



REALISIERUNG EINES VIDEOÜBERWACHUNGS-  
UND NUMMERNSCHILDERKENNUNGSSYSTEMS  
IN DEN MITGLIEDSGEMEINDEN DER  
BEZIRKSGEMEINSCHAFT ÜBERETSCH  
UNTERLAND

**AUSFÜHRUNGSPROJEKT**

**Unterlage**

**2**

FACHBERICHT: TECHNISCHER BERICHT ANLAGEN

Rev. **2**

v. **30.01.2019**

Ber.:

**Erstellt von**

Ing. Angelo Carpani – Ingenieurskammer der Provinz Como Nr.2368A

**Validierungen**

Verfahrensverantwortliche/Verantwortliche  
des Technischen Büros  
Dr. Arch. Elisa Bernardi

**Daten**

## 1. EINFÜHRUNG

In dieser Unterlage werden die *verschiedenen im Projekt enthaltenen Anlagen beschrieben, die angewandten Lösungen begründet, die Gesamtfunktion des anlagentechnischen Teils sowie die Wechselbeziehung zu vorhandenen Gebäuden angegeben und beschrieben.*

Wie bereits im Allgemeinen Bericht erläutert, umfasst das geplante Vorhaben die Realisierung von zwei Arten von Anlagen:

- **Videoüberwachungsanlagen**, wo die Installation von (feststehenden) "Erfassungskameras" und (beweglichen speed dome) "Übersichtskameras" vorgesehen ist, die in den einzelnen Gemeinden anhand eines Wireless-Netzes im freien Standardfrequenzband **ETSI HIPERLAN 2 (High Performance Radio LAN)** im Bereich **5,470-5,725 GHz** zu zentralisieren sind, wo PC's mit Server/Client-Funktion installiert werden. Die Videoüberwachungssysteme der einzelnen Gemeinden müssen dann anhand von ADSL-Leitungen verbunden werden. Darüber hinaus muss eine einzelne Software-Plattform **VMS (Video Management System)** eingerichtet werden.
- **Anlagen zur Nummernschilderkennung**, wo Videokameras zur Erfassung der Kfz-Nummernschilder installiert werden, mit Zeichenerkennungs-Algorithmus an Bord der Kamera, auch als **OCR (Optical Character Recognition)** bezeichnet. Diese müssen beim Sitz der Bezirksgemeinschaft in der Gemeinde Neumarkt anhand eines auch als **3G-Netz** bekannten Mobiltelefonnetzes **UMTS (Universal Mobile Telecommunications System)**, oder durch ein auch als **4G-Netz** bekanntes **LTE-Netz (Long Term Evolution)** angebunden werden. Die Gemeinden und die Ordnungskräfte können anhand der vorhandenen, über Web-Browser angebundenen PC-Stationen oder anhand von Tablets mit WiFi und 3G/4G-Anbindung auf die im zentralen Verwaltungssystem des Nummernschilderkennungssystems gespeicherten Metadaten zugreifen.

Die Anlagen müssen mit der allgemeinen Anforderungen konform sein, die in der **Richtlinie des Innenministeriums Nr. 558/SICP ART/421.2/70 vom 2. März 2012** zum Thema „Videoüberwachungssysteme auf Gemeindeebene“ und insbesondere in der *Technischen Dokumentation* beschrieben sind, das der „Plattform der integrierten Videoüberwachung“ beiliegt. Diese Anforderungen werden nachstehend in Erinnerung gerufen.

### Netzarchitektur

*Das Videoüberwachungssystem muss auf einer IP-Netzarchitektur basieren, die die Verbindung zwischen Feldgeräten und Leitstellen gestattet.*

*Unabhängig von den zu verwendenden Datenübertragungseinrichtungen (z.B. Faseroptik, Wireless-Geräte) muss der Netzaufbau in jedem Fall die folgenden Anforderungen erfüllen:*

- *Sie müssen die notwendige Bandkapazität für die Übertragung der Bilder in Abhängigkeit von den Merkmalen der Videokameras und der Technologie des Übertragungsnetzes aufweisen.*

- *Der Video-Datenfluss muss entsprechend den Anforderungen aus Abs. 3.3.1 Komma t) der „Verfügung zum Thema Videoüberwachung“ vom 8. April 2010 (Nutzung öffentlicher Netze und Wireless-Anbindungen) der Datenschutzbehörde verschlüsselt werden.*
- *Zuverlässigkeit*
- *Eventuelle Redundanz.*

### Aufzeichnungssystem

*Das System zur Aufzeichnung und Speicherung der Videoaufnahmen muss auch im Hinblick auf die Nutzung seitens der Justizbehörden folgendes gestatten:*

- *Zeitenplanarchivierung mit Playback;*
- *Aufzeichnungskapazität pro einzelner Kamera mit Abwicklung vor und nach dem Auftreten von Alarmen;*
- *Speicherung der von allen Videokameras kommenden Bilder mit der maximal möglichen Frame-Rate;*
- *Speicherung des Datenflusses mit Verdichtungsalgorithmus MJPEG/MPEG4/H264;*
- *Die Aufzeichnung der Bilder muss in verschlüsselter Form erfolgen, um ihre Geheimhaltung und Integrität zu gewährleisten;*
- *Die Videoaufnahmen müssen (lokal oder remote) anhand eines spezifischen Sichtgeräts exportierbar sein zwecks Entschlüsselung und Überprüfung ihrer Integrität;*
- *Die Speicherkapazität muss für die gleichzeitige Einspeicherung aller Bilder aller Videokameras bei maximal zulässiger Frame-Rate der Geräte selbst bzw. der Anbindung für 24 Std pro Tag an mindestens 7 Tagen ausreichend sein.*

Die realisierten Anlagen müssen eine **dauerhaft gleichbleibende Qualität** der Videosignale gewährleisten, auch bei Veränderungen der Wetter- und Umgebungsbedingungen. Insbesondere müssen alle im Freien installierten Geräte in klimatisierten Schutzgehäusen untergebracht werden, um die einwandfreie Funktion des Systems auch bei Temperaturen unter 0°C zu gewährleisten. Diese Schutzgehäuse müssen eine ausreichende IP-Schutzart aufweisen.

Alle Geräte müssen mit Zertifikaten ausgestattet sein, die ihre **Konformität mit den einschlägigen Gesetzen und Vorschriften** bescheinigen (z.B. CE-Kennzeichen, INRIM-Zertifikat usw.). Darüber hinaus müssen Produkte **erstklassiger, erkennbarer Marken** eingesetzt werden, die von anerkannt führenden Unternehmen der CCTV-Branche hergestellt und/oder eingebaut wurden, sowie mit einem Qualitätskennzeichen (z.B. IMQ, CE, TÜV, usw.).

Alle Versorgungsleitungen der Überwachungsstationen der Videoüberwachungs- und Nummernschilderkennungssysteme müssen durch einen Thermoschutz-Differentialschalter mit automatischer Rückstellung geschützt werden.

Nachstehend sind die Leistungen und die technischen Funktionen beschrieben, die beide Systeme besitzen müssen, wobei darauf hingewiesen wird, dass die Angabe von Bezeichnung und Typ eines Produkts mit Nennung des Herstellers bzw. die Rückführbarkeit von technischen Anforderungen auf ein bestimmtes Produkt ausschließlich zu dem Zweck erfolgt, unverwechselbare Eigenschaften des Produkts

anzugeben, das beschrieben werden soll. Die Teilnehmer an der Ausschreibung sind gehalten, Systeme und Geräte zu liefern, die vergleichbare und/oder bessere technische Leistungen bieten und in der Lage sind, die gleiche Funktion zu erfüllen.

## 2. VIDEOÜBERWACHUNGSANLAGEN

Die Videoüberwachungsanlagen müssen in Konformität mit der **Richtlinie des Innenministeriums Nr. 558/SICP ART/421.2/70 vom 2. März 2012** zum Thema „Videoüberwachungssysteme auf Gemeindeebene“ und insbesondere der *Technischen Unterlage* realisiert werden, die der „Plattform für integrierte Videoüberwachung“ beigefügt ist, wo die Bezugsmerkmale für neue städtische Videoüberwachungsanlagen mit der Zielsetzung bestimmt werden, den Zweck der Registrierung von Szenarien zu garantieren, welche dazu dienen, die betroffenen Ordnungskräfte bei ihrer Tätigkeit zur Verhinderung und Bekämpfung von Straftaten zu unterstützen.

### 2.1 Technische Merkmale der Videokameras und der Videosever

Nachstehend sind die technischen Mindestanforderungen aufgeführt, die die Videokameras und die Videosever erfüllen müssen und in der *Technischen Unterlage* beschrieben sind, die der vorstehend genannten **Richtlinie des Innenministeriums** beigefügt ist.

#### 2.1.1 Übersichts-Kameras (feststehend)

Die feststehenden Übersichts-Kameras müssen das breitestmögliche Aufnahmefeld gestatten. Die technischen Merkmale der Aufnahmegeräte müssen den nachstehend beschriebenen **Mindestanforderungen** entsprechen:

- IP-native Videokamera mit Update-Möglichkeit über IP;
- Feste, austauschbare oder Varifocal-Optik je nach den jeweiligen praktischen Erfordernissen, mit Richt-Aufnahmewinkel zwischen 20° und 120°;
- Farb-Aufnahmetechnologie mittels CMOS- oder CCD-Sensor;
- Empfindlichkeit des Aufnahmekomplexes mindestens 0,5 Lux bei Farbaufnahmen (bei Tag) und mindestens 0,05 Lux bei S/W-Aufnahmen (bei Nacht), gemessen bei 50 IRE;
- Mindestauflösung des Sensors: full HD (1920x1080);
- Mindestanforderungen an den Bildfluss: 1.3 Megapixel (1280x1024) und Bildfrequenz nicht unter 9 fps;
- Betriebsart „day&night“ mit automatischer Umschaltung;
- Verdichtungsalgorithmus des Bildflusses: Motion JPEG, H264 und dessen Weiterentwicklungen;
- Übertragungsalgorithmus des Bildflusses: RTSP;
- Eingebaute Activity Detector-Funktion;
- Client NTP;
- 1 Alarmeingang an Bord der Kamera;
- 1 Ausgang;
- Gewinnsteuerung, Weißabgleich: automatisch und per Software regelbar;
- Automatische Gegenlichtkompensation;

- Möglichkeit, eine Video-Analysesoftware direkt an der Kamera zu installieren;
- Stromversorgung: Niederspannung nicht über 48 Vac, PoE Klasse 3);
- Alarmgabe bei Störungen. Es müssen mindestens die folgenden Alarme verwaltet werden:
  - bei Öffnen des Schutzgehäuses
  - bei Ausfall des Videosignals
  - bei Verdunkelung der Videokamera
  - bei Veränderung des Aufnahmefelds (Verlagerung der Videokamera);
- Betriebsbedingungen: es ist Aufgabe des Unternehmens, die Art des Schutzgehäuses für jede Videokamera in Abhängigkeit von den klimatischen Mindest- und Höchstbedingungen (Temperatur, Feuchtigkeit) am Installationsort zu bestimmen. Das Gehäuse ist so zu wählen, dass die einwandfreie Funktion über das ganze Jahr hinweg gewährleistet wird. Das Intervall darf in jedem Fall nicht unter  $-10^{\circ}$ ;  $+45^{\circ}$  Temperatur und 20%;80% Feuchtigkeit liegen;
- Schutzart des Gehäuses: Das Gerät muss vor Wettereinflüssen wie Regen, Salzluf, am Installationsort typischem Staub geschützt werden, um maximale Funktionstüchtigkeit zu gewährleisten. Die Schutzart darf nicht unter IP65 liegen, und muss bei Anforderung der völligen Dichtheit auf IP66 erhöht werden;
- Lieferung von SDK für Entwicklung durch Dritte.

