Progetto Vi.So.Re. Trevigiano

Security Target

del

“Sottosistema Videosorveglianza Comunale

Versione 1.0”

Riepilogo delle modifiche

N.	Versione	Stato	Data	Autore	Approvato	Tipo di modifica
1	1.0	Rilasciato	05/12/2013	A.Mennini	A. Hummer	Prima Versione
2	1.1	Rilasciato	05/05/2014	A.Mennini	A. Hummer	Aggiornamento dei capitoli 1 e 2
3	1.2	Rilasciato	18/10/2014	A.Mennini	A. Hummer	Sono state apportate modifche rispetto al progetto originale e pertanto, trattandosi di una certificazione “concomitante”, si è dovuto modificare il ST.
4	1.3	Rilasciato	29/11/2014	A.Mennini	A. Hummer	Revisione capitolo 2, sostituzione FDP_ROL.1 con FRU_FLT.1 e correzioni ad alcuni SFR
5	1.4	Rilasciato	12/01/2015	A.Mennini	A. Hummer	Revisione capitolo 2, per fornire maggiori dettagli e chiarire alcuni aspetti operativi dell’ODV
6	1.5	Rilasciato	11/03/2015	A.Mennini	A. Hummer	Revisione capitolo 2 e cap. 7 , per fornire maggiori dettagli e chiarire alcuni aspetti operativi dell’ODV.
7	1.6	Rilasciato	19/08/2015	A.Mennini	A. Hummer	Revisionea seguito ROA
8	1.7	Rilasciato	30/09/2015	A.Mennini	A. Hummer	Revisione finale

Tabella 1 - Riepilogo delle modifiche

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

1. PREMESSA 5
1.1 OBIETTIVI DEL DOCUMENTO 5
1.2 STRUTTURA DEL DOCUMENTO 5
1.3 ACRONIMI 5
1.4 RIFERIMENTI 6
2. INTRODUZIONE AL SECURITY TARGET (ASE_INT) 7
2.1 IDENTIFICAZIONE DEL SECURITY TARGET 7
2.2 IDENTIFICAZIONE DELL' ODV 7
2.3 PANORAMICA DELL' ODV 7
2.4 DESCRIZIONE DELL' ODV 8
2.4.1 Ambito fisico 9
2.4.2 Ambito logico 14
2.5 CONFINI 15
2.6 RUOLI UTENTE 15
2.7 FUNZIONI DI SICUREZZA DELL'ODV 16
3. DICHIARAZIONE DI CONFORMITA' (ASE_CCL) 17
4. OBIETTIVI DI SICUREZZA (ASE_OBJ) 18
4.1 OBIETTIVI DI SICUREZZA PER L'AMBIENTE OPERATIVO 18
5. DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD) 19
6. REQUISITI DI SICUREZZA (ASE_REQ) 20
6.1 GENERALITA' 20
6.2 CONVENZIONI 20
6.3 REQUISITI FUNZIONALI DI SICUREZZA 20
6.4 DETTAGLIO DEI REQUISITI FUNZIONALI 22
6.5 REQUISITI DI GARANZIA 28
6.6 ANALISI DELLE DIPENDENZE 30
7. SPECIFICHE SOMMARIE (ASE_TSS) 33
7.1 RIEPILOGO DELLE FUNZIONI DI SICUREZZA 33
7.2 ODV_AC – ACCESS CONTROL 33
7.3 ODV_AUD – AUDITING 34
7.4 ODV_MGMT - MANAGEMENT 34
7.5 ODV_DP – DATA PROTECTION 35
7.6 TABELLA DI SINTESI 36

Indice delle Tabelle

Tabella 1 - Riepilogo delle modifiche....2
Tabella 2 - Acronimi....6
Tabella 3 - Infrastruttura ospitante l'ODV....13
Tabella 4 - Funzioni di sicurezza dell'ODV....16
Tabella 5 - Obiettivi di sicurezza per l'ambiente....18
Tabella 6 - ODV Security Functional Requirements (SFR)....21
Tabella 7 - Security Assurance Requirements (SAR)....28
Tabella 8 - Verifica delle dipendenze....32
Tabella 9 - Sintesi dei SFR soddisfatti dalle funzioni dell'ODV....36

Indice delle Figure

Figura 1 - Ambito Progetto Vi.So.Re.....8
Figura 2 - Schema Generale ODV....9
Figura 3 - Flusso interno telecamera e verso Sistema Centralizzato di Controllo....10
Figura 4 - Architettura generale (con dettaglio Sistema Centralizzzato di Controllo)....12

1. PREMESSA

1.1 OBIETTIVI DEL DOCUMENTO

Questo Security Target (ST) descrive gli obiettivi di sicurezza, i requisiti e le motivazioni del "Sottosistema Videosorveglianza Comunale 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:

- **Introduzione al ST [Rif. § 2]:** questa sezione fornisce le referenze, una descrizione dell'ODV che ne fornisce le caratteristiche e ne definisce l'ambito.
- **Dichiarazione di Conformità [Rif. § 3]:** questa sezione presenta le conformità con i Common Criteria.
- **Obiettivi di sicurezza [Rif. § 4]:** questa sezione descrive in maniera dettagliata gli obiettivi di sicurezza dell'ambiente.
- **Definizione di Componenti Estese [Rif. § 5]: q**uesta 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
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
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] DL 196/2003 e successive modificazioni

2. INTRODUZIONE AL SECURITY TARGET (ASE_INT)

2.1 IDENTIFICAZIONE DEL SECURITY TARGET

Titolo: **Security Target Sottosistema SVC v. 1.7**

Data : **30/09/2015**

Autore : **Andrea Mennini**

2.2 IDENTIFICAZIONE DELL' ODV

Nome del prodotto: **Sottosistema Videosorveglianza Comunale v. 1.0 (nel seguito per brevità anche SVC)**

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

2.3 PANORAMICA DELL' ODV

L'ODV è un Sottosistema di Videosorveglianza Comunale operante nell'ambito di iniziali 27 comuni della provincia di Treviso avente la finalità di prevenire attività di microcriminalità, atti vandalici, incendi dolosi, rilevare e ricostruire eventi criminosi e divenire un forte elemento deterrente. L'ODV costituisce una parte del più ampio Progetto Vi.So.Re. Trevigiano. L'ODV prevede un certo numero di telecamere installate in siti critici di diversi comuni, collegate con posti di visualizzazione/controllo 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 e visualizzazione delle immagini provenienti dalle iniziali 122 telecamere installate presso gli 89 siti iniziali identificati nei 27 comuni iniziali interessati dal progetto Vi.So.Re. Trevigiano. L'ODV è un Sistema di Videsorveglianza 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]. Il Capitolato Speciale di Appalto Progetto Vi.So.Re. Trevigiano [RF1] indica le funzioni di sicurezza che l'ODV deve soddisfare determinando i confini dello stesso.

