



Comune di Carinaro

Provincia di Caserta

Piazza Municipio, 1 – 81032 Carinaro (CE)



PROGETTO DI FATTIBILITÀ TECNICA ED ECONOMICA

CARINARO IN SICUREZZA

Realizzazione del sistema di videosorveglianza territoriale e di rilevamento dei transiti veicolari per la sicurezza urbana – Modalità di presentazione delle richieste di finanziamento a valere sulle risorse finanziarie fissate in 24,5 milioni di euro per l'anno 2024 dall'articolo 1, comma 676, della legge 29 dicembre 2022, n. 197.

IL PROGETTISTA

R.U.P.

Ufficio Tecnico Comunale

IL PROGETTISTA

U.T.C.

ELABORATO

DATA

FIRMA

Relazione Generale

REDATTO

VERIFICATO

APPROVATO

DATA

26/05/2025

Cod. Univoco Progetto

=====

REVISIONE

DATA

AGGIORNAMENTI

SCALA

=====

ELABORATO

NOME FILE

CRN_PFTE_A.01

A.01

Sommario

1.	Premessa	3
1.1.	Normative di riferimento	4
1.2.	Fondi di riferimento	5
2.	Stato attuale degli impianti esistenti	5
3.	Descrizione generale del progetto di videosorveglianza	6
3.1.	Scopo del progetto	7
3.2.	Elenco delle postazioni	8
4.	Sistema centrale della videosorveglianza urbana	9
5.	Centrale Operativa	10
5.1.	Sala Server	11
5.2.	Adeguamento Sala Server	11
5.3.	Allestimento Sala Server	11
5.4.	Sala Regia	12
6.	Elementi Software del Sistema – Sala Server e Monitoraggio	13
6.1.	Piattaforma Software per il Server – Telecamere di Contesto	13
6.2.	Piattaforma Software per il Server – Telecamere di Lettura Targhe	25
6.3.	Autonomia di Archiviazione	32
7.	Rete di trasmissione dati	33
7.1.	Connettività mediante Hiperlan criptata	34
8.	Postazioni periferiche di videosorveglianza	34
8.1.	Telecamera di Lettura Targhe	35
8.2.	Telecamera di Contesto	37
8.3.	Quadri di campo	41
8.4.	Sottosistema di alimentazione	44
8.5.	Struttura di sostegno	45
9.	Future integrazioni	46
10.	Addestramento e affiancamento generale	46
11.	Manutenzione della videosorveglianza	47

1. Premessa

Il Comune di Carinaro intende partecipare alla richiesta di finanziamenti da parte dei Comuni a valere sulle risorse finanziarie fissate in 24,5 milioni di euro per l'anno 2024 dall'articolo 1, comma 676, della legge 29 dicembre 2022, n. 197, secondo le modalità indicate dal decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, adottato ai sensi dell'articolo 1, comma 677, della medesima legge n. 197/2022. A tal proposito intende procedere alla realizzazione di un sistema di videosorveglianza che prevede l'utilizzo di telecamere lettura targa e di contesto, dotandosi di un software di analisi video per il monitoraggio attivo delle aree a rischio al fine di rafforzare le azioni di prevenzione e di contrasto alle forme di illegalità presenti nelle aree urbane del territorio di Carinaro con particolare riferimento alle aree di accesso al territorio. Il sistema prevede oltre all'installazione delle telecamere un sistema di trasmissione dei segnali tramite apparati radio operanti in bande di frequenze libere a 5GHz e una centrale operativa di visione e registrazione.

Il presente Progetto Esecutivo prevede:

- a) l'allestimento di una centrale operativa posta presso il locale esistente del Comando della Polizia Municipale del Comune di Carinaro;
- b) la realizzazione di un'infrastruttura di rete dati proprietaria mediante l'impiego di apparati radio;
- c) l'individuazione di punti di controllo sul territorio di concerto con la Polizia Municipale e le Forze dell'Ordine.

Per le considerazioni di carattere strategico e operativo che hanno condotto alla adozione della soluzione sistemistica di seguito riportata, si rimanda alla Relazione Generale che segue.

1.1. Normative di riferimento

1. D.M. 37/08: “Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n. 248 del 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici”.
2. D.Lgs 9/4/08 n.81 “Attuazione dell’art. 1 della legge 3/8/07 n. 123 in materia di tutela della salute e della sicurezza nei luoghi di lavoro”.
3. Norma CEI 64-8:” Impianti elettrici utilizzatori a tensione nominale non superiore a 1000 V in corrente alternata e a 1500 V in corrente continua”
4. Norma CEI 0-2:” Guida per la definizione della documentazione di progetto degli impianti elettrici”
5. Norma CEI 11-37: “Guida alla realizzazione degli impianti di terra”;
6. Norma CEI 11-17: “Impianti di produzione, trasmissione e distribuzione pubblica di energia elettrica – Linee in cavo”;
7. Norma CEI 23-116: “Sistemi di tubi ed accessori per installazioni elettriche Parte 24: Prescrizioni particolari - Sistemi di tubi interrati”;
8. Norma CEI 20-22: “Cavi non propaganti l'incendio”
9. Norma CEI 20-35: “Cavi non propaganti la fiamma”
10. Norma CEI 64-50: “Edilizia residenziale, guida per l’integrazione nell’edificio degli impianti elettrici utilizzatori, ausiliari e telefonici”.
11. Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Gazzetta Ufficiale n. 99 del 29 aprile 2010).
12. D.Lgs 196/03 “Codice in materia di protezione dei dati personali”.
13. Provvedimento generale “Videosorveglianza”, chiarimenti sull’applicazione del D. Lgs 196/03.
14. Art. 615bis del Codice Penale “Interferenze illecite nella vita privata”.
15. Legge 300/07 “Statuto dei Lavoratori”.

1.2. Fondi di riferimento

Decreto 27 dicembre 2024 del Ministero dell'Interno: Modalità di presentazione delle richieste da parte dei comuni interessati, nonché i criteri per la ripartizione delle risorse stanziare dall'art. 1, comma 676, della legge 29 dicembre 2022, n. 197, così come incrementate dall'art. 3 -ter del decreto-legge 15 settembre 2023, n. 123, convertito con modificazioni dalla legge 13 novembre 2023, n. 159, pari a 19 milioni di euro per l'anno 2024, finalizzate a potenziare gli interventi in materia di sicurezza urbana per la realizzazione degli obiettivi di cui all'art. 5, comma 2, lettera a), del decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48. Le risorse, per l'anno 2024, sono incrementate di euro 5,5 milioni con decreto del Ministro dell'interno del 3 luglio 2024, a seguito del riparto delle somme allocate sul capitolo n. 3000, piano gestionale n. 3, dello stato di previsione del Ministero dell'interno relative alla quota del Fondo di cui all'art. 61, comma 23, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, denominato «Fondo unico giustizia» spettante al Ministero dell'interno.

2. Stato attuale degli impianti esistenti

All'attualità il territorio di Carinaro è provvisto di un impianto di videosorveglianza cittadino che non risulta sufficiente a garantire il monitoraggio delle aree sensibili soggette a fenomeni di criminalità diffusa e predatoria. Con il presente Progetto Esecutivo si intende potenziare il controllo del territorio urbano, fornendo alle Forze dell'Ordine strumenti che gli consentano di:

- a) prevenire fenomeni di criminalità diffusa e predatoria, attraverso servizi e interventi di prossimità, in particolare a vantaggio delle zone maggiormente interessate da fenomeni di degrado;
- b) promozione del rispetto della legalità, anche mediante mirate iniziative di dissuasione di ogni forma di condotta illecita, comprese l'occupazione arbitraria di immobili e lo smercio di beni contraffatti o falsificati, nonché la prevenzione di altri fenomeni che comunque comportino turbativa del libero utilizzo degli spazi pubblici;
- c) promozione del rispetto del decoro urbano, anche valorizzando forme di collaborazione interistituzionale tra le amministrazioni competenti, finalizzate a coadiuvare l'ente locale nell'individuazione di aree urbane su cui insistono musei, aree e parchi archeologici, complessi monumentali o altri istituti e luoghi della cultura interessati da consistenti flussi turistici, ovvero adibite a verde pubblico, da sottoporre a particolare tutela ai sensi dell'articolo 9, comma 3 del decreto legge 15 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48.

3. Descrizione generale del progetto di videosorveglianza

Il comune di Carinaro è già dotato di una Sala CED atta ad ospitare le macchine che sono il “cuore” del sistema di videosorveglianza, che risulta adeguata alle più stringenti ed evolute necessità di sicurezza e adeguatezza tecnico funzionale e pertanto le attività che complessivamente si rendono necessarie risultano essere:

- Adeguamento dell'esistente locale del Comando della Polizia Municipale del Comune di Carinaro in modo da renderlo idoneo ad ospitare una sala;
- Fornitura in opera di un server per la gestione delle telecamere di contesto caratterizzato da un adeguato spazio di memorizzazione video su un dispositivo di storage integrato con almeno 32 TB di spazio a disposizione. Il sistema va dimensionato con complessive 20 licenze per telecamere;
- Fornitura in opera di un server per la gestione delle telecamere di Lettura Targhe caratterizzato da un adeguato spazio di memorizzazione video su un dispositivo di storage integrato con almeno 32 TB di spazio a disposizione. Il sistema va dimensionato con complessive 8 licenze per telecamere;
- Fornitura in opera di una centrale operativa che verrà collocata in un idoneo locale presso il Comando della Polizia Municipale, consistente in n.ro 1 postazione di controllo PC completa di monitor di almeno 27” e da n.ro 2 monitor a parete da 55”;
- Fornitura in opera di una rete di trasmissione video e dati su tecnologia radio Hiperlan, per il trasferimento delle riprese dalle postazioni distribuite sul territorio alla centrale operativa che ha come fulcro il Comando della Polizia Municipale.
- Fornitura in opera n.ro **10** postazioni di monitoraggio da installarsi nel territorio comunale, allestite su pali esistenti degli impianti di Illuminazione Pubblica o su pali di nuova fornitura, (idoneo per l'installazione di telecamere di Lettura Targhe) e completo di tutto quanto necessario per dare l'opera finita a perfetta regola d'arte.

Per quanto attiene le relative ubicazioni e dotazioni si rimanda agli specifici documenti denominati “*CRN_PFTE_B.01 - Relazione Specialistica - Postazioni di Ripresa*” che sono parte integrante del presente progetto.

I sistemi di videosorveglianza rappresentano un valido strumento d'ausilio per le forze dell'ordine nelle attività di controllo del territorio urbano.

Un'analisi delle principali applicazioni dimostra che la videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

- protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici e privati, alla razionalizzazione e miglioramento dei servizi al pubblico volto anche ad accrescere la sicurezza degli utenti;
- protezione della proprietà;
- rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici e privati;
- acquisizione di prove.

L'utilizzo di sistemi di videosorveglianza ha garantito negli ultimi anni differenti e decisivi risultati nelle attività di prevenzione degli eventi di microcriminalità nei territori urbani.

Il livello di prestazione di questi sistemi si è evoluto nel tempo con l'introduzione di nuove tecnologie sia dal punto di vista delle unità di ripresa delle immagini che da quello di trasmissione ed archiviazione delle stesse.

Le modalità di utilizzo e le prestazioni di questi sistemi dipendono direttamente dalla corretta analisi delle esigenze rilevate e da un approfondito studio tecnico sulle tecnologie applicabili.

3.1. Scopo del progetto

La proposta progettuale è finalizzata ad accrescere la sicurezza pubblica, a migliorare le condizioni di vivibilità della città ed aumentare l'efficacia del servizio delle Forze dell'Ordine. Obiettivo generale di progetto è quello di migliorare la sicurezza della città mitigando o rimuovendo i principali problemi dell'attuazione delle politiche per la sicurezza urbana che nel contempo generano disfunzioni e dispersione nel servizio di sicurezza ed un senso di insicurezza diffuso nella comunità cittadina. L'obiettivo è di migliorare l'interoperabilità con le Forze dell'Ordine facendo in modo che le stesse ricevano le immagini delle telecamere di nuova installazione ottimizzando i sistemi di controllo del territorio con l'attività di videosorveglianza ad aree sensibili allo stato scoperte e potenziando la sala di videocontrollo con dotazioni server per l'acquisizione e la gestione delle immagini e delle postazioni di monitoraggio.

La criticità del territorio richiede una copertura adeguata delle aree a vocazione commerciale nel centro urbano con un alto flusso di traffico veicolare e pedonale, dell'area mercatale e dei punti di maggiore transito veicolare e pedonale.

Lo scopo che si è prefissato, quindi, mediante l'installazione del sistema di videosorveglianza con lettori targa automatica, si può riassumere nelle seguenti azioni:

- Prevenzione ai fenomeni di microcriminalità;
- Prevenzione di atti vandalici nei confronti di siti sensibili;
- Rilevazione e ricostruzione di eventi criminosi;
- Controllo le traffico e soste vietate;
- Rilevazione sversamento rifiuti e monitoraggio delle strade periferiche;
- Tutela del patrimonio comunale.

I siti individuati come "sensibili" sono generalmente localizzati in complessi quali parchi, piazze vie del centro storico, stabili comunali, parcheggi, opere di pubblico interesse e di valore storico, luoghi di culto.

3.2. Elenco delle postazioni

La scelta delle ubicazioni dei siti risponde a diverse necessità:

- realizzazione di postazioni comprendenti telecamere di lettura targhe e di contesto in primis nelle zone di accesso al territorio comunale di Carinaro;
- realizzazione di postazioni di Videosorveglianza a servizio della Polizia Municipale con sede individuata dall'amministrazione comunale;
- l'ottenimento di un controllo completo delle vie di accesso al Comune ed avere un favorevole posizionamento geografico ai fini della raggiungibilità radio.

Pertanto, in sede di analisi di fattibilità sono state condotte approfondite analisi circa le ubicazioni dei siti "strategicamente" più rilevanti. Lo studio ha condotto alla determinazione delle seguenti postazioni.