### 2.1.2 Beobachtungs-Videokameras

Diese Videokameras müssen schwenkbar sein, einen Aufnahmewinkel von  $360^{\circ}$  auf der horizontalen Ebene und  $180^{\circ}$  auf der vertikalen Ebene gewährleisten und müssen einen außenstehenden Beobachter daran hindern, den aufgenommenen Bereich zu erkennen. Die technischen Merkmale der Aufnahmegерäte müssen den nachstehend beschriebenen **Mindestanforderungen** entsprechen:

- IP-native Videokamera, mit Update-Möglichkeit über IP;
- Farb- Videokamera mit Funktion „DAY/NIGHT“;
- Aktive Matrix des Sensors mit Pixelzahl nicht unter 704 x576 (4CIF);
- Frame-Rate nicht unter 15fps;
- Empfindlichkeit des Aufnahmekomplexes mindestens 0,5 Lux bei Farbaufnahmen (bei Tag) und mindestens 0,05 Lux bei SW-Aufnahmen (bei Nacht), gemessen bei 50 IRE;
- Autofokus-Objektiv mit Zoom (mindestens 25X optisch mit mindestens F.1.8 Auto-Iris);
- Verdichtungsalgorithmus Bildfluss: Motion JPEG, H264 und dessen Weiterentwicklungen;
- Übertragungsalgorithmus des Bildflusses: RTSP;
- Schwenkung mit variabler endless-Geschwindigkeit in horizontaler Richtung und fernsteuerbar in vertikaler Richtung
- Mechanischer PTZ
- Eingebaute Activity Detector-Funktion;
- Client NTP;
- 16 vorwählbare Winkelstellungen (Preset);
- 8 Vorwahl-Sequenzen (Tour);

- 1 Alarmeingang an Bord der Kamera
- Mindestens 1 Alarmausgang an Bord der Kamera
- 8 Ausschluss-Zonen (Privacy Mask).
- Automatische Patrouillenfunktion
- Stromversorgung: Niederspannung nicht über 48 Vac oder PoE Klasse 3);
- Betriebsbedingungen: es ist Aufgabe des Unternehmens, die Art des Schutzgehäuses für jede Videokamera in Abhängigkeit von den klimatischen Mindest- und Höchstbedingungen (Temperatur, Feuchtigkeit) am Installationsort zu bestimmen. Das Gehäuse ist so zu wählen, dass die einwandfreie Funktion über das ganze Jahr hinweg gewährleistet wird. Das Intervall darf in jedem Fall nicht unter  $-10^{\circ}$ ;  $+45^{\circ}$  Temperatur und 20%;80% Feuchtigkeit liegen;
- Schutzart des Gehäuses: Das Gerät muss vor Wettereinflüssen wie Regen, Salzluf, am Installationsort typischem Staub geschützt werden, um maximale Funktionstüchtigkeit zu gewährleisten. Die Schutzart darf nicht unter IP65 liegen, und muss bei Anforderung der völligen Dichtheit auf IP66 erhöht werden
- Lieferung von SDK für Entwicklung durch Dritte

### 2.1.3 Videosever

Die Videosever müssen in der Lage sein, gleichzeitig den in das System eingespeisten Bildfluss aller Videokameras aufzunehmen, wobei folgende Anforderungen erfüllt werden müssen:

- Verwaltung von Videokameras unterschiedlicher Hersteller, offene Plattform.
- Live View bis zu 30 oder mehr FPS.
- Verwaltung des Bildflusses mittels Verdichtungsalgorithmus MJPEG/MPEG4/H264.
- Funktion NVR.
- Export gespeicherter Dateien mit Verschlüsselung.
- Verwaltung PTZ Patrolling.
- Funktion WEB Client.
- Funktion Mobile Client.
- Verwaltung von Maps
- Integration mit Videoanalyse.
- Steuerung I/O und Ereignisse.
- Betriebssysteme neuester Generation (64 Bit-Plattformen).
- Unterstützung Multistream pro Kamera.
- Integrierte Funktion Video Motion Detection (VMD) mit Verwaltung von Ausschlusszonen.
- Unterstützung von Full Duplex Audio-Kanälen.
- Preset Positions pro Kamera.
- Verwaltung Preset nach Ereignis.
- Preset Patrolling.
- Privacy masking.
- Automatische Suche und automatische Erkennung der Videokameras.
- Export und Import von Konfigurationen.



- Verwaltung und Export von History-Archiven, die alle Informationen über die Zustands-Ereignisse des Systems und die von den Bedienern ausgeführten Operationen enthalten (Log-Dateien).
- Lieferung von SDK für Entwicklung durch Dritte.

Für die Videosever muss eine redundante Stromversorgung vorgesehen werden.

### Hinweise zu eventuellen Verbesserungen im „Technischen Angebot“ für die Videokameras

- Sofern ein Bewerber im Rahmen der Ausschreibung als „qualitative“ technische Verbesserung Videokameras mit einer höheren Auflösung zu bieten beabsichtigt (z.B. Kameras mit 5 Mega-Pixel), oder als „mengenmäßige“ technische Verbesserung eine höhere Anzahl von Videokameras, so muss die Speicherkapazität für die gleichzeitige Aufzeichnung aller Videokameras bei maximaler Frame-Rate derselben bzw. der Anbindung für die Dauer von 24 Std. an mindestens 7 Tagen ausreichend dimensioniert werden.

## **2.2 Merkmale der Software VMS (Video Management System)**

Im eigenen Angebot müssen die Bewerber berücksichtigen, dass alle VMS Software-Plattformen vom gleichen Hersteller stammen müssen.

Das VMS stellt das Element dar, mit dessen Hilfe es möglich sein muss:

- Die spezifischen Elemente des Videoüberwachungssystems zu verwalten;
- Die aktiven Videokameras zu überwachen durch Realisierung von Anzeigetafeln mit individuell gestaltbarem Anzeigen-Layout;
- Anzeige des Bildflusses in Modalität live oder aufgezeichnet;
- Ausführung von Suchfunktionen anhand unterschiedlicher, den Bildfluss betreffender Parameter (Aufnahmekamera, Uhrzeit, zugehörige Motion-Detection-Ereignisse usw.);
- Speicherung des Bildflusses aufgrund festgelegter Retention-Policies;
- Unterstützung der Alarme durch Bereitstellung einer Übersicht sowohl über die System-Alarme als auch über die Alarme peripherischer Sicherheitselemente.

Das VMS muss mindestens folgendes gestatten:

- Unterstützung einer breiten Palette von Videokameras unterschiedlicher Hersteller unter Gewährleistung der Übereinstimmung mit dem ONVIF-Standard und in jedem Fall unter Gewährleistung der vollen Kompatibilität und Funktionstüchtigkeit der angebotenen Kameras, ausgenommen solche zur Erfassung der Nummernschilder;
- Konfiguration unterschiedlicher Benutzer und Profile für den Zugriff auf das System. Jedem Benutzer und jedem Profil müssen unterschiedliche Berechtigungen zugeordnet werden können (z.B. Schreib-Lesevorgänge, Löschung usw.);
- Anlegen von Benutzergruppen;
- Jedem Benutzer bzw. jeder Benutzergruppe muss die Verwaltung unterschiedlicher Kameragruppen zugeordnet werden können, einschließlich der Anzeige der zugehörigen Alarme;
- Anzeige des Bildflusses (live und registriert) und Konfiguration des Systems sowohl anhand eines spezifischen Clients als auch über Web (mindestens über Internet

Explorer, Mozilla Firefox, Google Chrome, ohne am Client Komponenten beliebiger Art installieren zu müssen). Darüber hinaus muss es möglich sein, auf das System anhand von Mobilgeräten mittels Verwendung von App-Programmen für mobile Endgeräte zuzugreifen (kompatibel mit iOS, Android und Windows). An allen genannten Fällen wird der Zugriff nach entsprechender Anmeldung mittels Login und Passwort gestattet;

- Exportieren von statischen Bildern (mindestens .jpg) und Videodateien (mindestens .avi) in externe Datenquellen;
- Unterstützung eines sicheren Sendeprotokolls HTTPS (Hypertext Transfer Protocol Secure);
- Möglichkeit der Nutzung nicht proprietärer Hardware für die Realisierung der Lösung (Server, Aufzeichnungsdatenträger unterschiedlicher Art, Client). Darüber hinaus muss es möglich sein, in virtueller Umgebung zu arbeiten;
- Möglichkeit, skalierbare Architekturen zu realisieren;
- Automatische Erfassung und Installation der Videokameras, die das Protokoll ONVIF unterstützen;
- Es müssen mindestens die Verdichtungsformate H.264, MJPEG für den Bildfluss aller Geräte unterstützt werden, einschließlich der an den Encodern angeschlossenen Analog-Videokameras;
- Unterstützung des live Multistreamings der Videokameras unter Nutzung verschiedener Auflösungen, Formate und Bildgeschwindigkeiten für jeden Bildfluss;
- Möglichkeit der Erkennung der Bewegung im Bildfluss und Möglichkeit des Ausschlusses der Erfassung in besonderen vorbestimmten Zonen (Ausschlusszonen);
- Verhinderung der Anzeige von Teilen des von einer Videokamera aufgenommenen Bilds anhand der Konfiguration von Datenschutz-Zonen;
- Metadaten-Suchfunktion, d.h. Definition von einem bestimmten Ereignis zugeordneten Informationen. Es muss möglich sein, sowohl die von VMS generierten Metadaten zu unterstützen, als auch diejenigen, die durch eine an Bord der Kamera ausgeführte Videoanalyse generiert werden (ONVIF compliant);
- Unterstützung der Eingabe von Regeln/Handlungen bei Ereignissen und von Melde-Profilen für die Bestimmung von Regeln für die automatische Versendung von Meldungen per E-Mail;
- Möglichkeit der Anzeige auf Maps, die es gestattet, eine Übersicht über das System zu gewinnen und auf die in der Map aufgeführten Komponenten zuzugreifen (Videokameras, PTZ, Server, I/O usw.), die durch Ikonen des Typs „drag and drop“ dargestellt werden (es muss beispielsweise möglich sein, die *live*-Aufnahmen einer Videokamera einzusehen, indem einfach deren Ikone auf der entsprechenden Map angeklickt wird). Es müssen mindestens die Formate jpg und gif unterstützt werden. Im Fall mehrstufiger Maps muss das Umschalten zwischen den verschiedenen Stufen der Map möglich sein;
- Ordnungsgemäße Steuerung der angebotenen PTZ-Videokameras, die mindestens folgendes gestatten muss:
  - Änderung der Richtung und/oder das Zoomen anhand der spezifischen Funktionen PAN/TILT/ZOOM;
  - Einstellung vorbestimmter, konfigurierbarer Positionen für die Videokameras;
  - Bestimmung von Patrouillen-Profilen;





- Automatisches Umstellen der Videokamera auf eine bestimmte Voreinstellung bzw. Starten eines spezifischen Patrouillen-Profiles im Fall eines Ereignisses;
- Einstellung und Änderung der Geschwindigkeit für den Einsatz der Kameras;
- Möglichkeit, die Patrouillen-Funktion während des Handbetriebs auf Pause umzuschalten;
- Einsatz der angebotenen Control Boards und Joysticks;
- Unterstützung der Alarmverwaltung. Diese Funktion muss mindestens folgendes gestatten:
  - Aktivierung von Alarmen im Fall von Ereignissen
  - Anzeige der aktivierten Alarme
  - Individualisierbare Definition von Alarm-Kategorien und Verwaltung der Prioritäten derselben;
- Installation auf Plattformen mit Microsoft-Betriebssystem.

Die angebotenen VMS-Software muss die folgenden Leistungen/Funktionen gewährleisten:

### **Edge Storage**

Unter *Edge Storage* versteht sich die VMS-Funktion, anhand deren es möglich ist, die Filmaufnahmen peripherisch in den Speicherkarten der Videokameras zu speichern, wobei gewährleistet sein muss, dass Teile dieser Aufzeichnungen im Fall von Störungen der Verbindung zwischen Videokamera und VMS (fehlende Anbindung, Blockade des Aufzeichnungsservers usw.) aus dem Peripheriegerät wieder übernommen werden können.

### **Signatur der aufgezeichneten Videofilme**

Unter *Signatur der aufgezeichneten Videofilme* versteht sich die Funktion des VMS, die es gestattet, dem Videofilm sowohl während der Aufnahme als auch im Moment des Exports eine digitale Signatur zuzuordnen.

### **Verteiltes System**

Unter *Verteiltem System* versteht sich die Funktion des VMS, die durch einen VMS-System fortgeschrittener Generation die zentralisierte Verwaltung mehrerer VMS-Instanzen gestattet, die sich an entfernten Standorten befinden. Am zentralen Standort muss daher die volle Funktionsfähigkeit aller an Remote-Standorten angeschlossener Kameras gewährleistet werden (beispielsweise muss es möglich sein, den Bildfluss anzuzeigen und zu speichern, eventuelle Meldungen zu empfangen usw.). An den Remote-Standorten müssen die Administratoren und die lokalen Benutzer die Möglichkeit haben, auf das System zuzugreifen, um den Standort im Fall einer Unterbrechung der Verbindung mit der Zentrale vor Ort steuern zu können.



