



VERKEHRSKAMERASYSTEM IM ITS TESTFIELD MERZIG

Systembeschreibung und Datenschutz-
Mechanismen

Inhalt

1	Übersicht	2
2	Systemübersicht	2
2.1	Ablauf des automatisierten Verfahrens	3
2.2	Geräte-Übersicht	3
3	Komponenten.....	4
3.1	Whitelist Kamera	4
3.2	Whitelist Verarbeitungsrechner	4
3.3	Liveview	4
4	Schutz-Mechanismen	4
4.1	Speicherfristen personenbezogener Daten	4
4.2	Technische Schutzmaßnahmen	4
4.3	Organisatorische Schutzmaßnahmen	4
4.4	Zugangsbeschränkungen	5
4.5	Schutz-Mechanismen zum Liveview-Zugriff.....	5

1 Übersicht

Die Datenverarbeitung unbeteiligter Dritter kann wie folgt zusammengefasst werden:

- Ereignis
 - Ein Fahrzeug passiert den fest eingestellten Erfassungsbereich einer Kamera
- Kamera
 - Die Kamera generiert ein Bild auf dem das Fahrzeug und dessen Nummernschild erkennbar ist
 - Das Kennzeichen wird ausgelesen und an den Verarbeitungsrechner an der Kreuzung gesendet
 - Das generierte Bild wird auf der Kamera nach der Verarbeitung durch die Kamera nicht gespeichert und somit gelöscht
- Verarbeitungsrechner (im Kreuzungsbereich)
 - Das erfasste Kennzeichen wird dahingehend überprüft, ob es sich um ein Fahrzeug der FGVT oder um ein Fahrzeug eines unbeteiligten Verkehrsteilnehmers handelt
 - Im Falle eines unbeteiligten Verkehrsteilnehmers wird der allgemeine und anonyme Fahrzeugzähler erhöht und gewisse nicht personenbezogene Daten (z.B. Uhrzeit) des Ereignisses werden gespeichert
 - Im Falle eines unbeteiligten Verkehrsteilnehmers wird die Kennzeicheninformation durch den Verarbeitungsrechner nicht gespeichert und somit gelöscht

Eine weitere Verarbeitung, Speicherung oder Weiterleitung der Kennzeicheninformationen unbeteiligter Dritter findet nicht statt.

Kennzeicheninformationen unbeteiligter Dritter verlassen zu keinem Zeitpunkt den Kreuzungsbereich (genauer: die Kamera und den direkt im Kreuzungsbereich angeschlossene Verarbeitungsrechner).

Es sind keine Mechanismen verfügbar um besagte gelöschte Daten wiederherzustellen.

Eine detaillierte Beschreibung des Systems und der Verarbeitung von Daten von Mitgliedern und Fahrzeugen der Forschungsgruppe Verkehrstelematik (FGVT) und unbeteiligter Dritter Verkehrsteilnehmer findet sich in den folgenden Kapiteln.

2 Systemübersicht

Im ITS Testfield Merzig (ITeM) werden zur Validierung der ITS-Kommunikations- und Anwendungsszenarien Kamerasysteme im Kreuzungsbereich eingesetzt. Diese dienen einerseits der Erfassung der aktuellen Verkehrssituation durch anonyme Erfassung bzw. Zählung von Verkehrsteilnehmern mit Kennzeichen auf den Fahrspuren und andererseits der Erfassung und Identifikation von Testfahrzeugen der FGVT zur Validierung der Kommunikations- und Anwendungsszenarien. Eine Übersicht über den automatisierten Teil des Systems ist der folgenden Abbildung zu entnehmen (siehe Abbildung 1).