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 SVC, qui descritto;
- Il sottosistema SLT, dedicato alla lettura delle targhe
- 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 periferiferici e quelli centrali.

Il sottosistema SNV garantisce il collegamento sicuro tra le diverse componenti dell'ODV descritte al successivo paragrafo [Rif. § 2.4.1.2 Infrastruttura gestita].

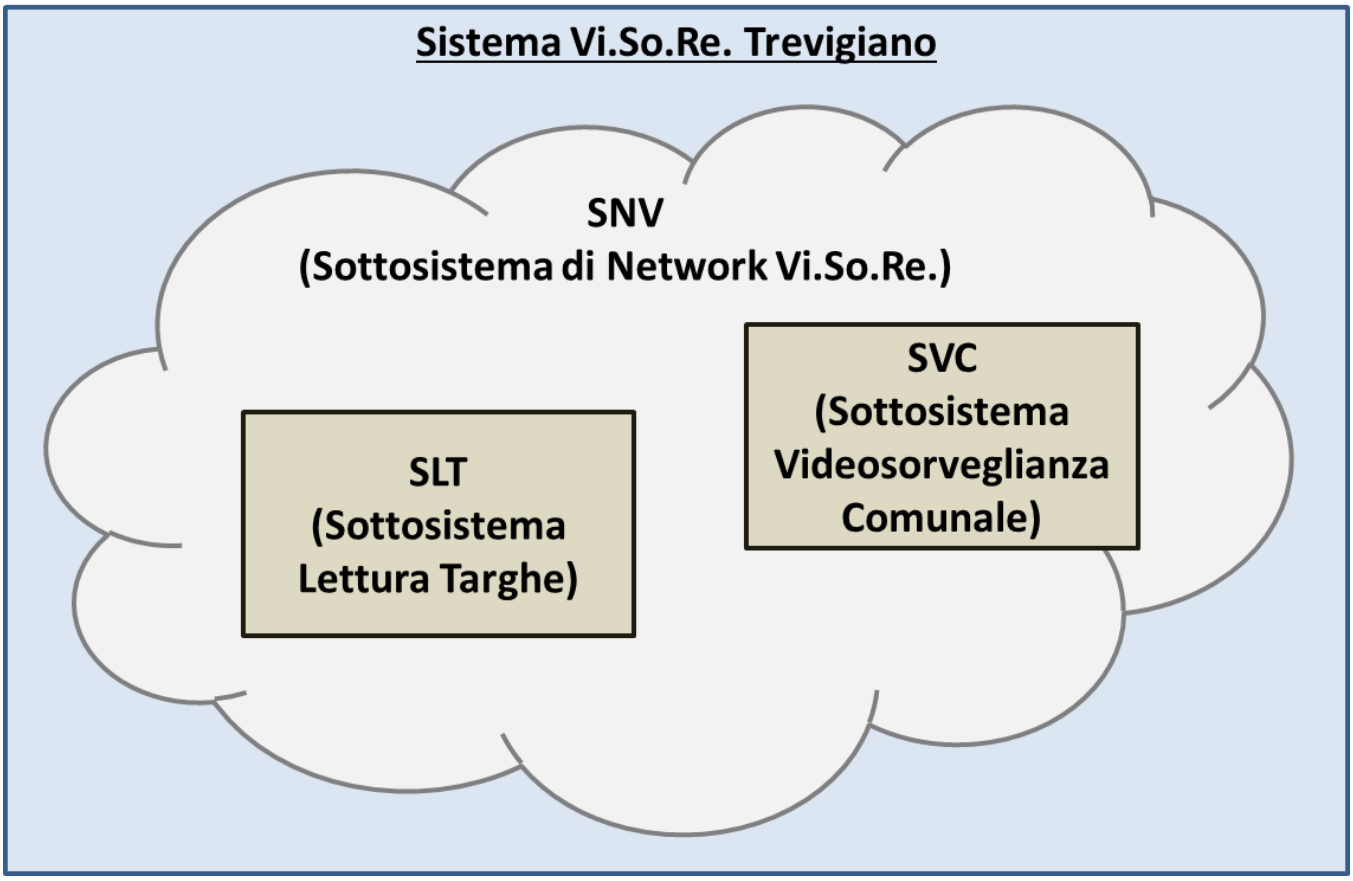

Figura 1 - Ambito Progetto Vi.So.Re.

2.4 DESCRIZIONE DELL'ODV

Gli obiettivi dell'ODV e del suo ambiente operativo sono la realizzazione di sistemi integrati di videosorveglianza territoriale (per ogni comune interessato) tesi a sorvegliare le più importanti aree di transito e gli accessi ai centri urbani, per finalità di Sicurezza.

L'ODV ed il suo ambiente si compongono di:

- 122 telecamere iniziali installate nei comuni che rientrano nel progetto Vi.So.Re. Trevigiano
- Sistema Centralizzato di Controllo ospitato nel data center SVC sito in Oderzo (TV) che è certificato ISO/IEC 27001:2005
- 27 posti operatore iniziali a livello comunale per funzioni di visione/controllo
- Posti operatore dedicati ad enti territoriali esterni come indicato nel bando di gara (Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza) per funzioni di visione e controllo

La seguente figura illustra lo schema logico generale dell'ODV e del suo ambiente con i ruoli utente previsti.