## 2.2.1 Integration der bereits installierten Videokameras und Videoüberwachungssysteme

Die Gemeinde Leifers hat in ihrem Gemeindegebiet bereits ein Videoüberwachungssystem mit Kameras für die Videoüberwachung und die Nummernschilderkennung installiert (35 Kameras für die Videoüberwachung + 4 Kameras für die Nummernschilderkennung). Das Projekt muss die Integration des derzeitigen Systems in die neue Plattform beinhalten.

Die Steuerungssoftware ist „Milestone XProtect Professional 2013“ und die Videokameras sind Marke „ACTI“, teils Modell B82 und teils Modell B46.

Eventuelle weitere bestehende Anlagen für die Videoüberwachung müssen ebenfalls in das neue System integriert werden können und müssen anlässlich des Lokalausgleichs durch die Techniker untersucht werden.

Um die Ausschreibungsteilnehmer mit der Wahl der VMS-Softwareplattform nicht an die bereits bestehenden technologischen Lösungen zu knüpfen, wird breite Wahlfreiheit gewährt, wobei zu berücksichtigen ist, dass die Integration der in den verschiedenen Gemeinden bereits bestehenden Videoüberwachungssysteme eines der Elemente für die Bewertung des wirtschaftlich vorteilhaftesten Angebots darstellt.

## 2.3 Eigenschaften des Standard Wireless-Netztes HIPERLAN 2

Zur Realisierung der Wireless-Anbindungen innerhalb der einzelnen Gemeinden müssen Geräte eingesetzt werden, die in der Lage sind, ausschließlich innerhalb nicht lizenzpflichtiger Bandbreiten (*freie Bandbreiten*) zu arbeiten, insbesondere 5,4GHz (zwischen 5470MHz und 5725MHz) Standard **HIPERLAN 2** gemäß der einschlägigen ETSI-Normen.

### 2.3.1 Der Standard HIPERLAN 2

Die mit dem Standard HIPERLAN 2 kompatiblen Geräte weisen elektromagnetische Emissionen auf, die nach gesetzlicher Vorschrift auf **1 Watt EIRP** (Effective Isotropic Radiated Power) beschränkt sind, was 30 dBm entspricht.

Was insbesondere die Dichte des Leistungsspektrums des abgegebenen Signals betrifft, so müssen die Sender der HIPERLAN 2 Outdoor-Geräte eine maximale Dichte von 50 mW/MHz aufweisen, was bedeutet, dass sie normalerweise Kanäle mit einer Breite von 20 MHz besitzen müssen ( $50 \text{ mW/MHz} \times 20 \text{ MHz} = 1 \text{ W}$ ). Abweichende Kanalbreiten sind zulässig, vorausgesetzt, dass die vorgeschriebenen Dichtengrenzwerte nicht überschritten werden. Aufgrund des Europäischen Standards ETSI EN 301 893 beträgt die maximal zulässige Kanalbreite 40 MHz.

Der Einsatz von HIPERLAN macht die Aktivierung von zwei Mechanismen obligatorisch:

#### **TPC (Transmitter Power Control)**

Der Sender muss mit einem System zur Kontrolle der Leistung ausgestattet sein, das einen Dämpfungsfaktor von mindestens 3dB gewährleisten muss. In anderen Worten



handelt es sich dabei um die Fähigkeit des Hiperlan-Geräts, seine Sendeleistung instantan in Abhängigkeit von verschiedenen Faktoren zu ändern. Die Geräte nutzen nur diejenige Leistung die notwendig ist, um das Senden erfolgreich ausführen zu können. Wenn die beiden Geräte nahe beieinander installiert sind, ist also nur eine Leistung von wenigen mW erforderlich. Bei größeren Abständen kann sie dagegen bis zu 1W bzw. 30dBm +/- 3dB ansteigen.

### **DFS (Dynamic Frequency Selection)**

Dies ist die Fähigkeit des Hiperlan-Geräts, instantan und stetig seine Sendefrequenz (Sendekanal) zu ändern. Es handelt sich um eine Software-Funktion, die es dem Master-Gerät gestattet, eine Störung der RADAR-Geräte für die Flugzeugnavigation zu vermeiden, indem dem Slave-Gerät die neue Sendefrequenz mitgeteilt wird. Die von Hiperlan verwendeten Frequenzen sind die gleichen, die für Radargeräte verwendet werden. Aus diesem Grund müssen die möglicherweise schädlichen Interferenzen mit solchen Geräten vermieden werden.

### **2.3.2 MIMO-Technologie**

Die geplante Maßnahme sieht die Implementierung von Wireless-Anbindungen zwischen den Punkten vor, die keine perfekte optische Sicht zwischen Sende- und Empfangspunkt bieten (**nLOS**: near-Line-Of-Sight) oder gar (**NLOS**: Non-Line-Of-Sight). Um diesem Nachteil aus dem Wege zu gehen ist es äußerst wichtig, dass die leistungsfähigsten Funktechnologien und -Standards angewandt werden, wie beispielsweise die **Technologie MiMo (Multi input Multi output)**. Diese gestattet es, gleichzeitig einen Datenstream zwischen zwei nicht in Sichtweite befindlichen Antennen mit gutem Anbindungsniveau zu senden und zu empfangen.

Die Technologie **MiMo** nutzt die **Multipath**-Erscheinung, d.h. ein sehr bekanntes Naturphänomen der Funkwellen. Diese Eigenschaft gestattet die Steigerung der Sendegeschwindigkeit, ohne notwendigerweise die Sendebandbreite vergrößern zu müssen. Das Signal wird von verschiedenen Quellen ausgesendet und erreicht dank des „Abprallens“ an Wänden und anderen im Raum vorhandenen Gegenständen die Empfängerantenne auf mehreren Strecken zu leicht verschiedenen Zeitpunkten, so dass verschiedene simultane Datenflüsse entstehen, die in der Lage sind, mehr Informationen zu transportieren, als ein einzelner „Standardfluss“.

Der Einsatz eines **MiMo**-Apparats ist, wie bereits vorstehend erwähnt, sinnvoll in Fällen von **nLOS** oder **NLOS**, d.h. wenn auf der Strecke zwischen zwei Punkten Hindernisse vorhanden sind, die die Qualität des Signals beeinträchtigen. Dank der Technologie **OFDM (Orthogonal Frequency Division Multiplexing)**, d.h. ein Sendetechnik, die in einer Multiplex-Modulierung der Trägerfrequenz besteht, was bedeutet, dass eine hohe Anzahl von zueinander orthogonal ausgerichteten Sub-Trägerfrequenzen verwendet wird. Das Frequenzband ist also in Sub-Trägerfrequenzen aufgeteilt, die in der Luft abweichende Strecken zurücklegen können, wenn Hindernisse vorhanden sind. Dadurch steigert sich die Wahrscheinlichkeit, dass eine höhere Anzahl Teilsignale den Empfänger erreicht. Der wichtigste Vorteil der Technologie OFDM gegenüber dem Aufbau mit einer einzelnen Trägerfrequenz besteht gerade in der Fähigkeit, auch bei schlechtesten Bedingungen des Sendekanals eine Kommunikation herzustellen.



### 2.3.3 Kriterien für die Dimensionierung der Wireless-Anbindungen

Für jede Wireless-Anbindung muss folgendes berechnet werden:

#### 1) EIRP (Effective Isotropic Radiated Power)

$$\text{EIRP (dBm)} = P_o - C_t + G_t$$

wobei:

- $P_o$  = output power transmitted (dBm)
- $C_t$  = transmitter cable/connectors attenuation (dB)
- $G_t$  = transmitting antenna gain (dBi)

Laut Vorschrift muss der Wert EIRP bei 5,4 GHz-Geräten kleiner/gleich 30dBm / 1W sein (bei 2,4GHz-Geräten dagegen kleiner/gleich 20dBm / 100mW).

#### 2) Freiraumdämpfung (free space path loss)

$$P_l \text{ (dB)} = 32,4 + 20 \log F(\text{MHZ}) + 20 \log R(\text{Km})$$

#### 3) RSSI (Receiver power level at receiver input)

$$\text{RSSI (dBm)} = \text{EIRP} - P_l + G_r - C_r$$

wobei:

- $G_r$  = receiving antenna gain (dBi)
- $C_r$  = receiver cable/connectors attenuation (dB)

#### 4) Verbindungsreserve des Systems (Link Margin)

$$\text{Link Margin (dB)} = \text{RSSI} - P_s$$

wobei:

- $P_s$  = die vom Hersteller des angebotenen Funkapparats erklärte „receiver sensitivity“ (dBm)

#### 5) Mindesthöhe der Antenne über dem Hindernis (Fresnel Zone Clearance)

#### 6) Garantierte Bandbreite für jede Verbindung mit Angabe des garantierten Mindestgeschwindigkeit (throughput) zwischen einem beliebigen Endpunkt des Netzes (Videokamera) und dem Sternpunkt des Wireless-Netzes bei voller Netzauslastung.

### Interferenzen

Die zu realisierenden Wireless-Netze müssen sich perfekt in die bereits bestehenden Funkverbindungen integrieren und die Zuschlagsfirma muss die auf den einzelnen Gemeindegebieten vorhandenen Funkfrequenzen prüfen. Im Projekt der Wireless-Netze müssen Überlagerungen vermieden werden (*non-overlapping channels*).

Bei Verwendung von *Funkgeräten HiperLAN 2*, die mit 5,4GHz im „freien Band“ arbeiten, ist die Funktion DFS (automatischer Wechsel des Sendekanals im Fall der Überlagerung mit anderen HiperLAN-Sendern oder zur Vermeidung von Konflikten mit Radarsystemen,



die das gleiche Frequenzband nutzen) obligatorisch vorgeschrieben. Die Aktivierung dieser Funktion macht allerdings das Funkgerät äußerst instabil, mit ständigen Wechseln des Kanals und daraus folgender kurzzeitiger Unterbrechungen der Verbindung, besonders in stark „gestörten“ Zonen. Um die Zuverlässigkeit und die Sicherheit zu verbessern, sollten bevorzugt spezielle Technologien zum Einsatz kommen, wie beispielsweise „Mesh“, die eine doppelte Funksendung auf 5.4 und 2.4 GHz mit redundanten „Bündel“-Verbindungen vorsehen, oder die Verwendung von Apparaten mit GPS-Synchronisation.

### **Bandbreite**

Für jeden Netzabschnitt muss die Bandbreite berechnet werden, die von den IP-Videoüberwachungskameras für den Bild- und Datenfluss benötigt wird. Außerdem ist zu prüfen, ob sie für jeden einzelnen Verbindungsabschnitt durch die garantierte Mindestbandbreite unterstützt werden.

Die für die IP-Videoüberwachungskameras benötigte Bandbreite ist von deren Konfiguration abhängig und variiert aufgrund verschiedener Faktoren, wie :

- Größe der Bilder
- Verdichtung
- Frame-Geschwindigkeit (Bilder pro Sekunde);
- Komplexität des Szenariums

Selbstverständlich muss die Nutz-Datendurchsatzkapazität (troughput) und die Routing-Kapazität bewertet werden, um die Leistungen des Netzes zu optimieren. Dabei ist besonders der beachtliche Bandbedarf der Videokameras für die Übertragung qualitativ hochwertiger Bilder an den Aufzeichnungsserver zu berücksichtigen. Die Videokameras dürfen nur den „Server“ „sehen“, während der Server „das gesamte Netz“ sehen muss.

### **2.3.4 Sicherheitsmaßnahmen**

Eine mangelnde Konfiguration der Sicherheitsfunktionen führt zu verletzlichen Schwachstellen des Wireless-Netzes, dessen Struktur in diesem Fall nicht geschützt ist und daher jedermann offensteht, der sich beispielsweise mit einer geeigneten Vorrichtung in den Aktionsbereich eines Verbindungsabschnitts begibt. Dies kann folgende Risiken bedingen:

- Zugriff auf geheim zuhaltende Informationen
- Betriebsunterbrechungen
- Angriffe Typ DOS ( Denial Of Service ).

