Lavori di realizzazione di un sistema integrato di videocontrollo territoriale costituito da un sottosistema di videosorveglianza delle zone interessate e uno di riconoscimento automatico delle targhe dei veicoli in transito.

Progetto Vi.So.Re. Trevigiano

Security Target

Sottosistema Lettura Targhe (SLT)

Versione 1.0

Riepilogo delle modifiche

N.	Versione	Stato	Data	Redatto	Approvato	Tipo di modifica
1	1.0	Rilasciato	21/11/2013	A.Mennini	A.Hummer	Prima Versione del documento
2	2.0	Rilasciato	28/02/2015	A.Mennini	A.Hummer	Ristrutturazione completa del documento
3	2.1	Rilasciato	14/03/2015	A.Mennini	A.Hummer	Revisione cap. 2 e cap. 7 per dare una visione più chiara e approfondita dell'ODV
4	2.2	Rilasciato	19/08/2015	A.Mennini	A.Hummer	Revisione a seguito ROA
5	2.3	Rilasciato	30/09/2015	A.Mennini	A.Hummer	Revisione finale

Tabella 1 - Revisioni del documento

Riferimento per l'amministrazione di stato e versione:
Stato:
Elaborato ("Processed") il documento è in corso di elaborazione
Rilasciato ("Released") il documento è stato verificato e rilasciato dal controllo qualità; può essere modificato solo se viene aggiornato il numero di versione.
Versioni:
Presentano due fasi. I documenti accettati ricevono il successivo numero intero di versione.
00-01, 00-02 ecc. versioni non rilasciate, con stato **"Elaborato"**
01 prima versione rilasciata con stato **"Rilasciato"**
01-01, 01-02 ecc. versioni che integrano la versione 01-00 e hanno stato **"Elaborato"**
02 seconda versione rilasciata con stato **"Rilasciato"**

Copyright

Sommario

Indice delle tabelle

Indice delle figure

1. PREMESSA

1.1 OBIETTIVI DEL DOCUMENTO

Questo Security Target (ST) descrive gli obiettivi di sicurezza, i requisiti e le motivazioni del "Sottosistema di Lettura Targhe (SLT) Versione 1.0" (ODV) del progetto Vi.So.Re. Trevigiano, progettato e realizzato dal RTI Kapsch TrafficCom s.r.l. con Infracom Italia S.p.A. (nel seguito anche semplicemente RTI). Il committente della valutazione è Kapsch TrafficCom s.r.l..

1.2 STRUTTURA DEL DOCUMENTO

Il Security Target è redatto in osservanza di quanto indicato nei CC Part.1 Version 3.1 Revision 4 relativamente ad un "Low Assurance Security Target" e contiene le seguenti sezioni:

- **Panoramica dell'ODV [Rif. § 2.3]:** questa sezione fornisce una visione di insieme dell'ODV e di come si colloca nell'ambito del progetto Vi.So.Re. Trevigiano.
- **Descrizione dell'ODV [Rif. § 2.34]:** questa sezione fornisce una descrizione dell'ODV, ne fornisce le caratteristiche e ne definisce l'ambito.
- **Dichiarazione di Conformità [Rif. § 3]:** questa sezione presenta le conformità con in CC.
- **Obiettivi di sicurezza [Rif. § 4]:** questa sezione descrive in maniera dettagliata gli obiettivi di sicurezza dell'ambiente operativo dell'ODV.
- **Definizione di Componenti Estese [Rif. § 5]:** Questa sezione definisce e giustifica l'utilizzo di componenti estese.
- **Requisiti di sicurezza [Rif. § 6]:** questa sezione definisce i Security Functional Requirements (SFR) ed i Security Assurance Requirements (SAR) per l'ODV.
- **Specifiche sommarie [Rif. § 7]:** questa sezione descrive le funzioni di sicurezza dell'ODV che soddisfano i requisiti di sicurezza.

1.3 ACRONIMI

ACL	Access Control List
CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
ODV	Oggetto Della Valutazione
PC	Personal Computer
PP	Protection Profile
RTI	RTI Kapsch TrafficCom s.r.l. con Infracom Italia S.p.A.
SAN	Storage Area Network
SAR	Security Assurance Requirement
SCE	Sistema Centrale di Elaborazione

SCNTT	Sistema Centralizzato Nazionale Targhe e Transiti
SD	Secure Digital
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SLT	Sottosistema di Lettura Targhe
SNV	Sottosistema Network Vi.So.Re.
ST	Security Target
SVC	Sottosistema Videosorveglianza Comunale
TOE	Target Of Evaluation
TSF	TOE Security Function
TSFI	TSF Interface

Tabella 2 – Acronimi

1.4 RIFERIMENTI

[RF1] Capitolato speciale di appalto Progetto Vi.So.Re Trevigiano

[RF2] Progetto Vi.So.Re Trevigiano Relazione tecnica

[RF3] Progetto esecutivo

[RF4] DL 196/2003 e successive modificazioni

[RF5] Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Gazzetta Ufficiale n. 99 del 29 aprile 2010)

2. INTRODUZIONE AL SECURITY TARGET (ASE_INT)

2.1 IDENTIFICAZIONE DEL SECURITY TARGET

Titolo: **Security Target Sottosistema SLT v. 2.3**

Data: **30/09/2015**

Autore: **Andrea Mennini**

2.2 IDENTIFICAZIONE DELL'ODV

Nome del prodotto: **Sottosistema Lettura Targhe SLT v.1.0 (nel seguito per brevità anche solo SLT)**

Sviluppatore: **Kapsch TrafficCom S.r.l.**

2.3 PANORAMICA DELL'ODV

L'ODV è un Sottosistema di Lettura Targhe operante lungo i principali nodi stradali nell'ambito di 12 comuni iniziali della provincia di Treviso e avente la finalità di effettuare la lettura delle targhe e rilevare l'immagine di contesto dei veicoli in transito così da consentire: la segnalazione del transito alle forze di Polizia dello Stato territoriali e al SCNTT. L'ODV costituisce una parte del più ampio Progetto Vi.So.Re. Trevigiano. L'ODV prevede un certo numero di telecamere installate presso i principali nodi stradali dei comuni interessati, collegate con posti di visualizzazione/controllo e il sistema centrale di elaborazione (SCE) mediante il sottosistema di comunicazione SNV. L'ODV garantisce la riservatezza dei dati mediante la profilazione degli utenti, impedendo ad utenti non autorizzati di accedere ai dati raccolti dalle telecamere ed acceduti tramite il sottosistema SNV dai siti di visualizzazione/controllo. Presso i siti di visualizzazione/controllo l'ODV permette agli utenti autorizzati, 24 ore su 24, un immediato accesso a SLT per la visualizzazione delle immagini acquisite dalle telecamere installate presso i siti identificati nei minimo 12 comuni iniziali interessati. L'ODV è un Sistema di lettura targhe costituito da un insieme omogeneo di componenti hardware e software che integrate tra di loro, e unitamente al proprio ambiente operativo, si prefiggono l'obiettivo di rispondere ai requisiti ed alle funzioni operative previste nel Capitolato Speciale di Appalto Progetto Vi.So.Re. Trevigiano [RF1].

AMBIENTE OPERATIVO PROGETTO VI.SO.RE. Trevigiano

Nella figura seguente viene presentato lo schema che mostra l'ambiente operativo complessivo del progetto Vi.So.Re. Trevigiano all'interno del quale l'ODV agisce. In particolare si identificano i tre diversi sottosistemi che costituiscono il progetto Vi.So.Re Trevigiano:

- Il sottosistema SLT, qui descritto dedicato alla lettura delle targhe
- Il sottosistema SVC, dedicato alla Videosorveglianza Comunale;
- Il sottosistema SNV, adibito all'infrastruttura dedicata di collegamento che garantisce la cifratura e la separazione dei flussi dati in transito tra tutti i sistemi periferici e quelli centrali.

