AGENZIA DELLE DOGANE E DEI MONOPOLI E DEI MONOPOLI
IN PARTENARIATO CON
UIRNET

PROCEDURA APERTA PER L'APPALTO "INTEGRAZIONE DEI SISTEMI INFRASTRUTTURALI DI SECURITY DELL'AREA AMPIA DI GIOIA TAURO CON I SISTEMI DI ANALISI DI RISCHIO DOGANALI NELL'AMBITO DEL PROGETTO SPORTELLO UNICO"

CIG 5312473766 CUP G59E12000420006

PROGETTO CO-FINANZIATO CON FONDI FESR DAL PROGRAMMA OPERATIVO NAZIONALE SICUREZZA PER LO SVILUPPO;
OBIETTIVO CONVERGENZA 2007 – 2013;
OBIETTIVO OPERATIVO 1.2

Procedura aperta: art. 3, comma 37 e art. 55, comma 5, Decreto Legislativo n. 163/2006 e Parte IV del D.P.R. n. 207/2010; criterio di aggiudicazione: offerta economicamente più vantaggiosa, ai sensi dell'art. 83 del Decreto Legislativo n. 163/2006

CAPITOLATO TECNICO

SOMMARIO

INDICE DELLE FIGURE

Nota

Nel presente documento, sono sempre usate le diciture “Committente” che indica l’Agenzia delle Dogane e dei Monopoli e dei Monopoli in partenariato con UIRNet e “Fornitore” che si riferisce all’impresa ovvero al Raggruppamento Temporaneo di Impresa che elaborerà l’offerta per la gara.

1. PREMESSA - SCENARIO

Il presente documento identifica l'oggetto della prestazione dei servizi e delle forniture necessarie a conseguire gli obiettivi sottesi alla gara d'appalto in argomento.

Esso costituisce, quindi, il capitolato speciale descrittivo e prestazionale minimo con riguardo alle caratteristiche e alle specifiche tecniche funzionali delle apparecchiature che compongono l'integrazione dei sistemi infrastrutturali di security dell'Area Ampia di Gioia Tauro con i sistemi di analisi di rischio doganali nell'ambito del progetto "Sportello Unico".

Altri elementi prescrittivi previsti dall'art. 279 del D.P.R. 207/2010 come necessari alla progettazione di servizi e forniture nell'ambito dei contratti pubblici sono contenuti nel documento "Disciplinare di Gara" consegnato contestualmente.

Il sistema in argomento è diretto all'integrazione e completamento degli strumenti in dotazione agli Enti che intervengono nei processi di sicurezza e doganali nell'ambito dell'area portuale di Gioia Tauro.

Le caratteristiche e le specifiche tecniche e funzionali descritte nel prosieguo del documento devono intendersi quali specifiche e requisiti minimi, che il concorrente potrà integrare, migliorare ed ottimizzare nell'offerta tecnica ammessa alla procedura aperta di appalto.

Il concorrente dovrà fornire per la completezza dell'offerta tecnica e per consentire la valutazione, i dettagli tecnici del dimensionamento proposto e dei razionali tecnici funzionali ed operativi che giustifichino le scelte effettuate, indicando ed evidenziando gli elementi ed i parametri migliorativi rispetto ai minimi indicati nel presente documento.

Tale progetto è stato ammesso a finanziamento da parte del PON "Sicurezza per lo Sviluppo - Obiettivo Convergenza 2007-2013".

La sicurezza portuale è una delle priorità del PON "Sicurezza per lo Sviluppo" Obiettivo Convergenza 2007-2013, poiché i grandi porti sono obiettivi sensibili potenzialmente soggetti a minacce dirette ed indirette dalle quali possono derivare danni ingenti all'economia ed alla vita associata nonché alla regolare operatività dell'infrastruttura.

Il porto di Gioia Tauro è il più grande terminal italiano per il transhipment del Mar Mediterraneo ed è il principale scalo commerciale marittimo situato nei pressi dell'area metropolitana di Reggio Calabria.

Inoltre il porto di Gioia Tauro è al terzo posto in Europa nella classifica dei porti che si occupano del transhipment dei Container (dopo Rotterdam ed Amburgo); è il primo nel Mediterraneo ed ha sostituito Malta come nodo di distribuzione dei traffici in partenza dal Nord America e dall'Estremo Oriente verso il Mediterraneo centrale ed orientale ed è in grado di svolgere un ruolo di rilancio dell'economia meridionale.

Gioia Tauro, inoltre, si inserisce in un contesto caratterizzato da indicatori socio-economici al di sotto delle media nazionale e del Sud-Italia in particolare.

Come documentato nella relazione annuale della "Commissione Parlamentare di inchiesta sul fenomeno della criminalità mafiosa o similare" del febbraio 2008, l'area allargata del porto rappresenta la principale attività economica strutturata dell'area calabrese e costituisce una ghiotta opportunità di finanziamento illecito per le attività condotte dalle numerose organizzazioni criminali ivi presenti.

Sin dalla sua realizzazione, l'area portuale ha rappresentato un'opportunità di sviluppo degli affari illeciti per imprese collegate alla criminalità organizzata, nonché una via di accesso privilegiata per beni di natura e/o provenienza illecita.

Droga, armi, rifiuti tossici e/o pericolosi beni contraffatti ed altro, sembrano aver trovato nell'area del porto di Gioia Tauro un canale privilegiato di accesso nei gangli vitali e sani del nostro sistema economico.

Per tali motivi l'Area Ampia del porto di Gioia Tauro è stata indicata come struttura di rilevanza strategica nazionale dall'omonimo programma edito dal Governo con delibera del 21 dicembre 2001.

Estesa su mq. 7.000.0000, e capace di movimentare oltre tre milioni di TEU ogni anno (con una stima di potenziale raddoppio in tre anni), l'Area Ampia del porto di Gioia Tauro costituisce un importante snodo nella filiera logistica nazionale ed internazionale.

L'Area Ampia può utilmente essere suddivisa in due sotto aree: il porto propriamente inteso e la cosiddetta area retro portuale.

L'Area Ampia ha avuto un finanziamento dal PON "Sicurezza" 2007 – 2013 per il progetto e la realizzazione di un Sistema Integrato di Sicurezza.

Queste ed altre iniziative di sicurezza nascono, oltre che per mitigare al massimo i rischi di sicurezza sulle vie di comunicazione, anche per rispondere alle normative in materia di sicurezza dei porti sempre più stringenti (ISPS Code; Container Security Initiative, Direttiva EU 2005/65/CE, ecc.).

Al momento di indire la procedura di gara per l'individuazione del fornitore del sistema di sicurezza realizzato dal 2010, il Ministero dell'Interno aveva già individuato, quale naturale proseguimento ed evoluzione del Sistema Integrato di Sicurezza in argomento un "Security & Alert Management" che avrebbe dovuto permettere l'integrazione di diversi sistemi esistenti ed, allora, in progetto, e la correlazione delle informazioni prodotte e rese disponibili da tali sistemi.

Oggi, grazie all'ammissione a finanziamento da parte del PON "Sicurezza per lo Sviluppo" Obiettivo Convergenza 2007-2013 del progetto "Integrazione dei sistemi infrastrutturali di security nell'Area Ampia di Gioia Tauro con i sistemi di analisi di rischio doganali nell'ambito del progetto Sportello Unico" avvenuto in data 8 ottobre 2012 a favore del Beneficiario Agenzia delle Dogane e dei Monopoli che opererà in partenariato con UIRNet, è possibile dare corso alla realizzazione del previsto percorso evolutivo del sistema integrato di security.

Il nuovo sistema dovrà configurarsi come un naturale completamento del Sistema Integrato di sicurezza dell'Area Ampia di Gioia Tauro, in grado di:

- analizzare eventi e correlare segnali provenienti dai diversi sistemi installati;
- analizzare i profili di minaccia e individuare i pattern ricorrenti e significativi;
- guidare gli operatori nelle attività di analisi dello scenario e nei processi e procedure di risposta;
- consentire una adeguata ed efficiente comunicazione tra gli Enti coinvolti nelle attività di controllo e di prevenzione

Il nuovo sistema, inoltre, dovrà mettere in relazione i dati così estratti ed analizzati, relativi ad eventi e residenti nei propri database, con i segnali provenienti dai sistemi di analisi del rischio doganali e dalla Piattaforma Nazionale Logistica UIRNet, nonché con i "segnali deboli" provenienti dal mondo esterno, con particolare riguardo all'attività di analisi comunemente denominata "OSINT", che permetta al Sistema integrato di gestione della sicurezza di godere di funzionalità avanzate di "situational awareness" e di "early warning" rispetto a minacce latenti.

1.1 Contesto

Il porto è caratterizzato dalla presenza di vari sistemi tecnologici, organizzazioni e procedure di sicurezza che lo hanno portato a conseguire la certificazione di conformità al codice ISPS.

La seguente figura rappresenta una planimetria sommaria del porto di Gioia Tauro.

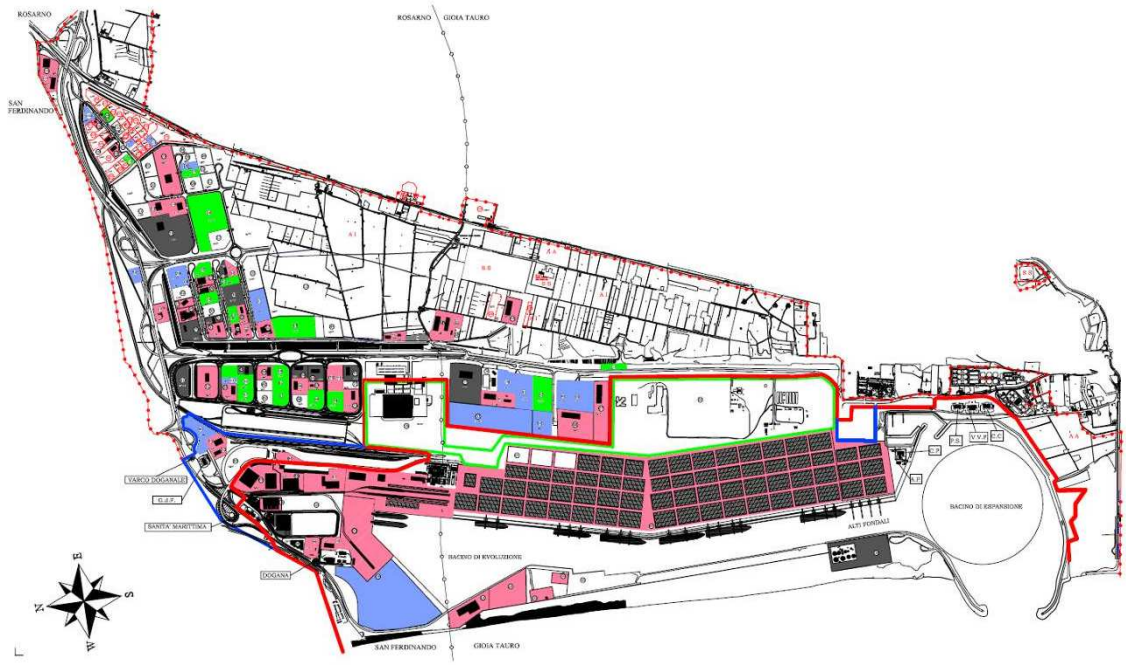

Figura 1 – Rappresentazione del porto di Gioia Tauro

Partendo dall'area più interna del porto e andando verso l'esterno e, quindi, verso l'area retro portuale sono state individuate le seguenti aree, ciascuna delimitata da barriere di diverso tipo e di competenza di uno o più attori tra quelli coinvolti nel processo di sicurezza del porto.

La prima è quella dei terminal MCT/BLG delimitata da rete di protezione con impianto di videosorveglianza perimetrale e protetta da un varco pedonale per i dipendenti ed un varco veicolare che regola gli accessi dei veicoli adibiti al trasporto e a tutti i veicoli più in generale.

L'area precedentemente descritta si trova all'interno dell'area portuale anche essa delimitata da reti di protezione e a cui si accede tramite il varco di S. Ferdinando dove operano sia la Guardia di Finanza sia l'Autorità Portuale (di seguito denominata anche come Port Security) per il controllo delle merci e degli accessi (rispettivamente) e da cui si accede alla prima zona industriale.

Appena fuori, è presente l'area doganale delimitata da una rete di protezione in cui si trova il terminal ferroviario.

All'esterno dell'area portuale si trovano infine la seconda e la terza zona industriale nella zona di Gioia Tauro e Rosarno accessibili tramite svincolo stradale; tali aree sono di competenza di ASIREG (Consorzio per lo Sviluppo Industriale della Provincia di Reggio Calabria) e sono interessate da un progetto di sicurezza che prevede la realizzazione di alcuni sistemi di videosorveglianza distribuiti sul territorio.

1.2 Enti e strutture operative coinvolti

I principali attori operanti all'interno della realtà portuale e retro-portuale di Gioia Tauro possono essere suddivisi nelle seguenti macro categorie:

1.2.1 Attori istituzionali

1.2.1.1 Autorità Portuale

L'Autorità Portuale ha il compito preminente di indirizzare, programmare, coordinare, promuovere, regolamentare e controllare le operazioni portuali e le attività commerciali e industriali esercitate nel porto. L'Autorità Portuale ha, inoltre, compiti relativi alla manutenzione ordinaria e straordinaria delle parti comuni in ambito portuale.

L'Autorità Portuale non ha quindi funzioni operative (che sono invece trasferite agli operatori privati) ma funzioni di pianificazione e coordinamento delle aree e dei servizi portuali.

1.2.1.2 Capitaneria di Porto

Le competenze della Capitaneria di Porto riguardano principalmente la sicurezza marittima e tutte le problematiche delle navi "lato mare" dalla gestione alla movimentazione/ormeggio delle navi. Il lavoro della Capitaneria di Porto si svolge in collaborazione con i Terminalisti.

1.2.1.3 Dogana

L'Agenzia delle Dogane e dei Monopoli può essere definita come l'organo principale deputato al controllo della sicurezza delle merci che entrano ed escono dal territorio Comunitario.

1.2.1.4 Chimico del porto

Le competenze del Chimico del porto si estendono su tutto il territorio del porto e riguardano il controllo e lo sbarco delle merci pericolose attraverso il sistema HacPack, più avanti descritto.

Il Chimico del porto è l'organo competente ad autorizzare/negare lo sbarco nel porto delle merci dichiarate come pericolose.

1.2.1.5 Polizia di Frontiera

Le competenze della Polizia di Frontiera attengono principalmente alla tutela della legalità circoscritta all'area portuale (furti, rapine, danneggiamenti, ecc.) con particolare riferimento al contrasto dell'immigrazione clandestina.

1.2.1.6 Guardia di Finanza

Le competenze della Guardia di Finanza nel porto sono legate al rispetto della legalità in ambito fiscale e tributario per quanto riguarda le merci in transito nel porto.

La Guardia di Finanza svolge la propria attività d'Istituto, relativa all'ispezione dei container, in collaborazione con l'Agenzia delle Dogane e dei Monopoli.

1.2.1.7 Commissariato di Pubblica Sicurezza di Gioia Tauro

Il commissariato ospita e gestisce i segnali del sistema di videosorveglianza denominato Piana Sicura e descritto nelle pagine che seguono.

1.2.1.8 Compagnia dei Carabinieri di Gioia Tauro

Le competenze della Compagnia dei Carabinieri di Gioia Tauro sono limitate alle tre aree industriali mentre l'area portuale non è di diretta competenza della Compagnia di Gioia Tauro.

1.2.2 Attori commerciali

1.2.2.1 Terminal MCT/BLG

Il terminal MCT/BLG esercita la sua attività sul piazzale che ha in concessione nell'area relativa alla banchina di levante.

Tale terminal svolge per il 99% attività di transhipment, per il restante 1% svolge attività di import/export (mediante trasporto sia su gomma che su rotaia).

1.2.2.2 ASIREG (Zone Industriali)

Esistono tre zone industriali: la prima all'interno del porto è raggiungibile attraverso lo svincolo di S. Ferdinando ed è di competenza dell'autorità' portuale; la seconda zona è accessibile tramite lo svincolo di Rosarno ed è fuori dall'area portuale alle spalle del porto stesso; mentre la terza sita nel comune di Rosarno è nuova, gli impianti di videosorveglianza sono in fase di allestimento ma non è ancora operativa a livello di presenza di industrie.

1.3 Panoramica dei sistemi e dei processi di sicurezza portuale

Nei paragrafi successivi sono descritti i principali processi in ambito di sicurezza portuale al momento esistenti ovvero in via di completamento nell'area portuale e retro portuale di Gioia Tauro.

Le componenti di sicurezza attualmente installate ed operanti sia nel porto che nella filiera logistica collegata, dovranno essere integrate in un sistema atto a fornire, in sede locale, tutte le informazioni necessarie alla prevenzione delle attività illegali.

Il tutto, grazie alle funzionalità dettagliate nel paragrafo dedicato all'idea progettuale, che prenderà le mosse dall'integrazione dei sottosistemi attualmente operanti e di seguito descritti.

1.3.1 Sistemi relativi all'Attività dell'Agenzia delle Dogane e

dei Monopoli

1.3.1.1 AIDA (Automazione Integrata Dogane Accise)

È il sistema informativo doganale, sviluppato in sintonia con le linee guida dell'Organizzazione Mondiale delle Dogane, con i piani informatici comunitari, con i piani nazionali di e-government e nel quadro delle innovazioni prescritte dal Codice dell'Amministrazione Digitale.

Il sistema opera in tempo reale su architettura web e dialoga per via telematica con gli operatori economici.

Il sistema esamina in tempo reale ogni dichiarazione doganale e, tramite una delle principali componenti del sistema afferenti la gestione della security (Circuito doganale di Controllo), effettua un'accurata analisi dei rischi, basata su elementi oggettivi (origine, provenienza, destinazione, confezionamento, qualità e valore delle merci) e soggettivi (soggetti della supply chain) desumibili dalla dichiarazione doganale e dalle dichiarazioni sommarie collegate (Manifesti di arrivo/partenza delle navi), associando tali informazioni ai profili di rischio catalogati a sistema e anch'essi modificabili in tempo reale.

In base al rischio rilevato le merci sono indirizzate a quattro crescenti livelli di controllo (automatizzato, documentale, scanner, ispezione fisica).

Il controllo scanner dei container è assistito da un sistema esperto di analisi delle immagini che agevola e velocizza l'intercettazione di difformità rispetto al dichiarato.

Basandosi sulla declinazione del paradigma single window - one stop shop è stato di recente reso operativo nell'ambito del progetto Sportello Unico doganale, un nuovo componente del sistema che consente, per ogni operazione doganale, di controllare l'avvenuto rilascio di documenti/certificazioni e l'avvenuta esecuzione di controlli demandati ad altri enti/amministrazioni (Ministero Salute, Ministero Interno, Ministero Sviluppo Economico, Ministero Politiche Agricole, ecc.).

Lo Sportello Unico doganale integra i processi di controllo in capo agli Enti coinvolti nello sdoganamento, secondo le regole ed i principi del Codice dell'amministrazione digitale (cooperazione applicativa/interoperabilità, unitarietà della Pubblica Amministrazione in rapporto agli utenti), a tutto beneficio dell'efficienza del processo di sdoganamento e dell'efficacia dei controlli.

Con il progetto CARGO è possibile sia anticipare il processo di sdoganamento prima dell'approdo in porto (pre-clearing), sia l'analisi dei rischi sulle merci sbarcate/imbarcate attraverso l'esame dei Manifesti Merci in Arrivo e in Partenza inviati per via telematica.

L'entrata in vigore dell'Emendamento Sicurezza (cfr. Reg. (CE) 648/2005 e Reg. (CE) 1875/2006) ha consentito di automatizzare il processo di controllo assicurando una maggiore efficienza del monitoraggio del flusso delle merci in entrata/uscita nei porti.

1.3.1.2 Sportello Unico doganale

La scelta del porto/aeroporto presso il quale compiere le attività di imbarco/sbarco, oltre che da valutazioni logistiche, è fortemente influenzata da tempi e costi di sbarco e di introduzione nel mercato.

Costi e tempi sono il risultato dell'interazione di tutti gli attori coinvolti a vario titolo nelle operazioni di sdoganamento, ovvero l'insieme dei processi di pertinenza doganale e di altri soggetti (Autorità Portuale, terminalisti, Guardia di Finanza, Capitaneria di Porto, Servizio di Sanità Marittima, Servizio Veterinario, Servizio Fitopatologico, Corpo Forestale, Agenzie Marittime, Case di Spedizione, Spedizionieri Doganali, ecc.).

La frammentazione del processo di sdoganamento può comportare il controllo di fino a 70 documenti diversi (fatture, licenze per import ed export, autorizzazioni, certificati fitosanitari e veterinari, ecc.) e, in corrispondenza, l'attesa dell'esito dei controlli esercitati da circa 20 Enti e soggetti diversi.

In assenza di un efficace coordinamento tra gli Enti coinvolti, i costi della frammentazione ricadono sulle imprese.

Per queste ragioni, l'Agenzia delle Dogane e dei Monopoli ha proposto la norma istitutiva dello Sportello Unico, inserita nella Legge 4 dicembre 2003 n. 350, prima che, nell'ordinamento comunitario, con il Regolamento del Parlamento e del Consiglio 648/2005, venisse introdotto un principio analogo.

La finanziaria 2004 stabilisce quindi che l'amministrazione doganale funge da punto di coordinamento e di controllo del complesso delle informazioni e dei dati necessari allo sdoganamento e demanda al DPCM appena pubblicato di definire le disposizioni applicative.

Nella G.U. n. 10 del 14 gennaio 2011, è stato pubblicato il DPCM n. 242 del 4 novembre 2010 "Definizione dei termini di conclusione dei procedimenti amministrativi che concorrono all'assolvimento delle operazioni doganali di importazione ed esportazione".

In Italia, per importare/esportare gli operatori nazionali erano obbligati ad inviare fino a 68 istanze a 18 amministrazioni diverse, trasmettendo ad ognuna informazioni e dati spesso simili se non identici nella sostanza, per ottenere le autorizzazioni, i permessi, le licenze e i nulla osta necessari, nella stragrande maggioranza dei casi rilasciati su carta.

Lo Sportello Unico mette fine a tali incombenze amministrative in quanto il citato DPCM obbliga le 18 amministrazioni ad integrare i processi di competenza, di cui rimangono titolari, offrendo a cittadini ed imprese una "interfaccia" unitaria.

Partendo dai dati presenti nella dichiarazione doganale si effettua il controllo della documentazione a corredo della dichiarazione (certificati, nulla-osta) accedendo alle basi dati delle amministrazioni che li hanno emessi.

Effetti: "digitalizzazione" di numerosi documenti cartacei, drastica riduzione dei costi, drastica riduzione dei tempi per l'effettuazione dei controlli (container controllato una sola volta ed in tempi definiti), miglioramento della qualità e dell'efficacia dei controlli.

Lo sportello è già operativo dal 2008 con il MISE per il trattamento dei titoli AGRIM ed AGREX e dal 2011 con il MAE per il trattamento delle licenze per l'importazione/esportazione dei materiali di armamento.

E' in corso la sperimentazione con il Ministero della Salute, che tratterà circa l'80% dei certificati sanitari collegati alle dichiarazioni doganali.

1.3.1.3 Sistema Cargo

Il sistema "Cargo" mette a disposizione degli attori del ciclo portuale funzionalità telematiche per il controllo elettronico del flusso delle merci, attraverso:

- la presentazione telematica del Manifesto Merci in Arrivo e Partenza (MMA e MMP);
- le dichiarazioni sommarie di entrata/uscita;
- il dialogo telematico con i Terminal-Container per la verifica in tempo reale dei container introdotti/estratti in base alle operazioni doganali compiute.

La recente introduzione dei cosiddetti emendamenti sulla sicurezza al codice doganale (Reg. 648/2005 e 1875/2006), rafforzano il ruolo della Dogana che, oltre ad assicurare la fluidità dei traffici, deve essere garante della "safety & security" della merce che attraversa i confini della comunità europea.

Dal 01/01/2011, infatti, in virtù dell'entrata in vigore dell'emendamento sicurezza al Codice Doganale Comunitario, per la merce che deve essere introdotta nel territorio doganale della Comunità è richiesta la trasmissione telematica della Dichiarazione Sommaria di Entrata (ENS – Entry Summary Declaration), che contiene gli elementi necessari per effettuare l'analisi dei rischi sicurezza da eseguire in base a criteri comuni a tutti gli Stati Membri, e l'obbligo dell'invio di una notifica elettronica di arrivo del mezzo di trasporto.

Analoga procedura è adottata per le merci in uscita dal territorio comunitario con la trasmissione della Dichiarazione Sommaria di Uscita (EXS – Exit Summary Declaration)

1.3.1.3.1 Processo di entrata delle merci

In particolare il processo di entrata delle merci prevede che il soggetto obbligato (art. 36 ter, par. 3 e 4 del Reg. (CE) 648/2005: chi introduce le merci e/o chi assume la responsabilità del trasporto) presenti la Dichiarazione Sommaria di Entrata (ENS).

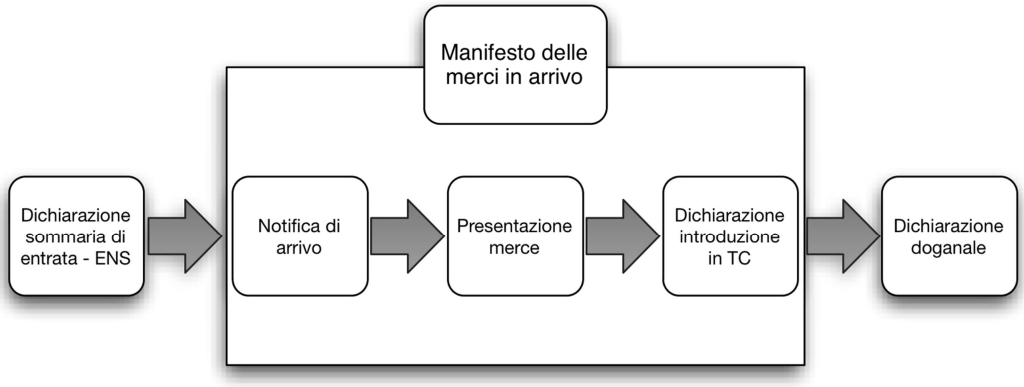

Figura 2 - Schema di processo di entrata delle merci

L'Operatore economico, identificato in modo univoco dal codice EORI (Economic Operator Registration and Identification), trasmette la ENS, in base alla tempistica prevista, prima del carico delle merci nel porto di partenza, e riceve da AIDA il relativo MRN – Movement Reference Number.

La dichiarazione deve contenere i dati identificativi del mezzo di trasporto (codice IMO o identificativo IATA).

La ENS può contenere fino a 999 articoli, ognuno dei quali è riferito ad una merce con elementi omogenei (origine, destinatario, ecc.).

Ogni singolo articolo può contenere, a sua volta, fino a 99 container ed ogni mezzo di trasporto può contenere diverse ENS.

Il servizio telematico doganale invia al dichiarante un messaggio di risposta con l'indicazione del MRN ed eventualmente, sulla base dell'analisi del rischio, il messaggio che la merce non può essere caricata (DO NOT LOAD).

Il messaggio, in ottica single-window, è reso disponibile anche al vettore.

Ai fini di una efficace analisi del rischio ai fini della Safety&Security, effettuata in base a medesimi profili per i 27 Stati Membri, è necessario, tra gli altri elementi, identificare le merci che, attualmente possono essere anche semplicemente descritte con un testo libero.

L'indicazione del codice merce a livello di Sistema Armonizzato (HS) è in fase di studio da parte dei servizi tecnici comunitari.

Al momento è possibile solo una raccomandazione per l'indicazione di un codice di almeno 4 cifre.

Un'altra semplificazione è stata introdotta per le tre fasi successive alla presentazione della ENS che sono state unificate in un unico momento utilizzando un documento doganale già adottato dagli operatori economici, il Manifesto delle Merci in Arrivo (MMA), completato con i riferimenti delle dichiarazioni Sommarie (MRN – Item Number) e l'indicazione della Entry Key (costituita da Tipologia del mezzo di trasporto, codice IMO o identificativo IATA e data dichiarata di arrivo al primo porto EU).

Tale documento, costituisce nello stesso tempo la Notifica di Arrivo, la presentazione delle Merci e la dichiarazione di introduzione in temporanea custodia, senza ulteriori adempimenti per gli operatori economici. Le informazioni sono rese disponibili a tutti gli attori del processo (responsabile MMA, vettore).

Da questo momento in poi, ogni singola merce iscritta a Manifesto, è identificata per le successive operazioni doganali dal codice di scheda partita (A3) di introduzione in Temporanea Custodia, la zona doganale del porto è vista come un magazzino virtuale, nel quale, le merci possono essere movimentate solo per le finalità consentite dallo stato della merce.

Così le merci, in un dato momento, potranno trovarsi in uno dei seguenti stati:

- svincolabile: la partita A3 è associata ad un item della ENS che non richiede il controllo sicurezza;
- in attesa di esito: nel caso in cui si sia in attesa del completamento dell'attività di valutazione del rischio;
- dichiarabile ma non svincolabile: la partita di merce è soggetta ad un controllo di sicurezza, ma è dichiarabile. Questo al fine di unificare i controlli della sicurezza ad eventuali controlli doganali;
- non dichiarabile: è il caso in cui la partita è soggetta ad un controllo sicurezza.

Le partite di A3 cambiano stato secondo il trattamento a cui sono sottoposte ed il responsabile del MMA può monitorare le variazioni di stato per procedere con le attività di propria competenza.

1.3.1.3.2 Processo di uscita delle merci

Analoga semplificazione è stata apportata al processo delle merci in partenza.

In questo caso il Manifesto delle Merci in Partenza – MMP, svolge anche le nuove funzioni richieste dal citato Emendamento Sicurezza.

Figura 3 - Schema di processo di uscita delle merci

Per l'uscita delle merci dal territorio doganale della Comunità è richiesta la comunicazione dei dati sicurezza (dati dell'allegato 30 bis del Reg.(CE) n.1875/2006 e 312/2009) da indicare nella Dichiarazione di esportazione.

Quando merci destinate ad uscire dal territorio doganale della Comunità non sono oggetto di una dichiarazione di esportazione deve essere presentata una EXS – Dichiarazione sommaria di uscita.

I vettori, siano esse compagnie di navigazione che vettori aerei, possono procedere al carico delle merci dopo l'autorizzazione della Dogana a che è tenuta a verificare che ogni spedizione sia corredata da MRN sicurezza (ovvero un MRN per ogni merce, collegato alla EXS di appartenenza, ovvero Dichiarazione di esportazione o ENS in caso di transhipment) e ad eseguire gli eventuali controlli presso l'ufficio di uscita.

Le specifiche comunitarie prevedono, infatti, che il vettore invii un messaggio elettronico all'ufficio di uscita per notificare l'arrivo della merce e renderla disponibile ad eventuali controlli di sicurezza.

Allo scopo di evitare duplicazione di adempimenti si è deciso di utilizzare il Manifesto delle Merci in Partenza in luogo del messaggio di notifica di arrivo presso l'ufficio di uscita delle merci dal territorio doganale comunitario.

A fronte dell'iscrizione delle partite di merce sul MMP la Dogana comunica diversi messaggi in risposta:

- il rilascio in sicurezza che equivale all'autorizzazione all'imbarco;
- in attesa di esito: attività di valutazione ancora in corso;
- da controllare: l'MRN è oggetto di controllo Safety&Security

Anche in questo caso, il responsabile del MMP può consultare l'aggiornamento degli esiti per verificare se la merce può essere imbarcata

Al fine di accelerare ulteriormente la semplificazione delle procedure nell'attività di sdoganamento e di decongestionare i porti storici italiani, sono stati avviati alcuni progetti sperimentali: Pre-Clearing e Trovatore.

1.3.1.3.3 Sistema di Pre-Clearing

Il Pre-Clearing è lo sdoganamento anticipato delle merci in arrivo nei porti e consente:

- immediato sbarco delle merci all'arrivo a banchina della nave
- sistemazione razionale delle stive a terra
- abbattimento del numero di spostamenti
- aumento dei tempi d'indagine preventiva per i servizi ispettivi
- anticipo dell'uscita della merce dal porto
- anticipo delle operazioni di imbarco

Il progetto di Pre-Clearing si pone l'obiettivo di semplificare ed ottimizzare le procedure doganali nei porti avvalendosi dei nuovi principi normativi adottati in materia, anche a livello comunitario [Reg. CE n. 312/2009 Reg. CE n. 450/2008 del 23 aprile 2008; Reg. CE n. 648/2005 del 13 aprile 2005; D.L. 14 marzo 2005 n. 35, convertito in Legge n. 80 del 14.05.2005].

Il processo di semplificazione si basa sulla creazione di un sistema unitario di comunicazione con collegamento e scambio di dati tra i soggetti interessati, pubblici e privati operanti presso l'infrastruttura portuale.

Il principio alla base di tale meccanismo è che attraverso il controllo integrato dei flussi delle merci si accresce l'efficienza dei controlli, si abbattono i tempi di effettuazione delle operazioni doganali e gli attori del ciclo portuale possono disporre delle informazioni di competenza in tempo reale.

Il MMA viene trasmesso dall'Operatore anticipatamente, in modalità telematica, almeno 24 ore prima dell'arrivo della nave.

Esso, corredato del codice identificativo del terminal di destinazione, o del codice magazzino virtuale "099" da utilizzare esclusivamente per lo sdoganamento in linea, costituisce richiesta di autorizzazione per le merci da sbarcare.

A seguito dell'avviso di arrivo della nave in rada da parte della Capitaneria di Porto, l'Operatore comunica il risultato dello sbarco.

Tale messaggio, inviato dal terminalista, sostituisce la comunicazione presentata su supporto cartaceo all'Ufficio doganale di competenza.

La Dogana si riserva la possibilità di chiedere, contestualmente alla presentazione del manifesto anticipato, anche la presentazione delle polizze di carico.

In base alla trasmissione telematica del MMA il sistema informatico genera le partite di A3.

Prima della convalida del flusso provvisorio da parte della Dogana l'Operatore può procedere alla rettifica dei dati iscritti a Manifesto.

Successivamente, l'Ufficio delle Dogane provvede alla convalida del MMA.

Eventuali rettifiche del manifesto dopo la sua convalida saranno consentite, ma dovranno essere autorizzate dal competente ufficio doganale secondo le modalità di rito.

A seguito della convalida del MMA, sussistendo le condizioni previste dall'art. 6, comma 2, del D.Lvo 374/90, gli operatori possono inviare telematicamente le dichiarazioni doganali delle merci.

All'atto della convalida delle dichiarazioni il sistema genera l'esito del controllo (CA, CD, CS o VM), il quale sarà immediatamente comunicato, via mail, al dichiarante delle merci.

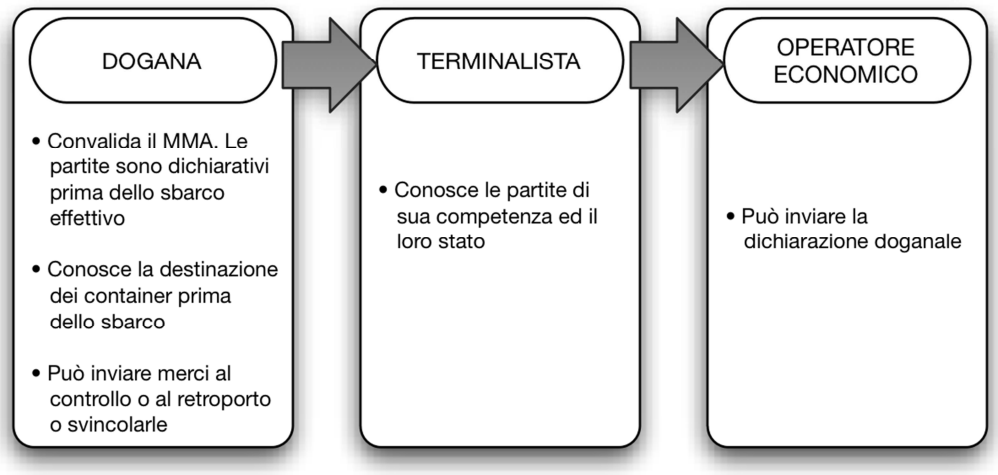

Figura 4 - Schema di processo di Pre-Clearing

Il gestore del terminal, attraverso l'interscambio delle informazioni con il sistema telematico doganale (procedura di colloquio con i terminalisti), conoscerà gli esiti delle dichiarazioni relative alle A3 di propria competenza.

In ciascuna dichiarazione doganale di esito, saranno riportati nella casella 40 gli estremi della relativa partita di A3 generata dal MMA.

In caso di interruzione del sistema informatico (doganale e/o dell'Operatore) si procede all'iscrizione delle partite di merci con l'analoga procedura prevista per la presentazione del MMA cartaceo.

