DGR 254/2023

Evoluzione Digitalizzazione

Settore ITS

Regione Campania

CUP: F29F23002240009

Sommario

1. Attivare nuove funzionalità all'interno dell'ITS

Attualmente i servizi forniti nell'ambito dell'ITS sono forniti per il tramite del sistema MOOVA con alcune funzionalità in produzione altre in collaudo. Con il presente intervento si tende al completamento funzionale dello stesso sistema, al fine di consentire il miglioramento dell'esperienza degli utenti, ottimizzazione nell'utilizzo dei mezzi pubblici, riduzione dell'impatto ambientale e aumento della qualità del servizio offerto.

Nel contesto delle evoluzioni in corso, sono state individuate delle ulteriori aree di intervento di seguito elencate e descritte in dettaglio dei successivi paragrafi:

- Integrazione Bidirezionale con MOOVA
- Gestione Dispositivi di protezione individuali del personale
- Assistenza PRM
- Prenotazione Posto
- Assistente conversazionale
- Integrazione Asset Inventory
- Pianificazione e Gestione circolazione ferroviaria infrastruttura
- Monitoraggio Infrastruttura
- Telemedicina
- Gestione CND (Controlli non Distruttivi)
- Gestione Strumenti di Misura
- Stato Corrente Flotta e monitoring KPI
- Assessment dismissioni App BSP
- Assistenza Applicativa

1.1. Integrazione Bidirezionale con MOOVA

Nell'ambito dell'attivazione di nuove funzionalità all'interno dell'ecosistema ITS, si prevede l'integrazione di ulteriori componenti ad oggi esterne al mondo MOOVA che potranno abilitare nuovi servizi e funzionalità.

In particolare si prevedono le seguenti integrazioni:

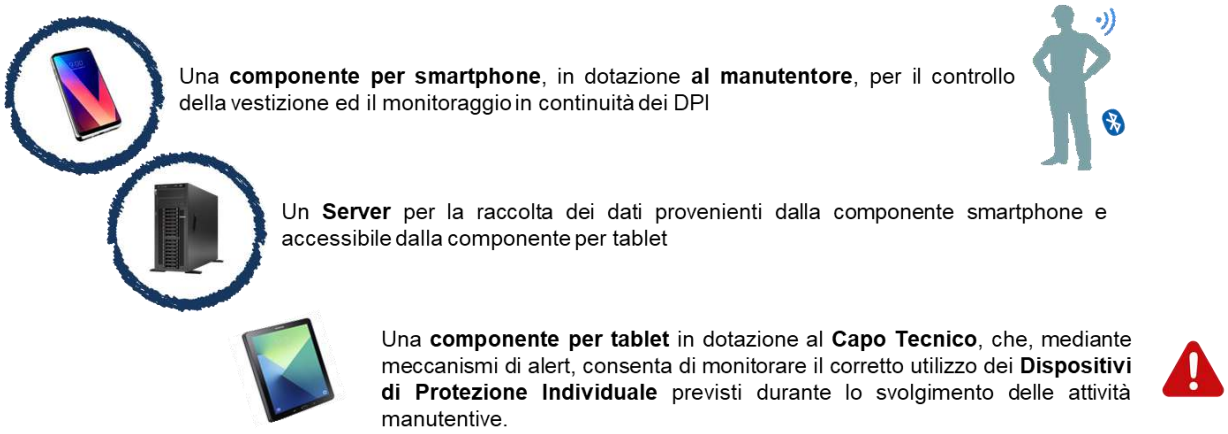
1. Interfaccia con web services MOOVA per la gestione della componente real time dei dati che consentirà:
   a. Invio push dei dati di localizzazione dei mezzi e relativi eventi in tempo reale.
   b. Invio push delle causali di ritardo.
   c. Web Service per acquisizione da MOOVA delle chilometriche dei veicoli.

   d. Web Service per acquisizione da MOOVA della codifica corrente delle causali di ritardo.
2. Interfacciamento completo con la programmazione della vestizione in MOOVA in modalità bidirezionale (acquisizione e invio variazioni), che consentirà:
   a. Web Services per l'acquisizione in tempo reale della vestizione da MOOVA verso TOLOMEO.
   b. Web Service per l'invio a MOOVA in tempo reale delle variazioni e integrazioni acquisite da TOLOMEO tramite input dati su piattaforma web o da APP del capotreno
3. Visualizzazione delle corse in real time su grafico;
4. Visualizzazione dell'esercizio su una struttura a grafo multi-binario;
5. Elaborazione dati di import integrabili in piattaforma Geolocalizzazione.

1.2. Gestione Dispositivi di protezione individuali del personale

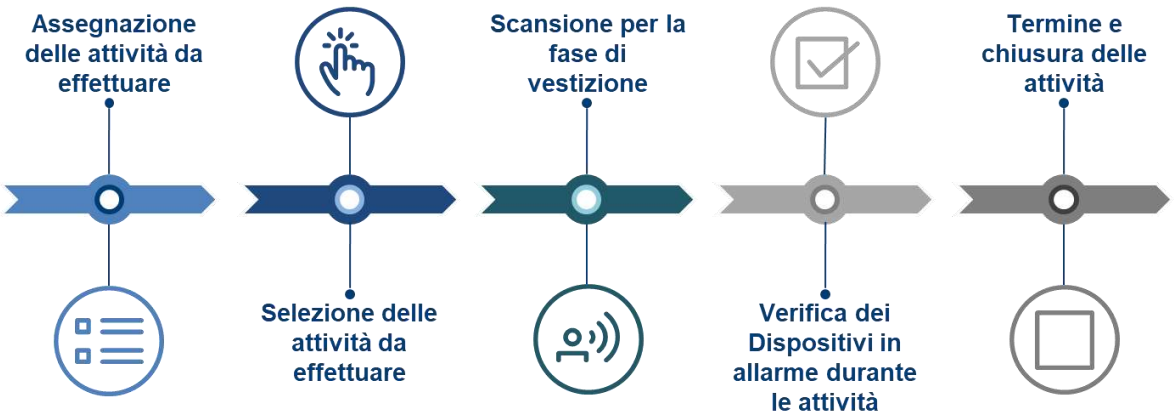
Al fine di monitorare e garantire la messa in sicurezza dei manutentori EAV intende adottare un sistema middleware e mobile per il monitoraggio della corretta vestizione (DPI) degli operatori di manutenzione.

Di seguito una rappresentazione schematica delle componenti coinvolte:

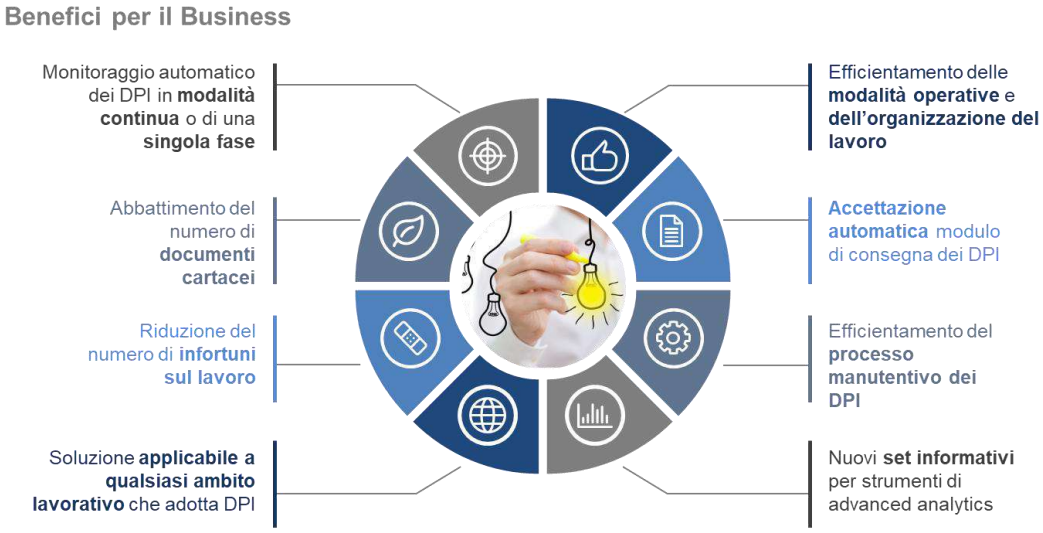


L'attrezzaggio certificato dei Beacon sugli strumenti di protezione individuale e l'acquisto di dispositivi mobile NFC ready con cui dotare il personale, sono invece esclusi dalla richiesta di fornitura.

Di seguito una rappresentazione schematica del processo:



A seguire una schematizzazione dei vantaggi di questo tipo di soluzione:

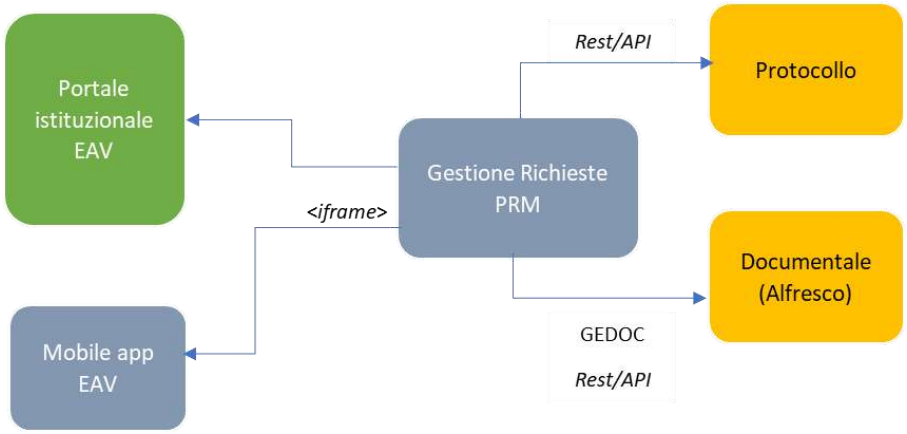


1.3. Assistenza PRM

Il servizio di trasporto di EAV prevede che i clienti con disabilità a mobilità ridotta (PRM) possano richiedere il servizio di accompagnamento di salita e discesa dal treno nelle stazioni dichiarate non accessibili. In tal senso è necessario implementare nel Portale Istituzionale e nel CRM MOOVA i seguenti workflow:

- Gli utenti via portale possono richiedere per un determinato viaggio, assistenza PRM di vario tipo, indicando, oltre alle generalità, numerosità (singolo/gruppo/comitiva), tipologia di assistenza richiesta, mezzo di trasporto/corsa, se in salita discesa o entrambi, etc ….
- L'azienda produce una pratica e inoltra il codice prenotazione della richiesta, oltre ai dettagli del servizio, al cliente
- In back-office sarà possibile quindi visualizzare tutte le pratiche gestite e/o da gestire categorizzate per stato ed esito.

Di seguito una rappresentazione schematica dell'architettura:



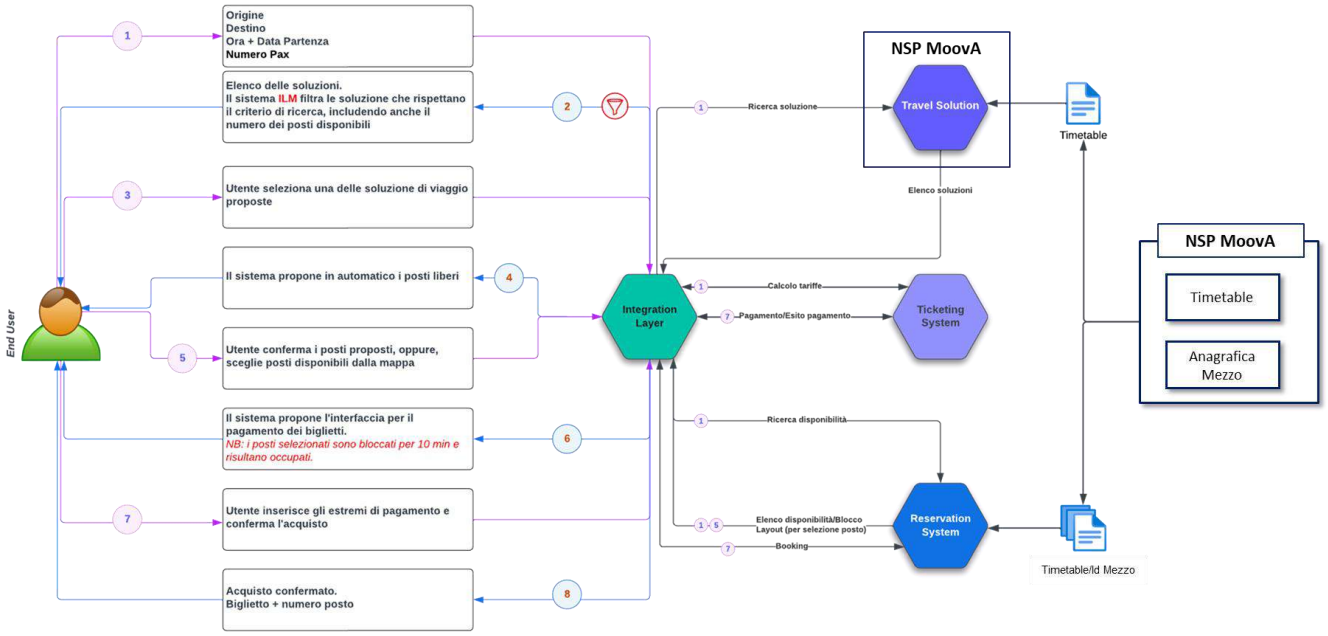
Inolte, gli operatori della azienda di trasporto, sia di terra che di bordo, che hanno in gestione la corsa dovranno avere la possibilità, tramite una apposita app mobile, di visualizzare in pre-partenza da singole località, le pratiche con indicazione dei servizi PRM richiesti nella località o a bordo e di "prenderle in carico" per dare evidenza al centro della effettiva esecuzione delle attività richieste

Gli operatori, a valle delle attività, dovranno poter, sempre tramite app, indicare il regolare svolgimento dell'assistenza e/o eventuali difformità per chiudere con esito positivo negativo o parziale la pratica di assistenza.

1.4. Prenotazione Posto

Alcuni prodotti EAV, come ad esempio il Campania Express, prevedono la prenotazione del posto. In particolare, la prenotazione è per tratta: lo stesso posto può essere prenotato, su tratte diverse, da clienti diversi. D'altra parte, il Sistema di Vendita unico dei trasporti pubblici della Regione Campania (SVR), in corso di adozione da parte di EAV, non prevede tale gestione di prenotazioni del posto. È pertanto richiesta una soluzione ad hoc che consenta tale gestione.

Di seguito una rappresentazione del flusso delle informazioni:



1.5. Assistente conversazionale

Si richiede l'attivazione di un assistente conversazionale testuale per la gestione in linguaggio naturale del processo di interazione con gli utenti del sito istituzionale di EAV.

La soluzione, esposta tramite widget sul Sito, dovrà fornire un supporto automatizzato veloce e attivo h24 alle richieste inviate quotidianamente dagli utenti, efficientando in questo modo il processo di assistenza EAV e migliorando la "customer experience".

La soluzione dovrà soddisfare i seguenti requisiti:

- gestione dell'interazione "naturale" sotto forma di dialogo, riconoscendo ed interpretando le diverse esigenze (intenti) degli utenti
- recupero delle informazioni da fonti "certificate" (es. FAQ)
- recupero delle informazioni e gestione di specifiche procedure interrogando sistemi aziendali.

L'esigenza è di fornire assistenza automatizzata ai viaggiatori sia su richieste informative (circa 20 richieste, tra quelle più frequenti) sia su richieste dispositive ovvero relative ai servizi "Calcola il percorso", "invia un reclamo" e "cerca la tariffa" che dovranno essere richiamati dal Chatbot per fornire risposte all'utente.

1.6. Integrazione Asset Inventory

EAV nel Gennaio 2023 ha indetto un Bando di gara per il SERVIZIO DIAGNOSTICA INFRASTRUTTURA FERROVIARIA DELLA RETE EAV. L'aggiudicatario è incaricato di procedere al censimento digitale di tutti gli impianti (asset) pertinenti alla sovrastruttura ferroviaria, in modo tale da avere a disposizione una banca dati digitale, consultabile e

operabile mediante un apposito sistema informativo territoriale, che possa rendere disponibili, per ciascuno degli impianti censiti, informazioni quali tipologia, georeferenziazione, caratteristiche, proprietà, etc.

Eav intende procedere all'integrazione il sistema informativo territoriale che conterà il censimento degli asset e le loro informazioni peculiari (quali tipologia, georeferenziazione, caratteristiche, proprietà, informazioni riguardanti la manutenzione degli impianti costituenti la sovrastruttura ferroviaria, etc.) all'interno del sistema di supervisione Moova. L'esigenza è data dalla volontà di efficientare la programmazione e, più in generale, la gestione delle attività manutentive relative alla sovrastruttura ferroviaria, per le quali, potendo disporre di una banca dati di riferimento degli asset, risulterebbe possibile condurre analisi statistiche e di dettaglio, utili ad interpretare il comportamento nel tempo dei binari e degli impianti ad esso collegati.