Il sottosistema SNV garantisce il collegamento sicuro tra le diverse componenti dell'ODV.

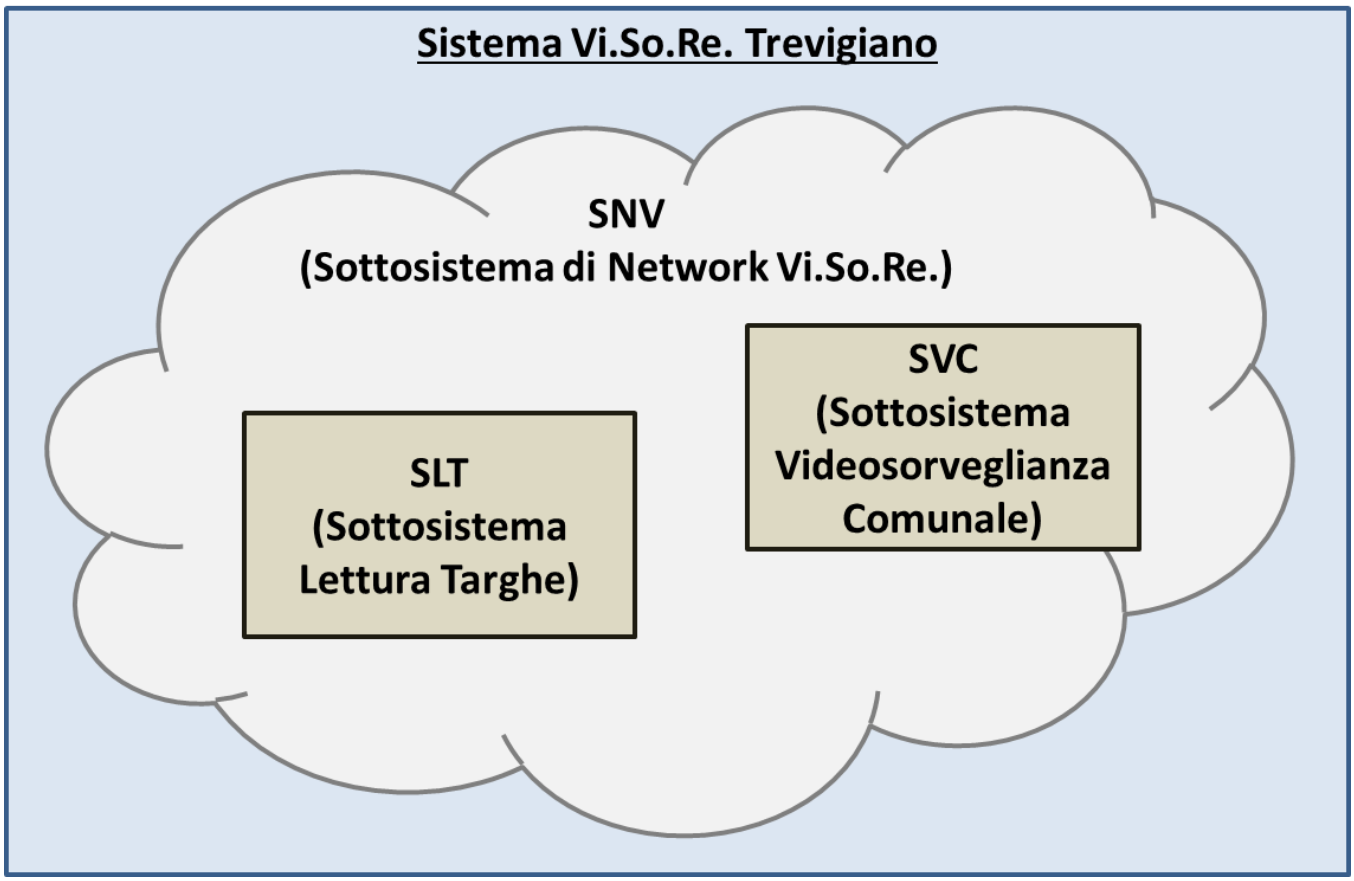

Figura 1 - Ambito Progetto Vi.So.Re

2.4 DESCRIZIONE DELL'ODV

Gli obiettivi del SLT sono quelli di effettuare la lettura automatica delle targhe e rilevare l'immagine di contesto dei veicoli in transito lungo i principali nodi stradali delle zone interessate per consentire la segnalazione del transito dei veicoli al SCNTT, in particolare:

- invio al SCNTT della foto in B/N della targa e dei metadati collegati (numero targa, data e ora, etc.) di tutti i mezzi in transito,
- invio al SCNTT per le targhe appartenenti alle categorie:
  - A1 (lista veicoli privi di assicurazione)
  - A2 (lista veicoli privi di revisione)
  - C (lista veicoli segnalati per furto ed altro),

  oltre alle informazioni di cui al primo punto anche della foto a colori del veicolo.

2.4.1 AMBITO FISICO

Il SLT si articola in quattro componenti principali di cui le prime due costituiscono l'ambito dell'ODV, il sottosistema SNV rientra nell'ambiente operativo, mentre i Sistemi Esterni sono interfacciati dall'ODV ma non fanno parte dell'ambiente operativo:

- **Sistemi su strada**
  Dispositivi, appositamente progettati, che integrano due telecamere per la rilevazione e lettura targhe e la rilevazione dell'immagine di contesto associata alla targa (foto del veicolo), in grado di analizzare, processare e inviare in tempo reale le informazioni rilevate (immagine di contesto a colori, immagine B/N della targa e relativi metadati). Questi dispositivi integrano al loro interno una memoria SD che viene utilizzata in caso di assenza di collegamento per la memorizzazione cifrata AES128 temporanea delle informazioni rilevate (immagine di contesto a colori, immagine B/N della targa e relativi metadati).
- **Sistema centrale di elaborazione**
  Tutti i moduli applicativi del SLT installati presso la Stazione centrale di controllo della Questura di Treviso ospitato in ambiente protetto.
- **Sottosistema SNV** per la comunicazione tra i Sistemi su Strada, il sistema centrale di elaborazione e il SCNTT.
- **Sistemi Esterni e infrastrutture hardware d'ambiente**
  Client operazionali installati presso le Stazioni Operative degli organi di Polizia; server centrali ospitanti il sistema centrale di elaborazione; SCNTT.

La figura seguente illustra lo schema logico complessivo del sottosistema.