L'Operatore trasmette i dati relativi alle provviste di bordo al sistema doganale, al più tardi al momento dell'arrivo della nave.

Per quanto riguarda infine gli adempimenti relativi allo sbarco, la Capitaneria di Porto ufficializza l'arrivo della nave porta-container, dandone immediata comunicazione, via mail, all'Ufficio delle Dogane e alla Guardia di Finanza

A seguito di tale adempimento, le merci esistenti a bordo si considerano arrivate negli spazi doganali.

Il visto sbarcare è effettuato dalla Guardia di Finanza al momento dello sbarco:

- per le merci esitate CA è previsto il rilascio immediato, fatti salvi tutti gli ulteriori adempimenti prescritti dalle altre Amministrazioni (Veterinario, Sanità marittima, Fitopatologo, CITES). Per le merci soggette al rilascio del N.O. sanitario, la bolletta doganale sarà trattenuta dal Capo Ufficio di Controllo fino alla presentazione del prescritto certificato;
- per le merci esitate CD, CS e VM è previsto il posizionamento in aree appositamente individuate dall'Autorità Portuale fino all'espletamento delle formalità doganali.

Nel caso in cui la merce non dovesse risultare idonea al controllo sanitario, il Responsabile dell'Ufficio è autorizzato a disporre l'annullamento della bolletta doganale adoperando tutte le cautele possibili affinché la merce abbia l'esito stabilito dall'Autorità sanitaria.

In ogni caso di annullamento della bolletta è sempre necessario procedere a visita fisica della merce. Il visto uscire dagli spazi doganali è effettuato dalla Guardia di Finanza.

Per le merci da introdurre nei magazzini/recinti di temporanea custodia, il gestore verifica le partite introdotte e comunica tempestivamente – entro due ore dall'introduzione in magazzino – all'Ufficio delle Dogane, ai fini delle dovute rettifiche, le eventuali incongruenze riscontrate.

Eventuali irregolarità o differenze riscontrate rispetto alle partite iscritte nel MMA convalidato, sono imputabili al vettore fino al momento della presa in carico da parte del gestore di magazzino/recinto di T.C. o della presentazione della dichiarazione di esito di cui sopra.

Per le partite non rispondenti ai dati del MMA, o non ricevute, il gestore del terminal è tenuto a darne tempestiva comunicazione – entro 2 ore – all'Ufficio delle Dogane, che provvederà alle rettifiche delle schede di A3.

Con l'invio all'Ufficio delle Dogane del messaggio di conferma di entrata delle partite di sua pertinenza, il gestore del terminal subentra nella responsabilità del vettore.

1.3.2 La Piattaforma Logistica Nazionale UIRNet

La PLN UIRNet è finanziata dal Ministero delle Infrastrutture Trasporti che ha delegato alla società UIRNet stessa (Società costituita tra gli Interporti Nazionali) la sua realizzazione e gestione.

E' il sistema di riferimento a livello nazionale per lo sviluppo di servizi di interesse sistemico a supporto della gestione dei processi logistici e del trasporto delle merci.

La PLN UIRNet, a regime, sarà il gestore centrale delle informazioni relative alla gestione e al monitoraggio del trasporto merci su strada, comprese quelle pericolose, e alla gestione delle informazioni relative al trasporto intermodale.

Il nuovo sistema, inoltre, dovrà mettere in relazione i dati così estratti ed analizzati, relativi ad eventi e residenti nei propri database, con "segnali deboli" provenienti dal mondo esterno, con particolare riguardo all'attività di analisi comunemente denominata "OSINT", che permetta al Sistema integrato di gestione della sicurezza di godere di funzionalità avanzate di "situational awareness" e di "early warning" rispetto a minacce latenti anche sul web.

1.3.3 Sistemi installati con il progetto Area Ampia di Gioia Tauro

1.3.3.1 Sistema di Videosorveglianza

Lo stesso è costituito, più in dettaglio, da:

1.3.3.1.1 Telecamere per videosorveglianza di contesto

Si tratta di 47 telecamere in grado di fornire immagini ad alta risoluzione di una determinata zona da tenere sotto controllo ed in grado di fornire allarmi in caso di rilevazione di movimento in aree (del fotogramma) non consentite o, ad esempio, rilevare del movimento in orari di chiusura.

1.3.3.1.2 Telecamere per videosorveglianza di osservazione

Si tratta di 36 telecamere in grado di fornire immagini di ampie aree del porto; hanno la possibilità di essere pilotate da un Operatore e di ruotare e zoomare su determinate aree; possono fornire allarmi in caso di rilevazione di movimento in aree (del fotogramma) non consentite o, ad esempio, rilevare del movimento in orari di chiusura oltre ad avere delle funzioni di ronda che permettono, ad esempio, di controllare un perimetro predeterminato e mandare un allarme in caso di rilevazione di movimento.

1.3.3.1.3 Telecamere long-range

Si tratta di cinque telecamere “speciali”, dotate di zoom e brandeggio (termiche e visibili), delle quali due con capacità di rilevamento antintrusione sino a 2 km di distanza utilizzate per proteggere il perimetro del porto dal lato mare, e tre con capacità di rilevamento antintrusione e funzione di videosorveglianza del perimetro interno che operano in asservimento automatico alla protezione antintrusione attiva (con agganciamento automatico della ripresa sulla zona in allarme).

1.3.3.1.4 Telecamere night & day

Si tratta di nove telecamere fisse per la copertura della visuale dell’area dello Scalo ferroviario.

1.3.3.1.5 Sistemi di videosorveglianza trasportabili e rimovibili

Si tratta di quattro telecamere che possono essere facilmente posizionate nei punti di interesse e poi rimosse secondo esigenza per la sorveglianza temporanea di aree di interesse (cantieri, stoccaggio di container, altro).

1.3.3.1.6 Sistemi di videosorveglianza veicolari

Si tratta di due telecamere da installare sulle autovetture in uso alla Polizia di Frontiera, in grado di registrare filmati video e contemporaneamente trasmetterli alla Sala Operativa.

1.3.3.2 Sistema Riconoscimento Targhe Container

Per il riconoscimento targhe veicoli e codici container viene utilizzato il sistema EASYgate.

Questo è costituito da software specifico e da un infrastruttura hardware installata presso i gate del varco di San Ferdinando.

Ogni gate è equipaggiato con una struttura metallica di sostegno per le telecamere e con i sensori di rilevamento della posizione del veicolo.

Un personal computer di elaborazione locale permette di acquisire le immagini e lo stato dei sensori.

Le immagini sono elaborate per estrarre la targa o i codici dei container.

Un server di concentrazione e supervisione può veicolare le informazioni verso altri sistemi.

1.3.3.3 Sistema Controllo Accesso Pedoni

Consente di autorizzare e monitorare il transito di personale autorizzato ai varchi previsti attraverso tornelli.

Il sistema utilizzato è Secure Perfect Ent della General Electric.

Questo gestisce l'accesso dei pedoni mediante lettori di badge e consente di effettuare le seguenti azioni:

- verifica della validità del badge;
- verifica dell'identità del possessore del badge;
- aggiornamento della base di dati di sistema;
- accesso o uscita, attivando remotamente il tornello relativo;
- segnalazione di eventuali anomalie ed attivazione di eventi da parte di altri sottosistemi;
- segnalazione di eventuali allarmi

1.3.3.4 Sistema Controllo Veicoli

Consente di autorizzare e monitorare il transito di veicoli che arrivano o escono dal porto.

Il software utilizzato è EASYgate che rileva, con le telecamere posizionate sul gate, le targhe di identificazione dei veicoli nella fase di ingresso o uscita.

Sulle sequenze video acquisite viene applicato un algoritmo di analisi video di tipo OCR (optical character recognition) per estrarre il numero di targa del veicolo.

EASYGate comunicherà l'informazione per verificare se la targa presente nel data base di sistema risulta autorizzata o meno.

In caso positivo viene permesso il transito in ingresso o in uscita aprendo la sbarra presso il gate.

1.3.3.5 Sistema Controllo Flusso Container

Consente di identificare i container in entrata ed uscita dai gate del porto.

Il software utilizzato è EASYGate; in particolare il modulo per la gestione dei container estrae dalle sequenze video acquisite dalle telecamere posizionate sul varco, i codici identificativi dei container.

Viene applicato un algoritmo di tipo OCR in grado di riconoscere i codici d'identificazione internazionali ISO 6346.

Se la sigla del container è presente nel data base di sistema viene concesso l'ingresso o l'uscita aprendo la sbarra presso il gate.

Il sistema non risulta essere attualmente attivo e funzionante sebbene previsto.

1.3.3.6 Sistema Acquisizione Segnali di Campo

Consiste in una piattaforma d'integrazione di tutti i segnali di campo e di tutti i sistemi TVCC (telecamere a lungo raggio ed NVR) installati.

Gli eventi acquisiti dai sottosistemi controllo targhe veicoli, controllo codici container, controllo accessi pedoni, telecamere termiche a lungo raggio, sonar, antintrusione perimetrale, potranno essere storicizzati.

Il sistema non risulta essere attualmente attivo e funzionante sebbene previsto.

1.3.3.7 Sistema Correlazione Eventi

Tale sistema è composto da due moduli distinti Facility Commander per la parte comando e controllo, e WEKA Explore per la parte di intelligence.

Facility commander mette a disposizione un'interfaccia web based per quanto riguarda la configurazione e correlazione degli eventi e un client java based per quanto riguarda sia il monitoraggio degli eventi che la visualizzazione delle telecamere.

Per quanto riguarda la parte Intelligence del sistema, essa consiste in un insieme di modelli di mining basati su tecniche di clusterizzazione e/o di classificazione, il cui tuning è effettuato con il framework opensource denominato Knowledge Explorer WEKA.

Tali modelli saranno in grado di suggerire anomalie e/o correlazioni fra eventi/allarmi che consentiranno all'Operatore di tarare in maniera adeguata la configurazione delle azioni da intraprendere a seguito di un certo insieme di eventi.

1.3.3.8 Sistema Supervisione Operatività

Il sistema software di supervisione delle attività costituisce un punto di accesso privilegiato che consente agli utenti autorizzati di avere una console integrata per le attività di monitoraggio, controllo operativo, analisi e supervisione in base alla tipologia ed alla profilazione dell'utente interessato.

1.3.3.9 Sistema di Sicurezza

Il sistema software di sicurezza sovrintende ai meccanismi con i quali è concesso l'uso delle funzioni del sistema complessivo, ai soli utenti autorizzati.

1.3.3.10 Sistema Comunicazione con altre Organizzazioni

E' un prodotto software che implementa le primitive di base per la cooperazione applicativa, corredato degli strumenti di amministrazione e monitoraggio delle attività.

1.3.3.11 Sistema Acquisizione Segnali di Campo

E' in via di sviluppo il sottosistema middleware d'integrazione SARA (Signal Acquisition and Reaction Automation) quale piattaforma d'integrazione di tutti i segnali di campo e di tutti i sistemi TVCC.

Gli eventi acquisiti dai sottosistemi controllo targhe veicoli, controllo codici container, controllo accessi pedoni, telecamere termiche a lungo raggio, sonar, antintrusione perimetrale, sono storicizzati nel data base integrato di sicurezza.

1.3.3.12 Sonar

Sistema sonar C-Tech installato presso l'imboccatura del porto per proteggere la struttura contro l'accesso non autorizzato di natanti di superficie o veicoli subacquei, inclusi eventuali sub, rivelandone la presenza ed inviando i relativi allarmi.

Il sonar è in grado di trasmettere:

- target id assegnato automaticamente ad ogni bersaglio rilevato per identificare la traccia.
- velocità
- profondità
- data, ora, minuti, secondi della rilevazione.

1.3.3.13 Sniffer

Si tratta di due rilevatori di tracce di esplosivi (ETDS-Explosive Trace Detection System), strumenti la cui funzionalità di base è quella di segnalare la presenza di particelle e vapori di esplosivo.

Caratteristiche essenziali per la portabilità sono le dimensioni ed il peso ridotto.

Il sistema non risulta essere attualmente attivo e funzionante ed è in via di realizzazione.

Gli eventi generati da tale sistema sono i seguenti:

- rilevazione movimento
- notifica registrazione contenuto multimediale
- ingresso veicolo
- uscita veicolo
- ingresso container
- uscita container
- ingresso persona
- uscita persona
- arrivo treno
- partenza treno
- malfunzionamento apparato

1.3.3.14 Sistema anti intrusione del porto

E' costituito da una rete Keller posta a protezione del perimetro del porto e fornisce protezione antintrusione attiva, tramite barriere a microonde o sensori sismici (in funzione della configurazione del terreno) posti sulla recinzione, a copertura dell'intero perimetro lato terra coincidente con la recinzione Keller.

Gli eventi generati da tale sistema sono i seguenti:

- rilevazione intrusione
- malfunzionamento apparato

1.3.3.15 Sistema comunitario di monitoraggio del traffico navale e d'informazione

Si tratta del cd. VTS, Vessel Traffic Service, e ha lo scopo di incrementare la sicurezza e l'efficienza del traffico marittimo e di favorire l'intervento delle autorità in caso di incidente o in presenza di situazioni potenzialmente pericolose in mare, comprese le operazioni di ricerca e soccorso, e di fornire un ausilio per migliorare la prevenzione e l'individuazione dell'inquinamento causato dalle navi.

Il VTS comprende tra l'altro i sottosistemi PMIS (Port Management Information Services) e MASM (Maritime Security Management) ed è in grado di erogare i seguenti servizi:

- informazioni;
- assistenza alla navigazione;
- organizzazione del traffico marittimo.

In particolare, il sistema VTS può fornire informazioni relative a:

- previsione di arrivo, avvicinamento/atterraggio, attracco e partenza del naviglio;
- tipologia del naviglio e carico trasportato;
- operatori portuali coinvolti;
- liste di imbarco e sbarco dei mezzi, merci e passeggeri;
- personale addetto di bordo;
- merci pericolose previste da scaricare, in transito e previste da imbarcare.

Il Sistema VTS è in fase di realizzazione/addestramento.

Gli eventi generati da tale sistema sono i seguenti:

- ingresso container
- uscita container
- ingresso nave
- uscita nave
- previsione arrivo nave
- prossimità nave
- malfunzionamento apparato

1.3.3.16 Sistema di controllo delle merci pericolose

Basato sul prodotto Hacpack (Hazardous Assessment Computer Package), questo sistema è strutturato attraverso differenti moduli, tutti interfacciati e comunicanti tra di loro, dedicati ai diversi soggetti interessati alle merci pericolose all'interno del porto.

- Hacpack Agenzie Marittime, utilizzato dai raccomandatari marittimi.
- Hacpack Terminals, utilizzato dagli operatori terminalistici.
- Hacpack Ais, sistema di rilevazione della posizione delle navi
- Hacpack Client, utilizzato dalle Autorità preposte alla sicurezza portuale.
- Hacpack DBMP, utilizzato dal chimico di porto per la valutazione del rischio
- Hacpack Multimodal, che aiuta i fornitori a compilare correttamente la Multimodal Dangerous Goods Form

Il raccomandatario marittimo, con il modulo Hacpack Agenzie Marittime, invia alle autorità preposte ed al Servizio Chimico di porto tutte le informazioni riguardanti il transito, lo sbarco e l'imbarco delle merci pericolose.

Il terminalista, tramite Hacpack Terminals, invia alle Autorità preposte ed al Servizio Chimico di porto, le informazioni relative alle merci pericolose stoccate nel proprio terminal.

A seguito delle informazioni ricevute, il servizio chimico di porto, utilizzando Hacpack DBMP (Data Base delle Merci Pericolose presenti in ambito portuale), elabora la valutazione del

rischio nave o del rischio terminal e rilascia alle autorità preposte un certificato con le adeguate prescrizioni di sicurezza.

Con il modulo Hacpack Client le autorità preposte alla sicurezza portuale (Autorità Marittima, Autorità Portuale, Vigili del Fuoco ecc.) hanno la possibilità di visualizzare la mappa del porto, le navi presenti agli accosti con a bordo merci pericolose, i dati nave e l'area di "danno" (calcolata con il Metodo Speditivo del Ministero degli Interni), la tipologia delle merci medesime, la loro classificazione secondo le normative internazionali, le Emergency Schedules di ogni merce, la valutazione del rischio nave espressa secondo gli indici F&EI, CEI e secondo il Metodo Speditivo e il certificato rilasciato dal servizio chimico di porto con le relative prescrizioni di sicurezza.

Il modulo Hacpack permette di aggiornare in tempo reale la situazione delle navi agli accosti. Nel complesso il software permette di far dialogare in tempo reale tutti i soggetti interessati alle merci pericolose, semplificando e velocizzando tutte le procedure relative alle autorizzazioni, allo scambio dei documenti, e alle verifiche.

Il sistema risulta attualmente in funzione.

1.3.3.17 Sistema per il controllo degli accessi veicolari e pedonali nell'area MCT/BLG

il sistema per il controllo degli accessi veicolari e pedonali nell'area terminal MCT/BLG è denominato STAC (System Terminal Control Access).

Tale sistema monitora l'accesso pedonale e veicolare sia dei dipendenti sia dei visitatori.

Attraverso l'utilizzo di un badge e di telecamere viene registrato l'ingresso/uscita al terminal.

All'interno di tale sistema sono inoltre presenti informazioni relative ai mezzi in entrata al porto (nome/Cognome driver, targa mezzo, codice container, documento di identità, numero di autorizzazione dell'Autorità Portuale, ecc).

Per quanto riguarda gli operatori presenti sulle navi sono previste delle procedure di Autorizzazione/Accompagnamento per accedere al terminal ed uscire dal porto.

All'interno del sistema STAC non è riportato lo specifico contenuto del container (tali informazioni sono di competenza della dogana).

Per la registrazione delle navi e dei relativi container in ingresso/uscita dal porto il sistema consente di definire delle finestre temporali durante l'anno che raccolgono informazioni sul carico e sulle navi.

Tali informazioni divengono sempre più dettagliate man mano che si avvicina il momento di arrivo al terminal. In questo modo è possibile gestire la schedulazione delle navi, l'allocazione dei container sul piazzale MCT/BLG anche in relazione al successivo imbarco su navi feeder (in modo tale da ridurre i costi di spostamento dei container).

Il sistema ottimizza l'allocazione dei container sulla base delle informazioni inserite a sistema (data di arrivo, data di partenza e tipologia di carico dichiarato).

1.3.3.18 Scanner

Gli scanner sono apparati utilizzati per il controllo a campione delle merci tramite scansione dei container ai raggi X.

Attualmente risultano attivi ed utilizzabili i due in uso alla Dogana: tali scanner sono collegati al sistema AIDA utilizzato dall'Agenzia delle Dogane e dei Monopoli.

I due in uso alla Guardia di Finanza non sono, invece, attualmente funzionanti.

Gli eventi generati da tale sistema sono i seguenti:

- risultato ispezione (manuale)

1.3.4 Sistemi installati con il progetto Piana Sicura

Piana Sicura è il sistema di videosorveglianza attualmente presente nell'Area Ampia di Gioia Tauro.

È dotato di 270 telecamere distribuite sul territorio nei comuni di Rosarno, San Ferdinando e Gioia Tauro, il sistema è attualmente funzionante.

Le immagini provenienti dalle telecamere di contesto, osservazione e LPR arrivano alla centrale operativa del Commissariato di Pubblica Sicurezza di Gioia Tauro ed alla Compagnia Carabinieri di Gioia Tauro.

2. FINALITA' DEL PROGETTO

Il nuovo sistema dovrà configurarsi come un naturale completamento ed ottimizzazione delle potenzialità operative dei sistemi presenti, in grado di:

- analizzare eventi e correlare segnali provenienti dai diversi sistemi installati;
- guidare gli operatori nelle attività di analisi dello scenario e nei processi e procedure di risposta;
- consentire una adeguata ed efficiente comunicazione tra gli Enti coinvolti nelle attività di controllo e di prevenzione.

L'attività di analisi consentirà di acquisire, analizzare e gestire elementi e dati complessi che, da un lato, accresceranno la capacità di gestire la sicurezza dell'ambiente che ospita l'infrastruttura critica in argomento, dall'altro, consentirà di condividere con altri Enti e con gli Organi di sicurezza pubblica utili elementi di conoscenza, preziosi per la tutela della sicurezza dei beni, delle infrastrutture, dei cittadini e dei commerci.

In linea con le previsioni normative in tema di sicurezza dei trasporti e di tutela delle infrastrutture critiche, come gangli vitali del sistema Paese.

In relazione a quanto previsto dalla Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni (Obiettivi strategici e raccomandazioni per la politica UE dei trasporti marittimi fino al 2018), è necessario potenziare le capacità del sistema di trasporto marittimo istituendo un sistema integrato di controllo per monitorare la presenza e la movimentazione di imbarcazioni che si spostano da e verso i porti europei o che transitano nelle acque dell'UE o in prossimità di esse.

A tale riguardo è stata avviata l'iniziativa E-MS (Electronic Maritime Simplification) a cui partecipa l'Agenzia delle Dogane e dei Monopoli in collaborazione con il Comando Generale Capitanerie di Porto.

2.1 Applicazione del concetto di "sicurezza"

La prima evidenza concerne il concetto stesso di sicurezza che, nell'ambito di Gioia Tauro, merita un approfondimento laddove posto in relazione con il mercato di riferimento delle attività svolte nel porto.

Il porto di Gioia Tauro è leader nel Mediterraneo nelle attività di transhipment, un mercato di respiro mondiale in cui la concorrenza è rappresentata da altre realtà internazionali ed il business si orienta, con immediatezza e consistenza, nel luogo ove le operazioni sono svolte con il minore costo.

L'attività di sicurezza può essere percepita come uno dei fattori di "attrito" alla convenienza economica (nel caso in cui le procedure e le modalità operative dovessero causare ritardi temporali nel movimento delle merci) e quindi allo sviluppo economico dell'intera area: il ritardo si traduce in un costo e il sito gioiese diventerebbe inappetibile per le rotte internazionali di movimento merci.

Purtuttavia, è di tutta evidenza che il dispositivo di sicurezza non potrà mai essere sacrificato nella propria consistenza ed effettività alle esigenze di business; è proprio il respiro internazionale del traffico merci ad imporre la certezza e la qualità delle operazioni di controllo svolte in ambito portuale.

In quest'ambito si inserisce anche l'adesione ad accordi e standard internazionali oltre che il rilievo negativo in ambito globale che avrebbe un qualsiasi significativo incremento della pressione criminale percepita sull'area e sull'infrastruttura.

Per quanto enunciato, l'applicazione del nuovo sistema deve sostenere il concetto di sicurezza in termini di compenetrazione della propria applicazione operativa con le attività del porto affinché sia perseguito e garantito l'aumento:

- di efficacia, in termini di accresciuta capacità di analisi e controllo da parte delle Organizzazioni deputate alla sicurezza;
- di efficienza (nel senso di ininfluenza, se non in termini di fattivo contributo al miglioramento) della capacità della struttura portuale di svolgere le proprie attività di riferimento.

2.1.1 Integrazione della sicurezza

Poiché l'intero progetto è incentrato sul concetto di "integrazione della sicurezza", è indispensabile chiarire come si intende interpretare la tematica ed implementare la soluzione.

Molti dei progetti avviati negli anni scorsi non sono ancora completati e, per questo, appare complessa una compiuta integrazione che veda come punto di partenza i sistemi in via di realizzazione.

La soluzione che si individua per questo progetto consisterà nella previsione di una serie di porte di comunicazione applicativa per l'interscambio di dati.

Per quanto descritto, la soluzione progettuale dovrà presentare una forte solidità intrinseca prefigurando la realizzazione di un sistema completo ma che, nel contempo, presenti aperture per future integrazioni che non dovranno comprometterne la consistenza ed il raggiungimento dei benefici attesi nei tempi previsti.

2.2 BENEFICI ATTESI

I dati statistici sulla criminalità e le analisi socio economiche del territorio su cui si sviluppa il porto di Gioia Tauro evidenziano l'urgenza e l'esigenza di garantire in modo continuativo il "presidio del territorio" non solo con le azioni di potenziamento di tipo tecnologico sinora perseguite, ma anche con interventi che promuovano il coordinamento tra le specifiche attività di tutti gli Enti (tra cui l'Agenzia delle Dogane e dei Monopoli e le Forze di Polizia a competenza generale, specialistica e locale) presenti sul territorio ed aventi un forte peso specifico sui processi di sicurezza del porto e, di riflesso, sullo sviluppo socio-economico dell'area stessa.

Nella fattispecie il presente progetto ben risponde a questa esigenza di coinvolgimento e di condivisione informativa ed operativa, avendo previsto che i vari Enti operanti nell'area avranno la possibilità di utilizzare le funzionalità del Sistema (che saranno inquadrate in processi e procedure ridisegnati per massimizzare l'efficacia, nel rispetto delle missioni istituzionali e dei vincoli di riservatezza) migliorando l'efficienza in termini di:

- fluidità delle operazioni in porto: l'integrazione e l'analisi avanzata dei dati, e il conseguente potenziamento dell'analisi del rischio doganale nonché l'interoperabilità rendono più fluide e sicure le operazioni di sdoganamento riducendo tempi e costi per gli operatori. L'invio anticipato dei dati relativi alle merci in arrivo consente all'Autorità Portuale e alla Dogana di selezionare le idonee aree di scarico container per l'esecuzione rapida dei controlli mentre, l'utilizzo dei sigilli elettronici, garantisce l'integrità e la sicurezza delle merci trasportate .

- sicurezza dei trasporti e delle vie di comunicazione: l'integrazione dei vari sistemi (dati, video, ecc.) gestiti da tutti gli attori coinvolti nel processo di sdoganamento consente un gestione tempestiva degli alert e quindi una maggior reattività in caso di eventi critici. L'implementazione di innovativi sistemi e processi di controllo *on route* permette di allargare lo spazio della possibilità di intervento da parte delle varie Agenzie interessate, al retro porto, all'Area Ampia, e all'intero percorso del vettore sino al punto denunciato di arrivo, incrementando la efficacia ed efficienza dei controlli ai fini della sicurezza pubblica (individuazione di armi, esplosivi) e la prevenzione di eventuali attentati.

In termini di prestazioni operative, il progetto mira ad ottenere:

- un aumento dell'efficacia dei controlli doganali e di sicurezza;
- una maggiore efficacia ed efficienza dell'intervento dei vari enti/amministrazioni coinvolte nel processo di sdoganamento (approccio "s*ingle window/one stop shop")*
- una riduzione del numero dei reati, sia nell'area portuale sia in quella retro-portuale;
- un aumento dell'efficienza dei controlli di sicurezza attraverso una sensibile riduzione dei loro tempi di attuazione;
- un incremento dell'individuazione precoce dei tentativi di reato o di eventi indesiderati,
- una maggior sicurezza del trasporto e del commercio marittimo afferente a Gioia Tauro;
- un miglioramento della percezione, da parte degli operatori economici e dei lavoratori, del livello di sicurezza e della possibilità di operare nel rispetto della legalità;
- una tempestiva individuazione di possibili minacce criminali e/o terroristiche attraverso la collaborazione delle istituzioni competenti.

Inoltre, il progetto mira a creare una "best practice" nel panorama portuale italiano che potrà essere punto di riferimento e di eccellenza nazionale e sovranazionale della realizzazione di un sistema integrato di sicurezza (organizzazione, processi / attività, tecnologie) in conformità con quanto disposto alla recente Direttiva EU sulla Protezione delle Infrastrutture Critiche.

Il sistema potrebbe essere già compliant all'iniziativa E-MS (Electronic Maritime Simplification) e incrementare la potenzialità commerciale del porto, favorendo lo scambio di informazioni con altre iniziative comunitarie (e-Freight, e-Customs, ecc.), in modo che si possa disporre di informazioni utili a tracciare la movimentazione merci non solo durante la fase del trasporto via mare o acque navigabili ma anche nelle altre fasi del trasporto, in una vera ottica di co-modalità.

A tal fine, il Sistema, in una logica territoriale di logistica integrata, prefigura la realizzazione di un modello di sviluppo della sicurezza integrata che sia replicabile ed applicabile a tutti i più grandi porti italiani.

2.2.1 Ulteriori aspetti da considerare ai fini dell'integrazione

Il porto di Gioia Tauro è interessato da un progetto (delibera CIPE(89/2003) per la costituzione un HUB interporto, ancora oggi a livello di progettazione preliminare, che prevede la realizzazione di diverse strutture al servizio del sistema logistico di cui il porto è il centro.

Il piano prevede entro il 2014 l'ampliamento del terminal container e la realizzazione di importanti strutture industriali asservite a garantire la catena del freddo per i container (terminale di rigasificazione e relativa piastra logistica del freddo).

Un altro aspetto che potrà caratterizzare a regime l'area portuale è costituito dalla cosiddetta "zona franca aperta" (cd. ZES) concessa con provvedimento dell'Autorità Doganale il 1 agosto 2003 sulla base del Codice Doganale Comunitario, secondo quanto previsto dall'art. 168bis del regolamento 2700/2000.

Si tratta di ulteriori aree portuali e retroportuali per circa 100 ha.

Lo scenario di implementazione del presente progetto non deve, quindi, limitarsi alla situazione attuale ma prendere in considerazione anche questi ulteriori aspetti che, quando realizzati e pienamente operativi, determineranno un'evoluzione degli scenari logistici.

Nell'ambito del sistema doganale, con particolare riferimento alle complesse attività che si svolgono nei porti, sono in corso di svolgimento sperimentazioni volte a rilanciare la competitività del sistema portuale nazionale per rendere più efficiente l'espletamento dei compiti istituzionali e migliorare la qualità dei servizi offerti all'utenza esterna attraverso l'incremento della sicurezza.

La Piattaforma UIRNet consente di disporre di un sistema per il monitoraggio dei mezzi su gomma sul territorio nazionale.

Anche il legislatore ha espresso la volontà di ampliare le possibilità dell'offerta intermodale modificando l'art. 46 del decreto legge 6 dicembre 2011, n. 201 (Decreto Legge 2 marzo 2012, n. 16 coordinato con la Legge di conversione 26 aprile 2012, n. 44).

Il presente documento descrive un modello di riferimento per il processo di importazione, con caratteristiche di scalabilità al fine di attuare, in via sperimentale, semplificazioni che consentano di accogliere merci, offrire servizi efficienti e garantire un'infrastruttura intermodale più ampia per la gestione della supply chain.

3. OBIETTIVI DI PROGETTO

3.1 ASPETTI GENERALI

Si ritiene necessario evidenziare, prima di ogni altra parte, i principi che ispirano il Sistema e dai quali discendono le contestuali scelte di carattere procedurale, tecnologico ed applicativo.

Come sopra evidenziato, la gara stimola l'identificazione e la proposta delle migliori soluzioni possibili da parte degli offerenti; per questo è necessaria non solo la mera descrizione del Sistema ma anche un approfondimento sui principi che lo ispirano e sugli obiettivi da perseguire.

3.1.1 Direttrici di intervento

Come accennato, il porto di Gioia Tauro è coinvolto nella realizzazione di precedenti progetti che stanno contribuendo ad un sensibile innalzamento del livello della sorveglianza fisica dell'area.

Al termine delle attività saranno disponibili un numero importante di dispositivi che consentiranno il controllo completo del contesto portuale.

Per questo, è stato ritenuto utile che l'investimento in questione, pur ponendosi in un'ottica di futura integrazione, contempli il coinvolgimento dell'entroterra portuale in un'ottica di estensione del contesto di sicurezza.

Tale aspetto rappresenta una novità assoluta nell'ambito dei finanziamenti per la sicurezza del porto di Gioia Tauro ma si identifica compiutamente con l'attuale fase di crescita del contesto portuale.

Difatti, si inserisce in una serie di iniziative che sono finalizzate:

- all'espansione del business che vada oltre il ruolo di transhipment;
- ad un forte coinvolgimento della confinante area industriale, anche con la previsione della realizzazione di un area ZES (Zona Economica Speciale);
- all'incremento del trasporto diretto merci via terra con aree industriali del Mezzogiorno ed interporti della parte peninsulare italiana.

Per quanto descritto, il sistema dovrà supportare una forte flessibilità con la capacità di adattamento a molteplici situazioni operative; tale caratteristica stimolerà una sempre più forte interazione con gli Organismi di sicurezza e le Agenzia governative di controllo

3.2 PANORAMICA DEGLI ELEMENTI FUNZIONALI

L'integrazione dei sistemi infrastrutturali di security dell'Area Ampia di Gioia Tauro con i sistemi di analisi di rischio doganali consisterà in una piattaforma in grado di correlare le informazioni dei sistemi operanti sul territorio per facilitare la visualizzazione integrata delle informazioni in tempo reale e di individuare, prevenire e supportare la gestione delle minacce e degli eventi di security.

Quindi, si tratta di un sistema integrato accentrato in un'unica "Sala di Regia" virtuale (e in una "Sala Crisi" che invece ne rappresenta il risvolto fisico) con il preciso scopo di mettere in campo attività ed azioni volte a ridurre il rischio per la sicurezza di ogni singolo elemento funzionale della filiera del trasporto e dei territori attraversati, anche attraverso l'utilizzo dei dati gestiti dai singoli sistemi di sicurezza e trasporto.

Il tutto avviene in una logica di integrazione sistemica verso il punto nevralgico costituito dal Centro destinato al controllo oltre che alla elaborazione e memorizzazione dati, dove convergono tutte le informazioni dei sottosistemi periferici e da dove vengono propagate le informazioni utili per il monitoraggio e per la gestione della sicurezza anche al fine fornire i relativi pre-allarmi ed allarmi verso gli Enti deputati al monitoraggio e decisione in modo da facilitare le azioni di intelligence, prevenzione e intervento.

L'integrazione con la Piattaforma UIRNet, invece, permetterà agli utenti del Sistema di entrare a far parte della rete logistica non solo nella dimensione fisica dei flussi, ma anche in quella informativa:

- sarà possibile ottenere informazioni sui veicoli in arrivo al porto, sia che essi abbiano dichiarato il porto come punto di arrivo delle loro missioni sia per logiche di prossimità;
- sarà possibile conseguire semplificazioni nelle attività di sdoganamento con un'evoluzione dell'attuale integrazione con AIDA;
- sarà possibile interagire con gli altri nodi logistici sulla base di un sistema comune;
- sarà possibile avere accesso ad un patrimonio informativo di sistema di enorme valore per l'incremento dell'efficienza e della sicurezza complessive.

Tale integrazione, nell'insieme, permetterà, in termini di sicurezza, di anticipare gli eventi indesiderati e di integrare le informazioni riguardanti eventi interni al porto (rilevati attraverso i sistemi a disposizione) con le informazioni provenienti dall'esterno, analizzandole simultaneamente attraverso lo strato middleware per la cross correlation (infrastruttura "trasversale" che consente l'organizzazione e l'analisi centralizzata degli eventi provenienti dai differenti ambiti, al fine di rilevare le combinazioni di informazioni ed eventi di interesse).

La struttura del Sistema oggetto del presente progetto, così come definita, è difatti in grado di garantire il monitoraggio ed il controllo dei diversi aspetti inerenti la sicurezza dei servizi erogati e dei processi sottesi ad essi, assicurando una efficace capacità di "early warning" rispetto a scenari di minaccia, una pronta ed efficace risposta in caso di incidenti o attacchi, nonché garantire la tempestiva comunicazione interna ed esterna.

Il Sistema, in sintesi, assicura la gestione della sicurezza in una modalità continua e che si auto-alimenta della quotidiana esperienza, capacità analitica ed operativa degli operatori e delle informazioni che provengono dagli apparati di campo.

Le informazioni provenienti dai sistemi da installare e da quelli già operanti, unitamente a quelle disponibili attraverso altre fonti possono essere utili a porre in essere azioni preventive di controllo e/o di investigazione/analisi.

E' quindi necessario prevedere un monitoraggio delle informazioni continuo (H24) che consenta di gestire in modo adeguato le possibili situazioni di pericolo e di emergenza.

La realizzazione del sistema dovrà includere le seguenti attività:

- analisi dei requisiti di business e dei vincoli tecnici per lo scambio di informazioni con operatori e agenzie pubbliche, attraverso interviste con gli operatori istituzionali e industriali coinvolti dal Sistema;
- analisi delle modalità di integrazione tecnica ed operativa con la PLN UIRNet per favorire le opportune e desiderate interoperabilità e sinergie;
- progettazione esecutiva del sistema;
- modellazione reporting, data-mining e case management derivanti dalla strutturazione, integrazione e cross-correlazione di informazioni derivanti da scambio informazioni con altri Enti e operatori, tracking e tracing di mezzi-merci-persone, sensori presenti a Gioia Tauro, informazioni da open source, ecc.;

- costruzione di un data center dedicato al sistema completo;
- realizzazione di una Sala Crisi.

Sotto il profilo della fruibilità da parte dell'utente, i Sistemi saranno accedibili ed utilizzabili in modalità web.