Aus diesem Grund muss das angebotene Wireless-Netz die folgenden Mindest-Sicherheitsfunktionen beinhalten:

#### **Änderung des Zugriffs-Passworts und der IP-Adressen der Wireless-Apparate**

Viele neue Geräte haben ein bekanntes oder gar deaktiviertes Default-Passwort. Gleiches gilt für die IP-Adressen, die werkseitig vorgegeben werden. Eindringlinge, denen die standardisierten Passworts und IP-Adressen bekannt sind, haben daher leichten Zugang zum Netz. Aus diesem Grund müssen die Passworts und die IP-Adressen der Apparate geändert werden.



### **Sperrung des Systems DHCP**

DHCP ist ein System zur Vereinfachung der Netzverwaltung durch automatische Zuordnung einer IP-Adresse zu jeder Maschine, die sich in das Netz einschaltet. Dies kann in verkabelter Umgebung bequem sein, ist jedoch in einer Wireless-Umgebung gefährlich, weil dadurch automatisch auch einem unbefugten Eindringling eine IP-Adresse zugeteilt würde. Aus diesem Grund muss das System DHCP gesperrt und die Adressen der einzelnen Wireless-Karten von Hand zugeordnet werden. Dem Client-Server wird somit eine statische IP-Adresse mitgeteilt.

### **Änderung des SSID ( Service Set Identifier )**

Das Wireless-Netz hat eine eigene Kennung, die als SSID bezeichnet wird und den Wireless-Steuerkarten bekannt sein muss, um die Verbindung herstellen zu können. Auch in diesem Fall werden die meisten Wireless-Geräte werkseitig so eingestellt, dass sie als SSID den Namen des Herstellers verwenden (z.B. „Tsunami“ – Cisco, „101“ – 3Com, usw.). Um Eindringlingen, denen diese werkseitigen Default-Einstellungen bekannt sind, das Leben etwas schwerer zu machen, muss die SSID-Kennung geändert und durch eine weniger intuitive ersetzt werden.

### **Verschlüsselung WEP / AES**

Normalerweise unterstützen die Wireless-Systeme zwei Algorithmen für die Verschlüsselung der Daten: WEP oder AES. WEP (Wired Equivalent Privacy) ist ein Algorithmus zur Verschlüsselung der Daten mit der Methode RC4 zum Schutz der Wireless-Netze. Diese basiert auf einem gemeinsamen Schlüssel, der 64 bis 128 Bit lang ist. Diese Methode hat einige bekannte Schwachpunkte, wegen denen der Algorithmus WEP fast nutzlos ist. WPA2 (Wi-Fi Protected Access 2) ist der neueste Algorithmus, der speziell zu dem Zweck entwickelt wurde, den Kommunikationen, die auf dem Standard IEEE 802.11 (Wireless) basieren, eine Sicherheitsschicht zu bieten. Dabei wurde der Verschlüsselungs-Algorithmus RC4 aufgegeben und stattdessen der AES (Advanced Encryption Standard) verwendet, der höhere Sicherheit bietet. Aus den oben genannten Gründen wird Systemen der Vorzug gegeben, die den Algorithmus AES verwenden.

### **Aktivierung von MAC Filtering oder MAC Address Authentication**

MAC Address ist eine Hardware-Adresse, die eindeutig jede Netzkarte (Wireless oder andere) identifiziert. MAC ist ein Kürzel, das für *Media Access Control* steht und für den Zugang zum physischen Datenübertragungsmedium auf Datalink-Ebene gemäß Standard ISO/OSI verwendet wird. Die Access Points oder Router Wireless können so eingestellt werden, dass die Verbindungen nur von Karten akzeptieren, die eine bestimmte MAC-Adresse aufweisen. Das bedeutet dass es trotz korrektem SSID und AES-Schlüssel nicht möglich ist, auf das Wireless-Netz zuzugreifen, wenn der jeweilige MAC nicht auf der Liste der zugelassenen Adressen steht. Aus obigen Gründen muss die Kontrolle der MAC-Adresse vorgesehen werden.

## **2.3.5 Technische Merkmale der Konnektivitätsgeräte**

In diesem Abschnitt sind die technischen Merkmale der Konnektivitätsgeräte beschrieben. Anhand dieser Geräte können Outdoor-Wireless-Netze realisiert werden, um die Sendung des Bildflusses an die Leitzentralen LS zu ermöglichen, welche wiederum die Geräte für die Aufzeichnung und Anzeige der Bilder hospitieren. Die Ausschreibungsteilnehmer sind

aufgefordert, keine Beschränkungen der Datendurchsatzkapazität der Geräte auf Software- oder Lizenzebene vorzusehen.

### **Bridge Wireless Point to Point (PtP)**

Merkmal	Geforderte Werte
Standard Wireless	ETSI HIPERLAN 2
	IEEE 802.11n
Betriebsfrequenzbereich	5,470–5,725 GHz
Modulationstechnik	OFDM
Max. Sendegeschwindigkeit der Daten	mindestens 300Mbps
Antenne	Eingebaut oder extern, im Preis inbegriffen, mit Gewinn von mindestens 20dBi
Ethernet-Port, Steckverbinder	Mindestens 1 Ethernet-Port 100/1000Base-TX Full Duplex mit Steckverbinder RJ-45
Datensicherheit	WEP, WPA, WPA2, Anmeldung mittels Server RADIUS, Mac Filtering
Unterstützung VLAN	IEEE 802.1Q
Qos	IEEE 802.1p
Fernbedienung, sowohl verkabelt als auch wireless oder lokal über Ethernet-Port/Serielle Schnittstelle, mit mindestens einem der nachstehenden Protokolle.	SSH, Telnet, HTTPS
Upgrade Software mittels mindestens einem der folgenden Protokolle	TFTP, FTP
SNMP	V1 und/oder v2 und/oder v3
Schutzart	IP67
Betriebstemperatur	Mindestens -30°C / +50°C

## Bridge Wireless Point to MultiPoint (PtMP)

Merkmal	Geforderte Werte
Standard Wireless	ETSI HIPERLAN 2
	IEEE 802.11n
Betriebsfrequenzbereich	5,470–5,725 GHz
Modulationstechnik	OFDM
Max. Sendegeschwindigkeit der Daten	Mindestens 300Mbps
Antenna	Eingebaut oder extern, im Preis inbegriffen, mit Gewinn von mindestens 16dBi
Horizontaler Öffnungswinkel	Mindestens 90°
Ethernet-Port, Steckverbinder	Mindestens 1 Ethernet-Port 100/1000Base-TX Full Duplex mit Steckverbinder RJ-45
Datensicherheit	WEP, WPA, WPA2, Anmeldung mittels Server RADIUS, Mac Filtering
Unterstützung VLAN	IEEE 802.1Q
Qos	IEEE 802.1p
Fernbedienung, sowohl verkabelt als auch wireless oder lokal über Ethernet-Port/Serielle Schnittstelle, mit mindestens einem der nachstehenden Protokolle.	SSH, Telnet, HTTPS
Upgrade Software mittels mindestens einem der folgenden Protokolle	TFTP, FTP
SNMP	V1 e/o v2 e/o v3
Schutzart	IP67
Betriebstemperatur	Mindestens -30°C / +50°C



## Wireless CPE

Merkmal	Geforderte Werte
Standard Wireless	ETSI HIPERLAN 2
	IEEE 802.11n
Betriebsfrequenzbereich	5,470–5,725 GHz
Modulationstechnik	OFDM
Max. Sendegeschwindigkeit der Daten	Mindestens 150Mbps
Antenne	Eingebaut oder extern, im Preis inbegriffen, mit Gewinn von mindestens 20dBi
Ethernet-Port, Steckverbinder	Mindestens 1 Ethernet-Port 100/1000Base-TX Full Duplex mit Steckverbinder RJ-45
Datensicherheit	WEP, WPA, WPA2, Anmeldung mittels Server RADIUS, Mac Filtering
Unterstützung VLAN	IEEE 802.1Q
Qos	IEEE 802.1p
Fernbedienung, sowohl verkabelt als auch wireless oder lokal über Ethernet-Port/Serielle Schnittstelle, mit mindestens einem der nachstehenden Protokolle.	SSH, Telnet, HTTPS
Upgrade Software mittels mindestens einem der folgenden Protokolle	TFTP, FTP
SNMP	V1 e/o v2 e/o v3
Schutzart	IP67
Betriebstemperatur	Mindestens -30°C / +50°C

### Switch 4 Ports 10/100BaseT + 1 Port SFP

Merkmal	Geforderte Werte
Anzahl Ports	Mindestens 4 Ports autosensing 10/100BaseT
	Mindestens 1 Port SFP zur Aufnahme der Uplink-Module
Poe	Unterstützung Poe(802.3at/af) an den 4 Ports 100BaseT
Mindestband der Schaltmatrix	Mindestens 10 Gbps
Unterstützte Standards und Protokolle	IEEE 802.1D Definition von Bridge und Switch Standard
	IEEE 802.1Q Virtual VLANs
	IEEE 802.1p Class of Service
	IEEE 802.1w Rapid Spanning Tree
	IEEE 802.3 Ethernet
	IEEE 802.3u Fast Ethernet
	IEEE 802.3z Gigabit Ethernet
	IEEE 802.3ab Gigabit Ethernet over Copper
	IEEE 802.3ad Link Aggregation
	IEEE 802.1x Port Based Network Access Control
	IEEE 802.1s Multiple Spanning tree
	SNMP v2 e/o v3
	Snooping IGMP v2 e/o v3
	Verwaltung mittels SSH
Unterstützung des Protokolls NTP und/oder SNTP	
Schutzart	Mindestens IP30
Betriebstemperatur	Mindestens -20°C / +50°C
Aufnahmemöglichkeit von zusätzlichen Transceiver-Komponenten :	1000Base-SX
	1000Base-LX
	1000BASE-LX10

## Switch 8 Ports 10/100BaseT + 2 Ports SFP

Merkmal	Geforderte Werte
Anzahl Ports	Mindestens 8 Ports autosensing 10/100BaseT
	Mindestens 2 Ports SFP zur Aufnahme von Uplink-Modulen
PoE	Unterstützung Poe(802.3at/af) an 8 Ports 100BaseT
Mindestband der Schaltmatrix	Mindestens 20 Gbps
Unterstützte Standards und Protokolle	IEEE 802.1D Definition von Bridge und Switch Standard
	IEEE 802.1Q Virtual VLANs
	IEEE 802.1p Class of Service
	IEEE 802.1w Rapid Spanning Tree
	IEEE 802.3 Ethernet
	IEEE 802.3u Fast Ethernet
	IEEE 802.3z Gigabit Ethernet
	IEEE 802.3ab Gigabit Ethernet over Copper
	IEEE 802.3ad Link Aggregation
	IEEE 802.1x Port Based Network Access Control
	IEEE 802.1s Multiple Spanning tree
	SNMP v2 e/o v3
	Snooping IGMP v2 e/o v3
	Verwaltung mittels SSH
Unterstützung des Protokolls NTP und/oder SNTP	
Schutzart	Mindestens IP30
Betriebstemperatur	Mindestens -20°C / +50°C
Aufnahmemöglichkeit von zusätzlichen Transceiver-Komponenten:	1000Base-SX
	1000Base-LX
	1000BASE-LX10



### **2.3.6 Hinweise zu den Wireless-Anschlüssen in den einzelnen Gemeinden**

Die Überwachungsstationen müssen in Wireless-Modalität an die PC's angeschlossen werden, die als Server/Client bei den Dienststellen der Stadtpolizei/den Rathäusern (Leitstellen) zu installieren sind.

Einige der Überwachungsstationen haben keinen direkten optischen Kontakt mit den Leitstellen und es erweist sich als schwierig, geeignete Zwischenpunkte zur Verstärkung der Wireless-Signale ausfindig zu machen. Aufgrund dieser Schwierigkeit werden alle Überwachungsstationen als „Standalone“- Stationen mit lokaler Registrierung angelegt.

Generell steht es den Teilnehmern an der Ausschreibung frei, als technische Verbesserung Wireless-Verbindungen anzubieten, die eine Installation der Wireless-Apparate ausschließlich auf eigenen Strukturen und Gebäuden der Bezirksgemeinschaft oder der Gemeinden vorsehen.

Wenn ein Ausschreibungsteilnehmer im Rahmen der Ausschreibung als qualitative technische Verbesserung beabsichtigt, Videokameras mit höherer Auflösung anzubieten (z.B. Videokameras mit 5 Megapixel), oder als quantitative technische Verbesserung eine höhere Anzahl von Kameras, muss die notwendige Bandkapazität für das Senden von Bildern in Abhängigkeit von den Merkmalen der Kameras und der Topologie des Sendenetzes ausreichend dimensioniert werden.