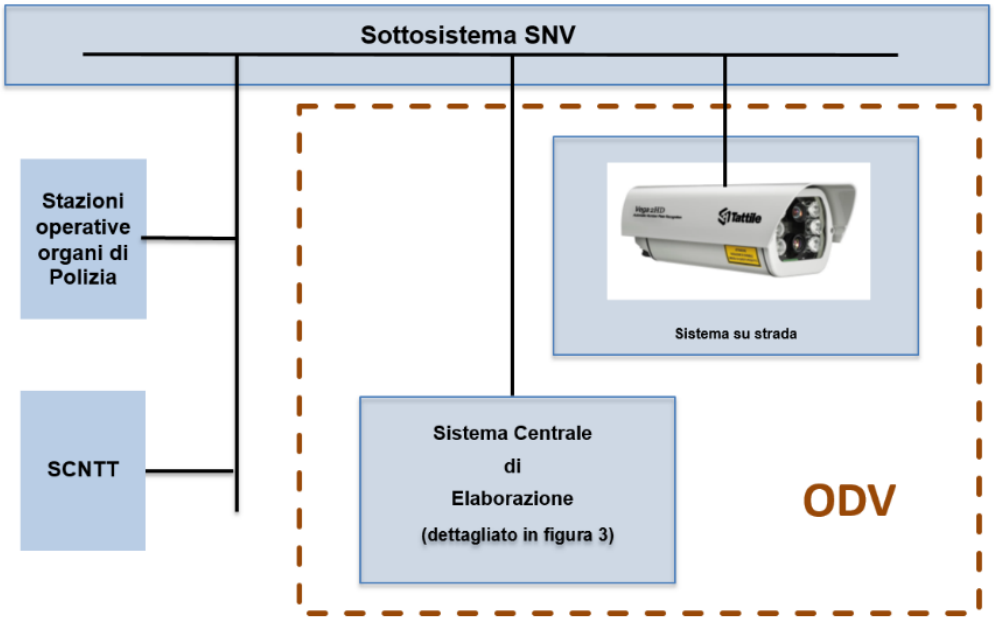

Figura 2 – Schema logico sottosistema SLT

2.4.1.1 Componenti dell'ODV

Sistema su strada, si compone delle seguenti componenti:

Numero iniziale di 79 Telecamere Tattile Vega 2HD - TOS, con le seguenti caratteristiche tecniche:

- Acquisizione (frames al secondo) 75
- Camera di contesto a colori
- Massima velocità dei veicoli 250 km/h
- Camera di lettura targhe Sensore CMOS 2560x2048 @ 75 fps
- Camera di contesto Sensore CMOS 2560x2048
- una scheda SD interna non direttamente accessibile per la conservazione delle immagini in caso di attività in modalità stand alone;
- Illuminatore IR 6 LED IR, alta potenza, 850 nm
- Ottiche Obiettivo attacco C
- Ingressi digitali 1 ingresso optoisolato
- Uscite digitali 1 uscita relè 1 uscita strobe
- Ethernet 10/100 Mbps
- Porta seriale RS485
- Distanza varco Distanza: da 12 fino a 25m
- Larghezza varco: fino a 7.5m
- Temperatura operativa da -20 °C a +55 °C
- Grado di protezione IP IP66

- Alimentazione 24 VDC +/- 10%, 16 W

Ogni sistema su strada è dotato di specifico software integrato con le seguenti caratteristiche:

- Componente elaborativa locale dell'immagine B/N della targa dedicata all'OCR della stessa;
- Componente elaborativa locale per le funzioni di hash (SHA1), cifratura (AES 128) e firma (DSA);
- Configurazione e monitoraggio da browser Web

Sistema Centrale di Elaborazione (**SCE**) dell'ODV si compone dei seguenti moduli software applicativi:

- **Modulo CPS**

  Il modulo CPS è un concentratore dei dati di transito e diagnostica provenienti dalle telecamere del sistema. L'architettura è modulare e sono previsti una serie di moduli CPS ognuno dei quali concentra i dati di un gruppo di telecamere. Ciò rende il sistema facilmente scalabile aggiungendo telecamere e moduli CPS opportunamente dimensionati per garantire un parallelismo di acquisizione dati sufficiente a gestire la mole di dati raccolta dal sistema. Il modulo CPS è realizzato in linguaggio C++ e fa uso delle librerie Chilkat.
- **Modulo DBINSERT**

  Questo modulo si occupa della effettiva memorizzazione sul database centrale dei dati di transito acquisiti dai moduli CPS. Possono essere presenti più moduli DBInsert in modo da garantire un parallelismo del flusso dati verso il database centrale sufficiente a gestire la mole di dati in ingresso.
- **Modulo – CORE GESTIONALE**

  Questo modulo rappresenta il core dell'applicazione web centrale, realizzata in tecnologia Java EE e installata presso la Stazione di Controllo (sala apparati) della Questura di Treviso.
- **Modulo – CLIENT OPERAZIONALE**

  Anche questo modulo fa parte dell'applicazione web centrale, realizzata in tecnologia Java EE e installata presso la Stazione di Controllo (sala apparati) della Questura di Treviso, e ne rappresenta, la parte utilizzata dagli utenti appartenenti ai ruoli: **Amministratore** e **Operatore**.
- **Modulo – SUPERVISORE**

  Anche questo modulo fa parte dell'applicazione web centrale, realizzata in tecnologia Java EE e installata presso la Stazione di Controllo (sala apparati) della Questura di Treviso, e ne rappresenta la parte utilizzata dagli utenti appartenenti al ruolo **Super-utente**
- **Modulo – CONFIGURATORE**

  Anche questo modulo fa parte dell'applicazione web centrale, realizzata in tecnologia Java EE e installata presso la Stazione di Controllo (sala apparati) della Questura di Treviso, e ne rappresenta la parte direttamente utilizzata dagli utenti appartenenti ai ruoli: **Amministratore** e **Manutentore**.
- **Modulo - INTERFACCIA CON SCNTT**

  Questo modulo è anch'esso realizzato in tecnologia Java EE e risiede presso la Stazione di Controllo (sala apparati) della Questura di Treviso, ma non fa parte dell'applicazione web centrale: costituisce

invece un'applicazione separata funzionante in modalità batch e senza interazioni con gli operatori umani.

2.4.1.2 Ambiente operativo dell'ODV

L'ambiente operativo dell'ODV si compone di due parti principali:

Sottosistema SNV, che garantisce le comunicazioni sicure tra le varie componenti (Sistemi su Strada, il sistema centrale di elaborazione e il SCNTT) mediante VPN dedicate al SLT e la separazione dei flussi dati dal SVC.

Infrastruttura hardware d'ambiente, così composta:

- **RDBMS:** Oracle 11g R2; all'interno del database sono archiviati i dati storici, statistici, e configurazioni di sistema.
- **Servers** N. 2 host fisici ospitanti la piattaforma di virtualizzazione VMWARE su cui sono resi operativi 5 server virtuali. L'architettura adottata è completamente ridondata e, pertanto, configurata in alta affidabilità a garanzia della continuità di servizio.
- **SAN** Storage Area network di tipo Enterprise connessa ai server in modalità Fibre Channel opportunamente dimensionata per accogliere le immagini ed i dati previsti ed in grado di supportare ampiamente il throughput richiesto.
- **Switch** L'interconnessione tra server ed i dispositivi di rete e sicurezza è garantita da una coppia di switch Cisco 10/100/1000 (o equivalenti) in alta affidabilità.
- **Client** PC con sistema operativo Windows 7 professional 64bit, con doppia uscita video, monitor dedicato da 21'' e joystick proporzionale a 3 assi, di Monitor/TV 42'' e di Ups di potenza adeguata 30 minuti, situate nelle sale dei comandi di Polizia preposti a tale scopo.

2.4.1.3 Flusso generale dell'ODV e del suo ambiente operativo

Nel seguito del presente paragrafo vengono illustrati i due flussi principali: quello relativo alle immagini ed informazioni correlate e quello relativo all'accesso al SLT da parte degli utenti dello stesso.

Flusso operativo delle immagini e delle informazioni correlate.

Il flusso operativo relativo all'acquisizione delle immagini parte dai sistemi su strada: dispositivi di acquisizione delle immagini (foto) composti da un unico apparato Vega 2HD al cui interno sono assemblate le diverse componenti già descritte al paragrafo precedente.