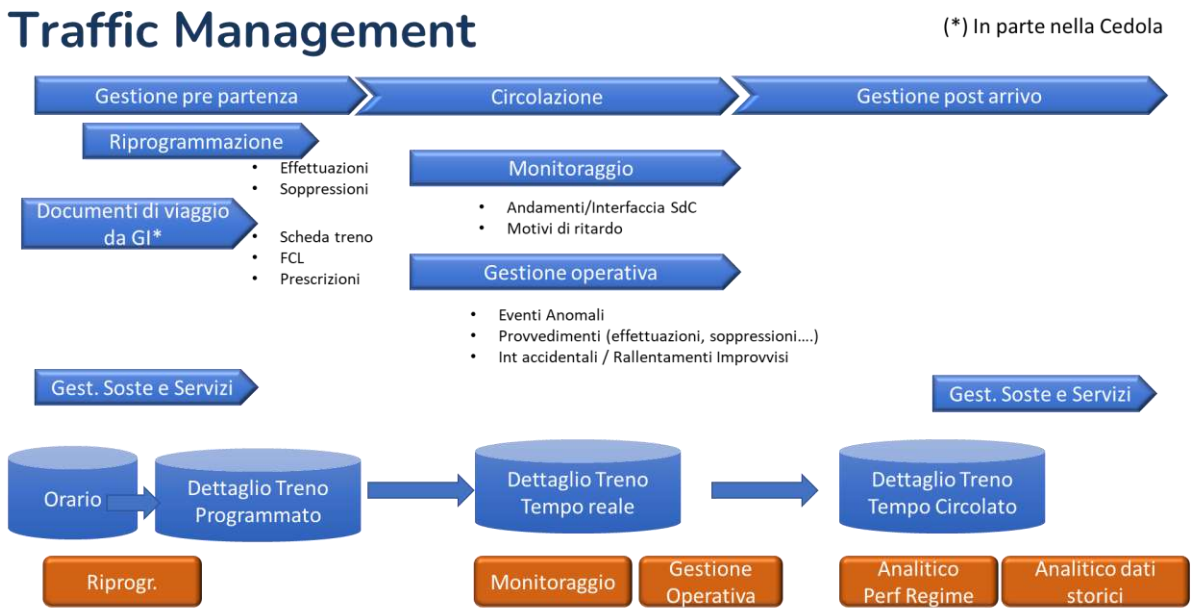
Inoltre, le informazioni relative agli asset saranno integrate con i dati derivanti dalle attività periodiche di diagnostica mobile, al fine di utilizzarli per l'implementazione di algoritmi che possano interpretare il degrado della sovrastruttura ferroviaria nel tempo, con riferimento alla possibilità di mettere in pratica politiche di manutenzione predittiva. Il risultato dell'integrazione deve, quindi, essere fruibile mediante una piattaforma web, accessibile da qualunque postazione, che sia in grado di mostrare, sia in formato tabellare sia su mappa, eventuali anomalie e/o eccezioni rilevate dalle attività di diagnostica.

1.7. Pianificazione e Gestione circolazione ferroviaria infrastruttura

Per raggiungere l'obiettivo di aumentare la sicurezza ed efficientare la capacità di offerta di servizio, incrementare la puntualità e l'affidabilità dei servizi ferroviari, ridurre i consumi energetici attraverso soluzioni tecnologiche innovative, ottimizzare l'utilizzo delle capacità utilizzando tecnologie di ottimizzazione automatica, che tengano conto anche della pianificazione degli interventi infrastrutturali e della capacità degli impianti, EAV chiede l'implementazione e l'integrazione all'interno della piattaforma di supervisione MOOVA, di un sistema di Modellazione della rete infrastrutturale, acquisizione informazioni in tempo reale dai sistemi di campo in fase di attivazione (CTC) e di futura attivazione (SCCM/ERMTS-2), grafico di circolazione, visualizzazione di interruzioni, rallentamenti e situazioni anomale, acquisizione orario e diffusione orario giornaliero ai sistemi di campo soprascritti. La soluzione deve consentire una gestione dell'impianto integrata con la circolazione e con i servizi connessi all'impianto (Multi modalità passeggeri, Gestione dei servizi in impianto, Monitoraggio rotabili), Efficientare le attività operative attraverso l'identificazione e la soluzione automatica di conflitti di circolazione e la valutazione di percorsi alternativi, identificando col maggior anticipo possibile le situazioni di perturbazione della circolazione,

Aumentare la resilienza di sistema tramite maggior integrazione con i sistemi di campo EAV per attuare le scelte di circolazione.

Di seguito una rappresentazione schematica dei processi in ambito:



1.8. Monitoraggio Infrastruttura

Per raggiungere l'obiettivo di aumentare la sicurezza ed efficientare gli interventi manutentivi, EAV chiede l'implementazione e l'integrazione all'interno della piattaforma di supervisione MOOVA, di un sistema dinamico di monitoraggio della rete e dei veicoli basato sull'applicazione di sensoristica sulle boccole dei carrelli, completamente autoalimentate in grado di comunicare il posizionamento GPS attraverso la rete 5G. Le informazioni registrate dai sensori saranno inviate alla piattaforma centrale MOOVA che rappresenterà sia tutte le anomalie proprie del carrello (rilevamento della temperatura, anomalia acustica dei cuscinetti, profilo ruota, conicità, ovalità, anomalie ammortizzatori) nonché permetterà di rilevare anormalità sui binari e sulla linea elettrica (pantografi).

1.9. Telemedicina

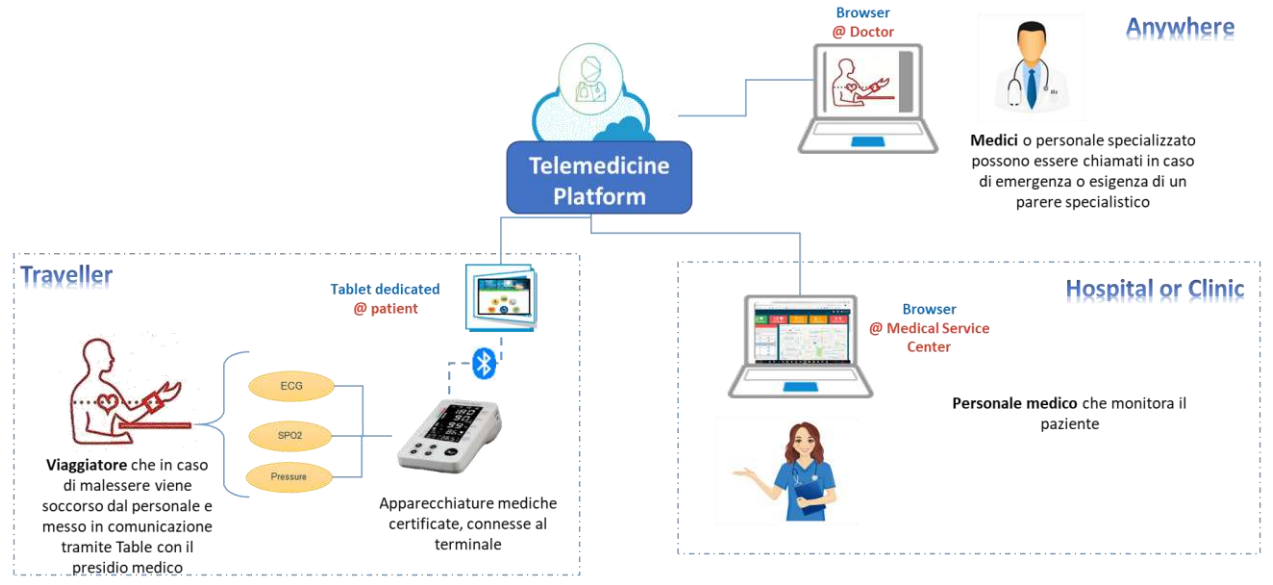
Per garantire la sicurezza della clientela, EAV intende dotarsi di un sistema in grado di eseguire una diagnosi empirica su un soggetto che manifesta segni di sofferenza.

Grazie alla diffusione sul mercato di sensori sanitari in grado di monitorare differenti parametri, il sistema dovrà consentire l'applicazione di un kit di sensori in grado di misurare i parametri del paziente, di rilevarne i parametri vitale e dare una prima empirica valutazione dello stato di salute.

Di seguito un esempio di sensori presenti sul mercato:

Il sistema dovrà condividere in tempo reale i dati ricavati dai sensori (applicati sul paziente) con la sala operativa remota dove un medico, in funzione delle informazioni ricevute, potrà dare una valutazione di massima sullo stato del paziente.

Di seguito una rappresentazione di alto livello dell'architettura e delle figure coinvolte:



1.10. Gestione CND (Controlli non Distruttivi)

L'esigenza è inerente alla ingegnerizzazione dei processi manutentivi relativi ai CND (Controlli Non Distruttivi) e ai moduli e processi di verifica e controllo su componenti che hanno impatto sulla sicurezza ferroviaria.

L'esigenza che EAV intende soddisfare è quella di implementare delle funzionalità sul Sistema SAP in dotazione in uso sia ad Ingegneria della Manutenzione (anche al fine di

gestire le autorizzazioni per gli operatori e relativi certificati ad operare, oltre che alla tracciabilità specifica dei componenti sottostanti ai CND, quali ad esempio Sale, Carrelli, etc.) sia in uso agli operatori di manutenzione (attraverso opportuni controlli e parametrizzazione negli Ordini di Lavoro) al fine di tracciare le attività svolte.

L'esigenza che EAV intende soddisfare è quella di implementare delle funzionalità sul Sistema SAP in dotazione in uso sia ad Ingegneria della Manutenzione (anche al fine di gestire le autorizzazioni per gli operatori e relativi certificati ad operare, oltre che alla tracciabilità specifica dei componenti sottostanti ai CND, quali ad esempio Sale, Carrelli, etc.) sia in uso agli operatori di manutenzione (attraverso opportuni controlli e parametrizzazione negli Ordini di Lavoro) al fine di tracciare le attività svolte.

In tal senso di seguito si fornisce, a puro titolo esemplificativo, una possibile declinazione del cruscotto SAP che dovrà essere fornito ad Ingegneria della Manutenzione di EAV al fine di garantire la gestione del processo in tutte le fasi sopra descritte:

- Gestione anagrafica delle apparecchiature e attrezzature di controllo inerenti ai processi CND
- Abilitazione utenti CND ad operare
- Moduli dei controlli CND espletati (ultrasuoni, etc.)
- Schizzi dei pezzi (disegni o quant'altro utile al processo, non richiede in tal senso implementazione di Sistema Documentale)
- Anagrafica a supporto
- Reportistica

1.11. Gestione Strumenti di Misura

L'esigenza è inerente alla ingegnerizzazione dei processi manutentivi legati agli strumenti di misura utilizzati durante le attività sugli asset ferroviari (materiale rotabile). Si richiede l'implementazione di opportuni controlli sul sistema SAP che certifichino e tracciano l'utilizzabilità degli strumenti di misurazione (quali ad esempio calibri, etc.) sia in termini quantitativi (tempo di utilizzo dello strumento) che qualitativi (intervalli di manutenzione programmata degli strumenti, manutenzione correttiva, etc.) con la parametrizzazione di appositi cicli di lavoro dedicati. EAV metterà a disposizione l'inventario degli strumenti da contemplare nell'esigenza. Al fine degli interventi sul sistema SAP, si ritiene opportuno utilizzare, configurandole ad hoc, le funzionalità presenti nei moduli PM e QM.

Di seguito si fornisce evidenza, a puro scopo esemplificativo, di un possibile dettaglio dei processi di misurazione strumenti. Si precisa che EAV potrà affinare e/o integrare tale esemplificazione in fase di progettazione. In fig, 1 si mostra il processo generale per la

gestione dello strumento, in fig. 2 il dettaglio comprensivo dell'introduzione nel processo del modulo QM.

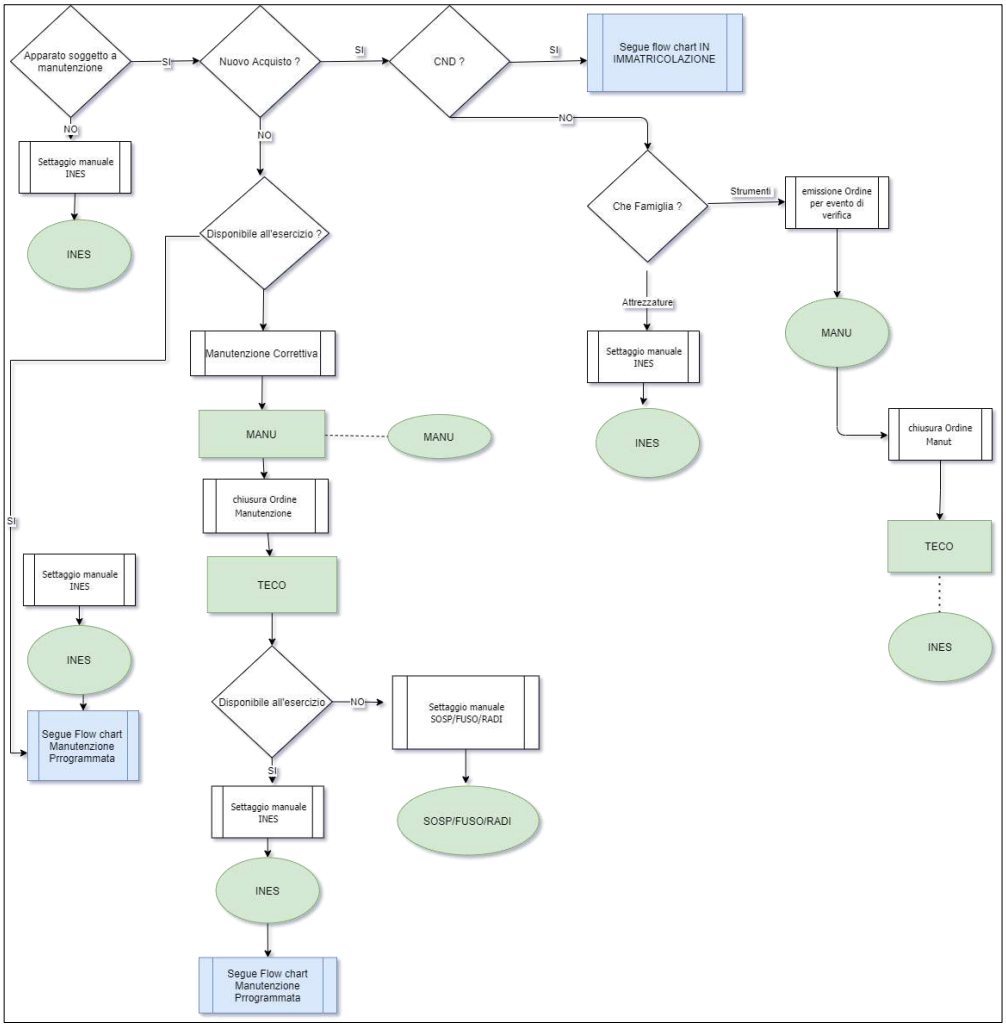


Fig. 1 Flusso esemplificativo del processo di gestione dell'asset per i processi di misurazione

fonte: http://burc.regione.campania.it

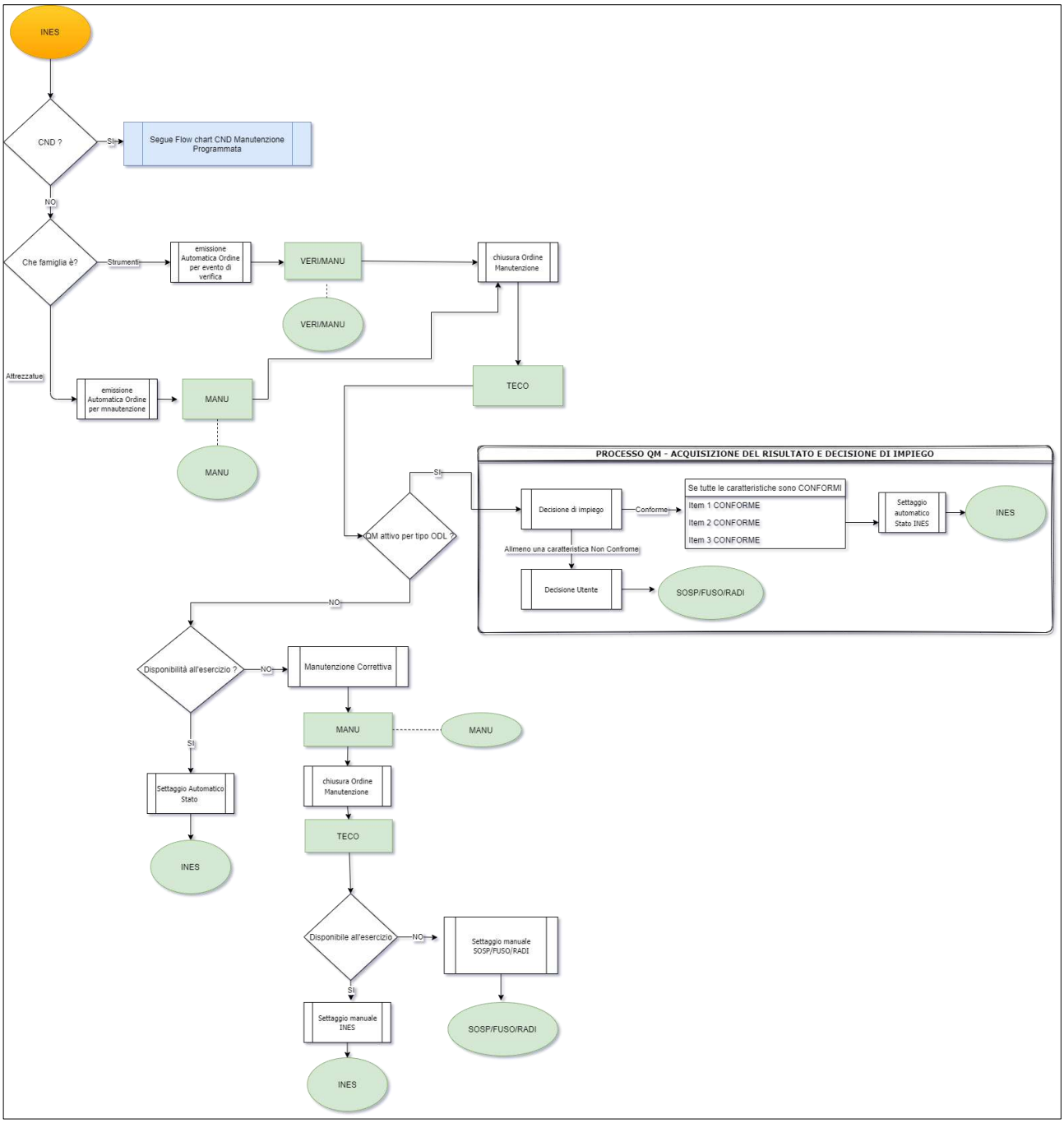


Fig. 2 Flusso esemplificativo del processo di gestione dell'asset (attrezzatura o strumento di misurazione) comprensivo dell'utilizzo del modulo QM

1.12. Stato Corrente Flotta e monitoring KPI

Al fine di aumentare il grado efficienza, di prevenzione e di rilevazione dei guasti, EAV intende dotare ulteriore materiale rotabile al rilevamento telediagnostico.

