. La clé symétrique nécessaire pour le décodage est également chiffrée, cette fois à l'aide d'un procédé asymétrique, et également envoyé au récipient. En utilisant sa clé privée, le récipient obtient la clé symétrique avec laquelle il peut ensuite déchiffrer le document.

**Remarque :** En essayant toutes les clés possibles, tous les codes peuvent être déchiffrés, théoriquement. Le temps et le travail nécessaires à cette fin augmentent de façon dramatique en fonction de la longueur de la clé. Ce qui vaut pourtant aussi pour les opérations de chiffrement et déchiffrement. Il s'agit alors de trouver le meilleur compromis entre la sécurité requise et les exigences en termes de travail et de temps pour chaque application individuelle d'une clé.

**Objectif du cryptage: Protection contre les accès non autorisés**

→ Les mécanismes de sécurité constituent des outils importants pour la protection des données numériques. Ce sont surtout les signatures (intégrité/authenticité) et le cryptage (protection contre les accès non autorisés) qui seront utilisés pour les enregistrements dans la surveillance automatique des transports.

## 4.6. Traitement ultérieur de l'image

Contrairement à l'imagerie traditionnelle, il est très facile de traiter ultérieurement et de façon abondante les images numériques. Dans le contexte des images numériques utilisées pour la surveillance automatique de la circulation, un traitement ultérieur n'est pourtant imaginable que dans l'objectif de permettre une meilleure reconnaissance des images. Dans l'exemple concret de l'installation de contrôle-sanction du système RPLP, il est possible de modifier à partir du terminal de commande la luminosité, la netteté et la valeur gamma des

images. De toute façon, on ne modifie jamais les données originales de l'image mais seulement leur copie sur l'écran afin d'améliorer la lisibilité des images pour l'utilisateur. Il s'agit donc seulement d'une « fonction d'assistance à l'affichage ».


Valeur gamma = 1 Valeur gamma = 2

**Figure 12 : Exemple pour le traitement ultérieur de l'image**

A la limite il serait concevable pour les applications futures de rendre certaines parties de l'image illisibles. Ce qui pourra devenir important dans le contexte du contrôle-sanction au-delà des frontières.

→ Le traitement ultérieur des images peut comprendre les plus diverses opérations. Dans le domaine du contrôle-sanction il s'agira cependant en première ligne de procédures de traitement liées à l'affichage des images qui seront appliquées pour permettre une analyse plus aisée des images.

# 5. Architecture du système

Dans ce chapitre il s'agit de décrire le déroulement du procédé de contrôle-sanction par un modèle approprié. L'objectif est de diviser le procédé global en différents blocs fonctionnels. D'une part, le modèle doit permettre la concentration sur les points centraux, d'autre part, il doit fournir les bases pour une prise en considération globale.

## 5.1. Description et analyse de systèmes exemplaires

Une analyse des systèmes existants de contrôle-sanction devra fournir des informations sur leur structure. Il s'agit de trouver des éléments parallèles des systèmes différents et de les traduire sur la conception du modèle.

### 5.1.1. Dispositif de surveillance des feux rouges avec boucles à induction

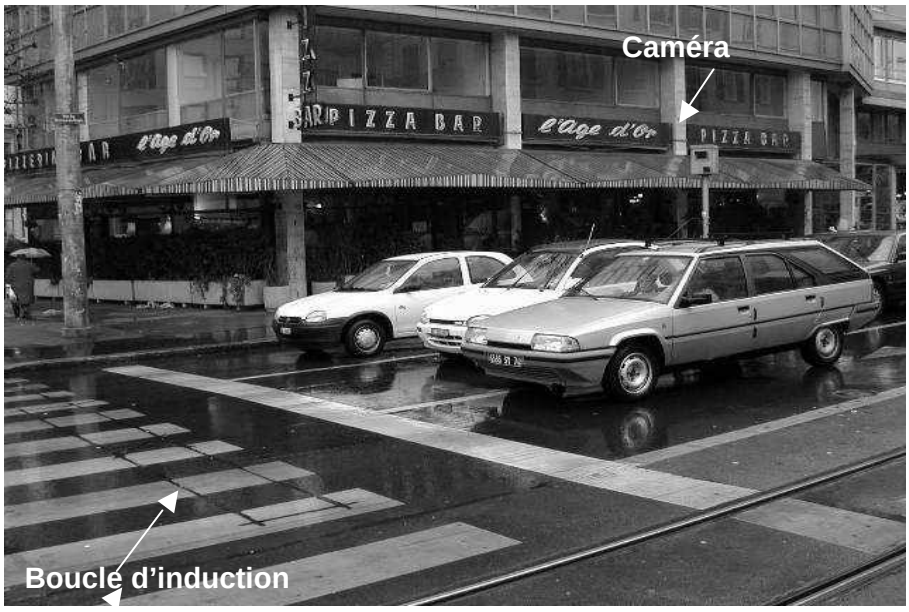



**Figure 13 : Contrôle automatique des feux rouges avec boucle d'induction après la barre d'arrêt**

Les installations de contrôle automatique des feux rouges du type décrit ci-après sont utilisées depuis longtemps en Suisse. Le système décrit est un exemple typique pour une application à film argentique.

**Architecture du système**

L'installation comprend les suivants composants :

- deux boucles d'induction
- une caméra pour la prise des images servant comme élément de preuve
- une logique pour traiter les signaux, contrôler la caméra, le temps de système etc.

Les deux boucles d'induction sont montées à une distance définie après la ligne d'arrêt. Les boucles transfèrent leurs signaux à une station centrale de contrôle où est installé l'ensemble des autres composants du système. Cet élément est d'ailleurs lié au dispositif de commande du feu rouge à surveiller. C'est donc à partir de là que le dispositif de surveillance reçoit les informations sur l'état (rouge, orange, vert) des feux.

**Déroulement du contrôle**

Les boucles d'induction reconnaissent un véhicule passant la ligne d'arrêt. En même temps, la vitesse du véhicule est mesurée. Les boucles envoient alors les valeurs mesurées à la station de contrôle qui en assure l'exploitation. Le système produit une image, quand :

- le feu est au rouge et le véhicule passe les boucles avec une vitesse >8km/h (cette dernière condition évite que des images superflues soient prises dans en cas de bouchons) → infraction = non-respect du feu rouge.
- le feu est au vert et le véhicule passe les boucles avec une vitesse > que la vitesse maximale autorisée → infraction = dépassement de la vitesse maximale autorisée.

Après un délai prédéfini (typiquement 0,5 ou 1 seconde), une deuxième photo est prise automatiquement. Cette photo est nécessaire pour répondre à l'exigence d'un deuxième procédé indépendant de mesurage.

Toutes les données et informations importantes (heure, temps écoulé depuis le début de la phase rouge etc.) sont directement incrustées dans l'image lors de la prise en photo ce qui rend les confusions lors de l'assemblage des images et des valeurs mesurées impossible. Afin de pouvoir vérifier ultérieurement l'état de l'installation de feux, le feu même est également inséré dans l'image – via fibres optiques.

Les pellicules (films argentiques) sont cherchées périodiquement au poste de contrôle et développées. Sur une pellicule complète se trouve toujours un grand nombre de photos, et ce fait est utilisé et accepté comme preuve de l'intégrité et de l'authenticité de l'image qui sert de pièce à conviction. C'est pourquoi la pellicule originale est archivée en une pièce pour pouvoir servir plus tard dans les argumentations éventuelles.

→ L'enchaînement physique des images sur la pellicule constitue un aspect important pour prouver ultérieurement l'authenticité des images.

**Traitement des données de contrôle-sanction**

Le traitement des données comprend de principe deux actions :

- la vérification manuelle et/ou évaluation de l'événement.
- la détection de la plaque d'immatriculation dans les images.

La vérification et l'évaluation manuelle de l'événement servent à confirmer si ou non il s'agit d'un non-respect du feu rouge et si les images captées suffisent pour documenter l'infraction de façon indiscutable.

Dans le cas où l'infraction serait confirmée par le procédé de jugement manuel, on procède à la reconnaissance de la plaque d'immatriculation. Cette reconnaissance des plaques d'immatriculation se fait soit par processus automatique soit par procédé manuel. Dans le cas d'une reconnaissance automatique il faut d'abord digitaliser l'image (scanner). Ensuite, le propriétaire de la voiture en question est déterminé et la procédure judiciaire est déclenchée.

### 5.1.2. Contrôle automatique de trajectoire

Le contrôle automatique de trajectoire est une application typique de contrôle-sanction qui est devenue possible grâce à l'imagerie numérique. Il constitue un très bon exemple pour la modification des cycles comparé aux installations traditionnelles.

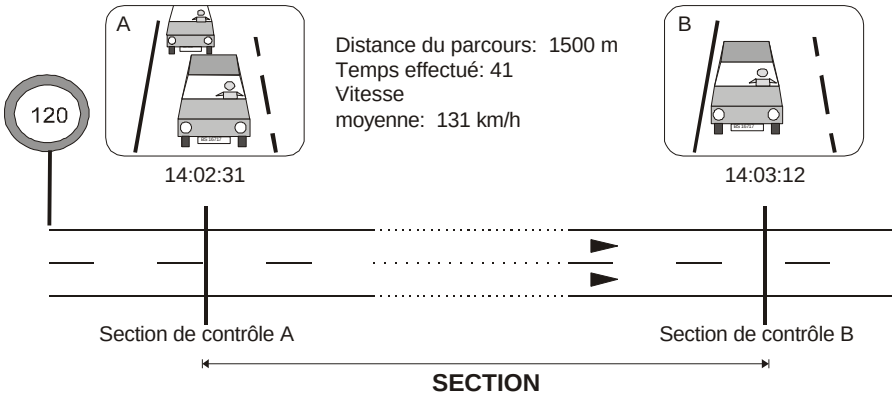



**Figure 14 : Contrôle de trajectoire**

**Architecture du système**

Le système de contrôle de trajectoire consiste en deux postes de contrôle qui sont chacun équipé d'une caméra avec éclairage et dispositif de déclenchement. Les deux postes sont liés par ligne de données. L'un des deux postes possède un logiciel d'exploitation à l'aide duquel se fait la comparaison des images, c'est-à-dire des véhicules montrés sur les images. Une station centrale assure le traitement et la gestion de toutes les données enregistrées

**Cycle de contrôle**

Le véhicule passe le premier poste de contrôle. Indépendamment de la vitesse et du type du véhicule une image est prise et le temps de passage est enregistré. L'enregistrement (image + temps de passage) ainsi établi est transmis au deuxième poste de contrôle où il est temporairement mis en mémoire. Ici aussi, une image est prise de chaque véhicule passant le poste et le temps de passage exact est enregistré. Le logiciel d'exploitation tente alors de corréler les deux enregistrements se référant à une même voiture. La comparaison des enregistrements n'est pas faite sur la base des plaques d'immatriculation mais sur la base d'une comparaison directe des caractéristiques du véhicule. Si les deux enregistrements se référant à un véhicule sont trouvés, le logiciel calcule la vitesse moyenne du véhicule sur la distance parcourue au moyen de la différence de temps entre les deux passages et de la distance entre les deux sections de contrôle. Les données sont immédiatement effacées, si la vitesse moyenne du véhicule est dans la limite admissible, Cependant, si la vitesse dépasse la limite admissible, les données sont transmises à la station centrale.