Di seguito si riporta una tabella riepilogativa delle postazioni di ripresa, sia in termini di localizzazione sia in termini di equipaggiamento, da realizzare presso il territorio comunale di Carinaro e meglio dettagliate nell'elaborato "CRN_PFTE_B.01 - Relazione Specialistica - Postazioni di Ripresa" che è parte integrante del presente Progetto Esecutivo:

ELENCO DELLE POSTAZIONI DA REALIZZARE				
ID-PST	Descrizione	Coordinate GPS	OCR	BLT
CED	Sala operativa - Polizia Municipale	Lat: 40°59'20,20"N - Lon: 14°13'1,50"E	-	-
P_01	Via Fiume	Lat: 40°58'52,08"N - Lon: 14°12'51,03"E	1	1
P_02	Piazza Municipio	Lat: 40°59'20,26"N - Lon: 14°12'58,46"E	0	3
P_03	Via Giuseppe Garibaldi	Lat: 40°59'11,76"N - Lon: 14°13'8,20"E	1	2
P_04	Via Fiume	Lat: 40°58'41,64"N - Lon: 14°12'54,28"E	1	2
P_05	Via Francesco Petrarca	Lat: 40°59'2,14"N - Lon: 14°12'49,66"E	0	2
P_06	Via Francesco Petrarca	Lat: 40°58'57,31"N - Lon: 14°12'50,68"E	1	2
P_07	Via Cinque Vie/Papa Giovanni XXII	Lat: 40°59'22,92"N - Lon: 14°13'9,88"E	1	2
P_08	Via Casignano	Lat: 40°59'32,23"N - Lon: 14°13'14,11"E	1	2
P_09	Via Casignano	Lat: 40°59'32,58"N - Lon: 14°13'55,94"E	1	2
P_10	Via Larga	Lat: 40°59'23,41"N - Lon: 14°13'58,20"E	1	2
TOTALE PER TIPO APPARATO			8	20
TOTALE COMPLESSIVO			28	
OCR: Telecamera di Lettura targhe				
BLT: Telecamera contestuale con singolo sensore di ripresa				

Pertanto, il presente Progetto Esecutivo prevede:

- la realizzazione di nr. 10 postazioni di monitoraggio veicolare equipaggiate complessivamente da:
 - nr. 20 telecamere di contesto;
 - nr. 8 telecamere di lettura targhe

4. Sistema centrale della videosorveglianza urbana

Il progetto di videosorveglianza prevede l'installazione di nuove postazioni di ripresa sul territorio della Comune di Carinaro una serie di postazioni dislocate in posti strategici ai fini del monitoraggio di aree sensibili attrezzate **con sistemi di telecamere di contesto e lettori targa collegati con la banca dati del Sistema Nazionale Targhe e Transiti (SCNTT).**

La soluzione progettuale prevede l'adeguamento del locale, messo a disposizione dell'Amministrazione Comunale, al fine di renderlo conforme alle più stringenti ed evolute necessità di sicurezza ed adeguati in termini tecnico funzionale e in linea con il contesto storico culturale a cui è soggetto il locale stesso.

Dal centro sarà possibile recuperare le registrazioni ai fini consentiti dalla legge ed in ottemperanza dei Regolamenti Comunali sulla videosorveglianza.

Le telecamere saranno collegate al centro di monitoraggio e controllo tramite una rete Hiperlan proprietaria. Tale rete è progettata con criteri di resilienza caratteristici di una topologia di rete "a stella" e di robustezza garantiti dall'attivazione di appositi contatori di nuova fornitura destinati esclusivamente all'alimentazione delle postazioni di videosorveglianza urbana e dei siti di raccolta e rilancio dei flussi video denominati "HOP", in modo da poter consentire il monitoraggio continuo di postazioni critiche senza interruzioni del servizio.

Il sistema è progettato come "sistema aperto", nel senso che, con le opportune autorizzazioni, sarà possibile trasmettere le immagini in tempo reale verso altri centri di monitoraggio sovracomunali, quali: Forze dell'Ordine, il sistema DSS della SMA, il SCNTT.

Il progetto prevede, per il comune di **Carinaro**:

- sistema di acquisizione, memorizzazione e visualizzazione ospitato nel CED del Comune.
- sala di controllo dotata di n.ro 1 large display e postazione operatore allocata presso la **Polizia Municipale**;
- n.ro 10 postazioni di avvistamento e rilevazione;
- una rete radio su tecnologia Hiperlan per convogliare le riprese alla sala CED;

Le postazioni sono state allocate, in siti ad alta sensibilità descritti nel documento allegato alla presente relazione descrittiva denominato *"CRN_PFTE_B.01 - Relazione Specialistica - Postazioni di Ripresa"*.

5. Centrale Operativa

La centrale Operativa rappresenta il cuore dell'intero sistema, il luogo in cui fisicamente e logicamente vengono trasmessi, elaborati, gestiti e archiviati i flussi video.

La Centrale Operativa sarà ubicata presso il Comando di Polizia Municipale e sarà sviluppata in due ambiti:

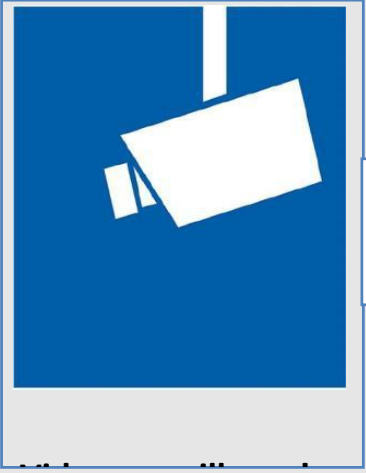
- Una sala controllo (per la visualizzazione e la gestione logica dei dati);
- Una sala apparati (per la gestione fisica e l'archiviazione dei dati).

Per quanto riguarda i requisiti del sistema da realizzare, si devono considerare come cornice di riferimento, le disposizioni di carattere generale contenute nella circolare del Ministero dell'interno del 23 febbraio 2005, n.558/A/421.2/70/456, con le quali si è proceduto alla definizione di linee guida alla luce dei provvedimenti varati in materia dal Garante per la protezione dei dati personali, dapprima con il "decalogo" del 29 novembre del 2000 e, in seguito, con il provvedimento del 29 aprile 2004, oltre al NUOVO CODICE PER LA PRIVACY GDPR.

Inoltre, il sistema di videosorveglianza da realizzarsi presso il territorio comunale dovrà essere conforme con le linee guida alla luce dei provvedimenti varati in materia dal Garante per la protezione dei dati personali ai sensi del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

La registrazione, in particolare, deve poter essere conservata per almeno 7 giorni e accessibile solo agli organi competenti e autorizzati.

I siti video-sorvegliati dovranno essere segnalati da apposita segnaletica conforme a quella riportata *EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020* nel provvedimento del Garante per la Protezione dei Dati Personali.

	LA REGISTRAZIONE È EFFETTUATA DA CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (se applicabile):
	LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI.....
	FINALITÀ DELLA VIDEOSORVEGLIANZA
	È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI A

L'informativa completa sul trattamento dei dati è disponibile:

- presso i locali del titolare (reception, casse, ecc.)
- sul sito internet (URL)...
- altro

5.1. Sala Server

Nella sala apparati saranno convogliati tutti i segnali elettrici e ottici raccolti sul campo.

A tal fine deve essere allestito un nodo di concentrazione e smistamento provvisto di apparati in grado di processare il traffico proveniente (e destinato) all'intera infrastruttura di rete.

Al nodo di concentrazione saranno associati anche tutti i sistemi di gestione dell'intero impianto e i sistemi di storage in grado di memorizzare il traffico secondo le normative vigenti.

5.2. Adeguamento Sala Server

Dovranno essere eseguiti tutti i lavori di adeguamento sia per la parte elettrica, sia per la parte di condizionamento, sia di opere, in particolare:

- Adeguamento elettrico conforme alle normative vigenti;
- Realizzazione cablaggio strutturato per collegare le apparecchiature della sala controllo con i dispositivi che andranno installati nell'armadio rack.

5.3. Allestimento Sala Server

All'interno del rack di sala apparati devono essere forniti, installati e configurati tutti gli elementi "minimi" indispensabili per il corretto funzionamento del sistema.

Oltre al cablaggio passivo per interfacciamento del nodo alla rete di trasporto sarà necessario fornire, installare e configurare gli apparati attivi da alloggiare nell'armadio previsto. Tutti i requisiti indicati sono da intendersi come requisiti minimi. L'offerente potrà proporre soluzioni diverse, purché siano garantiti i parametri funzionali e prestazioni indicati.

L'armadio rack, da ubicare all'interno del locale sopra menzionato, dovrà essere di tipo LAN - 42 U Armadio rack 19" a pavimento, 4 montanti, con porta anteriore in vetro e porta posteriore, dim. 2000x800x800 completo di:

- piastra tetto areata con 2 ventole;
- passacavi orizzontale 19" - 1U;
- Patch panel dati Patch panel estraibili 19" precaricati. 24 connettori RJ45, categoria 5e, fibre supportate 24 UTP, dimensioni 490x240x47 mm, norme di riferimento IEC 60297 - ISO/IEC 11801:ed. 2.2 - 2011 - NF C 20-150;
- pannello di alimentazione per rack 19" - 8 prese francesi o 8 Schuko con interruttore luminoso.

All'interno dell'armadio rack saranno allocati:

- nr. 1 Switch di Centro Stella;
- nr. 1 Firewall;
- nr. 1 Server completo di licenze video e piattaforma software per la gestione delle riprese video provenienti dalle telecamere di contesto dislocate sul territorio comunale di Carinaro;
- nr. 1 Server completo di licenze video e piattaforma software per la gestione delle telecamere di lettura targhe.

5.4. Sala Regia

Il centro di raccolta dati, unico per l'intera architettura di sistema, è ubicato presso il Comando della Polizia Municipale del Comune di Carinaro allestita con nr. 1 postazione di monitoraggio.

La postazione di monitoraggio sarà allestita all'interno del locale sopra menzionato e dovrà essere caratterizzata da:

- nr. 1 Workstation a Servizio delle FFOO per la gestione e videoanalisi del sistema di videosorveglianza sia per quanto concerne le riprese video delle telecamere di contesto sia per la gestione delle targhe con interfacciamento al sistema SCNTT. La Workstation dovrà essere completa di:
 - piattaforma software;
 - mouse;
 - tastiera;
 - monitor LED da 27"
- nr. 2 Monitor a LED 55";

6. Elementi Software del Sistema – Sala Server e Monitoraggio

6.1. Piattaforma Software per il Server – Telecamere di Contesto

La soluzione software di videosorveglianza per la gestione delle telecamere di contesto supporta il personale addetto alla sicurezza e consente la gestione dei dispositivi configurati in tempo reale, evidenziando gli eventi degni di attenzione che via via si verificano. La piattaforma software dovrà essere installabile su Workstation con sistema operativo Windows-based, sia su macchina “fisica” che in ambiente virtuale, la suite dovrà consentire di gestire da 1 fino ad un numero teoricamente illimitato di dispositivi IP, configurabili e gestibili da software client proprietario, sia in rete locale che da remoto, attraverso LAN o WAN.

Funzionalità principali della soluzione:

- integrazione dispositivi di videosorveglianza e sicurezza mediante SDK, Onvif (Profile S, G) e RTSP, HTTP/CGI;
- mediante client software proprietario, utilizzabile da remoto ed in locale, garantisce la visualizzazione delle telecamere, la ricezione di eventi, l'interazione con dispositivi di terze parti attraverso protocolli integrati, la configurabilità di tutti i dispositivi, dei parametri di sistema e la consultazione delle registrazioni;
- centralizzazione dei sistemi. Mediante una sola istanza del client proprietario, l'utente, dopo aver effettuato l'accesso, potrà gestire simultaneamente un numero teoricamente illimitato di sistemi aventi licenza adeguata;
- dovrà essere consentito un numero teoricamente illimitato di connessioni contemporanee dai client verso il server;
- dovrà essere consentito il controllo remoto/locale di un numero teoricamente infinito di server, simultaneamente, da ogni singolo client;
- le telecamere del sistema dovranno essere visibili anche su Browser Web cross-platform (Internet Explorer, Chrome, Firefox, Safari, etc.). Per tal funzione non dovrà essere richiesto il download di alcun plug in;
- la gestione video live e registrato dovrà essere eseguita anche mediante l'impiego di app installabile su dispositivi ios e Android, scaricabile gratuitamente presso i relativi store. L'applicazione dovrà consentire inoltre la ricezione di Notifiche Push (su evento) e condivisione degli eventi stessi attraverso le piattaforme di messaging installate sui dispositivi;
- le registrazioni dovranno essere gestite 24/24h, programmabile su base oraria/settimanale o su evento;
- gestione dello Storage;
- riproduzione simultanea di più flussi video registrati;
- accesso istantaneo alle registrazioni più recenti senza necessità di effettuare ricerche o cambiare ambiente;
- gestione Sub-stream delle telecamere IP per visualizzazione Live e/o archiviazione registrazioni e per attivazione analisi video embedded (Area Violata, Oggetto rimosso/abbandonato);
- registrazione su supporto storage di rete (NAS, SAN, shared paths, etc.);
- controllo PTZ: brandeggio, preset e sequenze con gestione manuale o automatizzata;
- gestione “dewarping” proprietaria per telecamere con ottica Fisheye attivabile sia sul flusso video live, che nel flusso video registrato;
- notifica eventi via Log, video, audio, email, output;
- ricerca eventi per data, tipologia di evento, dispositivo, dettaglio evento;

- forensic search disponibile per soluzioni di analisi video integrate certificate
- ricodifica video hardware @low-res a carico del Server, per gestione Live e registrato;
- RTSP Streaming Output: ricodifica ed invio flussi video dal VMS a sistemi di terze parti;
- Audio IN/OUT (disponibile per dispositivi Onvif);
- Webdevice: browser web integrato;
- External I/O e Input External State (ricezione/invio HTTP/CGI script);
- Privacy Mask (offuscatura) rimovibile da utente autorizzato sia da flusso video live che da flusso video registrato;
- gestione dispositivi via mappe grafiche dinamiche;
- Autenticazione utente mediante Microsoft Active Directory;
- assegnazione telecamere per utente (Live e registrato);
- User Policies: personalizzazione diritti a gruppi di utenti;
- riconoscimento di oggetti rimossi e/o abbandonati;

Autorizzazioni:

- la connessione da remoto dovrà essere protetta con autenticazione username e password, IP statico oppure URL associato ad IP dinamico ed unica porta TCP (configurabile).
- dovrà essere consentita la creazione di un numero illimitato di utenti.
- la soluzione software dovrà avere la possibilità di gestire differenti livelli di autenticazione permettendo di compiere differenti operazioni sul sistema, ad esempio:
 - o “Administrator” totale controllo e parametrizzazione del sistema.
 - o “PowerUser” visualizzazione delle telecamere in tempo reale, consultazione degli eventi recenti e quelli archiviati, movimentazione telecamere PTZ.
 - o “User” visualizzazione telecamere in tempo reale e consultazione eventi recenti.
- integrazione con Microsoft Active Directory.
- possibilità di definire ciascun User o Power user come “Supervisore”. Dopo aver inserito le proprie credenziali, un supervisore dovrà essere in grado di concedere a un altro utente la possibilità di effettuare esportazioni video.
- matrice per la modifica dei privilegi da abbinare ad Administrator, Power User e User.
- matrice per la l’assegnazione delle telecamere visualizzabili, sia a livello di live che a livello di registrazioni, per gli utenti di tipo “Power User” e “User”.

Il sistema dovrà essere dotato di un tracciamento delle azioni effettuate dagli utenti. Come da normativa vigente, l’archiviazione di tali dati è di 180 giorni.

La funzione di “*tracciamento*” consente agli amministratori di sistema di effettuare ricerche atte a conoscere alcuni comportamenti e situazioni “generate” dagli utenti, tra cui Login/Logout, Aggiunta/Rimozione Utenti, Aggiunta/Rimozione Dispositivi, Play Registrazioni, Play Eventi, Cancellazione Registrazioni, Cancellazione Eventi.