L'esigenza è quindi inerente all'estensione del rilevamento telediagnostico ad ulteriori flotte, oltre all'attuale Metrostar, secondo le caratteristiche funzionali ad oggi previste per la flotta

Metrostar e concretizzatesi nell'attuale piattaforma denominata Miko integrata con MOOVA in dotazione ad EAV.

Tale soluzione dovrà quindi essere disponibile alle strutture dell'Ingegneria della Manutenzione con le quali deve essere prevista una fase preliminare di analisi al fine di identificare, nello specifico, i rotabili che saranno oggetto del nuovo rilevamento.

In tal senso, in questa sede, vengono anticipate due possibili flotte sulle quali, alternativamente, dovrà essere estesa la rilevazione:

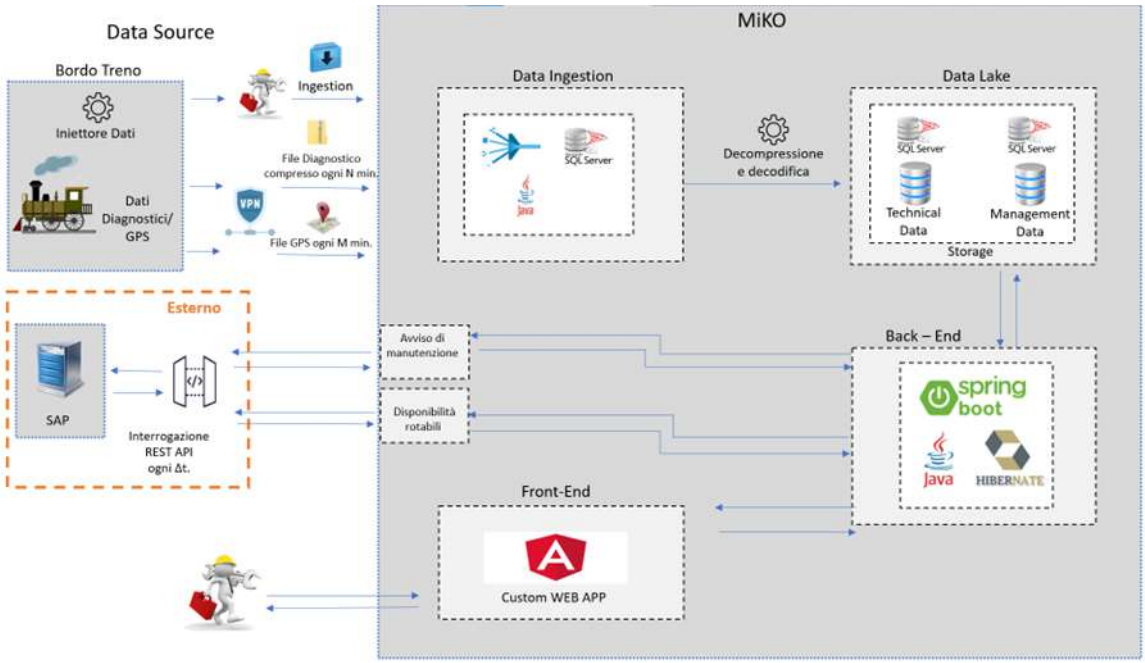
- Ipotesi 1) T21 e FE220
- Ipotesi 2) Alfa Star (ALFA2)

EAV si riserva di identificare, a valle della conclusione della fase preliminare e stante le condizioni propedeutiche del materiale rotabile, a scegliere una delle due ipotesi sopra citate.

Si precisa che l'architettura complessiva, in modo analogo a quanto già realizzato, dovrà prevedere l'integrazione delle informazioni di campo attraverso l'attuale rete EAV.

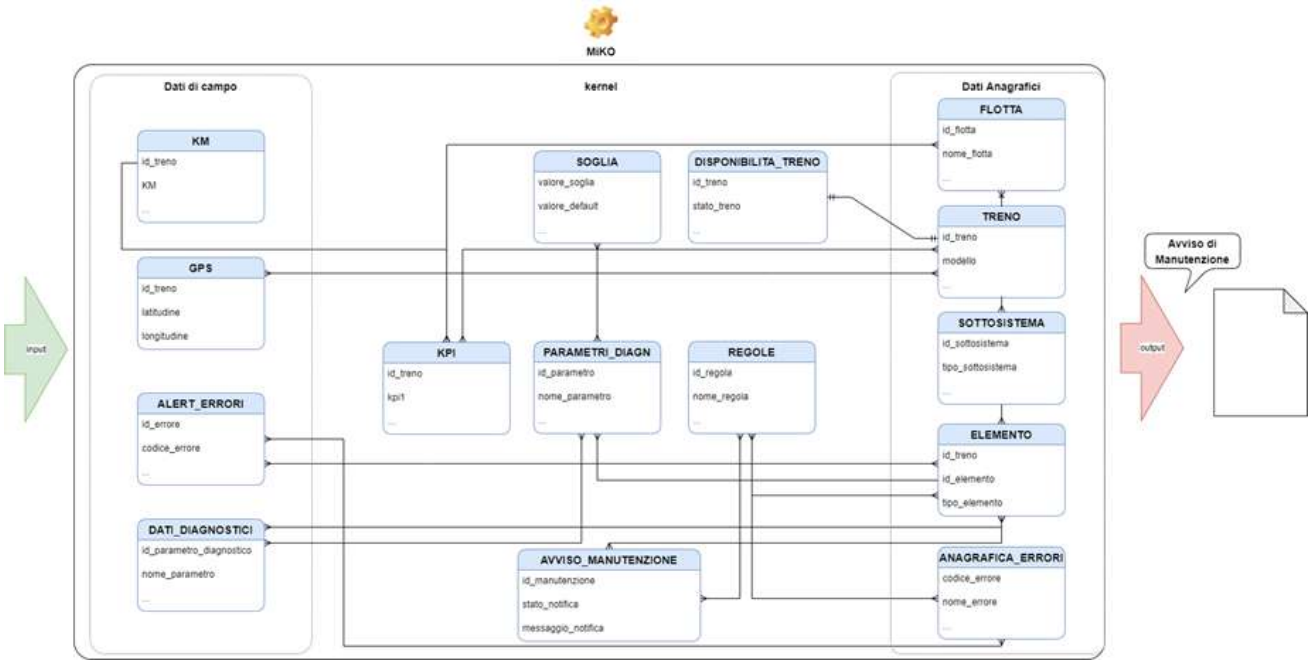
L'architettura di riferimento per l'interazione fra MiKO e sistemi esterni (SAP e/o MOOVA ad esempio) in continuità con quanto ad oggi presente in EAV, dovrà essere di tipo client-server e i servizi esposti dalla piattaforma dovranno essere di tipo REST, consultabili (previa autenticazione) con chiamate http, come da attualmente in essere.

Qui di seguito è mostrata una rappresentazione grafica dell'architettura appena proposta:



Nella figura successiva viene sintetizzato il modello logico E-R attualmente implementato, la cui suddivisione interna prevede le seguenti macroaree e che dovrà essere punto di riferimento per l'estensione alle altre flotte:

- dati di campo (generati dallo spacchettamento dei dati in input del rotabile, caricati a mano dall'operatore oppure trasmessi su cartella remota);
- dati anagrafici (con i dettagli su flotta, treno, sistema ed elemento del sistema);
- kernel di MiKO (contiene le principali entità coinvolte nel processo di monitoraggio e diagnostica).



1.13. Assessment dismissioni App BSP

EAV ha l'esigenza di predisporre un documento di Assessment per la dismissione delle attuali app BSP (sia area manutenzione sia contabilità) con fattibilità di sostituzione delle stesse in modo Isofunzionale con le app Fiori. Il documento di assessment sarà la base per una eventuale attività di progettazione e realizzazione della dismissione delle BSP ad oggi in uso.

1.14. Manutenzione Applicativa

EAV richiede la fornitura di servizi di Application Maintenance sulle personalizzazioni eseguite sui prodotti MOOVA, la maggior parte dei quali costituisce parte integrante del proprio ecosistema di mobilità.

Attività richieste

L'attività di Application Maintenance dovrà essere articolata su tre livelli, così organizzati:

Primo livello	Front-end rispetto all'utenza (costituita dal personale di EAV) e gestione del trouble ticketing
Secondo livello	Attività di Change and Test Management delle applicazioni gestite, attività di supporto applicativo alla conduzione tecnica, monitoring dei processi applicativi automatici schedulati, attività applicative sulla base dati
Terzo livello	Manutenzione correttiva software delle applicazioni, Build and Release management

Esclusioni: le attività di manutenzione evolutiva si intendono escluse dalla richiesta, in quanto saranno previste nell'ambito di altre forniture.

La tabella che segue descrive in dettaglio le attività di Application Maintenance richieste:

Service Management	
Governance delle attività, gestione della comunicazione, reporting ed analisi del livello di servizio erogato	
Assistenza applicativa change management	
Gestire il Change Management del Software applicativo in ambiente di esercizio e di collaudo	Secondo livello
Gestire il Change Management dei dati applicativi in ambiente di esercizio e di collaudo	Secondo livello
Effettuare controlli funzionali verificando la correttezza ed il buon esito di ogni intervento	Secondo livello
Supporto all'Utenza	
Assistenza funzionale al personale di EAV	Primo livello
Gestione dei Processi	
Gestione dei Processi: svolgere giornalmente attività di controllo volte a garantire la piena efficienza dei processi applicativi automatici schedulati	Secondo livello
Gestione applicativa del DataBase	
Interventi applicativi da svolgersi sulle basi dati	Secondo livello
Manutenzione correttiva delle componenti applicative	
Correzione dei malfunzionamenti delle applicazioni	Terzo livello
Build and release management per il rilascio degli interventi di manutenzione correttiva	Terzo livello

Orario di servizio

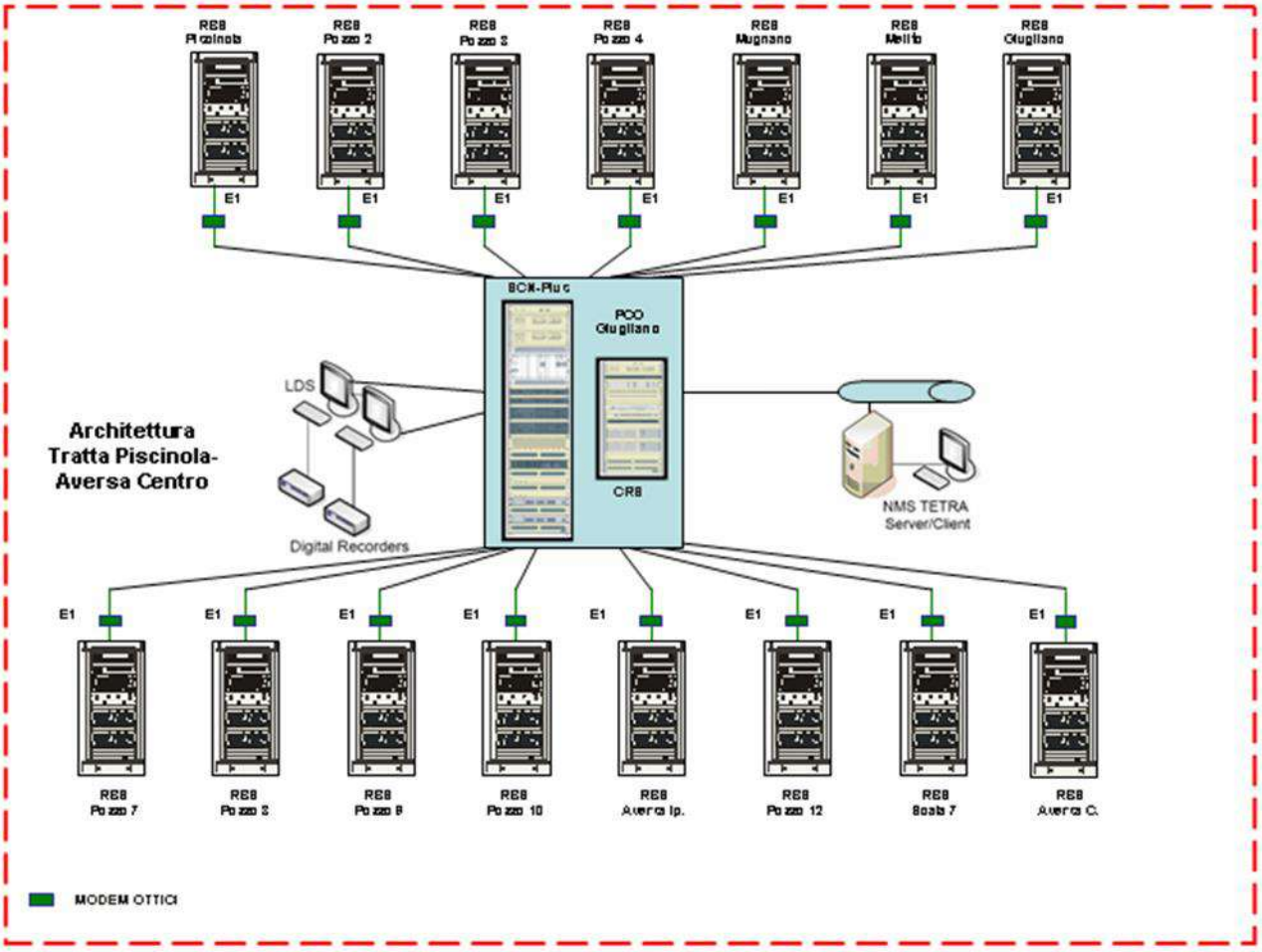
Il servizio di Application Maintenance dovrà essere erogato nei giorni dal lunedì al venerdì (tranne i festivi) dalle ore 09:00 alle ore 18:00.

2. Aumentare la sicurezza nelle stazioni e sulle linee di trasporto

Si prevede lo sviluppo di un sistema a supporto della sicurezza del trasporto non solo nelle stazioni, ma anche lungo le linee di tutta l'infrastruttura oltre che a bordo dei treni.

2.1. SISTEMA TETRA

Il sistema TETRA è in esercizio sulla tratta Piscinola-Aversa Centro ed è costituito da una centrale SCN EPS, Stazioni Radio Base (BS), Control Room Server e sistema di gestione NMS350, apparati terminali radio (VS3000 e PUMA T3), come schematizzato di seguito:



Funzioni principali svolte dal sistema: comunicazioni audio singole, di gruppo, di emergenza, messaggi SDS da posto centrale ad operatori di terra e macchinisti.

Il sistema TETRA dI EAV è da considerarsi come un sistema "vitale" per la corretta operatività del servizio: viste le caratteristiche del servizio operato, il malfunzionamento del sistema TETRA causerebbe il fermo dell'operatività del servizio pubblico, non essendoci più le condizioni di sicurezza richieste dalle normative per poter operare.

Il sistema è stato progettato oltre 10 anni fa ed allo stato non è possibile garantire la riparabilità e la risoluzione dei guasti dovuti a rotture hardware, a causa dell'obsolescenza di alcuni componenti.

Un aggiornamento radicale del sistema è necessario anche per innalzare il grado di protezione generale dal punto di vista della cybersecurity, tenendo presente l'epoca a cui risale la progettazione dell'impianto.

Pertanto, oggetto dell'intervento sarà un radicale upgrade dell'infrastruttura riguardante le componenti centrali del sistema.

2.2. Sistema di video analisi basati su intelligenza artificiale

Sarà implelemtata una soluzione di "Territorial recognition" effettuata tramite soluzioni specifiche tramite DRONI ed elelementi di visualizzazione di campo. Tale sistema sarà utilizzato per la supervisione delle opere d'arte che saranno monitorate sia in logica manutentiva ordinaria che nell'ambito delle valutazioni predittive e additive. Quest'ultimo approccio verrà ottenuto valutando le differenti rilevazione effettuate sul campo, tramite DRONI equipaggiati con ottiche e sensori innovativi, con confornitin real time e in post processing. La sala operativa, centro di coordinamento per eccellenza, funge così da piattaforma di visualizzazione e analisi dei dati messi a disposizione dell'ente dal Sistema; questa attività di raccolta ed analisi dei dati rilevati dal Sistema avviene sia su base storica (frutto di post elaborazioni) che real time e near realtime provenienti dall'APR specializzato. La capacità di fusione dei contenuti avviene sul tavolo tattico: il display multi-touch parte del Sistema, sul quale è installato il relativo software di comando e controllo su base cartografica tridimensionale. Il display garantisce la rappresentazione globale dell'intero quadro operativo al fine di assicurare la migliore interpretazione e contestualizzazione dell'evento. A fine, l'applicativo utilizza una base cartografica che permette la visualizzazione in 3D dell'intera area di interesse.

Sulla mappa in tempo reale vengono rappresentati i vari elementi collaboranti della missione così come tutti gli eventi che richiedono il monitoraggio e quindi tutti i contenuti multimediali scambiati fra i vari nodi.

In particolare, il software consente di caricare diversi layer informativi come, ad esempio, una mappa frutto di una recente acquisizione aerofotogrammetrica di precisione, piuttosto che le mappe

tematiche frutto di indici multispettrali.

Grazie alla sua struttura, il sistema garantisce la creazione di una struttura di rete bidirezionale, fornendo una capacità di condivisione dei dati a matrice collaborativa che permetta l'invio di immagini e dati verso le squadre impegnate per il rilievo al fine indirizzare in modo mirato la loro attività.