**Traitement des données enregistrées**

Le traitement des données enregistrées est assuré par le bureau central de traitement. L'action principale consiste à vérifier si la classification des images est correcte, c'est-à-dire, s'il s'agit vraiment du même véhicule sur les deux images. D'ailleurs, il s'agit de vérifier si la force probatoire des images contenant une infraction suffit pour répondre aux exigences (le conducteur et le véhicule sont-ils clairement reconnaissables ?). Ensuite, il faut détecter la plaque d'immatriculation soit par un processus automatique de reconnaissance des plaques d'immatriculation soit par procédé manuel. Ensuite, la procédure judiciaire peut être déclenchée.

→ Le déroulement des opérations peut varier considérablement en fonction de l'application concernée.

## 5.2. Modèle fonctionnel

L'objectif est d'établir un modèle fonctionnel pour la procédure entière de contrôle-sanction. Un modèle *contrôle-sanction numérique* généralement applicable doit d'abord permettre la réalisation technique des trois fonctions principales. En aucun cas le modèle ne doit poser des limites, surtout en ce qui concerne le déroulement chronologique des différentes fonctions du système.

En considérant les applications de contrôle-sanction décrites dans les chapitres 0 et 0, on peut clairement spécifier les fonctions communes. Ces fonctions communes sont particulièrement évidentes lorsque les cycles de contrôle-sanction sont divisés en les suivantes fonctions subordonnées :

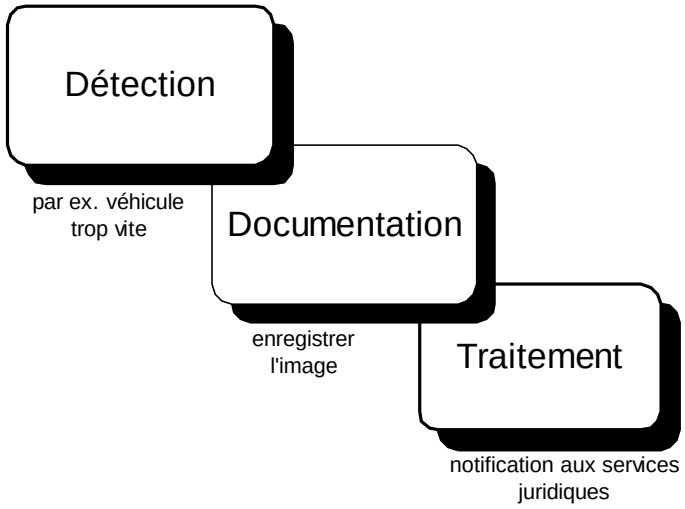



**Figure 15 : Sous-fonctions du cycle de contrôle-sanction**

Le modèle fonctionnel se décrit par les trois fonctions qui, pour une meilleure compréhension, sont appliquées ci-après sur deux procédés de contrôle-sanction.

| **Fonction** | **Contrôle automatique des feux rouges** | **Contrôle de trajectoire** |
|---|---|---|
| **Détection** | • Etat: feux="rouge" ET v>8km/h | • Différence de temps entre poste 1 et poste 2 inférieure à la limite admissible |
| **Documentation** | **Recueillir**<br>• Images servant de pièce à conviction (avec données supplémentaires incrustées dans l'image) | **Recueillir**<br>• Image 1 (poste de contrôle 1)<br>• Image 2 (poste de contrôle 2)<br>• Données supplémentaires (vitesse moyenne, date/temps, lieu etc.) |
| | **Transférer**<br>• Chercher la pellicule | **Transférer**<br>• Transmettre les données (par ex. via WAN) |

| | | |
|---|---|---|
| | **Archiver**<br>• Archivage des pellicules | **Archiver**<br>• Archivage des données sur un support approprié |
| **Traitement** | • Analyse manuelle de l'événement enregistré.<br>• Détection de la plaque d'immatriculation dans les images. | |

**Tableau 3 : Application du modèle sur des exemples de contrôle-sanction**

### 5.2.1. Détection de l'évènement

La fonction détection de l'événement sert à déterminer si et dans quelle mesure un conducteur a commis une infraction à la loi et aux règlements en matière du trafic routier en vigueur.

Souvent, la fonction de détection de l'évènement ne constitue pas un seul procédé mais se divise en plusieurs étapes. Alors que dans l'exemple 5.1.1. la fonction détection consiste en une seule action, la détection de l'exemple 5.1.2 comprend plusieurs opérations différentes. Pour satisfaire à cette exigence, il faut subdiviser encore le terme „détection des évènements" :

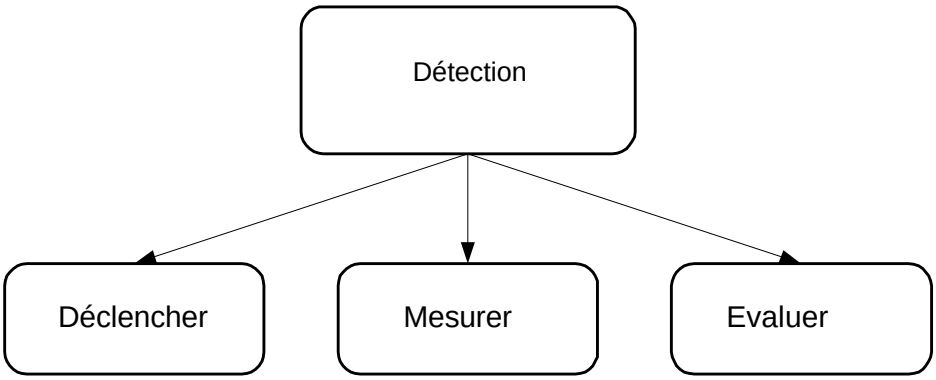



**Figure 16 : Sous-fonctions Détection**

Définitions:

| Terme | Définition |
|---|---|
| Détection | Ce terme désigne la procédure entière employée pour constater une infraction. |
| Déclencher | Mécanisme de déclenchement au cours du processus de contrôle-sanction, tel que par ex. l'impulsion de déclenchement pour la prise d'une photo. |
| Mesurer | Procédé qui procure une valeur mais qui, à elle seule, ne déclenche pas d'action. |
| Evaluer | Processus logique pour évaluer les valeurs mesurées. |

**Tableau 4 : Termes Détection/Déclencher/Mesurer/Evaluer**

### 5.2.2. Documentation

Le processus de documentation enregistre les infractions détectées à l'aide de données recevables comme éléments de preuve. La fonction principale de documentation peut être subdiviser en les trois fonctions suivantes :

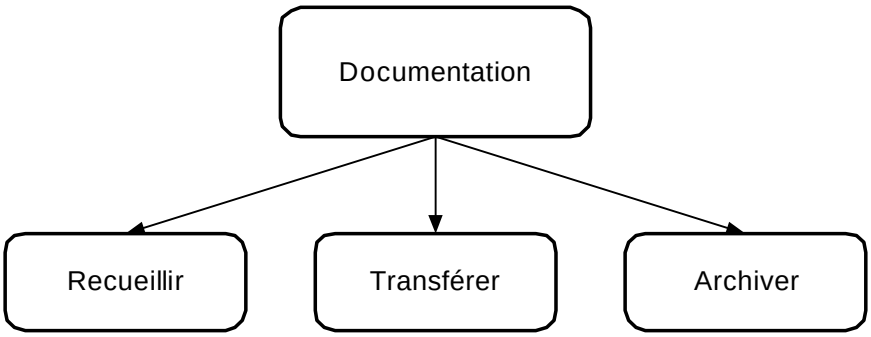



**Figure 17 : Sous-fonctions Documentation**

Définitions:

| Terme | Définition |
|---|---|
| Recueillir | Etant donné qu'il s'agit ici d'un procédé de contrôle automatique - c'est-à-dire qu'il n'y a pas de procès-verbaux supplémentaires donnés par ex. par des personnes assermentées – il est nécessaire que les données elles-mêmes documentent l'infraction d'une façon à garantir la recevabilité comme élément de preuve. Dans le cas du *contrôle-sanction numérique* l'image constitue l'élément principal de la documentation. Pourtant, des informations additionnelles sont possibles ou requises, par exemple : valeurs mesurées, paramètres, site de contrôle, temps etc. Le terme « recueillir » désigne ici le procédé qui comprend aussi la classification des données. |
| Transférer | Les données enregistrées doivent être transmises de l'installation de contrôle à l'endroit où le traitement ultérieur (par ex. bureau central) a lieu. Il y a toute une variation de supports utilisables à cette fin : transfert par ligne, transmission radio, supports de mémoire portables etc. |
| Archiver | Arrivées à leur destination, les enregistrements doivent être stockés/archivées de façon à permettre leur traitement ultérieur et toutes les opérations d'exploitation des données qui s'avèrent nécessaire. En plus, il faut assurer que les clés cryptographiques requises resteront disponibles pendant le temps complet de l'archivage. |

**Tableau 5 : Termes recueillir/transférer/archiver**

### 5.2.3. Traitement

Le traitement contient toute la gamme d'opérations d'exploitation après le transfert des données de l'installation du contrôle, ce qui peut comprendre :

- La vérification des résultats fournis du dispositif de contrôle
- La saisie des données nécessaires pour le traitement ultérieur (par ex. plaques d'immatriculation ou propriétaire du véhicule)
- Le traitement ultérieur des images
- L'exploitation supplémentaire des valeurs mesurées

Le type et le nombre des opérations de traitement dépendent en première ligne de l'application respective et du dispositif de contrôle. Pour cette raison, il n'est pas possible de présenter une liste exhaustive des opérations.

## 5.3. Structure des données

Les systèmes à traitement d'images numérique exploitent une quantité énorme de données. Il est donc d'une importance cruciale que ces pièces à conviction sous forme électronique soient traitées de façon correcte. Pour pourvoir considérer l'architecture d'un système de contrôle-sanction, il est indispensable que les enregistrements aient une structure claire et uniforme.