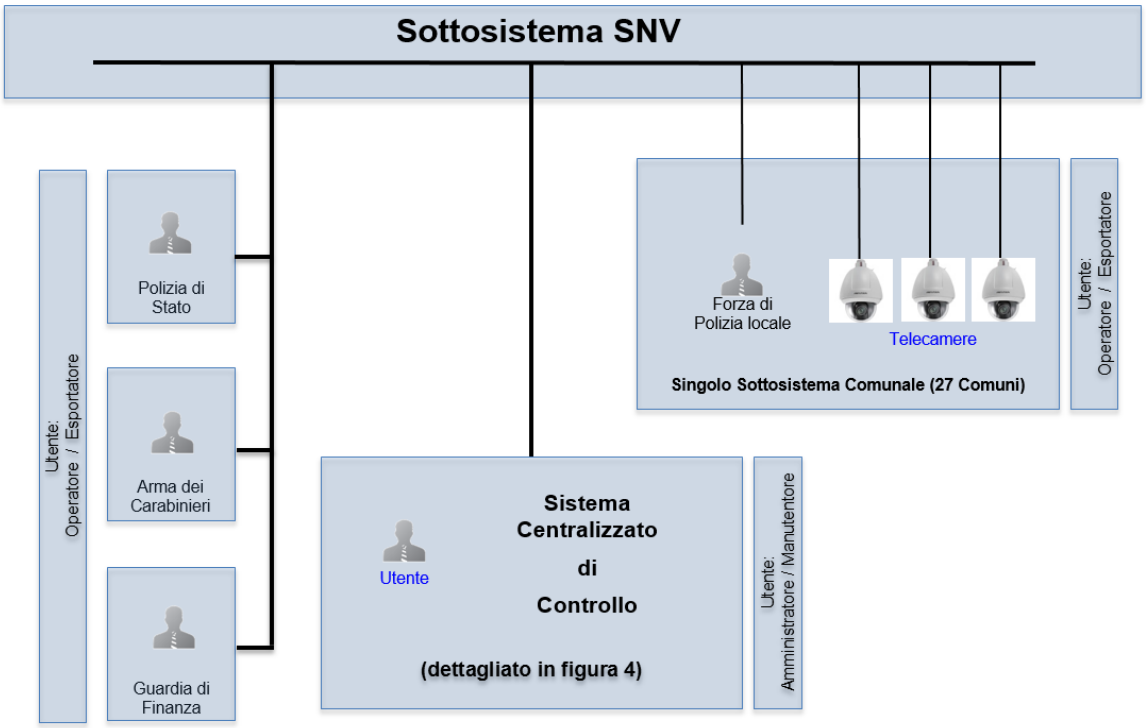

Figura 2 - Schema Generale ODV

2.4.1 AMBITO FISICO

2.4.1.1 *Flusso generale dell'ODV e del suo ambiente operativo*

L'architettura generale di funzionamento prevista per l'intero sottosistema è la seguente:

a) Nei siti comunali monitorati le telecamere di videosorveglianza raccolgono riprese video 24 ore su 24 e le codificano secondo standard di mercato (MJPEG, MPEG o H264). Le riprese video una volta codificate vengono da qui in avanti indicate come flusso video;

b) Le telecamere di videosorveglianza al loro interno rendono il flusso video contemporaneamente disponibile al Sistema Centralizzato di Controllo (Flusso video live) e verso la memoria interna SD dove vengono memorizzate dopo essere state cifrate (AES128) (Flusso video registrato).

c) Tramite il sottosistema SNV, la componente Sistema Centralizzato di Controllo (con protocollo TCP/IP) richiede alle telecamere i flussi video live per la loro registrazione nei server presso il data center SVC.

d) Nel caso di assenza temporanea di collegamento tra il Sistema Centralizzato di Controllo e la Telecamera, Il sistema Centralizzato di Controllo al ripristino del collegamento, richiede alla telecamera oltre al Flusso video

live (punto C) anche il Flusso video registrato. Il Flusso video registrato viene dalla telecamera decifrato e quindi reso disponibile al sistema Centrale di Controllo per la sua registrazione nei server presso il data center SVC.