L’operatore di sala operativa ha quindi la possibilità di visualizzare simultaneamente tutti i dati e gli elementi provenienti dalle squadre impegnate sul rilievo, potendo così paragonare i dati di precedenti missioni.
Il nodo di sala operativa funge oltre che da supervisore e fusione delle unità distribuite sul territorio anche da data center su cui vengono registrati ed archiviati i dati delle varie missioni con particolare attenzione ai dati dei rilievi effettuati dai droni.
All’interno della sala operativa è inoltre prevista la presenza della componente di processing avanzato in grado elaborare la vasta mole di dati proveniente dai sensori (droni inclusi).
Inoltre il dispositivo è in grado di archiviare tutti i dati rilevati dall’X1 e dal NEST250, ed è in grado di produrre dei report sui voli effettuati.
A seguito di un’attività di sviluppo ingegneristico dedicato e mirato, la piattaforma è in grado di svolgere la funzione di change detection, che consente di valutare le variazioni intervenute nel tempo sul territorio, fornendo preziose informazioni sulla rilevazione della trasformazione di infrastrutture e costruzioni.

Applicativo ARGO

Il software proposto per l’implementazione della soluzione software di comando e controllo su base cartografica tridimensionale è ARGO. ARGO è un framework applicativo di coordinamento tattico e sub tattico multi-dominio in grado di fornire un nuovo livello di situational awareness a favore delle forze sul campo e degli organi di comando tramite un’avanzata visualizzazione cartografica 3D.
Come detto, ARGO è la soluzione che permette la convergenza in un’unica piattaforma divisualizzazione real time di:

- piattaforme UAS (Droni automatici e tattici) o altri sistemi unmanned

- personale e mezzi impiegati su terra, mare e aria
- Sensori all'interno della rete (reti eterogenne e delocalizzate)

L'applicazione ARGO offre una nuova capacità di coordinamento delle risorse grazie alla combinazione di capacità di condivisione in tempo reale dei flussi video/dati proveniente dai droni, o da qualsiasi nodo facente parte della rete, e alla rappresentazione cartografica dello scenario operativo real time.

La soluzione ARGO presenta alcuni indubbi punti di forza:

- **Multi WaveForm**. ARGO ha la capacità di gestire infrastrutture di rete ibride. Da radio tattiche UltraWide Band Manet a sistemi radio narrow band, il motore di rete adattivo "RACE" adatta funzioni e servizi in base al Sistema di trasporto dati disponibile. Oltre ad essere perfettamente integrato con I ricevitori Ultrawide band dei droni può agilmente gestire il bridging verso tutte le piattaforme internet anche satellitari.
- **XPlatForm.** L'applicativo ARGO è nativamente in grado di funzionare su diversi sistemi operativi. Questa caratteristica permette una flessibilità impareggiabile nell'implementazione su larga scala del sistema potendo Dispositivi Windows, Android, IOS, Linux
- **3D Unity Engine.** Il motore grafico di ARGO consente una visualizzazione fluida della cartografia tridimensionale anche quando operato su dispositivi mobile (come smartphone). L'esperienza d'uso Applicativo ARGO, applicazione XPLATFORM in grado di operare su diversi dispositivi windows, IOS, android, ecc..;

Le funzioni principali di ARGO possono essere così descritte:

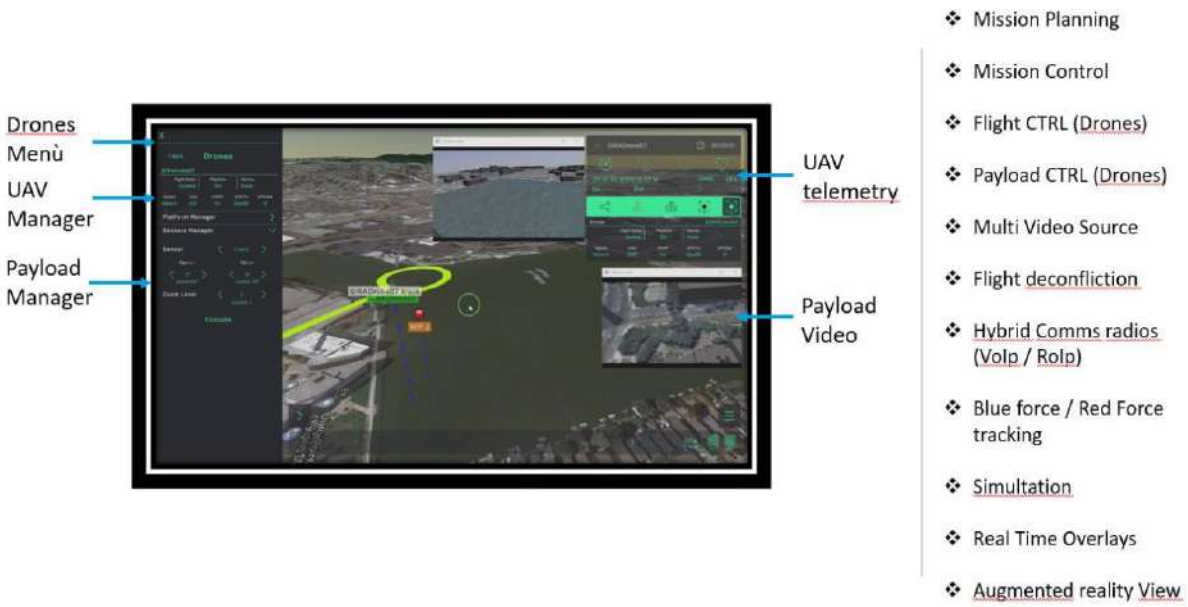
- Capacità di integrazione dei flussi dati/video di tutti i sensori (Droni o altro)
- Gestione sistemi di connettività a supporto delle comunicazioni
- Rappresentazione della COP Common Operational Picture distribuita e configurabile
- Rappresentazione Multi-Layer delle mappe informative frutto del processing near real time

Funzioni specifiche della soluzione consistono in:

- Disseminazione, handhover, remote UAS C2
- VoIP/RoIP, chatting, file sharing

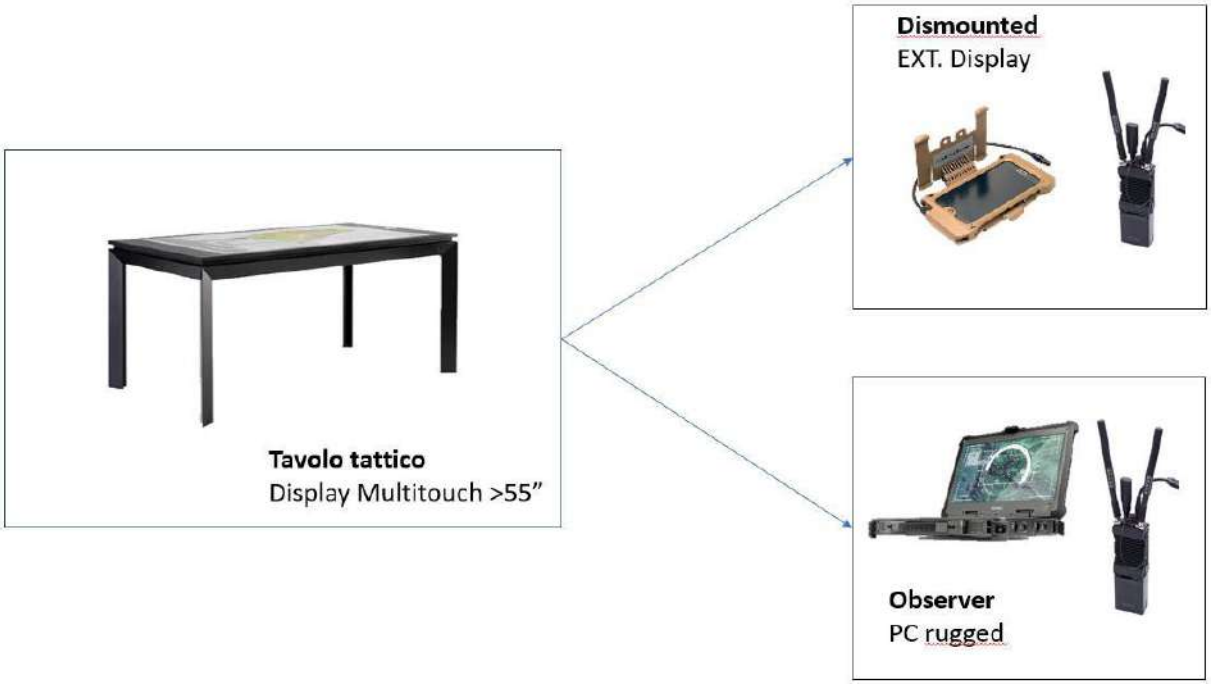
- Pianificazione, mission control e simulazione
- Sovrapposizione cartografica dei flussi informativi provenienti dalle aree di rilievo

L'architettura flessibile di ARGO prevede la possibilità di essere utilizzato su diversi



dispositivi in relazione al contesto di utilizzo e alle necessità operative. In particolare:

- Tavolo tattico (tipicamente in uso presso una sala operativa)
- Observer (PC rugged generalmente in uso presso unita di comando mobili)
- Ext Display (Smartphone rugged per unità appiedate)



Il Sistema è dotato di un’interfaccia utente di immediata lettura ed interpretabilità:
La suite ARGO è fortemente scalabile e consente all’utente di sviluppare applicazioni personalizzate. Questa elevata possibilità di personalizzazione (su piattaforma Xplatform, installabile su ogni tipo di dispositivo e personalizzabile secondo le esigenze dell’utente) permette di ottenere elevati standard di integrazione e scalabilità della soluzione, in linea con le specifiche esigenze della committenza.
La suite infatti è pensata per essere integrata con i sistemi di comando e controllo di classe superiore (C2 strategici di pianificazione) ed il suo motore tridimensionale permette una elevata scalabilità dei layer cartografici ed informativi da parte dell’utente: così sarà possibile ottenere una visuale completa ed integrata di tutti i layer informativi provenienti dai diversi dispositivi ed attori impegnati nella missione. Dati che, elaborati in post processing nella sala operativa, permette la lettura e l’interpretazione real time dei dati geospaziali.
ARGO rappresenta pertanto un’evoluzione del concetto verticistico di Comando e Controllo. In chiave moderna ARGO permette la rappresentazione del medesimo quadro tattico verso tutti i player coinvolti in una missione, in real time. Il nuovo concetto di situational aweranes condivisa e distribuita permette innumerevoli vantaggi:

- Maggiore confidenza operativa fra i vari nodi collaboranti
- Maggiore consapevolezza decisionale

- Tempestività nell'attuazione delle operazioni
- Flessibilità nella riorganizzazione del dispositivo operativo

Caratteristiche SW di sala operativa ed eventuali nodi distribuiti
Cartografia offline raster e vettoriale, 2D e 3D.
Disponibilità su piattaforme iOS, Windows, Linux, Android. (Xplatform)
Cifratura AES256 end-to-end con decifratura esclusivamente su dispositivo periferico.
Capacità di funzionamento contemporaneo su reti server-based e su reti server-less.
Inoltro automatico dei dati tra reti diverse (network fusion).
Creazione di diversi canali logici coesistenti sullo stesso canale fisico per il coordinamento delle sottounità.
Controllo remoto di droni da ogni nodo della rete.
Integrazione di possibili periferiche esterne come sensori e dispositivi di input multimediali (actioncam)

Il Sistema integrato tavolo tattico Xplatform, oggetto della presente offerta, è stato selezionato da un organo di polizia nazionale ed è attualmente in uso presso le loro centrali operative.

Il requisito per tale Organo era quello di gestire, coordinare e sviluppare la capacità di controllo delle coste e dei mari a difesa dell'Unione Europea per il contrasto all'immigrazione clandestina e per il controllo dei flussi migratori verso l'Unione.

Tale Organo ha avviato da alcuni anni un profondo ciclo di rinnovamento ed ammodernamento dei sistemi e delle flotte dove l'innovazione tecnologica riveste una valenza strategica, in quanto favorisce l'incremento dell'efficienza e dell'efficacia dell'attività di contrasto non solo all'evasione fiscale, ma anche agli illeciti in materia di spesa pubblica e alla criminalità economica e organizzata.

In questo contesto il Sistema integrato su tavolo tattico Xplatform rappresenta una eccellente capacità di gestione delle informazioni in grado di valorizzare efficacemente le necessità operative, evitando, al contempo, che si verifichino fenomeni di dispersione dei dati o di sottoutilizzo degli stessi.

Observer

Il Sistema offerto è costituito da un Observer articolato in PC Rugged e sistemi datalink per la ricezione dei dati dai droni e dai vari nodi della rete MANET / LTE.

La console consente piena operatività sia in ambiente chiuso che aperto, e può essere utilizzata all'interno di unità mobili come autoveicoli e presso infrastrutture temporanee. Il sistema offre la possibilità di visualizzazione simultanea e complessiva della missione in corso e dei dati provenienti da velivoli appartenenti ad una medesima flotta e consente altresì la supervisione dello scenario di missione utile a livello tattico per la migliore coordinazione degli assetti durante il volo. L'obiettivo prefisso e raggiunto dal Sistema consiste nell'ottimizzazione dei task di missione e razionalizzazione dei voli.

Aeromobili a Pilotaggio Remoto (APR – Droni) autonomi con Docking Station "NEST"

L'oggetto della fornitura è un sistema drone-in-a-box in grado di effettuare operazioni di sorveglianza e security senza necessita di presidio nel sito da monitorare. L'operatività remota del drone è interamente gestita dal Nest®, ovvero la soluzione brevettata sviluppata da Dronus che svolge le funzioni di base di partenza, atterraggio e stazionamento del velivolo. Una volta completata la fase di volo, Il Nest® è in grado di ricaricare le batterie del drone in modo da garantire operatività continua senza interventi manuali da parte di operatori.

K250 è un drone di categoria inoffensiva del peso complessivo minore di 300 grammi e dotato di una fotocamera Elettro-Ottica ed Infrarossi. Il K250 è dotato di una sofisticata tecnologia di decollo/docking e ricarica completamente autonoma.

Il K250 richiede un addestramento minimo per l'operatore e nessuna abilità di volo.

Gli operatori possono seguire le missioni in tempo reale, direttamente attraverso il sistema di gestione del centro di comando e controllo, o da un'applicazione per dispositivi mobili. Il K-250 è inoltre dotato di un sistema automatico (geo-fencing) che inibisce il sorvolo di aree non autorizzate.

Arianna è un sistema proprietario di localizzazione ad alta precisione progettato appositamente per permettere ai velivoli Dronus una navigazione precisa e sicura anche in condizioni di scarsa o assente copertura del segnale GPS o in ambienti complessi e indoor.

Specifica del sistema

Il Nest® è un sistema, protetto da brevetto nazionale (n. 102018000005252) e brevetto Europeo (n. 3790799), adibito alla gestione delle manovre di rientro in base e di rilascio (decollo/atterraggio). Inoltre, svolge la funzione "protettiva" contro condizioni meteo avverse. Di seguito sono elencate le ulteriori funzionalità della base:

- ricarica delle batterie automatica
- access point per la rete internet
- nodo per le comunicazioni con i droni
- Led per illuminazione esterna (opzionali)
- Camera fissa di videosorveglianza integrata
- Collegamento remoto tramite SIM dati standard (Opzionale)

Dronus Nest®	
Weight	8,5 kg
Dimension	700 x 550 x 350(height) mm
Mechanical I/F	4 screw M8
Power supply	AC 230V
Connectivity	Ethernet, Wi-fi, LTE (SIM non inclusa)
Comms	Wi-fi 2.4 GHz
Oper. Temp	-10°C + 50°C
Video Broadcast	Up to 1080p to 30fps

Il drone K250 ha ottenuto il Report di "inoffensività" rilasciato da EASA che gli permette di essere utilizzato in operazioni BVLOS su aree popolate.
Ad oggi, chiunque voglia effettuare questo tipo di operazione, può farlo solo con un drone in possesso del suddetto Report rilasciato da EASA e Dronus è la prima società a livello

europeo ad averlo ottenuto.

Drone K250 IoT equipaggiato con camera diurna (fino a full HD – 1080p) e camera IR

Dronus K-250 IOT	
MTOW	300g
Frequency	2.400GHz – 2.483GHz
EO Camera	1080p Video (Full HD)
IR Camera	160x120 px 57° FoV
Mission time	16-24min depending on mission profile
Charging time	25-50min depending on mission profile

- Sistema di localizzazione proprietario "Arianna" composto da un minimo di 6 Anchors per sistema
- I/F uomo macchina per PC e/o App di controllo
- Manuale + training

Integrazione ed ICD

Verrà fornito un ICD (Interface Control Document) che fornisce le indicazioni necessarie all'integrazione delle funzionalità del K250 con altri sistemi di videosorveglianza e controllo; come:

Ricezione flussi video in applicazioni di terze parti
Pianificazione ed esecuzione di piani missione
Ricezione telemetria e dati di volo

Funzionalità

Ispezione automatizzata programmata

Il drone K-250 può eseguire servizi di ispezione programmata in automatico, ad esempio a supporto della gestione patrimoniale in luoghi difficili. Le soluzioni autonome Dronus cambiano radicalmente la gestione delle risorse dispiegate in termini di sicurezza, efficienza e precisione. Inserendo dei Waypoints in modo semplificato tramite l'interfaccia utente, il drone può eseguire il percorso in modo automatico stazionando nel punto di interesse/ispezione per un tempo predeterminato, permettendo all'operatore da remoto di controllare e visionare l'oggetto della ispezione.

Monitoraggio Infrastrutture

Il servizio erogato dal drone K250 aumenta la sicurezza delle infrastrutture di trasporto stradale, autostradale e ferroviario, attraverso percorsi programmati in automatico presso i siti di interesse. La soluzione per il monitoraggio di ponti, viadotti e cavalcavia sviluppata da Dronus permette di tenere sotto controllo lo stato di strutture critiche anche con funzioni dedicate per mezzo dell'Intelligenza Artificiale (opzionale).