Per ognuna delle azioni sopra citate dovrà essere possibile visualizzare:

- Data e ora dell’azione
- Nome Utente
- Tipo utente
- Azione
- Descrizione

Vi dovrà essere la possibilità di esportare i Log in formato standard .csv.

Gestione sorgenti video

La soluzione software per la gestione delle telecamere di contesto dovrà essere **“aperta”** e, dunque, compatibile con oltre 20000 dispositivi IP di Brand di vario genere, pertanto, la soluzione dovrà essere certificata e conforme ai protocolli Onvif profile S e G, nonché certificata e conforme al protocollo RTSP.

Il sistema dovrà consentire la ricerca automatica delle telecamere in rete mediante protocollo UPnP e riuscire a riconoscere i flussi video provenienti dai dispositivi di ripresa mediante protocolli video H.265, H.264, MJPEG, MPEG-4 e MxPEG.

Il software di videoanalisi dovrà consentire una gestione e configurazione del flusso video indipendente per ogni canale. La gestione flusso video in visualizzazione Live è indipendente dalla gestione flusso video in modalità accesso alla registrazione. Inoltre, la trasmissione flussi video Live dovrà essere configurabile per ogni singolo canale, con la possibilità di selezionare una specifica visualizzazione sia per la singola postazione, oppure configurare un “profilo di default” per tutti i client collegati al sistema. I profili di visualizzazione disponibili dovranno essere: Main, Substream, MJPEG, MPEG4, Hardware H.264, Snapshot (se attivato plug-in analisi video proprietario).

La soluzione software dovrà essere in grado di gestire:

- telecamere con obiettivo fisheye, mediante de-warping proprietario applicabile sia sul flusso video live, che sul flusso video registrato;
- telecamere motorizzate PTZ IP.

Il software di gestione delle telecamere contestuali dovrà possedere le funzioni **“Preset”** e **“Sequenze”** configurabili e personalizzabili dal client video, nello specifico:

- sequenze di Preset programmabili per numero di passaggi e tempo di permanenza (sec) per ogni posizione
- indipendenza delle sequenze di Preset per ogni canale
- sequenze programmabili mediante la successione di più Preset (es. per creazione di Ronda)
- sospensione preset in caso di preset/sequenza richiamati da Input elettrici (modulo I/O opzionale o a bordo di dispositivi integrati), virtuali o External I/O (cgi/http)
- movimentazione delle telecamere PTZ in caso di Motion detection proveniente da altre telecamere o da input elettrici (modulo I/O opzionale o a bordo di dispositivi integrati), virtuali o External I/O (cgi/http)

Per ogni canale viene data la possibilità di attivazione/disattivazione del video attraverso un input, fisico o “virtuale”, configurato sul sistema.

Registrazione/Consultazione Filmati

Il sistema di gestione dovrà essere dotato di certificato di non manipolabilità delle registrazioni in maniera tale che può registrare le immagini sia su disco locale installato sulla workstation che su dispositivo/percorso di rete (es. NAS, SAN, etc.)

La soluzione software dovrà gestire e acquisire le immagini archiviate sui supporti di memorizzazione installati sui dispositivi Onvif G compliant mediante la funzionalità Edge Recordings retrieval. L'archiviazione delle immagini dovrà eseguirsi in continuo 24/24h o potrà essere programmato mediante calendario, indipendente per ogni canale e per tipo di registrazione.

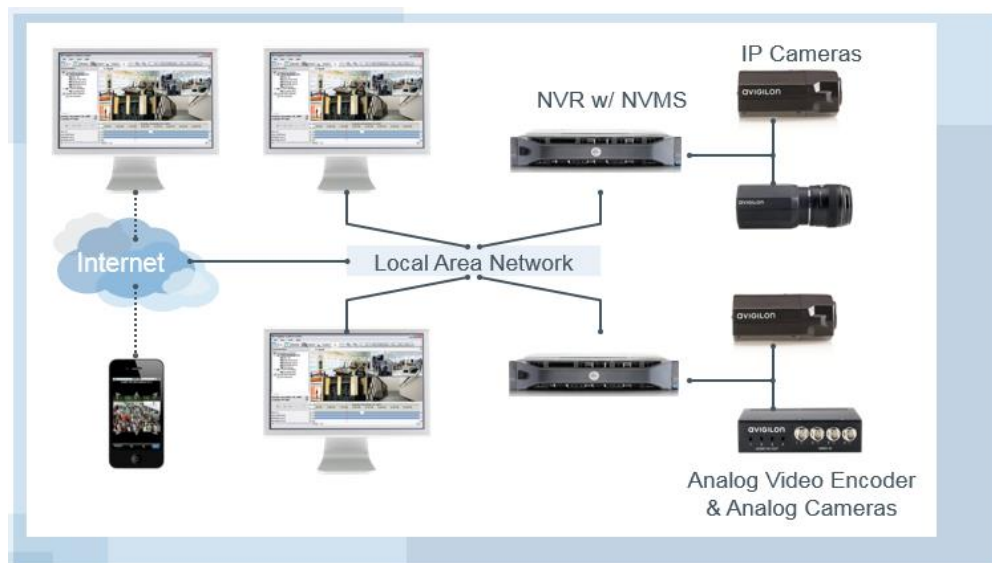
Il calendario dovrà essere programmabile giornalmente nelle 24h e dovrà dividersi in programmazione settimanale e giornaliera per ogni singolo canale.

La modalità di archiviazione dovrà avere la possibilità di poter essere impostata in modalità “*su evento*” qualora siano attivate le funzionalità di analisi video proprietarie tale da consentire l'archiviazione solo a seguito di un evento impostato ed identificato successivamente dal sistema di gestione.

La soluzione software dovrà avere la possibilità di poter archiviare tracce audio.

Per ogni flusso video in registrazione vi dovrà essere la possibilità di impostare uno dei seguenti encoder: Main, Substream, MPEG-4, MJPEG e Hardware H.264 e, per ogni flusso video, vi dovrà essere data la possibilità di allocare uno specifico spazio su disco, con funzione di auto-cancellazione, attivabile in automatico dal sistema al raggiungimento dello spazio allocato, o in base al numero di giorni di anzianità della registrazione.

L'architettura generale che deve implementare è rappresentata in figura seguente.



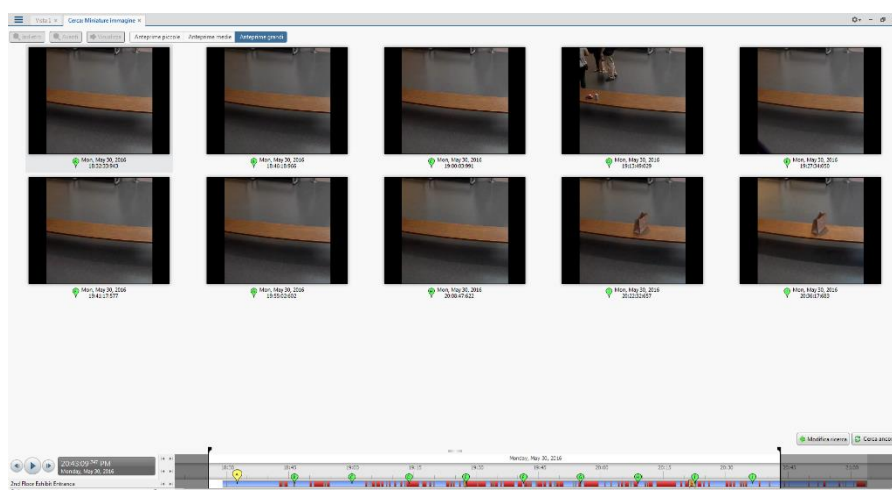
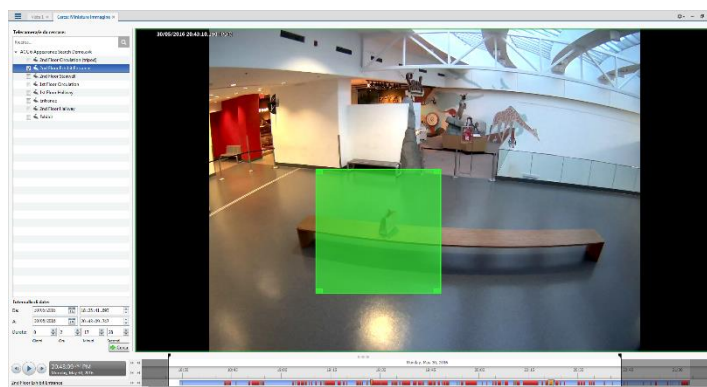
Il sistema consente agli operatori di visualizzare le registrazioni mentre il sistema visualizza immagini live ed eventualmente registra nuovi eventi. Per ogni flusso video in registrazione vi vi dovrà essere data la possibilità di impostare un tempo di registrazione pre e post evento (600 secondi max). Questo range temporale corrisponderà alla durata della registrazione salvata sul disco in caso di attivazione della funzione di registrazione su evento, così come corrisponderà alla durata del video corrispondente all'evento, quando esso sarà visualizzato dall'operatore dopo la sua presa in carico.

La soluzione software dovrà consentire di effettuare la ricerca delle registrazioni grazie all'indicazione della data e dell'orario e/o in base alla selezione di dispositivi di cui si vuole effettuare la ricerca delle registrazioni in modalità Automatica (dispositivo presente sul layout), Manuale (selezionato dall'utente).

Il sistema consente di specificare, ed evidenziare poi nel risultato della ricerca, la presenza di uno o più specifici tipologie di evento, così come un “parametro evento”, come ad esempio una descrizione o una parola chiave.

Al video registrato vi dovrà essere la possibilità di effettuare zoom digitale, Play/Reverse Play/Pause/Stop dei filmati, avanzamento/arretramento fotogramma per fotogramma, velocità ridotta o accelerata, skip ad evento precedente/successivo (se presenti).

Il sistema di gestione dovrà disporre della funzionalità “*Smart Search*”, che consiste nel poter cercare e visualizzare eventi in una porzione di video registrato, all’interno di un’area definita. Lo “*Smart Search*” dovrà essere basato sull’analisi video (Area Violata, Oggetto Rimosso/Abbandonato, etc.), le cui informazioni sono archiviate nel flusso di registrazione principale. La funzione “*Smart Search*” dovrà essere attivabile solo per quei canali in cui è attiva l’analisi video nel periodo selezionato.



Il sistema di gestione dovrà disporre della funzionalità “*Forensic Search*”, che consiste nel poter cercare e visualizzare eventi in una porzione di video registrato e definire una “*parola chiave*” che caratterizza l’evento desiderato verificatosi all’interno di un’area definita dall’utente. “*Forensic Search*” dovrà essere disponibile sui flussi video su cui è attivata l’analisi video, le cui informazioni sono archiviate nel flusso di registrazione principale.

Per i flussi video registrati dovrà essere disponibile l’esportazione in formato .mkv o .mpeg4. Il sistema dovrà consentire di esportare, assieme alle registrazioni in formato Nativo (proprietario) il client in modalità “eseguibile”, chiamato Next Portable. L’esportazione in formato proprietario dovrà essere disponibile per profilo utente di tipo “Administrator” o “Power User”. Si dà modo anche all’utente di ruolo “user” di potere eseguire l’esportazione in formato proprietario previo inserimento di password da parte di un utente “Supervisore” opportunamente configurato in precedenza. Inoltre, vi dovrà essere la possibilità di consultare le registrazioni in formato proprietario anche su supporti esterni di backup.



L’esportazione metadati, timestamp, area di privacy e tracce audio dovrà essere disponibile ed attivabile sulla base del profilo utente collegato e in relazione al formato di esportazione scelto. Mentre, Aree di Privacy potranno essere rimovibili dal video esportato solo da profilo utente autorizzato.

Opzioni di visualizzazione

Il sistema dovrà consentire di configurare un numero potenzialmente illimitato di layout di visualizzazione delle telecamere, ognuno dei quali configurabile in maniera indipendente e popolato da telecamere, mappe, periferiche, pagine web, sistemi di terze parti integrati. Se configurate, in maniera visuale ed anche uditiva è possibile evidenziare in tempo reale gli eventi generati dai suddetti dispositivi le relative notifiche.

La visualizzazione dovrà dare la possibilità di creare layout di visualizzazione “*Locale*”, ossia utilizzabile e salvato solo sul sistema pc client su cui si sta creando il layout, oppure “*Remoto*”, ovvero condiviso e gestibile da altre postazioni dotate del client software proprietario OMNIA. Ogni layout configurabile in termine di numero di numero di “frame”, detti anche riquadri, attraverso delle combinazioni predefinite (1, o 2x2, 3x3, 4x4, 5x5, 6x6, 7x7) oppure custom dove l’utente autorizzato può decidere il numero di colonne X ed il numero di righe Y che dovranno essere presenti.

Mediante la funzione “*drag-and-drop*” dal menu ad albero verso il Layout configurato, è possibile visualizzare flussi video, gestire dispositivi e mappe configurate, in tempo reale, per visualizzare video, modificare o accedere alle informazioni disponibili ed in generale interagire con essi.

Il sistema dovrà disporre della modalità di visualizzazione a “Schermo Intero” ed avendo configurato più layout, dovrà essere possibile attivare una modalità di “*Rotazione automatica*” dei Layout, denominata “*Ronda*”, che di fatto porta in evidenza uno dopo l'altro i layout sulla base degli intervalli di tempo impostati.

La visualizzazione dovrà disporre della funzionalità che permette di spostare uno o più layout su finestre e monitor secondari:

- modalità Popup su Evento o Ciclica con possibilità di definire un tempo di chiusura automatico del flusso video basato su tempo o su presa in carico evento
- per ogni telecamera presente sul layout è possibile accedere alla funzione Instant player. Mediante la funzione Instant Player si possono visualizzare le registrazioni più recenti (default 1 min.) senza dover accedere all'ambiente di Registrazione così come è possibile attivare la comunicazione audio bi-direzionale con il dispositivo, se opportunamente configurato.



Display

Per ogni canale video l'utente dovrà avere la possibilità di abilitare tre modalità di visualizzazione:

- *Reale*, ovvero il flusso video come fornito dalla telecamera fatto di immagini in tempo reale in bianco e nero, a colori o gradienti termici.
- *Elaborata* che mostra quello che il sistema elabora (bianco e nero)
- *Sovrapposta* ovvero è l'immagine reale in cui è stata sovrapposta l'immagine elaborata.

Inoltre, per ogni canale dovrà essere possibile abilitare la visualizzazione di dettagli in sovraimpressione, riportanti informazioni sugli oggetti che si trovano all'interno della scena:

- Perimetro in pixels o metri (feet nella versione Americana) in base all'attivazione della prospettiva
- Area in pixels² o metri² (feet² nella versione Americana) in base all'attivazione della prospettiva
- Fattore di forma (Perimetro/Area)
- Velocità

- Bounding Box
- Baricentro
- Traiettoria
- Zone Sensibili

Log Eventi

Il log degli eventi dovrà mostrare gli eventi relativi all'immagine selezionata o a tutti i server collegati, fornendo una segnalazione visiva immediata al verificarsi di un evento rilevante.