Gli apparati centrali per elaborazione e memorizzazione dei dati saranno collocati in locali idonei le cui caratteristiche ed ubicazione sono più avanti specificate.

Le performance del Sistema nel complesso dovranno essere adeguate all'uso e agli obiettivi del progetto.

Si assicureranno adeguate misure di sicurezza per far fronte ad eventuali malfunzionamenti (nonché aggressioni dall'esterno o usi impropri dall'interno) e garantire l'operatività continua del Sistema, con meccanismi di cura dell'integrità e di salvataggio dei dati.

Il Sistema dovrà garantire l'interconnessione delle componenti software sopra elencate e già operative.

Il modello di riferimento sarà quello della Cooperazione Applicativa finalizzato all'erogazione e alla fruizione di servizi tra i sistemi informatici della Pubblica Amministrazione.

Tale Sistema dovrà essere in grado di realizzare sia un'architettura orientata ai servizi (Service Oriented Architecture) sia un'architettura basata sulla notifica di eventi (Event Driven Architecture).

La tecnologia utilizzata per l'implementazione è quella dei Web Services e dei relativi standard/linguaggi/protocolli correlati: Schemi XML, Protocollo SOAP, Protocollo WSDL e il Registry UDDI.

L'elaborazione di queste informazioni consente agli utenti del Sistema (secondo i vari profili assegnati) di intraprendere e coordinare le azioni necessarie per la gestione dei rischi e degli eventi, fornendo l'eventuale supporto operativo alle funzioni coinvolte.

3.3 Scenario di integrazione

I sistemi di sicurezza, a valenza esclusivamente locale, possono integrare ed integrarsi con altri sistemi informativi, a valenza geografica più estesa, che possono fornire e/o ricevere informazioni utili a creare un sistema di sicurezza integrato più ampio.

Le logiche di integrazione delle diverse componenti del sistema di sicurezza portuale al fine di costituire il nuovo Sistema devono necessariamente essere ricondotte a logiche di integrazione di apparati tecnologici.

In maggior dettaglio si può affermare che il nuovo Sistema dovrà essere attuato in due fasi, non necessariamente propedeutiche l'una all'altra, e che l'integrazione finale, quella cioè che porterà alla creazione del sistema integrato, finalità dell'attuale progetto, dovrà essere attuata attraverso l'utilizzo di strumenti di una vera e propria cooperazione applicativa tra sistemi informativi.

Tale tecnica, già adeguatamente normata ed adottata a livello di colloquio tra amministrazioni pubbliche è l'unica che consente di mantenere elevati livelli di autonomia dei diversi sistemi e proporre, a seguito di specifici accordi tra i diversi attori istituzionali, quali informazioni rendere visibili attraverso la pubblicazione di una directory di servizi resi disponibili con differenti livelli di sicurezza a diversi attori.

Occorre quindi, in una prima fase far evolvere il sistema del porto verso un vero e proprio sistema informativo per poi procedere alla successiva integrazione.

Il primo step deve partire dall'analisi degli apparati esistenti nell'Area Ampia del porto di Gioia Tauro, dalle loro funzionalità e dal loro stato di realizzazione/attivazione.

Gli output che tali apparati forniscono dovranno essere oggetto di accurata analisi al fine di determinare il loro interesse in una più ampia disamina di processi che potrebbero determinare le minacce.

Per tutti gli apparati saranno quindi classificati gli output, ne saranno analizzate le caratteristiche, i valori che potranno assumere gli attributi delle segnalazioni (targhe di veicoli, codici di container, numero di badge del personale), il momento temporale in cui tali segnalazioni vengono attivate, la localizzazione (es. varchi controllati), il verso del movimento rilevato, e definiti i livelli di gravità dei segnali che tali apparati forniscono.

Per quanto detto in precedenza in merito agli interventi prospettati, le informazioni provenienti dai sistemi informativi esterni, oggetto dell'integrazione più ampia, saranno trattati nell'ambito della creazione del Sistema di sicurezza del porto di Gioia Tauro come degli apparati virtuali che, al pari degli altri dispositivi di sicurezza, a fronte di determinati eventi faranno scaturire delle segnalazioni.

L'adozione di tale modalità, resa possibile proprio dall'elevato livello di standardizzazione che è alla base della cooperazione applicativa, potrà costituire un modello e favorirne l'adozione in altre realtà portuali.

Ciascuno dei sistemi adottati ha un suo focus e specifiche sono le segnalazioni che da esso scaturiscono.

Ciascuna delle singole segnalazioni di un apparato ha un suo significato. In alcuni casi, da sole, possono costituire un elemento di allarme cui far seguire delle azioni, secondo uno schema di processo di reazione alla minaccia.

Inoltre, le diverse segnalazioni dei numerosi apparati, combinate tra loro sia come tipologia della segnalazione, localizzazione dell'evento, momento in cui l'evento si è verificato, livello di gravità della segnalazione possono essere correlate in sequenze di eventi che determinano, al loro accadimento, uno specifico profilo di minaccia.

Il personale addetto al controllo dovrà essere in grado di poter creare tali profili, in modo semplice, attraverso l'ausilio di un sistema che lo guiderà nella creazione dei diversi processi di minaccia illustrati da una rappresentazione grafica di eventi/segnalazioni correlate.

I profili, quando saranno operativi, saranno verificati dall'attuarsi dei singoli eventi, nella sequenza predefinita nel profilo stesso.

Sia al singolo evento/segnalazione che al profilo che lega più eventi minacciosi e che a sua volta definisce una minaccia complessa, sarà attribuito un valore di gravità della minaccia, che nel secondo caso sarà un valore determinato dai livelli riscontrati dagli eventi che costituiscono il profilo.

Dovranno essere definite un insieme di azioni da porre in essere al verificarsi di una minaccia. Queste azioni andranno a costituire un manuale operativo che individuerà i gruppi coinvolti, le responsabilità, il loro comportamento, la sequenza delle azioni da porre in essere, le informazioni da scambiare tra le diverse unità coinvolte nonché le modalità di colloquio da adottare.

3.3.1 Incremento dell'efficienza e dell'efficacia nei controlli doganali

Alcuni dei controlli avvengono alla presenza del personale doganale e della Guardia di Finanza, altri congiuntamente ad attori appartenenti ad altri organismi di controllo (veterinario, fitosanitario, Polizia di frontiera, ecc.).

L'integrazione può elevare l'efficienza dei controlli con l'introduzione di un sistema di workflow che consenta di pianificare le ispezioni delle merci in momenti in cui sia garantita la presenza di tutti gli attori coinvolti (chi deve fare cosa e quando).

Tale sistema non può prescindere dalla conoscenza preventiva dei turni di lavoro e quindi dalla disponibilità sul campo di rappresentanti degli organismi necessari al controllo.

Tale sistema potrà costituire un'agenda comune avvalendosi anche di una piattaforma di document management per la condivisione dei documenti necessari agli utenti per svolgere le proprie mansioni

L'integrazione si potrà avvalere anche delle informazioni fornite dalla PLN che consentiranno la migliore pianificazione di tutte le attività che si svolgono in ambito portuale, comprese le attività doganali.

I controlli doganali sono svolti sulla base dei risultati dell'analisi dei rischi che è svolta principalmente a livello centrale utilizzando il sistema dei profili di rischio.

Le informazioni per la determinazione dei profili provengono all'Ufficio Antifrode da diverse fonti e sono elaborate dai funzionari.

Sulla base delle loro investigazioni e delle correlazioni tra gli eventi che potrebbero determinare dei potenziali scenari di rischio vengono definiti i suddetti profili.

Il lavoro di intelligence svolto è molto complesso e richiede un continuo aggiornamento.

La proposta è di ottimizzare tale attività di monitoraggio delle fonti interne/esterne aumentando la capacità di riconoscimento dei rischi attraverso un approccio predittivo.

Si propone quindi di adottare un modulo di intelligence che sia in grado di:

- elaborare dati eterogenei;
- creare un archivio di modelli di rischio specifici delle attività doganali;
- estrarre in automatico dati da archivi operazionali;
- collegare in automatico le entità riconosciute nei dati;
- riconoscere scenari di rischio attraverso modelli predefiniti o specificamente progettati
- segnalare casi ad alto profilo di rischio;
- utilizzare i feedback per consolidare la base dati dei risultati e migliorare la qualità dei modelli adottati.

3.3.2 Integrazione con le informazioni provenienti dalla filiera del trasporto

La Piattaforma Logistica Nazionale mette a disposizione degli operatori del trasporto strumenti per organizzare ed ottimizzare il proprio business attraverso la creazione delle missioni, la pianificazione dei trasporti, l'ottimizzazione dei percorsi.

La piattaforma è in grado di offrire un servizio di tracciamento che, attraverso l'integrazione di ulteriori dispositivi (RFID, ecc.) può realizzare dei "corridoi virtuali sicuri".

Le informazioni provenienti dalla Piattaforma Logistica Nazionale contribuiranno ad aumentare l'efficienza dei controlli integrandosi con i sistemi di workflow e document management.

Inoltre costituiranno un'importante fonte di informazioni di cui si potrà avvalere sia il modulo di intelligence per accrescere l'efficacia dei controlli sia la Piattaforma Logistica Nazionale con i servizi offerti agli operatori del trasporto, minimizzando in tal modo i tempi della filiera.

In ragione di quanto sopra, si propone – di seguito - una descrizione dei macroblocchi di integrazione e dei relativi requisiti minimi richiesti:

- INTEGRAZIONE SEA-SIDE (SiSS)
- INTEGRAZIONE LAND-SIDE (SILS)
- FORNITURE HW/SW DI BASE
- INTEGRAZIONI INFRASTRUTTURALI

4. SOTTO-SISTEMA 1: INTEGRAZIONE SEA-SIDE (SISS)

4.1 I sistemi da integrare.

Il SiSS (componente Sotto-Sistema Sea-Side) che sarà realizzato dovrà, da un lato, interfacciare tutti i sistemi citati nei paragrafi precedenti, installati presso l'area portuale e retro portuale di Gioia Tauro, per avere la visione integrata di tutti gli eventi e i dati che caratterizzano l'ambiente operativo interno al porto, e dall'altro dovrà integrarsi con le attività ed il sistema informativo doganale, con il sistema Piana Sicura e con la Piattaforma Logistica Nazionale Digitale UIRNet, in grado di fornire i "segnali deboli" provenienti dal mondo esterno, per avere la visione completa del suo ecosistema

4.2 Sotto-Sistema proposto

L'obiettivo prioritario del progetto è la creazione di un sistema integrato di sicurezza ed analisi dell'operatività.

A partire dai sistemi preesistenti sarà necessario creare uno strato di integrazione che collezioni le informazioni di interesse da parte di ogni sottosistema per poi aggregarle e rappresentarle all'interno di un'unica interfaccia e un unico luogo (control room) eventualmente remotizzabile.

Il sistema oggetto della realizzazione prevede tre aree di attività:

- operative;
- safety & security;
- risk analisys.

Le tre aree di attività e di intervento avranno dei singoli moduli funzionali che risponderanno alle esigenze di ogni area, ma a livello più alto saranno unificate dal sistema di Analisi ed Intelligence vero centro di aggregazione di allarmi, eventi e informazioni.

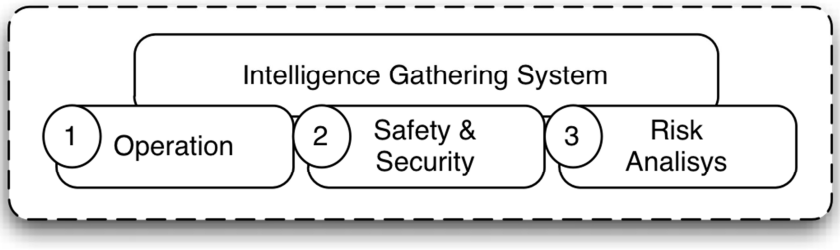

Figura 5 - Aree di attività del Sotto-Sistema proposto

Nell'immagine successiva è riportato uno schema degli elementi che compongono il Sotto-Sistema proposto, successivamente descritti singolarmente.

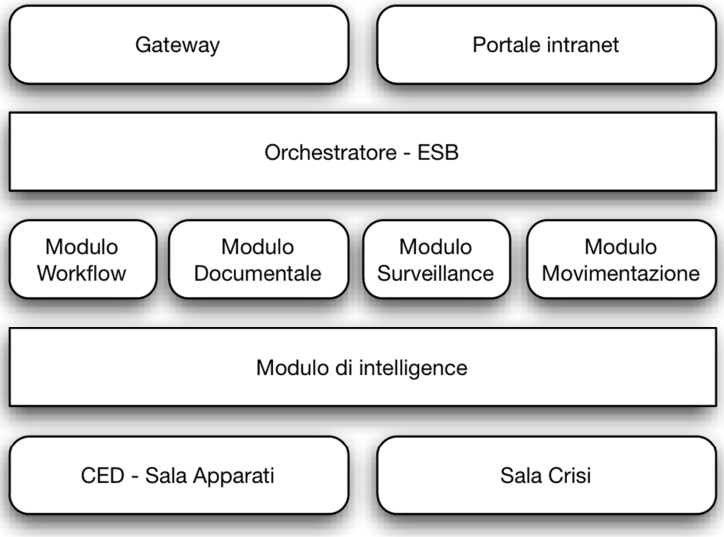

Figura 6 - SiSS: moduli componenti

Nell'immagine che segue sono riportati gli stessi elementi all'interno di un'architettura funzionale che delinea l'interazione di ciascun modulo con gli elementi interni ed esterni al SiSS.

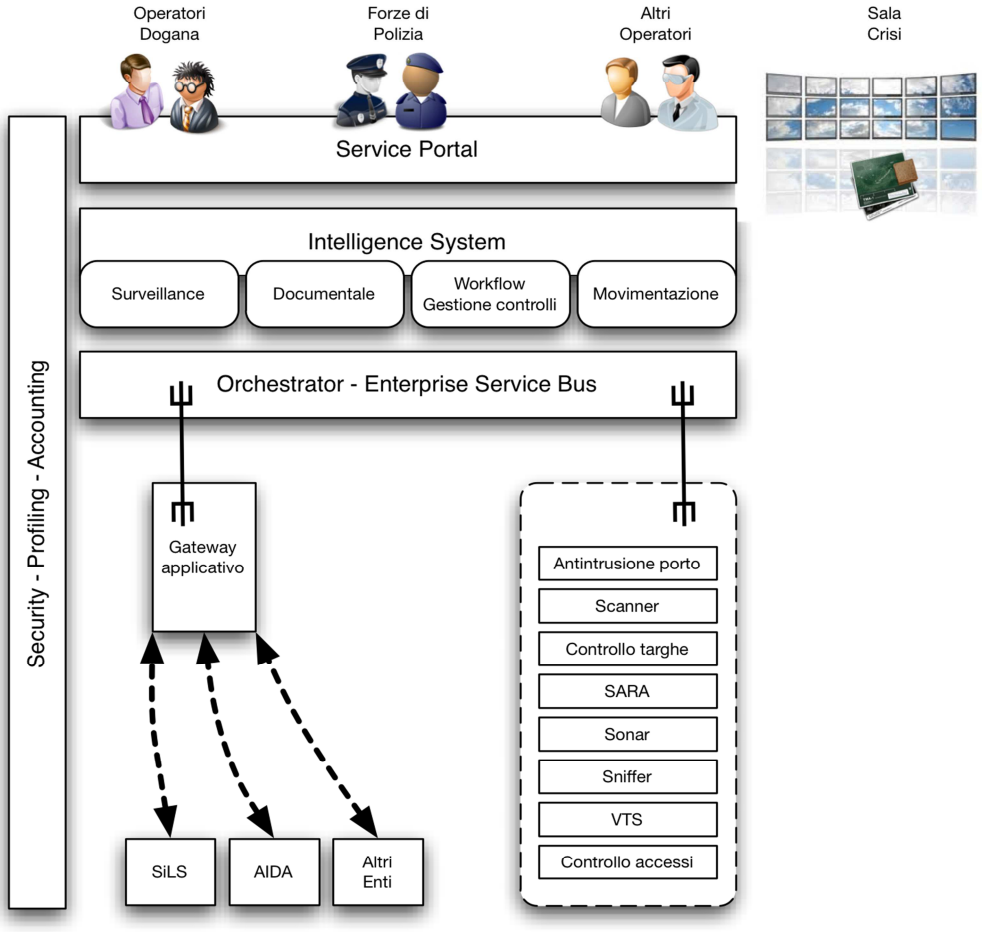

Figura 7 – Sotto-Sistema proposto: architettura funzionale

Dal punto di vista operativo la piattaforma ha i seguenti obiettivi:

- controllo e movimentazione dei mezzi e dei container nell'intera area-portuale allargata (porto/retroporto, nodi intermodali, zone franche, ulteriori aree di interesse) così come in corso di sperimentazione da parte dell'Agenzia delle Dogane e dei Monopoli in altre realtà nazionali e che beneficia della integrazione dei servizi della PLN e di AIDA;
- integrazione di tutte le informazioni di interesse ai fini della sicurezza provenienti dai sistemi locali;
- costituzione di un repository di tutta la documentazione a corredo delle merci e delle loro movimentazioni da mettere a disposizione, attraverso il sistema, di tutti gli organismi interessati nelle diverse fasi del ciclo di controllo;
- adozione di un business intelligence finalizzato ad ottimizzare tutte le attività, riducendo o annullando i tempi di controllo ed aumentando la capacità di riconoscimento dei rischi attraverso un approccio predittivo.

4.2.1 Soluzione architetturale

La soluzione dovrà poggiare sui più moderni paradigmi tecnologici, al fine di offrire una soluzione "agile e a prova di futuro", capace cioè di reagire "in tempo reale" a mutate esigenze di processo (es. modifiche normative), di organizzazione (es. variazioni del modello di funzionamento dell'organizzazione), di tecnologia (es. evoluzione dei sistemi), di integrazione (es. esigenza di inter-operare con nuovi sistemi), di sicurezza (es. nuove minacce e/o requisiti normativi).

Da un punto di vista logico il modello architetturale previsto per il Sotto-Sistema si basa su un'architettura software innovativa che ha l'obiettivo di supportare l'uso di servizi Web per garantire l'interoperabilità tra i diversi sistemi, cosi da consentire l'utilizzo delle singole applicazioni come componenti del processo di business e soddisfare le richieste degli utenti in modo integrato e trasparente.

Quanto detto si concretizza nell'implementazione di una Service-Oriented Architecture (SOA) declinata sul paradigma architetturale Event Driven Architecture (EDA) in grado di aumentare il livello di flessibilità e di reattività dell'intera soluzione.

Con la SOA si rende più veloce, agile e dinamica la creazione o la modifica di processi di Business grazie al riutilizzo di servizi condivisi, mentre attraverso l'Event-Driven si rende più reattiva e immediata la risposta da parte del Business ai cambiamenti nei processi.

Il continuo sviluppo dei sistemi informativi e la continua evoluzione delle tecnologie informatiche producono ciclicamente la necessità di sviluppare nuovo software.

Ogni qual volta avviene questa ristrutturazione, si pone il problema di evolvere il sistema evitando di perdere gli investimenti effettuati per sviluppare le applicazioni già presenti.

In quest'ottica s'inserisce il concetto d'integrazione tra le componenti che costituiscono un sistema informativo.

Lo scopo principale dell'integrazione è quello di ottenere lo scambio d'informazioni tra sistemi eterogenei ed autonomi in modo da sviluppare il business e mantenere gli asset già presenti.

L'Architettura che soddisfa pienamente quest'obiettivo è denominata SOA (Service Oriented Architecture).

SOA è un insieme di principi, processi e linee guida, indipendenti dalla tecnologia, volti alla scomposizione del sistema applicativo in "servizi" riusabili e interoperabili, destinati a semplificare l'evoluzione del business aziendale.

In altre parole, SOA rappresenta l'Architettura ottimale per minimizzare i costi di evoluzione e d'integrazione nei sistemi informativi complessi.

Nell'ambito di un'Architettura SOA è quindi possibile modificare, in maniera relativamente più semplice, le modalità di interazione tra i servizi, oppure la combinazione nella quale questi vengono utilizzati nel processo, così come risulta più agevole aggiungere nuovi servizi e modificare i processi per rispondere alle specifiche esigenze di business: il processo di business non è più vincolato da una specifica piattaforma o da un'applicazione ma può essere considerato come un componente di un processo più ampio e quindi riutilizzato o modificato.

L'Architettura orientata ai servizi si presenta particolarmente adatta per la realtà doganale che presenta una discreta complessità di processi e applicazioni, dal momento che agevola l'interazione tra i diversi sistemi permettendo, al contempo, alle attività di business di sviluppare processi efficienti, sia internamente che esternamente ed aumentarne la flessibilità e l'adattabilità.

Accanto ai vantaggi dell'Architettura SOA ci sono quelli del paradigma EDA (Event Driven Architecture) che costituisce uno stile architetturale in cui alcuni elementi applicativi entrano in esecuzione in risposta al verificarsi di eventi.

Tutto ciò rende la proposta architetturale flessibile, interoperabile e aperta e quindi adattabile alle esigenze di espansione in termini di necessità funzionali e di integrazione con i sistemi esterni.

l requisiti e le caratteristiche tecnico-funzionali del Sistema, dovranno essere opportunamente analizzati, arricchiti e validati nell'ambito della produzione del progetto esecutivo e delle attività di analisi specialistica previste nel Business Process Modeling (BPM), volte a definire i processi operativi che dovranno essere supportati dalla piattaforma da implementare.

4.2.1.1 Layer di implementazione

Il Sotto-Sistema proposto si basa su un'architettura web based e multi layer che si sviluppa sui seguenti livelli logico-funzionali:

4.2.1.1.1 Security Layer

Coincide con il modulo di Identity & Access Management (IAM) che garantisce un approccio integrato e sicuro alla gestione delle identità utente per automatizzare, accelerare, e semplificare l'autenticazione, l'autorizzazione e il controllo degli accessi al sistema e la trasmissione dei dati sicura in modalità criptata e quindi non intercettabile da terzi mediante l'utilizzo del protocollo Https.

Il Single Sign On permette all'utente di poter accedere a più applicazioni web attraverso un portale, con le medesime credenziali utente, che vanno fornite una sola volta, all'inizio della propria sessione di lavoro (e non ripetute all'accesso di ogni diversa applicazione).

Il modulo IAM si baserà sull'implementazione di Single Sign-on e Open Ldap come repository delle identità.

4.2.1.1.2 Presentation Layer

Rappresenta l'interfaccia di fruizione degli applicativi e garantisce l'accesso anche agli utenti con conoscenze limitate di informatica e strutture dati grazie all'uso di interfacce semplici ed intuitive.

E' costituita da un portale intranet quale punto di accesso unico ed integrato ai moduli applicativi e di supporto del sistema informativo.

4.2.1.1.3 Application Layer

E' costituito dai moduli applicativi del sistema informativo.

4.2.1.1.4 Business Process & Management Layer

Permette la gestione, il controllo e monitoraggio dei servizi basati su di una architettura SOA.

E' costituito dalle componenti di: Business Process Management (BPM), in grado di svolgere funzionalità di disegno dei processi e gestione dei task, un Workflow Engine, per l'esecuzione dei processi, il motore di definizione delle regole, che consente di mantenere separate le regole di business dalle applicazioni software e dai servizi che governano per massimizzare l'agilità della SOA ed un modulo per il controllo dei processi di business attraverso una consolle dove vengono presentati gli indicatori di performance del processo stesso (KPI).

4.2.1.1.5 Service Layer

Fornisce i servizi necessari a favorire l'interoperabilità tra i moduli applicativi interni del sistema informativo ed i sistemi esterni. Tali servizi sono realizzati principalmente con EJB, Web Services ed altre tecnologie e standard.

4.2.1.1.6 Integration Layer

Permette l'accesso e la comunicazione dei servizi fornendo meccanismi di integrazione.

E' costituito dalla componente di Enterprise Service Bus, il quale fornisce in maniera consistente servizi di sicurezza, messaggistica, routing intelligente e trasformazioni agendo come una dorsale attraverso la quale viaggiano servizi software e componenti applicativi nonché la componente di Registry, per la registrazione e classificazione dei servizi ed il Gateway applicativo per automatizzare lo scambio dati e informativo con specifici sistemi esterni.

4.2.1.1.7 Data Layer

Rappresenta lo strato dedicato alla gestione dei dati (Base di Dati) basato sul RDBMS e all'archiviazione e conservazione di documenti basato su Document Management System.

4.2.1.2 Vantaggi

L'utilizzo di un'architettura multi layer, web e basata interamente su tecnologia Java consentirà di ottenere un sistema informativo con caratteristiche di:

4.2.1.2.1 Scalabilità

L'architettura applicativa a layer proposta permette una scalabilità pressoché completa della piattaforma, sia verticale (aggiungendo nuovi nodi nei layer) che orizzontale (potenziando la capacità elaborativa dei nodi esistenti). In particolare, avendo scomposto in componenti e quindi in servizi l'intera piattaforma, in caso di necessità sarà possibile assegnare a componenti/servizi particolarmente esigenti in termini di carico dei sistemi dedicati potenziati nelle capacità elaborative.

Inoltre, un'Architettura SOA in cui i servizi sono disaccoppiati grazie anche alla presenza dell'ESB consentirebbe addirittura l'adozione di architetture di elaborazione di tipo "cIoud", rendendo cosi virtualmente infinita la capacità di scalare la piattaforma e conseguirebbe l'adottabilità del modello in realtà che rappresentano esigenze differenti.

I servizi potrebbero risiedere in nodi distribuiti e contribuire alle attività di elaborazione pur essendo fisicamente allocati in altri data center.

4.2.1.2.2 Flessibilità

Capacità di adattarsi rapidamente al mutare delle esigenze informative e, in particolare, ai cambiamenti di contesto (il quadro giuridico, lo sviluppo tecnologico) oltre che all'interazione con altri progetti.

Per ciò che riguarda l'architettura generale la flessibilità è garantita dal suo essere articolata in un insieme di componenti software organizzate in strati applicativi con responsabilità chiare e distinte, progettati secondo gli standard dell'Ingegneria del Software (User Interface, Business Logic Layer, Data Access Layer)

4.2.1.2.3 Modularità e estendibilità

Il Sotto-Sistema sarà sviluppato in maniera modulare grazie alla adozione dell'Architettura SOA, all'utilizzo di un ESB per la comunicazione tra servizi e della componente BPM per l'orchestrazione. Il sistema garantirà la possibilità di accogliere nuove applicazioni e tecnologie senza doverlo riprogettare integralmente.

Grazie alla modularità della piattaforma sarà possibile far evolvere il Sistema aggiungendo o eliminando moduli attraverso una operazione elementare e realizzabile a caldo, cioè senza interrompere l'erogazione dei servizi.

In particolare, la comunicazione del modulo aggiunto con i moduli già esistenti sarà governata attraverso l'ESB e i processi di business saranno orchestrati mediante il BPM, mentre l'autenticazione, i ruoli e i relativi privilegi degli utenti saranno garantiti dalla componente IAM.

E' da evidenziare che una simile architettura potrà essere in grado di integrare, secondo gli stessi principi, moduli provenienti da altre applicazioni o da prodotti COTS (Component Off The Shelf), indipendentemente se essi siano nativi SOA o meno.

In quest'ultimo caso si procederà alla realizzazione di servizi di integrazione che realizzino un "wrapping" dell'applicazione per consentirne una integrazione SOA mediante l'ESB.

4.2.1.2.4 Facilmente configurabile

I moduli software offerti per la realizzazione del Sotto-Sistema saranno tutti dotati di interfaccia grafica per consentire di configurare ed estendere i singoli componenti senza dover modificare manualmente il codice sorgente.

4.2.1.2.5 Affidabilità e robustezza

Il Sotto-Sistema garantirà la sopravvivenza e il mantenimento delle performance dei servizi di fronte a guasti o condizioni di carico notevoli, grazie a un'architettura tecnologica ridondante basata sull'implementazione dei sistemi in cluster e architettura replicata, assicurando al Sistema di non perdere i dati e di renderli sempre disponibili.

4.2.1.2.6 Manutenibilità

Dovrà essere garantita la facilità di apportare modifiche al Sotto-Sistema realizzato grazie all'utilizzo di framework di sviluppo e software di base ampiamente diffusi, consolidati sul mercato e completamente accessibili.

In questo modo sarà possibile apportare facilmente qualsiasi modifica al Sotto-Sistema quali correzioni o adattamenti del software a modifiche negli ambienti, nei requisiti e nelle specifiche funzionali.

4.2.2 Moduli funzionali

4.2.2.1 Modulo Controllo della Movimentazione

Al modulo è delegato il controllo della movimentazione di tutti i mezzi e delle merci all'interno e, per quanto di pertinenza ai processi operativi, all'esterno dell'area portuale.

In particolare il modulo consentirà il controllo della movimentazione di merci, soggette a controllo doganale, che sono movimentate all'esterno dell'area portuale (cfr. 5.2.3.4 Peculiarità della gestione dei carichi spostati dall'area doganale prima dei controlli) per consentire l'effettuazione del controllo stesso in un luogo a disposizione dell'operatore economico e precedentemente dichiarato nei documenti trasmessi al sistema informativo doganale AIDA.

Riceve le informazioni di interesse dal Sotto-Sistema SiLS, da AIDA, da tutti i sistemi di sicurezza portuali, dal gestore del terminal container e dagli altri moduli operativi indipendentemente se la movimentazione sia determinata a seguito di un'azione da questi prodotta.

Le informazioni in ingresso ed in uscita al/dal modulo sono gestite dal modulo gateway applicativo, che provvede all'effettiva trasmissione/ricezione delle informazioni con gli altri sistemi attraverso modalità standard e dal modulo Orchestrator - ESB.

Le informazioni saranno classificate ed oggetto di normalizzazione.

Il modulo consentirà di ottenere informazioni su tutti i mezzi e le merci (container) in entrata ed uscita dal porto, nonché durante il percorso di avvicinamento o allontanamento dall'area portuale.

Le informazioni saranno fornite a diversi livelli di aggregazione o puntuali o restituite in formato grafico evidenziando gli elementi di interesse anche su mappe digitali.

Nel seguito sono riportati, a solo scopo esemplificativo, i principali requisiti funzionali di massima del modulo.

Requisito	Descrizione requisito
Interrogazioni puntuali ed aggregate	Il modulo deve essere in grado effettuare ricerche sui diversi oggetti conosciuti dal sistema (container, mezzi di trasporto, ecc.) anche con chiavi parziali, o combinando parametri di ricerca (identificativo – targa del mezzo, codice container), localizzazione, nome della flotta, orario di partenza ed arrivo, ecc.) e mostrando le informazioni disponibili suddivise in classi (denominazione, posizione, informazioni doganali, controlli, ecc.). Le diverse classi potranno essere selezionate consentendo l'apertura di finestre contenenti le ulteriori informazioni di pertinenza della classe. Tra i diversi parametri di ricerca sarà possibile richiedere l'elenco dei mezzi (container, mezzi di trasporto, ecc.) che, in base al proprio piano di viaggio (informazioni provenienti da SiLS) saranno nell'area portuale entro un fissato arco temporale. Analogamente a partire da un determinato oggetto identificato, (identificativo – targa del mezzo, codice container), sarà possibile visualizzare le variazioni che sono intercorse allo stesso (localizzazione, tempo, controlli, presa in carico, ecc.) secondo una sequenza temporale. Il modulo fornirà le stesse informazioni a diversi livelli di aggregazione.
Reportistica	Analogamente il modulo dovrà consentire di produrre report in formato pdf o excel o dati raw esportabili.

4.2.2.2 Modulo Surveillance

Al modulo è delegato il compito di acquisire e correlare le informazioni dei sistemi di sicurezza operanti sul territorio per facilitare la visualizzazione integrata delle informazioni in tempo reale.

Quindi, un Sotto-Sistema integrato con il preciso scopo di mettere in campo attività ed azioni volte a ridurre il rischio per la sicurezza di ogni singola area territoriale, anche attraverso l'utilizzo dei dati gestiti dai singoli sistemi: doganale, di sicurezza e trasporto.

Il tutto, in una logica di integrazione verso la componente centrale di elaborazione dati, dove convergono tutte le informazioni dei sottosistemi periferici e da dove vengono propagate le informazioni utili per il monitoraggio, gestione della sicurezza territoriale, per fornire i relativi avvisi verso gli organismi deputati al monitoraggio e decisione, in modo da facilitare le azioni di intelligence, prevenzione e intervento.

Scopo del modulo è costituire l'interfaccia tra i sistemi/apparati di sicurezza alimentando il Sotto-Sistema con le informazioni elementari da essi generate.

Il modulo consentirà inoltre di visualizzare le informazioni relative ad un determinato sistema di sicurezza offrendo la possibilità di ottenere informazioni storiche sugli eventi generati, statistiche e report.

Nel seguito sono riportati, a solo scopo informativo, i principali requisiti funzionali di massima relativi all'acquisizione dei dati dai sistemi di sicurezza presenti.

Requisito	Descrizione requisito
Acquisizione degli eventi provenienti dai sistemi esistenti	Il modulo deve essere integrato con le piattaforme e i sistemi sviluppati per la sicurezza e per i trasporti, esistenti e operanti nell'area portuale e nel territorio così da aggregare in modo funzionale sia le informazioni/immagini generate dai sistemi di sicurezza, sia tutte le notizie e dati relativi ai trasporti navali e terrestri.
Normalizzazione degli eventi	Il modulo deve essere in grado di normalizzare le informazioni collegate agli eventi provenienti dai sistemi esterni e registrarle all'interno di un Data Base
Auto diagnostica del sistema	Il modulo deve essere in grado di segnalare eventuali anomalie e/o malfunzionamenti provenienti sia dai sistemi alimentanti sia degli apparati di sorveglianza.
Apertura a future integrazioni	Il modulo deve essere aperto a future integrazioni con altri sistemi di sicurezza.

4.2.2.3 Modulo Service Portal

Costituisce l'interfaccia per l'interazione con il SiSS da parte di tutto il personale.

Una funzionalità di profilazione consentirà di ritagliare le funzionalità disponibili in dipendenza del ruolo e del livello di autorizzazione e di propagarlo in automatico a tutti i sistemi web (SSO) ed, eventualmente, a tutti i sistemi non web predisposti a questa funzione.

Il modulo deve prevedere l'integrazione delle anagrafiche degli operatori autorizzati ad accedere al Sotto-Sistema e alla loro profilazione.

A titolo esemplificativo e non esaustivo, il Sistema dovrà prevedere almeno i seguenti profili:

- amministratore di sistema;
- Operatore Autorità Portuale;
- Operatore Forze dell'Ordine;
- Operatore Agenzia delle Dogane e dei Monopoli;
- Operatore esterno.

Ad ognuno di questi profili saranno associati sottoinsiemi di funzionalità in base all'analisi effettuata durante la fase iniziale di progetto.

Allo scopo di rendere pienamente funzionali gli aspetti di autorizzazione e profilazione sarà necessario fornire un sistema di Identity and Access Management per la gestione delle profilazioni, autorizzazione e autenticazione.

Il modulo includerà quindi una componente di IAM a cui sarà delegata la gestione degli accessi al sistema assolvendo i compiti di:

- autenticazione;
- controllo di accesso e autorizzazione;
- Single Sign On (SSO);
- servizi di directory;
- servizi di logging.

Sarà altresì presente un modulo di Autenticazione centralizzato per la validazione delle credenziali utente.

Il portale web dovrà avere una struttura di navigazione ed una fruibilità in accordo con le indicazioni del W3C.

La definizione dei servizi messi a disposizione dal portale interno e la struttura dell'alberatura delle pagine sarà oggetto di analisi congiunta con i referenti individuati dalla Committente.

Nel seguito sono riportati i principali requisiti funzionali di massima del modulo.

Requisito	Descrizione requisito
Visualizzazione	Dal portale di accesso dovrà essere possibile accedere ai diversi moduli (Intelligence, controllo della movimentazione, ecc.) in modalità redirect o integrata all'interno delle pagine web.
Conservazione log	Dovrà essere mantenuta una cronologia degli accessi utente avvenuti con successo e degli accessi errati.
Controlli di input	Dovranno essere previsti controlli formali su input utente e dovranno essere svolti tramite l'implementazione di opportuni meccanismi applicativi per la validazione dell'input.
Identificazione e autorizzazione	Si richiede l'identificazione ed autenticazione univoca e personale degli utenti.
Profilatura	Dovranno essere definite delle politiche di controllo accessi di tipo role-based, associando dei privilegi in base ai ruoli dei singoli o insiemi coerenti di utenti, rispondenti ai servizi per i quali sono intitolati. Dovrà prevedere almeno i seguenti profili: • amministratore di sistema; • Operatore Autorità Portuale; • Operatore Forze dell'Ordine; • Operatore esterno; • Operatore Agenzia delle Dogane e dei Monopoli.
Accesso SSL	La soluzione proposta deve poter consentire l'accesso crittografato alle funzionalità web autenticate in modo nativo tramite SSL via HTTPS.
Compatibilità WEB Browser	E' richiesta la compatibilità con i principali web browser (il Fornitore dovrà specificare eventuali limitazioni presenti). E' richiesta la compatibilità con le prescrizioni W3C.
Accesso ai diversi sistemi ed applicativi disponibili	La soluzione deve consentire l'accesso a tutti i sistemi ed applicativi disponibili e già in uso presso l'area portuale.