Sicurezza dinamica e supporto

Il drone K-250 può eseguire una "ronda", su percorso predeterminato, in tempo reale dando un supporto visivo da remoto, grazie alla App, anche agli operatori di vigilanza in movimento. Può anche supervisionare e supportare i punti di ingresso e le stazioni di guardia. La ronda può essere programmata per essere eseguita in modo casuale nel tempo non permettendo la previsione oraria del percorso. Le traiettorie e modalità possono essere concordate a seconda delle esigenze.

Risposta automatica

Quando viene attivato un allarme di sicurezza, il sistema invia automaticamente (se previsto) la posizione della sorgente dell'allarme al drone che, seguendo delle logiche pre-pianificate, decolla in modo automatico raggiungendo il punto "allarmato" e trasmettendo il video in diretta al team di sicurezza nella sala di controllo.
Di seguito sono riportate le funzionalità a disposizione dell'operatore:

- Funzione registrazione video e telemetria
- Supporto di registrazione con capacità di memorizzazione cifrata su memoria di bordo cancellabile a distanza dall'operatore
- Scatta foto con comando rapido one-touch
- Funzione "go-to"
- Funzione che consente al sensore/drone di orientarsi rapidamente verso un punto dell'immagine selezionato dall'operatore, tramite tocco dello schermo o puntamento di mouse.
- "Return-to-home" automatico
- Pilotaggio manual

SISTEMI di ANALISI E RILEVAZIONE DEL TERRITORIO E MORFOLOGICHE

Vengono di seguito riportati gli item previsti nella fornitura:

a) la fornitura di n. 3 sistemi APR, ciascuno dei quali costituito da:

- n. 1 aeromobile (UAV / APR) con capacità VTOL
- n. 1 stazione di comando e controllo integrata per la gestione di aeromobile e payload
- n. 1 sensore elettro-ottico e LWIR (nel campo del Termico) con capacit à ISRT –

  Intelligence, Surveillance, Reconnaissance and Targeting (Payload principale)
- n. 1 sensore Termico Radiometrico
- n. 2 pacchi batterie ad alta densità per ogni UAV
- n. 1 caricabatteria piattaforma aerea, con relativi cablaggi ed adattatore 12V cc
- n. 1 caricabatteria per le Ground Control Station, con relativi cablaggi ed adattatore 12V cc
- n. 1 Flycase per sistema per il trasporto veicolare

  n. 1 licenza life time per sistema del software di missione S-NAV corredato sistema cartografico, sistema di pianificazione missione e sistema di gestione dei sensori di missione
- n. 1 licenza life time dei software per le attività di decriptazione, post-processing, archiviazione ed esportazione dei dati acquisiti dai payload, con geolocalizzazione e rappresentazione cartografica
- n. 1 Kit di manutenzione, costituito da:

- 4 rotori (eliche)
- 4 supporti strutturali dei motori compresivi di ESC

- 4 motori
- 1 set di tool manutentivi per l'esecuzione di tutte le attività tecniche di competenza dell'operatore

b) il servizio di addestramento per 6 operatori/manutentori.

Composizione della fornitura e descrizione del sistema UAS SR-X1 e dei payload di missione

Sulla base dell'oggetto della fornitura previsto viene di seguito descritta la composizione prevista per il sistema proposto con una descrizione e le specifiche dei vari componenti.

UAS SR-X1

Il sistema SR-X1 basato sul velivolo UAV X1 di peso ridotto (inferiore a 2,5 kg nella sua configurazione standard) è orientato a scenari di utilizzo che necessitano della massima flessibilità, tempestività e semplicità di impiego, dove l'impronta logistica deve essere quanto più possibile ridotta. L'intero sistema è di facile trasporto tramite zaini tattici di piccole dimensioni spalleggiabili dal singolo operatore o tramite flycase facilmente trasportabili all'interno di automezzi di classe di segmento C.
Il peso ridotto è associato a caratteristiche tecniche che lo rendono adattabile a diverse tipologie di applicazioni, grazie ad un supporto standard dei vari payload intercambiabili in modalità plug & play rappresentando quindi un valido supporto alle attività investigative peculiari dell'Arma quali:

- sopralluoghi preliminari di siti di interesse per l'acquisizione e/o la verifica di determinati
  obiettivi con trasmissione in tempo reale delle immagini verso una sede remota;
- controlli diretti delle aree di interesse;
- rilievi aerofotografici e fotogrammetrici;
- supporto, verifiche e rilievi post-evento/incidente e ispezione di aree pericolose o inaccessibili;

UAV – X1 segmento velivolo

Il velivolo X1 è un VTOL dal peso e dalle dimensioni ridotte (peso 4kg MTOW) con avanzate capacità ISR elevate prestazioni e intercambiabilità dei payload. Il sistema è facilmente spalleggiabile su zaini di piccole dimensioni, ha tempi di azionamento minimi ed è pensato per operare in scenari tattici complessi e dinamici. È ottimizzato per avere bassa rumorosità e firma visiva in cielo al fine di garantire modalità di missione stealth. Anche se con dimensioni ridotte l'SR – X1 offre 60 minuti di autonomia e capacità ottiche tipiche dei sistemi in classe MINI molto più pesanti.
Il sistema SR-X1 in tutte le sue configurazioni è in fase di certificazione AER(EP).P-2 ed ha avviato l'iter di certificazione EASA ai sensi del Regolamento UE n. 945/2019.

Fattori chiave del velivolo:

- Minima impronta logistica assetto tattico orientato alla massima flessibilità e rapidità di impiego.
- Silenziosità combinata ad elevate capacità di Zoom (DRI) nelle configurazioni payload ISR
- Intercambiabilità dei payload per massime prestazioni day / night e missioni di telerilevamento ambientale e aerofotogrammetrico.
- Sensori EO di supporto alla navigazione e avanzati algoritmi AI integrati

Viene di seguito riportata una tabella di dati caratteristici:

Specifica	Capacità SR-X1	Note
Tipologia	Multirotore VTOL con capacità di decollo e atterraggio verticale pesi ed	Il SAPR è caratterizzato da architettura foldable al fine di ridurre l'impronta logistica nelle

	ingombri ridotti	fasi di trasporto
Peso MTOW	4 Kg	Con payload EO/IR installato
Capacità di carico	1,0 Kg	Il sistema dotato di supporto plug & play deve permette l'innesto di carichi utili fino al peso specificato.
Autonomia	60 minuti	Calcolata in condizione ISA Standard dal decollo all'atterraggio, in HOGE a 20 m di altezza, con Payload EO primario installato e attivo) o a velocità di osservazione non superiore a 4 m/s.
Raggio Operativo	8 km.	Con piene funzionalità dati e video con funzioni mesh a banda larga
Range temperature	L'APR è in grado di operare in condizioni di temperatura -15 °C/+45 °C	Il range di temperatura è in grado di coprire anche scenari di impiego di alta montagna
Tolleranza all'acqua	IP X5	Il sistema offre protezione completa all'acqua per utilizzo con pioggia battente e contatto con la neve
Tolleranza al vento	25 kts incluse raffiche	
Sistemi di sicurezza di missione, funzioni di failsafe	Il sistema dispone di procedure di fail safe per le quali è previsto: atterraggio automatico o ritorno automatico al punto di decollo in caso di avaria,	

	perdita del radio-link o batteria scarica. Le funzioni sono disattivabili dall'operatore	
Sistemi di sicurezza di navigazione, collision avoidance e surface follow	Camera in caccia EO/IR e sensori di collision avoidance frontale e verticale.	Il sistema possiede una specifica camera in caccia EO/IR per rappresentare la soggettiva di volo del drone ad ausilio del pilota. I sensori utilizzati per la collision avoidance sono in grado di operare in condizione diurna e notturna.
Sistemi di sicurezza del datalink	AES 256 bit	la componente datalink è protetta con criptaggio a 256 bit per tutte le comunicazioni previste per il sistema incluso il passaggio di correzioni RTK/PPK
Frequenze e modulazione del datalink	Copertura frequenze datalink: 2.2 Ghz a 2.5 Ghz con tecnologia COFDM.	La tecnologia datalink utilizzata consente la copertura di frequenze libere e allo stesso tempo la possibilità di lavorare su bande licenziate su specifica richiesta da parte dell'ente.

Tecnologia e capacità del sistema datalink	Il sistema offre piene capacità full mesh manet con funzione di broadcasting.	Consente l'interconnessione di più nodi sotto la stessa rete senza necessità di ulteriori dispositivi di rete. Il sistema radio deve permettere l'interconnessione automatica fra drone, GCS, dispositivi di coordinamento locale ed eventuali radio handeld del personale di terra.
Sistemi di sicurezza	Il sistema può installare un terminatore di volo (opzionale)	Il terminatore di volo indipendente e dissimile è conforme alla
	plug and play con paracadute	DO178C DAL B

GCS SR-X1 – segmento di terra

Il segmento di terra è basato sulla Console ground control station universale di Siralab (GCS – Tactical) che è comune a tutti gli UAV. In un dispositivo leggero e compatto dalle caratteristiche Rugged vengono integrati tutti i sistemi ridondati di trasmissione del segnale radio, un tablet ragged panasonic FZ-M1 ad elevata luminosità, le interfacce consentono l'interconnessione con molteplici sistemi di connettività sia tattiche WideBand che LTE per la disseminazione su protocolli proprietari o tramite implementazione di specifiche STANAG. La console tattica permette di effettuare tutte le attività di gestione e pianificazione degli UAV.

GCS Console Tactical

Fattori chiave della GCS Tactical:

- Compatta e con peso 1,4 kg basata su tablet PC Rugged panasonic FZ-M1
- Datalink conforme agli standard DO178C
- Doppio display per le informazioni safety critical. Le informazioni fondamentali di volo sono ridondate su un display dedicato ad alta luminosità con la possibilità di utilizzare

un link secondario a bassa signature RF separato dal link primario ultra wide band.

- Possibilità di prevedere doppia configurazione, singolo operatore e doppio operatore (Velivolo – Payload) con la stessa console GCS.
- Possibilità di utlizzare battery pack hot-swap per estendere la durata della batteria integrata oltre 8 ore di utilizzo continuativo.

Payload Primario ISR-ISTAR EO/LWIR

Il Payload ISR-ISTAR proposto dispone di avanzate capacità DRI grazie ad una innovativa combinazione di sensori Elettrottici e gli avanzati algoritmi di AI di cui dispone la board di real time processing di Siralab integrata nel velivolo.
Il payload è dotato di uno zoom ottico Ibrido 80X (40X Ottico e il 2X digitale) permettono di avere un elevato dettaglio.
Gli algoritmi di processing real time consentono di attivare il targetting di oggetti in movimento, una localizzazione precisa delle coordinate unita alla possibilità di attivare uno spotter laser al fine di indicare la posizione del target.
Il payload offre prestazioni elevate anche dal punto di vista della camera IR, grazie ad una risoluzione di 1280x720 pixel permettendo un'ottima qualità video nell'infra rosso in tutte le condizioni.
Con questo payload riusciamo a raggiungere FOV nel visibile che vanno dai 60° con 1x di zoom fino ai 0.75° utilizzando anche lo zoom digitale, permettendo all'operatore di mantenersi a distanze molto maggiori dal target raggiungendo comunque l'obiettivo della missione.

	Caratteristica	Descrizione
	Peso	- 700g
	Caratteristiche sensori EO	Resolution: up to 1920 x 1080 Zoom : x80 continuous zoom HFOV : 60° WFOV – 1.5° NFOV – 0.75° DFOV
	Caratteristiche dei sensori IR LWIR	LWIR uncooled (8-14µm) Resolution : 1280 x 720
	Stabilizzazione	3 assi con stabilizzazione meccanica ed elettronica. - Pan : 360 ° Pitch: 180° (complessivi meccanica ed elettronica)
	Accuratezza stabilizzazione	- < 50 µrad
	DRI (Johnson criteria)	Target uomo: Detection: 9000 m. Recognition: 2100 m. Identification: 1250 m. Target veicolo: Detection: 13000 m. Recognition: 4500 m. Identification: 3200 m.
	Laser Spotter Targeting	- 850-860nm

Specifiche Payload Termico Radiometrico

Viene di seguito riportata la tabella delle caratteristiche fondamentali del sensore

	Caratteristica	Descrizione
	Banda spettrale	- 7,5 – 13,5 µm

	Range di temperature non in esercizio	-	da -55 °C a +95 °C
	Range di temperature in esercizio	-	da -20 °C a +50 °C
	Full Frame Rate	-	7,5 Hz (NTSC); 8,3 Hz (PAL)
	Risoluzione del sensore	-	640 × 512

Equipaggiamenti di Missione

- n. 1 caricabatteria piattaforma aerea, con relativi cablaggi ed adattatore 12V cc;
- n. 1 caricabatteria per le Ground Control Station, con relativi cablaggi ed adattatore 12V cc;
- n. 1 cassa per il trasporto veicolare;

Kit di manutenzione

Si prevede la fornitura di un kit di manutenzione per sistema al fine di rendere possibile l'intervento di primo livello di intervento on field

- n. 1 Kit di manutenzione, costituito da:
- 4 rotori (eliche)
- 4 supporti strutturali dei motori compresivi di ESC
- 4 motori
- 1 set di tool manutentivi per l'esecuzione di tutte le attività tecniche di competenza dell'operatore

Addestramento

Il servizio di addestramento è previsto per 6 operatori/manutentori. Durante il corso verranno forniti:

- documentazione didattica e tecnica a supporto di tutti i partecipanti;
- corso in lingua italiana;

– utilizzo dei necessari supporti didattici multimediali.

L'addestramento del personale sarà volto a garantire un adeguato livello di familiarizzazione (type rating) col sistema APR offerto.

Tabella di Ricapitolazione Forniture

ITEM	Details	Nr.
Tavolo tattico Xplatform con applicativo ARGO		**1**
Observer		**1**
Sistema Nest+k250+Arianna (compresa installazione e servizi*3 anni)		**3**
Nest+k250+Arianna		**3**
SR-X1 + batterie	Velivolo X1 + due batterie	**3**
Ricevitore Radio Velivolo	Datalink Manet ultrawideBand UAS	**3**
GCS SCC	Ground Control Station Pilota	**3**
Trasmettitore Radio a terra	Handheld Manet	**3**

PL EO/IR	Payload Dragoneyes Nextvision 3 Assi: 40X FOV 60° WFOV – 3° NFOV – 1.5° DFOV THERMAL RESOLUTION 640 x 480	**3**
Termico radiometrico	Mapper IR: payload radiometrico in grado di misurare il valore di temperatura assoluto di ogni punto dell'immagine. Il sensore è in possesso delle seguenti caratteristiche: • Banda spettrale 7,5 – 13,5 µm • Range di temperature non in esercizio da -55 °C a +95 °C • Range di temperature di esercizio da -20 °C a +50 °C • Full Frame Rate 7,5 Hz (NTSC); 8,3 Hz (PAL) • Risoluzione del sensore 640 × 512	**3**
Logistica	Flycase Sistema X1 + carcicabatterie + kit manutenzione	**3**
Addestramento	**Formazione per n.6 piloti/ manutentori**	**1**

2.3. Rete di apparati mobili multifunzione

Verrà implementato un sistema mobile per il supporto al rilevamento e per la gestione degli allarmi di campo, in capo a controllori, macchinisti e biglietterie, al fine di inviare messaggi, dati ed informazioni alla corporate aziendale a tutela del patrimonio umano e strumentale aziendale. Nel contempo tale sistema sarà capace di emettere biglietti mediante SVR e/o multe per mancanza di biglietti.

Tale sistema sarà costituito da diversi dispositivi funzionali all'attivazione di specifici servizi. Ad esempio saranno previsti dispositivi mobili, in dotazione al personale viaggiante delle divisioni EAV Ferro e Gomma, che contribuiranno alla gestione dei seguenti processi:

- Rilevamento di criticità a bordo mezzo mediante la possibilità di inviare in centrale operativa EAV un segnale di allarme afferente le seguenti casistiche:
- Allarme treno, richiesta nuovo materiale;
- Allarme treno, richiesto intervento operatore;
- Richiesto intervento forze dell'ordine a bordo con segnalazione posizione del treno/autobus;
- Richiesto intervento squadra security EAV;
- Altro.
- Emissione del biglietto a bordo mezzo (autobus/treno) in forma digitale e contemplante la possibilità di pagamento mediante carta di credito;
- Emissione delle sanzioni a bordo mezzo (autobus/treno) in forma digitale e contemplante la possibilità di pagamento mediante carta di credito o forma differita presso uffici postali/portale web EAV;
- Centralizzazione del dato di vendita/sanzione in tempo reale presso piattaforma MOOVA per le attività di rendicontazione/altra gestione;

Tale sistema sarà realizzato per il raggiungimento dei seguenti obiettivi:

- Migliore gestione del dato di vendita e aumento della sicurezza del personale viaggiante in quanto viene emesso il biglietto al momento in forma cartacea eliminando "valore" al portatore, inoltre la possibilità di pagamento con carta riduce l'utilizzo di denaro contante (riduzione furti/rapine);
- migliore gestione del dato in forma digitale, aumento dei servizi all'utenza e maggior sicurezza per il personale viaggiante in quanto il pagamento, con carta/differito su portale EAV, riduce l'utilizzo di denaro contante (riduzione furti/rapine);
- Nell'ambito di tale intervento si prevede l'adozione ed attivazione di un sistema a supporto degli operatori nei casi in cui si verifica un incidente, oppure un urto con altro mezzo, piuttosto che nei casi di atti vandalici.