### **2.4 Zentralisierung der Videoüberwachungssysteme**

Das Videoüberwachungssystem sieht die Einrichtung mehrerer Leitstellen (LS) bei den Dienststellen der Stadtpolizei vor.

Die Videoüberwachungssysteme der einzelnen Gemeinden müssen untereinander durch ADSL-Leitungen verbunden sein, um die Videoüberwachung seitens der Ordnungskräfte (Carabinieri in Bozen und Neumarkt und Quästur in Bozen) zu ermöglichen, auch wenn die Systeme nicht mit Personal besetzt sind.

Auf diese Weise wird die vollständige Autonomie jedes lokalen Systems gewährleistet, das somit völlig von den anderen Systemen unabhängig ist. Die Verwaltung der Zugriffsberechtigungen der Benutzer und der Zulassungs- und Anzeigeprivilegien, eventuell auch nur für bestimmte Videokameras, gewährleistet den Schutz der Personaldaten innerhalb der einzelnen lokalen Systeme.

Zu diesem Zweck ist folgendes von grundlegender Bedeutung:

- Dass das VMS-System die vorstehend beschriebene Funktion „verteilter Betrieb“ besitzt;
- Dass die VMS Software-Plattformen der gleichen Marke angehören

Aus verschiedenen Gründen müssen die Videoüberwachungssysteme wie vorstehend bereits erwähnt anhand von ADSL-Leitungen miteinander verbunden sein:

- Derzeit wird in den verschiedenen Gemeinden des Unterlands das Faseroptik-Netz eingeführt, das in Zukunft die tragende Struktur des Systems sein wird;
- Einige Gemeinden (beispielsweise Aldein, Altrei, Truden usw.) sind mit Wireless-Verbindungen nicht leicht zu erreichen, da keine Sichtverbindung möglich ist;



- Die im freien 5.4 GHz-Band HIPERLAN verfügbaren Funkkanäle sind inzwischen gesättigt (d.h. sie sind belegt oder weisen starke Interferenzen auf). Wenn man darüber hinaus die Distanzen berücksichtigt, die im Spiel sind, und die Hindernisse in der sogenannten Fresnel-Zone, wäre es also kaum möglich, die in der o.g. Richtlinie des Innenministeriums verlangte „*notwendige Bandkapazität für das Senden von Bildern in Abhängigkeit von den Merkmalen der Videokameras und der Topologie des Sendernetzes*“ zu gewährleisten.

Es steht den Ausschreibungsteilnehmern jedoch frei, als verbesserte Lösung eventuelle Wireless-Verbindungen auf freien Bandfrequenzen anzubieten.

In Italien können die Inhaber einer generellen Zulassung für elektrische und elektronische Kommunikationsdienste neben den Frequenzbändern 2,4GHz und 5,4GHz für Punkt-zu-Punkt-Verbindungen auch 2 weitere freie Frequenzbänder nutzen:

- Band 24.000,0 – 24.250,0 MHz
- Band 71.000,0 – 86.000,0 MHz.

### **Band 24.000,0 – 24.250,0 MHz**

Vorteile: Kann für hohe Full-Duplex-Sendegeschwindigkeiten genutzt werden  
Parabolantennen ab 30 cm  
Wird nicht für PtMP genutzt, daher geringe Störfaktoren  
Niedrige EIRP-Grenze (20dBm max)

Nachteile: Wegen der Kombination von hoher Frequenz und niedriger EIRP-Grenze kann diese Frequenz für kurze Entfernungen genutzt werden.

### **Band 71.000,0 – 86.000,0 MHz**

Vorteile: Kann für hohe Full-Duplex-Sendegeschwindigkeiten genutzt werden  
Parabolantennen ab 30 cm  
Wird nicht für PtMP genutzt, daher geringe Störfaktoren  
Hohe EIRP-Grenze (75dBm max)

Nachteile: Wegen der besonders hohen Frequenz kann diese Frequenz für kurze Entfernungen von normalerweise 3-5 km verwendet werden.

### **Wichtige Hinweise:**

- Eventuelle Wireless-Verbindungen zwischen den Gemeinden müssen die Installation von Wireless-Apparaten ausschließlich auf Strukturen und Gebäuden der Gemeinde oder der Bezirksgemeinschaft vorsehen.
- Da die Ausschreibung normalerweise die Verbindung zwischen den Videoüberwachungssystemen der Gemeinden mittels ADSL-Leitungen vorsieht, wurden in der “Gesamtkostenrechnung” und im “Wirtschaftlichen Rahmen des Projekts” keine Beträge für die Realisierung eines Wireless-Verbindungsnetzes

ausgewiesen. Ein eventuelles Angebot für die Verbindung der Gemeinden mittels Wireless-Netz im freien Bandbereich wird im Rahmen der Ausschreibung als technische Verbesserung gewertet und bringt daher keine Zusatzkosten für die Gemeinden mit sich.

- Da das System zur Verbindung der Videoüberwachungssysteme den Zweck hat, eine Überwachung der Videokameras durch die Ordnungskräfte zu ermöglichen, ist es nur dann sinnvoll, Wireless-Verbindungen herzustellen (auch nur für bestimmte und nicht für alle Gemeinden), wenn diese an die verschiedenen Leitstellen der Carabinieri in Bozen und/oder Neumarkt bzw. bei der Quästur in Bozen angebunden werden.

### 3. ANLAGEN ZUR ERKENNUNG VON NUMMERNSCHILDERN

Die geplante Maßnahme sieht die Installation von Stationen zur Kontrolle und Erkennung von Nummernschildern an den wichtigsten Zufahrtsstraßen der Gemeindegebiete vor, die als "Durchgänge" bezeichnet werden. Die Systeme zur Erkennung der Nummernschildern sind in der **Richtlinie des Innenministeriums Nr.558/SICP ART/421.2/70 vom 2. März 2012** zum Thema der *Videoüberwachungssysteme auf Gemeindeebene* und insbesondere in der *Technischen Unterlage* als Beilage zur „Plattform für integrierte Videoüberwachung“ nicht beschrieben.

Die Systeme zur automatischen Nummernschilderkennung werden auch mit **ANPR (Automatic Number Plate Recognition)** bezeichnet. Im Rahmen der geplanten Maßnahme sind Systeme mit Nummernschilderkennungsalgorithmus an Bord der Videokamera vorgesehen, d.h. Videokameras mit **OCR (Optical Character Recognition)**.

Die Algorithmen zur Nummernschilderkennung, die an Bord der Kamera installiert sind, zeichnen sich im Vergleich zu Systemen mit auf Server zentralisiertem Nummernschilderkennungsalgorithmus durch höhere Realisierungskosten aus, bieten dafür aber auch eine wesentlich höhere Präzision bei der Erkennung der Nummernschilder unter beliebigen Betriebsbedingungen. Die Zuverlässigkeit ist höher, weil die Videokamera, sofern sie wegen eines Netzfehlers nicht auf den zentralen Server zugreifen kann, mit der notwendigen Technologie ausgestattet ist, um das Nummernschild selbständig erkennen zu können und es vorübergehend lokal zu speichern. Die Videokameras dieser Kategorie sind eigens für diesen Zweck ausgelegt: sie verfügen daher über eine spezifische DSP-Verarbeitungseinheit, über eine integrierte OCR-Software und über einen gepulsten Infrarot-Strahler zur Optimierung der Ausleuchtung des Nummernschildes. Darüber hinaus unterstützen diese Kameras mehrere Protokolle für die Übertragung sowohl der Bildaufnahme als auch der Metadaten zur OCR-Verarbeitung.

Die geplante Maßnahme verlangt die Installation von Nummernschilderkennungssystemen mit OCR-Sensor, der die geometrische und syntaktische Kontrolle der Nummernschilder der Fahrzeuge gestattet, mit einer „Übersichts-Kamera“, die das gesamte Fahrzeug aufnimmt und somit die Feststellung des KfZ-Modells ermöglicht.

Die Systeme zur automatischen Nummernschilderkennung müssen den gesamten, durch die Durchfahrtsstelle fließenden Verkehr erfassen. Sobald ein Nummernschild erkannt wird, schießt das Gerät eine Aufnahme und speichert die zu diesem Nummernschild



gehörigen Metadaten, das Datum und die Uhrzeit der Durchfahrt und die Kennung des Durchfahrts, an dem die Aufnahme gemacht wurde, in einer Datenbank.

Wenn ein spezifisches Nummernschild gesucht werden soll, muss der Benutzer über eine Schnittstelle verfügen, die es ihm gestattet, die gespeicherten Nummernschilder aufgrund verschiedener Suchkriterien wieder abzurufen, beispielsweise aufgrund der KfZ-Nummer oder eines Teils davon, aufgrund eines bestimmten Zeitraums und der spezifischen Durchfahrtsstelle. Dank dieser auf einer Datenbank basierenden Abfrage geht die Suche eines bestimmten Nummernschilds wesentlich schneller vonstatten, als dies bei gewöhnlichen Videoüberwachungssystemen der Fall ist, wo die gesamte Aufzeichnung „abgespult“ werden und das Nummernschild erkannt und von Hand festgehalten werden muss.

In jüngerer Zeit haben einige Hersteller von Software für die Verwaltung solcher Systeme einige interessante Funktionen eingeführt, durch die sich die Effizienz der Sicherheitsüberwachung noch zusätzlich steigert. Unter diesen interessanten Funktionen sind zu nennen:

- Die Verwaltung von „Blacklists“ mit Meldung der Durchfahrt von gesuchten Nummernschildern mittels SMS-Mitteilung oder E-Mail;
- Möglichkeit der Überprüfung, ob die erkannten Nummernschilder Fahrzeugen ohne Haftpflichtversicherungsdeckung oder solchen mit überfälliger Revision zugeordnet sind;
- Die Erkennung von ADR-/Kemler-Codes von Gefahrstoffen, die verschiedene Videokameras inzwischen zu verarbeiten fähig sind;
- Die automatische Zählung der durchgefahrenen Fahrzeuge.

Auf dem Markt werden darüber hinaus auch statistische Funktionen angeboten, die Daten nicht nur bezüglich der Sicherheit und der Verkehrszählung liefern, sondern auch strukturierte Informationen wie beispielsweise die Klassifizierung der Fahrzeuge, deren Zugehörigkeitsnation oder die Verkehrsgeschwindigkeit in den verschiedenen Zeitspannen.

Anhand des Nummernschilds kann auf das Zulassungsjahr des Fahrzeugs und auf die Schadstoffklasse nach Euro-Norm zurückgeschlossen werden, so dass wertvolle Informationen für eine Schätzung der durch den zirkulierenden Fahrzeugpark verursachten Umweltbelastung bereitgestellt werden.

Aufgrund einer Matrixanalyse ist das Verwaltungssystem in der Lage, auf einem grafischen Plan die Dynamik aufzuzeigen, mit der sich der Verkehr innerhalb des überwachten Gebiets entwickelt, und die Durchfahrtsdauer zu berechnen.

Das System kann veranlasst werden, an jedem Durchfahrtspunkt das durch Pendelverkehr bedingte Verkehrsaufkommen von dem der ansässigen Bevölkerung zu trennen, so dass anwendbare Änderungen der Verkehrswege geprüft werden können.

Die Systeme zur Erkennung der Nummernschilder werden also im Wesentlichen immer mehr zu Systemen zur Überwachung des Verkehrs werden, einschließlich der Interaktion mit Ampelsystemen und Wechselverkehrszeichen zur Optimierung des Timings in Abhängigkeit von der erfassten Verkehrsintensität.



### 3.1 Technische HW-Merkmale der Kamera für die Nummernschilderkennung

Nachstehend sind die technischen Merkmale beschrieben, die eine Kamera für die Nummernschilderkennung aufweisen muss.

Die vollständig integrierte Vorrichtung zu automatischen Nummernschilderkennung (ANPR) muss eine hochauflösende monochromatische Kamera für die OCR-Funktion beinhalten, eine hochauflösende Farbkamera für die Erstellung von Bildern des durchfahrenden Fahrzeugs (Übersichts-Kamera), einen leistungsfähigen Strahler mit langem Aktionsbereich, eine Hochleistungsplatine für die Verarbeitung der Bilder, sowie eine Speichereinheit. Das Ganze muss in einem Gehäuse mit Schutzart IP65 untergebracht sein.