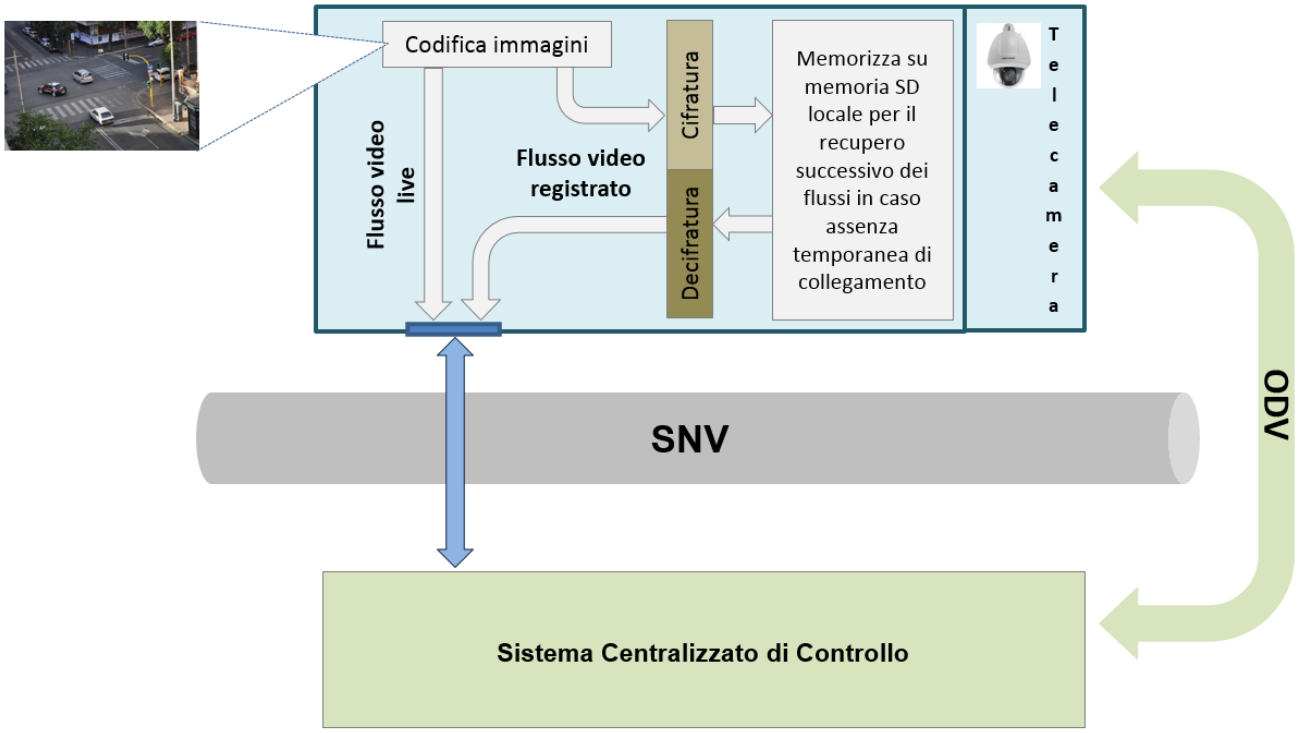

Figura 3 - Flusso interno telecamera e verso Sistema Centralizzato di Controllo

e) Fin dall'acquisizione sul campo le immagini del SVC vengono tenute separate da quelle del sottosistema SLT mediante il sottosistema SNV. Le immagini, le aree di memorizzazione e i dati memorizzati di ogni singolo comune vengono tenuti separati in base ai ruoli assegnai agli utenti SVC.

f) Dalle postazioni operatore delle forze di polizia locali (Sottosistemi Comunali), i titolari del trattamento dati accedono sia alle riprese in real-time che alle registrazioni; possono eseguire operazioni di zoom e di brandeggio delle telecamere. Ogni operatore può accedere alle riprese ed alle registrazioni esclusivamente del comune per il quale è individuato come titolare al trattamento dei dati.

g) Dalle postazioni operatore delle Forze di Polizia di Stato, così come dagli Enti Esterni (Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza), gli operatori, ciascuno con proprie e predefinite autorizzazioni, possono accedere, tramite il sottosistema SNV, sia agli streaming video che alle registrazioni del sistema ODV di tutti i siti di tutti i comuni e possono eseguire, con priorità rispetto agli operatori delle forze di polizia locali, operazioni di zoom e brandeggio delle telecamere.

h) Le registrazioni video vengono effettuate 24 ore al giorno e mantenute nel Sistema Centralizzato di Controllo per un periodo di 15 giorni, comunque configurabile, dopodiché automaticamente eliminate.

i) Il Sistema Centralizzato di Controllo fornisce una funzionalità amministrativa che consente di definire utenti, gruppi, titolari trattamento dati ciascuno con proprie autorizzazioni, il che consente di attribuire al sistema una configurabilità operativa finalizzata alla applicazione della Privacy by Design a garanzia dei principi di Privacy (art. 11 del D Lgs.vo 196/03) [RF2].

2.4.1.2 Componenti dell'ODV

Di seguito la componente fisica del Sottosistema di Videosorveglianza Comunale.

- **Telecamera Hikvision DS-2DF5286-A** - (IP, megapixel, zoom ottico 30 x, Day&Night, autofocus, autoiris, controllo automatico del guadagno, grado di protezione IP66). Il software residente sulle telecamere di videosorveglianza consiste in un Codificatore Video con algoritmi di compressione video H264 e sue evoluzioni e MJPEG/MPEG. Le telecamere sono dotate di uno slot SD per consentire di memorizzare i dati di ripresa nel caso di non funzionamento della rete di trasmissione dati. E' prevista la fornitura di una scheda SD da 32 GB che consente la memorizzazione delle immagini per un periodo minimo di 8 ore. I filmati registrati sono esportabili al ripristino dei collegamenti. Le telecamere hanno la possibilità di cifrare e decifrare le immagini con algoritmo di cifratura AES in caso di non funzionamento della rete di trasmissione dati.

Di seguito le componenti software che costituiscono il Sottosistema di Videosorveglianza Comunale.

La piattaforma di gestione usata per il sistema SVC è "Milestone Xprotect Management" nella versione Corporate 2014 mentre i componenti Client sono rappresentati da Milestone Xprotect Smart Client 2014.

Il Sistema Centralizzato di Controllo è costituito dai seguenti moduli.

- **Management Server** (Milestone Xprotect Management Client)

  Il Management Server è il centro del sistema. In esso risiede la configurazione di tutti i Siti, dei Recording Server, delle Telecamere, nonché dei ruoli utente di tutto il sottosistema SVC. Ad esso si accede mediante apposito client di management che fornisce la console come unico punto di gestione del sistema ed in questo modo l'amministratore può configurare e gestire tutti i siti, i server di registrazione, le telecamere.

- **Recording Server** (Milestone XProtect Management/Recording).

  Il Recording Server è il software installato sui Recording Server che processa la registrazione e la riproduzione dei flussi video acquisiti dalle telecamere. Questo si occupa del salvataggio della immagini sulla SAN sfruttando la architettura in Load Balancing e Failover resa disponibile dall'ambiente.

La componente software delle Postazioni Operatore è costituita da :

Smart Client (Milestone Xprotect Smart Client)

Il Client è l'unico punto di accesso configurato per l'utilizzo del Sistema SVC dal punto di vista degli utenti che operano mediante questo modulo SVC dalle postazioni operatore. Mediante il client l'operatore può effettuare tutte le operazioni specifiche del suo ruolo.

La figura seguente illustra l'architettura risultante.