All'interno dei sistemi su strada sulle foto acquisite in formato RAW al passaggio di un veicolo vengono svolte le seguenti elaborazioni locali:

- elaborazione dell'immagine B/N della targa e di quella a colori del veicolo per la creazione dei relativi file in formato standard JPEG;
- elaborazione OCR dell'immagine B/N della targa per il riconoscimento dei caratteri alfanumerici componenti la stessa;
- valorizzazione dei metadati dei due file JPEG (targa e contesto) con le informazioni di transito (data, ora, targa, id della telecamera, etc.);
- Creazione di un messaggio unico contenente entrambi i file identificati dai relativi header
- Invio dal sistema su strada alla componente server CPS del CSE del messaggio unico mediante l'apertura di una socket, con protocollo di comunicazione di tipo proprietario, mediante SNV (SNV garantisce la sicurezza delle comunicazioni e la separazione dai flussi rispetto a SVC).
- In assenza di collegamento di rete il messaggio unico viene memorizzato nella memoria SD locale, per essere poi trasmesso, alla riconnessione, con la modalità sopra indicata in maniera completamente trasparente all'utente e senza che l'utente possa avere accesso in alcun modo alla memoria SD.

Tutte le elaborazioni interne sopra descritte avvengono nella memoria RAM del sistema su strada.

Il modulo CPS, ricevuto il messaggio unico dal client sistema su strada:

- effettua la post elaborazione consistente nella applicazione di ulteriori e più sofisticati algoritmi sulle immagini tra cui: OCR di secondo livello, algoritmo MMR per l'analisi del colore, algoritmo di classificazione, algoritmo di ricerca del modello di veicolo, ed altri;
- Terminata questa post elaborazione richiama il Modulo DBInsert per la memorizzazione delle informazioni nel data base.

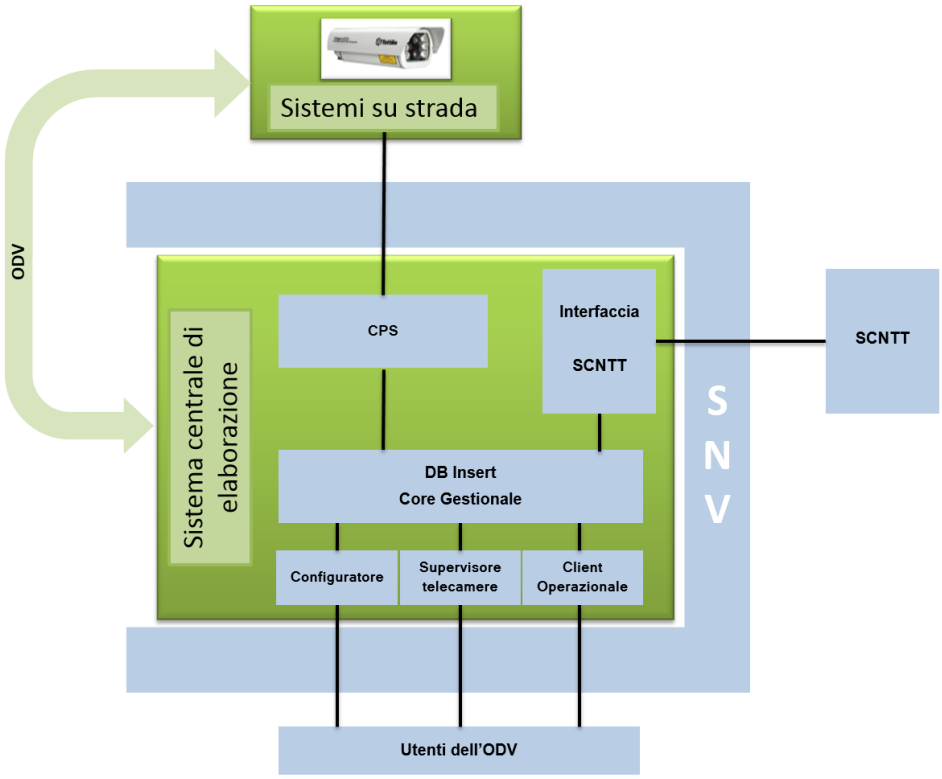

Figura 3 - Architettura complessiva

Il modulo DBInsert estrae le informazioni dai metadati dei file JPEG, a cui aggiunge le altre informazioni ottenute dal processo di post elaborazione, e inserisce il tutto unitamente alle due immagini JPEG all'interno del database ORACLE.

Il modulo Core Gestionale SLT svolge le operazioni di:

- verifica della presenza in tempo reale, nelle liste generali (A1, A2 e C) e locali, della targa rilevata nel transito.
- per ogni transito dialoga con il modulo di interfacciamento SCNTT per la spedizione delle immagini B/N della targa tramite SNV al SCNTT.
- nel caso in cui la targa rilevata risulti presente in una lista qualsiasi, genera un allarme del tipo corrispondente.
- in caso di allarme generato da corrispondenza trovata nelle liste generali dialoga con il modulo di interfacciamento SCNTT per la spedizione dell'immagine a colori del transito corrispondente tramite SNV al SCNTT.
- storicizza l'allarme nel database ORACLE
- allo scadere dei periodi di conservazione di 15 giorni e di 90 giorni per i veicoli di Lista C (comunque configurabili) nel database Oracle, le registrazioni dei transiti e degli allarmi vengono cancellate.

Flusso operativo relativo all'accesso degli utenti dell'ODV

Gli utenti dell'ODV afferenti ai ruoli di seguito indicati accedono all'ODV tramite interfaccia web; successivamente all'identificazione dell'utente, vengono assegnati il ruolo e le corrispondenti autorizzazioni e di conseguenza vengono abilitati i moduli Client autorizzati. I possibili moduli sono: Operazionale, Supervisore telecamere e Configuratore, questi garantiscono l'accesso alle rispettive attività connesse al ruolo specifico. Le operazioni riguardanti la gestione degli Utenti/Ruoli ed il trattamento delle telecamere/immagini comportano la scrittura nel file di log dell'operazione eseguita. L'utente dell'ODV per collegarsi allo stesso deve connettersi al SNV che garantisce il collegamento di tipo sicuro. L'interfaccia per gli utenti dell'ODV è di tipo WEB.

Ogni utente per accedere alle funzionalità del sistema deve prima superare la procedura di identificazione ed autenticazione di SLT che richiede nome utente e password. Al primo login l'utente è obbligato a cambiare password, poiché alla generazione dell'utente viene acceso un flag che avvisa di cambiare password al login. Ad ogni utente quindi viene assegnata una password di primo collegamento, che deve essere obbligatoriamente cambiata impostandone una propria con le seguenti caratteristiche minime:

a. la lunghezza minima della password deve essere composta da almeno 8 caratteri;
b. i caratteri contenuti nella password devono contenere almeno una cifra numerica, almeno un carattere speciale (ad esempio !, @, #, $), e sia lettere minuscole che maiuscole;
c. ogni password deve essere cambiata obbligatoriamente dopo 3 mesi;
d. ogni account scade dopo 6 mesi di inutilizzo.

2.4.2 AMBITO LOGICO

Il software SLT è sviluppato su piattaforma aperta e progettata per progetti su larga scala. Grazie agli applicativi client fornisce agli operatori tramite mappe grafiche interattive e di tipo multi livello, un eccezionale sistema di controllo panoramico per tutto l'impianto. L'ODV include un efficiente metodo d'amministrazione centralizzata, procedure guidate intuitive, flessibili regole di funzionamento del sistema. Queste caratteristiche permettono di gestire con facilità la personalizzazione di un impianto di lettura targhe pur se geograficamente esteso.

In particolare da un punto di vista della sicurezza l'ODV:

- consente una gestione selettiva delle immagini e delle telecamere dando agli amministratori la possibilità di configurare l'accesso alle funzioni, alle telecamere ed ai dati delle targhe in base al ruolo di ciascun utente.
- genera log relativi alle operazioni sulle telecamere e sugli utenti
- rende disponibili le immagini raccolte dalle telecamere anche nel caso di interruzione dei collegamenti,

- memorizza le immagini raccolte dalle telecamere, la loro visualizzazione, la loro conservazione e la loro eventuale esportazione per prove giuridiche.