Das Produkt muss für ANPR-Installationen für normale Verkehrswege im Ortsgebiet oder für Zufahrten, die aufgrund der Art der ein/ausfahrenden Fahrzeuge besonders aufwändig sind, wie beispielsweise bei Lastzügen, Lastwagen oder Nutzfahrzeugen generell.

Das Produkt muss technologisch innovativ sein und den neuesten Entwicklungen der LPR Anwendungen (*License Plate Recognition*) Rechnung tragen. Die für die Erkennung der Nummernschilder bestimmte OCR-Kamera muss synchron mit dem Beleuchtungssystem gesteuert werden, um ein perfektes Nummernschilderkennungssystem mit Mehrfachbeleuchtung zu gewährleisten, das in der Lage ist, Nummernschilder unter beliebigen Lichtverhältnissen bei Tag und bei Nacht zu erfassen.

Die hohe Framerate (60 Bilder pro Sekunde) muss auch ohne externe Trigger das automatische Erkennen der Fahrzeuge anhand von Bildanalysetechniken ermöglichen, durch die Kombination von Algorithmen zur Nummernschilderkennung und Algorithmen des Typs „Blob Motion Tracking“, die in der Lage sind, die Bewegung von Gegenständen innerhalb der Szene zu erkennen.

Die Übersichts-Farbkamera muss perfekt synchron zu der OCR-Kamera arbeiten, um einen Nachweis der Durchfahrt zu erzeugen, der aus zwei im gleichen Moment aufgenommenen Bildern besteht.

Sowohl die Übersichts- als auch die OCR-Kamera müssen mit unterschiedlichen Optiken in Abhängigkeit von den Erfordernissen des Kunden in Bezug auf das Sichtfeld ausgestattet werden können.

Das Produkt muss in der Lage sein, Nummernschilder bis zu einer Geschwindigkeit von 160 km/h ohne Triggersysteme (z.B. Schleifen, Laser, Radar) zu erfassen und zu erkennen.

Das Produkt muss für Installationen bis zu 25 m Entfernung und horizontalen und vertikalen Öffnungswinkeln bis zu 50° geeignet sein.

Die interne OCR-Library muss es gestatten, Nummernschilder mit unterschiedlichen nationalen Codierungen zu erkennen (gleichzeitige Erkennung von bis zu 28 EU-Ländern). Außerdem muss sie die Erkennung von Spezialcodes gestatten, wie beispielsweise solche für Gefahrstoffe (Kemler-Codes) und über eine spezifische Library für die Erkennung der Nummernschilder von Nutzfahrzeugen verfügen (Anhänger-Nummernschilder bei Lastzügen), deren Layout und Material deutlich vom Standard der



sonstigen Nummernschilder abweichen kann. Die Library muss darüber hinaus Sonder-Nummernschilder verarbeiten können (Militär- und Polizeifahrzeuge usw.).

Am Ende des Erfassungs- und Verarbeitungsprozesses muss das Produkt folgende Daten liefern können:

- Monochromatische OCR-Aufnahme mit eingespieltem Datum, Uhrzeit, Codierung des Nummernschilds.



Wie in der nachstehenden Abbildung dargestellt, muss das Produkt auch ein weiteres Bild mit einer auf den Bereich des Nummernschilds begrenzter Aufnahme bereitstellen.



Auf Anforderung muss das Produkt einen Detailausschnitt des Nummernschilds bereitstellen (CROP des Bilds).

- Zeitlich mit der OCR-Aufnahme übereinstimmendes Übersichtsbild, das ebenfalls das Datum, die Uhrzeit und die Codierung des Nummernschilds angeben muss.



Zusätzlich zu den Fotos, die die Durchfahrt des Fahrzeugs dokumentieren, muss das System die Durchfahrtsdaten ausweisen, d.h.: Zeichenfolge des Nummernschilds des Fahrzeugs, Nationalität, Uhrzeit der Durchfahrt in Stunden/Minuten/Sekunden, Datum, Kennung der Videokamera sowie weitere, zusätzliche Daten, die der Kunde im Moment der Installation des Produkts anhand der Web-Schnittstelle konfigurieren kann.

#### Video-Streaming-Funktion der Übersichtskamera

Das Produkt muss in der Lage sein, ein durchgängiges Video-Streaming mit einer Auflösung von 1020 x 1080 Pixel HD @ 15fps zu erzeugen, das auch in Video-Formaten mit geringerer Auflösung und niedrigerer Frame-Rate konfigurierbar sein muss. Das Streaming muss Typ H264 RTSP und muss bei Bedarf im Ereignisspeicher des Produkts für die Dauer einer einstellbaren Zeit gespeichert werden können.

#### Video-Klassifizierungsfunktion aufgrund von Übersichtsbildern

Das Produkt muss in der Lage sein, anhand des farbigen Übersichtsbilds des Fahrzeugs, zu dem das ermittelte Nummernschild gehört, auf den jeweiligen Fahrzeugtyp zu schließen und ihn auf dieser Grundlage zu klassifizieren als: Moped, Motorrad, Personenwagen, Lieferwagen/VAN, Lastwagen, Bus. Die Video-Klassifizierungsfunktion muss eine Präzision über 90% bei Tagesaufnahmen an Stationen zur Erkennung des Rückschilds aufweisen. Die Video-Klassifizierungsfunktion muss sowohl bei Stationen zur Erkennung des Rückschilds als auch des vorderen Nummernschilds aktivierbar sein. Bei Stationen zur Erkennung der vorderen Nummernschilder wird der Erkennbarkeits-Prozentsatz, der auf Mopeds und Motorräder keine Anwendung findet, möglicherweise auch bei kleineren Lieferwagen beeinträchtigt, da diese aufgrund ihrer Form leicht mit Personenwagen verwechselt werden können.

#### Farb-Klassifizierungsfunktion

Das Produkt muss in der Lage sein, anhand des farbigen Übersichtsbilds des Fahrzeugs, zu dem das ermittelte Nummernschild gehört, auf die Farbe des jeweiligen Fahrzeugs zu schließen und sie auf dieser Grundlage zu klassifizieren als: weiß, gelb, rot, grau, blau, schwarz. Die Farb-Klassifizierungsfunktion muss eine Präzision über 80% bei mit Tageslicht aufgenommenen Übersichtsbildern aufweisen. Das System zur Erkennung der Fahrzeugfarbe erkennt in Stationen zur Erkennung des Rückschilds im Fall von Hängerzügen und Sattelschleppern die Farbe des Anhänger-Teils.



### Funktion zur Schätzung der Fahrgeschwindigkeit

Das Produkt muss in der Lage sein, unter Nutzung der OCR-Bilder und der farbigen Übersichtsbilder für das Fahrzeug, dessen Nummernschild ermittelt wurde, auch die Fahrgeschwindigkeit im Ermittlungsbereich zu berechnen. Dieser Wert muss mit einem maximalen Fehler von +/- 15% im Vergleich zur realen Geschwindigkeit des Fahrzeugs angegeben werden.

### Interne Speicherung der Daten

**Das Produkt muss mit internen 120 GB SSD-Speicher** ausgestattet sein, der jedoch für zukünftige Erfordernisse auf eine Speicherkapazität von bis zu 1 TB erweiterbar sein soll. Darüber hinaus muss das Gerät die Möglichkeit bieten, für den Fall von Störungen des Hauptspeichers einen MicroSD-Backupspeicher zu montieren. Der interne Speicher muss die Speicherung der Durchfahrten (Bilder und Daten) geordnet nach Tag und Uhrzeit gestatten. Er muss einen spezifischen Speicherbereich für die Speicherung nicht erkannter Nummernschilder und Fahrzeugen mit nicht auswertbaren Nummernschildern (Bruch, Beschädigung, Unleserlichkeit aus verschiedenen Gründen wie beispielsweise Verdeckung, Verschmutzung, Verlust des reflektierenden Untergrunds usw. ) beinhalten, um alle Fahrzeug-Durchfahrten dokumentieren zu können.

Das Produkt muss in der Lage sein, auch bei mangelnder Kommunikation mit dem zentralen Supervisor-System bzw. dem eventuellen FTP-Server zu arbeiten. In diesem Fall muss das Produkt weiter in Betrieb bleiben und alle Durchfahrten im Bereich OCR registrieren. Wenn die Kommunikation wieder hergestellt wird, muss das Gerät eine Strategie zum Abruf der angesammelten Daten ausführen. Dieser Vorgang muss im Background anhand eines Prozesses mit niedriger Priorität stattfinden. Das bedeutet, dass das Lesegerät prioritär die Echtzeit-Durchfahrten senden muss, während die gespeicherten aufgearbeitet werden, wenn die OCR-Durchfahrt momentan nicht durch ein Fahrzeug in Anspruch genommen wird. Dieser Ablauf muss fortgesetzt werden, bis alle während des Kommunikationsausfalls gespeicherten Informationen aufgearbeitet wurden.

Im SSD-Speicher müssen Nummernschild-Listen (Whitelist und Blacklist) gespeichert werden können, die dann in Echtzeit mit den ermittelten Durchfahrtsdaten verglichen werden, um automatisch Alarme, Mitteilungen auslösen oder automatisch eine Zugangssperre aktivieren zu können (Schlagbaum, Verkehrsschwellen, Tore usw.).

### Unterstützung bei Wartung und Installation

Zur Unterstützung des Fernwartungsdienstes muss das Produkt automatisch statistische Berichte in grafischer Form erstellen, anhand deren die Leistungen des Geräts zu jeder Tages- und Nachtzeit kontrolliert werden können.

Zur Unterstützung der Installation und Wartung des Geräts muss dieses über einen PoE-Anschluss gespeist werden (Power over Ethernet), so dass der Betrieb anhand eines einzigen Kabels möglich ist.

Ebenfalls zur Erleichterung der Installation und Wartung muss das Produkt mit Wall Connectors IP66 ausgestattet sein, die ein rasches Lösen und eventuelles Entfernen gestatten, ohne Gefahr, die Infrastruktur der Durchfahrtsstelle oder das Gerät selbst zu schädigen.



### *Wichtigste Funktionsmerkmale des Produkts:*

- Deckung einer Durchfahrtsstelle bis zu 4 m Breite frontal;
- Erfassungsmöglichkeit der Nummernschilder in Free-run bei Geschwindigkeiten bis zu 160km/h;
- Herstellung eines farbigen, perfekt mit der OCR-Aufnahme synchronisierten Übersichtsbilds;
- Digitale OCR-Videokamera BW 1,3 Mpixel
- Infrarotstrahler 850nm 6 hochintensive Leds mit Stroboskop-funktion mit regelbarer Intensität und Dauer;
- Digitale Übersichts-Farbkamera 1,3 Mpixel
- Übersichts-Videokamera mit Modalität Day&Night (bei mangelnder Helligkeit muss auf BW-Bild umgeschaltet und der Infrarotfilter ausgeschaltet werden, um die Aufnahme-Empfindlichkeit zu steigern);
- Video-Streaming der Übersichts-Farbkamera H264 RTSP, Auflösung HD @15 fps.
- Feststehende Optik der OCR-Kamera, Anschluss Typ C;
- Varifocal-Optik IRIS der Übersichts-Videokamera
- Funktion Day&Night mit automatischer Ausschaltung des Infrarotfilters bei der Übersichts-Videokamera
- Stromversorgung 12:36Vdc 15W oder POE Plus IEEE 802.3at type2;
- Doppelter Steckverbinder IP67 (Ethernet Poe IEEE 802.3at typ 2 + power supply, I/O, RS485);
- 2 Digitaleingänge
- 2 digitale Relais-Ausgänge
- 1 Gigaethernet Port;
- 1 RS485 Port;
- Betriebstemperatur  $-20^{\circ}\text{C}$  bis  $+50^{\circ}\text{C}$ ;
- Schutzart IP66.



### *Wichtigste Funktionsmerkmale des Produkts:*

- Integrierter grafischer Web-service mit Konfigurationsschnittstelle
- Nummernschilderfassung mit Erkennung von bis zu 28 Ländern (EU) gleichzeitig
- Erkennen von Gefahrstoff-Codes (Kemler-Codes);
- Library für optimierte Erfassung von Anhänger-Kennschildern bei Lastzügen und von Spezial-Nummernschildern Carabinieri, Heer, Polizei, Rotes Kreuz, Diplomatisches Korps usw.);
- Bis zu 2 Blacklist/Whitelists gleichzeitig
- Fahrzeugklassifizierung durch Auswertung des Übersichtsbilds;
- Analyse mehrerer Nummernschilder innerhalb eines einzelnen OCR-Bilds
- Herstellung perfekt mit OCR synchronisierten Übersichts-Farbbildern
- Klassifizierung der Fahrzeuge aufgrund der Form im Übersichtsbild;
- Erkennung der Fahrzeugfarbe (6 Farben: weiß, gelb, rot, blau, grau, schwarz);
- Schätzung der Fahrgeschwindigkeit des Fahrzeugs;
- Erkennung der Fahrtrichtung und entsprechende Alarmgabe, sofern konfiguriert;
- Durchgängige Speicherung von Video-Streamings der Übersichtskamera, mit Möglichkeit der Konfiguration von Anzahl Tage, Bildformat, Frames per second.