L'evento rimarrà con lo stato "*aperto*" fino all'intervento dell'operatore. Mentre, quando l'evento viene preso in carico dall'operatore lo stato diventa "*chiuso*".

La riga di log viene aggiornata con il nome, data e ora di chi ha preso in carico l'evento e dovrà essere possibile contrassegnare ogni evento come "Bookmark".

La riga di log può contenere:

- Note inserite da utenti autorizzati, indicanti il nome dell'utente e data/ora dell'inserimento.
- processi:
 - o alta priorità;
 - o media priorità;
 - o bassa priorità;
 - o in lavorazione;
 - o segnalato;
 - o assegnato;
 - o non assegnato;
 - o rimandato;
 - o niente da segnalare;
 - o chiuso.

Inoltre dovrà essere possibile definire

- un colore specifico per ogni tipologia di evento/dispositivo;
- quali eventi vedere visualizzati nel log degli eventi, per ogni dispositivo configurato;

Il log degli eventi può essere esportato in formato ".csv"

Notifica eventi

Gli eventi rilevati potranno essere notificati in:

- Visiva
- Popup
- Uditiva
- Output
- E-mail
- SMS (optional)
- Notifiche Push (App Mobile)

La notifica Visiva consiste nel lampeggio di un riquadro rosso attorno alla vista allarmata (se la vista è sullo schermo) e di una riga di log (anche se la vista non è a monitor) con informazioni su:

- Preferito
- Server
- Dispositivo
- Descrizione dell'evento
- Data e Ora
- Stato
- Processato
- Username
- Tempo di presa visione
- Tipo di file
- Note

La notifica sonora dovrà prevedere la possibilità di scegliere tra diversi allarmi sonori predefiniti, oppure attivando il suono prodotto dal buzzer della scheda madre

Plug-in Area Violata e Oggetto Abbandonato/Rimosso

Il software di gestione dovrà avere la possibilità di poter essere integrato e predisposto per poter gestire funzioni aggiuntive, anche mediante l'attivazione di plug-in, fino a 32 zone configurabili e analizzabili dal sistema per ogni canale video.

La soluzione software dovrà avere la possibilità di associare un Output a ciascuna delle aree di motion per attivare la movimentazione di telecamere PTZ (preset e/o sequenze), o per creare logiche di funzionamento tra diversi dispositivi. Di seguito si riportano alcuni filtri che dovranno stabilire i criteri per la rilevazione dell'evento:

- Eventi Brevi (Sec.)
- Tempo Minimo Tra Due Eventi (Sec.)
- Area (%) - Minima
- Area (%) - Massima
- Larghezza (Pixels e Metri) - Minima
- Larghezza (Pixels e Metri) - Massima
- Altezza (Pixels e Metri) - Minima
- Altezza (Pixels e Metri) - Massima
- Isteresi (Frames)
- Filtro Distribuzione Pixel
- Persistenza (%)
- Sensibilità (%)
- Definizione
- Filtro rimozione blob (Area Min, Perimetro Min)
- Range fattore di forma (perimetro/area)
- Regole di fusione delle blob (area min di sovrapposizione)
- Corona virtuale aggiuntiva alle bounding box

Aree di Privacy

Il sistema dovrà consentire di configurare, su ogni canale, fino a 32 aree di Privacy aventi sfocatura di dimensione regolabile. La soluzione software potrà consentire di rimuovere la sfocatura del filtro Privacy per la protezione sia dal video Live che dal video registrato, solo se in possesso delle necessarie autorizzazioni e password di utente di livello Administrator.

Periferiche

Il sistema dovrà offrire la possibilità di configurare dispositivi diversi dalle sorgenti video, chiamati Periferiche, che attraverso una modalità I/O (Input/Output) danno la possibilità di beneficiare di numerose funzionalità, oppure interagire con sistemi di terze parti. Tali sistemi possono essere fisici, come ad esempio moduli I/O o supporto di I/O a bordo telecamere, oppure software.

Tramite le suddette Periferiche di I/O viene data la possibilità di creare combinazioni programmabili tra un input e più output per comandare in modo flessibile diversi sottosistemi. La soluzione software dovrà offrire:

- la possibilità di configurare External I/O ed Input External State, i quali possono inviare e/o ricevere comandi predefiniti http/cgi con dispositivi di terze parti per generare e ricevere eventi o attivare funzionalità.
- la configurazione illimitati moduli. La rilevazione del numero degli ingressi e delle uscite avviene automaticamente.
- la concessione, mediante GUI, monitorare lo stato degli ingressi e modificare lo stato delle uscite.

Integrazione analisi video a bordo telecamere Bosch

La soluzione software dovrà integrare gli algoritmi di analisi video Bosch IVA (Intelligent Video Analytics) ed EVA (Essential Video Analytics), chiamati TASK, ricevendone gli eventi e consentendo di associarli al video della telecamera. La configurazione degli algoritmi di analisi video deve essere precedentemente eseguita sulla telecamera stessa, mediante l'interfaccia web del dispositivo.

Mediante interfaccia video dovrà essere sufficiente immettere le credenziali del dispositivo affinché il sistema possa rilevare automaticamente gli algoritmi configurati nella periferica in questione, dando all'utente la possibilità di selezionare quali eventi ricevere.

Dovrà essere possibile “marcare” le registrazioni con gli eventi generati dalle TASK Bosch, sarà necessario impostare la Periferica Bosch Task configurata come “Input Allarmante” sulla telecamera corrispondente.

Se sulla telecamera sono presenti più task di analisi in modalità “AND”, dovrà essere possibile definire sulla telecamera l'invio di un comando CGI verso il VMS (un opportuno External I/O dovrà essere configurato) che consentirà di ricevere un evento generato dalla combinazione degli eventi, sulla base delle logiche configurate sul dispositivo stesso.

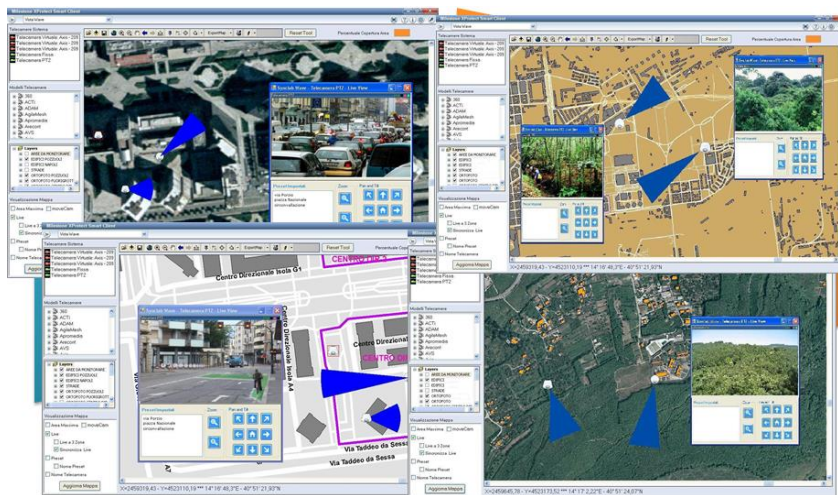
Mappe grafiche

La soluzione software dovrà essere configurata con un numero teoricamente illimitato di Mappe grafiche multilivello. L'immagine di riferimento della mappa dovrà essere di tipo statico, ed dovrà essere possibile utilizzare immagini in formato standard .bmp, .gif, .png e .jpeg

Ciascuna mappa può essere configurata per ospitare e consentire all'operatore di gestire tutti i dispositivi configurati attribuendo icone e FOV (field of view) personalizzabile per ogni dispositivo

L'attribuzione del nome e proprietà visive dovranno essere personalizzabile per ogni dispositivo offrendo la possibilità di visualizzare l'immagine o lo stato del dispositivo direttamente da mappa, in tempo reale, al passaggio del mouse sulle icone relative.

Per i dispositivi video, si dovrà utilizzare una funzione del tipo *"Instant player"* che consiste nel lampeggio delle icone, di durata configurabile, in concomitanza di eventi associati al dispositivo. Al doppio click sull'icona viene visualizzato l'ultimo evento verificatosi, nel relativo ambiente delle registrazioni.



Open Connector

La piattaforma software dovrà essere integrabile per l'interoperabilità tra sistemi, apparecchiature ed applicativi di diverso tipo, mediante protocolli standard. Il software dovrà consentire l'integrazione di dispositivi di terze parti in protocollo xml e comandi http/cgi, in modalità POST. Per ogni dispositivo integrato è possibile riceverne eventi, associare ad esso telecamere, webdevice e Periferiche, in modo da legare l'evento stesso a uno o più dispositivi configurati sul sistema.

SDK, documentazione e software "Simulator" sono fornibili gratuitamente ai partner.

Server Failover (predisposizione)

La piattaforma software dovrà essere dotata di una soluzione di ridondanza automatica (failover o hot backup). In caso di malfunzionamento del server principale dove risiede il Video Management System, il software dovrà prevedere un meccanismo di avvio automatico di un server secondario che fino a tale momento non è attivo. Il server secondario si attiva automaticamente e diventa accessibile con la stessa configurazione del server principale.

Security Connector (predisposizione)

Il software di gestione dovrà essere predisposto e integrabile con Plug-in che consentono di gestire un'ampia varietà di sistemi di sicurezza IP, come centrali di allarme antintrusione, sistemi di rivelazione incendio così come dispositivi che trasmettono allarmi mediante protocollo Modbus.

I plug-in dovrà prevedere un software dedicato, installabile su sistemi operativi Windows e su macchina virtuale. Il software dovrà essere dotato di una propria interfaccia software.

La soluzione software impiegata per la videoanalisi dovrà essere predisposta per un upgrade che consentirà di eseguire una videoanalisi più spinta in grado di:

- eseguire un'analisi video avanzata con filtri temporali, dimensionali, taratura della sensibilità e persistenza, regolazione del Background, ed include Smart Search. Inoltre, grazie all'algoritmo di Privacy Masking proprietario, l'offuscamento può essere rimosso anche dal video registrato.
- in caso di rilevato malfunzionamento di un percorso di registrazione, il sistema provvede a riallocare automaticamente le registrazioni su una porzione pre-configurata di un altro percorso funzionante.
- ridondanza server, che prevede la commutazione automatica verso uno o più sistemi in standby, affinché il nuovo dispositivo rimpiazzhi quello non più funzionante. (predisposizione)
- installabile su Server dedicato e applicabile su tutte le telecamere IP, pensata per le applicazioni più complesse, indoor e outdoor, offrendo inoltre funzionalità di Forensic Search (predisposizione)
- consente al VMS di registrare simultaneamente due flussi video, anche di qualità diversa, su due diversi supporti storage, siano essi installati sul Server o percorsi di rete.

6.2. Piattaforma Software per il Server – Telecamere di Lettura Targhe

La suite integrata per la Polizia Municipale al fine di poter gestire i portali di lettura targhe dovrà essere una piattaforma software compatibile con le più diffuse telecamere di lettura targhe ANPR-OCR, certificata ISDP:10003, che integra algoritmi d'intelligenza artificiale per il riconoscimento di marca, modello, tipo, colore, classe ambientale. Una soluzione completa, aperta, scalabile, utile alla Polizia Municipale per una efficace soluzione di sicurezza urbana integrata, finalizzato alla sicurezza stradale e alla prevenzione e repressione dei reati.

La piattaforma software oltre ad essere predisposta per l'interconnessione con la banca dati del Sistema Nazionale Targhe e Transiti (SCNTT), dovrà essere dotata di tutte le opportune licenze "lato comune" necessarie per l'interconnessione con il sistema SCNTT che non dovrà prevedere costi periodici a carico dell'Amministrazione Comunale.

Il software avanzato per la gestione e l'analisi delle targhe, certificato ISDP10003, a supporto del controllo delle infrazioni stradali delle indagini dovrà essere a zero canoni e quindi non dovrà prevedere dei costi ricorrenti per l'Amministrazione Comunale.

Funzionalità:

La piattaforma di Lettura Targhe dovrà essere un software operativo di gestione dei portali e dispositivi OCR di lettura targhe per la sicurezza urbana, stradale, analisi del traffico, contrasto della criminalità ed alla prevenzione e repressione dei reati. Il software si dovrà avere la possibilità di potersi collegare alle differenti banche dati Ministeriali e Statali come SCNTT. Inoltre, dovrà essere una soluzione aperta e compatibile con qualsiasi tipo di telecamere OCR standard di mercato e interabile con i più diffusi sistemi VMS di videoregistrazione digitale (Milestone, Genetec, Exacq, Qnap).

La piattaforma dovrà essere completo di APP per PC, Tablet e cellulari; è provvisto di moduli e algoritmi intelligenti di analisi video (Marca e Modello, Tipo, Colore e Classificazione ambientale dei veicoli) utili per soddisfare tutte le esigenze degli operatori di Polizia Locale e Forze dell'Ordine.

L'intera suite dovrà essere Certificata ISDP10003, privacy by design e privacy by default, a garanzia della diligenza con cui la soluzione è stata sviluppata a tutela della Privacy e nel rispetto di quanto richiesto dal regolamento GDPR.



La piattaforma di controllo targhe dovrà consentire di collegare tra loro portali eterogenei di lettura targhe – senza interferire o sostituirsi alla soluzione in possesso; senza alcuna modifica all'impianto; mantenendo in uso il software esistente che permette la connessione e sostiene la condivisione delle informazioni tra i comandi di Polizia, per un sistema di sicurezza territoriale realmente integrato, col vantaggio di:

- A) aumentare il contrasto alla criminalità e alla repressione e prevenzione dei reati;
- B) risparmiare tempo e impiego di personale per l'estrapolazione dei dati uso indagine.