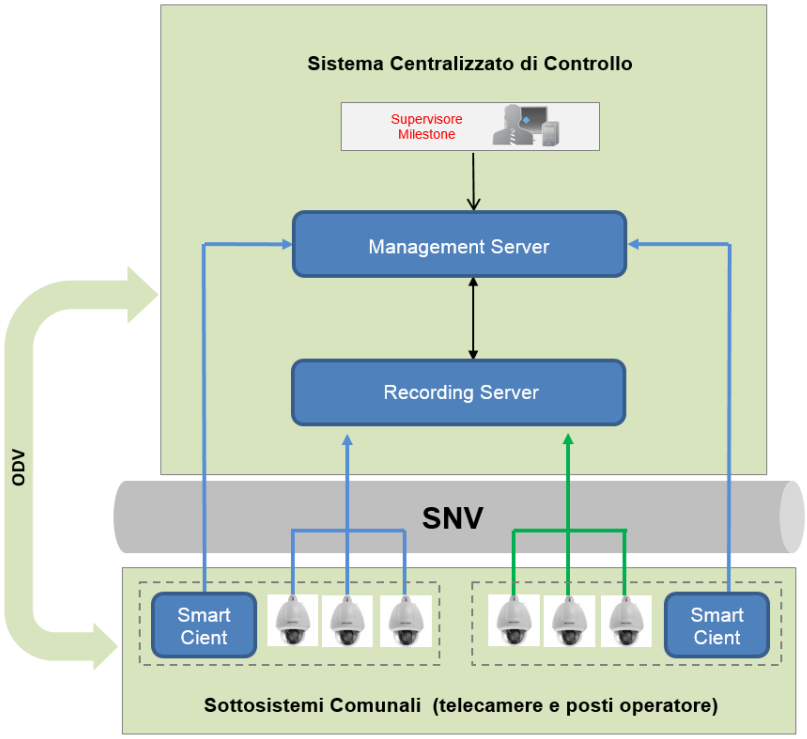

Figura 4 - Architettura generale (con dettaglio Sistema Centralizzzato di Controllo)

2.4.1.3 Componenti di ambiente

La componente esterna che interfaccia l'ODV è costituita dal sottosistema SNV che utilizza il protocollo MPLS e garantisce sia il trasporto delle informazioni video, sia l'accesso all'ODV agli enti esterni incaricati del loro trattamento.

L'ambiente operativo tramite funzioni del Sistema Operativo Microsoft implementa funzioni di Load Balancing, Failover e Cluster.

Segue un dettaglio specifico di quali apparati fisici sono a supporto delle componenti dell'ODV.

Funzionalità ODV		Apparato di supporto delle componenti dell'ODV	Numero di unità attuali
Sistema Centralizzato di Controllo	Management Server (Milestone Xprotect Management)	Dell PowerEdge R520	2
		Dell PowerEdge R520	2
		Nodo di Monitoring (Nagios) Dell PowerEdge R420	1
	Recording Server (Milestone Xprotect Management)	Nodo di Backup Symantec Dell PowerEdge R420 / TL2000	1
		SAN Storage EMC VNX5100	1
Postazioni Operatore	Smart Client (Operatore / Esportatore / Manutentore / Amministratore)	Personal computer	27
		Personal computer	1

Tabella 3 - Infrastruttura ospitante l'ODV

- **Apparati centrali di supporto delle componenti dell'ODV** – i server sono situati in un Data Center in provincia di Treviso certificato ISO 27001:2005. Il Sistema Centralizzato di Controllo è composto di base da 4 server fisici Dell modello PowerEdge R520 per l'applicazione "Milestone Xprotect Management", ed ha a bordo il Processor Intel® Xeon® processor E5-2400 Processor sockets: 2 Cache: 2.5MB per core; 6 core Chipset Intel C602 Memory 16GB DDR3 Storage 2 x 146 GB 3.5" hot-plug SAS disk Network Controller Embedded NIC: Broadcom® 5720 Dual Port 1Gb LOM 1Gb Ethernet: Broadcom 5720 Dual Port 1Gb NIC FC HBA Emulex LPe-12002-E 8Gb Dual Port FC HBA Form factor 2U rack Operating System Microsoft Windows Server 2008 STD R2 SP1, x64, SQLServer 2008 R2 Express.

  Il Sistema SVC prevede a tutela della sua operatività due nodi di gestione, il nodo di monitoraggio ed il nodo di backup.

  Il Nodo di Monitoring Dell PowerEdge R420 ha a bordo il Processor Intel® Xeon® processor E5-2407 Processor sockets 2, Cache 2.5MB per core, 4 core Chipset Intel C602 Memory 4GB DDR3 Storage 2 x 146 GB 2.5" hot-plug SAS disk 15k RPM Network Controller Embedded NIC: Broadcom® 5720 Dual Port 1Gb LOM 1Gb Ethernet Broadcom 5720 Dual Port 1Gb NIC Form factor 1U rack Operating System Suse Linux Enterprise Server 11 SP3.

Il Nodo di Backup è un Dell PowerEdge R420 con Processor Intel® Xeon® processor E5-2407 Processor sockets, 2 Cache 2.5MB per core, 4 core Chipset Intel C602 Memory 4GB DDR3 Storage 2 x 146 GB 2.5" hot-plug SAS disk 15k RPM SAS Controller 2 SAS 6Gbps HBA Network Controller Embedded NIC: Broadcom® 5720 Dual Port 1Gb LOM, Operating System Windows 2008 R2, Symantec Backup Exec 2012 con Dell Power Vault TL2000 Tape Library.

Il Sistema Centralizzato di Controllo prevede una SAN (un apparato di storage EMC VNX5100) per il salvataggio/recording.

- **Postazioni Operatore** – le postazioni operatore sono dotate di personal computer con doppia uscita video, monitor dedicato da 21'' e joystick proporzionale a 3 assi, di Monitor/TV 42'' e di Ups di potenza adeguata.

Di seguito l'elenco delle ulteriori componenti di ambiente:
Tutti i dispositivi supportano funzionalità di firewall da Layer2 fino ad Layer7 con possibilità di creare vpn L2TP, PPTP, SSTP, IPSec e OpenVPN.

- Switch: l'interconnessione tra server ed i dispositivi di rete e sicurezza è garantita da una coppia di switch Cisco 3560 24 porte 10/100/1000.
- La rete di distribuzione che a partire dal backbone si ramifica nelle varie sedi comunali facenti parte del SVC è realizzata tramite tecnologia Hiperlan, con apparati Fly NWBR-GIGA-500AN-20-CTAF.
- Su ognuno dei siti SVC sono presenti:
  - uno switch industriale, Etherwan EX78000, per la gestione delle vlan per garantire la separazione dei flussi di traffico,
  - due router/firewall, Mikrotik RB2011LS-IN per garantire la privacy-by- design;
  - apparato radio (oppure due apparati radio in caso di siti ad anello) con funzionalità di firewall/router, per garantire al massimo livello sicurezza e confidenzialità dei dati.
- Sistema Operativo Microsoft Server 2008 R2 Enterprise Edition.
- Repository LDAP di SNV per identificazione ed autenticazione degli utenti dell'ODV.