### **3.2 Technische Merkmale der Steuer- und Nummernschilderkennungssoftware**

Die Software muss die Kompatibilität mit den wichtigsten Herstellern von Nummernschilderkennungs-Kameras mit Algorithmus OCR an Bord der Kamera gewährleisten (beispielsweise Tattile, Selea, Vigilante, Hikvision usw.), sowie die Möglichkeit der Integration mit den wichtigsten VMS-Aufzeichnungssoftwares (z.B. Milestone, Genetec, Arteco usw.).

Die Suche der Nummernschilder muss anhand einer einfachen Schnittstelle erfolgen können, wo verschiedene Kriterien eingegeben werden können, um den zu untersuchenden Zeitraum mehr oder weniger eng abzugrenzen.

Die Suche der Nummernschilder muss aufgrund folgender Kriterien gefiltert werden können:

- Name der Durchfahrtstelle
- Zeitraum
- Art des Fahrzeugs (Lastfahrzeuge, Motorräder, Personenwagen, Mopeds);
- Provinz, in der das Fahrzeug zugelassen wurde
- Transportierte Gefahrstoffe (ADR-Code);
- Einzelne Blacklist oder Whitelist;
- Zugehörigkeitsland



Die Anzeige der Durchfahrten muss auch in einer Modalität erfolgen, die das Anzeigen einer Vorschau der Übersichtsbilder gestattet, so dass die Suche effizienter und rascher gestaltet werden kann, wenn von einem Fahrzeug nicht die KfZ-Nummer, sondern nur die Farbe bekannt ist.

Darüber hinaus muss das System mit separaten Angaben die Speicherung nicht erkannter Nummernschilder gestatten und ausschließlich den dazu vorab autorisierten Stellen die Möglichkeit bieten, über die Suchschnittstelle die nicht einwandfrei erkannten KfZ-Nummern zu ändern.

Die Speicherung muss auch die Bildaufnahme der Durchfahrt beinhalten, um dem zuständigen Personal das Auslesen zwecks „manueller“ Erkennung des KfZ-Zeichens zu ermöglichen.

Das System muss die Verwaltung der vom Betreiber erstellten Nummernschild-Listen (Blacklist /Whitelist) gestatten, sowie im Fall der Feststellung von in diesen Listen verzeichneten Fahrzeugen die automatische Meldung mittels SMS-Mitteilung und/oder E-Mail.

Es muss möglich sein, alle oder einen Teil der Durchfahrtsdaten eines bestimmten Zeitraums an einer oder mehreren Durchfahrtstellen zu exportieren einschließlich Angabe der erkannten KfZ-Nummer und des zugehörigen Bilds.

Die genannten Fahrzeuglisten müssen bei Bedarf verschiedenen, im System festgelegten Benutzern zugänglich sein.

Die Software muss anhand einer spezifischen Suchfunktion die Möglichkeit bieten, die ADR-Nummer (Kemler-Codes UN) für Fahrzeuge zu verwalten, die Gefahrstoffe transportieren.

Darüber hinaus müssen folgende Funktionen bereitgestellt werden:

- Möglichkeit, pro Tag die Anzahl der erkannten ADR-Codes anzuzeigen;
- Umwandlung der ADR-Nummer in die entsprechende Bezeichnung des transportierten Gefahrstoffs
- Anzeige der Waren, die in einem bestimmten Zeitraum die meisten Zufahrten bedingt haben, mit grafischer Darstellung der Daten
- Anzeige der Analyse der Gefährlichkeit der transportierten Stoffe für eine bestimmte Kemler-Nummer mit grafischer Darstellung der Daten
- Anzeige des pro Tag erreichten Risiko-Niveaus und anhand einer progressiven Zahlenskala in Bezug auf den Transport von Gefahrstoffen
- Generierung und Versand einer SMS-Mitteilung an eine oder mehrere Telefonnummern in Echtzeit bei Durchfahrt eines Fahrzeugs mit einer besonderen UN-Nummer;

Die Software muss die Möglichkeit des Anschlusses an externe Datenbanken bieten, wie beispielsweise an den automatischen Abfragedienst des KfZ-Nummernregisters der KfZ. Es muss die Möglichkeit bestehen, auf das **Sistema Centralizzato Nazionale Targhe e Transiti (SCNTT, Nationales Zentralsystem für KfZ-Zeichen und Fahrten)** unter Einhaltung der einschlägigen Vorschriften zuzugreifen, sofern dies durch die zuständigen Behörden genehmigt wird.

Gen Tarhe 4

il portale dell'Automobilista

Login:   
  
 Hai dimenticato le password?

Ti trovi in: Home > Categorie > Accesso ai servizi > Copertura Assicurativa

Ministero delle Infrastrutture e dei Trasporti
   
 Guida al portale | Mappa del sito | FAQ

Home | Chi siamo | Codice della strada | Multimedia | News | Link | Contatti | Ricerca | UTILITÀ

Ricerca Ufficio della Motorizzazione Civile
   
 Ricerca Officine Autorizzate
   
 Ricerca Medici Certificatori
   
 Ricerca Copertura Assicurativa
   
 Ricerca Imprese Trasporto Persone
   
 Ricerca Nulle Osta Aree di Fermata

Copertura Assicurativa

**Risultato ricerca**
  
 Tipo Veicolo: AUTOVEICOLI | Targa: DZ180SX | Copertura Assicurativa: Il veicolo risulta assicurato

Attenzione: I dati sono aggiornati con frequenza settimanale nella giornata di domenica.

Il portale dell'Automobilista
   
 WSC VITTEL 2.0 | WSC CBB

**Copertura Assicurativa**

**Risultato ricerca**

Tipo Veicolo	Targa	Copertura Assicurativa
AUTOVEICOLI	DZ180SX	Il veicolo risulta assicurato

**Autofahrer-Portal, Ministerium für Infrastrukturen und Transporte: Prüfung und Meldung von Fahrzeugversicherungen**

Gen Tarhe 4

il portale dell'Automobilista

Login:   
  
 Hai dimenticato le password?

Ti trovi in: Home > Categorie > Accesso ai servizi > Verifica Classe Ambientale

Ministero delle Infrastrutture e dei Trasporti
   
 Guida al portale | Mappa del sito | FAQ

Home | Chi siamo | Codice della strada | Multimedia | News | Link | Contatti | Ricerca | UTILITÀ

Ricerca Ufficio della Motorizzazione Civile
   
 Ricerca Officine Autorizzate
   
 Ricerca Medici Certificatori
   
 Ricerca Copertura Assicurativa
   
 Ricerca Imprese Trasporto Persone
   
 Ricerca Nulle Osta Aree di Fermata

Verifica Classe Ambientale

**Risultato ricerca**
  
 Tipo veicolo: AUTOVEICOLO | Targa: DZ180SX | Compatibilità ambientale: EURO4

Attenzione: I dati sono aggiornati con frequenza settimanale nella giornata di domenica.

Il portale dell'Automobilista
   
 WSC VITTEL 2.0 | WSC CBB

**Verifica Classe Ambientale**

**Risultato ricerca**

Tipo veicolo	Targa	Compatibilità ambientale
AUTOVEICOLO	DZ180SX	EURO4

**Autofahrer-Portal, Ministeriums für Infrastrukturen und Transporte: Prüfung der Klassifizierung von Fahrzeugen nach Euro-Norm**



Die Software muss Statistiken bieten für:

- Zahl der an einer oder mehreren Zufahrtsstellen durchgefahrenen Fahrzeuge auf Zeit-Basis mit parametrisierter Abfrage;
- Bereitstellung von Grafiken bezüglich des Verkehrsaufkommens nach Uhrzeiten zwecks Untersuchung der Stoßzeiten;
- Angabe der durchschnittlichen Fahrgeschwindigkeit mit grafischer Darstellung der 24-Stundendaten;
- Angabe der Anzahl von KfZ-Zeichen einer bestimmten Nation mit grafischer Darstellung der Daten;
- Angabe der Anzahl von Fahrzeugen einer bestimmten Klasse (mindestens 5, maximal 28 Klassen) mit grafischer Darstellung der Daten und zusätzlicher Integration von Laserscannern und Radar mit Einzel-/Doppeltechnologie;
- Angabe des Zulassungsjahrs des Fahrzeugs mit grafischer Darstellung der Daten
- Angabe der Schadstoffklasse nach Euro-Norm mit grafischer Darstellung der Daten;
- Angabe der Durchfahrtszeit durch die Zu- und Ausfahrten des Wohnbereichs mit grafischer Darstellung der Daten;
- Angaben bezüglich der Verteilung des Verkehrs innerhalb des überwachten Gebiets.

Die Software muss die Verwaltung von Laser-Sensoren gestatten und eine Einstufung in 28 verschiedene Kategorien bieten, die Erfassung der Durchfahrtgeschwindigkeit des Fahrzeugs, Zählung der Achsenzahl bei Anhängern und Vermessung der Fahrzeugabmessungen.

Die Software muss es gestatten, Fußgänger und Radfahrer anhand spezifischer Sensoren zu zählen und zu klassifizieren, die Fahrgeschwindigkeit und die Aufenthaltsdauer innerhalb eines bestimmten Areals zu berechnen. Diese Informationen sind in spezifischen Grafiken darzustellen.

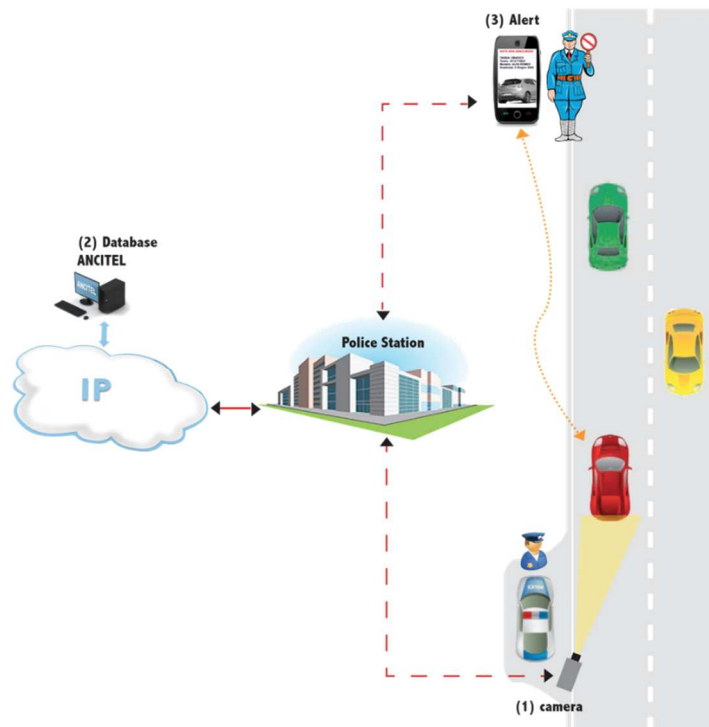
Die Software muss es gestatten, gleichzeitig mehrere GSM/UMTS-Modems für die automatische und differenzierte Weiterleitung der SMS-Mitteilungen zu verwalten. Dem im System definierten Benutzer muss ein spezifisches Modem zugeordnet werden, um eine Aufteilung der Telefonkosten zu ermöglichen. Die Software muss somit die Möglichkeit bieten, das Nummernschilderkennungssystem in Abhängigkeit von den auf das System zugreifenden Benutzern aufzuteilen und somit den Zugriff auf einen bestimmten Teil der installierten Durchfahrtsstellen zu beschränken.

Die Software muss die Möglichkeit bieten, Multiserver- und Multisite-Installationen vorzunehmen, ebenso wie die Möglichkeit, die im einzelnen System gespeicherten Datenbanken und Blacklisten für andere Benutzer zugänglich zu machen und somit die auf mehrere Server verteilte Suche von KfZ-Zeichen zu unterstützen.