4.2.2.4 Modulo Workflow

Il SiSS dovrà prevedere un motore di workflow, interfacciabile con tutti i moduli proposti, che consenta di definire processi di comunicazione e controllo di flussi (autorizzativi, documentali, ecc.).

Il disegno dei processi dovrà avvenire in modalità visuale utilizzando lo standard BPMN 2.0.

Il modulo consentirà, tra le altre, le seguenti funzionalità:

- creazione grafica dei processi di business mediante editor web-based;
- supporto delle specifiche WS-Human Task per l'inclusione di compiti che devono essere eseguiti da attori umani;
- console di gestione di processi, istanze, attività, gestione dei task e reporting;
- interrogazione, monitoraggio, analisi dello storico dei processi, istanze ed attività effettuate;
- funzionalità di integrazione con motori di regole.

All’interno del modulo sarà reso disponibile ed integrato un software per definire, distribuire, eseguire, monitorare e mantenere la varietà e la complessità delle logiche di decisione all’interno dell’organizzazione, con la possibilità di implementare politiche, requisiti ed istruzioni normalmente utilizzati per determinare azioni che si svolgono nelle applicazioni e nei sistemi.

Il modulo dovrà consentire in breve tempo l’adeguamento ad eventuali cambiamenti della regolamentazione senza dover intervenire e predisporre nuovi rilasci di codice, permettendo agli utenti business di gestire direttamente le regole, attraverso un’interfaccia facilmente comprensibile.

In particolare si intende utilizzare tale modulo per la gestione operativa dei processi di controllo dei container all’interno del porto e delle aree contigue o limitrofe, implementando opportune regole di gestione.

Il modulo consentirà di definire le specificità dei processi (BPEL) e degli attori in modo guidato, facilmente modificabile ed adattabile ad altre realtà portuali in modo che possa costituire un modello di riferimento più generale adottabile a livello nazionale.

Il modulo implementa, tra l’altro, lo scenario riportato in Fig. 8.

Il modulo riceve dalle altre componenti del Sistema le informazioni relative al flusso delle merci con l’indicazione del tipo, del momento e del luogo in cui effettuare il controllo.

Si avvale delle informazioni trasmesse dagli altri sistemi e moduli in merito alla presenza del personale necessario all’effettuazione del controllo e coordina, anche attraverso un sistema di messaggistica immediata, l’agenda dei controlli ai diversi attori selezionati in base alla costituzione del team ed al carico di lavoro.

Rende disponibile alle squadre di controllo, avvalendosi del modulo documentale, il manuale operativo e le indicazioni del tipo di controllo da effettuare; ne consente la registrazione dell’esito, rendendo immediatamente disponibili tali informazioni al sistema doganale AIDA, al modulo documentale ed al modulo intelligence per le successive elaborazioni.

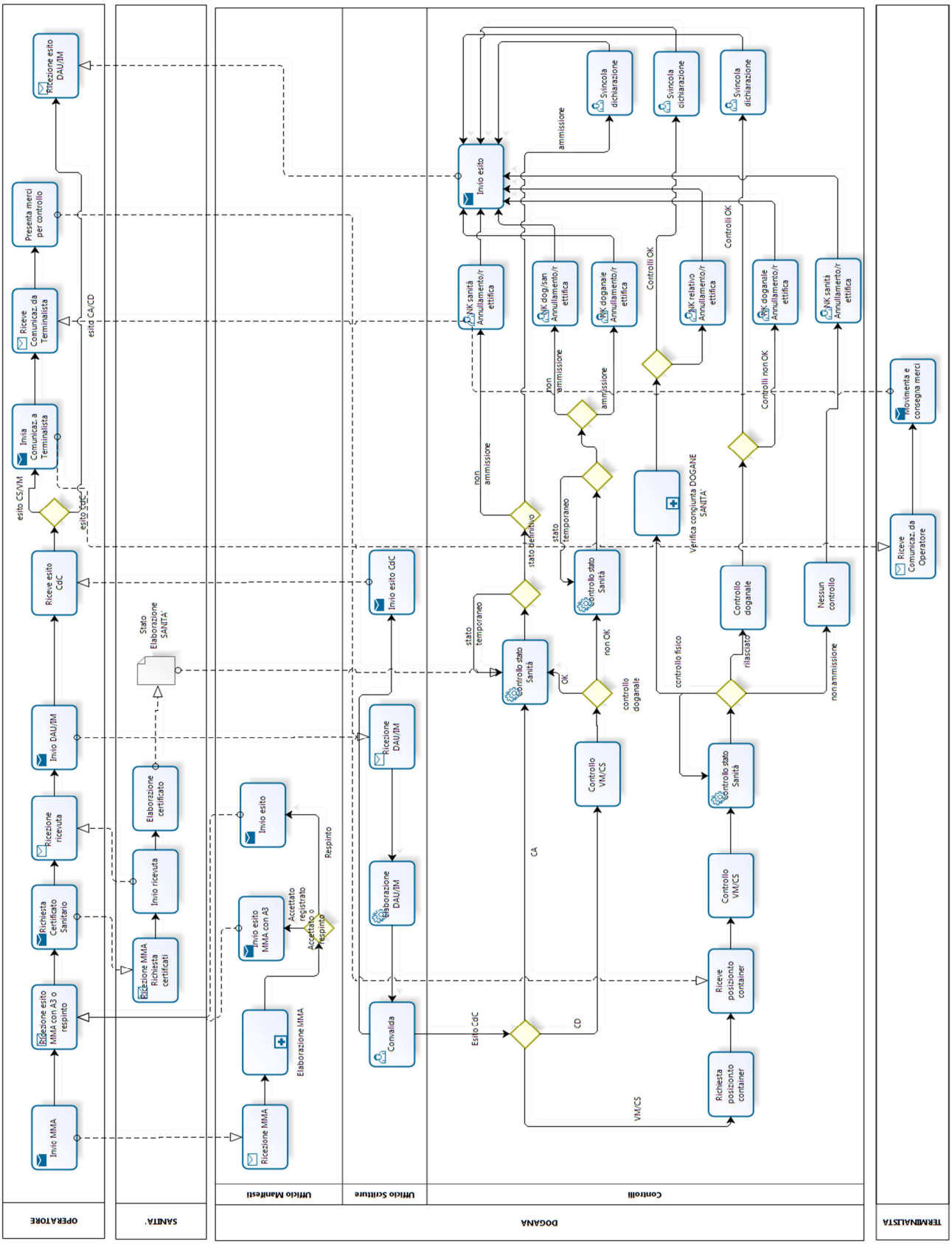

Figura 8 - Processo Controlli congiunti

Il software per l'implementazione di tali ulteriori funzionalità potrà essere selezionato tra i numerosi prodotti open source *Collaborative software* (conosciuti anche come *groupware* o *workgroup support systems*).

Si tratta di software progettato per facilitare la collaborazione di soggetti responsabili di task specifici all'interno di un framework comune.

Di seguito sono riportati i principali requisiti funzionali di massima del modulo

Requisito	Descrizione requisito
Interfacciabilità	Il modulo deve consentire di definire processi di comunicazione e controllo di flussi (autorizzativi, documentali, ecc.) tra i diversi moduli. Il disegno dei processi dovrà avvenire in modalità visuale utilizzando lo standard BPMN 2.0.
Usabilità	Il modulo deve consentire la creazione/modifica grafica dei processi di business mediante editor web-based nonché supporto delle specifiche WS-Human Task per l'inclusione di compiti che devono essere eseguiti da attori umani.
Gestione	Il modulo sarà provvisto di una console di gestione di processi, istanze, attività, gestione dei task e reporting.
Integrabilità	Il modulo dovrà essere in grado di integrare motori di regole. Dovrà essere inoltre possibile definire, distribuire, eseguire, monitorare e mantenere la varietà e la complessità delle logiche di decisione all'interno dell'organizzazione.
Funzionalità	Il modulo dovrà consentire almeno le seguenti funzionalità: interrogazione, monitoraggio, analisi dello storico dei processi, istanze ed attività effettuate.
Adattabilità	Il modulo consentirà agevolmente l'adeguamento al cambiamento della regolamentazione senza dover intervenire in nuovi rilasci di codice permettendo agli operatori abilitati di gestire direttamente le regole.

4.2.2.5 Modulo Documentale

Al modulo sono delegate le funzionalità di gestione della documentazione a corredo dei mezzi e delle merci.

Al fine di favorire e velocizzare i controlli si potrà valutare se anche i documenti già memorizzati su altri sistemi potranno essere replicati in via preventiva localmente attraverso delle estrazioni parziali.

Il modulo deve contemplare anche quella che viene identificata come Record Management System disponibile mediante:

- un'unità di rete condivisa, grazie allo standard CIFS (Common Internet File System);
- un'applicazione e-mail conforme a IMAP;
- un singolo repository accessibile tramite interfaccia web.

Di seguito sono riportati i principali requisiti funzionali di massima del modulo.

Requisito	Descrizione requisito
Gestione	Il modulo deve fornire una piattaforma di gestione dei contenuti

	che si possa utilizzare negli attuali contesti multimediali (cloud) o all'interno del firewall dell'organizzazione locale. Il modulo deve consentire l'archiviazione, la classificazione, indicizzazione e condivisione di tutti i documenti relativi a ciascun processo di business.
Usabilità	Il modulo deve consentire, in modo trasparente all'utente, di salvare un documento, creato con gli usuali strumenti di produttività individuale (MS Office, Open Office, Dreamweaver o AutoCad, ecc.), di catalogarlo in modo automatico in base al suo contenuto e di fornire chiavi di indicizzazione in modalità Google-like.
Versioning	Il modulo deve consentire il versionamento dei documenti mantenendo storia delle variazioni ad esso apportate.
Versatilità	Il modulo deve consentire modalità di fruizione da parte di utenti in movimento. Deve essere possibile lo sviluppo e l'integrazione di applicazioni personalizzate su dispositivi mobili (tablet).
Sicurezza	Il modulo deve consentire l'applicazione di criteri di sicurezza a livello aziendale, o di gruppo di lavoro, consentendo agli utenti di accedere solo ai contenuti per cui dispongono di un'autorizzazione.

4.2.2.6 Modulo Intelligence

E' il vero e proprio sistema di integrazione.

Si tratta di un sistema di intelligence e di analisi automatizzata dei rischi che viene alimentata sia dai dati contenuti nei documenti doganali e quindi resi disponibili dal sistema doganale AIDA (manifesti e dichiarazioni doganali) sia da altre informazioni, siano esse strutturate che nei più diversi formati, provenienti da tutti gli altri sottosistemi connessi; compagnie assicuratrici, armatori, registri navali, Forze di Polizia, ecc.

Il modulo deve poter fornire una vasta gamma di strumenti di analisi anti-frode, valutazione del rischio ed analisi investigativa, tra cui il monitoraggio delle transazioni, l'analisi comportamentale nonché l'analisi della rete dei collegamenti tra le diverse entità.

La soluzione deve poter analizzare un'ampia gamma di frodi e di tipologie di rischi nelle attività di controllo doganale tale da essere una piattaforma strategica che genera e gestisce i casi di accertamento attraverso tutti i settori (doganali, fiscali e frontiere) per:

- scoprire preventivamente traffici illeciti di merci in transito;
- ridurre i costi operativi dell'Agenzia delle Dogane e dei Monopoli, Autorità Portuale e Forze dell'Ordine;
- aumentare il tasso di scoperta e facilitare il passaggio dei carichi legittimi;
- contribuire alla protezione del Sistema-Paese e alla tutela del mercato.

Il modulo dovrà generare automaticamente comunicazioni personalizzate per casi di rischio di modesta entità, predisponendo allo stesso tempo rapporti documentati e dossier dettagliati con diagrammi di collegamenti per casi di media e alta pericolosità che richiedono interventi di accertamento e indagine.

La gamma di strumenti per l'analisi e l'investigazione dovrà includere:

- regole specifiche per controlli finalizzati alla scoperta del rischio nelle attività doganali;
- analisi statistica e di scenario, per identificare transazioni anomale alla luce dello scenario in cui si verificano (Social Network Analysis);
- evidenza di comportamenti che si discostano dalle medie/abitudini.

Tale modulo, infatti, avrà come obiettivo quello di consentire alla Committente di estrarre, gestire, integrare, aggregare ed analizzare grandi quantità di dati, al fine di offrire una sola base informativa, centralizzata e adeguata alla definizione di un sistema di supporto alle investigazioni.

Il modulo deve supportare le funzionalità di Data Management tramite un'interfaccia grafica che permetta il trattamento delle fonti dati, l'identificazione di dati invalidi, dati duplicati o già caricati, ecc.

Deve essere possibile la ripetibilità dei processi di acquisizione, trasformazione e caricamento dei dati e la loro pianificazione.

La piattaforma tecnologica utilizzata deve avere un modello dati predefinito e personalizzabile e fornire strumenti di reporting sia via web, sia attraverso l'integrazione di strumenti di uso comune quale ad esempio la suite di Microsoft Office o altri formati aperti.

Il modulo di intelligence sarà strutturato come nello schema seguente

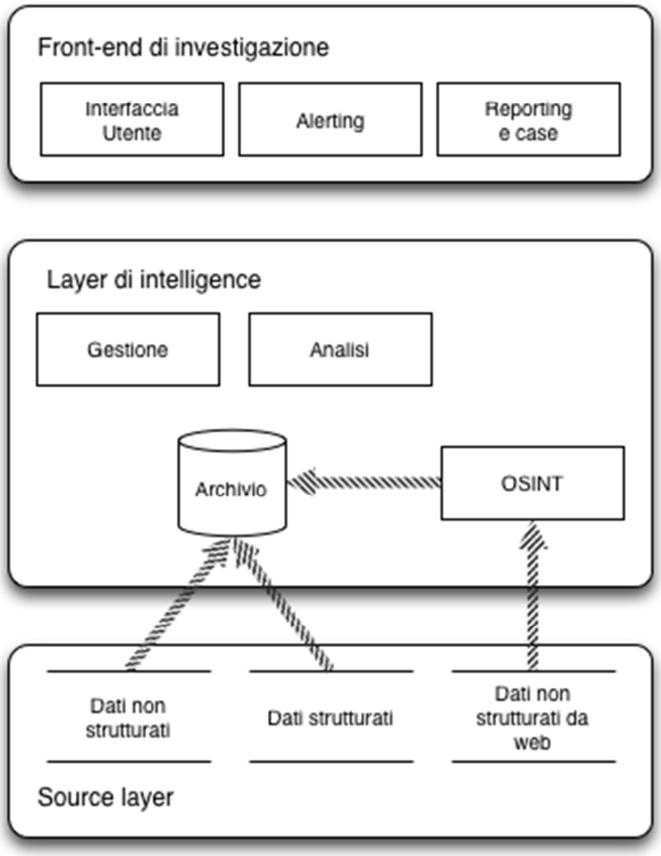

Figura 9 - Modulo di Intelligence

4.2.2.6.1 Source layer

Rappresenta le sorgenti dati logiche in input alla piattaforma.

Le sorgenti del modulo sono caratterizzate da due diverse tipologie: dati strutturati (es. database, fogli di calcolo, ecc.) e non strutturati (es. file di log, testi liberi, pagine web, ecc.).

4.2.2.6.2 Layer di intelligence

Elabora i dati provenienti dalle diverse fonti e li archivia in un proprio repository, identificando automaticamente al loro interno le entità (identità, luoghi, identificativi, numeri, ecc.) di interesse e collegandole tra loro in modo da mantenere tali relazioni e correlazioni stabilmente conservate al suo interno.

Il modulo è quindi costituito da:

- archivio unico degli eventi e delle reti di relazioni;
- modulo di gestione delle regole di correlazione e dei criteri di riconoscimento degli eventi, che effettua una analisi semantica e deterministica in grado di evidenziare collegamenti oggettivi, potenziali correlazioni e similitudini tra gli eventi;
- modulo di analisi predittiva, che opera la valutazione del rischio secondo le suddette regole e criteri;
- modulo OSINT per la raccolta di dati da fonti web aperte (almeno web 1.0, web 2.0, forum, social network) elaborate in parallelo senza alcun limite nel numero di fonti da gestire, e la contestuale importazione all'interno dell'archivio unico degli eventi e delle relazioni.

4.2.2.6.3 Presentation layer

Rappresenta la componente di "front-end" del sistema investigativo predittivo ed è composta logicamente da:

- Interfaccia utente di analisi e investigazione: consente la visualizzazione delle schede di allarme generate da matching positivi e di effettuare analisi di dettaglio sui dati contenuti nel data-warehouse incidenti;
- alerting: gestisce la visualizzazione degli alert derivanti dal modulo di analisi investigativa predittiva;
- case management e reporting: ambiente di lavorazione del case (insieme di più alert, dati dell'analista, ecc.) secondo workflow, di generazione di report e di consultazione degli eventi aggregati dal sistema.

Principali caratteristiche funzionali del sistema:

Macro funzionalità:

- Controlli di primo livello (singoli eventi) integrabili con interfacce native nel front-end operativo;
- Controlli di secondo livello (dati aggregati) dei dati transazionali dei diversi sistemi elaborabili in funzione di parametri/dimensioni disponibili;
- Verifiche di indagine integrabili con interfacce native con repository esterni, volte a identificare corrispondenze (esatte e approssimate sulla base di algoritmi di assonanza e traslitterazione) tra i dati disponibili e quelli di nominativi dei soggetti iscritti in liste (es. terrorismo, persone politicamente esposte, crimini finanziari, ecc.);
- Controlli di secondo livello, tramite indicatori e modelli già implementati e funzionanti rappresentativi dell'operatività del contesto:
- Disponibilità di una base dati interna volta ad acquisire attraverso un processo di alimentazione automatica da repository interni o esterni all'organizzazione, da fonti non strutturate testuali (analisi semantica) e web, storicizzare e utilizzare tutte le informazioni necessarie alle funzionalità;
- La base dati di cui al punto precedente consentirà un'articolazione dei legami di tipo "relazionale", navigabile mediante funzionalità native della soluzione, di utilizzare le informazioni acquisite e storicizzate in modo da esplodere operazioni/gruppi di operazioni in modalità "drill down" navigabile mettendo in relazione tutte le informazioni collegate;
- Estrazione automatica e profilatura delle entità: strumenti di riconoscimento e classificazione di qualsivoglia tipologia di entità (identità, luoghi, matricole, organizzazioni, ecc.) e di analisi investigativa che consentano di creare viste singole sulle entità e profili identificativi di ciascuna di esse, un approccio che consenta

l'estrazione di dati da tipologie eterogenee di fonti di informazione e li combini tra di loro in maniera automatica;

- Automatismi di scoperta e di costruzione dei legami esistenti (c.d. rete sociale) tra le entità riconosciute nei dati in input (sia strutturati che non strutturati, ovvero a testo libero), che consentano di individuare le cosiddette reti sociali e di attribuire automaticamente un livello di rischio sulla base di classificazioni, modelli di comportamento, relazioni ricorrenti, similitudini tra nomi, ecc. Tali legami possono essere anche affiancati da legami di tipo "light" che siano generati dal sistema su riconoscimento di similitudini, ripetitività e occorrenze tra eventi ed entità coinvolte in uno scenario di rete comune;
- La soluzione dovrà prevedere la possibilità di definire nuovi indicatori di rischio basati su qualsiasi elemento del patrimonio informativo disponibile. Le regole alla base degli indicatori saranno gestibili mediante uno strumento user-friendly senza supporto di risorse IT. Le attività di deployment degli indicatori in ambiente di "produzione" saranno altrettanto direttamente gestibili dagli utenti (analisti);
- Disponibilità di scenari predefiniti di riconoscimento che combinino regole logiche e tecniche di analisi, specifici dei diversi campi di intelligence. Possibilità di incorporare scenari di rischio esterni, modificare quelli disponibili e costruirne di nuovi attraverso l'interfaccia web di amministratore;
- Funzionalità native per interfacciare in modalità "near" real-time l'operatività di front-end con il set degli indicatori di rischio. Al ricorrere delle condizioni previste dalle regole degli indicatori, la soluzione deve disporre di funzionalità native per la gestione di un workflow che, alternativamente, a seconda dell'indicatore richiamato, segnali o blocchi l'esecuzione di un'operazione o attivi un workflow che consenta l'analisi di rischio presso una specifica entità organizzativa deputata alla concessione dell'autorizzazione;
- Il sistema di reporting integrato deve consentire la rappresentazione sintetica degli indicatori elaborati a livello di fenomeno e di tipologia di Indicatore. Il modulo di reporting dovrà essere in grado di comporre documenti e cruscotti con qualsiasi informazione presente nel sistema o importata attraverso documenti esterni al sistema, rendendoli disponibili, secondo diversi formati, a tutti i livelli di utenza, in funzione degli specifici livelli di autorizzazione;
- Funzionalità native (analitiche e grafiche) per l'individuazione di relazioni tra soggetti/entità in merito all'operatività svolta e di analisi della rete sociale così costruita, con relativa attribuzione di rischio;
- Funzionalità di watch-list caratterizzate da un set di campi chiave che possono essere utilizzati per la verifica dell'appartenenza di un'entità o delle entità ad essa collegate a liste di sorveglianza. Tale set potrà essere integrato/modificato. Le funzionalità di watch-list dovranno consentire di gestire in modo sistematico l'attivazione di alert a fronte della ricorrenza di specifici nominativi anche non ricompresi nelle corrispondenze di nominativi all'interno delle liste;
- Accessibilità anche ad eventuali fonti esterne per l'individuazione di soggetti/entità appartenenti a liste esterne;
- Sistema sarà di tipo Web-Oriented per lo strato di presentation (no Rich-Client) e conforme allo standard J2EE per la parte server-side;
- Completa riusabilità delle singole componenti, mediante disaccoppiamento dello strato di presentation da quello di business;
- Scalabilità della piattaforma, in termini di capacità del sistema di mantenere il tempo di risposta al crescere dell'utenza che lavora simultaneamente. Per il layer presentation dovranno essere supportati i più comuni apparati di load-balancing (locale e geografico);

L'archivio unico sarà costituito da un RDBMS con le seguenti caratteristiche:

- Funzionalità evolute di storage management (strumenti di recovery delle informazioni, tool di backup management);
- Elevata flessibilità nella gestione del sistema e dei dati, con la possibilità di eseguire la maggior parte delle operazioni di routine senza interruzione del servizio e dell'accesso ai dati (copie di backup e riorganizzazioni online, ristrutturazione degli archivi,

modifiche ai parametri critici del sistema, possibilità, in ambiente cluster, di applicare patch o migrare a nuovi rilasci senza interrompere l'operatività dell'intero sistema, ecc.);

- Gestione efficiente del locking (preferibilmente implementata in modo coerente con gli standard ISO/ANSI) per applicazioni ad alto throughput e ad alta concorrenza di accessi agli stessi dati, con risoluzione automatica delle situazioni di deadlock e la possibilità di escludere il ricorso alla lock escalation;
- Possibilità di compiere attività di auditing degli accessi ad ogni livello dell'RDBMS, dall'intero database al singolo oggetto (tabella, colonna) per singolo utente;
- Massima integrabilità con le più diffuse tecnologie RDBMS;
- Supporto di sistemi ed architetture in alta affidabilità;
- Compatibilità con i sistemi di "strong authentication", di gestione di certificati digitali e firma digitale;
- Rispetto degli standard, procedure e requisiti di sicurezza e qualità, con particolare riguardo alle specifiche dettate dal framework OWASP - Open Web Application Security Project;
- I dati operazionali provenienti dai sistemi e dalle applicazioni di interesse saranno archiviati in una base storica comune in cui devono essere custoditi per un periodo di tempo sufficiente a consentire elaborazioni ed analisi statistiche;
- Fonti esterne: la piattaforma deve consentire l'inserimento dei dati da sottoporre ad analisi, sia utilizzando la propria base dati storica, sia tramite importazione diretta di fogli Excel, file di testo, pagine web, dati via ODBC;
- La componente di intelligence e analisi predittiva ha lo scopo di guidare l'Operatore alla comprensione degli eventi, all'identificazione più efficace di potenziali rischi, delle cause e delle loro relazioni, attraverso l'applicazione di una vasta gamma di metodologie statistiche (es. Frequency Analysis and Profiling, Logistical Regression, Outlier analysis, Text mining / Sentiment Analysis, Decision trees, Conditional / Random Forest, Forest Garrotte). Tale componente dovrà inoltre consentire all'Operatore di compiere analisi esplorative dei dati, attraverso grafici con visualizzazione interattiva, reti sociali, indicatori di analisi, modelli profilazione, modelli predittivi. L'interfaccia dovrà essere comprensibile da utenti analitici senza competenze di data warehousing o linguaggi di gestione di basi dati;
- Le segnalazioni di rischio dovranno tener conto di fattori di più tipi e diversa provenienza, attribuibili alla singola entità, al suo pregresso storico, alle entità ad esso correlate, in relazione a modelli di riconoscimento e scenari di comportamento predefiniti capaci di generare segnalazioni in maniera predittiva. La soluzione dovrà generare automaticamente un "codice" di rischio e il relativo punteggio (risk scoring), evidenziando le "regole" che lo hanno fatto generare per rendere immediata la sua comprensione. Gli eventi di rischio saranno anch'essi registrati nel repository condiviso e centralizzato del sistema ed associati allo scenario in cui si sono verificati;
- Sulla base del rischio il sistema proporrà i casi agli investigatori, aggregando ad essi tutta la rete di relazioni e i dati (eventi) originali che hanno dato origine al caso;
- Sarà possibile effettuare l'analisi della rete delle associazioni e delle sequenze (c.d. tecnica delle social network analysis) con la possibilità di gestire una gerarchia tassonomica (categorie, sottocategorie, ecc), di utilizzare variabili temporali per identificare le sequenze e fornire algoritmi di Web Path Analysis. Le relazioni dovranno essere conservate nell'archivio unico del sistema ed aggiornarsi al crescere dei nuovi dati in ingresso.

4.2.2.6.4 Componente OSINT

La componente dovrà prevedere la possibilità di raccogliere contenuti (pagine e siti web tradizionali o web 2.0, quali forum, wiki o blog di pubblico accesso) attraverso dei robot (c.d. web crawler) che saranno programmati attraverso una specifica console di amministrazione del modulo con le coordinate delle pagine da visitare.

I contenuti così raccolti saranno forniti in input al modulo di intelligence, il quale li analizzerà e ne estrarrà automaticamente, attraverso un'analisi semantica, le entità secondo le tassonomie e le categorie di interesse in esso definite.

L'analisi investigativa (OSINT) verrà condotta centralmente dal modulo di intelligence e le informazioni del mondo "open" verranno unite a quelle di altra tipologia con l'obiettivo di individuare automaticamente eventuali collegamenti tra entità.

4.2.2.6.5 Modulo di front-end

Il modulo costituirà l'ambiente di gestione alert, indagine e case management integrato in un'unica console, profilabile per i diversi ruoli e tipologie di utenti e consentirà:

- Case management
- un'interfaccia per la visualizzazione delle schede dei casi di rischio che forniscono informazioni aggregate dei dati contenuti e possibilità di drill down sul dettaglio delle schede;
- la possibilità di assegnare casi in base alla tipologia a diversi utenti analisti;
- di gestire degli alert in caso di matching positivi derivanti dal modulo investigativo-predittivo con la possibilità di assegnarli ad utenti/gruppo di utenti per la relativa gestione e tracciare lo stato e le azioni intraprese;
- la possibilità per l'utente di effettuare analisi storiche sui dati e sulle schede gestite;
- di fornire dati aggregati sui trend di rilevamento derivanti dal modulo di analisi investigativa-predittiva;
- di disporre di una interfaccia Web per la visualizzazione dei risultati delle analisi ed della reportistica prodotta dal sistema;
- agli utenti di effettuare il drill down sugli indicatori del cruscotto per visualizzare maggiori dettagli. Il drill down dovrà poter essere eseguito lungo diverse dimensioni definite dall'utente (es. temporale, geografica, per fonte, ecc.).
- di esportare un dossier contenente report, struttura della rete di collegamenti relativa ad un caso e i relativi documenti ad essa collegati, nei comuni formati per l'office automation (pdf, excel, ecc.).

Nel seguito sono sintetizzati i requisiti funzionali e di massima del modulo di intelligence.

Requisito	Descrizione requisito
Soluzione applicativa	Integrazione con interfacce native con repository esterni, volte a identificare corrispondenze (esatte e approssimate sulla base di algoritmi di assonanza e traslitterazione) tra i dati di diverse banche dati anagrafiche, black list, ecc.
Funzionalità esistenti	La soluzione applicativa disporrà di indicatori già implementati e funzionanti rappresentativi dell'operatività portuale, sicurezza, risk assessment doganale, implementati e funzionanti (se opportunamente alimentati con le informazioni necessarie) .
Datamart	La soluzione disporrà di una base dati interna volta ad acquisire attraverso un processo di alimentazione automatica da repository interni (es. Anagrafe generale, Anagrafe settoriale, Sistemi Gestionali/Legacy, ecc.) ed esterni (AIDA, PLN, ecc.), storicizzare e utilizzare tutte le informazioni necessarie alle funzionalità descritte: • caratteristiche delle transazioni eseguite; • anagrafe dei soggetti e delle entità; • elementi caratterizzanti il profilo di rischio della merce (es. storico operatività); • elementi caratterizzanti il profilo di rischio di aree geografiche/territori (es. indice di criminalità).

Gestione regole indicatori	La soluzione deve prevedere la possibilità di definire nuovi indicatori di rischio basati su qualsiasi elemento del patrimonio informativo disponibile. Le regole alla base degli indicatori saranno gestibili mediante uno strumento user friendly. Le attività di deployment degli indicatori in ambiente di produzione saranno gestibili direttamente dagli utenti (analisti, personale tecnico).
Rappresentazione sintetica su più livelli	La soluzione include uno strumento integrato dedicato al reporting. Il sistema di reporting integrato deve consentire la rappresentazione sintetica degli indicatori elaborati a livello di fenomeno e di tipologia di Indicatore. Il modulo di Reporting dovrà essere in grado di comporre documenti e cruscotti con qualsiasi informazione presente nel sistema o importata attraverso documenti esterni al sistema, rendendoli disponibili, secondo diversi formati, a tutti i livelli di utenza, in funzione degli specifici livelli di autorizzazione, creare, modificare, eliminare, visualizzare gli oggetti creati, salvandoli su cartelle pubbliche o personali.
Black/white list	Le funzionalità di watch list consentiranno di gestire in modo sistematico l'attivazione di alert a fronte della ricorrenza di specifici nominativi (black list) ovvero di gestire in modo sistematico l'esclusione degli alert a fronte di corrispondenze di specifici nominativi all'interno di ulteriori liste (white list).
Predisposizione accessibilità fonti interne ed esterne	La soluzione dovrà prevedere l'accessibilità anche a eventuali fonti esterne.
Controllo simultaneo liste	Saranno previste funzionalità di watch list per: • eseguire controlli sul grado di assonanza fonetica e letterale delle informazioni anagrafiche che riguardano i soggetti censiti (es. controlli su nome, cognome, indirizzo di residenza, paese di nascita, ecc. del titolare dell'operazione; • verificare l'assonanza fonetica tenendo anche in considerazione le differenti modalità di scrittura delle lingue non occidentali (es. arabo, cinese, giapponese) e i conseguenti impatti sulle possibili traduzioni dei dati anagrafici.
Livelli e servizi: architettura	La soluzione sarà realizzata su un'architettura software a livelli, in cui ogni componente offre un servizio del proprio livello di appartenenza: • Presentation Layer: livello privo di componenti che sviluppano logiche di business e dedicato esclusivamente al colloquio diretto con l'utenza; • Application Layer; • Deployment Layer: livello di pubblicazione dei servizi applicativi disponibili; • Business Layer: livello detentore delle logiche di business ovvero delle regole di business applicate ai dati del contesto; le componenti di questo livello non dovranno accedere direttamente ai dati (che verranno richiesti al Data Layer) e dovranno poter essere installate indipendentemente dalle componenti di deployment; • Data Layer: le componenti di questo livello presentano solo funzionalità di accesso ai dati.
Standard tecnologici	La soluzione prevederà la modalità Web-Oriented per lo strato di

	presentation (no Rich-Client) e conforme allo standard J2EE per la parte server-side.
Multicanalità e riusabilità	La soluzione sarà conforme al principio della multicanalità, a garanzia della rapida distribuzione dei servizi a tutti i canali di accesso. Le applicazioni saranno sviluppate in un'ottica di completa riusabilità delle singole componenti, mediante disaccoppiamento dello strato di presentation da quello di business.
Scalabilità della piattaforma	La soluzione dovrà garantire la scalabilità della piattaforma, in termini di capacità del sistema e di mantenere il tempo di risposta al crescere dell'utenza che lavora simultaneamente.
Affidabilità della piattaforma	La soluzione dovrà garantire l'alta affidabilità di tutte le componenti architetturali della piattaforma, in modo da minimizzare gli impatti legati al fermo di uno o più componenti.
Integrazione con IAM	Sarà prevista l'integrazione della soluzione con il sistema di IAM - Identity & Access Management.
Strong authentication	La soluzione sarà compatibile con i sistemi di strong authentication, di gestione di certificati digitali e firma digitale.
Realizzazione software: standard di sicurezza e qualità	La soluzione sarà conforme agli standard, procedure e requisiti di sicurezza e qualità, con particolare riguardo alle specifiche dettate dal framework OWASP - Open Web Application Security Project.

4.2.2.7 Modulo Orchestrator

Per orchestratore si intende il modulo che fornisce i servizi di supporto all'Architettura SOA del progetto e rappresenta l'interfaccia unica attraverso cui transita ogni richiesta di comunicazione tra i servizi (siano essi di business, di integrazione, di dati) che devono interoperare.

Si basa sul paradigma ESB e rappresenta l'infrastruttura software per facilitare l'integrazione delle applicazioni. Implementa quindi un'architettura orientata ai servizi (SOA), perché scambia messaggi, esegue transazioni e svolge funzioni di pubblicazione e sottoscrizione tra applicazioni diverse e distribuite.

L'ESB si basa su sistemi disparati, interconnessi con tecnologie tipicamente eterogenee, e fornisce in maniera consistente servizi di sicurezza, messaggistica, routing intelligente e trasformazioni (oltre che interagire in modo stretto con il BPM) agendo come una dorsale attraverso la quale viaggiano servizi software e componenti applicativi.

Alcuni di questi servizi vengono forniti in maniera nativa dall'ESB, mentre altri vengono messi a disposizione da adapter e wrapper che si collegano al bus.

Di seguito sono riportati i principali requisiti funzionali di massima del modulo.

Requisito	Descrizione requisito
Gestione	Le funzionalità di orchestrazione dei servizi saranno realizzate poggiando su un Enterprise Service Bus che fungerà da interfaccia tra i molteplici sistemi ed apparati che compongono lo scenario al fine di ridurre la complessità dell'architettura. Sarà consentito in maniera agevole l'accesso ad applicazioni e servizi (anche legacy) al fine di integrare le informazioni provenienti dal mondo esterno e presentarle in modo semplice attraverso

	un'interfaccia consistente agli utenti finali.
Funzionalità	Il modulo deve consentire l'organizzazione ed il coordinamento dei servizi e dei flussi di informazione tra sistemi eterogenei attraverso una schedulazione dei servizi disponibili asserviti alla logica dei processi.
Sicurezza	Il modulo deve consentire la definizione degli opportuni criteri di sicurezza e propagare ai servizi gli stessi criteri di sicurezza definiti a livello generale.
Modelli e formati	Il modulo supporterà: • l'eterogeneità dei messaggi, intesa sia in termini di molteplicità di modelli (sincroni, asincroni, publish e subscribe), sia in termini di molteplicità di formati (SOAP, XML, ecc.); • diversi protocolli di trasporto per l'instradamento (FTP, HTTP, JMS, ecc.). • una gestione centralizzata e un accesso distribuito ai servizi.
QoS	Il modulo consentirà anche di garantire le caratteristiche di Quality of Service, quali persistenza del messaggio, garanzia di consegna, gestione dei fallimenti, ecc.

4.2.2.8 Modulo Gateway

È il modulo che consente lo scambio di informazioni con altre entità, siano essi sistemi per la gestione di apparecchiature di controllo che complessi sistemi informativi.

La finalità è la ricezione e/o la trasmissione di tutte le informazioni necessarie all'effettuazione dei controlli.

Attraverso il paradigma XML/Web Services saranno definiti i diversi messaggi necessari al ciclo di vita del sistema nel suo complesso.