Si l'on compare les applications de contrôle-sanction décrites dans les 0 et 0, on découvre des parallèles de la structure des données. De façon analogue à la description des différentes étapes du cycle de contrôle, il est nécessaire de définir séparément les différents éléments de données. Dans la suite les termes cités dans le tableau 6 seront utilisés :

| Terme | Définition |
|---|---|
| Enregistrement | Données de description d'un événement. Le contenu de l'enregistrement se subdivise en plusieurs éléments de données, voir 5.4. |
| Cas | Un cas décrit (au niveau administratif) une infraction à suivre. Eventuellement, le cas peut être décrit par plusieurs enregistrements |

**Tableau 6 : Définition enregistrement / cas**

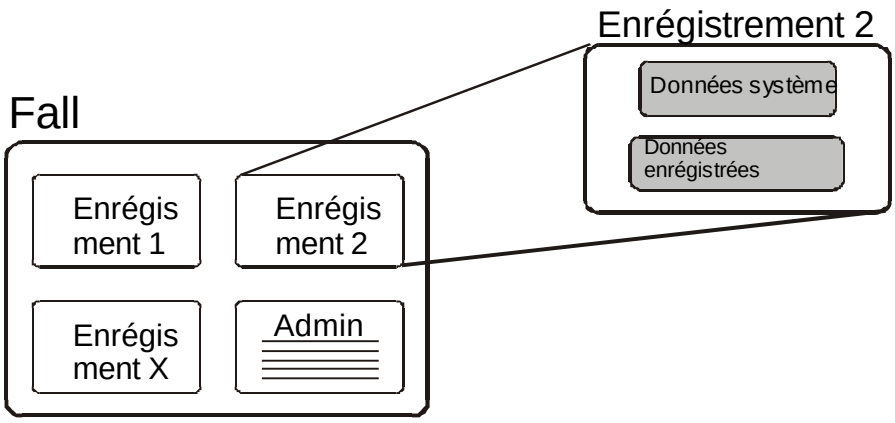



**Figure 18 : Contenu cas / enregistrement**

L'enregistrement pour sa part constitue en plusieurs éléments de données. Les éléments peuvent être divisés en deux groupes :

| Groupe | Description |
|---|---|
| Données système | Informations sur le dispositif de contrôle telles que type du système, version, n° de l'appareil, réglage, statut etc. Ces données sont indépendantes du véhicule contrôlé. |
| Données enregistrées | Les informations sur le véhicule contrôlé telles que vitesse, données de déclaration, catégorie, résultat LPR/OCR etc. Ces données sont recueillies pour chaque véhicule contrôlé. Les données comprennent aussi les données numériques des images, comme les photos et/ou les séquences vidéo. |

**Tableau 7 : Classification des données au sein d'un enregistrement**

## 5.4. Structure physique

De façon analogue au modèle fonctionnel, il est possible de subdiviser le système global (physique) d'une installation de contrôle-sanction en plusieurs sous-systèmes. La division en les trois parties suivantes paraît raisonnable :

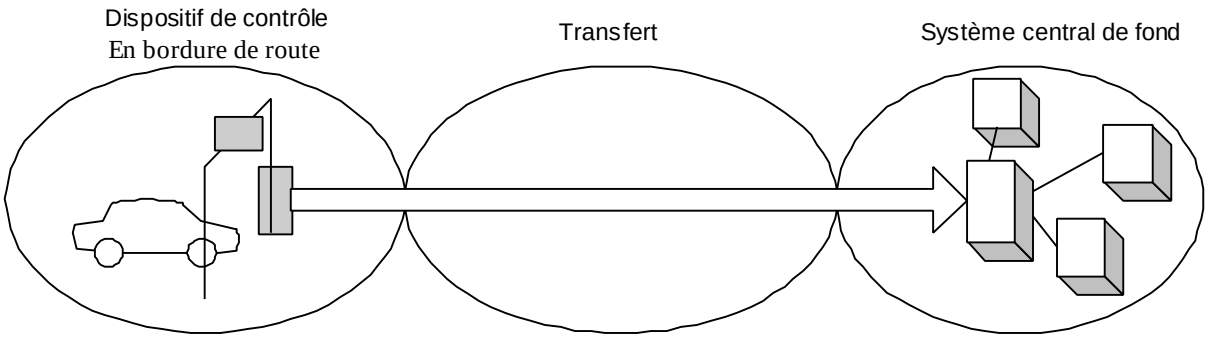



**Figure 19 : Les parties subordonnées d'un système de contrôle-sanction**

**Dispositif de contrôle en bordure de route**

Cette partie englobe l'ensemble des dispositifs de contrôle sur site et consiste en particulier des dispositifs de saisie d'image, de l'équipement de mesurage et, le cas échéant, d'un système électronique d'exploitation d'images.

**Canal de transmission**

Le terme désigne en première ligne le canal de transmission des données entre le dispositif routier de contrôle et le système central de fond. Pourtant, cela n'exclue pas les autres voies de transmission éventuellement existantes telles que, par exemple, des liaisons entre les composants individuels d'un système, comme on les trouve dans les installations de contrôle de trajectoire.

**Système central de fond**

Ce système assure le traitement ultérieur des enregistrements, par exemple la confirmation manuelle des résultats LPR/OCR (reconnaissance automatique des plaques d'immatriculation/reconnaissance des chiffres et caractères), ou bien la vérification des résultats du processus de classification. A la suite, le système assure l'archivage et la gestion des données.

# 6. Analyse des lacunes normatives

## 6.1. Délimitation des lacunes normatives

Pour la norme à mettre en œuvre la question se pose à savoir quels domaines peuvent et/ou seront à décrire par la norme.

Il faut examiner les trois sous-fonctions définies dans le chapitre 0 :

- Détection
- Documentation
- Traitement

en vue d'un besoin éventuel de normalisation. Cette étude doit être établie sous les trois angles – structure fonctionnelle / structure des données / structure physique.

**Sujet du projet de recherche**

Le titre officiel de cette mission de recherche est : *« Systèmes pour les contrôles routiers automatiques (Enforcement) avec traitement d'images numériques et les systèmes pour la reconnaissance automatique des plaques d'immatriculation « .* En considérant ce titre on supposerait que la norme se réfère à et/ou traite au moins le traitement d'images numériques et la reconnaissance automatique des plaques d'immatriculation (LPR/OCR).

En considérant le modèle fonctionnel, cela n'est plus aussi évident.

**Qu'est-ce qui a changé?**

Qu'est qu'il y a de nouveau dans les systèmes considérés ici ? Ce n'est pas tellement le traitement d'images numériques et le processus LPR/OCR, mais plutôt l'utilisation de la technologie numérique pour la prise d'images dans les dispositifs automatiques de contrôle. Le LPR/OCR peut aussi être utilisé (et est utilisé) dans des installations traditionnelles à film argentique. La seule différence est que l'image doit être scannée / digitalisée avant son exploitation. Mais à ce point (traitement dans le système central de fond) le processus central et essentiel est déjà complété. L'image comme élément de preuve, qui contient toutes les informations importantes, est déjà disponible dans une forme recevable par les tribunaux. Le traitement électronique ne constitue alors qu'un procédé purement auxiliaire, sans grande importance du point de vue juridique. Que ce soit une personne ou un appareil à reconnaître la plaque d'immatriculation dans l'image ne joue qu'un rôle mineur pour la procédure. L'essentiel est ce qui est réellement documenté sur l'image ou par enregistrement utilisé comme élément de preuve.

**Bilan**

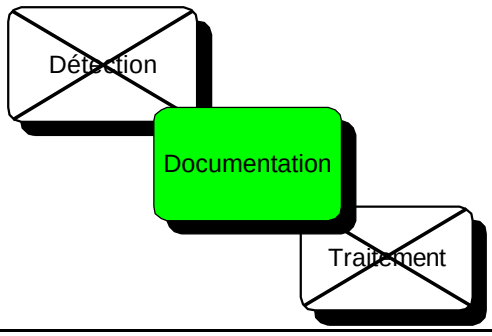
Appliqué sur les fonctions décrites ci-dessous, cela signifie que la documentation constitue le procédé central dans le processus global de contrôle-sanction. C'est dans cette étape que l'enregistrement comme élément de preuve est recueilli, transmis et archivé. Il s'agit alors de mettre en œuvre des mesures appropriées pour assurer que :

- l'enregistrement provient d'une source autorisée.
- L'intégrité de l'enregistrement est garantie.
- Les données ne peuvent pas être lues par de tiers (surtout lors du transfert).

La fonction traitement, par contre, ne présente pas de lacunes normatives, car l'utilisation d'images numériques ne demande pas des modifications spécifiques en ce qui concerne la norme en vigueur.

La situation pour la dernière fonction – la détection – est comparable à celle pour le traitement. En fin de compte, la méthode utilisée pour la détection n'a qu'une importance très réduite pour l'analyse de l'enregistrement Le déclenchement par l'image vidéo, par exemple, est une nouvelle technique de mesure, ce qui n'a en principe rien à faire avec l'image numérique comme élément de preuve. Naturellement, les outils de détection doivent répondre aux exigences requises, mais ces exigences sont indépendantes du type et de la structure de l'enregistrement, qui est le point de mire de cette étude.

→ La norme doit en première ligne couvrir le domaine de la documentation (enregistrement/transfert/archivage).




## 6.2. Adaptation aux bases juridiques existantes

### Ordonnance réglant l'admission des personnes et des véhicules à la circulation routière

Du fait que l'ordonnance dit seulement que les règles relatives aux contrôles automatiques sont données dans les instructions techniques correspondantes, il n'y aucun besoin d'adapter de cette ordonnance pour l'utilisation de l'imagerie numérique dans les contrôles automatiques de la circulation.

### Directives techniques

Les directives suivantes sont importantes quand il s'agit d'une application possible du contrôle-sanction numérique :

| **Instruction sur les dispositifs de contrôle des feux rouges** |
|---|
| **Chiffre 3.5 Contrôle de fonctionnement sur place ou lors du changement de pellicule**<br>Chaque fois que l'on change d'emplacement ou de pellicule, il y a lieu de Vérifier si le dispositif fonctionne correctement.<br>**→ En cas de l'imagerie numérique il n'y a pas de changement de la pellicule.** |
| **Chiffre 4.5**<br>Le temps enregistré sur la photo (à partir du début de la phase rouge) ne doit pas être plus court que la durée du retardement de 0,5 seconde au minimum, choisie lors du réglage.<br>**→ Dans l'imagerie numérique la possibilité technique existe de ne pas insérer directement dans l'image les données supplémentaires (comme le temps enregistré), mais de les attacher en tant que partie (non affichée) de l'enregistrement. La formulation actuelle ne considère pas cette possibilité.** |

**Tableau 8 : Modification instructions techniques surveillance feux rouges**

Les instructions techniques supposent en général l'utilisation de la technologie à film argentique – sans pour autant exclure l'application des méthodes numériques de saisie

d'images – et devraient être revues sous cet aspect. La liste donnée ci-dessus montre bien que les adaptations requises sont modestes.

**Remarque :** Cela ne vaut pas pour l'introduction de nouvelles technologies de mesure, telles que le contrôle de trajectoire. Ici il faudra compléter les instructions de manière adéquate.