2.4.2 AMBITO LOGICO

Il software di gestione video è sviluppato su piattaforma aperta e progettata per progetti di sicurezza 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. La disponibilità delle mappe grafiche, la funzionalità drag-and-drop e configurazione basata su regole – conferisce alla sala di controllo una supervisione sistemica completa e un'eccellente comprensione della situazione fisica soggetta a vigilanza.
L'ODV include un efficiente metodo d'amministrazione centralizzata, procedure guidate intuitive, flessibili regole di funzionamento del sistema e scansione automatica della rete con rilevamento automatico del modello della

telecamera connessa. Queste caratteristiche permettono di gestire con facilità la personalizzazione di un impianto di videosorveglianza 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 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 SVC, proprie dell'ambiente operativo e descritte nel successivo par. 4, concorrono al raggiungimento degli obiettivi prefissati.

2.5 CONFINI

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

L'ODV gestisce i seguenti ruoli utente:

- amministratore

  Gli utenti con ruolo "Amministratore" possiedono i diritti di amministratore e possono accedere alle funzioni di configurazione che permettono di gestire le seguenti voci:

  - Inserimento, modifica, disabilitazione delle utenze del sistema, gestione di gruppi e ruoli assegnati ad ogni utente
  - Configurazione parametri dell'intero sistema

- operatore

  Gli utenti con il ruolo "Operatore" sono gli utilizzatori dei Sottosistemi Comunali e degli Enti Esterni con diverse competenze territoriali. Questi utenti avranno i diritti (configurabili) per accedere ed usufruire alle diverse funzionalità del software:

  - Visualizzazione immagini dal campo
  - Gestione delle telecamere (puntamenti, zoom, etc)
  - Visualizzazione degli allarmi provenienti dal campo

- esportatore

  Gli utenti con ruolo “Esportatore” possiedono i diritti degli utenti con il ruolo “Operatore” ed inoltre hanno accesso alle funzioni di:

  - Esportazione a fini forensi delle immagini registrate
  - Accesso alle funzioni di ricerca immagini nei limiti di persistenza delle stesse nei sistemi
  - Esportazione delle immagini nei formati standard AVI e/o JPEG e/o MKV.

- manutentore

  Gli utenti con ruolo “Manutentore” possiedono i diritti che consentono di accedere alle funzioni di:

  - Configurazione delle telecamere e tuning delle stesse
  - Disattivazione e attivazione di telecamere per attività di manutenzione programmata o eccezionale.

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_AC	**Access control**	L’ODV consente agli amministratori di configurare l’accesso alle funzioni, alle telecamere ed ai dati in base al ruolo di ciascun utente.
ODV_AUD	**Auditing**	L’ODV genera log relativi alle telecamere (rilevazione delle operazioni di gestione) ed agli utenti (operazioni di autenticazione).
ODV_MGMT	**Gestione**	L’ODV provvede al controllo delle seguenti operazioni: a) Operazioni su ruoli e utenti b) Operazioni sulle telecamere.
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 4 - Funzioni di sicurezza dell’ODV

3. DICHIARAZIONE DI CONFORMITA' (ASE_CCL)

Il ST e l'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, 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.

Questo ST non prevede l'utilizzo di componenti estese.

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 SVC 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 SVC 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 5 - Obiettivi di sicurezza per l'ambiente

5. DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD)

Questo ST non definisce alcuna componente estesa.

6. REQUISITI DI SICUREZZA (ASE_REQ)

6.1 GENERALITA'

Questa sezione definisce i requisiti di sicurezza e di garanzia soddisfatti dall'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
FMT: Security Management	FMT_MSA.1	Management of security attributes

Functional Requirements		
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
FRU: Resources utilization	FRU_FLT.1	Degraded fault tolerance

Tabella 6 - ODV Security Functional Requirements (SFR)

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) Attivazione/rimozione di telecamere (funzione del ruolo manutentore)**. **]**
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 **b)** For each audit event type, based on the auditable event definitions of the functional components included in the ST **[Evento a): ID utente riassegnato, nuovo ruolo** **Evento b): ID telecamera**].
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	Le funzioni di audit si svolgono esclusivamente nel Sistema Centralizzato di Controllo ad opera del Management Server.

FDP_ACC.1	
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**SVC access control SFP**] on [**Soggetti:** **a) Utente** **Oggetti:** **a) Immagini** **b) Telecamere**

	Operazioni: **a) Gestione immagini** **b) Gestione telecamere**]
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	La policy di controllo accessi prevede tutte le operazioni avvengano nel Sistema Centralizzato di Controllo e che l'unico punto di accesso al Sistema Centralizzato di Controllo sia rappresentato dal Management Server.

FDP_ACF.1	
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**SVC access control SFP**] to objects based on the following: [**Subject attribute:** **Ruolo: amministratore, operatore, esportatore, manutentore** **Object attributes:** **a) Tempo di conservazione (delle immagini)** **b) ID (delle telecamere)**]
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 sottostante "Componenti di controllo accessi", che sintetizza la "SVC access control SFP", 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		
SOGGETTI **ATTRIBUTI**	**OGGETTI** **ATTRIBUTI**	**OPERAZIONI**
Utente/Amministratore	• Immagini/Tempo di conservazione • Telecamere/ID	• L'utente amministratore può modificare il tempo di conservazione delle immagini nel Sistema Centralizzato di Controllo attraverso il Management Server • L'utente amministratore può accedere alle telecamere in base all'ID per modificarne l'assegnazione a ruoli utente • L'utente amministratore attraverso il Management Server ha la possibilità di gestire il ruolo assegnato ad ogni utente
Utente/Operatore	• Immagini/Tempo di conservazione • Telecamere/ID	• L'utente operatore ha la possibilità di vedere le immagini provenienti dalle telecamere, in base alla assegnazione dei rispettivi ID
Utente/Manutentore	• Telecamere/ID	• L'utente manutentore ha la possibilità di accedere al Sistema Centralizzato di Controllo attraverso il Management Server, per disattivare e attivare le telecamere in base al loro ID, per attività di manutenzione programmata o eccezionale
Utente/Esportatore	• Immagini/Tempo di conservazione	• L'utente esportatore può accedere alle funzioni di ricerca immagini del Management Server nei limiti di persistenza delle stesse nei sistemi • L'utente esportatore può esportare a fini forensi immagini registrate nei limiti di persistenza delle stesse nei sistemi.