Nel caso di interfacciamento con sistemi esterni di altre Pubbliche Amministrazioni, questi saranno raggiunti con l'utilizzo della Porta di Dominio.

La Porta di Dominio è un componente software che funge da adattatore fra due reti; essa consente a ciascuna Pubblica Amministrazione che espone i propri servizi ad altre Pubbliche Amministrazioni di comunicare facilmente con esse condividendo e adottando lo stesso linguaggio.

Ogni Ente è in grado di fungere sia da fornitore che da fruitore di un dato servizio.

Di seguito sono riportati i principali requisiti funzionali di massima del modulo.

Requisito	Descrizione requisito
Connettività	Il modulo deve consentire di scambiare flussi di informazioni con i principali apparati e sistemi di sicurezza presenti. Le modalità di scambio prevederanno, secondo i casi, almeno la implementazione dei seguenti meccanismi: • file di scambio; • web services; • interfacciamento attraverso Porte di Dominio; • protocolli di file transfer;

	• transazionalità.
Normalizzazione	Tutti le informazioni oggetto di scambio saranno analizzate, classificate e per ciascuna sarà predisposto un tracciato normalizzato nel formato XML/WSDL.
Continuità del servizio	Il sistema garantirà un opportuno sistema di accumulo dei messaggi in ingresso e/o in uscita a fronte di fermi temporanei dei sistemi alimentati/alimentanti. Il sistema, in automatico, garantirà lo smaltimento delle code a fronte della risoluzione del fermo.
Conservazione dei log	Dovrà essere mantenuto un log dei messaggi scambiati, con l'indicazione del sistema di input e/o output, della data ed ora e della tipologia del messaggio.
Backup dei messaggi	I messaggi oggetto di scambio saranno salvati su un database locale, e storicizzati per consentire eventuali ricerche a fronte di indagini e/o situazioni particolari. Il periodo di tempo durante il quale i messaggi saranno tenuti in linea, sarà dimensionato in base alle informazioni da trattare e concordato con la Committente.
Implementazione di nuovi messaggi	Il sistema dovrà consentire l'implementazione di nuovi messaggi in modo agevole e senza la necessità di modificare eventuale codice sorgente.

5. SOTTO-SISTEMA 2: INTEGRAZIONE LAND-SIDE (SILS)

In questo capitolo è analizzata la componente progettuale definita di Land-Side che, sostanzialmente, costituisce l'elemento di integrazione della sicurezza portuale con la Piattaforma Logistica Nazionale UIRNet.

Il Sotto-Sistema (di seguito SiLS) si presenta come formato da apparati hardware e soluzioni software che, nella propria complessità, trovano una compiuta organicità nel costituire una soluzione completa di tutte le problematiche connesse all'argomento, a vantaggio di tutti gli attori, a diverso titolo, coinvolti.

Di seguito, si forniscono gli elementi necessari alla comprensione del SiLS ed alla formulazione di soluzioni fattive da parte dei partecipanti alla gara.

Si intende, da subito, evidenziare che, sotto il profilo prettamente tecnico, saranno fornite indicazioni costituenti le caratteristiche e le prestazioni minime che dovranno possedere i diversi elementi (apparati hw e soluzioni sw) del SiLS.

L'intento è di stimolare proposte con contenuti innovativi in grado di rispecchiare lo stato dell'arte in materia, senza che le indicazioni fornite in questo documento possano costituire un limite rispetto alle disponibilità tecnologiche degli offerenti.

5.1 Descrizione sommaria del SiLS

La componente "integrazione della sicurezza portuale con la Piattaforma Logistica Nazionale (di seguito "PLN") " prevede la realizzazione di una soluzione hardware e software in grado di conseguire i seguenti obiettivi operativi:

- garantire la sicurezza dei trasportatori, degli automezzi, e dei beni trasportati, in arrivo ed in partenza dal porto di Gioia Tauro, da atti illeciti con particolare riferimento a quelli di tipo predatorio;
- estendere virtualmente l'area di controllo doganale a zone circostanti il porto, con specifica evidenza dell'area industriale, consentendo lo spostamento di container ancora non verificati senza che sia violato il contenitore del carico sino ad autorizzazione;
- creare un interscambio di informazioni tra l'ambito della PLN e quello delle Forze di Polizia oltre che degli Organismi dedicati al mantenimento di idonei livelli di sicurezza in riferimento al porto di Gioia Tauro, alla sua circostante area industriale ed anche al più ampio entroterra.

Agli stessi si affiancano, non secondariamente, elementi di coerenza della soluzione:

- con la PLN UIRNet in modo che sia consentita la completa integrazione tra i dati della componente e quelli di competenza della citata PLN;
- con protocolli aperti in modo che sia consentito l'accesso ai dati sia ad Organizzazioni dello Stato che a privati (trasportatori, società di spedizioni ed altro) ognuno esclusivamente secondo la propria competenza.

Il SiLS ha un doppio baricentro:

- in un apparato hardware e software associato all'automezzo, ed installato a bordo dello stesso, che svolge il compito di raccogliere una serie di dati e trasmetterli ad un centro di raccolta ed elaborazione dati;
- un centro di raccolta ed elaborazione dati, ove gli stessi sono immediatamente sottoposti ad una serie di elaborazioni software che provvedono a preparare le informazioni per le diverse classi di utenza che accederanno al SiLS.

I diversi fruitori del SiLS disporranno di accessi, sicuri e controllati, al centro di raccolta ed elaborazione dati mediante l'utilizzo di un browser web; saranno disponibili soluzioni applicative, dedicate alle esigenze delle differenti tipologie di utenza.

E' stata evidenziata la coerenza con la PLN UIRNet come obiettivo progettuale; si rammenta che UIRNet è "... *il soggetto attuatore unico del Ministero delle Infrastrutture e Trasporti per la realizzazione e gestione del sistema telematico di riferimento per la gestione della rete logistica nazionale finalizzato a permettere l'interconnessione dei nodi di interscambio modale* [...] *con l'obiettivo di migliorare efficienza e sicurezza nella logistica in Italia, così come definito dal D.M. n. 18T del 20 giugno 2005 e poi ripreso dalle Leggi n. 27 del 24 marzo 2012 all'art. 61bis (Legge "Cresci Italia") e n. 135 del 7 agosto 2012 all'art. 23 (Legge "Spending Review")* ..." (sito internet UIRNet.it).

Pertanto, l'obiettivo di conformità si inserisce in questo progetto al fine di evitare la realizzazione di un sistema isolato ma si inserisce nel percorso di sviluppo in corso in ambito nazionale introducendo, allo stesso tempo, l'assoluta innovazione costituita dagli aspetti di security.

Questi ultimi hanno caratteristiche non ancora sviluppate nell'ambito della PLN UIRNet, poiché il presente progetto prevede, sommariamente:

- l'invio di allarmi, automatici e su iniziativa del trasportatore, che possono essere raccolti e gestiti direttamente da Operatori di Sala e/o Centrale Operativa delle Forze dell'Ordine;
- la possibilità per pattuglie delle Forze dell'Ordine di controllare mezzi in movimento ed effettuare verifiche approfondite anche prima dell'eventuale decisione di fermare il veicolo;
- la possibilità di gestire il movimento di container fuori dall'area doganale mantenendo intatto il carico per le ispezioni da svolgere in un momento successivo;
- un forte raccordo tra Forze dell'Ordine ed autotrasportatori futuri sviluppi funzionali, anche se non esplicitamente previsti in questo progetto.

5.2 ARCHITETTURA LOGICA DEL SiLS

Il SiLS, sotto il profilo logico architetturale, conferma la visione della realizzazione di due pilastri fondamentali sui quali si concentrano le funzioni che lo stesso svolge: si tratta di una unità di bordo (di seguito "OBU", On Board Unit) ed il Centro di raccolta ed Elaborazione Dati (di seguito "CED").

In quest'ambito, si intende sottolineare che le complessità legate ai due elementi devono essere concentrate nella fase di produzione e, una volta a disposizione degli utenti, saranno prioritari gli aspetti di semplicità, nel senso che

- la OBU dovrà essere facilmente installabile e manutenibile; l'elevato numero di OBU che, potenzialmente, saranno in circolazione non dovrà creare un collo di bottiglia nel rapporto con centri di assistenza;
- il CED dovrà essere essenziale nella componentistica hardware al fine di non pregiudicare una futura, eventuale, ricollocazione presso altri siti – differenti da quello al momento indicato – senza pregiudizi per la fruibilità operativa.

5.2.1 On Board Unit

Come detto si tratta di uno dei due elementi di baricentro del SiLS ed è fisicamente costituito:

- da un'unità primaria che risponde alle norme ISO 7736 nelle misure singolo DIN ovvero, al massimo, doppio DIN; questa deve essere installata e sempre associata in maniera univoca ad un veicolo;
- da una seconda unità, collegata via cavo alla precedente, che costituisce il dispositivo che ospita una SIM card (ISO 7810:2003 ID-000) per il collegamento dati; questa è costruita con caratteristiche tipicamente rugged e collocata in una posizione non accessibile se non in una fase di installazione e manutenzione.

Inoltre, il conducente avrà a propria disposizione anche un tablet PC, che comunica con la PLN tramite SIM card, necessario alla realizzazione di una serie di comunicazioni che avvengono tramite interfacciamento web ovvero applicazioni dedicate.

Per questo ultimo dispositivo occorre considerare quanto di seguito.

Nella quasi totalità dei casi il conducente è un dipendente di un'azienda di spedizioni ovvero un imprenditore che svolge in proprio l'attività di autotrasportatore.

Tale distinzione è necessaria, perché la gestione delle informazioni potrebbe essere svolta:

- nel primo caso, pressoché interamente da un ufficio centrale con il conducente che esegue disposizioni ricevute ed origina, quasi esclusivamente, informazioni relative allo stato dell'esecuzione delle direttive impartite;
- nel secondo caso, il conducente potrebbe svolgere l'intero arco di attività gestionale delle informazioni, soprattutto relative all'inserimento dati, se non addirittura essere responsabile di altri conducenti in quanto propri dipendenti.

La differenza di ruolo influisce sulla modalità di interfacciamento tra conducente e SiLS nella fase di inserimento e consultazione dei dati soprattutto nell'ambito della gestione delle missioni di viaggio.

Nei casi sopra citati, sarà più agevole svolgere il lavoro su un dispositivo munito di schermo ampio e tastiera mentre al di fuori di tali ipotesi si può anche ipotizzare come sufficiente, da parte del conducente, l'uso di un tablet PC.

Pertanto, si ritiene necessario prevedere che a bordo del veicolo sarà presente, al minimo un tablet PC ma potrebbe essere anche utilizzato un tablet PC con tastiera od anche un PC portatile.

Quando si prende in considerazione una delle anzidette tipologie di apparato, occorre considerare che queste dovranno essere collegate con il SiLS, tramite una SIM card con un servizio di comunicazione dati.

Nel corso delle pagine che seguono il termine OBU indica le due unità nel proprio insieme, se non specificato in maniera differente (OBU unità primaria); da parte del lettore, l'accezione deve essere logica ancora prima che fisica.

I compiti svolti dal OBU consistono:

1	nel fornire connessioni bidirezionali con	apparati e dispositivi a disposizione del conducente
2		altri apparati installati a bordo
3		sistemi nativi di bordo
4		apparati prossimi ed esterni all'automezzo
5		il CED raggiunto su rete geografica
6	nel raccogliere dati provenienti dagli apparati al fine di	mantenerli in memoria per un tempo prestabilito
7		assistere le azioni di trasmissione e ricezione dei dati su rete geografica con funzioni di buffer e cache
8	nell'accogliere un firmware nel quale sono contenute informazioni di base relative al OBU stesso	
9	nell'offrire un interfacciamento semplificato per lo svolgimento di funzioni di base, per la rappresentazione di elementi di stato relativi al OBU ed alla sua alimentazione, per l'utilizzo automatico e semplificato in assenza di altri dispositivi di interfacciamento uomo/macchina.	

Seguendo l'ordine degli argomenti citati in tabella, si descrive compiutamente l'architettura logica della OBU.

5.2.1.1 Connessione con apparati e dispositivi a disposizione del conducente

Un primo dispositivo connesso alla OBU consiste in un telecomando portatile che consente l'invio semplice e rapido di un allarme per richiesta di intervento, funzionante anche se il conducente si trova all'esterno del veicolo.

Per esigenze logicamente simili, si prevede anche un'altra tipologia di dispositivo, consistente in un congegno per la segnalazione dello stato di uomo-a-terra, similmente a quelli già in uso in molte attività professionali come, ad esempio, il settore cantieristico.

I citati dispositivi saranno a disposizione del conducente che, solamente se lo riterrà necessario, sceglierà l'eventuale attivazione ed utilizzo secondo la esigenze che egli stesso ravviserà nel corso delle proprie attività.

Un'ulteriore connessione è stabilita con il tablet PC, attraverso un cavo dedicato che si connette alla OBU tramite una porta USB che avrà caratteristiche specifiche tali da consentire che la stessa sia unidirezionale, esclusivamente dalla OBU verso il tablet.

Si dirà più avanti della connessione della OBU con la centralina di bordo del veicolo; questi dati, a propria volta, saranno l'oggetto della trasmissione immediata via USB verso il tablet.

5.2.1.2 Connessione con altri apparati installati a bordo

Il primo dispositivo, assolutamente necessario, è il ricevitore del segnale di posizionamento trasmesso da costellazioni satellitari per determinare la posizione del veicolo, velocità e direzione.

Ad esso dovrà essere associato un secondo dispositivo (munito almeno di un odometro ed una bussola) per consentire la navigazione stimata.

La OBU dovrà essere in grado di ricevere il dato da differenti sistemi:

- GPS (Global Positioning System);

- GLONASS (GLObal NAvigation Satellite System);
- GALILEO (Galileo Positioning System).

Il ricevitore dovrà gestire il cd. anti-spoofing per la correzione degli eventuali errori indotti dai sistemi, qualora sussistano, per limitare la precisione d'uso nei sistemi civili.

Un secondo dispositivo consiste in una telecamera, installata a bordo, che riprende la strada di fronte al veicolo; la funzione della stessa è intuitiva, a vantaggio del conducente ma anche per offrire la possibilità di accedere ad informazioni utili da parte delle Forze dell'Ordine[1].

Si prevede una fruizione soprattutto post—evento ma deve essere prevista la possibilità di accedere da remoto anche a brevi sequenze che possano aiutare ad interpretare una situazione in caso di richiesta di ausilio giunta dal conducente.

La telecamera sarà munita di una propria memoria, preferibilmente una scheda rimovibile in formato SD e mini-SD, che potrà essere consultata con semplicità; in ogni caso, gli ultimi dieci minuti di registrazione sono invece memorizzati sulla OBU.

Un altro dispositivo consiste in un lettore di dispositivi a tecnologia RFID (Radio Frequency IDentification) che comunica con elementi (ad esempio, fascette e targhette) che possono essere applicate al carico trasportato.

Nel momento in cui il carico è spostato dalla propria sistemazione a bordo del veicolo ovvero il dispositivo è sottoposto a rottura e/o rimozione, sempre mentre si trova a bordo del veicolo, la OBU registra l'evento ed invia il dato al CED.

L'adozione di tale procedura consente lo spostamento di carichi dall'area doganale ad altre zone del retro porto, se non dell'entroterra, prima che siano compiute le necessarie procedure.

In questo modo può essere puntualmente tracciato lo spostamento del carico e controllato l'eventuale indebito accesso allo stesso, segnalato dalla rimozione delle fascette che costituiscono, di fatto, un sigillo applicato al contenitore del carico.

La soluzione da individuare può prevedere che la componente di ricezione della richiesta dal sistema di terra RSE (cd. Road Side Equipment) e di successiva trasmissione del codice univoco della OBU sia esterna all'unità stessa.

Un altro collegamento dovrà riguardare un dispositivo che svolge il compito di sensore inerziale tale da rilevare il movimento del veicolo.

[1] *In merito alla possibilità di effettuare le previste riprese da bordo veicolo, l'Autorità Garante della Privacy ha emesso un proprio provvedimento in data 8.4.2010 che prevede:*
"... 6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali
6.2.1. Consenso
Nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed Enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso (artt. 23 e 24 del Codice). Nel caso di impiego di strumenti di videosorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un'idonea alternativa nell'ambito dei requisiti equipollenti del consenso di cui all'art. 24, comma 1, del Codice.
6.2.2. Bilanciamento degli interessi
Tale alternativa può essere ravvisata nell'istituto del bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice). Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro. A tal fine, possono essere individuati i seguenti casi, in relazione ai quali, con le precisazioni di seguito previste, il trattamento può lecitamente avvenire pure in assenza del consenso. Il Garante invita tutti i titolari dei trattamenti di dati personali effettuati tramite sistemi di videosorveglianza ad attenersi alle prescrizioni indicate nel presente provvedimento.
Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:
• all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (art. 11, comma 2, del Codice);
• all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (art. 143, comma 1, lett. c), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
• all'applicazione delle pertinenti sanzioni amministrative o penali (artt. 161 e ss. del Codice) ..."
Quindi, a parte l'utilizzo esclusivamente personale del materiale registrato, circostanza consentita, ogni altro uso deve rispettare tali regole pena sia l'inutilizzabilità, sia sanzioni amministrative e penali.

L'attivazione di quest'ultimo dispositivo attiva il funzionamento della OBU anche scavalcando il tasto di accensione/spegnimento.

5.2.1.3 Connessione con sistemi nativi di bordo

Si prevede che la OBU si interfacci con la centralina di bordo di gestione del veicolo, laddove presente, registrando i principali dati relativi alla gestione dello stesso in termini di utilizzo mezzo e di status dello stesso.

La connessione dovrà essere realizzata tramite lo standard FMS (Fleet Systems Management Interface).

Esula dagli obiettivi del SiLS la realizzazione di sistemi di controllo che sono invece regolati da Regolamenti dell'Unione Europea (di rilevanza i Regolamenti CE n. 1266/2009 e n. 561/2006 e precedenti citati nell'ambito degli stessi) ed applicati con tachimetri digitali omologati che non sono, in alcun caso, sostituiti dalla OBU.

Si chiede, comunque, che sotto il profilo terminologico oltre che di calcolo di parametri richiesti come funzionalità della OBU, sia applicato il dizionario e le formule di calcolo già stabiliti dai citati Regolamenti.

Come già descritto, i dati raccolti nella centralina devono essere posti nella condizione di essere trasferibili nel minor tempo possibile al tablet PC esterno collegato via USB unidirezionale; si evidenzia che il tablet, tramite altra applicazione non inserita in questo Sotto-Sistema dovrà compiere elaborazioni con risultati in tempo reale in merito al comportamento del veicolo.

Per questo, non vi devono essere ritardi nella disponibilità e nel trasferimento di questi dati.

5.2.1.4 Connessione con apparati prossimi ed esterni all'automezzo

Si prevede che la OBU possa interconnettersi con rilevatori esterni installati, nella maggiore totalità dei casi, in varchi di accesso/uscita.

Per questo dovrà essere previsto il fatto che la OBU abbia un ricevitore RFID in grado di rispondere ad apparati a terra che interrogano il veicolo in merito ai dati identificativi che lo caratterizzano.

La OBU risponderà alla richiesta con un messaggio contenente i dati identificativi del veicolo e della OBU stessa.

Il ricevitore RFID può essere il medesimo che è utilizzato per il controllo del carico.

5.2.1.5 Raccolta dei dati provenienti da apparati e dispositivi

A bordo della OBU dovrà essere prevista l'installazione di un dispositivo di memorizzazione, (preferibilmente una unità a stato solido, "solid state drive"), in grado di svolgere una serie di compiti riassumibili come di seguito indicato:

- in linea di principio s'intende conservare una quantità di dati equivalente a non meno di 120 ore solari di dati raccolti dai dispositivi, anche se non ritrasmessi al CED; oltre il limite temporale sarà possibile la riscrittura dei dati più vecchi; è ritenuto preferibile un limite superiore rispetto a quello indicato;
- il dispositivo di memorizzazione servirà anche per le funzioni di bufferizzazione e caching a supporto della trasmissione dei dati;
- il dispositivo deve contenere gli ultimi dieci minuti di registrazione provenienti dalla telecamera.

5.2.1.6 Componente fisica di comunicazione

Deve essere prevista la distinzione fisica tra OBU unità primaria e componente di comunicazione che ospita la SIM dati; quest'ultima deve essere attiva sino al proprio scollegamento con l'alimentazione diretta del veicolo.

La rimozione della OBU unità primaria non comporta l'interruzione del funzionamento della componente di comunicazione che, comunque, invia al CED il posizionamento, con un messaggio di attenzione legato al fatto che è rimasta isolata dalla OBU.

Nel caso in cui vi sia anche la disconnessione dall'alimentazione del veicolo, la componente deve essere in grado di inviare un messaggio di attenzione al CED in cui comunica l'avvenuto scollegamento e il dato di posizionamento del veicolo.

Ovviamente, attesa la necessità, dovrà essere presente una alimentazione ed una memoria tampone che sostenga la fattibilità dell'effettuazione di quest'ultimo messaggio.

Per facilitare questa operazione, in memoria dovrà sempre essere conservato il rilevamento delle ultime cinque posizioni del veicolo, trasmesse dalla logica della OBU.

5.2.1.7 Caratteristiche costruttive

In senso generale, la OBU unità primaria non deve essere accessibile al proprio interno se non tramite operazioni condotte dal produttore; in qualche modalità (che dovrà essere specificata nel documento di offerta) non deve più essere possibile utilizzare una OBU unità primaria che è stata aperta e solo il produttore dovrà essere in grado di procedere alla chiusura.

Inoltre, le connessioni via cavo ai vari dispositivi sinora descritti devono essere attestate ad una docking e non direttamente alla OBU unità primaria; quest'ultima dovrà essere estraibile in modo che l'intervento di manutenzione possa contemplare una rapida sostituzione.

In casi speciali, potrebbero essere necessarie la rimozione della OBU e la successiva apertura della stessa per asportare il dispositivo di memorizzazione al fine di mantenere i dati conservati nella modalità originale; per questi motivi, il dispositivo di memorizzazione deve essere asportabile dal resto dell'elettronica della OBU.

La OBU dovrà essere conforme alle normative ed alle omologazioni europee in materia; il produttore dovrà presentare le certificazioni relative all'atto della consegna della prima OBU.

5.2.1.8 Firmware

Il firmware della OBU contiene informazioni inerenti l'apparato tra le quali un dato di identificazione univoca; le stesse sono inserite dal produttore e non possono essere modificate da altri.

La memoria ove sono inseriti i dati non deve essere riscrivibile in alcun modo, allorquando la stessa è alloggiata all'interno di una OBU.

Fa eccezione la possibilità di effettuare aggiornamenti del firmware, tramite una comunicazione dati gestita dal supervisore della PLN; la comunicazione con i contenuti di aggiornamento deve essere supportata dal riconoscimento del mittente (il SiLS) ed il destinatario (la OBU).

Nel corso di una qualsiasi comunicazione tra OBU e SiLS, i dati di riconoscimento univoco della OBU sono inviati al SiLS secondo una frequenza temporale predefinita; il SiLS, per proprio conto, controllerà la congruenza tra l'identificazione della OBU e gli altri dati che sta trasmettendo.

In questo senso, l'elemento di congruenza sempre verificato concerne l'accoppiamento tra OBU e veicolo.

5.2.1.9 Interfaccia utente

La OBU si interfaccia con l'utente esclusivamente tramite tasti e luci di stato.

Devono essere presenti:

- un tasto di accensione/spegnimento;
- uno di start/stop missione, da utilizzare quando il mezzo è in movimento per l'esecuzione di un'attività programmata;
- uno di avvio manutenzione, da premere prima dello spegnimento per la successiva attività di rimozione dell'unità per successivi interventi sulla stessa;
- ai tre tasti precedenti corrisponde una luce di stato;
- una ulteriore luce corrisponderà al momento dell'allontanamento di un carico cui è associato un segnalatore RFID; la luce potrebbe essere attiva per un tempo congruo per poi tornare allo stato di spegnimento;
- altre luci potrebbero essere attivate per guasti di dispositivi.

Riguardo l'interfaccia utente, si attende uno schema rappresentativo della parte frontale della OBU unità centrale in sede di offerta.

5.2.1.10 Comunicazioni

La OBU dovrà consentire comunicazioni mobili secondo gli standard 3G e 4G LTE; saranno utilizzate SIM card[2] che fanno parte della disponibilità di UIRNet, al fine di assicurare l'omogeneità del SiLS con la PLN.

5.2.2 Centro di raccolta ed elaborazione dati

Il CED è individuato dall'insieme dei software di sistema e applicativi necessari a svolgere le funzioni necessarie alle diverse classi di utenza per lo svolgimento dei primi compiti.

E' di interesse che l'insieme del software non sia in alcun modo vincolato ad alcuno degli apparati hardware.

Il SiLS deve essere in grado di operare in molte e differenti situazioni che potrebbero anche succedersi nel tempo, a puro titolo di esempio, dapprima in una struttura realizzata ad hoc ovvero in housing presso un fornitore di servizi e, in seguito, in un'altra situazione.

Il vincolo tra software ed hardware è costituito, esclusivamente, dai requisiti minimi che gli apparati devono possedere per consentire al software di svolgere i propri compiti e conservare i dati, corrispondendo ai parametri funzionali che saranno più avanti indicati.

---

[2] *In merito ai servizi di comunicazione, si riporta l'informazione seguente, da agenzia stampa del febbraio 2011:*
"... Telecom Italia ha siglato un accordo con UIRNet per la fornitura di servizi e prodotti di telefonia mobile. L'intesa tra la principale azienda italiana di telecomunicazioni e UIRNet, società costituita nel 2005 dai maggiori interporti italiani, si traduce in un investimento di circa 15 milioni di euro.
"La convenzione, che fa seguito all'aggiudicazione della relativa gara d'appalto, – si legge in una nota – ha una durata decennale e prevede da parte di Telecom Italia la fornitura in esclusiva, a UIRNet e alle sue società operative, di SIM e servizi di fonia, messaggistica, trasmissione dati a larga banda, localizzazione e caring dedicato. A questi servizi – prosegue il comunicato – potrà aggiungersi, in via opzionale, la dotazione di terminali mobili veicolari e personali, dei relativi sistemi di gestione centralizzata e di ulteriori servizi tecnologicamente avanzati".
"L'accordo, strategico per UIRNet, – spiega ancora la nota – consentirà di garantire il necessario flusso di informazioni da e verso le imprese di autotrasporto e gli operatori del settore rendendo operativa la piattaforma di gestione della rete logistica nazionale realizzata per conto del Ministero delle Infrastrutture e dei Trasporti. Attraverso l'implementazione di tale piattaforma, UIRNet punta a rendere più efficiente l'intero sistema grazie alla possibilità di tracciare, monitorare e gestire i flussi in tempo reale e di velocizzare le operazioni logistiche nei diversi nodi di interscambio" ..."

Lo spostamento da una situazione ad un'altra successiva deve essere condotta con meccanismi semplici che possono rispecchiarsi in un trasferimento piuttosto che in una serie di installazioni successive.

Nel corso dell'operazione di trasferimento è necessario che il servizio non subisca interruzioni e che non sia richiesta la configurazione di alcun parametro in elementi esterni quali OBU, software client ed altro.

5.2.2.1 Dati raccolti dal CED

Il SiLS persegue gli obiettivi provvedendo all'elaborazione dei dati che riceve da tutte le OBU attive sul territorio; si intende evidenziare che dalle OBU al CED la comunicazione è praticamente unidirezionale.

I dati che arrivano dalle OBU si identificano in:

- posizionamento del veicolo in navigazione GPS ovvero stimata;
- allarme-utente qualora attivato dal conducente;
- allarme-veicolo attivato automaticamente nel caso in cui un sensore passa la propria soglia limite;
- allarme-carico inviato se si verifica un imprevisto cambiamento di stato dei dispositivi di controllo dello stesso;
- stato-OBU in occasione di variazioni di stato quali accensione, spegnimento, spostamento dell'unità dalla propria collocazione, upload e download locale di dati.

Una seconda categoria di dati raccolti proviene dai software client utilizzati dagli utenti; per un'esatta comprensione di questo ambito, è necessario considerare preliminarmente una serie di elementi.

Il SiLS si integra compiutamente con la Piattaforma Logistica Nazionale UIRNet al punto da poterne essere considerato un subset estremamente specializzato, per lo svolgimento delle funzioni legate alla security.

Il SiLS ha una propria completezza che, in ogni caso, non comprende tutte le funzioni della PLN poiché non avrebbero senso, per gli aspetti di security, l'elaborazione e la memorizzazione di tutti i dati legati alla Piattaforma e, non secondariamente, deve essere massimizzato l'investimento pubblico nel conseguire gli obiettivi progettuali.

Lo schema seguente intende fornire una prima rappresentazione, non standard, del rapporto tra i vari elementi.

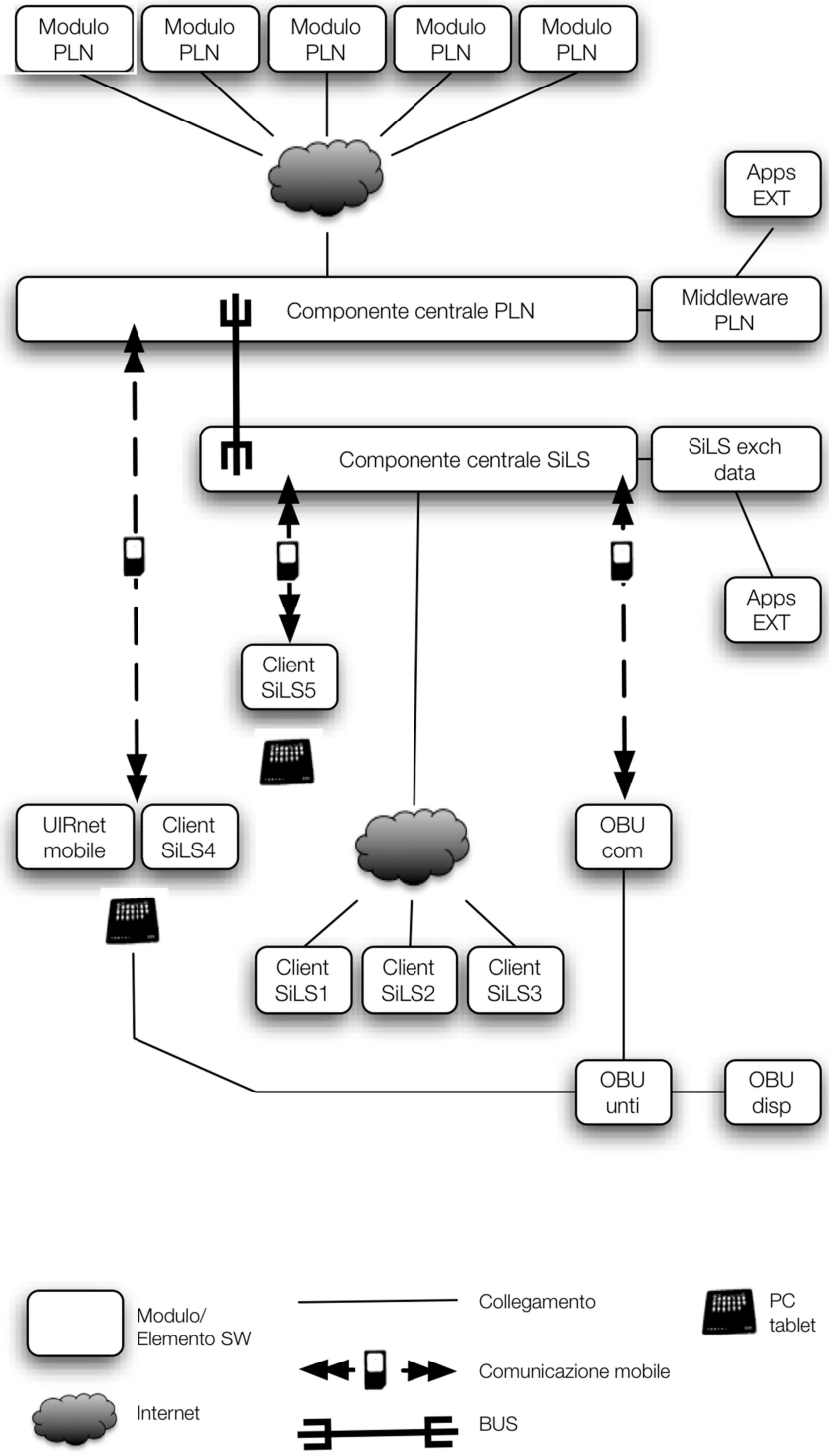

Figura 10 - Schema non standard dell'architettura logica SiLS

Il SiLS si interfaccia con gruppi omogenei di software client per i quali si renderanno necessarie differenti tipologie di interventi:

- applicazioni client della Piattaforma Logistica Nazionale (PLN), destinata agli attori dei settori dell'autotrasporto e degli interporti, per la quale sono necessari interventi di integrazione finalizzati all'interscambio di dati;

- applicazioni client, da sviluppare ex novo, dedicate ad utenti chiamati a gestire gli aspetti di sicurezza quali Forze dell'Ordine (per gli aspetti generali di sicurezza) e Autorità doganale (per quanto concerne carichi destinati a successivo controllo);
- applicazioni esterne che rilevano ovvero detengono informazioni utili ai fini del perseguimento degli obiettivi generali di security.

Per quanto concerne il primo gruppo di applicazioni, occorre considerare che sarà necessaria un'attività di integrazione, al fine di non sovraccaricare gli utenti con doppi inserimenti e non realizzare sovrapposizioni di software client.

La complessità sarà così trasferita a livello di automatismi, gestiti dal SiLS in collegamento con la componente centrale della PLN tramite un bus ed un layer applicativo dedicati al trasferimento dei dati inseriti in moduli PLN.

Il citato layer applicativo dovrà essere realizzato nell'ambito del progetto SiLS da parte del Fornitore.

Di seguito si evidenzia che:

- dalla PLN verso il SiLS, tramite componente centrale PLN e bus, sono trasmessi dati inerenti l'inserimento nella gestione anagrafica generale, delle informazioni riguardanti il veicolo, i conducenti, l'eventuale appartenenza a società di spedizioni;
- sempre dalla PLN verso il SiLS, tramite componente centrale PLN e bus, nel corso delle attività ordinarie di lavoro, sono trasmessi dati inerenti la missione del singolo veicolo e riguardanti il conducente, il carico, la partenza, il percorso e la destinazione, la tipologia merceologica trasportata, il mittente ed il destinatario del trasporto. In caso di modifiche di una missione programmata, è effettuata una nuova trasmissione dei dati che aggiornano i precedenti. Non sono inviati altri dati oltre quelli sopra indicati;
- i dati di cui al punto precedente sono un subset di quelli che, nell'ambito della PLN, realizzano il rapporto tra la PLN ed il modulo UIRNet mobile, quest'ultimo è a disposizione del conducente ed installato su un tablet che ha una connessione diretta, tramite SIM card, con la componente centrale PLN. Su UIRNet mobile il conducente riceve i dati della missione che deve compiere e per la quale deve corrispondere con propri inserimenti quali, ad esempio, lo start e lo stop della missione. Per quanto affermato, i dati di missione che partono da PLN arrivano contemporaneamente al SiLS tramite il bus e al tablet con UIRNet mobile tramite la connessione mobile stabilita con l'utilizzo della SIM card;
- quando sono, invece, trasmessi i dati da UIRNet mobile a PLN, gli stessi sono inviati tramite la connessione mobile del tablet; gli stessi raggiungono la componente centrale della PLN ed è quest'ultima a trasmettere i dati di UIRNet mobile al SiLS tramite il bus;
- la gestione del traffico dati descritta nei tre punti precedenti è svolta da un layer di connessione, sopra citato, che dovrà essere realizzato nell'ambito di questo progetto.

Lo schema seguente illustra, sempre facendo riferimento allo schema rappresentato nella figura 10, il percorso compiuto dai dati che compongono la programmazione di una missione, e dai dati risultanti da eventuali modifiche della stessa se già programmata, inserite nella PLN.