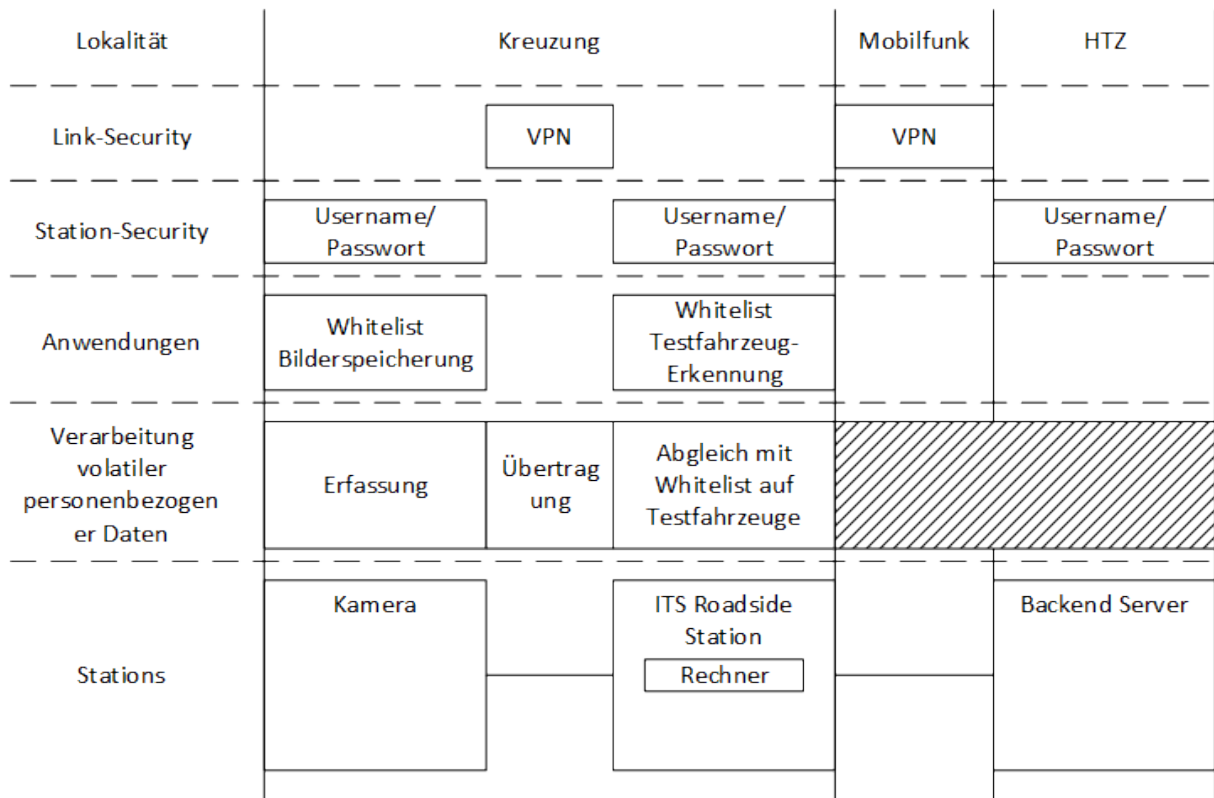


Abbildung 1: Systemübersicht des automatisierten Verfahrens

Kernelement eines Kreuzungsbereichs bildet die ITS Roadside Station (IRS), die neben ihrer Kommunikationskomponenten aus einem Verarbeitungsrechner besteht. Die Kameras sind auf den Ampelarmen montiert und in einem Ethernet-Netzwerk via Kabel an den Verarbeitungsrechner angeschlossen. Die IRS ihrerseits ist mittels Mobilfunk an das Server-Backend am Hochschul-Technologie-Zentrum (HTZ) in Saarbrücken angebunden.

2.1 Ablauf des automatisierten Verfahrens

Fährt ein Fahrzeug in den Erfassungsbereich der Kamera, wird dies durch die Erkennung eines Nummernschildes im Bildbereich der Kamera registriert. Die Kamera liest das Kennzeichen und sendet eine Nachricht mit der Kennzeicheninformation und Metadaten der Erfassung (z.B. Uhrzeit, Qualität der Erkennung, Koordinaten des Kennzeichens im Bildausschnitt) an den angeschlossenen Verarbeitungsrechner. Die Nachricht wird dort mit einer Whitelist, deren Einträge die Nummernschilder der Testfahrzeuge der FGVT enthalten, abgeglichen.