Altre funzioni del sottosistema SLT, proprie dell'ambiente operativo e descritte nel successivo par. 4, concorrono al raggiungimento degli obiettivi prefissati.

2.5 CONFINI

Come si vede dalla figura 3, l'ODV si interfaccia con il sottosistema SNV, che realizza i collegamenti con i sistemi su strada, con gli utenti e con il SCNTT.

In base a quanto descritto nel precedente par. 2.4 e relativi sottoparagrafi, si evince che:

- **il confine fisico dell'ODV è rappresentato dal sottosistema SNV, con la precisazione che il sottosistema SNV fa parte dell'ambiente operativo (v. par. 2.4.1.3)**.
- **il confine logico dell'ODV è rappresentato dalle funzioni descritte nel successivo par. 2.7.**

2.6 RUOLI UTENTE

SLT gestisce i seguenti ruoli utente:

- Amministratore
- Super-utente
- Operatore
- Manutentore

Gli utenti del sistema hanno accesso all'interfaccia web degli specifici moduli SCE (rif. Figura 3 - Architettura complessiva).

Ogni utente è caratterizzato da uno e un solo profilo:

Amministratore: è il gestore dell'applicazione, e come tale controlla il corretto funzionamento dei moduli creando le aree geografiche e i super-utenti; ha accesso soltanto alla parte di interfaccia del modulo "Configuratore". Questi utenti avranno i diritti (configurabili) per accedere ed usufruire delle seguenti funzionalità dell'ODV:

- Inserimento, modifica, disabilitazione delle utenze del sistema, gestione di gruppi e ruoli assegnati ad ogni utente.
- Configurazione di allarmi, azioni applicabili a seguito di allarmi, priorità di intervento per ogni allarme
- Gestione soglie di allarme sui flussi di traffico
- Configurazione dei tempi di conservazione dei dati

- Configurazione parametri dell'intero sistema e parametri di connessione per l'integrazione verso SCNTT

Super-utente: viene definito come gestore dei dati legati a una o più aree geografiche, ha accesso soltanto alla parte di interfaccia del modulo "Configuratore", limitatamente alla gestione dei dati legati alle aree geografiche e gruppi di Utenti di sua competenza. Questi utenti avranno i diritti (configurabili) per accedere ed usufruire delle seguenti funzionalità dell'ODV:

- Gestione delle aree geografiche (Provincie, Dipartimenti, comuni, Sottoaree comunali) Anagrafica (georeferenziata) dei varchi e corsie di ubicazione apparati di campo.
- Connessioni logiche tra gruppi di utenti, aree geografiche e varchi, per la gestione settorializzata di transiti, allarmi, priorità di intervento, etc. per ogni Sede Operativa
- Gestione delle liste targhe (white list, hot list locali, targhe merci pericolose) con interazione eventuale con liste di SCNTT

Manutentore: gestisce gli allarmi derivanti dai malfunzionamenti degli apparati coordinando gli interventi di riparazione, è responsabile di una o più aree e ha accesso soltanto alla parte di interfaccia del modulo "Supervisore";

Operatore: ha accesso soltanto alla parte di interfaccia del modulo "Client Operazionale". Gli utenti del sistema utilizzatori del "Client Operazionale SLT" saranno gli Operatori delle Stazioni Operative (Sale Operative) con diverse competenze territoriali. Questi utenti avranno i diritti (configurabili) per accedere ed usufruire delle seguenti funzionalità dell'ODV:

- Gestione delle liste targhe locali di competenza
- Visualizzazione degli allarmi del sistema (Apparati di campo di competenza)
- Visualizzazione dei transiti con gestione evidente (colori differenti) delle differenti tipologie di allarmi transito con possibilità di annotazione testuale su specifica segnalazione
- Avvertimento in tempo reale di allarmi su transiti segnalati su liste
- Avvertimento in tempo reale di allarmi su apparati di campo
- Visualizzazione cartografica interattiva georeferenziata di:
  - o Liste transiti
  - o Ricerca transiti per targa, intervallo date, etc..
  - o Elementi periferici di campo ed eventuali allarmi di malfunzionamento
  - o Successione cronologica dei transiti di una targa
- Azioni verso SCNTT:
  - o Inserimento targhe da segnalare in lista C
  - o Ricerche su transiti
  - o Prelievo dati ai fini giudiziari ed investigativi, previa autorizzazione
- Visualizzazione ed export di dati statistici, contatori, e report.

2.7 FUNZIONI DI SICUREZZA DELL'ODV

La tabella seguente fornisce una sintetica descrizione delle funzioni di sicurezza dell'ODV.

Codice	Funzione di sicurezza	Descrizione
ODV_IDAU	**Autenticazione utenti**	L'ODV deve provvedere alla identificazione ed autenticazione degli utenti, mediante funzioni di: • controllo userid e password • controllo della composizione delle password • controllo di validità • controllo di prima autenticazione • controllo del numero dei tentativi di autenticazione.
ODV_AC	**Access control**	L'ODV consente agli amministratori di configurare l'accesso alle funzioni dell'ODV stesso ed ai dati in base al ruolo di ciascun utente.
ODV_AUD	**Auditing**	L'ODV genera log relativi agli accessi degli utenti alle funzioni dell'ODV, sia ai tentativi positivi sia a quelli falliti (operazioni di autenticazione). L'ODV genera log relativi alla gestione delle immagini inviate dalla telecamere.
ODV_MGMT	**Gestione**	L'ODV provvede al controllo delle seguenti operazioni: a) Operazioni su ruoli e utenti b) Operazioni sulle telecamere ed all'assegnazione di un riferimento temporale affidabile per ciascuna delle operazioni suddette.
ODV_DP	**Data Protection**	L'ODV garantisce la disponibilità delle immagini anche in caso di interruzione dei collegamenti fra telecamere e Sistema Centralizzato di Controllo, mediante il salvataggio delle stesse nella memoria SD delle telecamere. L'ODV provvede alla cancellazione delle immagini registrate dopo il periodo di tempo stabilito dalle politiche di accesso, nel rispetto della privacy.

Tabella 3 – Funzioni di sicurezza dell'ODV

3. DICHIARAZIONE DI CONFORMITA' (ASE_CCL)

Il ST e il ODV sono conformi alla versione 3.1 (Revision 4) of the Common Criteria for Information Technology Security Evaluation.

La dichiarazione di conformità si riferisce a:

Common Criteria for Information Technology Security Evaluation. Version 3.1 Rev.4 Part 1 september 2012

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012

Il pacchetto di garanzia dichiarato è EAL1.

Questo ST non dichiara la conformità ad alcun Protection Profile.

4. OBIETTIVI DI SICUREZZA (ASE_OBJ)

In linea con quanto previsto dal livello di garanzia EAL1, il paragrafo contiene definizioni concise degli obiettivi che devono essere soddisfatti dall'ambiente a supporto dell'ODV.