→ Les adaptations requises sont relativement simples. Et cela surtout parce que les directives et instructions publiées dans ce domaine sont très fonctionnelles. En principe, il est suffisant de formuler, à l'aide d'une norme, les exigences-cadres en matière des installations de contrôle-sanction fondées sur imagerie numérique. L'essentiel y est le fait que toutes les applications imaginables (aussi en dehors de la loi sur la circulation routière) puissent baser sur cette norme.

# 7. Exigences relatives aux images et aux enregistrements

Après avoir établi les lacunes normatives dans les fonctions subordonnées (voir chapitre 6), il s'agit maintenant de déterminer les conséquences et exigences concrètes en matière de la *documentation.*

## 7.1. Exigences fonctionnelles relatives aux enregistrements

Aucun agent administratif ne se trouvant sur les lieux dans le cas des contrôles automatiques, il faut que l'enregistrement soit recevable comme élément de preuve. Ceci engendre trois exigences principales en matière des enregistrements :

**Authentication vérifiable**
L'enregistrement doit provenir d'une source autorisée (installation de contrôle), c'est-à-dire, il doit être possible de vérifier avec des moyens appropriés qui a crée l'enregistrement. Ce procédé doit permettre d'empêcher que de fausses enregistrements puissent être entrés dans le système. D'ailleurs, il est indispensable de pouvoir identifier la source des données afin d'en assurer la vérifiabilité ultérieure.

**Intégrité vérifiable**
Il doit être possible de prouver sans aucun doute possible qu'un enregistrement soit intact. Deux examens sont destinés à ce but :

- L'enregistrement, est-il intact dans son ensemble ? C'est-à-dire, est-ce que des éléments de données ont été effacés ou ajoutés depuis le recueil de l'enregistrement au dispositif de contrôle ?

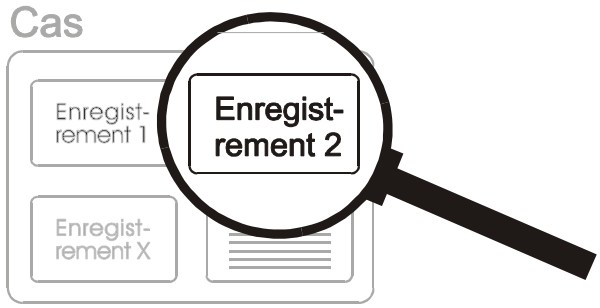



**Figure 20 : Intégrité de l'enregistrement**

- Est-ce que tous les éléments de l'enregistrement (données sur l'image, le système et le véhicule) se trouvent à leur état original, sont-ils intacts ?

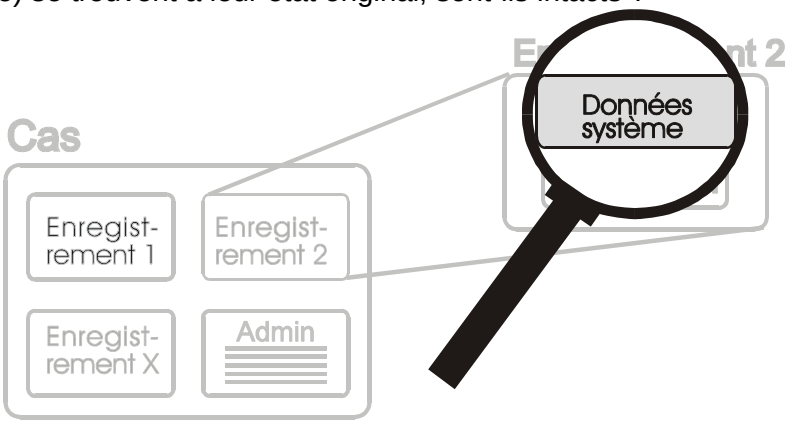



**Figure 21 : Intégrité des éléments de données**

La vérification de l'authentication et de l'intégrité des données doit impérativement être faite avant le traitement ultérieur. Si le procédé de vérification détecte une violation de l'authentication / de l'intégrité de l'image, ceci doit être marqué de forme visible sur l'image (ou les images), par exemple en y insérant un symbole approprié.

**Figure 22 : Exemple pour le marquage d'une violation de l'intégrité**

**Documentation exhaustive de l'infraction**
L'enregistrement doit décrire de façon exhaustive l'infraction constatée. L'image (numérique) y joue un rôle principal. Les exigences relatives au contenu fonctionnel de l'image varient en fonction de l'application (plaque d'immatriculation identifiable, conducteur identifiable, type de véhicule identifiable etc.).

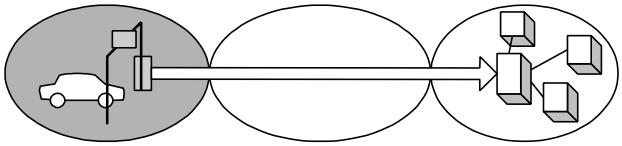
***Remarque :*** *Outre les exigences fonctionnelles en matière des enregistrements il y a aussi des exigences relatives au traitement de ces données. Une exigence particulièrement intéressante se réfère à la sécurité des données. Etant donné que les données enregistrées sont des données personnelles elles doivent être protégées à tout moment contre l'accès non autorisé par de tiers. Ceci est important surtout lors la transmission des données.*

→ L'enregistrement ne peut servir comme élément de preuve qu'à condition qu'il réponde à toutes les exigences en matière de l'authentication, de l'intégrité et de la documentation. En plus, l'aspect de la protection de la personnalité doit être pris en compte.

## 7.2. Exigences relatives à la protection de la personnalité et à la sécurité des données

Les données enregistrées sont toujours des données personnelles particulièrement précieuses, qui doivent être protégées contre tout accès non autorisé par de tiers. Cette protection doit être garantie pour l'ensemble du système, y compris tous les sous-systèmes.

### 7.2.1. Sécurité des dispositifs de contrôle en bordure de route



Le terme dispositif de contrôle en bordure de route se réfère à tous les composants sur le site de contrôle jusqu'à, et y compris l'interface au canal de transmission (caméras,

capteurs, éclairage, unité de mémoire locale etc.) Le dispositif de contrôle en bordure de route doit répondre aux exigences suivantes relatives à la protection de la personnalité :

- Protection contre les interventions non autorisées dans les composants du système.
- Sauvegarde exclusivement temporaire des données.

**Protection contre les interventions non autorisées dans les composants du système**

Tous les composants de l'installation routière doivent être protégés contre les interventions non autorisées. En pratique cela signifie qu'ils doivent être équipés d'au moins une barrière mécanique. Les interfaces aux réseaux non-protégés (voir chapitre 0) doivent en outre être protégés par des mécanismes appropriés contre les accès non autorisés au système (principe du Firewall).

Outre cette protection contre les accès non autorisés les composants doivent comporter un système permettant de surveiller les accès. Ce système doit reconnaître et enregistrer positivement tout accès au système – surtout les accès non autorisés Les mécanismes utilisés varient selon le type d'installation :

- Plombage des ouvertures des boîtiers
- Contacts aux ouvertures des boîtiers → alarme
- Détecteurs de mouvement dans les conteneurs → alarme
- Fichier compte rendu (Logfile) pour documenter les accès au système

Les fichiers compte rendu servent également à documenter les accès de maintenance et de mise à jour. La maintenance du système comprend toutes les opérations qui ne modifient pas les logiciels du système ni leurs certificats (par ex. réglage du timer). En cas d'accès pour mise à jour, par contre, les logiciels sont modifiés ce qui n'est plus compris dans le terme maintenance. Après chaque mise à jour l'installation ou plutôt les logiciels doivent être soumis à une nouvelle procédure de calibrage et vérification. Tous les accès de maintenance et de mise à jour doivent être enregistrés dans le fichier de compte rendu.

Si toutes ces exigences relatives à la protection et à la surveillance sont respectées, on peut parler d'un environnement sûr à l'intérieur d'un composant du système.

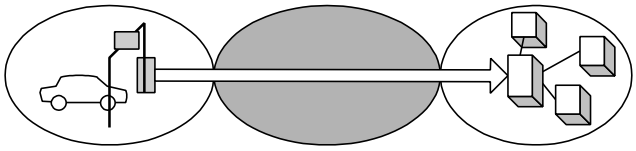
→ Il faut protéger les dispositifs de contrôle en bordure de route de manière efficace contre toute sorte d'accès non autorisé. En outre, il faut que tous les accès non autorisés soient reconnus sans faille et que la distinction par rapport aux accès autorisés soit possible de façon indubitable.

**Stockage temporaire des données**

Du fait que les possibilités pour surveiller les installations de contrôle en bordure sont limitées, il est recommandable que les enregistrements soient transférés le plus vite possible à des offices centrales et effacés à l'installation. En aucun cas, les données doivent être archivées sur le site de contrôle. Cette manière d'agir contribue à minimiser le danger que les données soient perdues au site de contrôle (par ex. en cas de défaillances du système) et que des accès / manipulations non autorisés aient lieu.

→ Il est recommandable que les données enregistrées ne restent pas plus longtemps dans la mémoire des installations de contrôle qu'absolument nécessaire.

### 7.2.2. Sécurité des données lors de leur transfert



Le terme « transfert » se réfère principalement à la communication entre le dispositif de contrôle et le système central de fond. Mais il peut également y avoir des transferts de données à l'intérieur de l'installation ou du système central de fond. La liaison entre les deux appareils routiers de contrôle dans les systèmes de contrôle de trajectoire en est un exemple.

La distinction est faite entre deux types de canaux de transmission :

- Canal protégé
- Canal non-protégé

**Canal de transmission protégé**

Un canal de transmission protégé doit être conçu de façon à empêcher de manière efficace les accès par de tiers. Il n'y a aucune importance quel support physique est choisi pour la transmission (cuivre/fibres optiques/radio). L'essentiel est que seul les personnes et offices autorisés aient accès au réseau et aux données transmises. En plus, il faut assurer que les accès sont limités à un groupe d'utilisateurs définis. Un exemple typique d'un canal de transmission protégé est le réseau à fibres optiques de la police municipale de Zurich (réseau découplé physiquement).

Lorsque de tels canaux protégés sont utilisés pour la transmission des données enregistrées, les données ne doivent plus être cryptées pour le transfert. Cela n'a cependant aucune influence sur les exigences relatives aux mécanismes mis au point pour la vérifiabilité de l'authentication et de l'intégrité.

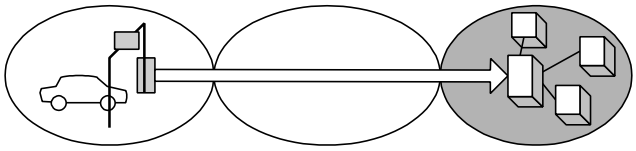
**Canal de transmission non-protégé**

Un canal de transmission non-protégé est une liaison qui n'est pas protégée par des restrictions d'accès spécifiques. Un exemple typique d'un canal de transmission non-protégé est l'Internet.