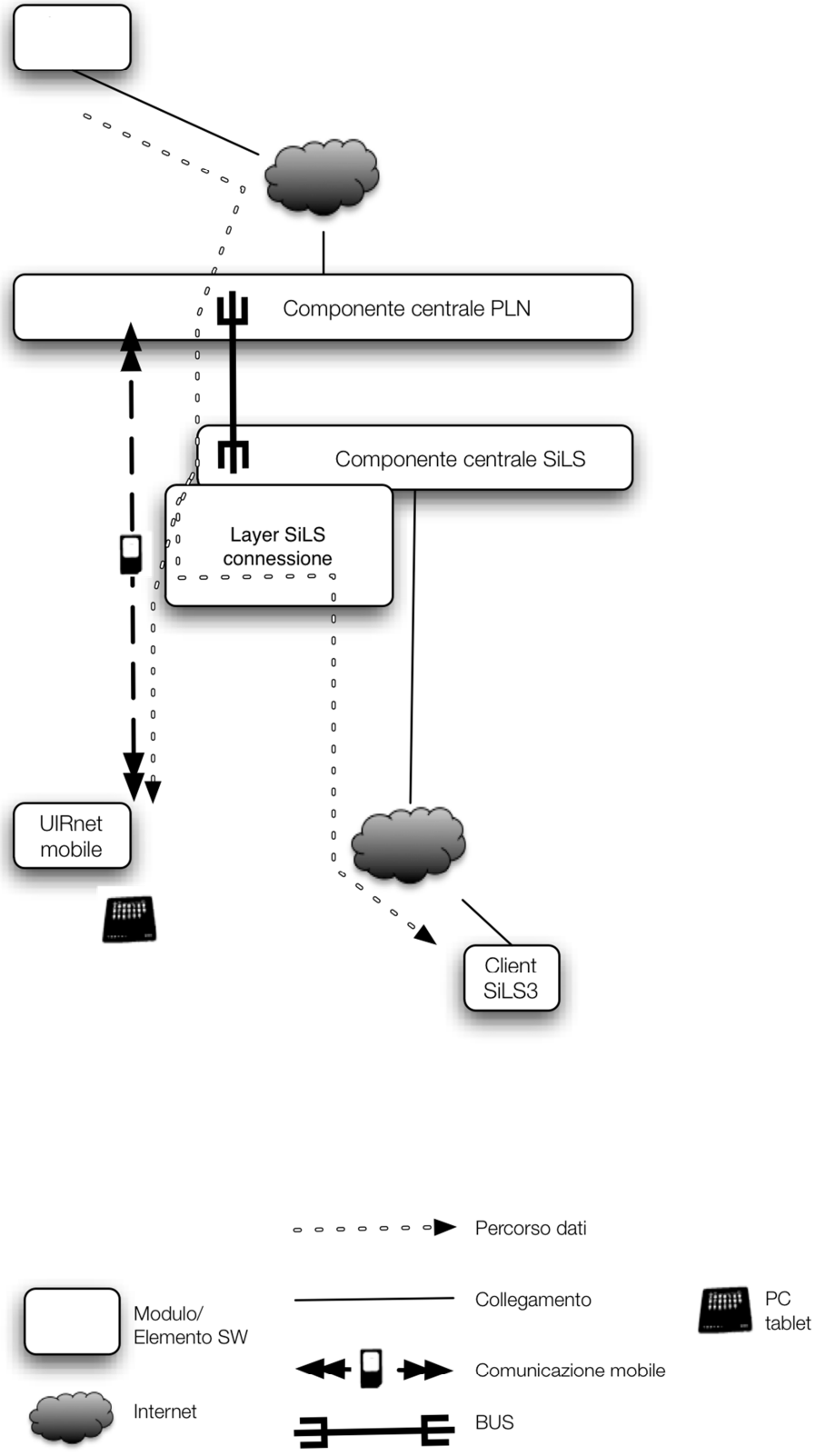

Figura 11 - Schema non standard del percorso dati inerente la programmazione di missione in ambito SiLS

Si anticipa che il dato di localizzazione del veicolo inviato dalla OBU al CED, è trasmesso in modalità push dal CED alla componente centrale della PLN, in modo che questa possa proseguire, a propria volta, le attività di elaborazione e rappresentazione all'utente sui moduli PLN.

Per quanto attiene al secondo gruppo, riguardante applicazioni client da realizzare ex novo, i dati da trasmettere al CED saranno originati:

- da un Primo client finalizzato alla registrazione ed amministrazione degli utenti che possono accedere al SiLS;
- da un Secondo client per la registrazione e la gestione anagrafica, di installazione e di manutenzione delle OBU;
- da un Terzo client di gestione ordinaria della sicurezza con moduli destinati;
- alle Forze dell'Ordine per tutte le attività di sicurezza;
- all'Autorità doganale per le sole attività di spostamento del carico da controllare;
- ad utenti centrali e di supervisione della PLN per la visione dei soli casi in cui è originato un allarme che sta richiedendo l'attenzione delle Forze dell'Ordine e dell'Autorità doganale;
- da un Quarto client destinato ai conducenti che attivano le funzioni di sicurezza anche se non è in corso una missione UIRNet;
- da un Quinto client, destinato alle attività di controllo condotte da appartenenti alle Forze di Polizia nel corso di controlli effettuati sul territorio.

Un terzo ed ultimo gruppo di dati inviati al CED concerne quelli ricavabili da altre applicazioni e consistenti in:

- rilevamenti da parte di lettori targhe; il dato è di interesse se è composto da posizione e direzione del dispositivo di lettura, targa veicolo, data e orario del rilevamento;
- posizionamenti di telecamere per ripresa; in questo caso è di interesse la collocazione e l'area di copertura della ripresa (verosimilmente rappresentata dall'orientamento della stessa espressa in gradi sessagesimali).

Questi dati saranno utili in quanto:

- la lettura targa accerta l'effettiva presenza del veicolo in un luogo ed in un momento definito; lo stesso risulterà nei risultati delle ricerche dati che hanno origine dall'inserimento della targa del veicolo per conoscere l'attività effettuata;
- il posizionamento e direzione della telecamera troverà una utile collocazione nella rappresentazione geografica del territorio; l'Operatore che usufruisce della visualizzazione potrà vedere in tempo reale che un veicolo è in prossimità di una ripresa e potrà vedere le immagini sul monitor dedicato a quella funzione.

La tabella seguente riassume quali dati sono trasmessi al CED.

<table>
<tr><td>Fonte dati</td><td colspan="3">Tipo</td></tr>
<tr><td rowspan="8">OBU</td><td rowspan="6">Diretto da OBU</td><td rowspan="2">Dati navigazione</td><td>GPS</td></tr>
<tr><td>Stimata</td></tr>
<tr><td>Stato missione</td><td>In corso/Stop</td></tr>
<tr><td rowspan="4">Stato apparato</td><td>Accensione/Spegnimento</td></tr>
<tr><td>Upload/Download locale di dati</td></tr>
<tr><td>Collegamento a dispositivo</td></tr>
<tr><td>Scollegamento unità da Tx/Rx</td></tr>
<tr><td rowspan="2">Da dispositivi tramite OBU</td><td rowspan="2">Allarmi</td><td>Da conducente</td></tr>
<tr><td>Da veicolo</td></tr>
</table>

			Da carico
APPLICAZIONI CLIENT	PLN	Gestione anagrafica	Veicolo
			Conducente
			Azienda
		Programmazione e modifica di Missione	Veicolo
			Conducente
			Azienda
			Percorso
			Inizio (Luogo, Data, Ora)
			Fine (Luogo, Data, Ora)
	UIRNet mobile	Missione	Inizio/Fine
	Primo client	Gestione anagrafica	Utenti
			Permissions
	Secondo client	Gestione OBU	Registrazione
			Matricole/Versione
			Installazione
			Manutenzione
	Terzo client	Gestione Forze di Polizia	Attività di sicurezza
		Gestione Dogane	Carichi in regime doganale
		Supervisor PLN	Allarmi in corso di gestione
	Quarto client	Trasferimenti	Veicolo
			Conducente
			Percorso
			Inizio (Luogo, Data, Ora)
			Fine (Luogo, Data, Ora)
	Quinto client	Controllo	Data, Ora, Luogo del controllo
			Veicolo, Conducente, Azienda
			Esito in termini sintetici
SISTEMI ESTERNI	Sistemi lettura targhe	Estremi della lettura in formato testo	
	Telecamere	Posizionamento	Collocazione
			Copertura ripresa

5.2.3 Elaborazione dati

In questo paragrafo è approfondito il lavoro svolto dal CED in termini di elaborazione ed i cui risultati sono disponibili per le esigenze dell'utenza.

Gli obiettivi che l'attività di elaborazione deve conseguire sono di seguito descritti.

5.2.3.1 Gestione degli utenti del SiLS

L'amministrazione del SiLS è demandata alle stesse figure che si occupano della medesima attività in ambito di PLN, provvedendo, in quell'ambito, al caricamento dei dati ed alla successiva profilazione degli utenti.

Per quanto riguarda gli utenti del SiLS dovrà essere prevista una gestione a sé stante in quanto alcuni di essi, ad esempio gli appartenenti alle Forze dell'Ordine ed alle Autorità statali di controllo, devono avere una trattazione separata, e ben protetta, del proprio dato anagrafico.

Dovranno essere previsti gruppi di utenza che si associno immediatamente all'accesso alle applicazioni client.

Per quanto riguarda gli appartenenti alle Forze di Polizia ed alle Autorità statali di controllo dovrà essere previsto un account riservato ad ogni responsabile di singola unità organizzativa che potrà solo visualizzare, tramite il proprio accesso, quali persone della propria unità sono inserite nell'anagrafica del SiLS.

In tal modo sarà possibile, per quel Responsabile, rivolgersi all'Amministratore di SiLS al fine di disporre correzioni/integrazioni rispetto ai dati inseriti.

Sono preferiti meccanismi di protezione della comunicazione (anche con rilascio di certificato al momento della connessione) al Primo client e registrazione su un log dedicato di tutte le operazioni compiute in termini di registrazione, modifica, accesso.

Allo stesso modo dovrà essere registrato su log il dato riguardante l'identificazione del client per quelli che sono i parametri identificabili (indirizzo IP, sistema operativo, browser, ecc.).

Il SiLS dovrà elaborare ed evidenziare, in una componente del Primo client, eventuali anomalie in merito ai dati raccolti dalle attività svolte dagli utenti anche in relazione ai dati relativi alla postazione ed al collegamento utilizzati.

5.2.3.2 Gestione dei dati relativi alle OBU

I dati riguardanti la gestione degli apparati di bordo sono gestiti in ambito di Secondo client, utilizzato dai diversi soggetti che sono coinvolti dalle operazioni che riguardano:

- la fornitura degli apparati, per cui il fornitore degli stessi inserisce i dati relativi alla produzione ed alla spedizione ad installatori e manutentori; allo stesso modo gestisce il rientro di apparati dalle aziende che ha fornito. La propria visibilità è relativa esclusivamente ai luoghi di fornitura degli apparati ed alle aziende autorizzate alla installazione e manutenzione ed al censimento delle OBU rubate e/o distrutte;
- l'installazione e la manutenzione, per cui l'azienda, partendo dai dati inseriti dal fornitore, immette i dati relativi alla OBU che installa e/o manutiene; relativamente al cliente egli potrà solo inserire la targa del veicolo su cui si compie l'attività. Sarà il SiLS a rappresentare i dati relativi alla proprietà del veicolo in quanto verifica la presenza nell'anagrafe del veicolo. Il gestore della installazione/manutenzione potrà consultare solo i dati relativi alle OBU in carico presso di sé e quanto relativo alle operazioni che ha compiuto nel tempo;
- la gestione dei dati relativi agli apparati oggetto di furto e/o distruzione che potrà essere effettuata da un installatore/manutentore, anche se non si tratta di un apparato che non è stato mai trattato presso quella azienda;
- la consultazione completa della situazione e della storia dettagliata di ogni OBU che può essere condotta dagli utenti appartenenti alle Forze di Polizia e dalla supervisione della PLN. Il SiLS deve anche elaborare, per questi utenti, una serie di elenchi che comprendono lo sforamento da medie logiche riguardanti le attività di manutenzione, furto, distruzione. Le elaborazioni che si riferiscono a quest'ultimo ambito dovranno

essere accessibili anche dal Terzo client sempre da parte degli utenti appartenenti alle Forze di Polizia.

5.2.3.3 Gestione di una missione o di un trasferimento di un veicolo senza carico

I due casi sono originati in maniera differente.

Le missioni hanno origine dalla PLN mentre gli altri trasferimenti, che non costituiscono missione, possono essere originati dal Quarto client creato nell'ambito del SiLS.

Il SiLS deve essere in grado di associare automaticamente i dati che provengono dalla PLN e quelli che giungono dalle OBU in termini di posizionamento.

Nel caso in cui vi sia uno spostamento del veicolo al di fuori di una missione od anche di un trasferimento, il SiLS provvederà comunque alla elaborazione dei dati ricevuti aprendo egli stesso una missione identificata, ad esempio, con data/ora che sarà, ovviamente, associata al veicolo.

5.2.3.4 Peculiarità della gestione dei carichi spostati dall'area doganale prima dei controlli

La visibilità degli Operatori delle Autorità statali di controllo è corrispondente esclusivamente ai casi di veicoli con il carico spostato dall'area doganale prima dei controlli.

Per questa categoria di utenti, tutte le tipologie di statistiche e le tipologie di dati rappresentati saranno relativi esclusivamente a questo ambito; anche la rappresentazione cartografica sarà riferita alle aree autorizzate ad accogliere i carichi da controllare.

Il SiLS elaborerà i dati che riceve dalla OBU e dai dispositivi di bordo ad essa collegati con i seguenti criteri:

- il distacco del carico dal veicolo: segnalato dai dispositivi RFID segnalerà uno stato di attenzione; l'Operatore verificherà che l'attività è avvenuta nel luogo programmato;
- rottura del dispositivo RFID mentre è ancora nell'ambito di ricezione del veicolo: per cui sarà inviato un allarme e l'Operatore valuterà se è necessario un intervento immediato;
- uscita del veicolo con il carico non solo da un percorso ma anche da un'area di territorio che è stata definita e preimpostata nel SiLS come quella destinata ad ospitare i carichi; anche in questo caso il SiLS provvederà a generare un allarme.

5.2.3.5 Gestione dei dati operativi relativi all'allarme

Si considerano dati operativi quelli gestiti primariamente in ambito di Terzo client nel quale sono rappresentati:

- le missioni e i trasferimenti fuori missione in corso;
- gli allarmi originati da conducente, dal veicolo, dal carico;
- gli allarmi originati dal SiLS.

La terza tipologia rappresenta il risultato delle elaborazioni che compie il SiLS basandosi sul dato di posizionamento e sul suo rapporto con parametri pre-impostati.

Questi ultimi possono riferirsi ad una variazione non attesa dal percorso programmato, ad una sosta non corrispondente alla segnalazione di "stop missione" da inviare tramite l'interfaccia della OBU, ad un ritardo eccessivo nella tabella di marcia calcolata al momento dell'inserimento di una nuova missione o trasferimento senza il carico.

Difatti, l'insieme dei dati provenienti dal totale delle OBU può anche essere utilizzato per analizzare, in un tratto di strada, la velocità media dei veicoli che la percorrono e, in questo modo, il SiLS può calcolare il ritardo da tollerare rispetto alle missioni sotto gestione di sicurezza.

E' fondamentale che il SiLS compia anche una serie di elaborazioni, rispetto agli allarmi che riceve e/o calcola in proprio, per fornire all'Operatore una rappresentazione contestualizzata delle segnalazioni degne di attenzione.

Si pensi al caso di più allarmi generati da conducenti in un'area molto ristretta: è ipotizzabile che gli stessi possano essere testimoni di un evento che sta coinvolgendo uno solo di loro e gli altri attivino il dispositivo perché testimoni di ciò che sta accadendo.

Chiaramente, non deve essere creata confusione nella rappresentazione che, evidentemente, riguarda un evento di interesse in una determinata area e l'Operatore deve essere coadiuvato nel comprendere l'area di riferimento ancora prima che la lista dei veicoli coinvolti.

Altro caso potrebbe riguardare la variazione dal percorso di un numero eccessivo e consecutivo, sotto il profilo temporale, di veicoli.

In quel caso si può supporre che si tratti di una deviazione disposta per motivi di viabilità per cui deve essere comunque gestita l'attenzione dell'Operatore, ma con il giusto grado di intensità dell'allarme.

Il citato concetto di intensità è un elemento che può essere gestito come elaborazione con l'utilizzo, in fase di rappresentazione, di livelli di allarme in modo che l'Operatore possa essere aiutato nella valutazione di ciò che sta accadendo ed organizzare l'intervento nel migliore modo possibile.

E' atteso che in ambito di elaborazione dell'offerta di riferimento, sia proposta una tabella di rappresentazione delle diverse tipologie di casi che si ritiene possano verificarsi, con l'ipotesi dei contestuali livelli di allarme che non dovranno essere superiori a tre.

5.2.3.6 Gestione dell'allarme ricevuto

L'Operatore dovrà notificare al SiLS il fatto di aver preso in carico un allarme; potrà inserire una nota a testo libero ovvero selezionare una descrizione predefinita su una serie di testi pre-costituiti.

Ovviamente, lo stesso proseguirà la propria attività di lavoro presso la propria postazione di gestione delle risorse operative delle Forze di Polizia.

Una seconda attività richiesta all'Operatore consiste nell'inserimento della verifica dell'allarme ricevuto; difatti, saranno possibili falsi allarmi, errori ed altri casi diversi da azioni illecite; allo stesso modo, sarà necessario distinguere se si tratti di allarmi lanciati non per esigenze di sicurezza ma di safety.

Dovrà essere redatta una lista di scelte tra le quali l'Operatore selezionerà uno dei casi previsti anche aggiungendo il giorno e l'ora di intervento sul posto.

La lista degli allarmi in gestione resterà aperta all'attenzione dell'Operatore sino al momento in cui sarà fatto anche l'inserimento della verifica; solo a questo punto, la gestione dell'allarme sarà conclusa.

La gestione delle liste descritte in questo paragrafo sarà a cura del supervisore della PLN sempre nell'ambito, come in altri casi di configurazione generale, del Primo client.

5.2.3.7 Rappresentazione spaziale dei dati operativi

Come detto, il Terzo client è utilizzato per le attività operative dalle Forze dell'Ordine e dalle Autorità statali di controllo, con particolare riferimento a quella doganale interessata al movimento di merci non ancora sottoposte a controllo.

L'interfacciamento dati principale sarà costituito da una pagina web nella quale saranno presenti dati testuali ma anche un frame contenente la rappresentazione geografica di porzioni del territorio.

In conformità con quanto già esistente nella PLN, la tecnologia di riferimento sarà quella di Tele Atlas; il Fornitore si impegna a realizzare uno sviluppo che sia compatibile, anche sotto il profilo grafico e della nomenclatura, con quello della PLN.

In ambito di rappresentazione geografica, dovranno essere riprodotti:

- il posizionamento del veicolo in missione o in trasferimento; dovrà essere distinta la tipologia se veicolo in missione, in trasferimento, se sta effettuando un trasferimento di carico fuori dell'area doganale prima del controllo, se si tratta di un veicolo da seguire con particolare riferimento in quanto segnalato dalle statistiche;
- il posizionamento di un allarme e la tipologia dello stesso (allarme veicolo, conducente, carico, OBU);
- poligoni che rappresentino il dato statistico di pericolosità e densità che è stato sopra descritto.

La selezione sulla componente geografica di uno degli elementi di cui alla lista precedente dovrà comportare la contestuale rappresentazione testuale delle informazioni di riferimento.

5.2.3.8 Gestione dei dati anagrafici e descrittivi; ricerche

Tutti i dati raccolti in termini di anagrafe veicoli, apparati, dispositivi, soggetti, missioni, luoghi e tempi dovranno essere posti in relazione tra loro in modo che i collegamenti possano essere utilizzati nel corso delle attività di gestione operativa.

Pertanto, il SiLS dovrà essere in grado di gestire tali collegamenti e rappresentare quanto disponibile in modalità di navigazione ipertestuale; qualora nel SiLS sia presente una informazione riguardante un termine, lo stesso dovrà essere evidenziato come collegamento ipertestuale.

Oltre a tale modalità, dovrà essere possibile effettuare ricerche che diano come risultato elenchi di dati che vedono come chiave principale di classificazione l'elemento ricercato; nell'ambito dei dati raccolti, ogni elemento può essere chiave di classificazione ed oggetto di ricerca.

5.2.3.9 Gestione dei dati operativi di approfondimento

Per conseguire la migliore rappresentazione possibile della situazione operativa e per agevolare il lavoro degli operatori, dovranno essere previste una serie di funzioni di supporto che consistono in quello che di seguito è elencato:

- soglia generale di variazione del percorso; dovrà essere realizzata una funzione che consenta l'inserimento in metri lineari dello spazio di allontanamento dal percorso prestabilito. L'eventuale allontanamento del veicolo dal percorso programmato, in termini di superamento fisico dello spazio impostato quale soglia di tolleranza, origina un allarme. La funzione di inserimento dello spazio di allontanamento dal percorso prestabilito è a disposizione del supervisore della PLN, e ha validità per l'intero SiLS con l'intento di uniformare la soglia di allarme. La stessa può essere inserita in una gestione che fa parte del Primo client;

- soglia generale di ritardo temporale nell'esecuzione della missione; dovrà essere realizzata una funzione, sempre a disposizione del supervisore della PLN in cui si inserisce un tempo medio di ritardo ammissibile espresso in percentuale ovvero in ore/minuti. Anche questa può essere inserita nella gestione descritta in precedenza. Con l'aumento dei dati memorizzati dal SiLS, lo stesso dovrà essere in grado di proporre, all'attenzione del supervisore, una serie di nuove percentuali e di nuovi tempi, elaborati sulla base dei dati effettivamente raccolti sul campo. Questi andranno a sostituire gli inserimenti da parte del supervisore nel momento in cui saranno logicamente attendibili. Tali soglie automatiche dovranno essere distinte per località in riferimento a percorsi, in modo da raffinare il confronto tra tempi reali e soglie di allarme;
- visualizzazione delle missioni; dovrà essere possibile visualizzare set di missioni, secondo logiche impostate da un elenco, in cui l'Operatore può compiere le proprie scelte. Si ritiene che sia di scarso interesse operativo la rappresentazione totale di tutte le missioni se riferite ad un territorio troppo ampio. Allo stesso modo, potrebbe essere invece d'interesse seguire un determinato set di veicoli in un'ampia porzione di territorio a causa della preesistente ipotesi di minaccia. La soluzione da adottare deve tenere presente questi due casi come estremi, ed agevolare una gestione operativamente logica dei dati da rappresentare.
- calcolo statistico; il SiLS dovrà elaborare statistiche utili a rappresentare alcuni elementi che possono essere di interesse per gli operatori.

In merito al calcolo statistico, sarà utile conoscere ed utilizzare la rappresentazione

- delle aree più pericolose in genere ovvero distinte per tipologia di origine di allarme (da veicolo, conducente, carico, OBU); la rappresentazione dovrà tenere conto di parametri temporali (fascia oraria, giorno, mese, stagionalità, ecc.) e di parametri spaziali quali strade e porzioni di territorio;
- delle tipologie effettive di allarme verificato (secondo la nomenclatura che distingue la lista di scelta descritta nel paragrafo precedente) sempre con i medesimi parametri temporali e spaziali sopra descritti;
- delle aree con maggiore densità di veicoli sempre con i medesimi parametri temporali e spaziali sopra descritti;
- dei veicoli maggiormente esposti in quanto appartenenti ad aziende che hanno subito il maggior numero di episodi che hanno generato allarmi;
- dei tempi medi di intervento dopo un allarme da parte delle Forze di Polizia rispetto ad una località.

5.2.3.10 Controlli sul territorio e rating

Il SiLS deve essere di supporto ai controlli che le Forze di Polizia effettuano su strada.

Per questo è prevista la realizzazione del Quinto client dal quale gli Operatori delle Forze di Polizia desumono informazioni in merito a conducenti, veicoli, aziende.

Effettuati i controlli di rito, gli Operatori inseriscono un dato esclusivamente relativo al risultato positivo/negativo dei controlli in riferimento a conducente/veicolo; per negativo si intende che non ci sono rilievi a carico delle entità.

In alcun modo è specificato altro elemento oltre ai termini positivo e negativo.

Il SiLS, che riceve il dato unitamente agli estremi temporali e geografici del controllo effettuato, elaborerà un rating espresso in decimi in merito al conducente ed all'azienda, basandosi su una serie di parametri quali il risultato positivo/negativo, il numero di controlli effettuati ed altro.

Il Fornitore proporrà gli indici sui quali baserà l'elaborazione dell'informazione del rating.

Il dato di rating sarà disponibile sul Primo, Terzo e Quinto client per essere riprodotto, contestualmente a qualsiasi rappresentazione e risultato di ricerca, agli utenti appartenenti alle Forze di Polizia e quelli delle Autorità statali di controllo.

5.2.3.11 Disponibilità dei dati per altre applicazioni.

Una delle elaborazioni più importanti realizzate dal CED, concerne la messa in disponibilità dei propri dati per applicazioni esterne.

Per questo, dovrà essere realizzata una struttura logica che ospiti i dati in un formato di interscambio che consenta ad altre applicazioni, autorizzate, la lettura e l'acquisizione dei contenuti.

Tra questi dati si evidenziano quelli di posizione ricevuti dalle OBU che dovranno essere utilizzati dalla PLN per le proprie peculiari attività; questi saranno trasmessi secondo logica push alla PLN con un intervallo temporale predeterminato.

Tutto ciò che concerne la configurazione di collegamenti esterni con autorizzazioni all'accesso da parte di applicazioni, modifiche al tracciato dati del formato di interscambio, assegnazione di eventuali logiche push con definizione dell'intervallo di trasferimento sarà gestito dall'amministratore del SiLS.

Sarà il Primo client l'applicazione ove ospitare la relativa interfaccia di gestione.

5.3 Client del SiLS

Alla luce di quanto sinora descritto, è possibile fornire una migliore descrizione dei client.

Nella tabella seguente sono indicate quali gestioni dati sono accessibili in consultazione ed inserimento dai diversi client di utilizzo.

Elaborazioni	Client					
	Consultazione					Inserimento
Gestione utenti	1					Anagrafica PLN 1
Dati OBU		2				2
Gestione missione			3			PLN
Gestione trasferimento				4		4
Spostamento carichi ante dogana			3			PLN
Dati di allarme			3			
Gestione dell'allarme ricevuto			3			
Rappresentazione spaziale			3			

Dati anagrafici/descrittivi; ricerche			3		5	
Dati operativi di approfondimento			3			
Rating			3		5	5

5.3.1.1 Primo client

Da qui sono inseriti ed inviati al CED i dati che riguardano i soggetti che possono accedere al SiLS come fruitori; più nel dettaglio, l'amministratore del SiLS definisce i supervisori PLN, gli utenti delle Forze dell'Ordine e delle Autorità statali di controllo.

Inoltre, si registrano in questo modulo anche i conducenti e gli automezzi che sono destinatari di attività di sicurezza, al di fuori di missioni gestite in ambito di PLN.

Un'altra categoria di utenti registrati sono i produttori, gli installatori e i manutentori delle OBU.

I dati delle entità che il SiLS gestisce (conducenti, veicoli, aziende) sono invece importati da PLN ed il loro aggiornamento comporta l'aggiornamento di quelli del SiLS; tramite il Primo client, i supervisori della PLN possono controllare la completezza e l'integrità dei dati importati.

5.3.1.2 Secondo client

Questo è riservato, in prima istanza, agli attori tecnici del SiLS quali produttori di OBU, installatori e manutentori; si rammenta che si tratta di identità anagraficamente già acquisite con il Primo client.

I produttori di OBU inseriranno i dati relativi all'apparato in termini di identificazione unitaria (numero seriale, versione ed altro) che corrisponderanno a quelli contenuti nell'OBU in un firmware da loro non scrivibile.

Allo stesso modo, inseriranno i dati relativi alle SIM card installate sulla OBU e sul tablet fornito ai conducenti.

Gli installatori ed i manutentori inseriranno dati inerenti gli interventi di propria competenza, sempre completando la definizione anagrafica relativa all'operazione compiuta.

5.3.1.3 Terzo client

Come sopra affermato, questo modulo client costituisce la componente prettamente operativa del SiLS sulla quale gli operatori seguono la situazione in corso.

Gli operatori inseriscono pochi dati soprattutto derivanti da variazioni di stato come, ad esempio, "allarme ricevuto", "inviate risorse" ed altro similare.

Questo anche perché, in seguito alla constatazione di un'anomalia, gli operatori delle Forze dell'Ordine si attivano su un'altra postazione, da dove possono gestire le risorse destinate all'intervento.

All'inserimento di una variazione di stato corrisponde la possibilità di inserire una nota a testo libero che può essere utile in un secondo momento.

5.3.1.4 Quarto client

Questo client riguarda un conducente, già registrato come utente, che compie un viaggio di trasferimento senza che lo stesso costituisca una missione specificamente gestita da UIRNet.

In questo caso, l'utente costruirà una missione in maniera del tutto semplificata specificando tutto ciò che concerne la partenza, l'arrivo ed il tragitto in modo che possa essere seguito dal SiLS.

Tale modalità gli consente di usufruire dei vantaggi offerti in materia di security.

5.3.1.5 Quinto client

Riguarda il controllo che le Forze dell'Ordine dislocate sul territorio possono eseguire nel corso della propria attività.

Il client fornisce informazioni ed elaborazioni statistiche in merito a conducenti, veicoli ed aziende assistendo in modo rapido ed efficace gli Operatori nel controllo anche senza fermare il veicolo.

Di rilievo la rappresentazione del rating; in ogni caso, le informazioni e le modalità di rappresentazione dovranno essere del tutto affini a quelle del Terzo client in modo che gli Operatori in strada e in centrale/sala operativa possano consultare le informazioni negli stessi termini.

6. FORNITURE HW/SW DI BASE

E' richiesto agli offerenti di individuare gli apparati hardware ed i software di sistema e di protezione, necessari al compimento delle attività descritte nel documento.

6.1 Caratteristiche di base

Si ribadisce il principio per cui non vi deve essere alcuna dipendenza tra gli apparati hardware e il software applicativo; quest'ultimo può essere spostato da una collocazione ad un'altra senza la necessità di compiere processi di installazione delle singole componenti di base ovvero applicative.

Il Fornitore dovrà proporre un'architettura tecnica, scalabile, che potrà prevedere, in funzione dei livelli di disponibilità da implementare, l'utilizzo di diversi server tra di loro interconnessi ed interoperabili su cui saranno ospitati i diversi componenti applicativi e di middleware dell'intero sistema.

Ciascun server dovrà essere opportunamente configurato in funzione del carico e del suo inserimento nell'ambito dell'architettura complessiva.

Si evidenzia il principio generale per cui i due Sotto-sistemi SiSS e SiLS dovranno risiedere, rispettivamente, in macchine virtuali differenti pur condividendo gli stessi apparati fisici di elaborazione e memorizzazione.

6.2 Utilizzo di soluzioni open source

Si evidenzia che la scelta delle soluzioni per piattaforme ed architetture sarà preferibilmente basata su tecnologie *open-source*, quale scelta strategica per l'ottimizzazione delle risorse economiche e per la creazione di asset durevoli in forza al Committente.

Le scelte dovranno essere effettuate secondo quanto stabilito dalla Legge del 7 agosto 2012 n. 134 - Conversione in legge, con modificazioni, del decreto-legge 22 giugno 2012, n. 83, recante misure urgenti per la crescita del Paese, pubblicato in Gazzetta Ufficiale n. 187 del 11 agosto 2012 al supplemento ordinario, con particolare riferimento all'art. 22 comma 10, che per completezza si riporta nel seguito:

"... *Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato: a) software sviluppato per conto della pubblica amministrazione; b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione; c) software libero o a codice sorgente aperto; d) software combinazione delle precedenti soluzioni. Solo quando la valutazione comparativa di tipo tecnico ed economico dimostri l'impossibilità di accedere a soluzioni open source o già sviluppate all'interno della pubblica amministrazione ad un prezzo inferiore, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso. La valutazione di cui al presente comma è effettuata secondo le modalità e i criteri definiti dall'Agenzia per l'Italia Digitale, che, a richiesta di soggetti interessati, esprime altresì parere circa il loro rispetto* ..."

6.3 Requisiti funzionali minimi

Le caratteristiche dell'hardware e del software di base oggetto dell'offerta del Fornitore devono soddisfare i requisiti funzionali minimi descritti nella tabella che segue

PRESTAZIONI			Sotto-Sistema
ELABORAZIONE			
Potenziale numero di OBU contemporaneamente connesse	10.000	unità	SiLS
Misura della maggiore frequenza possibile di invio dei dati da ogni singola OBU	30	unità di misura: secondi	SiLS
Tempo massimo delle operazioni push per le informazioni di localizzazione	5	unità di misura: minuti	SiLS
Tempo massimo di refresh delle informazioni di localizzazione sulla cartografia	5	unità di misura: secondi	SiLS
Tempo massimo di rappresentazione di un allarme sulla cartografia	5	unità di misura: secondi	SiLS
Tempo massimo di calcolo e refresh delle informazioni statistiche	60	unità di misura: secondi	SiLS
Tempo massimo di aggiornamento dei file di scambio dati	60	unità di misura: secondi	SiLS
Potenziale numero di client contemporaneamente connessi	150	unità	SiLS
Dimensione minima del frame con la rappresentazione cartografica	640X480	unità di misura: pixel	SiLS
Numero di documenti da gestire per anno	1.000.000	unità	SiSS
Dimensione media di un documento	200	unità di misura: KB	SiSS
Utenze contemporanee dei moduli SiSS	20	unità	SiSS
Container gestiti per anno	3.000.000	unità	SiSS
Manifesti doganali per anno	10.000	unità	SiSS
Dichiarazioni doganali per anno	300.000	unità	SiSS
MEMORIZZAZIONE			
Periodo dati conservati e disponibili in linea comprese elaborazioni statistiche	5	unità di misura: anni	SiSS e SiLS
Periodo localizzazioni conservati e disponibili in consultazione (eccezione del precedente)	6	unità di misura: mesi	SiLS

6.4 Definizione tecnologica dell'hardware e del software di base

Di seguito si descrivono alcuni aspetti centrali relativi alla fornitura di quanto necessario alla realizzazione del centro di elaborazione.

Occorre sottolineare che è prioritaria la rispondenza ai requisiti funzionali minimi sopra espressi rispetto agli aspetti tecnici; questi ultimi non possono, nel minimo, derogare alle indicazioni fornite in questo paragrafo.

La fornitura dovrà essere comprensiva di rack 42U completo di ventole di raffreddamento e PDU, consolle KVM con switch 16 porte e relativi apparati di rete.

La fornitura dovrà essere posta in opera comprensiva delle licenze dei sistemi operativi, della licenza Tele Atlas per il sistema SiLS.

Il Fornitore dovrà identificare ed indicare in offerta eventuali DBMS, application server e quant'altro necessario a rendere la propria soluzione completa e perfettamente funzionante.

Allo stesso modo, il Fornitore dovrà identificare ed indicare tutte le soluzioni necessarie per la sicurezza e l'integrità del Sistema (es. antivirus, antimalware, firewall ed altro).

Il Fornitore inoltre dovrà certificare la compatibilità dell'hardware con le versioni software installate.

Il sistema, pur condividendo alcune risorse del centro elaborazione primario ospitante, sarà strutturato secondo criteri di autonomia e di indipendenza con una propria rete locale IP, un proprio sistema di firewall, una propria storage area network.

6.4.1 Piattaforma tecnologica ed architettura

Il progetto si basa sull'utilizzo di strumenti tecnologici pienamente integrati fra loro e disponibili con continuità nel tempo e nello spazio al fine di consentire a tutti gli utenti e sistemi collegati di poter usufruire del servizio senza limiti di tempo.

La composizione della piattaforma tecnologica, oggetto di fornitura, è sintetizzabile in un sistema elaborativo informatico basato su server collegati in rete e specializzati per funzioni.

Alla base delle infrastrutture ICT del centro di elaborazione dovranno essere presenti:

- la Storage Area Network (SAN);
- la rete IP che interconnette i vari elementi del centro nonché il centro stesso alle reti esterne;
- le componenti server.

E' compresa nel presente appalto la fornitura dell'hardware (comprensiva della consegna, installazione e collaudo di prodotti) e la fornitura delle licenze dei sistemi operativi, dei data-base server e degli application server.

Il Fornitore dovrà inoltre prevedere anche la pianificazione, l'esecuzione delle configurazioni di base delle apparecchiature e l'attivazione dei prodotti hardware e software al fine di renderli operativi nei tempi e nei modi previsti in sede di offerta tecnica.

Sarà cura del Fornitore dimensionare e dettagliare nell'offerta tecnica l'infrastruttura tecnologica logica e fisica proposta sulla base delle piattaforme offerte e dei servizi richiesti dal capitolato tecnico.

6.4.1.1 Storage Area Network

La SAN per la memorizzazione dei dati dovrà essere basata su tecnologia Fiber Channel (FC) con le caratteristiche minime riportate di seguito.

CARATTERISTICA	VALORE RICHIESTO
Tipologia	Rack da 19
Porte	Tutte le porte degli apparati offerti devono essere 8 Gbit/sec
Numero di porte	Minimo 24
Upgrade delle porte	L'upgrade delle porte aggiuntive, deve essere realizzato attraverso l'attivazione del codice a caldo per ridurre la dipendenza dalle interruzioni.
Caratteristiche di affidabilità	Le unità di raffreddamento e le unità di alimentazione dei prodotti proposti, devono essere del tipo hot-swap, ridondanti e integrati
Software di management	Il software di management dovrà essere del tipo "Web Based", intuitiva e facile da usare, attraverso una grafica che consenta di monitorare e gestire la rete SAN.