4.1. OBIETTIVI DI SICUREZZA PER L'AMBIENTE OPERATIVO

Obiettivo	Descrizione
OE.Admin	Gli Amministratori dell'ODV devono essere scelti tra il personale fidato e addestrati al corretto utilizzo dell'ODV.
OE.Physical	I responsabili del sottosistema SLT devono assicurare che l'infrastruttura tecnologica dell'ODV sia custodita in locali nei quali l'accesso è consentito solamente al personale autorizzato.
OE.External	I responsabili del sottosistema SLT devono assicurare la protezione e sorveglianza agli apparati posti all'esterno.
OE.Crypto	I sistemi su strada devono provvedere alla cifratura delle immagini raccolte dalle telecamere e non immediatamente trasmesse al Sistema Centralizzato di Controllo, con l'obiettivo di preservarne la riservatezza.
OE.Network	Il sottosistema SNV ha il compito di assicurare la connettività fra le seguenti componenti l'ODV: • Sistema Centrale di Elaborazione; • Telecamere; • Utenti dell'ODV Il sottosistema SNV deve proteggere la trasmissione dei dati raccolti dalle telecamere realizzando canali cifrati e separati in base alla destinazione dei dati stessi.
OE.Policy	L'Organizzazione deve assicurare, per quanto di competenza, la conformità alle leggi e normative in vigore sulla privacy.
OE.Time	L'ambiente operativo dell'ODV deve fornire riferimenti temporali affidabili per le operazioni sotto il controllo dell'ODV.

Tabella 4 - Obiettivi di sicurezza per l'ambiente

5. DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD)

Questo ST esclude la definizione di componenti estese.

6. REQUISITI DI SICUREZZA (ASE_REQ)

6.1. GENERALITA'

Questa sezione definisce i requisiti di sicurezza e di garanzia soddisfatti dal ODV.

Ogni requisito è stato estratto dai Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012 e dai Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012.

6.2. CONVENZIONI

Assegnazione L'operazione di assegnazione consente di specificare un parametro all'interno di un requisito. Le assegnazioni sono indicate usando un testo in grassetto all'interno di parentesi quadre **[assegnazione]**.

Selezione L'operazione di selezione permette di selezionare uno o più elementi da una lista. Le selezioni sono indicate usando testo in corsivo all'interno di parentesi quadre **[***selezione***]**.

Raffinamento L'operazione di raffinamento consiste nel dare un ulteriore dettaglio a un requisito. Le operazioni di raffinamento sono indicate usando un testo in grassetto per le aggiunte e barrando il testo da cancellare.

Iterazione L'operazione di iterazione permette di utilizzare più di una volta un componente per effettuare operazioni diverse. Una iterazione si effettua ponendo uno slash "/" alla fine del componente seguito da un unico nome che identifica l'iterazione.

6.3. REQUISITI FUNZIONALI DI SICUREZZA

Functional Requirements		
Classes	**Families**	**Description**
FAU:Security Audit	FAU_GEN.1	Audit data generation
FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_RIP.1	Subset residual information protection
FIA: Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication

Functional Requirements		
	FIA_SOS.1	Verification of secrets
	FIA_UID.2	User identification before any action
FMT: Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_MTD.1	Management of TSF data
	FMT_SMR.1	Security roles
FRU: Resources utilization	FRU_FLT.1	Degraded fault tolerance

Tabella 5 – Requisiti Funzionali di Sicurezza dell'ODV

6.4. DETTAGLIO DEI REQUISITI FUNZIONALI

FAU_GEN.1	
Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: 1. Start-up and shutdown of the audit functions; 2. All auditable events for the [*not specified*] level of audit; and 3. **[The following auditable events:** **a) Modifiche nelle assegnazioni di utenti ai ruoli previsti (funzione del ruolo amministratore)** **b) User login/logout e tentativi falliti di login** **c) Gestione delle immagini: registrazione, invio al SCNTT, cancellazione** **d) Gestione delle telecamere: attivazione, disattivazione** **]**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

FAU_GEN.1	
	b) For each audit event type, based on the auditable event definitions of the functional components included in the ST **[none]**.
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	

FDP_ACC.1	
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**SLT access control SFP**] on [**Soggetti:** **a) Utenti** **b) Sistemi su strada** **Oggetti:** **a) Immagini di transito** **b) Veicoli** **Operazioni:** **a) Gestione immagini**]
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	Le operazioni sopra indicate sono raggruppate per tipologia. Le stesse vengono dettagliate nella Tabella 6 “Componenti di controllo accessi”.

FDP_ACF.1	
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**SLT access control SFP**] to objects based on the following: [**Attributi dei soggetti:** **Ruolo (per gli utenti): amministratore, super-utente, manutentore, operatore** **ID (per i sistemi su strada)** **Attributi degli oggetti:** **a) Varco (Immagini)** **b) Tempo di conservazione (Immagini)** **c) Targa (Veicoli)**]

FDP_ACF.1	
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**La tabella 6 "Componenti di controllo accessi" stabilisce la relazione fra soggetti, oggetti e operazioni**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	

COMPONENTI DI CONTROLLO ACCESSI La tabella sottostante definisce soggetti, oggetti, operazioni e attributi, come regolati dalla SLT Access Control SFP.				
SOGGETTI	**ATTRIBUTI**	**OGGETTI**	**ATTRIBUTI**	**OPERAZIONI**
Sistemi su strada	ID	Immagini di transito	Varco	Il sistema su strada provvede alla creazione del messaggio per SCE e all'invio alla componente server CPS del CSE. In assenza di collegamento di rete il messaggio viene memorizzato nella memoria SD locale, per essere poi trasmesso, alla riconnessione, con la modalità sopra indicata.
Utenti	Amministratore	Immagini di transito	Tempo di conservazione	L'utente amministratore può modificare il tempo di conservazione dei dati di transito nel SCE L'utente amministratore ha la possibilità di gestire

COMPONENTI DI CONTROLLO ACCESSI La tabella sottostante definisce soggetti, oggetti, operazioni e attributi, come regolati dalla SLT Access Control SFP.				
SOGGETTI	**ATTRIBUTI**	**OGGETTI**	**ATTRIBUTI**	**OPERAZIONI**
				l'associazione fra i varchi e gli operatori
Utenti	Superutente			Operazioni non gestite dalle TSF
Utenti	Operatore	Veicolo	Targa	L'utente operatore ha la possibilità di vedere le immagini provenienti dai sistemi su strada, in base alla assegnazione dei varchi
Utenti	Manutentore			Operazioni non gestite dalle TSF

Tabella 6 - Componenti di Controllo Accessi

FDP_ETC.1	
Hierarchical to:	No other components.
FDP_ETC.1.1	The TSF shall enforce the [**SLT access control SFP**] when exporting user data, controlled under the SFP, outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
Notes:	L'ODV provvede ad inviare le immagini in chiaro al SCNTT

FDP_RIP.1	
Hierarchical to:	No other components.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource*

FDP_RIP.1	
	from] the following objects: **[immagini conservate nel Sistema Centrale di Elaborazione**].
Dependencies:	No dependencies
Notes:	Tutte le immagini memorizzate nel Sistema Centrale di Elaborazione vengono cancellate dopo un periodo di tempo di 15 giorni per i transiti e di 90 giorni per gli allarmi.

FIA_AFL.1	
Hierarchical to:	No other components
FIA_AFL.1.1	The TSF shall detect when [**5**], unsuccessful authentication attempts occur related to [**autenticazione dell'utente**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**bloccare l'utente**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	Notes:

FIA_ATD.1	
Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a) User ID** **b) Password** **c) Ruolo** **d) Stato (bloccato, abilitato ad operare)** **].**
Dependencies:	No dependencies
Notes:	

FIA_UAU.1	
Hierarchical to:	No other components
FIA_UAU.1.1	The TSF shall allow [**il cambio della password al primo accesso di un utente**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	Ad ogni nuovo utente viene assegnata una password di default, con l'obbligo di cambiarla al primo accesso al sistema secondo le regole stabilite in FIA_SOS.1.