Lorsque des canaux de transmission non-protégés sont utilisés pour le transfert des données, il faut protéger les données à transmettre contre la lecture non autorisée. A cette fin, il faut crypter les données en utilisant des algorithmes de chiffrement qui, d'après l'état de la technique, sont considérés comme sûrs.

→ Il faut chiffrer toutes les données qui doivent être envoyées sur un canal de transmission non-protégé. Le chiffrement n'est cependant pas obligatoire pour les données transmises sur un canal protégé.

### 7.2.3. Sécurité au système central de fond



Le système central de fond assure l'archivage des données enregistrées et c'est ici que le traitement ultérieur et la poursuite des cas sont entrepris. Dans cet environnement aussi, il est indispensable que les données soient protégées contre les accès non autorisés. Seul les personnes autorisées doivent pouvoir accéder au système et ainsi aux données. Les

accès et les opérations principales de traitement ultérieur devraient être enregistrés de façon à permettre leur vérification à tous moments.

→ Il faut empêcher de manière efficace tout accès non autorisé aux données stockées dans le système central de fond.

## 7.3. Exigences relatives à l'intégrité et l'authenticité

Pour pouvoir utiliser un enregistrement comme élément de preuve, on doit pouvoir prouver que les composants individuels appartiennent réellement à l'enregistrement. Par exemple: il doit être sûr que les valeurs mesurées se réfèrent vraiment au véhicule représenté sur l'image. En outre, il faut mettre en œuvre des mesures garantissant que les données ne seront pas modifiées ou échangées de manière inaperçue.

Jusqu'à maintenant, on a répondu à ces exigences (pour les contrôles-sanction vidéo) en incrustant les données requises directement dans l'image avant de l'enregistrer. Cette méthode est aussi applicable pour les images numériques, mais elle n'est plus obligatoire.

→ L'enregistrement doit être pourvu d'une signature électronique pour que son intégrité puisse être vérifiée. Selon l'architecture du système, il peut éventuellement être nécessaire/raisonnable de signer séparément certaines parties de l'enregistrement.

En plus, tous les éléments doivent porter des estampilles, pour pouvoir vérifier si les éléments ont été assemblés de façon correcte avant leur signature.

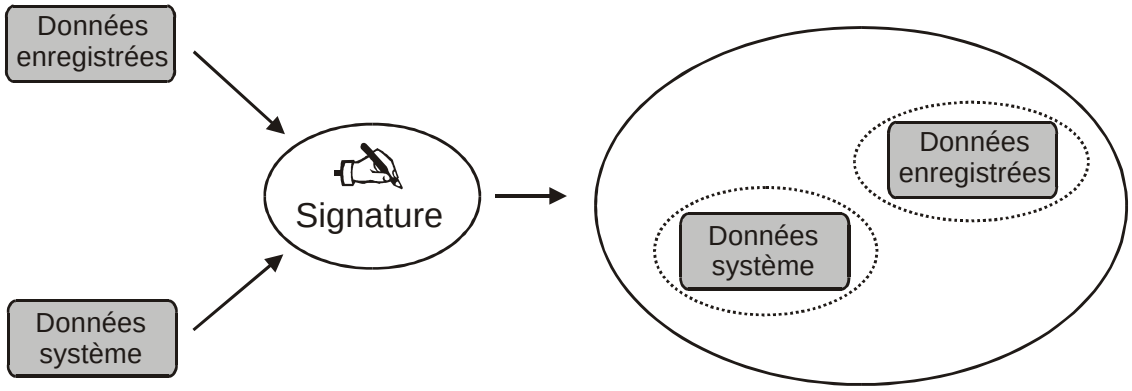



**Figure 23 : Signature de l'enregistrement**

En règle générale, les données enregistrées, qui contiennent les données-images, représentent la partie majeure de l'encombrement total de l'enregistrement, d'où il peut être raisonnable, dans certains cas, de créer un enregistrement additionnel sans l'image. L'enregistrement contient alors seulement la référence au fichier de l'image qui peut être chargé, si besoin en est. Dans ce cas, il faut assurer que l'image ne peut être échangée ultérieurement, c'est-à-dire après l'établissement de l'enregistrement.

A cette fin, le nom du fichier doit être compris dans la signature. On signe donc d'abord l'image, le nom du fichier compris, avant de signer les données système, les données de contrôle et la signature de l'image.

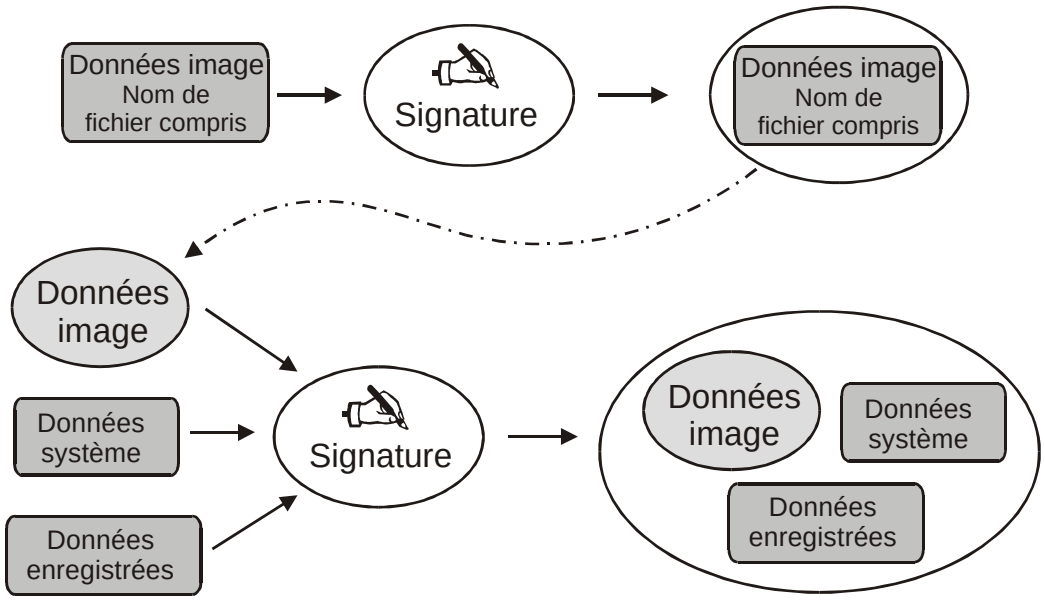



**Figure 24 : Enregistrement signé avec fichier d'image séparé**

Cette méthode permet de sauvegarder et de gérer les données de l'image séparément sans mettre en danger l'intégrité de l'enregistrement. Ce principe ne fonctionne naturellement pas seulement avec les données de l'image mais peut être utilisé, par exemple, aussi pour les données système.

**Remarque :** Même segmenté de la façon, l'enregistrement consiste toujours en données système et données enregistrées

## 7.4. Exigences en matière du traitement ultérieur

Au cours de leur exploitation les données de l'image sont soumises, le cas échéant, à certains traitements ultérieurs. Du fait que chaque traitement de l'image constitue une violation de la signature et donc de l'intégrité/l'authenticité, il est absolument exclu que des manipulations soient faites à enregistrement original. Cette séquence doit absolument être conservée dans son état original parce que seulement ainsi il est possible de prouver à tout instant qu'il s'agit d'un enregistrement « vrai « .

| → L'enregistrement original comme élément de preuve ne doit en aucun cas être modifié avant sa mise en mémoire. |
|---|

## 7.5. Exigences relatives à la sauvegarde et à la gestion

Les enregistrements de contrôle-sanction se créent souvent à l'aide de procédures et algorithmes propriétaires, ce qui résulte naturellement en une certaine dépendance des outils de gestion et de stockage. De toute façon, il faut que les points suivants soient garantis pour la période entière de stockage des données :

- Les données doivent être accessibles à tout moment. Les données doivent pouvoir être présentées sous forme appropriée et rappelées si besoin en est.
- Il faut pouvoir prouver à tout moment l'authenticité et l'intégralité des données. La gestion des clés de décryptage doit être assurée pour la période requise.
- Le traitement ultérieur de l'image doit être possible à tout moment (exigence relative à l'exploitation).

## 7.6. Exigences en matière de la qualité de l'image

La définition fonctionnelle des exigences relatives à la qualité de l'image comme élément de preuve est la suivante : L'image doit fournir une documentation indiscutable de l'infraction. Dans la plupart des cas cela veut dire que la plaque d'immatriculation et le conducteur doivent pouvoir être identifiés de manière indubitable. Cette condition donne lieu à certaines exigences relatives au nombre de pixels et à des restrictions concernant le degré de compression des données.

**Nombre de pixels**

montre comment l a lisibilité de la plaque d'immatriculation diminue dans la même mesure que baisse le nombre de pixels. A partir de 4 pixels sur l'épaisseur d'un chiffre, au plus tard, une identification sûre de la plaque d'immatriculation ne peut plus être garantie dans tous les cas. Il est pourtant difficile de formuler une limite précise relative au nombre de pixels requis, 6 pixels par épaisseur de chiffre devant être considéré comme la limite minimale absolue.


~20 pixels / épaisseur d'un chiffre


~10 pixels / épaisseur d'un chiffre


~8 pixels / épaisseur d'un chiffre


~6 pixels / épaisseur d'un chiffre


~5 pixels / épaisseur d'un chiffre


~4 pixels / épaisseur d'un chiffre

**Figure 25 : Exemples pour différentes résolutions**

La limitation s'avère encore un peu plus difficile lors qu'il s'agit de la représentation des conducteurs, car le nombre de pixels requis y est variable. L'identification précise d'un conducteur est plus ou moins difficile selon la nature et les caractéristiques du conducteur. D'où il n'est pas possible de déterminer de façon incontestable un nombre de pixels requis. Au fond, on peut constater que la résolution requise pour permettre une identification exacte d'un conducteur n'est pas supérieure à celle nécessitée de toute façon pour l'identification exacte de la plaque d'immatriculation.

***Remarque :*** *Evidemment le nombre de pixels n'est pas le seul paramètre ayant une influence sur la qualité de l'image. Le nombre de niveaux de gris également y joue un rôle, sans pour autant constituer le facteur restrictif pour les produits disponibles sur le marché.*

→ Sans connaître la syntaxe, il doit être possible d'identifier sans aucun doute les signes représentés.

**Degré de compression**

Comme chapitre 0 le décrit déjà, la compression des images peut entraîner des falsifications du contenu. Pour les méthodes de compression travaillant sans pertes d'informations il n'y aucune restriction. Pour les méthodes de compression avec pertes d'informations il y a cependant certaines restrictions relatives au degré de compression.