In ogni caso sarà cura del Fornitore configurare gli apparati richiesti con un numero di porte e relativi cavi FC necessari ad assicurare la connessione dei server oggetto di fornitura con le unità di storage.

La soluzione di storage dovrà garantire l'integrità e protezione dei dati in caso di problemi di alimentazione esterna.

Il sistema di storage richiesto dovrà avere intrinsecamente le seguenti caratteristiche minime

CARATTERISTICA	VALORE RICHIESTO
Montaggio Rack	Il sistema deve essere offerto completo degli armadi rack necessari al montaggio dell'intero sistema.
Ridondanza componenti hardware	Controller alimentatore e sistema di raffreddamento
Scalabilità dei controller	Il sottosistema di storage deve poter scalare 4 controller di base, in modalità "cluster"
Numero di controller	Il sistema di storage dovrà essere configurata con almeno 2 controller
Funzionalità di replica Sincrona e Asincrona	Il sottosistema di storage deve avere un software, che consenta la copia dei dati sia in modalità sincrona che asincrona.
Cache	> 12 GB
Espandibilità massima dei dischi	Il sottosistema di storage deve poter scalare con un numero minimo di alloggiamenti dischi > 100

Tipo di dischi supportati:	Il sistema di storage dovrà supportare almeno le seguenti tipologie di dischi: • SSD • FC • SATA
RAID supportati	Il sistema di storage dovrà supportare almeno 3 delle seguenti tipologie di RAID: 0, 1, 5, 6
Capacità Storage minima richiesta	> 20 TB raw di cui 5 TB con dischi SSD; 15 TB con dischi SATA II a 7200rpm
Connettività max supportata	> 12 porte FC
Connettività minima richiesta	> 4 porte FC
Software per le repliche locali	Il sottosistema di storage deve avere un software, in grado di supportare la replica locale sia in modalità "Snap" che "Clone"
LUN Migration	Possibilità di muovere le LUN tra Tier di tipo diverso, on-line ed in maniera trasparente all'applicazione.
Provisioning	Deve essere previsto per la capacità fornita
Remote support	Si
Prestazioni	Il sottosistema di storage deve avere prestazioni certificate secondo lo standard SPC-1 $\geq$90.000 IOps o throughput equivalente

6.4.1.2 Rete IP

La rete che interconnette i vari server, anch'essa oggetto di fornitura, dovrà operare almeno ad 1 Gbps.

Le unità di switching dovranno essere dotate di un numero di porte sufficienti a connettere i server ed i vari apparati facenti parte del centro di elaborazione e, per motivi di affidabilità, dovranno essere ridondate.

Tali unità di switching saranno connesse tra di loro in alta affidabilità e configurate in modalità "active-active".

La protezione perimetrale dell'infrastruttura del sistema dovrà essere assicurata da firewall, anch'essi oggetto di fornitura.

6.4.1.3 Le componenti server

La componente tecnologica hardware e la struttura di rete minime richieste, salvo quanto descritto in precedenza, e comunque oggetto di verifica in sede di stesura del progetto esecutivo, dovrà corrispondere, al minimo, a quattro funzioni fondamentali di servizio:

- autenticazione, accesso e presentazione dei servizi messi a disposizione per ognuno dei Sotto-Sistemi e per le classi di utenza che, rispettivamente, ne fanno parte;
- accesso, in modalità http/https, dai client web di cui sono dotati gli utenti; i supporti potranno essere integrati negli application server oppure operare come server separati di front-end;

- funzionamento, in termini elaborativi, dei moduli applicativi;
- memorizzazione dei dati intesi sia come file (File System) che come DBMS, strutturato secondo il modello relazionale.

Come già cennato, deve essere previsa la virtualizzazione dei server.

In tale logica sarà necessario, pertanto, distinguere il server fisico dal concetto di server virtualizzato che mette a disposizione un insieme ben determinato di risorse e di servizi per ognuno dei due sotto-sistemi.

Per le prime due funzioni dell'elenco precedente, si ritiene necessario prevedere almeno due server bilanciati e dedicati per la funzione di gestione ed erogazione dei relativi servizi; ciascun server dovrà rispondere ai seguenti requisiti minimi

CARATTERISTICA	VALORE RICHIESTO
Form factor	Rack mounting
Processore	Dual Intel Xeon 4C 1,73 GHz o equivalente
Numero processori	2
RAM	16 GB
Hard Disk	2 serial ATA driver 160 GByte
Driver controller	Embedded SATA controller
Scheda di rete	Dual integrated 10/100/1000 Ethernet 2 HBA FC8
Drive	Lettore DVD/Blue Ray
Power	Dual power supply (ridondante)

Ciascuno dei sistemi dedicati al terzo ed al quarto punto di cui al precedente elenco di funzioni saranno costituiti da 2 server in configurazione cluster; ciascun server dovrà rispondere ai seguenti requisiti minimi;

CARATTERISTICA	VALORE RICHIESTO
Form factor	Rack mounting
Processore	Dual intel Xeon 6C 2 GHz o equivalente
Numero processori	2
RAM	32 GB

Hard Disk	2 serial ATA driver 320 GByte
Scheda di rete	Dual integrated 10/100/1000 Ethernet
	2 HBA FC8
Drive	Lettore DVD/Blue Ray
Power	Dual power supply (ridondante)

6.5 Web browser per client

La soluzione proposta dovrà essere fruibile da tutti i browser standard di mercato (Explorer 6.x o superiori, Safari 3.x o superiori, Firefox 2.x o superiori), disponibili sia su piattaforma Windows 2000/NT/XP/7/Vista che su Mac OS o Linux/Ubuntu.

6.6 Proprietà del software

Le forniture, le licenze software, il software sviluppato dal Fornitore per il presente sistema e quant'altro derivi dalle fasi di progetto, divengono di proprietà del Committente al termine di ogni fase di sviluppo e dopo esito positivo di collaudo.

6.7 Garanzia

Il Fornitore dovrà prestare garanzia su tutti gli apparati, i sistemi hardware e i prodotti software forniti per la realizzazione del sistema oggetto di fornitura.

La garanzia vale per un periodo di almeno 24 (ventiquattro) mesi a decorrere dal collaudo dell'intera fornitura.

Inoltre, gli apparati ed i prodotti dovranno essere conformi a standard e norme che riguardano le emissioni elettromagnetiche, la sicurezza, l'ergonomia e l'accessibilità.

6.8 Fornitura OBU per SiLS

La fornitura per la realizzazione del SiLS deve comprendere, tra l'altro, gli elementi di seguito indicati:

- n. 50 OBU complete di tutti i dispositivi descritti nel capitolato ad eccezione delle stazioni a terra per interrogazione ai varchi ma comprensive di un totale di n. 70 tablet. Il sistema operativo di riferimento preferito per i tablet è Android o Microsoft Windows ed i tablet dovranno essere al 50% appartenenti alla classe dei cd. 7 pollici e

il 50% appartenente alla classe dei cd. 10 pollici. I tablet dovranno essere abilitati alla comunicazione via SIM card. Al termine di ogni fase di sviluppo e dopo esito positivo di collaudo, le applicazioni realizzate per il funzionamento delle OBU e per il collegamento con gli apparati collocati a bordo dei veicoli diventeranno di proprietà di UIRNet S.p.A. unitamente ai cd. codici sorgenti, documentazione di progetto, ecc.

- licenza tecnologia Tele Atlas, attivata per un tempo pari al termine della Fase di Gestione, addizionato di tre mesi solari e continuativi, per il suo utilizzo in ambito di Terzo client del SiLS.

7. INTEGRAZIONI INFRASTRUTTURALI

7.1 La Sala Crisi

Il Comitato tecnico e il Comitato ristretto previsti quali fruitori dei sistemi in argomento, dovranno disporre di un idoneo ambiente (denominato da qui in avanti Sala Crisi) da attrezzare e da collocare all'interno dell'Area Portuale di Gioia Tauro, in spazi messi a disposizione dall'Autorità Portuale presso la palazzina della ex-sede della suddetta Autorità.

Per consentire ai Comitati di svolgere i compiti di monitoraggio, controllo e direzione strategica, descritti nel paragrafo "Obiettivi e scopi del progetto", la Sala Crisi sarà attrezzata in termini di componenti hardware, arredi e complementi, in conformità alle disposizioni vigenti in materia di sicurezza sul lavoro.

La Sala Crisi dovrà essere opportunamente attrezzata e il modello operativo che si configura è quello proprio di una *Situation Room*.

In definitiva, il Comitato:

- coordina delle azioni da porre in essere all'atto dell'individuazione di merci pericolose ed in particolare al loro continuo monitoraggio dal momento della loro identificazione sino all'uscita dall'area portuale o alla loro distruzione;
- opera ed in tale ambito cura, in sinergia con gli altri organi statali competenti a livello regionale/centrale le attività di prevenzione e di contrasto alle attività malavitose;
- gestisce per il tramite di sistemi tecnologici, informatici e multimediali la previsione, l'allerta, il coordinamento di situazioni di crisi;
- cura i rapporti con gli altri organi istituzionali dello Stato che operano sul territorio regionale ai fini della sicurezza del territorio;
- attiva e coordina la logistica, nonché l'utilizzo dei mezzi e delle attrezzature per la gestione ed il superamento delle emergenze;
- istituisce, se del caso, team di lavoro di pronto intervento per una immediata risposta alle emergenze al fine di rendere più efficace l'azione di tutela del territorio;
- provvede, in caso di emergenza, alla definizione di piani di evacuazione di persone, mezzi e materiali, eventualmente coordinando le attività con la Protezione Civile.

Sarà cura del Fornitore proporre e dettagliare l'intervento tecnologico, infrastrutturale, di arredo ed impiantistico che si propone per i locali in argomento avendo cura di soddisfare almeno i requisiti funzionali minimi di cui di seguito.

Il numero minimo di postazioni da realizzare ed attrezzare nell'ambiente ad operatività condivisa è di quindici postazioni complete di tutti gli strumenti di supporto (audio, video e telefoniche) e di postazioni informatiche client da cui sarà possibile utilizzare le funzionalità del sistema.

Le postazioni dovranno essere configurate sotto il profilo HW e SW dal Fornitore in base alle funzionalità offerte che dovranno essere pienamente utilizzabili e dovranno avere una capacità di elaborazione in grado di rappresentare le immagini, i dati e la cartografia senza ritardi, per quest'ultima negli specifici casi di ingrandimento, riduzione e "scroll".

Per una prima sommaria informazione e per consentire una stima tecnico-economica si precisa che le dimensioni fisiche dell'ambiente sarà di circa trentacinque mq, con altezza di circa tre metri.

Le descrizioni sono di massima e dovranno essere approfondite dal Fornitore in fase di progettazione esecutiva.

Il Fornitore delineerà il layout definitivo e le relative lavorazioni necessarie in contraddittorio con il Committente; tuttavia una sommaria lista di attività, forniture e lavorazioni nell'area interessata da tener presenti e valutare, anche ai fini dell'offerta, dovranno essere:

- pavimento flottante;
- controsoffitto;
- demolizioni;
- istallazioni pareti mobili vetrate (circa quindici mq);
- sostituzione porta (una in alluminio e vetro con serratura elettrificata e maniglione antipanico);
- adeguamento impianto elettrico;
- impianto di illuminazione;
- impianto di condizionamento (caldo/freddo);
- realizzazione impianto trasmissione dati;
- fornitura ed installazione di 4 monitor da 55" a parete;
- rifinitura e tinteggiatura pareti;
- impianto antintrusione;
- tavolo riunioni attrezzato con minimo 15 postazioni complete di sedute.

La natura particolare della Sala Crisi, attivata secondo necessità per supportare le esigenze connesse al verificarsi di un evento rilevante, non richiede strutturazioni complesse, ma una predisposizione che enfatizzi i seguenti aspetti:

- presentazione di quadro di situazione per logiche generali;
- spiccata capacità di comunicazione, anche mediante sistemi di alta tecnologia;
- possibilità di ampio ricorso alle videoconferenze, per massimizzare il rapporto frontale con l'interlocutore ed esaltare la logica di centro di comando e controllo.

Per consentire la continuità operativa della sala crisi, anche in presenza di interruzione dell'alimentazione elettrica di rete, si dovrà procedere alla realizzazione dei sistemi d'energia o alla loro integrazione, qualora necessaria.

Per Sistemi d'Energia intendiamo quelle apparecchiature che servono ad assicurare una corretta alimentazione elettrica ai sistemi, anche quando l'erogazione dell'Ente fornitore subisca un'interruzione.

Un elenco, non esaustivo, delle necessità da soddisfare è il seguente:

- gruppo elettrogeno (di potenza e caratteristiche adeguate per alimentare tutti gli apparati tecnologici della sala crisi, compreso l'impianto di condizionamento)
- adeguamenti infrastrutturali per l'ospitalità, secondo le norme in vigore, del gruppo elettrogeno in un ambiente da definire in fase di sopralluogo.
- gruppo di continuità (che serve ad assicurare l'alimentazione in continuità dal momento della mancanza d'energia, al momento in cui il motore diesel del gruppo elettrogeno entri in funzione) di capacità adeguata a mantenere in funzione gli apparati IT per il tempo necessario all'avvio del G.E.;
- raccordi d'energia tra i vari componenti il nuovo impianto;
- realizzazione di quadri elettrici e prese elettriche distinte per le linee sotto continuità.

Anche questi apparati dovranno essere forniti con un'adeguata copertura di assistenza tecnica.

Tutti i quadri elettrici e le potenze dei gruppi andranno dimensionati in modo da sopportare un adeguato "buffer" di potenza per future esigenze di alimentazione; si dovrebbe così scongiurare la possibilità di future alimentazioni da quadretti elettrici non correttamente posizionati ed alimentati.

7.2 La Sala Apparati ed i Sistemi d'Energia

Appare chiara la necessità di un ambiente tecnico che ospiti i server a servizio del sistema in argomento, ma che raggruppi in un unico luogo sicuro protetto ed attrezzato tutti gli apparati informatici e di telecomunicazione.

Questo sarà un ambiente fisico, che potremmo definire di back office, ove saranno attestate tutte le diverse tecnologie necessarie al funzionamento del Sistema.

La Sala Apparati dovrà essere allestita presso i locali del Centro di Elaborazione Dati della Direzione Interregionale per la Campania e la Calabria dell'Agenzia delle Dogane e dei Monopoli e dei Monopoli, con sede in Napoli.

Il Fornitore dovrà provvedere ad effettuare gli interventi che si dovessero rendere necessari al fine di integrare il Sistema con l'infrastruttura esistente presso detto Centro, quali integrazione all'impianto di cablaggio strutturato esistente mediante stesura cavi UTP e/o fibre ottiche con relativa fornitura di interfacce ottiche laddove necessario nonché integrazione all'impianto elettrico mediante apposizione di cassette di derivazione opportunamente configurate.

Il dimensionamento delle predette attività è funzione del numero di armadi rack che saranno offerti nella presente fornitura.

Si dovranno altresì prevedere le necessarie acquisizioni e conseguenti attività di integrazione dei sistemi software di gestione dell'infrastruttura (networking, backup, etc.).

In ragione di quanto sopra, insieme alla sala Crisi, il Fornitore si deve far carico di progettare e realizzare anche gli adeguamenti necessari per configurare in maniera ottimale la sala apparati.

Sarà cura del Fornitore proporre e dettagliare l'intervento tecnologico, infrastrutturale, di arredo ed impiantistico che si propone per i locali in argomento avendo cura di soddisfare almeno i requisiti funzionali minimi di cui di seguito.

- pavimento flottante;
- controsoffitto;
- demolizioni;
- rifinitura e tinteggiatura pareti;
- sostituzione porta (una porta REI 120 con larghezza di almeno 120 cm con serratura elettrificata e maniglione antipanico);
- impianto trasmissione dati;
- adeguamento impianto elettrico;
- impianto di illuminazione;
- impianto di condizionamento (solo freddo);
- impianto antintrusione;
- impianto rilevazioni fumi e allagamento.

La conformazione tipo di questo locale è pensata come un ambiente di circa 20 mq, ad accesso controllato e con una impiantistica adeguata (condizionamento, rilevazione di fumi e di allagamento, allarme di temperatura, ecc.).

Si ribadisce che il Fornitore dovrà fornire anche tutti i componenti e sistemi di rete, di trasmissione dati, di protezione atti a sostenere le comunicazioni e l'accesso ai sistemi in modalità locale, nonché ad assicurare l'esposizione dei servizi verso la rete internet con le dovute regole e soluzioni tecniche orientate alla sicurezza, protezione dei dati, protezione degli accessi, protezione da attacchi informatici.

Si possono distinguere due zone funzionali all'interno della sala apparati: la sala vera e propria e la sala energia.

In sede di progettazione si avrà cura di determinare sulle planimetrie anche le posizioni di eventuali rack non ancora presenti, in modo di ottimizzare l'uso, anche futuro, dello spazio.

Tali informazioni saranno desumibili dalle interviste effettuate in fase di analisi.

La sala energia è il luogo ove sono raggruppati i quadri elettrici e dove sono istallati i gruppi di continuità e le batterie.

Di norma essa è situata in un locale ricavato all'interno della sala apparati ma può, anch'essa, trovarsi separata da questa o, per motivi di spazio, essere costituita semplicemente da una specializzazione degli spazi all'interno della sala.

Per consentire il continuo funzionamento degli apparati costituenti il sistema degli altri apparati, infatti, si deve procedere alla realizzazione dei sistemi d'energia o alla loro integrazione, qualora necessaria.

Per Sistemi d'Energia intendiamo quelle apparecchiature che servono ad assicurare una corretta alimentazione elettrica ai sistemi, anche quando l'erogazione dell'Ente fornitore subisca un'interruzione.

A grandi linee si tratta di:

- gruppo di continuità (che serve ad assicurare l'alimentazione in continuità dal momento della mancanza d'energia, al momento in cui il motore diesel del gruppo elettrogeno entri in funzione);
- raccordi d'energia tra i vari componenti il nuovo impianto.

Anche questi apparati dovranno essere forniti con un'adeguata copertura di assistenza tecnica.

Tutti i quadri elettrici e le potenze dei gruppi andranno dimensionati in modo da sopportare future esigenze di alimentazione; si dovrebbe così scongiurare la possibilità di future alimentazioni da quadretti elettrici non correttamente posizionati ed alimentati.

La Sala Apparati dovrà consentire l'ottimale conservazione dei sistemi tecnologici sotto il punto di vista del loro ottimale funzionamento e gestione (sistemi di condizionamento, illuminazione, rilevazione fumo, spegnimento manuale, ecc.) e della loro sicurezza (antiintrusione, ecc.).

7.3 Adempimenti a carico del Fornitore in merito alle integrazioni infrastrutturali.

Il Fornitore dovrà fornire gli elaborati progettuali relativi alla Progettazione Preliminare e alla Progettazione Esecutiva completi di quanto all'uopo previsto dalle norme vigenti in materia a firma di tecnico abilitato, previa condivisione delle soluzioni progettuali da parte del Committente, nonché dovrà provvedere a trasmettere prova dell'avvenuto deposito dei suddetti documenti progettuali presso gli Enti preposti per gli eventuali e/o necessari autorizzazioni/pareri, ove previsto dalla normativa vigente in materia;

Il Fornitore si impegnerà a provvedere e ad individuare, ai sensi del D.Lgs. 9 aprile 2008 n. 81, in qualità di committente e responsabile dei lavori che dovessero essere necessari per l'allestimento della Sala Situazioni: (i) un progettista, (ii) un tecnico in funzione di direttore dei lavori e, ove ricorrano le fattispecie previste dalle norme, (iii) un coordinatore per la sicurezza in fase di progettazione dei lavori ed (iv) un coordinatore della sicurezza in fase di esecuzione dei lavori, nonché a verificare che l'impresa esecutrice dei lavori medesimi provveda a

redigere un apposito piano di sicurezza e che sia in possesso delle qualificazioni richieste dalla legge per l'esecuzione dei lavori che dovranno essere realizzati;

Il Fornitore si impegna a consegnare al Committente le opere realizzate - ivi compresi gli impianti - munite di certificato di regolare esecuzione/collaudo e dei certificati di conformità.

8. FASI DI REALIZZAZIONE E ATTIVITA' CORRELATE

8.1 Suddivisione del Progetto in Fasi

In sede di offerta è richiesto di organizzare la realizzazione della fornitura in una Fase di implementazione ed in una di gestione; di seguito si proseguirà ad usare i termini Committente e Fornitore per indicare le due Parti contrattuali oltre che le responsabilità e gli obblighi ad ognuno associati.

- Fase di Implementazione, che porta alla finalizzazione da parte del Fornitore delle specifiche funzionali e tecniche, alla realizzazione del progetto, al successivo collaudo e all'avviamento della realizzazione con la contestuale consegna finale della documentazione tecnica e la valutazione dei risultati;
- Fase di Gestione, comprendente servizi di esercizio.

Per la Fase di implementazione è prevista una durata complessiva non eccedente dodici mesi solari e continuativi, mentre per quella di gestione sono previsti ulteriori sei mesi solari e continuativi.

8.2 Fase di implementazione

8.2.1 Attività da svolgere

Nel seguito sono elencate le attività minime che devono essere svolte da parte del Fornitore per la fase di implementazione del progetto; resta inteso che alcune di queste attività hanno carattere iterativo ed incrementale.

L'implementazione ha inizio con il Piano di progetto, contenente tra l'altro la progettazione di dettaglio e il Piano di qualità, entrambi redatti dal Fornitore, e sottoposti alla vincolante approvazione del Committente.

8.2.1.1 Elaborazione del Piano di progetto e del Piano della qualità

Il Piano di progetto e il Piano della qualità dovranno essere presentati entro 60 giorni solari e continuativi dalla data di avvio delle attività.

Il Piano di progetto dovrà indicare, tra l'altro, una proposta relativa alle date di inizio e fine di tutte le attività relative alle diverse fasi di attuazione che saranno vincolanti, una volta accettate dal Committente, per entrambe le parti.

Il Piano di progetto sarà sottoposto a monitoraggio da parte del Committente con una frequenza almeno mensile ai fini della verifica periodica dello stato di avanzamento delle attività e della definizione degli elementi che costituiscono il SAL.

8.2.1.2 Progettazione di dettaglio

La Progettazione di dettaglio (da intendersi anche come progettazione esecutiva, secondo terminologia standard) fa parte, come detto, del Piano di progetto ed ha, quale punto di partenza, i contenuti che il Fornitore ha rappresentato nella propria offerta.

Gli stessi costituiscono un vincolo a carico del Fornitore quale elemento minimo per lo sviluppo della Progettazione di dettaglio; pertanto, la stessa non potrà derogare agli eventuali impegni assunti in sede di offerta ma costituirne, auspicabilmente, un miglioramento.

Nella Progettazione di dettaglio devono essere contenuti, al minimo, gli elementi di seguito indicati:

8.2.1.2.1 Analisi di dettaglio dei processi inerenti il progetto.

L'analisi di dettaglio dovrà partire da quanto già descritto nel presente documento, dalla normativa nazionale e comunitaria di riferimento, e da quanto sarà fornito dal Committente all'atto dell'aggiudicazione.

L'analisi di dettaglio deve essere orientata alla rilevazione di ulteriori, eventuali, oggetti informativi esistenti ed utilizzati, alla rilevazione della mappatura dei sottosistemi applicativi e delle basi di dati presenti presso gli attori del sistema, oltre che all'approfondimento di ulteriori, eventuali, processi che emergessero in fase di analisi.

L'analisi deve prevedere l'integrazione con i sistemi informativi laddove è stato previsto uno scambio informativo continuativo e diretto.

Il Committente, inoltre, a supporto della fase di analisi e dell'intero processo di sviluppo potrà individuare e coinvolgere nel processo un gruppo di key-user, intesi come utenti tipo ed esperti del dominio.

8.2.1.2.2 Disegno del modello organizzativo

Dovrà essere individuato nel dettaglio e compiutamente descritto il modello organizzativo relativo ai processi individuati afferenti il progetto.

E' attesa l'esatta definizione delle competenze, responsabilità e vincoli che fanno capo a ciascuna tipologia di utenza del sistema.

Contestualmente, sarà definita l'analisi dello scostamento (gap analysis) tra le attuali abilità e quelle richieste alle diverse tipologie di utenza per lo svolgimento dei propri compiti.

Fa capo alla citata gap analysis anche la definizione degli elementi e dei contenuti di change management che sarà necessario mettere in campo per colmare l'eventuale divario di competenze.

8.2.1.2.3 Assessment dell'infrastruttura di sicurezza portuale e dei sistemi connessi

Sarà necessario procedere ad un puntuale assessment delle infrastrutture di sicurezza portuale oltre che ai sistemi connessi a questo progetto (con particolare riferimento al sistema AIDA ed alla PLN) esistenti al momento dell'effettivo inizio di progetto.

L'assessment sarà condotto, al minimo, in termini di procedure e sistemi tecnologici, con particolare, ma non esclusivo, riferimento:

- alle caratteristiche ed alla effettiva disponibilità delle basi di dati che dovranno essere connesse al sistema previsto dal progetto;
- ai sistemi di comunicazione necessari, relazionandoli con quelli, in quel momento, disponibili oltre che con quelli eventualmente previsti da piani di sviluppo insistenti sulle aree interessate;
- ai locali ove saranno ospitate le infrastrutture tecnologiche previste.

Trattandosi di infrastrutture e sistemi in via di realizzazione ed in continua evoluzione, l'assessment si rende necessario per aggiornare gli elementi di progetto alla effettiva data di avvio dello stesso.

8.2.1.2.4 Definizione e disegno del sistema

Tali attività comprendono, a partire da quanto illustrato in questo capitolato e a ulteriori, eventuali, documenti forniti all'atto della contrattualizzazione, la definizione dell'inventario dei servizi da realizzare, delle relative interfacce, delle caratteristiche dello sviluppo/personalizzazione di ogni componente da realizzare, le eventuali integrazioni di ogni nuovo componente realizzato con altri sistemi.

E' necessario utilizzare appropriate metodologie e processi di sviluppo che descrivano e documentino in modo appropriato l'architettura (dei processi, informativa e tecnologica) con particolare riguardo ai servizi coinvolti comprendendo le regole, gli standard e le informazioni sul ciclo di vita dei sistemi per ottimizzare e mantenere l'ambiente operativo ed applicativo desiderato.

In particolare andrà esplicitamente definito ed utilizzato un processo di sviluppo adeguato alle esigenze del progetto e sottoposto alla vincolante approvazione del Committente.

8.2.1.2.4.1 Specificità per SiSS

Un Sotto-Sistema complesso come il SiSS per la sua progettazione e per il governo della sua Architettura SOA richiede adeguate metodologie di sviluppo e pianificazione che consentano di mantenere l'allineamento continuo dell'IT ai processi ed agli obiettivi.

A prescindere dallo specifico processo di sviluppo adottato, la Progettazione di dettaglio dovrà evidenziare due rilevanti attività necessarie alla progettazione della SOA:

- definizione della Business Architecture;
- definizione di un Service Inventory Blueprint.

Con la prima attività, si intende una definizione completa dell'architettura di business oggetto dell'intervento in termini di :

- processi business;
- organizzazione;
- data model.

La seconda attività, sulla base dei modelli definiti nell'architettura di business definisce un inventario dei servizi da implementare (service candidate) e realizzare in ottica SOA.

Si richiede quindi la fornitura e la messa in esercizio di un'architettura software di tipo Services Oriented Architecture (SOA); gli elementi essenziali dell'architettura SOA oggetto della fornitura saranno:

- servizi ESB: deve prevedersi la fornitura di un componente ESB che abbia almeno i requisiti minimi di gestione, validazione, normalizzazione e codifica del messaggio, inclusa la trasformazione dello stesso, supporto della modalità publish/subscribe, predisposizione di diversi tipi di adapter, wrapper e supporto per l'integrazione con LDAP e Active Directory;
- componenti di governance: la fornitura dovrà includere funzionalità che permettono il governo dei processi e, attraverso l'integrazione di web services, di sistemi differenti, nonché un BPM per la gestione dei processi;
- servizi di management & monitoring (BAM) che consenta la gestione dei log, il monitoraggio delle risorse assegnate al singolo servizio tale da poterne definire e modificare le modalità di funzionamento in modo puntuale e del sistema nel suo complesso, la creazione di report sulle attività dell'ESB, l'integrazione con gli altri componenti della piattaforma;

- sistema IAM - Identity and Access Management (IAM) che consenta la definizione di un processo di applicazione di policy appropriate per gestire le informazioni riguardanti le identità degli utenti e controllare l'accesso alle risorse informatiche.

Si fa presente che:

- la soluzione offerta per la piattaforma SOA dovrà avere un'architettura modulare, scalabile e flessibile in termini di performance e affidabilità;
- nel processo di selezione della piattaforma infrastrutturale del sistema verranno privilegiate le proposte tecniche che massimizzeranno l'utilizzo di soluzioni a codice sorgente aperto (open source);
- per ciascun ulteriore requisito proposto (corredato di adeguata documentazione) sarà valutata la caratteristica migliorativa.

8.2.1.2.4.2 Specificità per SiLS

La fase di implementazione comporta le seguenti attività:

- finalizzazione delle funzionalità e delle esigenze che possono essere espresse dal mondo dell'autotrasporto;
- progettazione del modello architetturale relativo alle OBU ed alle comunicazioni della stessa con il SiLS con indicazione delle specifiche dettagliate, individuando funzionalità, livelli di servizio;
- descrizione dettagliata delle integrazioni della OBU con gli apparati esterni;
- modalità di realizzazione delle OBU;
- proposta di un calendario di prove e messa a punto sul campo di eventuali prototipi della OBU e della propria componente di comunicazione con utenti di test;
- proposta di un piano dei test della OBU e della propria componente di comunicazione (es. unit test, application test, no-regression test);
- proposta di un piano di collaudo specifico per la OBU e la propria componente di comunicazione.

I prodotti realizzati dovranno essere configurati come prodotti aperti esenti da vincoli di carattere tecnologico e/o organizzativo che potrebbero impedire la loro gestione nelle fasi successive del progetto da parte di altri operatori di mercato.

8.2.1.2.5 Capacity Planning

Dovranno essere individuate e definite in termini di tuning finale, le componenti HW/SW di base che costituiscono la piattaforma tecnologica del progetto; come cennato, questa non potrà essere diminutiva rispetto a quella indicata in offerta.

Il Committente potrà individuare elementi dei componenti HW/SW di base costituenti versioni successive rispetto a quanto indicato in offerta da parte del Fornitore, qualora disponibili sul mercato al momento della contrattualizzazione con un valore economico equivalente a quello dichiarato in offerta.

Il HW/SW di base saranno oggetto dell'effettiva fornitura che dovrà essere predisposta ed operante presso i locali resi disponibili dall'Autorità Portuale di Gioia Tauro presso il porto o in altro luogo, indicato dal Committente e comunque localizzato nelle Regioni Obiettivo Convergenza.

8.2.1.3 Piano di qualità

Il Fornitore è tenuto a redigere un Piano della Qualità volto a descrivere l'organizzazione del Sistema di Gestione per la Qualità creato ad hoc per il progetto.

Per il controllo della qualità dei prodotti e dei servizi forniti dovranno essere individuati strumenti che, attraverso un'accurata descrizione delle modalità di fornitura ed una definizione dei livelli di servizio e dei sistemi per la loro misurazione, consentano il monitoraggio del

sistema (processi di assicurazione qualità, gestione di azioni correttive e preventive) facendo riferimento a parametri ed indicatori individuati anche con il supporto di auditor interni ed esterni.

Il Committente opererà il monitoraggio costante sulle attività e sui risultati via via conseguiti sulla base della rispondenza alle attese delle funzionalità e dei livelli di servizio dei prototipi realizzati.

Analogamente il Committente procederà alla valutazione dei prototipi realizzati e dei risultati conseguiti rispetto agli obiettivi definiti nel documento e nelle specifiche dettagliate di progetto predisposte.

8.2.1.4 Requisiti minimi di sicurezza e di osservanza alla normativa sulla privacy

Nel Progetto di dettaglio dovranno essere dettagliatamente descritte le soluzioni che il Fornitore intende adottare al fine di garantire un adeguato livello di sicurezza del sistema.

Le attività richieste nell'ambito del security management prevedono:

- l'analisi dei rischi di gestione della piattaforma;
- la definizione delle politiche di sicurezza;
- la verifica dell'attuazione delle politiche di sicurezza e di gestione della privacy;
- l'amministrazione della sicurezza;
- il controllo dei log e degli account;
- l'esecuzione periodica di test di intrusione, allarme e pronto intervento;
- l'analisi delle risorse critiche;
- il recupero dei dati e dei sistemi da attacchi informatici;

Le funzioni di sicurezza dovranno prevenire accessi non autorizzati, sia volontari che accidentali, sia ai programmi che ai dati.

Dovranno, dunque, essere progettate e realizzate opportune procedure atte ad assicurare i seguenti requisiti minimi di carattere generale:

- identificazione ed autenticazione: verifica dell'identità allo scopo di prevenire accessi non autorizzati al sistema e alle risorse di rete:
- autorizzazione: controlla quale sistema, informazione e applicazione può essere data ad un utente;
- integrità: assicura sia che i dati presenti negli archivi sia quelli che transitano sulla rete non vengano cambiati o compromessi da manipolazioni non autorizzate;
- riservatezza: intesa come prevenzione dell'utilizzo indebito delle informazioni. Tale requisito presuppone che l'accesso alle informazioni venga controllato attraverso adeguate misure di protezione;
- protezione della privacy previene la lettura di dati privati da parte di utenti non autorizzati.
- non-ripudio: verifica che la trasmissione dei dati è stata comunque eseguita in modo da non legittimare proteste basate su mancati invii;
- disponibilità: intesa come prevenzione dei pericoli di occultamento e/o di impossibilità di accesso ai dati, necessari per la conduzione di una attività lecita.

Dovrà essere predisposta una procedura di controllo logico e fisico degli accessi che consente l'accesso alle informazioni e alle risorse del sistema informatico secondo due livelli:

- per classi di utenza, che indicativamente sono le seguenti: amministratore, utente call center, utente esterno, ecc.;
- con granularità su base utente (identificazione univoca dell'utente).

Il controllo degli accessi dovrà essere effettuato, in modalità integrata, su tutte le unità elaborative costituenti il sistema informatico in esame, per consentire lo sviluppo certo ed univoco della politica di sicurezza sui dati e si baserà su:

- identificazione ed autenticazione degli utenti, sia interni che esterni;
- assegnazione controllata delle risorse (profili di abilitazione su base selettiva) sia in lettura che in scrittura;
- gestione dei log con adeguati meccanismi di auditing per garantire il mantenimento della traccia degli accessi e dei tentativi effettuati.

Dovranno essere realizzate delle procedure controllate di backup e ripristino dei dati.

Dovrà inoltre essere effettuato il controllo antivirus delle informazioni in ingresso e in uscita dai sistemi, mediante software opportuno; è richiesta la verifica almeno giornaliera dell'aggiornamento del database dei virus.

8.2.1.5 Collaudi

Per quanto riguarda i singoli elementi del sistema, le attività che devono essere svolte, per ciascuno di essi, da parte del Fornitore dovranno essere, al minimo, le seguenti:

- presentazione al collaudo tecnico delle varie componenti del sistema, collaudo funzionale di ciascun modulo e collaudo complessivo di integrazione del sistema
- funzionale e sistemistico dei nuovi apparati visti come elementi singoli che nella integrazione generale prevista nel progetto
- presentazione alla verifica, oltre che delle funzionalità previste dal Progetto di dettaglio, anche dell'efficace integrazione del sistema con i servizi preesistenti che devono essere collegati in termini di connessione dei dati in entrata/uscita.

8.2.1.6 Avviamento

A seguito del positivo collaudo e messa a punto del nuovo sistema nel suo complesso e di ogni suo singolo elemento, si procede all'avviamento dello stesso.

Tale passo rappresenta l'inizio della Fase di gestione che, come detto, avrà una durata di sei mesi solari e continuativi.

All'avviamento corrisponde la consegna della documentazione ufficiale del sistema, intendendo l'ultima versione aggiornata della stessa, il cui sviluppo ed aggiornamento è onere a carico del Fornitore.