Tale sistema, costituito primariamente da un app mobile consentirà l'attivazione dei seguenti servizi:

- URTO CON ALTRO MEZZO: il conducente di un mezzo potrà effettuare delle fotografie ai danni del mezzo del terzo soggetto ed al bus che verranno inviate ad un sistema centrale di gestione
- MONITORAGGIO SCOCCHE: ogni conducente dei bus, al momento della presa in carico del mezzo all'uscita del deposito, potrà effettuare delle foto alle scocche per rilevare anomalie significative
- URTO CON OSTACOLO: il conducente di un mezzo potrà effettuare delle fotografie ai danni del proprio mezzo al verificarsi di un evento di questo tipo
- ATTI VANDALICI: il conducente di un mezzo potrà effettuare delle fotografie ai danni del proprio mezzo al verificarsi di un evento di questo tipo

Per garantire, poi, un utilizzo corretto e conforme rispetto alle policy aziendali dei dispositivi mobili forniti in dotazione al personale EAV nell'ambito delle relative mansioni, verrà introdotto un sistema MDM (Mobile Device Management).
L'MDM rappresenta una metodologia collaudata dotata di una serie di componenti volti a fornire strumenti e applicazioni di produttività mobile alla forza lavoro, salvaguardando nel contempo la sicurezza dei dati aziendali.
I dispositivi mobili aziendali, offrendo l'accesso a dati aziendali critici, possono costituire un pericolo, specie se hackerati, rubati o smarriti. La gestione dei dispositivi mobili si è perciò evoluta ed è cresciuta di importanza: ai responsabili IT e della sicurezza è oggi richiesto, nei rispettivi ambienti aziendali, sia di fornirli, che di gestirli, che di metterli in sicurezza.
Con una piattaforma MDM matura, i reparti IT e sicurezza potranno gestire tutti i dispositivi dell'azienda, indipendentemente dal tipo e dal sistema operativo. Una piattaforma MDM efficace aiuta a mantenere in sicurezza tutti i dispositivi rendendo nel contempo la forza lavoro flessibile e produttiva. La soluzione si integrerà con l'ecosistema EAV a beneficio di una rapida messa in servizio e nell'ottica di una sempre più spinta gestione integrata.

3. Aumentare la resilienza dei servizi offerti e dell'infrastruttura IT

I servizi legati all'ITS diventano sempre più strategici al fine di assicurare l'efficienza, la sicurezza, la soddisfazione dei passeggeri e la sostenibilità del TPL. Tali servizi sono erogati tramite una infrastruttura di DataCenter che gestisce un'enorme quantità di dati in tempo reale (dati che sono essenziali per il funzionamento del sistema) ed una complessa infrastruttura di rete/trasporto.

Se tali infrastruttura non fossero resilienti, potrebbero verificarsi interruzioni del servizio, errori di elaborazione dei dati e tempi di risposta lenti, che potrebbero causare disagi ai passeggeri e ritardi dei mezzi. Inoltre, tali infrastrutture sono esposte a potenziali minacce esterne, come attacchi informatici o eventi naturali, che potrebbero compromettere la sicurezza dei dati e mettere a rischio l'affidabilità del sistema e quindi la continuità operativa di tutti i servizi che ne derivano.

Pertanto, per garantire la continuità del servizio e una buona qualità di fruizione dello stesso è essenziale che per l'infrastruttura di DataCenter vengano adottate misure di sicurezza informatiche adeguate, procedure costanti di controllo della qualità ed una corretta manutenzione dell'hardware e del software, tutto ciò monitorando costantemente il sistema e testando regolarmente la sua resilienza attraverso esercitazioni e simulazioni di emergenza.

Tutto questo ha fatto emergere l'esigenza di centralizzare in ottica cloud gli applicativi in una apposita area del DataCenter di Regione Campania (che può assicurare una gestione specialistica e sicura delle attività), prevedendo un ampliamento della struttura attuale da dedicare alle infrastrutture della mobilità.

Oltre agli aspetti tecnologici con il progetto si realizzeranno e adotteranno anche le istruzioni operative necessarie a garantire la compliance tra le tecnologie acquisite e le procedure di Gestione del Sistema Qualità ISO 27001 (certificazione ottenuta da EAV ad aprile 2023)

Essendo la rete l'elemento fondante per sostenere il cloud, sarà necessario andare a potenziare le infrastrutture di rete ed i meccanismi di controllo, in modo complementare ad altri interventi già in atto, secondo gli aspetti di seguito elencati:

a) aumentare l'affidabilità e la disponibilità dell'interconnessione dell'intera infrastruttura IT;

b) incrementare la resilienza cyber a livello centrale e periferico, in linea con le direttive del perimento nazionale di sicurezza;
c) ridurre la complessità dell'Operation Management.
d) monitoraggio dell'infrastruttura con control room dedicata.

L'Ente Autonomo Volturno si pone pertanto l'obiettivo di costituire un'infrastruttura tecnologica che possa essere solido fondamento per l'erogazione dei servizi IT, sia di quelli attualmente in essere sia quelli innovativi come la gestione delle informazioni ai cittadini (PIS), controllo accessi, pagamenti, videosorveglianza, fonia VoIP etc etc. Inoltre, è obiettivo dell'Ente aumentare significativamente il livello di sicurezza di rete attraverso il meccanismo della segregazione, aderendo così alle raccomandazioni del perimento nazionale di sicurezza e delle principali raccomandazioni internazionali (NIS).

Pertanto in definitiva, si intendono implementare le seguenti azioni:

1. Realizzazione in un'apposita area del CED di Regione Campania, del "sistema cloud" dei servizi IT anche al fine di assicurare una gestione specialistica e sicura delle attività, prevedendo un ampliamento della struttura attuale dedicata alle infrastrutture della mobilità; il tutto previa una fase di assessment sui livelli di sicurezza/rischio dell'infrastruttura esistente sulla quale si andrà ad innestare questo intervento;
2. Adozione di misure di sicurezza informatiche adeguate anche mediante la redazione di procedure di controllo della qualità e della corretta manutenzione dell'hardware e del software, monitorando costantemente il sistema e testando regolarmente la sua resilienza attraverso esercitazioni e simulazioni di emergenza.
3. Assicurare un processo di formazione avanzata per il personale specialistico sia del CED della Regione Campania che del CED EAV
4. Implementazione di un'infrastruttura di rete sicura, attraverso l'installazione e la configurazione di apparati tecnologici abilitati a rendere la rete EAV resiliente e monitorata.

Gli apparati tecnologici implementeranno:

a) Funzioni SD-WAN con controllo delle policy centralizzato, implementazione di politiche di bilanciamento di carico di rete e di politiche di qualità del servizio su base applicazione/utente.

b) Funzioni di autenticazione e crittografia del traffico di rete.
c) Segregazione dei domini di rete locale attraverso la gestione del routing/policy di sicurezza
d) Generazioni di big data relativi ai flussi di traffico intercettati e gestiti
e) Implementazione di una piattaforma per il controllo degli accessi fisici e logici che consenta il monitoraggio dei sistemi e degli utenti che si connettono alla rete dell'EAV e la gestione delle politiche di accesso alla stessa, sia dei dispositivi sia degli utenti.
f) Servizi di valutazione del rischio digitale attraverso attività atte ad individuare e valutare la superfice d'attacco esterna all'Ente Autonomo Volturno per indentificare potenziali imminenti minacce e stabilire se ci sono utilizzi malevoli dei domini dell'amministrazione.

L'implementazione delle misure descritte porta ad ottenere i seguenti benefici

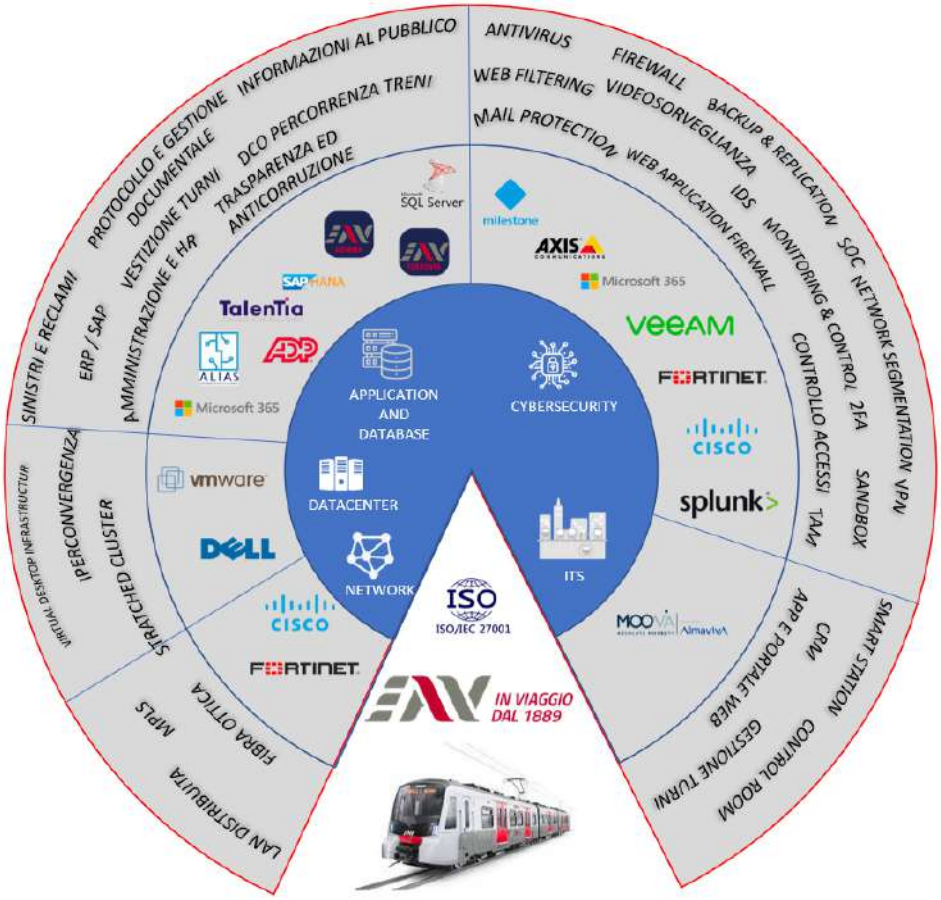
1. Aumento della resilienza dei servizi ITS, del servizio di connettività ed aumento delle prestazioni
2. Indipendenza da operatori (ISP) e servizi di connettività
3. Agilità nella modifica della postura della rete geografica, dei fornitori di connettività, della attuazione delle politiche di sicurezza e di qualità del servizio
4. Predisposizione all'adozione sicura di servizi IT in modalità cloud e cloud-ibrido
5. Raccolta e rappresentazione delle misure di traffico utilizzabili ai fini del monitoraggio in tempo reale delle prestazioni di rete, dell'utilizzo delle risorse e del capacity planning, dell'analisi comportamentale
6. Segregazione dei domini di rete per la resilienza agli attacchi attraverso il contenimento dei movimenti laterali, per la conformità alle raccomandazioni del perimento nazionale di sicurezza e delle principali raccomandazioni internazionali (NIS)
7. Riduzione del rischio derivante da attacchi interni grazie al controllo automatico degli accessi dei dispositivi e degli utenti, monitoraggio in tempo reale di asset e utenti connessi alla rete e della loro postura di sicurezza. Riduzione dell'attività operativa grazie all'automazione della gestione della rete.
8. Riduzione del rischio di errori di configurazione e semplificazione operativa mediante la centralizzazione e l'automazione dell'attuazione delle policy del configuration management.

3.1. Il cloud dei servizi IT

EAV intende sviluppare in un'apposita area del Data Center di Regione Campania, il cloud dei servizi IT anche al fine di assicurare una gestione specialistica e sicura delle attività. Per poter implementare tale infrastruttura sarà duplicata l'architettura di EAV al fine di poter costruire un DR operativo in sede distaccata previo adeguamento tecnologico delle aree che saranno messe a disposizione dalla Regione Campania. Le necessità del DR saranno focalizzate sui sistemi strategici, ma sarà in ogni caso predefinita la consistenza del funzionamento DR come da best practice e indicazioni della direttiva NIS II.

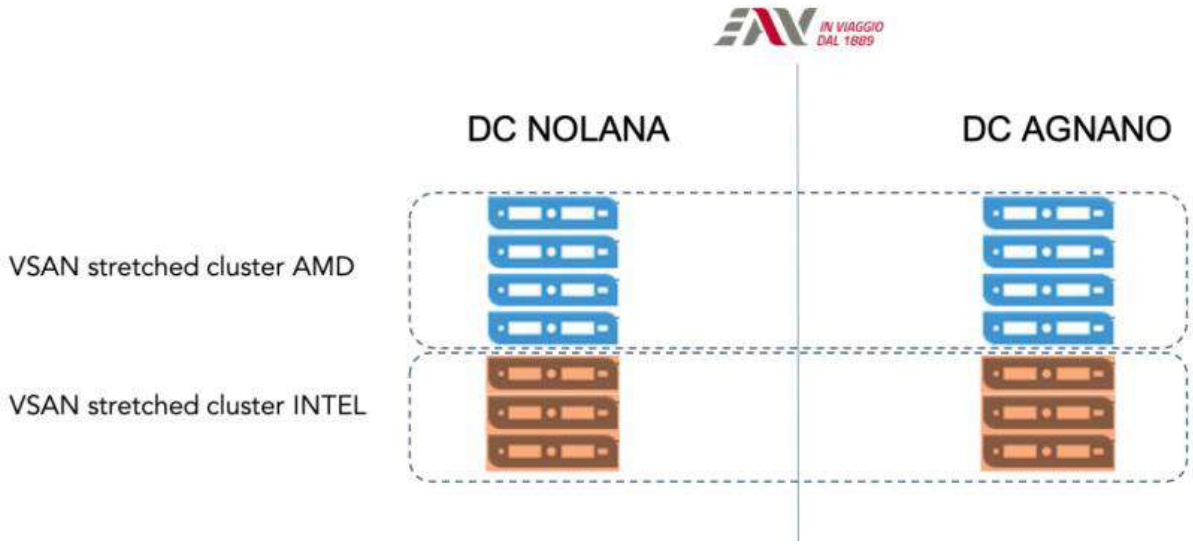
Attualmente la consistenza in termini di server presenti presso i DataCenter EAV di Agnano e Porta Nolana è pari a circa 40 nodi DELL (tra biprocessori e quadri processore Intel e AMD). Mediante il collegamento in fibra ottica tra il DataCenter di Porta Nolana di EAV ed il DataCenter di Don Bosco di Regione si garantirà la continuità operativa dell'infrastruttura tecnologica. Per traguardare l'obiettivo, nell'ambito dell'allestimento del sito di DR, oltre che i sistemi hardware, dovranno essere acquisiti sistemi di virtualizzazione e gestione dell'infrastruttura. Attualmente i sistemi di virtualizzazione in EAV sono VMVare e Nutanix. Al fine di garantire la continuità e la compatibilità dei sistemi si definiranno con Regione Campania le caratteristiche tecniche dei software da acquisire.

Di seguito si riporta lo schema dei software, dei sistemi e dei vendor presenti in EAV:



Ad oggi, una parte dell'infrastruttura DataCenter di EAV è in Business Continuity. L'infrastruttura in BC è costituta da una soluzione iperconvergente basta su tecnologia Vmware VSAN 7 ed implementata mediante l'utilizzo di 2 stretched cluster tra i DataCenter di Nolana ed Agnano così come schematicamente riportato in figura:

fonte: http://burc.regione.campania.it



Tale implementazione consente ad EAV di fruire di una continuità operativa in caso di fault e/o non disponibilità temporanea e/o permanente dei nodi server che insistono su uno dei 2 DataCenter. Ad ogni modo non esistono piani di test e di business continuity che possano certificare/garantire l'affidabilità della BC al momento del bisogno. Inoltre, la presenza di server con tecnologie di processore differenti ha comportato l'impossibilità di creare un unico streatched cluster e pertanto, in termini di Business Continuity, le VM che insistono sul cluster AMD non possono essere spostate a caldo (per opportunità o per necessità) sul cluster INTEL e viceversa. Ad ogni modo l'attuale infrastruttura garantisce l'esercizio dei sistemi IT di EAV a beneficio dell'intera organizzazione anche se andrebbero effettuate alcune attività specialistiche di ottimizzazione al fine di consentire alla stessa di operare al meglio ed in efficienza.

L'altra parte che gestisce il sistema MOOVA e SAP/H4 è in ambiente Nutanix senza nessuna politica di Business Continuity, insistendo l'infrastruttura server sottostante esclusivamente presso il DataCenter di Porta Nolana.

3.2. Infrastruttura di rete sicura e resiliente

La modernizzazione di un'infrastruttura WAN non riguarda solo la sostituzione di hardware o software fuori uso; la riprogettazione dell'edge WAN è una soluzione aziendale e non semplicemente un requisito tecnologico.

SD-WAN è una delle principali innovazioni alla base della modernizzazione dell'edge WAN. Le sue capacità principali includono il controllo multi-percorso, il riconoscimento delle applicazioni (come con le soluzioni SaaS) e il conseguente governo dinamico delle applicazioni. Queste capacità permettono l'instradamento del traffico di rete su Internet pubblico o su infrastruttura privata (MPLS), sul percorso più efficace per garantire una user experience più efficiente, delle prestazioni ottimizzate e una disponibilità elevata delle applicazioni. La Digital Transformation è il driver per la modernizzazione del branch edge.
Le organizzazioni stanno avviando progetti per affrontare nuovi modelli di connettività WAN (MPLS, banda larga, LTE, 5G), consolidamento dei dispositivi perimetrali (router, firewall, sicurezza avanzata, ecc.) e aggiunta di funzionalità SD-WAN per migliorare esperienza dell'utente della filiale, mantenere le prestazioni delle applicazioni e aumentare la disponibilità delle applicazioni.
L'architettura della soluzione SD-WAN è composta dai seguenti elementi:

- Edge Devices: i nuovi apparati SDWAN sono responsabili dello startup degli overlay (tunnel IPSec tra le sedi secondarie e le sedi principali e tunnel tra le varie sedi on demand in caso di comunicazione sede a sede) su cui instradare tutto il traffico Intranet.
- Gestione Centralizzata: utilizzata per gestire centralmente i vari Edge device implementando la configurazione su tutte le sedi: Overlay, Underlay, SD-WAN policy, Security Policy, Zero Touch Provisioning.
- Log & Reports Centralizzato: dove è possibile raccogliere centralmente i log generati dai vari Edge Device e fornire informazioni circa il traffico gestito su un sistema centralizzato.
- Monitoraggio apparati mediante una room specializzata.