Controllo:

La soluzione software che oltre al processo di accertamento delle infrazioni, dovrà possedere anche funzionalità intrinseche di controllo delle connessioni dati tra centrale operativa e telecamere (varchi). I controlli principali dovranno essere:

- controllo automatico della **copertura assicurativa e della revisione dei veicoli**, tramite collegamento alla banca dati del Ministero dei Trasporti e delle Infrastrutture;
- controllo dello stato delle telecamere sia da pannello che da Mappa;
- controllo dello stato live delle telecamere grazie a funzione live e check control (Live, Cps, Ftp, Vpn) per la verifica del funzionamento dell'intero sistema;
- verifica continua della connessione dati delle telecamere di lettura targhe con eventuale aggiornamento dei transiti registrati su memoria interna alla telecamera in caso di perdita del collegamento temporaneo della rete;
- possibilità di collegamento verso altre banche dati per un controllo manuale (es: banca dati Ania);

Gestione:

Il software di Lettura Targhe dovrà, quindi, gestire codici alfanumerici, siano essi provenienti da telecamere di lettura targhe, da lettori container e/o tabelle merci pericolose: dati che vengono memorizzati all'interno di un database SQL integrato nella suite software. Una soluzione che rende la piattaforma software molto veloce nella ricerca delle informazioni e delle relative immagini anche su grandi volumi di dati memorizzati. Dovrà presentare le seguenti funzionalità:

- gestione credenziali di accesso e utenti multipli (in HTTPS) con la definizione dei permessi e privilegi utenti (allarmi, telecamere, liste di competenza) separati utente per utente;
- resa obbligatoria l'impostazione di una scadenza per gli utenti per questione di sicurezza (cambio password e trasferimenti);
- possibilità di esportare gli ultimi log;
- modulo "*report*" per l'invio automatico di statistiche dei transiti e ambientali;
- gestione di utenti multipli (in HTTPS) con credenziali di accesso;
- gestione multi dispositivo (PC, tablet, cellulari, etc.);
- gestione sia in modalità centralizzata sia in modalità multi siti/impianti, con distribuzione delle risorse e degli allarmi verso specifici utenti;
- gestione multi dispositivi OCR: lettura targhe, container, merci pericolose;
- gestione liste (white/black, no list, etc.) con importazione delle liste o relativa esportazione;
- gestione degli allarmi: invio email, Snapshot, richieste HTTPS; attivazione relè; esecuzioni programmi esterni .exe; segnalibro dell'allarme su software di videoregistrazione VMS come Milestone, Genetec etc.; segnalazione su APP e TELEGRAM; **segnalazione in sintesi vocale su terminali radio Motorola e Tetra (Hytera)**;

- gestione della privacy attraverso auto cancellazione dei dati e delle immagini dopo un certo periodo temporale, come richiesto dal Garante della privacy;
- gestione delle registrazioni su server locali o su NAS remoti;
- gestione della sicurezza tramite standard HTTPS;
- gestione delle informazioni su database integrato (già installato) o su DB esterni MySQL;
- gestione automatico del backup del database;
- gestione delle liste (white/black, no list) con funzionalità di allarme;
- **Black List:** segnalazione multipla su lista personale, importata o scaricata da database;
- gestione di un numero illimitato di liste;
- possibilità d'importare banche dati in formato standard CSV (Excel);
- gestione di uno o più banche dati interne (white o black) personalizzate e/o proprietarie;
- gestione degli allarmi con azioni multiple;
- personalizzazione dell'invio degli allarmi specificando gli utenti e i varchi di competenza;
- partizione territoriale: permette di suddividere i varchi per aree e utenti di competenza, secondo diritti specifici a seconda della tipologia di allarme;
- esportazione delle notifiche e dei transiti (codici/targa) delle ricerche in formato CSV, PDF e di tutte le immagini corrispondenti (comprese le contesto ove presenti);
- registrazioni su server locali o su NAS remoti;
- possibilità di assegnare alle targhe in lista una validità per fasce orarie;
- possibilità di memorizzazione del database su disco dedicato;
- salvataggio sincronizzato di: metadati e immagini cattura codice/targa e di contesto.

Comunicazione:

La comunicazione è un aspetto importante della soluzione software, pertanto, la soluzione proposta dovrà inviare comunicazioni verso gli utenti abilitati in base al criterio di competenza. I dispositivi di ricezione delle comunicazioni possono essere:

- tablet;
- smartphone;
- smart watch;
- PC portatili e/o fissi;
- software di videosorveglianza VMS o applicativi di terze parti;
- radio di servizio.

Il software non dovrà limitarsi a trasmettere: allarmi sonori e inviare immagini, ma dovrà possedere la funzionalità di *vocal speaker* in grado di comunicare vocalmente il numero di targa e la tipologia d'allarme in corso.

Un' ulteriore funzione è la possibilità di trasmettere delle immagini e delle informazioni direttamente sullo schermo dello smart watch, per essere avvisati per esempio dell'ingresso di veicoli rubati o veicoli segnalati, ed inoltre dovrà fornire:

- la possibilità d'inoltare i transiti ad un secondo server o ad un server FTPS generico.
- la segnalazione pericolo transito di particolari merci pericolose configurabili;
- integrazione di un server email di default per l'invio di notifiche o avvisi;
- inserimento di liste regionali che possono inviare notifiche per ogni targa a utenti specifici
- la possibilità d'inoltare i transiti attraverso protocollo TCP o HTTPS (GET/POST) a un software di terze parti personalizzando il formato della notifica (XML, JSON, etc.);
- la possibilità di segnalare allarmi su Mappe grafiche con posizione GPS, con evidenza dei percorsi e della direzione di transito;

- la trasmissione, su allarme, dell'immagine associata alla cattura della targa segnalata, verso dispositivi remoti (**come radio mobili MOTOROLA e HYTERA, PC, Tablet etc.**) con ricezione vocale del numero di targa;
- la possibilità di supportare la compressione delle richieste in modo da utilizzare meno banda possibile durante i trasferimenti dei risultati delle ricerche;
- un motore integrato ottimizzato per un'elevata velocità di scrittura e ricerca, sia a livello di connessione FTPS che HTTPS;
- modulo di tipo *"tutore"* che consente di creare percorsi virtuali tra due varchi e ricevere segnalazioni in caso di superamento di una velocità impostata o di superamento del tempo medio stabilito per segnalare eventuali problematiche sul tratto stradale;
- segnalazione superamento livelli di guardia dell'inquinamento da polveri sottili PM2,5 e PM10.

Sicurezza e Privacy:

L'aspetto della sicurezza dei dati e della privacy è al centro del sistema di Lettura Targhe da realizzarsi, pertanto, risulta necessario il requisito del software di gestione targhe di possedere la certificazione ISDP10003 a garanzia dell'attenzione che ha riposto sulla questione sicurezza dei dati al fine di ottemperare al rispetto della privacy e del regolamento GDPR. Certificazione utile per agevolare il lavoro del DPO nella stesura del DPIA nella valutazione dei rischi. La sicurezza dei dati e delle immagini dovranno essere garantite tramite:

- crittografia HTTPS e FTPS su protocollo TLS/SSL;
- cancellazione automatica dei dati e delle immagini dopo un certo periodo temporale;
- creazione di log delle richieste FTPS e HTTPS in ingresso per monitoraggio del sistema;
- gestione delle comunicazioni client-server tramite standard HTTPS;
- sicurezza di sistema garantita anche attraverso l'invio notifiche su anomalie di sistema, password scadute, telecamere non raggiungibili, spazio disco esaurito;
- integrazione con LDAP (ActiveDirectory) per l'importazione di utenti di sistema su dominio;
- gestione semplificata di un grosso numero di utenti e dei loro permessi;
- aggiunta dell'ufficio di competenza e della possibilità di personalizzare i permessi ad alto livello per tutti gli utenti che ne fanno parte;
- aggiunta di un utente con privilegi che è un utente operativo che può agire su telecamere, utenti, liste, azioni e modificare ad alto livello la configurazione[SICUREZZA];
- possibilità di abilita per gli utenti l'autenticazione in due passaggi su email o Telegram.
- indicatori di robustezza per le password;
- impostazione scadenze password obbligatorie per maggior sicurezza.

Indagini:

Quando un sistema, come quello della lettura delle targhe, genera una massiccia quantità di dati di transito (mediamente milioni di dati) è importante, soprattutto se utilizzati per effettuare delle indagini, considerare due aspetti fondamentali:

1. la precisione di lettura OCR delle telecamere. Telecamere poco precise generano centinaia di migliaia di dati errati o mancanti. Errori che possono inviare falsi allarmi, depistare l'investigazione e non favorire un uso corretto e utile delle informazioni;
2. la velocità con cui è possibile ricevere allarmi e ricercare i dati, per un'efficace prevenzione ed un immediato intervento.

Tra le funzionalità d'indagine che il software deve possedere vi dovrà essere la possibilità di offrire:

- ricerca dei *"Complici"* legati a una targa sospetta che ha commesso un reato;

- segnalazione dei veicoli radiati intestati a “Prestanome” (rif art. 94 bis);
- ricerche per *Marca* e *Modello* del veicolo;
- ricerche per Classe del veicolo;
- ricerche per Nazionalità;
- ricerche per Colore del veicolo;
- filtri multipli tipicamente per codici/targa anche parziali, data, ora, varco, direzione, liste o segnalazioni;
- filtri complessi che effettuano l'intersezione (match) dei numeri di targa ottenuti mediante due o più selezioni differenti (per esempio per periodo temporale o varco). Operazione che dovrà consentire di estrapolare, da questo incrocio dei dati, una lista di tutte le targhe presenti in entrambe le selezioni;
- filtro di aggregazione dei diversi dati su base giornaliera/settimanale/mensile e/o tra i diversi varchi attivi;
- ricerche per tipo (anche parziale) di codice/targa, data/ora, etc, attraverso l'uso di espressioni logiche;
- ricerca targa incrociate per giorno, fascia oraria, varco, etc;
- ricerche per proprietario del veicolo;
- ricerca targhe su server remoti collegati;
- possibilità di caricare un file di targhe da cercare o codici fiscali di prestanome;
- ricerca con più filtri per unione o intersezione su più giorni o su più sistemi;
- possibilità di ricercare su più giorni nella medesima fascia oraria (personalizzabile);
- ricerca per velocità massima o minima;
- funzionalità di ricerca o esclusione dei pendolari;
- filtri veloci per ogni colonna nei risultati di ricerca molto utili in fase di indagine;
- possibilità di visualizzare un'anteprima del transito evidenziandolo o di tutti i transiti risultanti;
- rinfresco e aggiornamento dell'ultima ricerca fatta;
- copia veloce delle targhe risultanti o dei codici proprietari per ulteriori indagini;
- esportazione dei risultati di ricerca in file CSV completamente personalizzabili;
- esportazione delle immagini dei transiti o di PDF delle ricerche in file criptati;
- download facilitato delle singole immagini del transito visualizzato;
- esportazione massiva dei transiti per successive indagini o da consegnare alle forze dell'ordine con scelta targa criptata o in chiaro, CSV dei transiti o immagini e criptazione con password dei file risultanti.

Analisi e Statistiche:

La piattaforma di Lettura Targhe dovrà integrare la funzione di analisi e statistiche, grazie alla quale sarà possibile visualizzare sotto forma grafica le molteplici informazioni che si possono ricavare da un sistema di lettura targhe e dalle banche dati annesse. Queste informazioni, oltre alla loro utilità ai fini statistici per la rilevazione del traffico, si sono dimostrate anche utili per l'analisi dei fenomeni criminosi, **la prevenzione, la repressione dei reati**, la sicurezza stradale e l'analisi delle violazioni al codice della strada, consentendo in questo modo di verificare l'efficacia delle azioni correttive messe in campo allo scopo di ridurre tali fenomeni. Tra le funzionalità che il software dovrà offrire troviamo:

- conteggio e rappresentazione grafica dei transiti;
- conteggio e rappresentazione grafica delle segnalazioni;
- conteggio e rappresentazione grafica dei transiti dei veicoli non assicurati;
- conteggio e rappresentazione grafica dei transiti dei veicoli non revisionati;
- conteggio e rappresentazione grafica dei transiti dei veicoli rubati (SCNTT);
- conteggio e rappresentazione delle statistiche relative alle liste SCNTT;

- conteggio e rappresentazione grafica dei transiti dei veicoli Merci Pericolose (KEMLER);
- conteggio e rappresentazione della classificazione dei veicoli transitati;
- conteggio e rappresentazione della Provincia di immatricolazione dei veicoli italiani transitati;
- conteggio e rappresentazione della Nazionalità di provenienza dei veicoli transitati;
- conteggio e rappresentazione degli allarmi per velocità massima superata;
- classificazione e rappresentazione grafica per marca e modello dei veicoli;
- classificazione e rappresentazione grafica delle tipologie di veicoli:

- automobile;
- motociclo;
- rimorchio;
- ciclomotore;
- mezzi pesanti;
- Van e mini Van;
- autobus;
- Forze dell'Ordine;
- targhe quadrate;



- rappresentazione statistica della stima di velocità media di transito sui varchi;
- rappresentazione statistica del tempo di percorrenza medio attraverso i varchi;
- stima della velocità e del tempo medio di percorrenza;
- distribuzione del traffico origine/destinazione;
- analisi livelli d'inquinamento delle polveri sottili PM2,5 e PM10;
- analisi delle classi ambientali dei veicoli circolanti.

Integrazioni:

La piattaforma software dovrà essere del tipo “aperta”, che gestisce anche **telecamere OCR di terze parti**, e può funzionare come soluzione indipendente con qualsiasi altro sistema gestionale di lettura targhe di terze parti. Attraverso appositi SDK e plugin si dovrà avere la possibilità d'interagire con i software di videoregistrazione VMS più diffusi:

- plug-in d'integrazione per VMS Xprotect di Milestone;
- plug-in d'integrazione per VMS Security Center di Genetec;
- plug-in d'integrazione per VMS Exaq di Tyco;
- integrazione per NAS-VMS di QNAP;
- ad ogni telecamera OCR dovrà essere possibile associare fino a tre telecamere IP esterne di contesto delle più note marche (Axis, Bosch, Hikvision, Mobotix, Sony, Avigilon, etc.);
- compatibilità con qualsiasi telecamera IP di contesto purché consultabile tramite GET HTTPS;
- integrazione telecamere ANPR-OCR di terze parti provviste d'invio notifiche FTPS;
- possibilità di realizzare sistemi integrati in multiserver e multiclient protetti;
- possibilità d'integrare (rendere intercomunicanti) tra loro impianti Comunali di lettura targhe realizzati con software e telecamere di brand differenti. Dovrà essere, inoltre, possibile collegare tutti i Comuni a Questure, Comandi provinciali dei Carabinieri e Prefetture senza bisogno d'inviare tutte le notifiche;
- possibilità d'integrazione con soluzioni di terze parti, attraverso richiamo di semplici GET HTTPS o Plug-in specializzati a seconda del tipo di necessità;
- integrazione con sistemi di elaborazione delle contravvenzioni;
- integrazione con gestori delle classi ambientali.

Sinottico:

- interfaccia grafica web (restyle);
- la piattaforma software dovrà interagire sui seguenti sistemi operativi:
 - o Windows Desktop 7 o superiore;
 - o Windows Server 2012 o superiore;
 - o Distribuzioni Linux Debian;
 - o su NAS con sistema operativo QNAP;
 - o su NAS con sistema operativo EXACQ;
- compatibilità con qualsiasi marca e modello di telecamera di contesto TCP/IP purché consultabile tramite GET HTTPS;
- compatibilità con qualsiasi marca e modello di telecamera ANPR-OCR di lettura targhe.

Certificazione:

La soluzione software e le **telecamere** di lettura targhe dovranno essere certificate secondo schema Europeo ISDP10003, al fine di rispettare tutti i requisiti richiesti dal GDPR in materia di Data protection nel rispetto del principio di **Privacy by design e Privacy by default**.

Di seguito si riportano alcune caratteristiche peculiari della piattaforma di lettura targhe

BANCHE DATI

Modulo Alert per il collegamento alla banca dati del Ministero dei Trasporti e delle Infrastrutture (portale dell'automobilista) per la verifica della copertura assicurativa e stato di revisione dei veicoli.