Die Software muss mit allen handelsüblichen Browsern kompatibel sein und in Modalität Web sowohl anhand von PC's als auch anhand von Mobilgeräten wie Tablets oder Smartphones sowohl des Typs Android als auch des Typs IOS abgefragt werden können. Nachstehend ist ein Beispiel für den Betrieb eines Nummernschilderkennungssystems beschrieben:



1. Die Videokamera erkennt das Nummernschild und muss es über das 3G/4G-Netz dem zentralen Nummernschildverwaltungssystem beim Sitz der Bezirksgemeinschaft senden.
2. Die Software der Zentrale muss die Datenbank der freigegebenen Körperschaften abfragen (zB. Staatspolizei/Quästuren, ANIA, ANCITEL usw.) und in Echtzeit die Durchfahrt von gemeldeten Fahrzeugen mitteilen.
3. Wenn das Nummernschild gemeldet ist, sendet die Software per Smartphone/Tablet eine Meldung mit Foto und Fahrzeugdaten. Das Ganze muss innerhalb weniger Sekunden vonstattengehen.
4. Der Sicherheitsbeamte muss das Fahrzeug aufhalten, prüfen und eine Strafe verhängen können.



### 3.3 Verbindungsnetz zwischen den Nummernschilderkennungssystemen und Schätzung der Datenübertragungskosten

Die Systeme zur Erkennung von Nummernschildern müssen beim Sitz der Bezirksgemeinschaft in der Gemeinde Neumarkt zentralisiert werden anhand eines auch als **3G** bekanntes Mobiltelefonnetzes **UMTS** (*Universal Mobile Telecommunications System*) oder eines auch als **4G** bekannten Netzes **LTE** (*Long Term Evolution*). Die Gemeinden und die Ordnungskräfte können anhand von an einem Web-Browser angeschlossenen PC-Stationen oder anhand von Tablets mit WiFi- und 3G/4G-Anbindung auf die Metadaten/Bilder zugreifen, die im zentralen Verwaltungssystem der Nummernschilderkennung gespeichert sind.

Die Kosten der Konnektivität gehen zu Lasten der Gemeinden.



Die geplante Maßnahme umfasst zwei Kostenfaktoren:

- **Ausgabe auf Kapitalkonto oder Investitionskosten** für die Anschaffung des Materials (z.B. HW, VMS usw.);
- **Laufende Kosten** für den Betrieb der Anlage, die durch den Telefonverkehr für die Übertragung der von den Kontrollstationen kommenden Daten bedingt sind.

Bei der Schätzung der Kosten für die Datenübertragung wird Bezug genommen auf die **TARIFE UND GEBÜHREN – MOBILTELEFONVERKEHRSKLASSE** von CONSIP, die unter [aquistinretepa.it](http://aquistinretepa.it) eingesehen werden können, d.h. dem Einkaufsportal der Öffentlichen Verwaltung.

### 3.4 Zentrales System zur Speicherung der Kfz-Zeichen

Das zentrale System zur Speicherung der Kfz-Zeichen muss im Sitz der Bezirksgemeinschaft in der Gemeinde Neumarkt eingerichtet werden.

Das System muss die Speicherung der Durchfahrtsdaten und deren Abfrage mit hoher Zuverlässigkeit gewährleisten, d.h. anhand von mindestens zwei, in ihren Hardware-Komponenten redundanten Servern, während die Speicherung der Bilder mit einer einfachen Redundanz als RAID des Speicherplatten-Subsystems verwaltet werden kann.

Die wesentliche Anforderung besteht in der Aufrechterhaltung der Speicherfunktion der von den Videokameras erfassten Nummernschildern und der Abfrage derselben seitens der Bediener, auch bei Ausfall einer beliebigen Komponente des angebotenen Systemaufbaus.

Dem Anbieter wird die Wahl der Art des hochzuverlässigen Systemaufbaus freigestellt (Clustering-Typ, Lastverteiler usw.).

Die Failover-Modalität des Systems (d.h. die Funktion, die die Aktivierung des zweitrangigen oder Failover-Servers im Fall einer Störung des erstangigen Servers gewährleistet) muss automatisch und transparent ohne Zutun der Bediener ansprechen. Die akzeptable Dauer eines Systemausfalls muss auf 5 Minuten begrenzt sein.

Die Funktionen Failover und Failback des Systems müssen für die Bediener des Systems und der Videokameras im Feld transparent sein, d.h. es darf keinerlei Neu-Konfiguration notwendig sein, um den Betrieb wieder aufnehmen zu können.

Die Clustering-Modalität des Systems muss „active/active“ sein, um das Verarbeitungspotential bestmöglich nutzen zu können, d.h. die Server müssen gleichzeitig aktiv und erreichbar sein, so dass die gleichzeitig abgefragt werden können.

Dieser Aufbau gestattet eine Verteilung der Last auf alle verfügbaren Maschinen bzw. die Möglichkeit, die langwierigeren Verarbeitungen für die Erstellung der statistischen Berichte auf der Sekundärmaschine abzuwickeln, während die von den Videokameras erkannten Nummernschilder mit niedriger Latenz dem Primär-Server gesendet werden.



## **Netzinfrastruktur**

Die Netzwerkarchitektur muss unterteilt sein in Front-End und Back-End-Netz:

- Das Front-End-Netz hat eine vom Back-End-Netz getrennte Adressierungsebene und muss den Zugang zum System seitens der Benutzer gewährleisten.
- Das Back-End-Netz hat eine vom Front-End-Netz getrennte Adressierungsebene und muss die Konnektivität mit den im Feld installierten Videokameras gewährleisten.

Darüber hinaus muss ein internes, isoliertes Netz zur Verwaltung der Backup-Dienste und eventueller interner Kommunikationen der Cluster-Dienste vorhanden sein.

## **Backup-Dienste**

Der Daten-Backup-Dienst muss sowohl das Backup der Anwendungsdaten (Datenbank) als auch die von den Videokameras aufgenommenen Fotos beinhalten.

Dieser Dienst wird nicht anhand der zum Anwendungs-Cluster gehörigen Produktions-Server, sondern durch einen spezifischen Apparat/Servers erbracht.

## **Anwendung zur Speicherung der Durchfahrten und der Nummernschilder**

Angesichts der hohen Anzahl der an diesem Projekt beteiligten Videokameras, muss die Anwendung zur Speicherung der Nummernschilder und Durchfahrten auf einer relationalen Datenbank basieren, die akzeptable Leistungen auch bei Millionen registrierter Durchfahrten gewährleisten muss. Außerdem erleichtert die Nutzung dieser Technologie die zukünftige Erstellung spezifischer Reports für künftige Erfordernisse der Gemeinden.

## **Modem 3G/UMTS**

Im zentralen Nummernschild-Speichersystem ist auch die Installation von 17 zertifizierten Modems 3G/UMTS für den Versand der SMS-Mitteilungen vorgesehen, wenn beispielsweise vom System ein in der Blackliste enthaltenes Nummernschild erkannt wird. Die Modems senden weder Bilder noch Videoaufnahmen (Daten-SIM nicht inbegriffen).

Diese 17 Modems sind wie folgt unterteilt: ein Modem für jede der 16 Gemeinden der Bezirksgemeinschaft + ein Modem für die Carabinieri in Bozen und Neumarkt und in der Quästur Bozen.

In der Zentrale wird demzufolge eine ADSL-Leitung mit VPN-Konzentrator benötigt, die die Daten übernimmt, die von allen im Feld (Durchfahrtsstationen) installierten Modems gesendet werden.

Die Software des Nummernschilderkennungssystems muss die SMS-Warnmitteilungen korrekt den 17 Modems zuleiten, um dafür zu sorgen, dass jeder Benutzer nur für die eigenen bezahlen muss.



## **Typische Merkmale des Servers**

### *PROZESSOR*

Anzahl eingebauter Prozessoren: 1  
Max. Anzahl möglicher Prozessoren: 2  
Technologie: Xeon Six-Core  
Clock-Geschwindigkeit: 2,4 GHz  
Bit: 64

### *SPEICHER*

Installierter RAM-Speicher: 16 GB  
Maximal mögliche RAM-Kapazität: 768 GB  
Technologie: DDR3

### *STORAGE CONTROLLER*

Controller-Typ: SAS / SATA  
Unterstützte RAID-Stufen: 0/1/10

### *STORAGE*

Anzahl eingebauter Speicherplatten: 2  
Max. mögliche Anzahl Speicherplatten: 8  
Unterstützter Speicherplattentyp: SAS  
Verfügbare Nettospeicherkapazität: 1.2 Tb

### *BETRIEBSSYSTEM*

Windows Server 2012 R2 ITA STD Edition

### *KONNEKTIVITÄT*

Anzahl Netzkarten: 4  
Netzkartentyp: Gigabit Ethernet  
2 Karten 10 GbE  
Karte für Fernverwaltung

### *STORAGE CONTROLLER*

Controller-Typ: SAS / SATA  
Unterstützte RAID-Stufen: 0/1/5/10  
Installierter Cache-Speicher: 1.000 MB  
Upgrade Cache-Speicher möglich  
Maximal installierbarer Cache-Speicher: 4.000 MB  
Anzahl Kanäle: 0

### *STORAGE*

Anzahl eingebauter Speicherplatten: 0  
Max. möglich Anzahl Speicherplatten: 8  
Unterstützter Speicherplattentyp: SAS / SATA  
Gesamtgröße Datenträger: 0 GB  
Größe Datenträger: 10 GB  
Freie Slots für Hot Swap-Platten: 8  
Gesamtzahl Slots für Hot Swap-Platten: 8



## Merkmale Typ NAS

<b>Memory</b>	Total memory slots: 4 System memory: 8 GB DDR3 non-ECC RAM Memory module pre-installed: 4 GB x2 Memory expandable up to: 32 GB (8GB x4)
<b>Flash Memory</b>	512MB DOM
<b>Internal Cache Port</b>	Two mSATA port on board for read caching
<b>Hard Drive</b>	8 x 3.5-inch SATA 6Gbps/3Gbps hard drive or 2.5-inch SATA, 6Gbps/3Gbps hard drive SSD hard drive
<b>Hard Drive Tray</b>	8 x hot-swappable and lockable tray
<b>LAN Port</b>	Built-in 2 x 10 GbE (SFP+) and 4 x GbE 40GbE is optional
<b>USB</b>	4x USB 3.0 port (rear) 4x USB 2.0 port (rear) Support USB printer, pen drive, USB hub, and USB UPS etc.
<b>Buttons</b>	System: Power button and reset button
<b>Form Factor</b>	2U, Rackmount

## Kenntnisse Netz-Switch

Technische Merkmale:

- Verwaltung: Managed
- Routing-Träger (Layer 3)
- Quality Of Service (QOS)
- Unterstützte Vlan-Leitungen: 256
- Stacking-Modalität: physisches Stacking
- Größe Tabelle MAC: 16.000

Konnektivität:

- Typ und Geschwindigkeit LAN- Ports: RJ-45 10/100/1000 Mbps
- Anzahl LAN-Ports: 24
- Anzahl Uplink-Ports Faser/Optik (Slot SFP): 4
- Anzahl Uplink-Ports 10Gb: 2
- Anzahl gleichzeitig nutzbarer Ports (LAN + Uplink): 24
- Konsolen-Port

## Kenntnisse UPS

- Leistungsabgabe 2.700 Watt
- Wirkungsgrad bei voller Last: 90%
- Steckertyp: IEC C13 – IEC C19
- Ausgangsfrequenz min.: 57Hz
- Verzerrung Ausgangsspannung: unter 5%
- Wellenform: Sinuswelle
- Leistungsabgabe: 3.000 Va
- Anschließbare Stiftstecker: 9
- Ausgangsspannung: 220V, 230V, 240V
- Ausgangsfrequenz max.: 63Hz



#### **4. BAUARBEITEN**

Die Zuschlagsfirma muss auch die mit der Realisierung der Anlage verbundenen Bauarbeiten realisieren, d.h. Lieferung und Einbau von geraden, nach oben verjüngenden und auskragenden Tragmasten für die Videokameras einschließlich Herstellung der zugehörigen Bodenplatten und Inspektionsschächte.

Die Bauarbeiten, die zum Anschluss an den Stromleitungen erforderlich sind, wie beispielsweise Straßen-Aushub von Verbindungen mit Lieferung und Verlegung von Wellenrohren sind aus der vorliegenden Ausschreibung ausgeschlossen.