Tutte le aziende stanno attualmente vivendo una fase di trasformazione digitale per migliorare la soddisfazione dei clienti e aumentare la produttività dei dipendenti. Le sedi remote sono essenziali nel modo in cui forniscono i propri prodotti e servizi e quelle sedi sono in genere in prima linea nell'innovazione digitale. Il maggiore utilizzo di piattaforme basate su cloud e applicazioni SaaS, la popolarità del BYOD e l'ampia varietà di dispositivi IoT stanno mettendo a dura prova la rete delle filiali. Espandendo il concetto di connessioni WAN controllate da software, è possibile estendere tale controllo remoto alle reti cablate e wireless

delle filiali con una soluzione chiamata SD-Branch. L'approccio SD-Branch, applicato al mondo delle stazioni, fornisce una soluzione di rete e sicurezza complete e integrate comprensive di funzionalità SD-Wan, routing, Ethernet, Wi-Fi, controllo dell'accesso alla rete e firewall di nuova generazione. Il provisioning di nuove stazioni diventa così rapido e semplificato ed è possibile ridurre i costi complessivi della componente di operation nonchè fornire una sicurezza integrata e completa.

3.3. Descrizione soluzione

La soluzione Secure SD-WAN offre sicurezza di nuova generazione e funzionalità di rete per migliorare l'efficienza della WAN di stazione senza compromettere la sicurezza, garantisce lo stesso livello di funzionalità fornito dai fornitori di SD-WAN pure-play, supportando tutti i casi d'uso comuni, con sicurezza avanzata integrata in un'unica offerta. La soluzione è supportata da test indipendenti per offrire un'esperienza di qualità eccellente per voce e video, un elevato throughput VPN e il miglior rapporto prezzo/prestazioni. La funzionalità SD-WAN è stata sviluppata internamente in modo organico ed è una caratteristica di ogni modello FortiGate. I processori di sicurezza appositamente progettati (SoC e ASIC) e l'intelligence sulle minacce informatiche di FortiGuard Labs garantiscono ulteriormente che la sicurezza sia parte integrante della soluzione SD-WAN di Fortinet.

Le funzionalità SD-WAN sono integrate all'interno del sistema operativo FortiGate FortiOS, i processi decisionali, di scelta del percorso e di rilevamento dell'integrità del percorso sono locali e distribuiti su ogni singolo dispositivo perimetrale WAN. Le configurazioni delle logiche SD-WAN, delle politiche di selezione del percorso, delle policy di sicurezza e della componente Overlay sono generalmente centralizzate. Ogni elemento periferico della soluzione SD-WAN è completamente autonomo e un'architettura SD-WAN distribuita continuerà a funzionare con o senza connettività all'infrastruttura di controllo/gestione centrale. Poiché ogni elemento periferico è responsabile del proprio processo decisionale e del monitoraggio end-to-end, la soluzione diventa veramente altamente scalabile. Fortinet SD-WAN sfrutta i molti anni di esperienza nel networking e nella sicurezza, inclusa la capacità di rilevamento delle applicazioni di livello 7, funzionalità di rete ottimizzate per hardware e software.

SD-WAN funziona instradando le applicazioni sulla connessione WAN più efficiente in qualsiasi momento, per garantire prestazioni applicative ottimali. È possibile identificare un'ampia gamma di applicazioni e applicare policy di routing a un livello molto granulare utilizzando un database di controllo delle applicazioni con firme che ad oggi permettono il riconoscimento di oltre 4.000 applicazioni con firme aggiunte e aggiornate regolarmente dal servizio di intelligence sulle minacce di FortiGuard Labs. FortiOS utilizza anche un Internet Service DB locale su ciasun FortiGate e costantemente aggiornato dai Fortiguards Labs contenente una combinazione di IP e porte TCP dei principali servizi Internet che permette di identificare e classificare le applicazioni (anche il traffico di applicazioni cloud crittografate) fin dal primo pacchetto.

Specificando i criteri di qualità da soddisfare per ciascuna applicazione, insieme alla definizione di SLA rigorosi basati su una combinazione di metriche di jitter, perdita di pacchetti e latenza, il FortiGate seleziona il collegamento corrispondente in base alle regole SD-WAN applicate. È possibile implementare diverse regole, dando priorità alle prestazioni del collegamento, alla larghezza di banda o al bilanciamento del carico rispetto ai collegamenti disponibili.

Le funzionalità di implementazione semplificate di Fortinet Secure SD-WAN consentiranno ad EAV di spedire appliance FortiGate NGFW in ogni stazione con relativo provisioning attraverso consolle centralizzata.

L’architettura della soluzione Fortinet Secure SD-WAN è composta dai seguenti elementi:

- **Edge Devices**: i FortiGate implementati presso le stazioni che implementano le funzionalità di SD-WAN e di Next Generation Firewall. Sono responsabili dello startup degli overlay (tunnel IPSec tra le stazioni secondarie e le principali e tunnel tra le varie sedi on demand in caso di comunicazione sede a sede).
- **Gestione Centralizzata**: il FortiManager è l’elemento responsabile di gestire centralmente i vari FortiGate implementando la configurazione (Overlay, Underlay, SD-WAN policy, Security Policy, Zero Touch Provisioning...) sui vari FortiGate.
- **Log & Reports Centralizzato**: il FortiAnalyzer è l’elemento responsabile di raccogliere centralmente i log generati dai vari FortiGate e di fornire informazioni circa il traffico gestito e genera reports che riassumono gli aspetti salienti.

La soluzione Fortinet ha anche la capacità di estendere l'ecosistema Software Defined a LAN e servizi Wi-Fi collegati localmente per fornire Secure SD-Branch. Questi servizi sono integrati nella piattaforma FortiGate e il FortiManager è l'unico pannello di configurazione e la piattaforma Zero Touch sia per Secure SD-WAN che per Secure SD-Branch.

3.4. Elementi di Sicurezza

La sicurezza integrata nella CPE è una peculiarità della soluzione Fortinet, altri vendor tipicamente adoperano terze parti per aggiungere capacità di sicurezza di tipo NGFW alla soluzione, sfruttando logiche di tipo VNF Service Chaining o soluzioni di security in Cloud, che richiede che tutto il traffico venga tunnellizzato verso i datacenter di questo vendor per essere ispezionato, facendo cadere i benefici del local breakout per l'accesso diretto ad Internet presso i vari branch, oltre che, di fatto, aggiungendo complessità all'architettura complessiva che non può essere così gestita per tutte le sue componenti da un'unica console. Integrare sicurezza ed SD-WAN in una singola appliance si traduce anche in riduzione dei costi e semplificazione e consolidamento della gestione attraverso un single-pane-of-glass, che aiuta anche ad abbassare i costi operativi. La riduzione dei costi è da sempre uno dei driver del SD-WAN.

L'approccio di Fortinet nel fornire una soluzione SD-WAN è quella di integrare le diverse funzionalità disponibili in una soluzione SD-WAN con le funzionalità di sicurezza Next Generation Firewall consolidate e comprovate da decenni di sviluppo sugli apparati FortiGate. Fortinet implementa le diverse funzionalità necessarie accelerandole in HW (SOC4, NP7, CP9), questo consente per esempio il riconoscimento delle applicazioni dei clienti (Skype, Salesforce, Office 365..) mediante Deep Packet Inspection e SSL Inspection, così che sia possibile scegliere esattamente quale applicazione cliente deve essere instradata, su quale link (MPLS, Internet..) e con quale politica (Bilanciamento, SLA, Throughput Massimo..).

Il FortiGate offre varie funzionalità di sicurezza NGFW convalidate da terze parti, tra cui:

- Web/Video filter,
- Anti-Virus (con disponibilità firme Anti-Malware specifiche e dedicate per Mobile Malware e per Industrial Security)

- Intrusion Prevention/Detection System
- Data Leak Prevention
- Anti-Spam
- Web Application Firewall
- Zero-Day/ATP Integration con tecnologia Fortinet Sandbox esterna
- Application Control
- VPN IPSec con strong encryption (AES256 SHA256 o superiori)
- SSL VPN

La decrittografia SSL con accelerazione hardware consente un'ispezione approfondita di SSL con un degrado minimo.

FortiGate implementa la funzionalità Virtual Domains (VDOM) in modo nativo; I VDOM possono essere utilizzati per dividere FortiGate in più dispositivi virtuali che funzionano in modo indipendente. In ogni VDOM si possono creare diverse configurazioni (incluse politiche SD-WAN, link, VPN…). Poiché ogni VDOM è un dominio di routing indipendente, è possibile utilizzare reti sovrapposte sullo stesso dispositivo. Non è necessaria alcuna licenza aggiuntiva per abilitare la funzione VDOM.

Il numero di VDOM disponibili è di 10 anche sui FortiGate entry level; sui fortigate di fascia più alta è possibile aumentare la disponibilità di VDOM con opportune licenze.

All'interno di ciascun VDOM è possibile configurare anche le vrf (fino ad un massimo di 32) per separare logicamente le diverse tabelle di routing. Ogni interfaccia fisico/logica può essere associata ad una vrf all'interno della quale poi verranno configurati i relativi protocolli di routing statico / dinamico per la corretta propagazione delle network.

Tutte le configurazioni possono essere gestite centralmente sul FortiManager e monitorate sul FortiAnalyzer (per approfondimenti si rimanda al paragrafo 5.3 Strumenti SW).

3.5. Architettura tecnologica

La tecnologia Secure SD-WAN scelta consente di utilizzare uno stack di routing completo che supporta i protocolli di routing unicast dinamico più comunemente utilizzati (BGP, OSPF, RIP, IS-IS) e multicast (PIM-SM o PIM-DM) utilizzabili sia in ambito WAN (Overlay o Underlay) che in ambito LAN per interfacciarsi al meglio con apparati esistent. Fortinet Secure SD-WAN supporta completamente anche IPv6 per quanto riguarda il

networking, le policy di sicurezza e le policy SD-WAN. È possibile configurare gli indirizzi delle varie interfacce sia in modo statico che dinamico mediante DHCP. Non ci sono limitazioni in termini di architetture possibili considerando link di connettività underlay e overlay, la soluzione FortiGate Secure SD-WAN è costituita da interfacce underlay e overlay autonome aggregate in un singolo collegamento WAN virtuale con tutte le funzionalità supportate indipendentemente su quale link viene instradato il traffico.

Presso ogni stazione è possibile prevedere molteplici tipologie di connettività privata o pubblica sulle quali sono instaurate delle connessioni Overlay IPSec tra i FortiGate delle differenti sedi. Il FortiGate controlla lo stato di ciascuna interfaccia membro SD-WAN incluso in uno Performance SLA, inviando health-check a un server target attraverso ciascun collegamento membro e misurando la qualità del collegamento in base a latenza, jitter e perdita di pacchetti. È possibile configurare fino a due server per testare l'integrità dei percorsi attraverso i vari membri SD-WAN. Ciò aiuta a garantire che se i controlli di integrità identificano problemi di connettività, l'errore è dell'interfaccia e non del server. Se uno dei server soddisfa i criteri di stato del collegamento (SLA), il collegamento è buono. Il FortiGate rimuove un'interfaccia del collegamento SD-WAN se la sua connettività è inattiva o fuori SLA. È possibile configurare i seguenti protocolli per i controlli di stato: Ping, HTTP, TCP-Echo, UDP-Echo e Two-Way Active Measurement Protocol (TWAMP), dns, tcp connect, ftp.

L'instradamento del traffico sul percorso migliore viene fatto con delle SD-WAN Rule che identificano uno specifico traffico secondo parametri L2-L7 (e/o su base utente) e in caso di percorsi multipli lo instradano seguendo una delle seguenti logiche:

- Manual: il traffico viene instradato sempre attraveso una stessa interfaccia fin tanto che resta attiva;
- Best Quality: instrado il traffico sul percordo migliore in termini di packet loss o di jitter o di Round trip delay;
- Lowest Cost SLA: definisco uno SLA in termini di jitter, packet loss e round trip delay ed instrado il percorso solo sui link che rispettano lo SLA; in caso di più link che rispettano lo SLA viene scelto un solo percorso su base priorità;

Maximize Bandwitdh (SLA): in caso di più percorsi in SLA posso decidere di instradare il traffico su più percorsi multipli in contemporanea sfruttando meccanimi su base occupazione di banda Inbound, Outbound, source-ip, source-dest-ip, round robin

Dopo aver discusso la soluzione tecnologica nei paragrafi precedenti, l'obiettivo del seguente paragrafo è contestualizzare l'architettura SD-WAN Fortinet nel contesto del cliente. Sono dunque riportati:

- Il disegno architetturale di alto livello proposto e i modelli di Fortigate ipotizzati
- Le informazioni dettagliate inerenti i modelli di Fortigate proposti per tutte le tipologie di sedi.

I sistemi FortiGate costituiscono il tassello di base per il deployment di una "Security Fabric", cioè un insieme di apparati in grado di dialogare e correlare gli eventi per una maggiore efficacia nella protezione e mitigazione degli emergenti attacchi di natura avanzata.

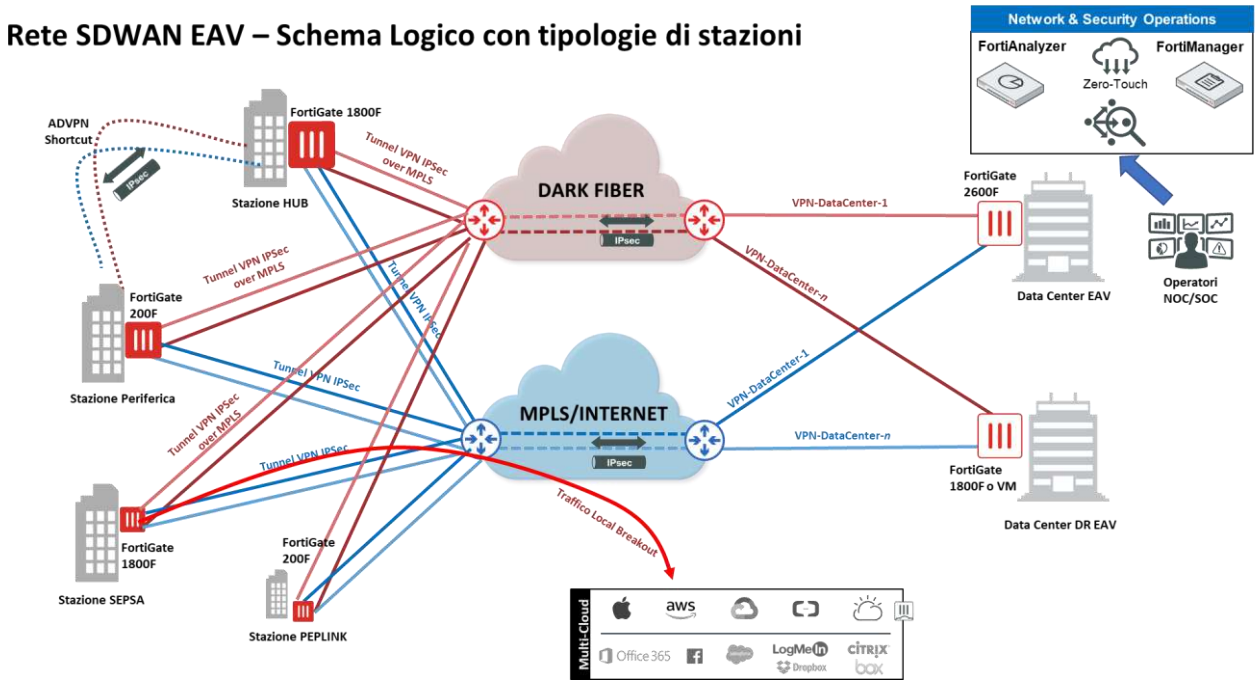
Il valore aggiunto della proposta tecnologica Fortinet è basato su molteplici fattori, il principale dei quali è una semplificazione e consolidamento tecnologico dell'infrastruttura di sicurezza cliente, laddove essa sia composta da molteplici tecnologie e componenti disgiunte, con sistemi di gestione separati e nessuna condivisione delle informazioni sulle minacce presenti sulla rete o una limitata e marginale disponibilità e usabilità delle stesse. La risposta all'eterogeneità, complessità di rete e difficoltà di gestione è un sistema coordinato di sicurezza che risponda a tre principali requisiti:

- **Segmentazione** – le reti necessitano di essere separate intelligentemente in zone funzionali di sicurezza. La segmentazione end-to-end, dall'IoT al cloud, ed attraverso ambienti eterogenei sia fisici che virtuali, fornisce visibilità piena del traffico che attraversa reti distribuite, limitando la diffusione di malware e permettendo l'identificazione e la quarantena dei dispositivi infetti.
- **Intelligenza Collaborativa** – l'intelligenza locale e globale deve essere condivisa tra i diversi dispositivi di sicurezza ed avvalorata da una orchestrazione centralizzata che permetta una risposta coordinata tra i sistemi.
- **Universal policy** – la determinazione dei livelli di trust tra i vari segmenti di rete, la collezione delle informazioni derivanti dalla convidisione e collaborazione tra le entità

sono mantenuti da una policy engine centralizzata che stabilisce in maniera unificata e coerente la security policy e ne orchestra la distribuzione sui punti di enforcement della rete.

3.6. Architettura di rete proposta

Dalle prime analisi effettuate ricostruendo l'architettura di rete esistente, viene proposto un primo modello logico sintetizzato nel seguente schema per l'infrastruttura SD-WAN nelle sedi coinvolte.