Les falsifications résultant d'une compression (avec perte d'informations) se divisent en trois catégories :

a) Falsifications conduisant seulement à une réduction de la qualité mais sans influence sur le contenu fonctionnel de l'image.

b) Falsifications détruisant le contenu fonctionnel de l'image → par exemple, la plaque d'immatriculation ne peut plus être identifiée de façon sure suite aux pertes d'informations au cours de la compression.

c) Falsifications modifiant le contenu fonctionnel de l'image → par exemple, un chiffre dans la plaque d'immatriculation change sa valeur suite à la compression. Le terme „contenu fonctionnel de l'image" désigne par exemple la plaque d'immatriculation représentée sur l'image. Tant que la plaque d'immatriculation reste identifiable de façon incontestable, le contenu fonctionnel est resté intact.

Alors que les falsifications de la catégorie a) ne constituent pas de problème majeur pour le *contrôle-sanction numérique*, les modifications des catégories b) et c) sont inacceptables. Les falsifications de la catégorie c) sont particulièrement problématiques car elles peuvent entraîner, le cas échéant, une poursuite pénale de personnes innocentes, alors que dans le cas b), dans le pire des cas, le contrevenant échappe à la poursuite.

De façon analogue à la question sur la résolution requise, il n'est pas possible non plus de déterminer une valeur précise pour le degré de compression admissible. Ce qui est dû, entre autres, au fait que différents algorithmes de compression sont utilisés.

→ Pour les méthodes de compression sans pertes il n'y a aucune restriction relative au degré de compression. Pour les méthodes de compression avec perte d'informations, par contre, il faut assurer que la compression ni détruit ni modifie le contenu fonctionnel des images . Ce dernier doit être considéré avec priorité.

**Exemple:** L'exemple suivant montre comment l'image est modifiée en fonction du degré croissant de compression. On reconnaît que c'est seulement à partir d'un certain niveau de compression (~80% dans ce cas) que la représentation de la plaque d'immatriculation détériore. Avant ce seuil, c'est bien la qualité de l'image qui diminue mais ne pas le contenu fonctionnel de l'image. La limite peut cependant varier selon la méthode de compression

utilisée. Dans ce cas, une image de 1024x768 pixels a été comprimée avec la méthode JPEG. Le nombre de pixels est resté constant :


**Figure 26 : Exemple pour l'effet de la compression sous JPEG**

# 8. Glossaire

| Terme | Définition |
|---|---|
| Enregistrement | Dans ce rapport, ensemble de données qui décrivent uniquement **un** événement. |
| DSRC | **D**edicated **S**hort **R**ange **C**ommunication. Interface radio sur une fréquence 5.8GHz, pour les applications dans le domaine du péage électronique. |
| Intensité de la couleur | L'intensité de la couleur indique combien de niveaux de couleur et/ou de gris sont représentés. L'intensité de la couleur est mesuré en nombre de bits qui décrivent la couleur.<br>• 1 bit = 2 couleurs (noir/blanc)<br>• 4 bits = 16 couleurs/degrés de gris<br>• 8 bits = 256 couleurs/degrés de gris<br>• 16 bits = 32'767 ou 65'535 couleurs<br>• 24 bits = 16,7 millions de couleurs |
| Scanner laser | Dispositif pour déterminer les dimensions (hauteur, largeur, longueur) d'un véhicule de passage à l'aide de la technologie laser. Avec des logiciels d'exploitation enchaînés, les véhicules de passage peuvent être classifié par catégorie (VP, PL, bus etc.) |
| LPR | **L**icence **P**late **R**eading |
| OBU | **O**n **B**oard **U**nit – Unité embarquée |
| OCR | **O**ptical **C**haracter **R**ecognition – reconnaissance des chiffres et caractères |
| TRIPON | Appareil de saisie pour la redevance des poids lourds liée aux prestations (RPLP) en Suisse. |
| VES | **V**ideo **E**nforcement **S**ystem – Système vidéo de contrôle-sanction |
| Hash | Une fonction hash est un procédé pour la compression des données à l'aide d'une fonction à sens unique, c.-à-d. les données originales ne peuvent pas être récupérées par calcul en sens inverse. La fonction hash fournit pour chaque valeur en entrée d'une longueur quelconque une valeur de sortie à longueur fixe, et elle est structurée de façon que chaque modification des données en entrée entraîne très vraisemblablement une modification de la valeur hash calculée (c.-à-d. la valeur en sortie). Un algorithme de hachage typique est l'algorithme SHA-1. Le résultat d'une fonction hash est la valeur hash, souvent désignée comme l'empreinte numérique. |
| Framegrabber | Un « Framegrabber » est une unité électronique utilisée pour tirer des photos d'un signal vidéo analogique et dynamique. |
| DETEC | Département fédéral de l'environnement, des transports, de l'énergie et de la communication |
| metas | Office fédérale de métrologie et d'accréditation |
| VERA | Video Enforcement for Road Authorities; Système video de cotnrôle-sanction destine aux autorités routières – projet de recherche de l'UE |
| ADVICE | Advanced Vehicle Classification and Enforcement; projet de recherche de l'UE |
| C.A.S.E. | Contrôle de trajectoire (Continuous Applied Speed Enforcement C.A.S.E.) |
| DES | Standard de cryptage de données d'après ANSI X3.92. Le système de chiffrement le plus répandu. |
| UNI | Ente Nationale Italiano di Unificazione, autorité italienne de normalisation |

# Annexe A: Projet de norme

(voir pages suivantes)

Vereinigung Schweizerischer Strassenfachleute
Union des professionnels suisses de la route
Unione dei professionisti svizzeri della strada

Schweizer Norm
Norme Suisse
Norma Svizzera

XXX XXX

EINGETRAGENE NORM DER SCHWEIZERISCHEN NORMEN-VEREINIGUNG SNV NORME ENREGISTREE DE L'ASSOCIATION SUISSE DE NORMALISATION

# Automatische Kontrollanlagen mit digitaler Bildtechnik

# Norm (Entwurf)

## Inhalt



# Systèmes pour la surveillance automatique fondé sur imagerie numérique

# Projet de norme

## Table des matières



## A. Allgemeines

### *1. Geltungsbereich*

Die Norm gilt für Kontrollanlagen für den Strassenverkehr, die automatisch Widerhandlungen gegen rechtliche Vorschriften feststellen und protokollieren.

### *2. Gegenstand*

Gegenstand sind Systemausführungen von automatischen Kontrollanlagen, wo digitale Bilder mit zugehörigen Beweisdaten erfasst, übertragen und gespeichert werden.

## A. Généralités

### *1. Domaine d'application*

La norme se réfère aux systèmes de contrôle de la circulation routière qui détectent et enregistrent de façon automatique les infractions au règlement.

### *2. Objet*

L'objet sont les types de système de contrôle automatique qui enregistrent, transfèrent et sauvegardent des images numériques et les données liées.

Herausgeber:

Editeur:

Entwurf: RAPP AG, Basel

***3. Zweck der Norm***

Die Norm definiert zu Referenzzwecken eine allgemeingültige Systemarchitektur für automatische Kontrollanlagen mit den wesentlichen Teilfunktionen der Kontrollabläufe.

Für die gemäss dieser Architektur zentrale Teilfunktion der Kontrollabläufe, nämlich die Dokumentation des vermuteten Verstosses, werden funktionale Anforderungen an die Abläufe, an die Beweisdatensätze sowie an Anlagekomponenten gestellt.

***4. Begriffe***

Im Rahmen dieser Norm gelten folgende Bedeutungen:

Automatische Kontrollanlage
Einrichtung, die ohne menschliches Zutun Vorgänge erkennt und dokumentiert, bei denen Verkehrsteilnehmer gegen rechtliche Vorschriften verstossen haben.

Beweisdatensatz
Ein Beweisdatensatz umfasst alle Daten, welche eine Widerhandlung dokumentieren.

Signatur
Eine Signatur wird aus einem Datensatz durch Anwendung von kryptographischen Algorithmen nach Stand der Technik mit einem anerkannten Verfahren gebildet. Anhand der Signatur kann nachgewiesen werden, ob die Signatur eindeutig von einer bestimmten Entität (Person, Anlage) erzeugt und der zugehörige Datensatz seit der Erzeugung der Signatur verändert wurde.

## B. Architektur von automatischen Kontrollanlagen

***5. Aufbau***

Bei einer automatischen Kontrollanlage werden drei Anlagenteile unterschieden:

Strassenseitige Kontrolleinrichtung: Die strassenseitige Kontrolleinrichtung dient der Erfassung von Beweisdatensätzen. Dieser Anlagenteil beinhaltet sämtliche Kontrolleinrichtungen vor Ort. Dazu gehören insbesondere die Bilderfassungsanlage, die Messeinrichtung(en), sowie allenfalls vorhandene Auswertungselektronik.

Übertragungskanal: Der Übertragungskanal

***3. But***

La norme définit, aux fins de référence, une architecture généralement valable pour les systèmes de contrôle automatique et les fonctions principales des cycles de contrôle.

Les exigences fonctionnelles relatives aux procédés, aux enregistrements comme éléments de preuve et aux composants du système sont formulées pour la fonction centrale de cette architecture, la documentation des cycles de contrôle.

***4. Définitions***

Dans le cadre de la norme sont valables les suivantes définitions :

Dispositif de contrôle automatique
Installation qui, sans intervention humaine, reconnaît et enregistre des évènements où le conducteur d'un véhicule a commis une infraction à la réglementation.

Enregistrement (comme élément de preuve)
L'enregistrement comprend l'ensemble de données servant à décrire une infraction.

Signature
La signature est crée à l'aide d'un procédé reconnu à partir d'un enregistrement par application d'algorithmes cryptographiques selon l'état de la technique. La signature permet de prouver si la signature a réellement été crée d'une entité (personne, dispositif) et si l'enregistrment a été modifé depuis sa création.

## B. Architecture des systèmes pour la surveillance automatique

***5. Structure***

Un dispositif de contrôle automatique peut être divisé en trois parties :

Installations de contrôle en bordure de route : Les installations de contrôle en bordure de route servent à l'enregistrement des données utilisées comme élément de preuve. Cette partie de l'installation comprend l'ensemble des dispositifs de contrôle sur site, qui sont, principalement, le système de saisie d'image, l(es) appareil(s) de mesurage et les logiciels d'exploitation

umfasst zumindest die Datenübertragungseinrichtung zwischen der strassenseitigen Kontrolleinrichtung und dem Hintergrundsystem. Weitere Übertragungsstrecken können hinzukommen. Zum Übertragungskanal zählen jedenfalls alle Datenverbindungen, die durch die äusseren Gehäuse von Anlagekomponenten treten.

Hintergrundsystem: Das Hintergrundsystem dient der Verarbeitung der Beweisdatensätze. Vorgänge im Hintergrundsystem umfassen beispielsweise die Bestätigung der Widerhandlung, die Identifikation des Fahrzeugs, die Archivierung und Verwaltung der Beweisdatensätze und die Einleitung der Strafverfolgung.

### *6. Teilfunktionen*

Der Kontrollablauf wird in die folgenden drei Teilfunktionen aufgeteilt:

Ereignis-Detektion: Vorgang bei welchem festgestellt wird, ob und in welchem Masse sich ein Verkehrsteilnehmer gegen bestehende Regeln und Gesetze verhält.