FIA_UID.2	
Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies
Notes:	

FIA_SOS.1	
Hierarchical to:	No other components
FIA_SOS.1.1	TSF shall provide a mechanism to verify that secrets meet [**la password:** • **deve avere la lunghezza minima di almeno 8 caratteri;** • **i caratteri devono contenere almeno una cifra numerica, almeno un carattere speciale (ad esempio !, @, #, $), e sia lettere minuscole che maiuscole;** • **deve essere cambiata obbligatoriamente dopo 3 mesi;**]
Dependencies:	No dependencies
Notes:	

FMT_MSA.1	
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**SLT access control SFP**], to restrict the ability to *[modify*] the security attributes [**ruoli, tempo di conservazione delle immagini di transito**] to [**amministratore**].
Dependencies:	[FDP_ACC.1 Subset access control, or

FMT_MSA.1	
	FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	

FMT_MSA.3	
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**SLT access control SFP]** to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**amministratore**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	Le regole di conservazione delle immagini di transito prevedono che il loro tempo di conservazione abbia un valore di default che stabilisce a 15 giorni la durata di conservazione.Il “tempo di conservazione” è stato dichiarato come attributo ed il valore imposto è di tipo restrittivo.

FMT_MTD.1	
Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [*unlock*] the [**stato**] to [**amministratore**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Function
Notes:	

FMT_SMF.1	
Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [

FMT_SMF.1	
	a) Inserimento, modifica, disabilitazione delle utenze del sistema, gestione dei ruoli assegnati ad ogni utente, riattivazione di utenti disabilitati **b) Modifica del tempo di conservazione dei dati di transito**].
Dependencies:	No dependencies
Notes:	Tutte le funzioni di gestione vengono realizzate tramite le interfacce fornite dal modulo "Configuratore". L'inserimento di nuovi utenti comprende anche l'assegnazione di userid e password di default.

FMT_SMR.1	
Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**a) Amministratore** **b) Superutente** **c) Operatore** **d) Manutentore**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	

FRU_FLT.1	
Hierarchical to:	No other components.
FRU_FLT.1.1	The TSF shall ensure the operation of [**salvataggio delle immagini raccolte dalle telecamere**] when the following failures occur: [**interruzione della trasmissione delle immagini dalle telecamere al Sistema Centrale di Elaborazione**].
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
Notes:	In caso di interruzione del collegamento fra le telecamere ed il Sistema Centrale di Elaborazione, le telecamere hanno la capacità di trattenere le immagini nella propria memoria SD, fino al ripristino del collegamento.

6.5. REQUISITI DI GARANZIA

I requisiti di garanzia per il ODV sono quelli previsti al livello EAL1, come specificato nella Parte 3 dei Common Criteria, senza potenziamenti.

EAL1 è stato scelto come livello di garanzia in quanto il ODV opererà in un ambiente protetto, con amministratori competenti e con utenti specializzati e fidati. In questo contesto si assume che eventuali attaccanti avranno un potenziale di attacco limitato, di conseguenza il livello EAL1 è appropriato per fornire la garanzia necessaria a contrastare attacchi a limitato potenziale.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1Labelling of the TOE
	ALC_CMS.1TOE CM coverage
ATE: Tests	ATE_IND.1Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1Vulnerability survey
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification

Tabella 7 - Security Assurance Requirements

ADV_FSP.1 Basic functional specification

Dependencies:

None.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

AGD_OPE.1 Operational user guidance

Dependencies:

ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_PRE.1 Preparative procedures

Dependencies:

None.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

ALC_CMC.1 Labeling of the TOE

Dependencies:

ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMS.1 TOE CM coverage

Dependencies:

None.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ASE_INT.1 ST introduction

Dependencies:

None.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_CCL.1 Conformance claims

Dependencies:

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies:

None.

Developer action elements:

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

ASE_ECD.1 Extended components definition

Dependencies:

No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_REQ.1 Stated security requirements

Dependencies:

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

ASE_TSS.1 TOE summary specification

Dependencies:

ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ATE_IND.1 Independent testing - conformance

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

AVA_VAN.1 Vulnerability survey

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

6.6. ANALISI DELLE DIPENDENZE

La seguente *Tabella 8* mostra le dipendenze richieste dai Common Criteria per ogni SFR e SAR a livello di garanzia EAL1.

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
SFR		
FAU_GEN.1	FPT_STM.1 Reliable time stamps	**Nota 2**
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 Security attribute based access control
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ETC.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Subset access control
FDP_RIP.1	None	None
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_ATD.1	None	None
FIA_SOS.1	None	None

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	None	None
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 Subset access control, FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_SMF.1	None	None
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Function	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Function
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FRU_FLT.1	FPT_FLS.1 Failure with preservation of secure state	**Nota 1**
SAR		
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1 Basic functional specification
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1 TOE CM coverage	ALC_CMS.1 TOE CM coverage
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
AVA_VAN.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1 Basic functional specification

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

Tabella 8 - Verifica delle dipendenze

Nota 1 – Nel caso in cui l'ambiente non fornisce il collegamento ad una telecamera, l'ODV si preoccupa di salvare le immagini, ma non vengono effettuate altre funzioni per il mantenimento dello stato sicuro in quanto non necessarie per il funzionamento del sottosistema.

Nota 2 - La dipendenza non è soddisfatta in quanto il riferimento temporale affidabile viene fornito dall'ambiente operativo.

7. SPECIFICHE SOMMARIE (ASE_TSS)

Questa sezione fornisce le specifiche sommarie dell'ODV, una definizione ad alto livello delle funzioni di sicurezza che soddisfano i requisiti funzionali di sicurezza e di garanzia.

7.1. RIEPILOGO DELLE FUNZIONI DI SICUREZZA

Le funzioni di sicurezza rappresentate nel Security Target sono le seguenti:

1. ODV_IDAU – Identification and authentication
2. ODV_AC – Access Control
3. ODV_AUD - Auditing
4. ODV_MGMT - Management
5. ODV_DP – Data Protection

7.2. ODV_IDAU – IDENTIFICATION AND AUTHENTICATION

Amministratori ed utenti devono identificarsi ed autenticarsi prima di accedere alle funzioni dell'ODV.
L'ODV applica una rigorosa procedura di accesso, di seguito sintetizzata, prima di abilitare l'utente ad operare a seguito di autenticazione positiva, in particolare la procedura:

1) Richiede le credenziali di accesso
2) Verifica la rispondenza con quanto registrato dal sistema di autenticazione
3) In caso di primo accesso da parte di un utente, obbliga al cambio della password
4) Informa l'utente in caso di esito negativo
5) Gestisce l'autorizzazione per l'accesso alle diverse funzionalità dell'applicativo

L'ODV mediante le funzioni dei moduli Client Operazionale, Supervisore e Configuratore gestisce l'identificazione e l'autenticazione di un utente che vuole operare con SLT. I tre moduli presentano la finestra

di inserimento delle credenziali di accesso (utente e password) e mediante i controlli operati sulle stesse garantiscono che:

1) Inserendo le credenziali di un utente registrato e non scaduto, l'ODV abilita ad utilizzare l'applicativo con i diritti ad esso assegnati in base al ruolo di afferenza
2) Inserendo credenziali errate o scadute, l'ODV non consente alcun accesso al sistema, mostrando l'errore a video e consentendo di ripetere l'immissione nei limiti previsti per credenziali errate
3) In caso di primo accesso da parte di un utente, l'ODV obbliga l'utente a cambiare la propria password assegnata automaticamente da SLT all'atto della sua creazione. Questo viene ottenuto accendendo un flag dell'utente che dice di cambiare password al login.
4) Nel caso l'account risulti scaduto, l'ODV impedisce all'utente l'accesso.

Inoltre l'ODV provvede a registrare come evento di log qualsiasi operazione di login o logout.

Le operazioni sopra riportate realizzano le SFR **FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.2, FAU_GEN.1**.