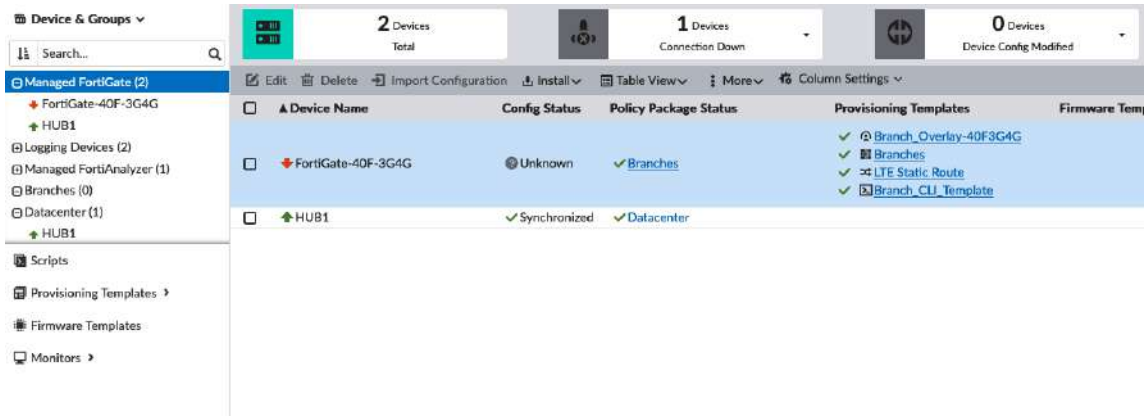


3.7. Deployment della soluzione

Il deployment della soluzione avverrà secondo i seguenti passi e configurazioni:

- Progettazione di High Level Design
- Progettazione di Low Level Design, definizione della strategia di migrazione, procedure di rollback e schemi di collaudo

- Migrazione legacy del FortiGate attualmente in produzione (FortiGate 1800 Perimetrali) su nuovo cluster FortiGate 2600F. Tale cluster avrà il ruolo di hub nella configurazione hub-spoke
- Definizione delle zone sdwan e delle strategie di steering del traffico sull'HUB (application, business critical, ottimizzazione delle connettività disponibili).
- Definizione dell'AS BGP per lo steering dinamico del traffico HUB-SPOKE
- Installazione, configurazione e tuning del FortiManager, soluzione di management centralizzata. Saranno definiti gli oggetti e le relative normalizzazioni, template di Provisioning e Policy Package per la configurazione automatizzata delle sedi remote (spoke). La figura seguente riporta uno screen esemplificativo della soluzione.



- Installazione, configurazione e tuning del FortiAnalyzer includendo customizzazione, Reportistica e policy di Incident Handling. Il FortiAnalyzer sarà aggunto come managed device al FortiManager per una gestione e consultazione del real time analytics da un'unica console.
- Setup degli overlay ridondati sui vari branch (o spoke, sedi remote) per la connessione datacenter (HUB) e le connettività internet sia attraverso l'hub e attraverso le connessioni di backup delle singole sedi. Saranno quindi configurati i tunnel IPSEC e il routing dinamico sull'AS BGP e le policy che consentiranno le interconnessioni intra-sede/internet richieste dall'IT di EAV.

fonte: http://burc.regione.campania.it

- In estensione e on top a quanto previsto dal progetto, il FortiGate 2600F è l'apparato che consente di introdurre DataCenter segmentation. Nelle fasi fin qui descritte il 2600F ha il ruolo di SDWAN HUB e di gestire la protezione del network public edge; trasportando il ruolo di L3 Gateway dagli switch interni alla rete sul FortiGate e ottimizzando la gestione attraverso VDOM (con il vantaggio del Virtual Clustering) sarà possibile applicare alle direttrici di traffico policy di Intrusion Prevention, garantendo che eventuali malware o movimenti di attacco non possano diffondersi sull'intera rete.

3.8. Architettura segmenti di rete EAV

Il principio guida nel disegno architetturale è il seguente: rendere il servizio di rete proprietario resiliente alla guastabilità ed alla poca flessibilità nella gestione degli elementi di prioritizzazione e differenziazione del traffico di rete. Per raggiungere tale obiettivo si è in primis pensato di dotare i nodi attualmente raggiunti da collegamenti L2 o L3 più importanti di una coppia di firewall fortigate (dimensionati adeguatamente a seconda della dimensione dei nodi) che utilizzerà l'attuale infrastruttura di rete proprietaria, implementata su circuiti in fibra stesi lungo il percorso ferroviario, come uno link di underlay su cui verrà costruito il circuito logico di overlay di connessione IPSEC. Come elemento di ridondanza dell'attuale underlay sarà utilizzato il collegamento su rete mobile messa a disposizione del fortiextender che utilizzerà SIM di operatore pubblico a seconda della copertura su ogni stazione. Il tipo di collegamento previsto per le postazioni 4G sarà di tipo internet; questo scelta non preclude la possibilità di utilizzare eventuali APN esistenti. I generale per ogni punto può essere previsto in futuro anche uno o più link aggiuntivi per incrementare ulteriormente la resilienza della stazione locale.

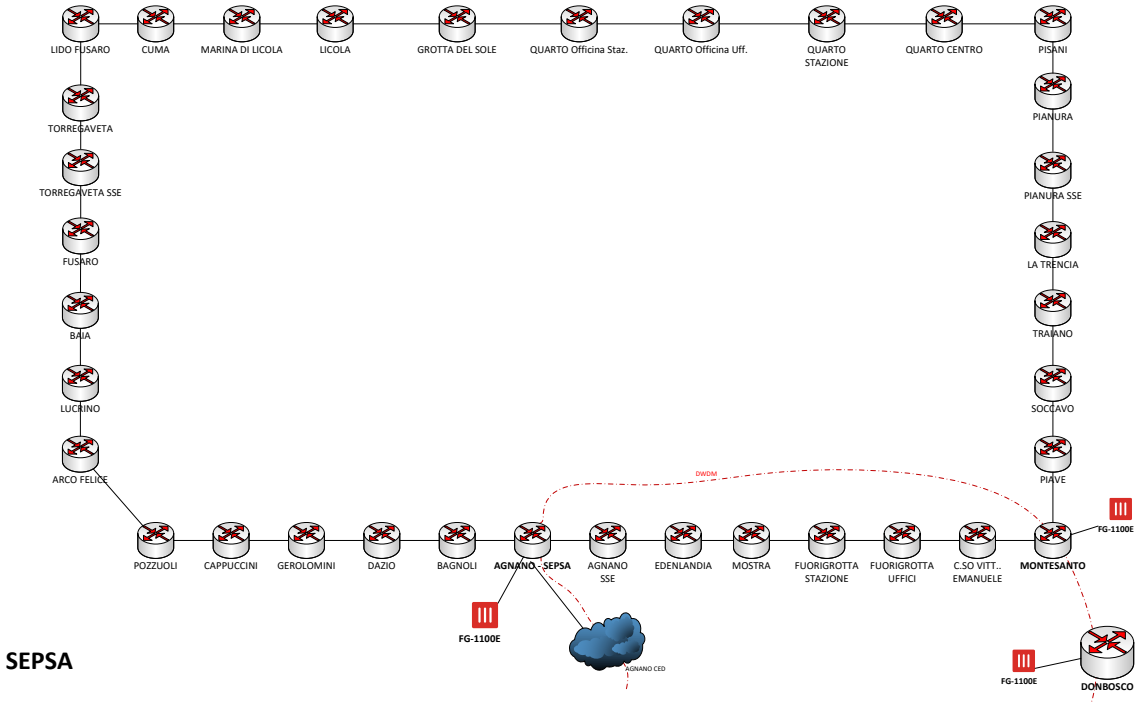
La realizzazione di un unico ulteriore processo di routing BGP e OSPF sui link di overlay, implementando le policy dinamiche dell'sdwan, garantirà la ridondanza e la gestione della rete secondo logiche di alta disponibilità.

Principio generale adottato per ogni punto è quello di installare sempre i Fortigate in coppia ed in cluster e dotare ogni punto del SD-WAN di un FEX che ridondi l'attuale accesso alla rete proprietaria con una connessione su media diverso (in questo caso 4G).

Più in dettaglio possiamo descrivere gli interventi puntuali nei vari sotto segmenti della rete EAV in questo modo.

3.9. Rete SEPSA

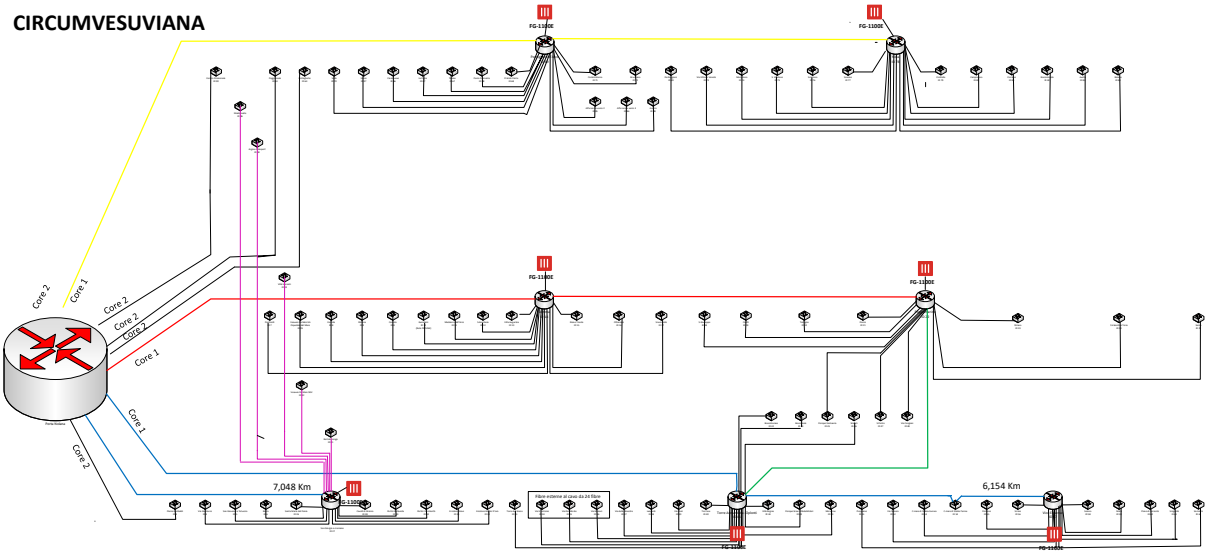
I tre nodi che saranno dotati di Fortigate in ridondanza saranno: Montestanto, Agnano, Don Bosco cioè quelli attualmente partecipanti all'anello in fibra proprietaria implementato tramite DWDM.



3.10. Sedi Hub Circumvesuviana

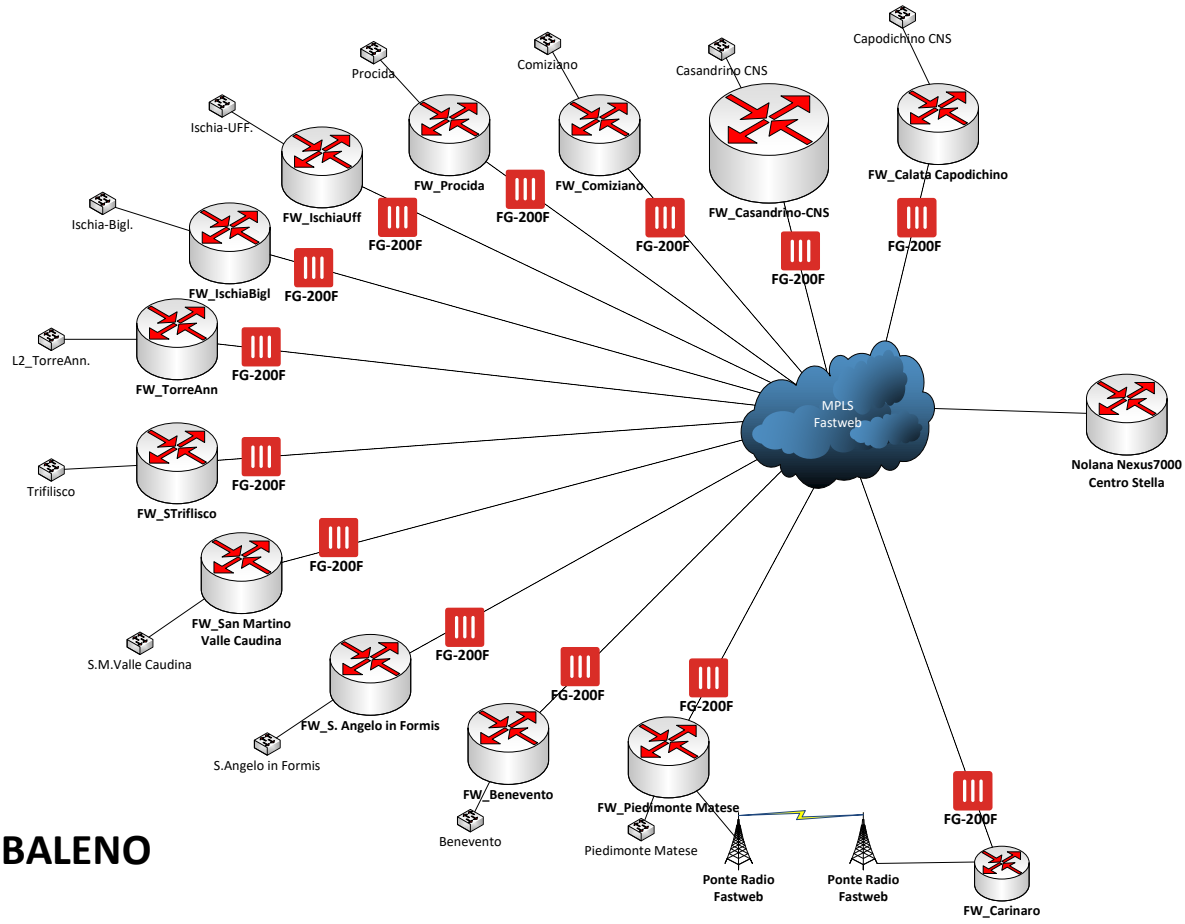
I nodi partecipanti all'SD-WAN saranno Pomigliano, Nola, San Giorgio, Torre Annunziata, Vico Equense, Poggiomarino. Su queste sedi sarà prevista l'installazione di Fortigate 1100E in alta affidabilità

fonte: http://burc.regione.campania.it



3.11. Rete Arcobaleno e Peplink

I nodi previsti con servizio SD-WAN saranno coperti mediante Fortigate 200F



ARCOBALENO

fonte: http://burc.regione.campania.it

Stessa macchina è stata individuata per le sedi etichettate come “peplink”.

3.12. Centrostella

L'hub del SD-WAN sarà dislocato al centro stella ed implementato su Fortigate 2600F che sostituiranno gli attuali 1800F di frontiera. Il primo collegamento gestito sarà quello della rete proprietaria L2/L3 di EAV e il secondo sarà gestito tramite internet e connessione nelle rispettive stazioni via FEX con sim 4G.

Inoltre l’infrastruttura SDWAN consentirà il collegamento di eventuali sedi in cloud come nodi HUB, cioè ospitanti servizi della rete EAV, sia sedi sul territorio non raggiunte dalle infrastrutture di rete proprietarie come sedi SPOKE.

L’attuale alta affidabilità gestita su due sedi fisiche del DataCenter (Porta Nolana ed Agnano) sarà comunque rispettata installando i fortigate 2600F uno per DataCenter e realizzando un cluster geografico.

4. Gantt

ID	Cap. Prog	Descrizione	M0	M1	M2	M3	M4	M5
Evoluzione Digitalizzazione Settore ITS Regione Campania								
1		Decreto di Concessione / stipula convenzione con Regione Campania						
	1	**Attivare nuove funzionalità all'interno dell'ITS**						
2		Affidamenti in Convenzione/Accordo Quadro Consip						
3		Inizio Lavori						
4		Realizzazione intervento						
5		Collaudo e saldo Finale						
	2	**Aumentare la sicurezza nelle stazioni e sulle linee di trasporto**						
2		Affidamenti in Convenzione/Accordo Quadro Consip						
3		Inizio Lavori						
4		Realizzazione intervento						
5		Collaudo e saldo Finale						
	3	**Aumentare la resilienza dei servizi offerti e dell'infrastruttura IT.**						
2		Affidamenti in Convenzione/Accordo Quadro Consip						
3		Inizio Lavori						
4		Realizzazione intervento						
5		Collaudo e saldo Finale						

fonte: http://burc.regione.campania.it

5. Piano finanziario

Descrizione		*Budget*
1. Attivare nuove funzionalità all'interno dell'ITS		**11.200.000,00 €**
2. Aumentare la sicurezza nelle stazioni e sulle linee di trasporto		**7.500.000,00 €**
2.1.	Sistema TETRA	3.000.000,00 €
2.2.	Sistema di supervisione e analisi territoriali su strutture critiche	2.100.000,00 €
2.3.	Rete di apparati mobili multifunzione	2.400.000,00 €
3. Aumentare la resilienza dei servizi offerti e dell'infrastruttura IT		**11.300.000,00 €**
3.1.	Il cloud dei servizi IT	7.200.000,00 €
3.2.	Infrastruttura di rete sicura e resiliente	4.100.000,00 €
	Totale	**30.000.000,00 €**

Voce di Costo	*Budget*
a) Personale adibito ad attività di Consulenza specialistica, tutoraggio, ecc.;	
a1. personale dipendente;	350.000,00 €
i) Impianti ed attrezzature produttive e/o tecnologiche;	29.240.000,00 €
l) Spese per la preparazione e la gestione dell'operazione;	300.000,00 €
m) IVA, oneri ed altre imposte e tasse (CONSIP);	10.000,00 €
n) Imprevisti (per gli interventi materiali);	100.000,00 €
Totale Investimento netto	**30.000.000,00 €**