FDP_RIP.1/SD	
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 from*] the following objects: **[immagini registrate nelle telecamere**].
Dependencies:	No dependencies
Notes:	Le immagini memorizzate criptate nella memoria SD delle telecamere vengono cancellate per sovrascrittura.

FDP_RIP.1/Sistemi centrali	
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 from*] the following objects: **[immagini conservate nel Sistema Centralizzato di Controllo**].
Dependencies:	No dependencies
Notes:	Tutte le immagini memorizzate nel Sistema Centralizzato di Controllo vengono cancellate dopo un periodo di tempo di 15 giorni, comunque modificabile da un utente amministratore.

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

FMT_MSA.3	
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**SVC 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 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_SMF.1	
Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions**: [** **a) Gestione dei ruoli assegnati ad ogni utente** **b) Assegnazione di immagini a ruoli utente** **c) Assegnazione di telecamere a ruoli utente** **d) Modifica del tempo di conservazione delle immagini** **e) Configurazione delle telecamere e tuning delle stesse** **f) Disattivazione di telecamere per attività di manutenzione programmata o eccezionale e successiva riattivazione** **]**
Dependencies:	No dependencies
Notes:	Tutte le funzioni di gestione vengono realizzate tramite le interfacce fornite dal Management Server.

FMT_SMR.1	
Hierarchical to:	No other components.

FMT_SMR.1	
FMT_SMR.1.1	The TSF shall maintain the roles [**a) Amministratore** **b) Operatore** **c) Esportatore** **d) Manutentore**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	

FDP_ETC.1	
Hierarchical to:	No other components.
FDP_ETC.1.1	The TSF shall enforce the [assignment: **SVC 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:	

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 Centralizzato di Controllo**].
Dependencies:	FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1	
Notes:	In caso di interruzione del collegamento fra le telecamere ed il Sistema Centralizzato di Controllo, le telecamere hanno la capacità di trattenere le immagini, in forma criptata, nella propria memoria SD, fino al ripristino del collegamento.

6.5 REQUISITI DI GARANZIA

I requisiti di garanzia per l'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 l'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.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability 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 (SAR)

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 ODV 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 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 3**
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

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
		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/SD	None	None
FDP_RIP.1/sistemi centrali	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_SMR.1	FIA_UID.1 Timing of identification	**Nota 1**
FRU_FLT.1	FPT_FLS.1 Failure with preservation of secure state	**Nota 2**
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

Functional Requirements	Dipendenze richieste dai CC	Dipendenze soddisfatte
AVA_VAN.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

Tabella 8 - Verifica delle dipendenze

Nota 1 – Un utente che vuole collegarsi all'ODV trova il primo punto di contatto nel sottosistema SNV, ovvero nell'ambiente, che provvede, attraverso Active Directory, alla identificazione ed autenticazione dell'utente.

Nota 2 – 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 3 – 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

1. ODV_AC – Access Control
2. ODV_AUD – Auditing
3. ODV_MGMT – Management
4. ODV_DP – Data Protection

7.2 ODV_AC – ACCESS CONTROL

L'ODV garantisce un controllo stringente relativamente all'accesso alle sue risorse, che di base non sono rese disponibili. Per utilizzare le risorse dell'ODV ogni utente deve essere associato ad uno specifico ruolo da parte di un utente Ammnistratore. Solo un utente associato al ruolo Amministratore può inserire nuovi utenti nel sistema ed attribuire ad essi un ruolo specifico nell'ODV. Mediante questa associazione l'ODV consente ad un distinto utente di accedere ad una specifica telecamera per vedere i flussi video da questa generati (ruolo Utente Operatore), esportare i flussi video di una specifica telecamera (ruolo Utente Esportatore), mettere in manutenzione una specifica telecamera (ruolo Manutentore).

Prima di accedere all'ODV un utente deve superare una fase di identificazione e autenticazione che avviene mediante accesso al Server LDAP fornito dall'ambiente, in particolare dal sottosistema SNV. Solo se il nome utente e password vengono ricosciuti nel Server LDAP SNV consente l'accesso all'ODV. Superata questa fase di identificazione ed autenticazione, l'ODV, mediante le funzioni del Management Server, provvede a controllare il ruolo assegnato all'utente per garantire che ciascun utente acceda alle sole funzioni previste per il ruolo specifico.

L'ODV mediante la funzionalità amministrativa del Management Server, per ciascuna risorsa, mantiene una Access Control List che mappa gli utenti ed i rispettivi ruoli alle operazioni che sono permesse.

L'ODV mediante la funzionalità amministrativa del Management Server riconosce 3 ruoli utente e 1 ruolo amministratore, aventi differenti diritti sui dati e sulle funzionalità dell'ODV, come specificato al precedente par. 2.6.

Queste operazioni realizzano le SFR FDP_ACC.1, FDP_ACF.1, e FMT_SMR.1.

7.3 ODV_AUD – AUDITING

L'ODV mediante una apposita funzione del Management Server è in grado di registrare in un file di log due tipologie di eventi: quelli relativi alla disattivazione/attivazione a fini manutentivi dalle "telecamere" e quelli relative agli "utenti". Queste registrazioni consento agli utenti afferenti al ruolo di Amministratore di poter visualizzare quali eventi hanno interessato un utente e/o una telecamera.

L'ODV consente agli utenti con ruolo di Amministratore di modificare le associazioni fra gli utenti del SVC e i ruoli previsti nell'ODV mediante apposita funzione del Management Server. Per ogni modifica così effettuata l'ODV mediante apposita funzione del Management Server genera automaticamente una registrazione nel file di log con l'ID dell'utente e il riferimento temporale. Questa tipologia di eventi viene definita come evento "utenti".