INTERFORZE

Nelle mani delle Forze di Polizia, lo strumento più efficace per essere informati **in tempo reale su eventi critici** di pubblica sicurezza. Modulo APP per Telegram (utilizzabile con *Windows, Linux, Android, IOS*) che trasforma un qualsiasi cellulare, tablet o PC portatile in dispositivo di segnalazione acustica e visiva degli eventi critici, mettendo in connessione, in modo sicuro e crittografato, Polizia Locale, Questura e Arma dei Carabinieri per una videosorveglianza urbana partecipativa e integrata. Inoltre il sistema "Bot" **non dovrà lasciare alcuna traccia dei dati** e delle immagini su alcun server neppure su quello di Telegram.

MONITOR

Per visualizzare i transiti, ricevere segnalazioni, allarmi o fare ricerche, dovranno essere messi a disposizione due tipologie diverse di "**MONITOR**", una che sfrutta un normale browser (*Firefox, Chrome*) e l'altra basata su una APP per tablet e cellulari Android (*disponibile su Google PlayStore*).

PLUG-IN

Plugin che consentono l'integrazione della piattaforma software all'interno del sistema di videosorveglianza VMS dei maggiori produttori presenti sul mercato come Milestone Systems, Genetec, Exacq e Qnap. Il Plug-ing dovrà consentire, in tempo reale, di associare al passaggio di una targa/codice, un "segnalibro" al flusso video registrato, in modo da poter rivedere (digitando il numero di targa /codice) lo spezzone di video relativo al transito di quel specifico veicolo.

TUTOR

Modulo per la stima della velocità media, di uno o più veicoli, tra un varco e l'altro. Utile per l'analisi del traffico e la valutazione dei tempi di percorrenza.

INTEGRAZIONE TELECAMERE OCR TERZE PARTI

Licenza per integrare nella piattaforma software, telecamere ANPR-OCR di lettura targhe di altri produttori.

MARCA & MODELLO



Algoritmo di video analisi (deep learning) per il riconoscimento della marca e del modello dei veicoli. L'algoritmo dovrà riconoscere più di 9000 modelli e 400 marche, con tempi di risposta inferiori ai 0,3 sec e una precisione fino al 95%. I dati di marca e modello dovranno essere associati a quelli della targa per un recupero completo delle informazioni del veicolo. Il modulo dovrà riconoscere marca e modello di autovetture ed una vasta gamma di veicoli commerciali fino ad arrivare alla categoria dei furgoni. Questa funzione dovrà poter essere applicata su

tutte le telecamere OCR di lettura targhe, anche di terze parti.

COLORE & CLASSE

Algoritmo di video analisi (deep learning) per il riconoscimento del colore e della classe dei veicoli. L'algoritmo dovrà riconoscere 12 classi di colore e 11 classi di veicoli, con precisione fino al 93% e tempi di risposta inferiori ai 0,5 sec. I dati di colore e classe dovranno essere associati a quelli della targa per un recupero completo delle informazioni del veicolo.

(SCNTT) - COLLEGAMENTO AL CEN DI NAPOLI



Modulo per la Polizia di Stato (Questura) che consente al CPS di collegarsi alla banca dati del Ministero degli Interni del CEN di Napoli per la segnalazione dei veicoli rubati, delle targhe clonate, targhe smarrite o sotto indagine.

INTEGRAZIONE SISTEMI OCR

Speciale plug-in utile per connettere tra loro gli impianti di lettura targhe (portali) di differenti brand, sparsi sul territorio, affinché gli Operatori alla Sicurezza e le Forze dell'Ordine possano, sfruttare queste risorse distribuite sul territorio, aggregandole insieme per la prevenzione dei crimini e la repressione dei reati. La particolarità di questa soluzione è quella né d'interferire, né sostituirsi, all'esistente soluzione software di lettura targhe in uso presso i singoli Comuni. Semplicemente s'integra per lo scambio dei dati. In altre parole dovrà funzionare da "collettore" dei portali di lettura targhe.

6.3. Autonomia di Archiviazione

Il sistema di stoccaggio delle informazioni video sarà gestito dalla Polizia Municipale con possibilità di accesso da remoto (client) ad altri operatori autorizzati mediante sistemi di firewall con username e password.

L'autonomia del sistema di archiviazione dei filmati, rispetterà i limiti di tempo indicati dal Garante della Privacy per le attività nei comuni H24 (7 giorni), cancellando in automatico, mediante sovrascrittura i files/filmati più vecchi del periodo preimpostato.

7. Rete di trasmissione dati

Le singole postazioni di videosorveglianza invieranno i flussi video codificati in digitale direttamente alla Centrale Operativa, mediante una infrastruttura di rete in tecnologia Hiperlan operante in bande di frequenza libere a 5GHz.

Il progetto, dunque, si sviluppa principalmente su una sola linea di interventi infrastrutturali (Hiperlan) che insistono su aree sensibili del Comune di Carinaro.

È previsto che il Nodo di Concentrazione del Sistema di Videosorveglianza presso il Comando della Polizia Municipale del Comune di Carinaro.

L'impianto dovrà essere conforme ai requisiti generali descritti nella Direttiva del ministero dell'Interno n.558/SICP ART/421.2/70 del 2 marzo 2012, avente per oggetto i Sistemi di Videosorveglianza in ambito comunale.

L'impianto dovrà garantire una qualità costante nel tempo dei segnali video, anche al variare delle condizioni atmosferiche e ambientali; in particolare, tutte le apparecchiature installate in campo aperto dovranno essere alloggiare in custodie climatizzate, al fine di garantire il corretto funzionamento del sistema anche per temperature inferiori allo 0°C e con un adeguato grado di protezione IP.

Tutti gli apparati dovranno essere dotati di certificazione attestanti la conformità alle leggi e alle normative vigenti (es. marcatura CE, certificazioni INRIM, ecc.) e dovranno essere impiegati prodotti di marche primarie riconoscibili costruiti e/o assemblati da aziende riconosciute quali leader nel settore dei prodotti per sistemi TVCC e con marchio di qualità (es. IMQ, CE, ecc.).

Di seguito vengono descritte le prestazioni e le funzionalità tecniche che deve possedere il sistema di rete HIPERLAN 2 precisando che, tutte le volte che sarà indicato il nome e la tipologia di un prodotto, con la menzione della specifica casa costruttrice, o le specifiche tecniche saranno riconducibili ad un determinato prodotto, esso sarà fatto al solo scopo di fornire elementi inconfutabili del prodotto che si vuole descrivere. Le ditte concorrenti, partecipanti alla gara d'appalto, dovranno fornire apparecchiature aventi le caratteristiche tecniche similari e/o superiori in grado di assicurarne la medesima funzionalità d'uso.

7.1. Connettività mediante Hiperlan criptata

Per quel che attiene alla rete Hiperlan criptata è stato effettuato uno studio della morfologia del territorio finalizzato alla individuazione di punti posti a quote sopraelevate rispetto ai punti di installazione delle postazioni di videocontrollo. Successivamente si è provveduto alla verifica dei campi di visibilità tra detti punti, in modo tale da garantire una condizione di vista (LOS) tra le antenne riceventi e trasmettenti. Tutti i link saranno a 5 GHz.

Varrà realizzata un'infrastruttura di rete wireless in grado di interconnettere le postazioni di videosorveglianza posizionate sul territorio del comunale alla centrale di videoregistrazione e management ubicata all'interno dell'edificio municipale. La tecnologia di riferimento, è quella operante nella banda ISM liberalizzata dei 5 GHz sia per quanto riguarda il "CED dell'edificio della Polizia Municipale" e le CPE delle postazioni periferiche.

La potenza massima permessa in Italia dalla legislazione vigente (EiRP = 1 Watt) consente tratte radio anche di qualche decina di chilometri in spazio libero ed è ideale per collegamenti tra punti posti in visibilità reciproca anche a notevole distanza.

Inoltre le prerogative della codifica OFDM (Orthogonal Frequency Division Multiplexing) consentono la ricostruzione del segnale anche in casi di non visibilità tra i due capi del ponte radio (NLOS – Non Line of Sight). Tale codifica funziona benissimo quando gli ostacoli sono in gran numero e molto diversi, creando una notevole quantità di cammini multipli (effetto Fading). L'OFDM sfrutta i cammini multipli e massimizza l'efficienza in ricezione.

In particolare, sono stati identificati alcuni siti che per la loro posizione geografica in primis, le caratteristiche proprie (altezza della struttura, disponibilità da parte della proprietà, etc), meglio si prestano ad essere utilizzati come punto di raccolta (HOP/centro stella) a cui connettere in wireless i nodi periferici costituiti dalle postazioni di videosorveglianza. Detti siti, collegati tra loro con connessioni punto-punto costituiranno il backbone di trasporto fino alla postazione di video management.

Il link dovrà essere dimensionato per garantire il trasporto di tutta la banda generata dai dispositivi di video ripresa. La regola generale utilizzata per il dimensionamento della rete è quella che fa capo alla banda richiesta da ogni telecamera; in particolare occorrerà garantire 15 Mbps netti per ogni telecamera (fissa e speed dome).

Sia l'infrastruttura di accesso che di trasporto, dovrà essere realizzata considerando che tutti i siti dovranno essere in reciproca visibilità (Line of Sight).

8. Postazioni periferiche di videosorveglianza

In questo paragrafo sono descritti gli elementi che compongono il sistema periferico annesso alle postazioni di monitoraggio veicolare.

Le principali componenti della stazione di rilevazione sono, dunque:

1. requisiti della telecamera di lettura targhe;
2. requisiti della telecamera di contesto;
3. quadri di campo;
4. sottosistema di alimentazione;
5. struttura di sostegno.

Di ciascuna delle componenti indicate si andrà di seguito e definirne le principali caratteristiche.

8.1. Telecamera di Lettura Targhe

La telecamera di lettura targa dovrà essere di nuova generazione e dovrà essere di tipo IP, in grado di leggere le targhe su singola corsia e provvista di doppio sensore (OCR + contesto da 5 Mpx a colori) di lettura targhe, ad elevata risoluzione, provvista anche di un sensore di contesto a colori ad alta risoluzione e conforme alle specifiche richieste dall'SCNTT per la lettura a media velocità dei veicoli su varchi a singola corsia di marcia.

Di seguito le caratteristiche minime della telecamera ANPR:

Sensore OCR di Lettura Targhe	2 MP
Sensore a Colori di Contesto	5 Megapixel, CMOS Rolling Shutter a colori
Lente OCR	lente fissa da 25 mm con apertura focale F1.2 e attacco C/CS
Lente di Contesto	lente fissa da 12mm con filtro IR di serie
Velocità MAX di cattura	140 Km/h
Precisione di Lettura	99%
Tipo di Lettura	Lettura targhe (OCR)
Alimentazione	POE+ (Power Over Ethernet Plus) comprensivo di injector ad alta potenza

La telecamera dovrà possedere un sensore ed illuminatore delle alte prestazioni tanto da consentire il riconoscimento dei veicoli (*Marca, Modello, Tipologia e Colore*) in tutte le condizioni atmosferiche, di giorno e di notte.

Le immagini debbono essere significative per dimostrare la capacità della telecamera OCR di sapere leggere anche le seguenti tipologie di targhe e tabelle:

- sporche;
- danneggiate;
- con caratteri rovinati;
- semicoperti;
- in sovraesposizione;
- con ombre nette;
- targhe deformate;
- angolazione orizzontale fino a 60°;
- sia di giorno che di notte;
- frontali di notte con fari abbaglianti accesi;
- durante pioggia, neve e nebbia;
- le immagini di lettura devono essere autentiche, prodotte dalla telecamera oggetto dell'offerta e non soggette ad elaborazione.



Le apparecchiature di lettura targhe da impiegare nell'ambito della realizzazione di codesto sistema di videosorveglianza urbana dovranno essere conformi alla certificazione ISDP 10003, determinando la conformità al GDPR, garantendo una completa valutazione della conformità dei processi interni in merito alla protezione dei dati personali con particolare riferimento alla corretta

gestione dei rischi, secondo i criteri del privacy by Design e privacy by Default a garanzia e nel rispetto delle norme in materia di sicurezza e privacy.

Di seguito si riportano le specifiche tecniche minime da tenere in conto nella scelta del dispositivo di lettura targhe:

SENSORE

Sensore OCR: 2 Megapixel, Global Shutter, CMOS B/N, con frame rate di 60 Fps;
Sensore a colori di contesto: di serie -> 5 Megapixel, CMOS Rolling Shutter a colori.

LENTE

- Lente OCR lente fissa da 25 mm con apertura focale F1.2 e attacco C/CS;
- Lente di contesto lente fissa da 12mm con filtro IR di serie.

ALIMENTAZIONE

L'alimentazione dovrà essere in POE+.

Potenza assorbita: 9 Watt max.

PROTEZIONI INTERNE

La telecamera dovrà essere protetta contro:

- le inversioni della polarità di alimentazione;
- gli sbalzi di tensione superiori ai 30 Vdc;
- i sovraccarichi, tramite protezione termica;
- sovratensioni (TVS) su porte USB e Ethernet.

MEMORIA INTERNA

Tipologia ed espandibilità di serie: microSD SLC da 8 GB (espandibile a richiesta fino a 256 GB di tipo MLC) di tipo industriale High Endurance (da -40° a + 85°).

CERTIFICAZIONI

- OCR: 100% di precisione secondo certificazione UNI 10772:2016 in classe A, su targhe posteriori, a due righe, moto e motorini.
- Sicurezza dati: ISDP10003:2018 - Privacy by Default e Privacy by Design.

GENERALI

- Temperature di esercizio da -40°C a +65 °C senza uso di ventole e riscaldatori;
- Grado di protezione IP66 di serie e a richiesta anche IP67 e IK10.

8.2. Telecamera di Contesto

Con organizzazioni e operazioni sempre più collegate tra loro, il panorama commerciale globale è innegabilmente complesso. Una criticità che il settore della videosorveglianza urbana sta affrontando a livello mondiale è la minaccia, reale o percepita, alla sicurezza informatica e le sue implicazioni potenzialmente ad ampio raggio per la sicurezza e la sorveglianza.

Il National Defense Authorization Act 2019 (NDAA) promosso da John S. McCain è una legge federale degli Stati Uniti entrata in vigore il 13 agosto 2018. Tra le tante disposizioni della legge, la Sezione 889 definisce il divieto per le agenzie federali e i loro appaltatori di usare e procurarsi determinati servizi, apparecchiature e componenti per telecomunicazioni e videosorveglianza realizzati da specifici produttori.

Ciò significa che le agenzie federali non possono utilizzare telecamere prodotte da una qualsiasi delle società inserite nella blacklist.

Pertanto le apparecchiature di ripresa da impiegare nell'ambito della realizzazione di codesto sistema di videosorveglianza urbana dovranno supportare la conformità all'NDAA in tutta la linea di prodotti e a conformarsi a tutti i regolamenti commerciali domestici e internazionali.

La suite di dispositivi scelti dovranno essere conformi alla certificazione UL CAP (*Programma di certificazione eseguito da UL: leader globale nella scienza della sicurezza che valuta le potenziali criticità connesse alla sicurezza informatica e il livello di rischio degli hacker*).