Dokumentation: Umfasst die Aufzeichnung einer Widerhandlung. Die Teilfunktion Dokumentation kann wiederum unterteilt werden in:

- Erstellung: Zusammenstellen der relevanten Daten zu einem Beweisdatensatz.
- Übertragung: Übertragung des Beweisdatensatzes von der strassenseitigen Kontrolleinrichtung zum Hintergrundsystem.
- Aufbewahrung: Speicherung und Indizierung des Beweisdatensatzes, so dass der Zugriff auf die Originaldaten im rechtlich relevanten Zeitraum möglich ist.

Verarbeitung: Beinhaltet sämtliche Verarbeitungsschritte nach der Übertragung des Beweisdatensatzes an das Hintergrundsystem.

éventuellement disponibles.

Canal de transmission : Le canal de transmission comprend au moins les installations pour le transfert de données entre le dispositif de contrôle en bordure de route et le système central de fond. D'autres voies de transmission peuvent s'y ajouter. De toute façon, le canal de transmission comprend toutes les lignes de transmissions sortant des boitiers extérieurs des composants du système.

Système central de fond : Le système central de fond assure l'exploitation des enregistrements. Les procédés exécutés par le système central de fond sont, par exemple, la confirmation de l'infraction, l'identification du véhicule, l'archivage et la gestion des enregistrements ainsi que le déclenchement de la poursuite pénale.

### *6. Sous-fonctions*

Le cycle de contrôle est divisé en trois fonctions subordonnées, comme suit :

Détection : Procédure au cours de laquelle est établi si, et dans quelle mesure, un conducteur a commis une infraction aux lois et réglements en vigueur.

Documentation : Le process de l'enregistrement d'une infraction. La fonction documentation peut être subdivisé en les fonctions :

- Recueillir: Rassembler les données pertinentes pour en créer un enregistrement
- Transférer: Transfert de l'enregistrement du dispositif en bordure de route dans le système central de fond
- Archiver: Stockage et marquage de l'enregistrement de sorte que l'accès aux données originales reste possible durant toute la période juridiquement significative.

Traitement : L'ensemble des opérations de traitement après le transfert de l'enregistrement dans le système central de fond.

***7. Beweisdatensatz***

Ein Beweisdatensatz kann folgende Gruppen von Daten beinhalten:

**Anlagedaten**

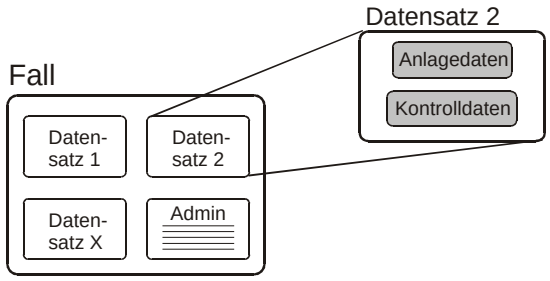
Angaben zur Kontrolleinrichtung wie Anlagetyp, Version, Gerätenummer, Einstellungen, Status, usw.. Diese Angaben sind unabhängig vom kontrollierten Fahrzeug.

**Kontrolldaten**

Diese Daten sind für jeden Kontrollfall verschieden. Die Datengruppe kann weiter unterteilt werden in:

- Kenndaten (Z.B. Datum / Uhrzeit, laufende Nummer)
- Bilddaten: Digitales Bildmaterial (Einzelbild oder Videosequenzen)
- Messdaten: z.B. Geschwindigkeit oder Fahrzeugkategorie
- Fahrzeugdaten: z.B. Kontrollschild, vom Fahrzeug übermittelte Daten.

Bei der Verarbeitung können bei Bedarf mehrere Beweisdatensätze zu einem Fall zusammengefasst werden.




## C. Anforderungen an automatische Kontrollanlagen

***8. Abgrenzung***

Die Norm für Anlagen mit digitaler Bildtechnik beschreibt ausschliesslich Anforderungen an die Teilfunktion Dokumentation.

***7. Enregistrement (comme élément de preuve)***

L'enregistrement peut contenir les groupes de données suivants :

**Données système**

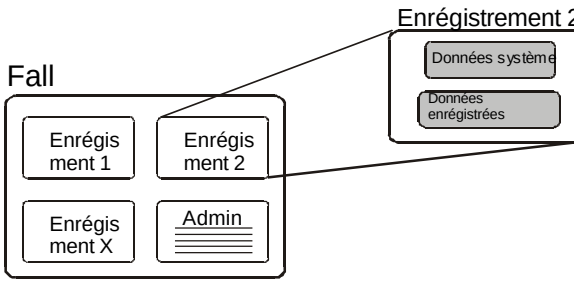
Informations sur le dispositif de contrôle comme type de l'installation, version, n° de l'appareil, réglage, statut etc. Ces données sont indépendantes du véhicule contrôlé

**Données enrégistrées**

Les données enrégistrées varient selon le cas. Ce groupe de données se divise en :

- Données système (par ex. date/heure, n° de série)
- Données image : Images numériques (photo ou séquences vidéo)
- Données mesurées : par ex. vitesse ou type de véhicule
- Données véhicules : par ex. plaque d'immatriculation, données transmises par le véhicule.

Il est possible de regrouper plusieurs enregistrements en un seul cas aux fins de l'exploitation.




## C. Exigences relatives aux systèmes de contrôle automatique

***8. Délimitation***

La norme pour les installations fondées sur l'imagerie numérique décrit exclusivement les exigences en matière de la fonction principale documentation.

### *9. Funktionale Anforderungen an Beweisdatensätze*

Vollständigkeit und Eindeutigkeit

Ein Beweisdatensatz enthält alle zum Nachweis einer Widerhandlung benötigten Informationen. Ein Beweisdatensatz umfasst zumindest eine eindeutige Aufzeichnung des Vorgangs, der die Widerhandlung darstellt, eine Identifikation der Kontrollanlage und relevanter Einstellungen sowie Datum und Uhrzeit.

Die Zusammengehörigkeit der Daten – z.B. Bild und Messwerte – ist nachweisbar.

Prüfbare Authentizität

Der Beweisdatensatz muss überprüfbar von einer autorisierten Kontrollanlage stammen. Die Kontrollanlage muss eindeutig identifiziert werden können.

Prüfbare Integrität

Die Integrität des Beweisdatensatzes muss jederzeit nachweisbar sein. Sie ist nachgewiesen, wenn

- alle Datenelemente des Beweisdatensatzes in unversehrtem d.h. unverändertem Zustand sind, und
- der Beweisdatensatz als Ganzes in unversehrtem Zustand ist, d.h. es wurden keine Datenelemente zugefügt oder entfernt.

### *10. Anforderungen an Nachweise für Authentizität und Integrität*

Der Beweisdatensatz muss mit einer Signatur versehen werden. Die Signatur muss für folgende Nachweise tauglich sein:

- Die Zusammengehörigkeit der Daten – z.B. Bild und Messwerte – ist nachweisbar gegeben.
- Im Datensatz wurden weder Datenelemente verändert, noch hinzugefügt oder entfernt.
- Der Datensatz stammt nachweislich von einer authorisierten Kontrollanlage.

*Anmerkung:*

Je nach Architektur der Anlage müssen zur Erfüllung dieser Anforderung nicht nur der Datensatz als Ganzes,

### *9. Exigences fonctionnelles relatives aux enregistrements (comme éléments de preuve)*

Intégralité et clarté

L'enrégistrement contient l'ensemble des informations nécessaires pour prouver une infraction. L'enrégistrement comprend au moins un enrégistrement indiscutable de l'événement montrant l'infraction, l'identification du dispositif de contrôle et les paramètres pertinents ainsi que la date et l'heure.

La corrélation entre les données – par ex. entre l'image et les valeurs mesurées – doit pouvoir être vérifiable.

Authenticité vérifiable

Il doit être vérifiable que l'enrégistrement provient d'une installation de contrôle autorisée. Le dispositif de contrôle doit pouvoir être identifié sans aucun doute possible.

Intégrité vérifiable

L'intégrité de l'enrégistrement doit être vérifiable à tout moment. L'intégrité est prouvée, quand

- tous les éléments constituant l'enregistrement sont dans un état intact, c.-à-d. non modifés, et
- l'enregistrement dans son ensemble est dans un état intact, c.-à-d. aucun élément de données a été modifié ou effacé.

### *10. Exigences en matière des preuves de l'authenticité et de l'intégrité*

L'enrégistrement doit être pourvu d'une signature. La signature doit permettre de vérifier comme suit:

- La corrélation entre les données – par ex. l'image et les valeurs mesurées – est prouvée sans aucun doute possible.
- Dans l'enrégistrement aucun élément de données n'a été modifié, ni ajouté ni effacé.
- Il est prouvé que l'enrégistrement a été crée par un dispositif de contrôle autorisé.

*Remarque :*

Pour répondre aux exigences présentées, et en

sondern zusätzlich auch einzelne Datenelemente (z.B. die Bilddaten) mit einer separaten Signatur versehen werden.

### *11. Anforderungen an denZugriffsschutz*

Aus Gründen des Datenschutzes und der Anlagensicherheit müssen Anlagenteile und Daten wie folgt geschützt werden.

Zugriffsschutz an der Kontrollanlage

Komponenten der Kontrollanlage müssen vor dem physischen und elektronischen Zugriff durch nicht berechtigte Personen geschützt werden. Anlagenteile der strassenseitigen Kontrolleinrichtung sind so zu schützen, dass eine Veränderung von funktionalen Komponenten erkannt werden kann.

Beweisdatensätze oder Elemente von Beweis-datensätzen sollen möglichst kurz an der strassenseitigen Kontrolleinrichtung gespeichert werden. Die Aufbewahrung erfolgt in einer dafür geeigneten zugriffssicheren Umgebung.

Zugriffsschutz bei der Datenübertragung

Es wird unterschieden zwischen geschützten und unge-schützten Übertragungskanälen:

- Geschützter Übertragungskanal: Ein geschützter Über-tragungskanal muss so gestaltet sein, dass ein Zugriff durch Dritte wirkungsvoll verhindert wird. Nur authorisierten Stellen oder Personen ist der Zugriff auf den Übertragungsweg und die darauf übertragenen Daten möglich. Das eingesetzte physikalische Medium (Diskette, Kupferleitung, Glasfaser, Richtfunk) ist dabei nicht von Bedeutung. Auf solchen Übertragungs-kanälen ist eine Verschlüsselung bei der Übertragung nicht zwingend notwendig.
- Ungeschützter Übertragungskanal: Darunter werden Übertragungswege verstanden, welche über keine besonderen Zugriffsschutz-Mechanismen bzw. Restriktionen verfügen (z.B. Betriebsfunk, Internet). Auf ungeschützten Netzen müssen die Daten bei der Übertragung zwingend nach Stand der Technik verschlüsselt und so gegen Einsicht geschützt werden.

dépendance de l'architecture du système il ne faut non seulement que l'enregistrement soit signé dans son ensemble, mais, en plus, que des éléments particuliers (par ex. l'image) soient pourvus d'une signature séparée.