L'ODV consente all'utente con ruolo di Manutentore la disattivazione e la riattivazione di telecamere del SVC a seguito di specifiche esigenze di manutenzione. Per ogni modifica effettuata dal Manutentore l'ODV mediante apposita funzione del Management Server genera automaticamente una registrazione nel file di log con l'ID della telecamera e il riferimento temporale. Questa tipologia di eventi viene definita come evento "telecamera".

Ogni evento generato automaticamente dal Management Server e registrato nel file di log riporta o l'ID dell'utente (evento "utenti") o l'indirizzo ID della telecamera (evento "telecamere"), oltre a un riferimento temporale affidabile.

Queste operazioni vengono fatte tramite il Management Server del Sistema Centralizzato di Controllo e realizzano la SFR **FAU_GEN.1**.

7.4 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 la funzione del Management Server i seguenti ruoli utente: amministratore, operatore, esportatore, manutentore.

L'ODV mediante la funzione del Management Server 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, modifica del tempo di conservazione delle immagini, assegnazione delle immagini provenienti dalle telecamere a ruoli utente, in modo che venga creato l'abbinamento fra le telecamere installate in un comune ed il sottosistema comunale relativo.

L'ODV mediante la funzione del Management Server consente ad un utente appartenente al ruolo Operatore di visualizzare i flussi video provenienti dal campo in base alla autorizzazioni concesse dall'utente Amministratore.

Consente ad un utente Operatore inoltre, di gestire la telecamera in ternimi di operatività della stessa, cioè di modificare il suo puntamento standard e di effettuare degli zoom sulle immagini, di modificare i parametri di ronda, di modificare le aree di obliterazione, e gli altri paramentri operativi utili nella corrente attività di vodeosorveglianza. Un utente operatore è anche in grado di visualizzare gli allarmi derivanti dall'analisi delle immagini con algoritmi dedicati all rilevazione di eventi specifici (oggetto rimosso, oggetto abbandonato, transiti in aree proibite, etc.).

L'ODV mediante la funzione del Management Server consente ad un utente appartenente al ruolo di Esportatore di effettuare tutte le operazioni autorizzate ad un utente di tipo Operatore, con in più la possibilità di: esportare a fini forensi le immagini registrate; accedere alle funzioni di ricerca immagini nei limiti di persistenza delle stesse nei sistemi, esportare le immagini nei formati standard AVI e/o JPEG e/o MKV per esigenze delle forze di Polizia.

L'ODV mediante il Management Server permette ad un utente appartenente al ruolo di Manutentore le seguenti funzioni di gestione delle telecamere: attivazione e disattivazione delle telecamere per attività di manutenzione programmate e eccezionali, configurazione dei parametri di funzionameto della telecamera. L'ODV mette a disposizione un Wizard per la sostituzione guidata di una telecamera guasta: grazie ad una semplice procedura guidata, l'utente può sostituire una telecamera guasta con una nuova, facendole ereditare tutte le impostazioni, i presets PTZ, la configurazione video e il database delle immagini collegato alla telecamera precedente.

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 e FMT_SMR.1**.

7.5 ODV_DP – DATA PROTECTION

L'ODV garantisce che le riprese video efettuate dalle telecamere e trasformate in flussi video mediante codifica negli standard di mercato (MJPEG, MPEG, H264) siano disponibili agli utenti per le operazioni su di esse rese possibili in base allo specifico ruolo di appartenenza. L'ODV già nella sua componente telecamera, dopo avere codificato la ripresa video, rende parallelamente disponibile il flusso video ottenuto al Sistema Centrale di Controllo in modalità live, mentre memorizza lo stesso flusso sulla memoria SD locale con algoritmo AES a 128 bit. In questo modo in caso di interruzione del collegamento fra il Sistema Centralizzato di Controllo e le telecamere, solo il Sistema Centrale di Controllo può richiedere alla telecamera i flussi che non ha potuto rilevare in modalità live. Quando, al ripristino del collegamento, il Sistema Centrale di Controllo richiede i flussi video registrati dalla telecamera, questa li decifra localmente e quindi li rende disponibili. La memoria SD della telecamera viene gestita in sovrascrittura secondo una logica FIFO (First In First Out).
Il Sistema Centrale di Controllo acquisti i flussi video dalle telecamere attiva i Recording Server per la loro memorizzazione ordinata temporalmente nello storage.
Le registrazioni dei flussi video video vengono effettuate 24 ore al giorno e memorizzate mediante i Recording Server nello Storage, dove vengono mantenute per un periodo di 15 giorni, comunque modificabile da un utente

amministratore per ottemperare a quanto stabilito dal DL 196/93 e successive modifiche, dopodiché automaticamente eliminate.

I flussi video ottenuti dalle telecamere vengono resi disponibili agli utenti in base ai ruoli a loro assegnati. In base al ruolo l'utente sarà abilitato allo specifico trattamento ed avrà accesso agli specifici flussi video di sua pertinenza in quanto provenienti dalle telecamere al ruolo di appartenenza associate. I flussi video memorizzati possono essere esportati all'esterno dell'ODV dagli utenti associati al ruolo di utente Esportatore, per fini forensi o per richieste dell'autorità giudiziaria.

Queste operazioni realizzano le SFR **FRU_FLT.1, FDP_ETC.1, FDP_RIP.1/SD e FDP_RIP.1/sistemi centrali**.

7.6 TABELLA DI SINTESI

La tabella seguente fornisce la sintesi dei SFR soddisfatti dalle funzioni di sicurezza dell'ODV.

	ODV_AC	ODV_AUD	ODV_MGMT	ODV_DP
FAU_GEN.1		X		
FDP_ACC.1	X			
FDP_ACF.1	X			
FDP_RIP.1/SD				X
FDP_RIP.1/sistemi centrali				X
FDP_ETC.1				X
FMT_MSA.1			X	
FMT_MSA.3			X	
FMT_SMF.1			X	
FMT_SMR.1	X		X	
FRU_FLT.1				X

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