Inoltre, le telecamere dovranno essere conformi alla vigente normativa del GDPR ed impedire l'accesso, la copia o la manomissione dei dati riservati.

La telecamera di contesto dovrà essere di ultima generazione, con fattore di forma di tipo Bullet da esterno, con grado di protezione IP66, di risoluzione 5MP e capace di realizzare immagini a colori e passare in automatico in modalità bianco e nero, se necessario, per ottenere un'adeguata qualità dell'immagine anche nel caso di scarsa luminosità della scena ripresa. Questa funzione deve essere abbinata ad un filtro Day & Night ICR motorizzato automatico che permetterà di ottenere il massimo della qualità di immagine in qualsiasi condizione di illuminazione.



La telecamera dovrà essere dotata di un sensore di immagine minimo da 1/2,8" Progressive Scan CMOS, che dovrà avere una sensibilità minima garantita di 0,007Lux@F 1,6 in modalità a colori, e dovrà integrare un obiettivo varifocale motorizzato 3,2-10,2mm, per mantenere le caratteristiche di flessibilità richieste, nonché essere dotata di funzione di messa a fuoco manuale da interfaccia software ed auto focus.

Sia la compensazione del controluce (backlight compensation) che il WDR dovranno essere parametrizzabili per garantire un ampio range dinamico della telecamera, che deve arrivare almeno a 120dB, ed ottenere immagini nitide anche in condizioni di luce molto contrastate.

La telecamera dovrà raggiungere una risoluzione almeno di 2592x1944 pixel con un frame rate di almeno 25fps (risoluzione e frame rate scalabili a discrezione dell'utente) e utilizzare gli algoritmi di compressione video H.265/H.264 e sue evoluzioni e MJPEG, in modalità multistreaming, tale da permetterle di generare 5 flussi video contemporanei e singolarmente configurabili.

La telecamera dovrà disporre inoltre di slot per alloggiamento di schede SD/SDHC/SDXC in grado di conservare le registrazioni di streaming video o singole immagini anche localmente, per una capacità totale sino a 256GB.

I protocolli di comunicazione supportati dovranno essere IPv4, IPv6, TCP/IP, UDP/IP, RTP (UDP), RTP (TCP), RTCP, RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3 (MIB-2), ARP, DNS, DDNS, QoS, UPnP, Bonjour, LLDP, SRTP (TCP, UDP Unicast); **si sottolinea l'imprescindibilità della completa compatibilità allo standard ONVIF profilo S/G/T/M e SUNAPI (HTTP API).**

La telecamera dovrà supportare diversi algoritmi di analisi video a bordo camera quali:

- tipo di oggetto classificato: persona/veicolo;
- attributi: Veicolo (tipo: auto/autobus/camion/moto/bicicletta);
- supporta DetectionShot
- eventi di analisi basati sul motore AI:
 - o rilevamento di movimento;
 - o rilevamento di oggetti;
 - o linea virtuale (incrocio/direzione);
 - o area virtuale (loitering/intrusione/ingresso/uscita);
 - o eventi di analisi
 - o rilevamento sfocatura;
 - o rilevamento movimento;
 - o manomissione;
 - o linea virtuale (comparsa/scomparsa).

Specificando che alcune analisi video funzionano solo con la rilevazione di persone e veicoli.

Di seguito si riportano le specifiche tecniche minime da tenere in conto nella scelta del dispositivo di ripresa:

DISPOSITIVO DI IMAGING

video CMOS 1/2,8"

Risoluzione 2592x1944, 2560x1440, 1920x1080, 1280x960, 1280x720, 800x600, 800x448, 720x576, 720x480, 640x480, 640x360, 320x240

Velocità max. di fotogrammi H.265/H.264: Max. 30 fps/25 fps (60 Hz/50 Hz)

MJPEG: Max. 30 fps (@5MP Max. 5 fps)

Distanza oggetto min. Colore: 0,07 lux (F1.6, 1/30 sec)

B/N: 0,007 lux (F1.6, 1/30 sec, 30 IRE), 0 lux (LED IR acceso)

Uscita video USB: Micro USB tipo B, 1280 x 720 per installazione

OBIETTIVO

Lunghezza focale (Rapporto di zoom) 3,2 ~ 10,2 mm (3,2x) varifocale motorizzato

Velocità max. di apertura F1.6 (grandangolo) ~ F3.1 (teleobiettivo)

Campo di visione angolare H: 95° (grandangolo) ~ 29° (teleobiettivo)

V: 69° (grandangolo) ~ 21° (teleobiettivo)

D: 126° (grandangolo) ~ 36° (teleobiettivo)
Distanza oggetto min. 1,2 m (3,93 piedi)
Controllo della messa a fuoco Messa a fuoco semplice
Tipo di obiettivo DC auto iris (con correzione IR)

CARATTERISTICHE OPERATIVE

Nome telecamera Visualizzazione fino a 85 caratteri
Giorno e notte Auto (ICR)
Compensazione del controllo luce BLC, WDR, SDDR
Wide Dynamic Range 120 dB
Riduzione digitale del rumore SSNR V, WiseNR II (basato sul motore AI)
Rilevamento del movimento 8 zone poligonali a 8 punti
Mascheramento privacy 32 zone quadrangolari a 4 punti
Controllo del guadagno Basso/Medio/Alto
Bilanciamento del bianco ATW/AWC/Manuale/Interno/Esterno
LDC Supportato
Velocità dell'otturatore elettronico Minima/Massima/Anti-sfarfallio (1/5 ~ 1/12.000 sec)
PTZ digitale Supportato
Rotazione video Inversione, speculare, vista corridoio (90°/270°)
Ingressi/uscite allarme 1 ingresso/1 uscita
Trigger di allarme Analisi, disconnessione dalla rete, ingresso allarme
Eventi di allarme Innesco allarme

- Caricamento file (immagine): e-mail/FTP
- Notifica: e-mail
- Registrazione: Registrazione tramite schede SD/SDHC/SDXC o NAS in caso di innesco allarme
- Uscita allarme
- Trasferimento (preimpostazione PTZ, invio messaggio tramite HTTP/HTTPS/TCP)
- Riproduzione clip audio

Ingresso audio Selezionabile (ingresso mic./ingresso di linea)
Uscita audio Uscita di linea, livello max uscita: 0,5 Vrms
Lunghezza visualizzabile IR 30 m (98,42 piedi)
Lunghezza d'onda IR LED IR 850 nm a lunga durata

RETE

Ethernet RJ-45 (10/100 BASE-T)
Compressione video H.265/H.264: Principale/Alto, MJPEG
Compressione audio G.711 u-law/G.726 selezionabile
G.726 (ADPCM) 8 kHz, G.711 8 kHz
G.726: 16 Kbps, 24 Kbps, 32 Kbps, 40 Kbps
AAC-LC: 48 Kbps a 16 kHz
Codec intelligente Manuale (5 aree), WiseStream II → (sarà supportato come R/C a luglio)
Manuale (5 aree), WiseStream II, WiseStream III (basato sul motore AI)
Regolazione qualità video H.264/H.265: Controllo livello bitrate di destinazione
MJPEG: Controllo livello qualità
Controllo del bitrate H.264/H.265: CBR o VBR
MJPEG: VBR
Streaming Unicast (20 utenti)/Multicast
Streaming multipli (fino a 5 profili)

Protocollo IPv4, IPv6, TCP/IP, UDP/IP, RTP (UDP), RTP (TCP), RTCP, RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3 (MIB-2), ARP, DNS, DDNS, QoS, UPnP, Bonjour, LLDP, SRTP (TCP, UDP Unicast)

Interfaccia di programmazione

applicazioni

ONVIF profilo S/G/T/M

SUNAPI (HTTP API)

SICUREZZA

OS/Protect firmware Avvio sicuro, firmware firmato, crittografia firmware

Autenticazione utente Autenticazione Digest, impedisce l'attacco di forza bruta

Autenticazione rete Autenticazione 802.1X (EAP-TLS, EAP-LEAP, EAP-PEAP MSCHAPv2)

Comunicazione sicura HTTPS, SRTP, WSS (websocket sicuro)

Controllo accessi Controllo degli accessi in base all'indirizzo IP

Protezione dei dati Crittografia delle informazioni di autenticazione, crittografia della compressione ZIP

Audit Gestione accesso utente/sistema/registro eventi

ID dispositivo: Certificato dispositivo (Hanwha Techwin Root CA)

Archiviazione sicura Crittografia partizione della scheda SD

Certificato di sicurezza Sicuro per impostazione predefinita

CARATTERISTICHE GENERALI

Archiviazione periferica 1 slot per schede micro SD/SDHC/SDXC da 256 GB

Memoria RAM 2 GB, Flash 1 GB

CARATTERISTICHE AMBIENTALI ED ELETTRICHE

Temperatura/Umidità di esercizio -30 °C ~ +55 °C (-22 °F ~ +131 °F) / 0~95% RH (senza condensa)

*L'avvio deve essere effettuato a una temperatura superiore a -30 °C

Controllo dell'umidità con presa d'aria

Temperatura/Umidità di stoccaggio -50 °C ~ +60 °C (-58 °F ~ +140 °F)/0~95% RH

Certificazioni IP66, IK10

Alimentazione in ingresso PoE (IEEE802.3af, Classe 3)

Potenza assorbita PoE: Max 12 W, tipica 5,3 W

CARATTERISTICHE MECCANICHE

Colore/Materiale Bianco/Alluminio

Codice RAL RAL9003

Dimensioni/peso del prodotto ø 93,4 x 245,8 mm (ø 3,68 x 9,68"), 930 g (2,05 lb)

Foro di installazione/scatola

di derivazione compatibile

Foro di installazione: Nessuno

Scatola di derivazione (SBO-090GP): Singolo/doppio, ottagonale da 4" (venduto separatamente)

Scatola di collegamento SBO-140BW

CERTIFICAZIONI E STANDARD

EMC FCC 47 CFR 15 Sottoparte B Classe A

ICES-3 (A) / NMB-3 (A)

CE/UKCA

- EN 55032 Classe A, EN 50130-4, EN 61000-3-2, EN 61000-3-3

VCCI CISPR 32 Classe A

RCM AS/NZS CISPR 32 Classe A

Sicurezza UL 62368-1, CAN/CSA C22.2 N. 62368-1

IEC/EN 62471

Ambientali IEC/EN 63000

IEC/EN 60529 IP66, IEC/EN 62262 IK10

DORI (STANDARD EN62676-4)

Rilevazione (25 PPM/8 PPF) Grandangolo: 42,7 m (140,20 piedi)/Teleobiettivo: 186,9 m (613,28 piedi)

Monitoraggio (63 PPM/19 PPF) Grandangolo: 17,2 m (56,08 piedi)/Teleobiettivo: 75,4 m (245,31 piedi)

Riconoscimento (125 PPM/38 PPF) Grandangolo: 8,5 m (28,04 piedi)/Teleobiettivo: 37,4 m (122,66 piedi)

Identificazione (250 PPM/76 PPF) Grandangolo: 4,3 m (14,02 piedi)/Teleobiettivo: 18,7 m (61,33 piedi)

8.3. Quadri di campo

I quadri delle postazioni di ripresa saranno di tipo “Armadio Stradale” in vetroresina al fine di non inficiare sulla stabilità del palo esistente della Pubblica Illuminazione impiegato a sostegno delle apparecchiature di videosorveglianza, a due vani di uguale altezza, con portello cieco, di dimensioni di ingombro complessivi 540x1080x305 mm e dimensioni interne (singolo scomparto) 515x520x255 mm, con aerazione interna ottenuta mediante labirinto tra il coperchio e le pareti perimetrali, completo di serratura a chiave triangolare e lucchettabile e telaio di fondo caratterizzato da pannelli modulari porta apparecchiature, installato a pavimento mediante l'impiego di apposito telaio per fissaggio posto in opera entro basamento in calcestruzzo armato per armadio stradale, incluse le opere di scavo e reinterro. L'armadio di campo è completo di:

- apparecchiature di protezione;
- SPD;
- alimentatore per switch industriale con montaggio su guida DIN, 48V/ 480W;
- switch di tipo GbE Industrial switch 4*90W bt PoE, 2*SFP, 2*RJ45 Total power budget: 360W 6KV PoE surge protection Operating temperature: - 40°C ~ 75°C;

I quadri di campo saranno dotati di switch del tipo PoE industriale unmanaged con 4 porte PoE (90W) protette da sovratensione per ciascuna porta Ethernet PoE IP30, e temperatura di funzionamento compresa tra -40°C e 75°C in condizioni atmosferiche avverse.



Oltre a consentire le connessioni di PD PoE at, dovrà essere conforme ai recenti standard PD PoE bt PoE (90 W) come telecamere IR PTZ, telecamere multisensore e applicazioni PoE a lungo raggio.

Lo switch dovrà fornire multiporte Gigabit PoE (10M/100M/1G) con l'obiettivo di interscambiare dati e alimentazione ai PD PoE su un singolo cavo di rete, nonché agli slot ricetrasmittitore SFP aggiuntivi per uplink flessibile.

Caratteristiche principali

- 30 W per porta conforme a IEEE802.3at
- Protezione da sovratensione da 6 KV su ciascuna porta PoE
- Temperatura di funzionamento compresa tra -40°C e 75°C
- Porte ricetrasmittitore SFP flessibili per uplink
- Supporta velocità dati 10/100/1000Mbps
- Montaggio su guida DIN e montaggio a parete
- Grado di protezione IP30
- Standard Ethernet ad alta efficienza energetica IEEE 802.3az

Specifiche tecniche

Networking Specifications

Total Gigabit Ports	8
Gigabit PoE Port (10M/100M/1G)	4 x 90W PoE
30W IEEE802.3 at Power over Ethernet	Support
Gigabit SFP Slots	2
Forwarding Capacity	11.904Mpps
Mac Table	4k
Jumbo Frames	9,216 Bytes
Switching Capacity	16 Gbps

Power Specifications

Power 1: Input Voltage	48VDC ~ 56VDC
Power 2: Input Voltage	48VDC ~ 56VDC
Output Voltage Range / per PoE Port	48~56 VDC

PSE Power Pin Assignment

Switch power consumption (without PoE) 5W

PoE Power Budget

PoE 802.3af (15.4W) output

PoE+ 802.3at (30W) output

PoE++ 802.3bt (90W) output

12(-),36(+),45(+),78(-)

5W

48VDC:360W

Mechanical Specifications

Dimensions (DxWxH)

43.5 x 122 x 150 mm

Weight

0.9KG

Connectors

RJ45 x 8, SFP x 2,

Terminal Block x2

Environmental Specifications

Operating Temperature

-40°C~ 75°C (-40°F~ 167°F°F)

Storage Temperature

-40°C~ 85°C (-40°F~ 185°F°F)

Operating Humidity

5% ~ 95% non-condensing

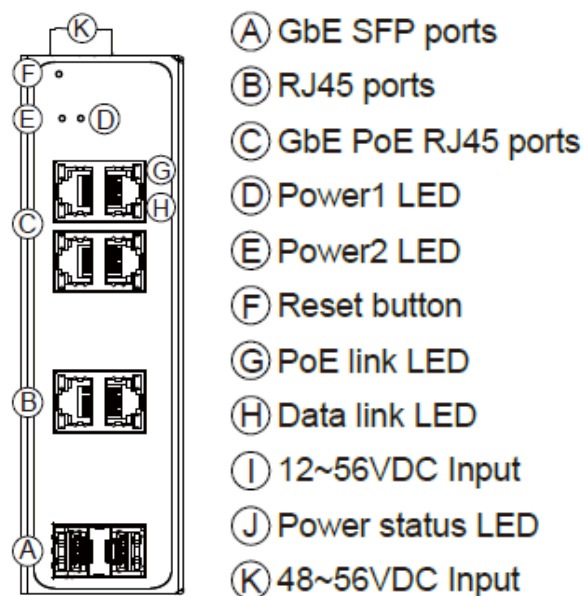
Certifications

EMC

CE, FCC, VCCI, C-Tick

Safety

EN62368-1

Tipologico installativo**⚠ IMPORTANT:**

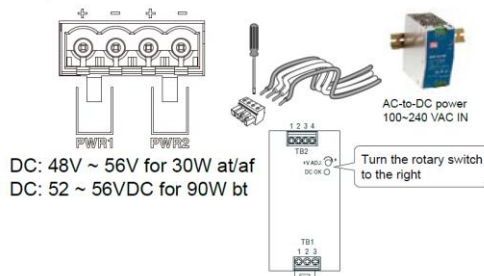
Ground screw

* Make sure the grounding resistance is lower than 0.5Ω.