7.3. ODV_AC – ACCESS CONTROL

L'ODV, mediante le "Componenti di controllo accessi", definisce soggetti, oggetti, operazioni e attributi che, sotto il controllo delle TSF, realizzano le funzioni di sicurezza dell'ODV. Di seguito le operazioni che l'ODV effettua sotto il controllo delle TSF:

- L'ODV mediante le funzioni del modulo CPS verifica lo stato di collegamento dei sistemi su strada.
- L'ODV mediante le funzioni del modulo CONFIGURATORE mantiene una lista degli utenti e abilita l'utente ad uno specifico ruolo tra quelli previsti (Amministratore, Superutente, Operatore, Manutentore).

L'accesso a queste operazioni viene realizzato dalle TSF che supportano le SFR **FDP_ACC.1, FDP_ACF.1, e FMT_SMR.1**.

7.4. ODV_AUD - AUDITING

L'ODV controlla le operazioni effettuate sul SCE e per ognuna di quelle nel seguito descritte, eseguita dai relativi moduli applicativi, viene memorizzata nel file di log eventi l'evento corrispondente contenente data ed ora, utente, tipo di operazione effettuata.

Le operazioni che generano un evento nel file di log sono le seguenti:

1) Per ogni tentativo, riuscito o meno, di login mediante la digitazione del nome utente e della password l'ODV archivia nel file di log degli eventi le informazioni identificative dell'evento.
2) Per ogni azione compiuta da utenti del sistema mediante i tre moduli: Client operazionale, Configuratore e Supervisore, l'ODV archivia nel file di log degli eventi le informazioni identificative dell'evento.

3) Per ogni operazione di invio a SCNTT delle informazioni di transito l'ODV tiene traccia cronologica della operazioni di lettura e scrittura effettuate dal modulo Interfaccia con SCNTT.
4) Per ogni operazione di cancellazione dei transiti per il superamento del tempo di conservazione l'ODV registra l'evento nel file di log degli eventi.

Queste operazioni vengono fatte tramite il modulo "Core Gestionale" del Sistema Centrale di Elaborazione e realizzano le SFR **FAU_GEN.1**.

7.5. ODV_MGMT - MANAGEMENT

L'ODV, mediante le funzioni di sicurezza ODV_AC – Access Control consente l'accesso alle funzioni dell'ODV agli utenti autorizzati. L'ODV, come descritto nel par. 2.6 del Security Target, gestisce mediante il modulo applicativo Configuratore i seguenti ruoli utente: Amministratore, Superutente, Operatore e Manutentore.

L'ODV mediante il modulo applicativo Configuratore di SCE consente ad un utente appartenente al ruolo di Amministratore di gestire tutti i parametri del sistema. In particolare consente la gestione di ruoli e utenti in termini di: inserimento e gestione dei ruoli, gestione dei ruoli assegnati ad ogni utente, inserimento dei nuovi utenti, modifica delle autorizzazioni degli utenti, disabilitazione/abilitazione delle utenze del sistema, disattivazione/riattivazione di utenti e sistemi su strada, modifica del tempo di conservazione delle immagini, assegnazione dei Sistemi su Strada agli utenti appartenenti al ruolo Operatore, in modo che venga creato l'abbinamento fra Sistema su strada e Operatore.
In particolare relativamente alla modifica dei tempi di conservazione delle immagini l'utente appartenente al ruolo di Amministratore, mediante il modulo applicativo Configuratore di SCE, può modificare i parametri di data retention sia dei transiti, sia degli allarmi di transito associati alla lista C. In ogni modo questo utente potrà modificare detti valori solo aumentando i parametri di data retention impostati come default all'inizializzazione del sistema e che sono fissati in: 15 gg per i transiti e 90 gg per gli allarmi di transito associati alla lista C.
Ad ogni operazione sopra descritta l'ODV assegna un riferimento temporale affidabile alla registrazione.
Queste operazioni realizzano le SFR **FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_MTD.1**.

7.6. ODV_DP – DATA PROTECTION

L' ODV si pone l'obiettivo di garantire la riservatezza ed integrità dei dati trattati, in maniera adeguata al livello di garanzia prescelto, attraverso le operazioni di seguito illustrate.
I dati raccolti dalle telecamere vengono spediti dalle stesse al SCE per la memorizzazione nel DB Oracle. In caso di interruzione del collegamento fra le telecamere ed il SCE, le telecamere hanno la capacità di trattenere le immagini in forma cifrata nella propria memoria SD, fino al ripristino del collegamento.

Gestione dei dati

1) L'allarme di transito può ricadere in una delle tipologie possibili: allarme legato alla rilevazione di targa in lista A1, A2, C, lista locale; allarme legato alle soglie di traffico; allarme di tipo targa mancante o parzialmente leggibile; allarme di tipo merci pericolose.
2) L'allarme viene visualizzato soltanto dagli operatori loggati e appartenenti ai gruppi la cui area di competenza contiene il varco in cui esso ha avuto origine.
3) Nel caso di allarme derivante dalla lista C, esso viene notificato agli operatori loggati e appartenenti ai gruppi competenti, solo se la rispettiva targa è configurata come visibile.
4) In caso di transito che non ha generato allarmi o che ha generato un allarme di interesse locale (targa in lista definita localmente, targa in lista A1 o A2, targa assente o parzialmente leggibile, merci pericolose), entro 30 minuti dal riconoscimento del transito stesso l'ODV tenta l'invio dei metadati relativi al transito e dell'immagine completa in bianco e nero al metodo *updateTransits* esposto dal web service di SCNTT. SCNTT risponderà inviando un array (*Result*) con i transiti non archiviati, dal quale sarà possibile ricavare gli eventuali errori presenti.
5) In caso di errori presenti, si procede alla correzione dei dati errati e si esegue nuovamente l'invio, entro i tempi previsti di conservazione del dato (15 gg). In caso di irraggiungibilità di SCNTT o di errori imputabili a SCNTT, si ritenta l'invio successivamente, fino a esito positivo e comunque entro i tempi previsti di conservazione del dato (15 gg).
6) In caso di transito che ha generato allarmi di interesse globale (targa in lista C), l'ODV tenta l'invio in tempo reale al metodo *updateAlarms* esposto dal web service di SCNTT dei metadati relativi all'allarme, dell'immagine completa in bianco e nero e dell'immagine di contesto a colori. SCNTT risponderà inviando un array (*Result*) con i transiti non archiviati, dal quale sarà possibile ricavare gli eventuali errori presenti.
7) In caso di errori presenti, si procede alla correzione dei dati errati e ad eseguire nuovamente l'invio, entro i tempi previsti di conservazione del dato (90 gg). In caso di irraggiungibilità di SCNTT o di errori imputabili a SCNTT, si ritenta l'invio successivamente, fino a esito positivo e comunque entro i tempi previsti di conservazione del dato (90 gg).

Queste operazioni realizzano le SFR **FRU_FLT.1, FDP_ETC.1, FDP_RIP.1**.

7.7. TABELLA DI SINTESI

La tabella seguente fornisce la mappatura dei SFR con le funzioni di sicurezza dell'ODV.

	ODV_IDAU	ODV_AC	ODV_AUD	ODV_MGMT	ODV_DP
FAU_GEN.1	**X**		**X**		

	ODV_IDAU	ODV_AC	ODV_AUD	ODV_MGMT	ODV_DP
FDP_ACC.1		X			
FDP_ACF.1		X			
FDP_RIP.1					X
FIA_AFL.1	X				
FIA_ATD.1	X				
FIA_SOS.1	X				
FIA_UAU.1	X				
FIA_UID.2	X				
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_SMF.1				X	
FMT_MTD.1				X	
FMT_SMR.1		X		X	
FRU_FLT.1					X
FDP_ETC.1					X

Tabella 9 - Sintesi dei SFR soddisfatti dalle funzioni dell'ODV