### *11. Exigences relatives à la sécurité des fichiers*

Pour garantir la protection de la personnalité et la sécurité des systèms de contrôle il faut mettre en œuvre les suivants mesures de protection.

Sécurité des fichiers au dispositif de contrôle

Il faut protégér les composants des dispositifs de contrôle contre tout accès physique ou élèctronique par des personnes non autorisées. La protection des composants des dispositfs de contrôle en bordure de route doit être de sorte à garantir que chaque modification entreprise aux composants fonctionnels peut être détéctée.

Le temps de sauvegarde des enregistrements ou éléments d'enregistrements dans les dispositifs de contrôle en bordure de route doit être aussi court que possible. Les données sont stockées dans un environnement sûre, approprié à cette fin.

Sécurité des fichiers lors du transfert

La distinction est faite entre canaux de transmission protégés et non-protégés.

- Canaux protégés : Un canal de transmission protégé doit être conçu de façon à empêcher de manière efficace les accès par de tiers. Seul les personnes et offices autorisés doivent avoir accès à la voie de transmission et aux données transmises. Il n'y a aucune importance quel support physique est choisi pour la transmission (cuivre/fibres optiques/radio). Lorsque de tels canaux protégés sont utilisés pour la transmission des données enregistrées, les données ne doivent pas forcément être cryptées pour le transfert.
- Canaux non-protégés :Un canal de transmission non-protégé est une liaison qui n'est pas protégée par des mécanismes ou restrictions d'accès spécifiques (par ex. Internet, radio d'entreprise). Lorsque des canaux de transmission non-protégés sont

***12. Anforderungen an die Nachbearbeitung***

Bei der Nachbearbeitung muss der originale Beweisdatensatz in jedem Fall unverändert erhalten bleiben, d.h. die Nachbearbeitung erfolgt immer an einer Kopie des Originaldatensatzes. Nachbearbeitete Beweisdatensätze sind zu kennzeichnen.

***13. Anforderungen an die Aufbewahrung***

Folgende Punkte müssen für die Dauer der Aufbewahrung gewährleistet werden können:

- Der Zugriff auf Kontrolldaten muss möglich sein. Die Daten müssen in geeigneter Form dargestellt und bei Bedarf ausgegeben werden können.
- Die Integrität und Authentizität der Daten muss jederzeit nachgewiesen werden können. Die benötigten kryptographischen Schlüssel müssen über den geforderten Zeitraum sicher verwahrt werden.

***14. Anforderungen an die Bildqualität***

Die Bildqualität muss hinreichend sein, dass der funktionale Bildinhalt zweifelsfrei erkennbar ist. Der funktionale Bildinhalt ist eine eindeutige und vollständige Dokumentation des Vorgangs, der dem Enforcementfall zugrunde liegt. (In den meisten Fällen beinhaltet dies, dass der Lenker sowie das Kontrollschild zweifelsfrei identifiziert werden können müssen.)

Konkret bedeutet diese funktionale Anforderung an die Bildqualität, insbesondere folgende detaillierte Anforderungen an die Anzahl der Bildpunkte sowie Restriktionen hinsichtlich Datenkompressionsgrad.

- Anzahl der Bildpunkte (Pixel): Mit abnehmender Anzahl der Pixel sinkt auch die Lesbarkeit des Kontrollschildes bzw. die Erkennbarkeit des Lenkers. Um Fehler bei der Kontrollschilderkennung ausschliessen zu können, soll das Kontrollschild mit einer Mindestanzahl von 6 Pixel pro Ziffernbreite aufgenommen und dargestellt werden.

Kompressionsgrad: Für verlustfreie, reversible

utilisés pour le transfert des données, il faut impérativement chiffrer les données à l'aide d'un procédé de pointe pour les protéger contre toute lecture non autorisée.

***12. Exigences en matière du traitement ultérieur***

Il faut assurer que l'enregistrement original demeure tout à fait intact, c.-à-d., le traitement ultérieur est toujours fait sur une copie de l'enregistrement original. Il faut marquer les enregistrements traités.

***13. Exigences en matière de l'archivage***

Les points suivants doivent être garantis durant le temps de stockage des données :

- Il faut pouvoir accéder aux données enrégistrées. Les données doivent pouvoir être présentées sous forme appropriée et rappelées si besoin en est.
- Il faut pouvoir prouver à tout moment l'authenticité et l'intégralité des données. La gestion des clés de décryptage doit être assurée pour la periode requise.

***14. Exigences en matière de la qualité de l'image***

La qualité de l'image doit être suffisante pour permettre une reconnaissance incontestable du contenu fonctionnel de l'image. Le contenu fonctionnel de l'image est la documentation complète et incontestable de l'événement déclencheur du processus contrôle-sanction. (Dans la plupart des cas, cela implique une identification incontestable du conducteur et de la plaque d'immatriculation.)

En termes concrets, cette exigence fonctionnelle relative à la qualité de l'image donne lieu surtout aux exigences détaillées relatives au nombre de pixels et aux restrictions relatives au dégré de compression de données.

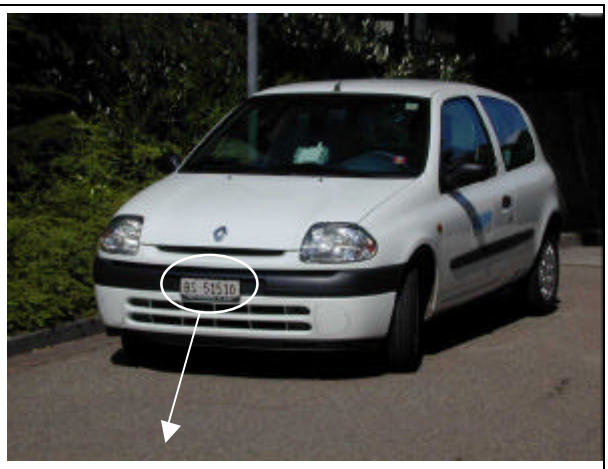
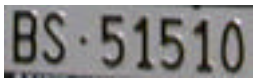
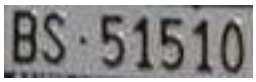
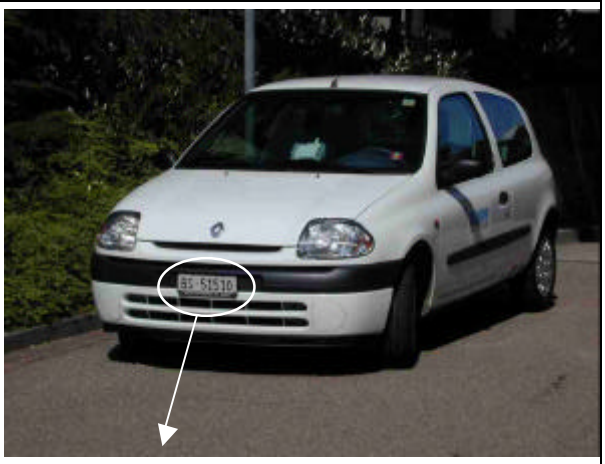
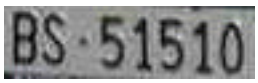
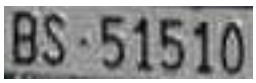
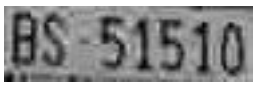
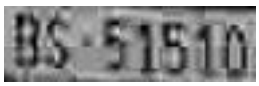
- Nombre de pixels : La lisibilité de la plaque d'immatriculation et/ou la possibilité de reconnaître le conducteur diminuent dans la mesure que baisse le nombre de pixels. Pour exclure toute reconnaissance fautive de la plaque d'immatriculation, le nombre de 6 pixels par épaisseur d'un chiffre doit constituer la

Kompressionsverfahren bestehen keine Beschränkungen hinsichtlich Kompressionsgrad. Für verlustbehaftete Kompressionsverfahren darf durch die Kompression der funktionale Bildinhalt nicht verändert werden. Da verschiedene Algorithmen eingesetzt werden, kann kein fester Wert für den maximal zulässigen Kompressionsgrad angegeben werden. Das Beispiel im Anhang soll jedoch einen Anhaltspunkt geben.

limite minimum pour l'enregistrement et la représentation de la plaque d'immatriculation.

Dégré de compression : Il n'y aucune restriction relative au dégré de compression pour les méthodes de compression reversibles, sans pertes d'informations. Cependant, pour les procédures de compression avec pertes d'informations, il faut assurer que le contenu fonctionnel de l'image ne subisse pas de modification due à la compression. Du fait que différents algorithmes sont utilisés pour la compression des données, il n'est pas possible de définir une valeur fixe pour la limite maximale du dégré de compression. Toutefois, l'exemple donné en annexe devrait servir comme point de repère.

| | |
|---|---|
| ***Anhang A***<br>**Beispiel:** Das folgende Beispiel zeigt, wie sich ein Bild mit zunehmendem Komprimierungsgrad verändert. Im vorliegenden Fall wurde ein Bild mit 1024x768 Pixel mit dem Verfahren JPEG komprimiert. Ab einem gewissen Komprimierungsgrad wird die Darstellung des Kontrollschilds merklich verschlechtert. Bei einem Komprimierungsgrad über 80% erscheint bei diesem Verfahren Gefahr zu bestehen, dass der funktionale Bildinhalt verfälscht wird (d.h. Zeichen des Kontrollschilds verändert werden). Bei weniger als 80% Komprimierungsgrad verschlechtert sich wohl die Bildqualität, nicht aber der funktionale Inhalt des Bildes. | ***Annexe A***<br>**Exemple:** L'exemple suivant montre comment une image est modifiée en fonction du dégré de compression des données. Dans le cas présent, une image de 1024x768 pixels a été comprimée à l'aide du procédé JPEG. A partir d'un certain dégré de compression la qualité de représentation de la plaque d'immatriculation commence à déteriorer sensiblement. Il paraît qu'à partir d'un dégré de compression plus élevé à 80% le danger existe que le contenu fonctionnel de l'image soit falsifié (c'est-à-dire les chiffres de la plaque d'immatriculation sont modifiés). Pour les dégrés de compression inférieurs à 80% la qualité de l'image déteriore mais pas le contenu fonctionnel de l'image. |

| | |
|---|---|
|  |  |
|  Compression: 0%<br>Taille: 163Ko |  Compression: 50%<br>Taille: 71Ko |
|  |  |
|  Compression: 75%<br>Taille: 44Ko |  Compression: 80%<br>Taille: 38Ko |
|  |  |
|  Compression: 90%<br>Taille: 25Ko |  Compression: 95%<br>Taille: 18Ko |