Solid or stranded (AWG): 12-24/14-22

Wire strip length: 7-8mm

Torque: 5lb-In/0.5Nm/0.56Nm



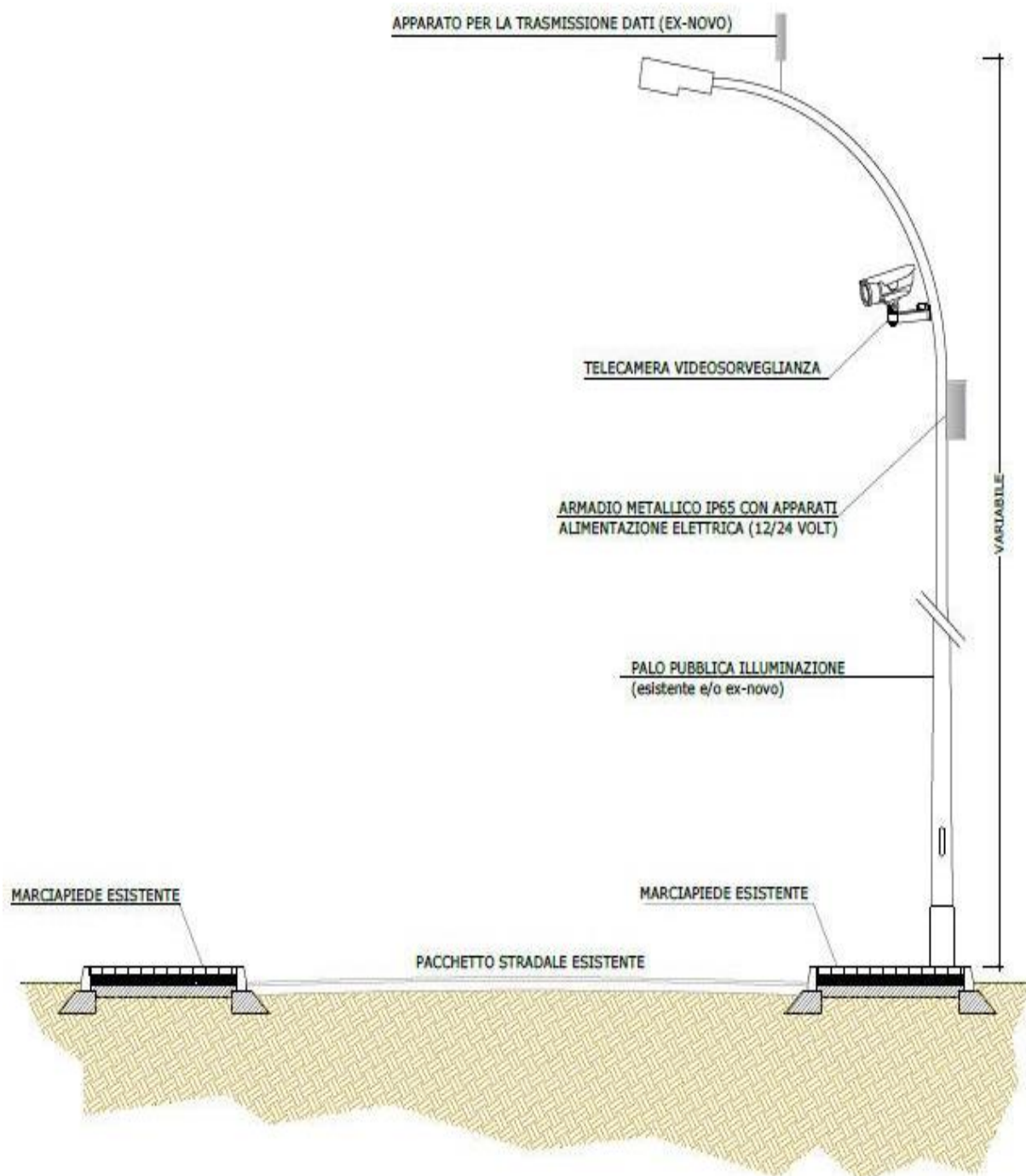
8.4. Sottosistema di alimentazione

La natura POE (power over ethernet), sia degli eventuali futuri apparati radio sia di quelli di videosorveglianza, semplifica la realizzazione infrastrutturale di terminazione, ma il problema della presenza della alimentazione elettrica dei siti deve essere valutato e risolto quale parte imprescindibile di una realizzazione "chiavi in mano".

I siti di avvistamento, da un punto di vista di elettrificazione, sono tali da presentare l'alimentazione elettrica prelevabile dal circuito della Pubblica Illuminazione.

8.5. Struttura di sostegno

Le postazioni di videosorveglianza sono previste prevalentemente su pali esistenti di pubblica illuminazione, al fine di limitare la proliferazione di ulteriori pali di nuova fornitura. Laddove si è riscontrata l'assenza di infrastrutture esistenti, la scelta progettuale prevede la fornitura in opera di pali di nuova fornitura aventi caratteristiche riportate di seguito.



Al fine di non inficiare sulle parti strutturali e, dunque, la staticità del palo esistente della Pubblica Illuminazione impiegato a sostegno dei dispositivi attivi e passivi adibiti alla videosorveglianza urbana, sarà realizzato un armadio di campo del tipo shelter stradale dal quale saranno diramati

i cavi di collegamento agli hardware installati mediante la posa di cavi UTP Cat. 6 entro tubazione TAZ opportunamente ancorata al palo mediante l'impiego di fascette in acciaio. Le apparecchiature di campo, inoltre, saranno installate mediante appositi collari di ancoraggio.

La scelta progettuale impedirà la promiscuità degli impianti di videosorveglianza con gli impianti a servizio della pubblica illuminazione.

9. Future integrazioni

Il progetto prevede la realizzazione di una rete dedicata che si configura a tutti gli effetti come una rete privata, basata sul protocollo IP, a larga banda. È quindi una struttura già pronta per l'introduzione di servizi innovativi da affiancare alla videosorveglianza.

Inoltre, la piattaforma di videosorveglianza fornita è basata sui maggiori standard internazionali ed è quindi facilmente interfacciabile con altre applicazioni.

A titolo di esempio e in modo non esaustivo, si indicano possibili integrazioni del sistema:

- Hot spot Wi-Fi (per copertura Internet del territorio comunale o per accesso wireless alla Intranet del Comune – p.es quindi applicativi da utilizzare tramite portatile PDA)
- Trasmissione di fonia-video-file
- Accessi Internet centralizzati
- Sistema di allarmistica
- Sistemi di monitoraggio ambientale
- ZTL
- Sistemi di rilevamento infrazioni
- Sistemi di analisi dei video
- Sistemi di rilevamento targhe
- Segnaletica stradale dinamica (tramite cartelloni a messaggi variabili, gestibili centralmente da una centrale di controllo)
- Cartellonistica dinamica, per comunicare informazioni e messaggi a cittadini e turisti
- Controlli con sensoristica IoT;
- Messaggistica pubblicitaria dinamica.

10. Addestramento e affiancamento generale

Ogni processo di sviluppo e di introduzione di nuovi applicativi e soluzioni tecnologiche, necessita di un adeguato piano di addestramento per garantire il pieno successo e la massima utilizzazione delle soluzioni in tutte le potenzialità. Pertanto, l'adozione di nuove soluzioni, non è semplicemente una scelta in cui la componente tecnologica è isolata, ma coinvolge soprattutto un metodo organizzativo teso a migliorare i processi di lavoro. In tal senso, per garantire la produzione di un maggior valore, è necessario prevedere e progettare interventi adeguati di formazione e di addestramento delle persone.

Da quanto esposto nasce l'esigenza di garantire la progettazione e l'attuazione di interventi formativi che accompagnino l'implementazione delle soluzioni proposte.

La formazione dovrà avvenire sia sulla parte tecnica di gestione che sull'area funzionale, prevedendo un approccio sia frontale che di affiancamento on-the job, con l'obiettivo di rendere autonomo la struttura di gestione.

Si dovranno prevedere i seguenti moduli formativi:

- Addestramento per il personale tecnico per la conduzione della infrastruttura nel suo complesso.
- Addestramento per il personale operatore per l'utilizzo del sistema di videosorveglianza.

Deve essere prevista anche una assistenza tecnica specialistica per un periodo di tempo da definire. Il servizio dovrà prevedere sia l'assistenza remota e on-line, che l'assistenza nella sede del Comune.

La formazione per il personale tecnico dovrà prevedere i seguenti contenuti:

1. Corso di formazione sulla architettura tecnica nel suo complesso.
2. Corso di formazione sulla gestione della infrastruttura server.
3. Corso di formazione sulla gestione della infrastruttura radio.
4. Corso di formazione sulla gestione e amministrazione del sistema di videosorveglianza.
5. Corso di gestione dei dati: backup, restore, recovery.

La formazione per il personale addetto al monitoraggio dovrà prevedere i seguenti contenuti:

1. Corso di formazione sulla architettura tecnica nel suo complesso.
2. Corso di configurazione del sistema di monitoraggio.
3. Corso di gestione del sistema di monitoraggio.
4. Corso di gestione dei dati: retrieval, analisi video evolute, esportazione.

I corsi di formazione dovranno essere affiancati anche da un periodo di supporto operativo on-the-job e da una assistenza telefonica agli operatori.

L'attività di addestramento sarà svolta, in accordo con il Comune, al termine della fase di implementazione del sistema di videosorveglianza.

Sarà necessario garantire che:

- i docenti messi in campo dovranno possedere un adeguato profilo ed esperienza professionale.
- dovranno essere previsti e forniti materiali didattici documentali ed illustrativi.

L'approccio perseguito nella definizione del piano di addestramento, dovrà essere orientato a fornire un efficace e continuativo supporto al personale coinvolto nella fase classica di apprendimento ma soprattutto nella delicata fase di trasferimento delle attività e competenze, in modo da garantire la piena autonomia nell'esercizio dei nuovi sistemi.

Dovrà essere previsto un periodo iniziale, della durata minima di 5gg, di "affiancamento" con il personale preposto del Comune, per assicurare, per il primo periodo di conduzione, il supporto necessario per il corretto e rapido avvio del Sistema.

In particolare, è prevista la presenza on-site di una persona qualificata in giorni feriali.

11. Manutenzione della videosorveglianza

L'amministrazione Comunale si impegna a iscrivere a bilancio dalle proprie casse le somme occorrenti ad assicurare la corretta manutenzione degli impianti e delle apparecchiature tecniche dei sistemi di videosorveglianza da realizzare per i 5 anni dalla data di ultimazione dei lavori. Il sistema sarà quindi fornito, installato e funzionante, presso la sede Comunale, previa attività di test, collaudo ed accettazione. Parimenti saranno incluse la fornitura completa della manualistica in forma cartacea ed elettronica (manuale operatore, manuali di sistema, manuali di diagnostica e manutenzione, ecc.) e la formazione in sede del personale responsabile.

Gli interventi descritti sopra già sono inclusi nella stima dei costi attuale che verranno meglio specificati nelle fasi successive degli elaborati progettuali.

La manutenzione del sistema si esplicherà attraverso un'azione finalizzata al mantenimento di due sostanziali condizioni:

l'affidabilità nel tempo degli impianti;

il ripristino dell'eventuale disservizio nel minor tempo possibile, in caso di guasto.

La manutenzione sarà pertanto articolata mediante interventi che si distingueranno secondo la seguente tipologia:

- interventi di manutenzione ordinaria di tipo preventivo;
- interventi di manutenzione ordinaria di tipo correttivo e del software;
- interventi di manutenzione straordinaria.

Gli interventi di manutenzione ordinaria di tipo preventivo comprendono tutte le operazioni periodiche programmate inerenti i controlli e le misure alle quali viene sottoposto l'impianto prima del manifestarsi dei guasti al fine di prevenire l'eventuale insorgere di degradi o irregolarità delle prestazioni.

La manutenzione preventiva sarà ovviamente effettuata per quei componenti che presentano un tasso di guasto crescente perché in tal caso riduce il tasso di guasto medio e quindi aumenta l'affidabilità.

Gli interventi di manutenzione ordinaria di tipo correttivo e del software sono interventi non programmati effettuati per riparare o sostituire componenti in avaria onde ripristinare il funzionamento del sistema. Si effettua al verificarsi di un guasto, con o senza disservizio, ed è mirata all'eliminazione del guasto per rimettere l'impianto e/o il sistema a norma e quindi nelle condizioni di affidabilità originarie, in relazione all'evento verificatosi ed alla configurazione che presenta l'impianto stesso. La manutenzione di tipo correttivo può prevedere la sostituzione di componenti guasti anche senza effettuare alcuna manutenzione.

Gli interventi riguardano le opere e le modifiche necessarie per rinnovare e sostituire componenti del sistema.

La manutenzione straordinaria si riferisce ad interventi finalizzati a mantenere in efficienza ed adeguare all'uso il sistema in caso di guasti bloccanti, atti vandalici e/o calamità naturali.

La manutenzione straordinaria indicativamente comprende le opere per il ripristino funzionale degli impianti, atti a stabilire le loro condizioni originarie nella struttura impiantistica e tecnologica con eliminazione di anomalie. Questo tipo di interventi del servizio di manutenzione vengono effettuati saltuariamente al di fuori delle normali strategie di manutenzione e comprende di norma il completo smontaggio dell'apparecchiatura del componente o del sub assieme tecnologico e la sua revisione totale.