2.2 Geräte-Übersicht

- Kameras
 - Hersteller: MACQ (Belgien)
 - Typ-Bezeichnung: iCar
 - Betriebssystem: Linux
- Verarbeitungsrechner
 - Hersteller: Sintrones
 - Typ-Bezeichnung: VBOX-3110
 - Betriebssystem: Linux

3 Komponenten

3.1 Whitelist Kamera

Die Whitelist im Betriebssystem der Kamera wird zur Speicherung der Erfassungsbilder verwendet. Nur Bilder von Fahrzeugen, deren Kennzeichen einem Muster der Whitelist entsprechen, werden auf der Kamera gespeichert. Eine Anpassung der Whitelist ist nur durch direkten Zugriff auf das Kamerasystem möglich.

3.2 Whitelist Verarbeitungsrechner

Die Whitelist im Verarbeitungsrechner dient der Überprüfung auf Testfahrzeuge der FGVT.

- Bei einer Übereinstimmung wird die Information über das erkannte und identifizierte Testfahrzeug mitsamt der übermittelten Metadaten gespeichert.
- Stimmt das erkannte Kennzeichen nicht mit einem Eintrag auf der Whitelist überein, werden lediglich die Metadaten der Erfassung ohne die personenbezogenen Informationen (die Kennzeicheninformation) zum Zwecke einer anonymen Verkehrsteilnehmerzählung und Statistik gespeichert. In diesem Fall ist die personenbezogene Information ab diesem Zeitpunkt verloren.

Eine Anpassung der Whitelist ist nur durch direkten Zugriff auf das Kamerasystem möglich.

3.3 Liveview

Zur Konfiguration der Kamera und der Prüfung der korrekten Ausrichtung gibt es eine Liveview auf das aktuelle Kamerabild. Diese ist über eine Weboberfläche einsehbar.

4 Schutz-Mechanismen

4.1 Speicherfristen personenbezogener Daten

Die einzigen personenbezogenen Daten die vom automatisierten Verfahren erhoben werden, sind die Kennzeichenerfassungsinformationen. Diese werden nicht persistent gespeichert und liegen auf Anwendungsebene, nach deren Verarbeitung durch den Whitelist-Abgleich, nicht mehr vor. Mechanismen zur Wiederherstellung dieser Daten sind nicht integriert.

4.2 Technische Schutzmaßnahmen

Der Zugriff zum Kamerasystem, ebenso wie der Zugriff zum Verarbeitungsrechner, ist durch Benutzername und Passwort geschützt. Die Kommunikation der Daten von Kamera zum Verarbeitungsrechner erfolgt über ein VPN. Die Zugangsdaten sind einem verschlüsselten Passwortsafe innerhalb des FGVT Intranets gespeichert.

4.3 Organisatorische Schutzmaßnahmen

Da die persistente Speicherung von Bildern zum aktuellen Zeitpunkt weder technisch erforderlich noch datenschutzrechtlich geklärt ist, beinhaltet die Komponente Whitelist Kamera keine Einträge. Daher werden keine Bilder persistent gespeichert.

Der Zugriff auf die Testfeld-Systeme erfolgt nur durch oder unter Überwachung des Testfeld Supervisors oder dessen Stellvertreters. Das Masterpasswort zum entsprechenden Passwortsafe ist ebenfalls nur diesen beiden Personen bekannt und entspricht den Empfehlungen des BSI.

Der Zugang zu den Komponenten im Testfeld ist durch Schlösser gesichert. Die Schlüssel liegen in der Verantwortung des Testfeld Supervisors und dessen Stellvertreters.

4.4 Zugangsbeschränkungen

Der Direktzugriff auf die Kamerahardware wird durch Schlösser geschützt. Der Verarbeitungsrechner liegt im abgeschlossenen Steuergeräteschrank der jeweiligen Kreuzungsanlage. Der Zutritt zur IT-Infrastruktur, über welche die Anlagen erreicht werden, ist durch einen abgeschlossenen Gebäudeeingang (Zugang für Mitarbeiter des Hochschul-Technologie-Zentrums) und abgeschlossene Büroräume (Zugang für Mitarbeiter der Forschungsgruppe Verkehrstelematik) abgesichert.

4.5 Schutz-Mechanismen zum Liveview-Zugriff

Das Passwort für den Liveview-Zugriff ist lediglich dem Leiter der Forschungsgruppe bekannt. Testfeld Supervisor und Stellvertreter kennen jeweils eine Hälfte des Passwortes um überwachte Adaptionen an den Einstellungen der Kameras vornehmen zu können.