Il Fornitore dovrà considerare l'avviamento del sistema come inclusivo, al minimo, delle seguenti prestazioni:

- configurazione e messa in esercizio garantendo, se necessario, il popolamento iniziale dei dati;
- attivazione adeguata connettività internet;
- eventuali connessioni vpn verso il sistema;
- eventuali connessioni verso apn;
- fine-tuning del sistema, recependo anche le indicazioni e i feedback dell'utente finale;
- rendere il sistema pronto all'uso e consegnare la documentazione tecnica, utente e di manutenzione che illustri tutte le configurazioni effettuate nelle specifiche attività che compongono l'avviamento;
- individuare le situazioni critiche di natura tecnica o organizzativa che potranno essere rilevate durante la fase di avviamento e che saranno analizzate per eventuali iniziative di approfondimento o miglioramento.

L'avviamento del sistema sarà considerato concluso nel momento in cui sarà stata perseguita le configurazione ottimale degli ambienti di esercizio, con l'obiettivo della massima stabilità e performance;

8.2.2 Documentazione del Sistema

La documentazione del Sistema da realizzare dovrà essere predisposta secondo gli standard indicati in seguito e dovrà raccordarsi al processo di sviluppo definito; la qualità della documentazione del sistema realizzato è considerata un aspetto estremamente rilevante della fornitura.

La produzione della documentazione dovrà avvenire nel rispetto delle richieste del Committente dovendo perseguire gli obiettivi di chiarezza, comprensione, utilizzo, manutenibilità ed estendibilità dei sistemi rilasciati.

In relazione alle specifiche del sistema, la documentazione dovrà essere realizzata in forma documentale in formato .rtf e .pdf secondo template concordati con il Committente ed allineati al processo di sviluppo.

I modelli e i diagrammi dovranno essere conformi all'attuale versione dello Unified Modeling Language (UML) utilizzando un set di diagrammi adeguato per rappresentare sia gli aspetti strutturali (sia a livello logico che di deployment) che comportamentali (behavior) del sistema complessivo e dei componenti.

Per la rappresentazione dei processi sarà utilizzato lo standard BPMN ver. 2.

Dovranno altresì essere forniti i manuali per l'attuazione dello scambio dati con altri sistemi come esplicitato nei requisiti.

I modelli dovranno essere rilasciati in formato .xml e tramite l'eventuale formato proprietario dello strumento di modellazione concordato all'inizio del progetto.

I manuali che si riferiscono all'utenza dovranno essere predisposti, in relazione ai ruoli definiti di concerto con l'Amministrazione, con una descrizione dettagliata dei processi e delle funzionalità resi disponibili dalle soluzioni realizzate; lo standard da utilizzare sarà lo SCORM, ver. 1.2 o superiore.

Il sorgente del codice sviluppato dovrà essere scritto a regola d'arte ed adeguatamente formattato e commentato.

Si riporta nel seguito il dettaglio della documentazione tecnica ritenuta, al minimo, come necessaria da produrre all'atto dell'avviamento:

- progetto esecutivo
- architettura di sistema
- architettura funzionale
- architettura applicativa
- architettura tecnologica
- modello dei dati (logico e fisico)
- specifiche funzionali di tutti gli sviluppi software realizzati
- piano di test e collaudo
- report dei test di fabbrica e di collaudo
- codice sorgente di tutti gli sviluppi software, commentato e mantenibile
- documentazione della configurazione di dettaglio di tutte le componenti hardware e software
- manuali utente
- manuale di gestione
- catalogo dei servizi
- catalogo dei webservice e dei parametri delle interfacce esposte

- piano di qualità
- piano di manutenzione periodica dei sistemi
- piano temporale di garanzia dei sistemi
- le certificazioni ed autocertificazioni prodotte dal Fornitore e richieste da norme di legge
- supporti (cd, dvd, ecc.) di installazione (da consegnare ad ogni fase di implementazione) completo di documentazione della procedura e degli script di installazione
- documentazione necessaria per la successiva implementazione di training e cd rom di autoformazione che saranno realizzati in altro ambito progettuale.

8.2.3 Principali garanzie di servizio della fase di implementazione

Il Fornitore, durante la fase di implementazione del progetto, si obbliga a rispettare i tempi e le scadenze definite nello schema tecnico-economico di cui all'art 16 comma 3 dello schema di contratto, con particolare riferimento ai deliverable ivi definiti ed approvati dal Committente.

8.3 Fase di gestione

8.3.1 Organizzazione della Fase di Gestione

La piena gestione dell'esercizio dei sistemi realizzati dovrà essere garantita per un periodo di almeno sei mesi solari e continuativi a partire dal collaudo con esito positivo.

Tre mesi prima del termine dello stadio di gestione il Fornitore dovrà inoltre consegnare tutta la documentazione necessaria alla presa in carico del sistema, al fine di permettere al Committente di operare una selezione di un nuovo fornitore dei servizi di gestione, per il periodo successivo a quello indicato nel presente bando.

8.3.2 Principi generali delle attività della Fase di gestione

Il Fornitore dovrà prevedere, al minimo, quanto di seguito indicato:

- dovrà essere conseguito il massimo coordinamento con il personale del Committente;
- dovranno essere prodotti reporting mensili che contengano, tra l'altro, gli SLA conseguiti;
- i servizi di security management, system & network management, assistenza hardware, assistenza sul software di base, di gestione operativa e di comunicazione dovranno essere erogati nella sede di Napoli ove è collocata la Sala Apparati ed i Sistemi di Energia, oltre che prevedere interventi nella sede di Gioia Tauro ove è installata la Sala Crisi;
- i servizi di assistenza inerenti le OBU dovranno essere erogati presso gli installatori/manutentori indicati in offerta;
- i servizi di assistenza all'utenza dovranno essere erogati presso una struttura collocata geograficamente presso una delle Regioni Obiettivo Convergenza nel solo caso in cui si garantisca una immediata comunicazione e accesso al sistema di trouble ticketing, ai tecnici dislocati nelle altre situazioni sopra indicate.

Le attività da svolgere nel corso della Fase di Gestione sono sommariamente descritte nella scheda seguente.

Gruppo di servizi	Dettaglio servizi
Security management	
System & Network Management	
Assistenza hardware	
Assistenza sul software di base	
Gestione operativa	Performance Management
	Job Scheduling
	Backup/Restore
	Accounting Management
	Capacity Management
	System Technical Support specifico per modulo di Intelligence
	System Technical Support specifico per OBU e comunicazioni
Servizi di comunicazione	
Servizio di assistenza agli utenti	Gestione Failure
	Front-level

8.3.3 Dettaglio dei servizi della Fase di Gestione

Di seguito sono raggruppati come servizi, le prestazioni minime che devono essere erogate dal Fornitore nella Fase di Gestione

8.3.3.1 Servizio di Security Management

Si richiede che il Fornitore gestisca gli aspetti legati alla sicurezza dei Sistemi e che in tale ambito provveda a quanto di seguito:

- progettazione del servizio di sicurezza, sulla base delle politiche concordate con il Committente;
- organizzazione dei processi di erogazione del servizio;
- preparazione documentazione di servizio;
- attivazione, esercizio e gestione del servizio.

8.3.3.2 Servizio di System & Network Management

Si richiede che il Fornitore gestisca il sistema e le comunicazioni di supporto, nella propria interezza, attraverso propri amministratori di sistema e fornisca una reportistica puntuale sui livelli di servizio offerti ed erogati.

Entro tre mesi prima del termine della fornitura, il Fornitore dovrà impegnarsi a fornire tutta la documentazione necessaria ad esercire il sistema di modo che il Committente sia pienamente autonomo nel poter identificare una struttura di terze parti per la fornitura dei servizi continuativi.

8.3.3.3 Servizio di assistenza hardware

Il Fornitore dovrà garantire un servizio di assistenza di carattere preventivo e/o adattativo su tutto l'hardware fornito nei termini di seguito indicati.

Le attività del servizio di assistenza hardware riguardano gli interventi on-site sugli apparati e sui dispositivi e consistono in:

- effettuare interventi proattivi su tutti gli apparati installati;
- individuare/identificare il problema e la sua risoluzione;
- inserire nel parco apparati e dispositivi forniti eventuali elementi aggiuntivi;
- eseguire attività di gestione dei guasti delle apparecchiature, anche interfacciandosi con gli eventuali fornitori delle garanzie e/o i produttori;
- ripristinare le funzionalità delle apparecchiature, qualora sia stata effettuata la sostituzione/acquisizione di dispositivi.

L'attività di assistenza hardware dovrà prevedere, oltre all'assistenza sugli apparati fisici nei termini sopra indicati, anche le connesse attività che riguardano i sistemi operativi, se necessario, e tutte le attività per mantenere le apparecchiature in condizione ottimale di efficienza.

Quanto descritto nel presente paragrafo non sostituisce, altera o modifica in alcun modo la garanzia prevista dalla Legge.

8.3.3.4 Servizio di assistenza sul software di base

Il Fornitore dovrà erogare questo servizio che ha le seguenti finalità:

- assistenza preventiva, con lo scopo di prevenire l'insorgere di malfunzionamenti mediante controllo del perfetto funzionamento e configurazione di tutte le componenti fornite; questo servizio dovrà prevedere una pianificazione degli interventi di prevenzione, con cadenza almeno bimestrale, da espletare presso tutte le sedi che erogano il servizio;
- assistenza adattativa, con lo scopo di adattare e aggiornare tutte le componenti fornite sulla base delle seguenti necessità: upgrade in seguito al passaggio a nuove versioni del software di base; installazione di patch (es. relative alla sicurezza) per il software di base; necessità di garantire l'operatività del sistema con nuovo software anche per l'entrata in esercizio di nuovi dispositivi così come ipotizzato nel precedente paragrafo 8.3.3.3.

Gli interventi di assistenza dovranno rispettare i livelli di servizio indicati nel capitolato, con particolare riferimento ai tempi di intervento ed alla disponibilità del sistema.

Quanto descritto nel presente paragrafo non sostituisce, altera o modifica in alcun modo la garanzia prevista dalla Legge.

8.3.3.5 Servizi di gestione operativa

I servizi richiesti si basano sulle seguenti linee di attività.

8.3.3.5.1 Performance Management

Monitoraggio del funzionamento dei sistemi, al fine di individuare tempestivamente situazioni anomale e colli di bottiglia ed attivare interventi operativi per garantire le condizioni ottimali di funzionamento.

8.3.3.5.2 Job Scheduling

Gestione sistemistica e controllo dei servizi batch e di trattamento dell'output, assicurando la pianificazione ed il controllo delle procedure per la gestione dei sistemi; modifica della schedulazione pianificata a fronte di una richiesta di variazione della stessa.

8.3.3.5.3 Backup/Restore

Attività per garantire la conservazione dei dati ed il ripristino dei medesimi predisponendo e controllando le procedure di salvataggio e di copia; attivazione di procedure di backup e restore straordinarie al fine di garantire la continuità del servizio agli utenti.

8.3.3.5.4 Accounting Management

Creazione, gestione e manutenzione degli account relativi al Sistema nella propria interezza e anche per quanto specificatamente necessario ai Sotto-Sistemi SiSS e SiLS, con controllo delle politiche di accesso e organizzazione e strutturazione in gruppi e contesti.

Le attività svolte in questo ambito devono necessariamente essere in armonia con quanto previsto per quelle del Servizio di Security Management sopra enunciate.

8.3.3.5.5 Capacity Management

Gestione procedure e attività, anche in modalità preventiva e proattiva, finalizzate alla riconfigurazione e all'eventuale potenziamento hardware o a miglioramenti software.

8.3.3.5.6 System Technical Support, specifico per modulo di Intelligence

Al fine di assicurare un adeguato servizio tecnico specialistico nelle attività di supporto, è prevista l'attivazione di un supporto specialistico di livello superiore, qualora fossero rilevati degli inconvenienti in merito al funzionamento specifico del modulo di Intelligence del SiSS

8.3.3.5.7 System Technical Support, specifico per OBU e comunicazioni

Allo stesso modo del precedente, è prevista l'attivazione di un supporto specialistico di livello superiore, qualora fossero rilevati degli inconvenienti in merito al funzionamento specifico delle OBU e delle comunicazioni delle stesse con il Centro di elaborazione e memorizzazione dei dati.

8.3.3.6 Servizi di comunicazione

E' richiesto al Fornitore di fornire servizi di configurazione del networking (lan locale, accesso internet, ecc.), e di interoperabilità (ad esempio, i servizi di indirizzamento, domain name service, directory service, tempo ufficiale di rete, system management & network, ecc.).

8.3.4 Servizio di assistenza agli utenti

Il Fornitore dovrà fornire un servizio di assistenza agli utenti, sempre nell'ambito della Fase di Gestione, per una durata temporale equivalente alla stessa.

Tutti i prodotti software oggetto della fornitura, prioritariamente evidenziando quello di trouble ticketing, posti in esercizio dal Fornitore dovranno essere assistiti e manutenuti almeno fino al termine del periodo di erogazione del servizio.

Nel periodo di erogazione del servizio di assistenza all'utenza, il Fornitore dovrà assicurare una tempestiva correzione degli errori e delle disfunzioni, segnalate sia tempestivamente dalla struttura di monitoring del Fornitore, sia dagli utenti che utilizzeranno il sistema.

La disponibilità complessiva del servizio deve essere non inferiore al 98,00% nell'arco di ogni trimestre.

Il servizio si intenderà a totale copertura delle spese necessarie per gli interventi di assistenza e manutenzione, eventuale addestramento suppletivo del personale all'uso delle nuove funzionalità introdotte, spese di trasporto ed altro materiale necessario alla manodopera, spese di viaggio e soggiorno del personale addetto all'intervento.

Si intendono come parte del servizio di assistenza agli utenti i servizi di seguito indicati.

8.3.4.1 Gestione Failure

Nel caso in cui il sistema incorra in un failure tale da provocare il fermo dello stesso si deve garantire che non siano persi messaggi e che, al ripristino del sistema, la situazione preesistente sia recuperata.

Si vuole qui ancora indicare che il sistema costituisce un'infrastruttura destinata al supporto delle attività senza soluzione di continuità e, pertanto, deve essere gestito in un'ottica mission critical.

8.3.4.2 Front-level

Il servizio di assistenza, con l'obiettivo di garantire i livelli di servizio concordati, deve provvedere a:

- assicurare la comunicazione tempestiva ed efficace con l'utenza del sistema;
- provvedere all'accoglimento ed alla registrazione delle richieste di assistenza;
- risolvere i problemi più ricorrenti, di non elevata complessità;
- smistare a strutture di assistenza specifiche la risoluzione di incidenti e problemi non risolvibili al primo livello, ad esempio attivando le citate assistenze sull'hardware e il software di base;
- controllare i processi di risoluzione attivati e verificarne gli esiti;
- rendicontare all'utente sullo stato dell'intervento;
- analizzare le statistiche sugli interventi, al fine di identificare i fabbisogni e definire azioni di prevenzione di incidenti e problemi.

Il Fornitore deve disporre di strumenti di supporto adeguati che consentano di classificare e gestire gli incidenti, mediante un apposito sistema di trouble ticket.

Il sistema di trouble ticket dovrà permettere di registrate e catalogare almeno le seguenti informazioni:

- data e ora della richiesta di intervento;
- data di apertura del ticket;
- utente che ha segnalato l'incidente/problema;
- descrizione della segnalazione;
- descrizione dell'intervento;
- data di chiusura (risoluzione del incidente/problema);
- livello di criticità attribuito al incidente/problema.

La gestione degli Incident Report dovrà comprendere eventuali test d'integrazione e di non regressione.

8.3.5 Principali garanzie di servizio nella Fase di Gestione

Il Fornitore deve offrire il servizio di gestione nel corso della Fase, tenendo conto della priorità del perseguimento della Customer Satisfaction.

In tal senso, l'erogazione minima dei servizi dovrà prevedere un profilo temporale pari a H12 per cinque giorni feriali.

Si ritiene, pertanto, che il Committente sarà posto in condizione di avere sempre la disponibilità di un Referente del Fornitore, per ogni tipologia di servizio svolto nella Fase di gestione da parte di quest'ultimo.

Le richieste dei responsabili del Committente dovranno avere la certezza della reperibilità dei referenti del Fornitore che saranno attivati via telefono ovvero mail.

9. DEFINIZIONE DELLA FORNITURA

9.1 Oggetto della fornitura

Sono oggetto di fornitura i servizi elencati nella tabella che segue; nella prima colonna si fa riferimento ai Lemmi del Dizionario ICT di cui a *http://www.digitpa.gov.it/qualitaICT/elenco_lemmi_qualita_ICT*.

#	Lemma	Fase di implementazione	Fase di Gestione	
1	PGE Gestione e processi organizzativi	Servizi di consulenza e supporti: Project Management		
2	PAQ Assicurazione della Qualità	Servizi di consulenza e supporti: elaborazione del Piano di Progetto (comprensivo del Progetto di Dettaglio e del Piano della Qualità)		
3	SSW Sviluppo e MEV di software ad hoc	Sviluppo sistemi software delle componenti SILS e SISS		
4	SSC Sviluppo e MEV mediante soluzioni commerciali	Integrazione componenti applicative e applicazione soluzioni: architettura SOA		
5		Integrazione componenti applicative e applicazione soluzioni: On Board Unit		
6	FPD Fornitura Prodotti HW e SW	Fornitura Hw e Sw di base		
7		Fornitura e configurazione Moduli di Intelligence per SiSS		
8	GSI Gestione sistemi		Security management	
			System & Network Management	
			Assistenza hardware	
			Assistenza sul software di base	
			Gestione operativa	Performance Management
				Job Scheduling
				Backup/Restore
				Accounting Management
				Capacity Management
9	GSW Gestione applicativi e Basi Dati		Gestione operativa	System Technical Support specifico per modulo di Intelligence
10	GMR Gestione e			System Technical

	manutenzione reti			Support specifico per OBU e comunicazioni
			Servizi di comunicazione	
11	ASS Assistenza in remoto e in locale		Servizio di assistenza agli utenti	Gestione Failure
				Front-level
12		Fornitura apparati non IT		
13		Fornitura sala apparati e sistemi di energia		
14		Fornitura sala crisi		

9.2 Struttura di coordinamento e profili professionali richiesti

9.2.1 Organizzazione del Committente

Il Committente svolge attività di supervisione e controllo del progetto includendo attività di:

- pianificazione degli obiettivi da raggiungere, relativamente al progetto;
- controllo delle attività progettuali e delle attività di gestione del servizio;
- partecipazione ai test finali ed ai collaudi e di supporto alla valutazione finale;
- accettazione dei deliverable prodotti dal Fornitore;
- reporting di progetto tramite la raccolta ed evidenziazione dei dati di avanzamento lavori e degli elementi necessari alla valutazione dei risultati;
- controllo qualità.

9.2.2 Organizzazione del Fornitore

Il Fornitore ha in carico l'intero progetto e svolge le varie attività per realizzarlo sino alla messa a punto dei prototipi finali ed alla loro gestione oltre che al passaggio in produzione dell'intero Sistema.

Più in dettaglio le attività previste sono:

- il project management con la supervisione della progettazione di dettaglio e della sperimentazione delle varie componenti prototipali, supervisionando i vari elementi che costituiscono il progetto complessivo, controllandone la pianificazione di dettaglio e partecipando al disegno di dettaglio;
- system integration del progetto, con l'obiettivo di garantire la coerenza delle soluzioni progettuali adottate e delle scelte definite nei documenti di progetto, effettuando i test di integrazione a livello del sistema complessivo anche gestendo l'ambiente di prova (test bed d'integrazione);
- gestione dell'applicazione del sistema di qualità e dei piani di qualità;
- realizzazione e gestione del change management (cioè la gestione del ciclo di vita di prodotti e servizi), che comprende l'attività di provisioning (cioè la gestione di nuove adesioni e dismissioni);
- realizzazione e gestione dei servizi e dell'integrazione con i sistemi applicativi degli utenti, effettuando l'analisi funzionale e partecipando allo sviluppo del software fino alla presa in carico;
- realizzazione e gestione del sistema, nei suoi vari componenti.

Il Fornitore:

- progetta e mette a disposizione i prodotti relativi alle infrastrutture tecnologiche, anche impiegando eventuali semilavorati già disponibili come risultato di altre ricerche e progetti;
- garantisce lo sviluppo software ed integrazione con i sistemi applicativi degli utenti e gli altri sviluppi software necessari;
- collabora alla system integration e al project management;
- fornisce inoltre consulenza e supporto tecnico/operativo per l'organizzazione dei processi relativi ai servizi a supporto e aggiuntivi sino a rendere UIRNet autonoma nella gestione operativa del servizio;
- supporta le attività di gestione di UIRNet.

9.2.2.1 Gestione delle attività di Project management

Il Fornitore si farà carico del project management, nominando un responsabile di progetto che coordinerà i vari responsabili dei moduli di progetto.

Il responsabile di progetto provvederà a riportare lo stato di avanzamento mediante la redazione di un gantt di progetto (con indicazione dei costi, tempi, propedeuticità delle attività, risultati, rischi) e di una analisi dei rischi di progetto con una rendicontazione mensile dello stato di avanzamento (status report) completa di aggiornamento dello stesso gantt, dello stato delle azioni decise (issue & action log) e del registro dei rischi.

Il Committente supervisionerà l'avanzamento di progetto nominando una figura di responsabile ed un eventuale tavolo di steering committee.

Il Fornitore dovrà inoltre gestire l'integrazione del Sistema dei diversi moduli applicativi programmando e gestendo sia le attività verso i team che gestiscono i servizi di nodo sia verso i team che stanno realizzando la PLN e i servizi di connettività, includendo tutti gli aspetti legati ai servizi da erogare al completamento del progetto.

Nell'ambito del processo di sviluppo il Fornitore dovrà gestire le change request e la documentazione di progetto complessiva.

Per la gestione dell'intero progetto sarà costituita una struttura di coordinamento secondo lo schema riportato di seguito.

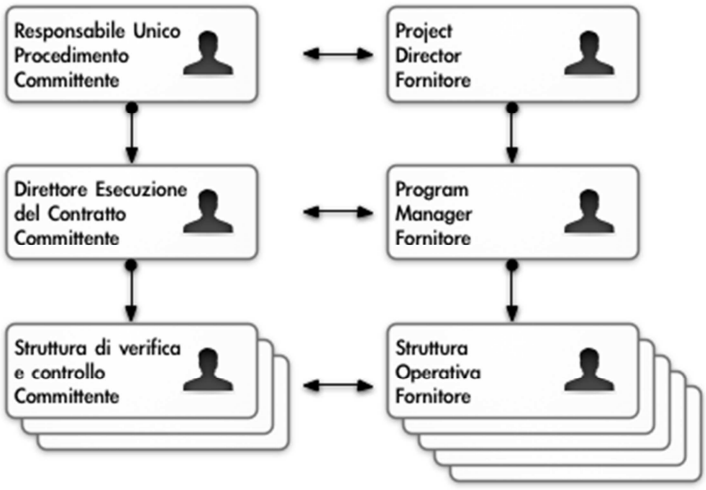

Figura 12 - Struttura di coordinamento del progetto

9.2.2.2 Requisiti richiesti per le Figure Professionali

Di seguito, sono indicati i requisiti richiesti per le varie figure professionali, qualora inserite nella struttura di progetto del Fornitore.

In considerazione degli obiettivi del progetto, il team di consulenza dovrà comprendere risorse di elevata seniority a cui è richiesta, tra l'altro, una provata competenza nell'ambito della progettazione ed implementazione di architetture SOA/ESB.

Al momento dell'offerta il Fornitore dovrà presentare i curricula delle risorse professionali del gruppo di lavoro proposto.

Nella proposta il Fornitore dovrà prevedere la copertura almeno dei ruoli di seguito indicati, e un dimensionamento di risorse professionali adeguato allo svolgimento delle attività precedentemente descritte.

Alcuni dei ruoli dovranno essere coperti, secondo il contesto, anche da personale con una specifica competenza ai fini coprire parti della fornitura (ad es. sicurezza).

Revisore di Sistemi Informativi	Fornisce (riferendo ai più alti responsabili aziendali o agli organi direttivi) un livello indipendente di garanzia su sicurezza, qualità, conformità e valore aggiunto dei sistemi informativi in una particolare organizzazione. Deve dimostrare forti competenze tecniche, indipendenza di giudizio, aderenza all'etica professionale. Tipicamente questo profilo di competenza trova applicazione nei processi di quality assurance e nella gestione della configurazione.
Consulente per la vendita e l'applicazione di Tecnologie Informatiche	Deve abbinare alla competenza in una specifica tecnologia (legata al contesto, es. CAD) anche la conoscenza di concetti avanzati di marketing e delle esigenze tipiche dei clienti. E' indispensabile l'efficacia persuasiva nel presentare soluzioni, dimostrazioni pratiche e proposte commerciali.
Capoprogetto di Sistemi Informativi	Deve essere molto efficace nell'organizzare le risorse umane e tecniche per il raggiungimento degli obiettivi sostanziali del progetto, nel rispetto dei vincoli concordati di qualità, tempi e costi. E' richiesta una particolare competenza delle tecniche di gestione dei progetti (sia nel caso di soluzioni preconfezionate, sia per sviluppi personalizzati), oltre ad una vasta conoscenza dell'ICT e dei sistemi informativi.
Analista di Sistemi Informativi	Deve essere molto efficace nell'identificare i requisiti per i sistemi ICT e nel definire modelli di flussi informativi e di oggetti da gestire. Ad una competenza ICT ampia ed approfondita deve essere abbinata la capacità di interagire con utenti e colleghi. Questo profilo mostra numerose analogie con l'Analista di Business con il quale condivide numerose categorie di conoscenza. Si differenziano invece le attività in cui tipicamente sono impegnati. Nel contesto delle acquisizioni delle pubbliche amministrazioni, può essere più usuale la richiesta di una figura professionale che combini le competenze di questi due profili.
Analista Programmatore	Assume un ruolo tecnico di rilievo nella progettazione di sistemi informativi e deve essere molto efficace nella realizzazione e manutenzione di moduli software complessi, che tipicamente dovranno essere integrati in un più ampio sistema informativo.

	Sono possibili diverse specializzazioni, sia nel campo degli applicativi e dei servizi web, sia nel software a livello di sistema.
Tecnico di Collaudo e Integrazione di Sistemi	Deve essere molto efficace in varie aree dello sviluppo di sistemi: preparazione della documentazione per l'utente finale, allestimento di sistemi ICT, test delle loro funzioni, sia nel complesso che per singoli moduli componenti, identificazione delle anomalie e diagnosi delle possibili cause. È richiesta anche una conoscenza specifica su come vengono costruite le interfacce tra moduli software. Nella generalità delle acquisizioni di servizi ICT da parte delle amministrazioni, si rileva normalmente che al profilo di analista programmatore vengono attribuite anche le competenze del profilo TCI.
Progettista di Sistemi Informatici	Assume un ruolo centrale nella progettazione, integrazione e miglioramento di sistemi IT – con particolare riguardo alle architetture software – curandone anche la sicurezza e le prestazioni; oltre ad una vasta competenza dell'ICT (in tutti i campi: software, hardware e reti) e di tecniche di progettazione specifiche, è richiesta la capacità di descrivere un sistema in termini di componenti e flussi logici.
Progettista delle Telecomunicazioni	Deve abbinare alle competenze in TLC anche una particolare efficacia nell'identificare e mettere in opera soluzioni IT per la convergenza digitale. E' richiesta una profonda competenza di comunicazione digitale senza fili su mezzi analogici, così come di trasferimento di segnali analogici su reti digitali. Sono inoltre importanti le competenze professionali per la consulenza e una competenza generale nello sviluppo di sistemi.
Progettista per la Sicurezza	Deve essere molto efficace nell'identificare i requisiti di sicurezza dei sistemi ICT e nel definire soluzioni affidabili e agevoli da gestire. Ad una competenza dell'ICT ampia e approfondita deve essere abbinata la capacità di interagire con altre funzioni ICT per favorire l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT.
Responsabile della Configurazione e del Centro Dati	Deve avere un approccio strutturato alla progettazione, allestimento e manutenzione di un ambiente di lavoro supportato dall'ICT, sia nel caso di un ambiente di sviluppo, sia nel caso di un sistema "in produzione" destinato agli utenti finali; è richiesta una particolare competenza sulle procedure di qualità e su strumenti e sistemi di gestione procedurale delle attività.
Responsabile di Basi di Dati	Assume un ruolo centrale tanto nella progettazione di strutture di dati quanto nella gestione ordinaria dei DB; tra i requisiti figurano dunque una profonda competenza in tutti gli aspetti delle tecnologie dei DB, un approccio collaborativo ai contesti di progetto, esperienza nelle tecniche di modellazione dei dati, ma anche l'efficacia nel definire e applicare le procedure e nell'organizzare le operazioni ordinarie. Si rileva che nel contesto delle acquisizioni ICT delle amministrazioni, questo profilo svolge anche le attività più "tecniche" normalmente attribuite al DB Administrator.
Responsabile di Rete	Deve essere molto efficace nel gestire un sistema informativo di rete di media complessità e nel migliorarne le prestazioni.

	Deve inoltre saper interagire con i progettisti di reti e con eventuali fornitori esterni in merito a tutte le fasi del ciclo di vita di una rete.
Supervisore di un Centro di Assistenza	Deve essere efficace nel fornire supporto tecnico; ciò richiede competenza di una tecnologia specifica (legata al contesto, es. servizi in rete), ma anche dimestichezza con contratti SLA, consapevolezza delle priorità operative nell'attività del Cliente e delle problematiche tipiche degli utenti, così come un atteggiamento positivo nel reagire ai problemi e nel rapportarsi con il Cliente.
Sistemista	Deve avere una particolare competenza su vari sistemi operativi e sui rispettivi metodi per affrontare i problemi, sull'ottimizzazione delle prestazioni, sulla programmazione a livello di sistema e sull'integrazione tra piattaforme diverse; l'attitudine alla diagnosi e alla risoluzione dei problemi è richiesta per dare supporto su sistemi proprietari o aperti e su configurazioni ibride.

9.3 Composizione dei gruppi di lavoro

Di seguito si riporta, per ognuno dei servizi di cui alla tabella al par. 9.1 “Oggetto della fornitura”, il mix relativo alle diverse figure professionali, considerato come ottimale in base alle schede servizi in appendice.

	PGE	PAQ	SSW	SSC	FPD	GMR	GSI	GSW	ASS
			(misure espresse in percentuali)						
Analista di Sistemi Informativi			21,5						
Analista Programmatore			15,5						
Capo Progetto di Sistemi Informativi	64,2	2,5							
Consulente per la Vendita e l’Applicazione di Tecnologie Informatiche	0,8		1,0	68,0	3,3	1,3	0,9	1,1	2,0
Personale esecutivo					51,7	13,1	25,5		16,0
Progettista delle Telecomunicazioni						1,3			
Progettista di Sistemi Informatici	0,8			2,0			7,7		
Progettista per la sicurezza	0,8		1,5			1,3		1,1	1,0
Responsabile della Configurazione e del Centro Dati	3,3		5,0	6,0	35,0		31,8	65,0	
Responsabile di Basi di Dati	5,0		7,0	4,0			4,1	25,0	4,0
Responsabile di Rete	5,0		4,0			51,3	0,9		
Revisore di Sistemi informativi	16,7	97,5							
Sistemista	1,7		4,0	4,0			8,6		
Supervisore di un Centro di Assistenza			2,0	4,0		21,9	8,2	3,3	75,0
Tecnico di Collaudo e Integrazione di Sistemi	1,7		38,5	13,0	10,0	10,0	12,3	4,4	2,0

I mix riportati nella tabella precedente sono quelli ritenuti ottimali dal Committente, tuttavia il fornitore può variarne la composizione sia pur in misura contenuta e coerente con le percentuali di impiego generalmente utilizzate per risorse di servizi analoghi, per modulare i gruppi di lavoro secondo la propria usuale organizzazione lavorativa, garantendo comunque la qualità del servizio prestato.

Eventuali scostamenti, nel corso delle Fasi di Implementazione e/o di Gestione, dovranno essere preventivamente comunicati e motivati dal Fornitore e accettati dal referente della Committente.

9.4 Valorizzazione del Punto Funzione

Per gli obiettivi misurati in Punti Funzione:

- la produttività, calcolata come valore medio su tutti i servizi di sviluppo e manutenzione evolutiva, è pari a 1,7 Punti Funzione/Giorno Uomo.

9.5 Servizi oggetto di fornitura

Rimandando per il dettaglio alle schede in appendice, si forniscono di seguito le informazioni prioritarie che concernono i vari servizi elencati nella tabella di cui al precedente par. 9.1 “Oggetto della fornitura”.

9.5.1 Servizi di consulenza e supporti

Per il servizio di consulenza si intendono le seguenti attività che di norma non modificano la baseline del sistema:

- attività di project management con la supervisione della progettazione di dettaglio e della sperimentazione delle varie componenti prototipali, supervisionando i vari elementi che costituiscono il progetto complessivo, controllandone la pianificazione di dettaglio e partecipando al disegno di dettaglio;
- attività di progettazione di dettaglio, gestione dell’applicazione del sistema di qualità e dei piani di qualità; system integration del progetto, con l’obiettivo di garantire la coerenza delle soluzioni progettuali adottate e delle scelte definite nei documenti di progetto, effettuando i test di integrazione a livello del sistema complessivo anche gestendo l’ambiente di prova (test bed d’integrazione);

L'elenco non si può considerare esaustivo ed immutabile, ma potrà subire delle revisioni nel periodo di validità contrattuale per comprendere attività affini e comunque orientate a supportare lo sviluppo, la manutenzione e la gestione del Sistema.

I servizi di consulenza sono dimensionati in un massimale di Giorni Uomo stimato in base alle necessità delle singole applicazioni.

Si tratta di valori medi stimati al meglio delle conoscenze attuali, delle esigenze utente e della relativa evoluzione pianificata.

Al mutare delle esigenze, e perciò delle risorse impegnate, in quantità e qualità, il piano potrà essere rivisto ed aggiornato, come regolato a contratto, nel limite del massimale di Giorni Uomo prestabilito.

Per approfondimenti si rimanda alle allegate schede di descrizione delle componenti:

- PGE Gestione e processi organizzativi;
- PAQ Assicurazione della Qualità.

9.5.1.1 Dimensioni del Servizio

Il servizio di consulenza e supporto è dimensionato in un massimale di 233 GG.U. per la figura di Project Manager e 317 GG.U. per la componente di fornitura relativa al Progetto di dettaglio e al Piano della qualità (Piano di Progetto).

9.5.2 Sviluppo sistemi software delle componenti SiLS e SiSS

Il servizio di Sviluppo sistemi software delle componenti SiLS e SiSS si riferisce alla realizzazione di prodotti software volti a soddisfare le esigenze espresse dalla Committente.

Nella fattispecie, sono inclusi in questo servizio:

- Sviluppo di software ad hoc, che comprende lo sviluppo dei sistemi informativi come dettagliati ai capitoli 4 e 5. E' incluso lo sviluppo di applicazioni secondo vari metodi, mezzi e modalità, singolarmente o in modo congiunto, in dipendenza dagli obiettivi, funzionali o meno, richiesti dalla Committente;
- Integrazione di componenti applicative individuate per l'implementazione dell'Architettura SOA e personalizzazione delle soluzioni individuate per le OBU

Il Fornitore è tenuto a fornire tutti gli elementi di misurazione necessari a mantenere aggiornata la baseline.

Per approfondimenti si rimanda alle allegate schede di descrizione delle componenti:

- SSW Sviluppo e MEV di software ad hoc;
- SSC Sviluppo e MEV mediante soluzioni commerciali.

9.5.2.1 Dimensioni del Servizio

Il servizio di Sviluppo e Mev di software ad hoc è dimensionato in un massimale di Punti Funzione (PF).

La valutazione della dimensione dei servizi per le aree SiLS e SiSS è stata realizzata attraverso l'uso del calcolo dei Punti Funzione, metodo Early&Quick Function Point.

Il massimale di impegno in PF previsto per lo sviluppo di software ad hoc suddiviso per Area di attività è pari a 909 Punti Funzione per l'Area SiSS e 3.387 per l'Area SiLS,

La ripartizione dei massimali per Area non è vincolante; è stimata al meglio delle conoscenze attuali e, pertanto, sarà possibile una diversa ripartizione dei massimali, nel corso della durata contrattuale, sempre nel rispetto del massimale globale del servizio.

La componente di fornitura relativa all'Integrazione delle componenti applicative e personalizzazione delle soluzioni è stata dimensionata in 549 Giorni Uomo in relazione all'impegno per la realizzazione dell'Architettura SOA ed in 330 Giorni Uomo per lo sviluppo del software delle OBU.

9.5.3 Fornitura Hw e Sw

La classe di Fornitura Hw e Sw include le attività relative all'acquisto, la consegna, l'installazione ed il collaudo di prodotti hardware e/o di prodotti software.

Un prodotto hardware può essere genericamente un personal computer, un sistema server, un dispositivo di rete, una stampante o qualsiasi accessorio come scanner e periferiche.

Con il termine prodotto software si intende in questa classe il software di base, il software d'ambiente ed il software di rete.

Ognuna delle tipologie sopra riportate svolge specifiche funzioni nell'ambito di un sistema informatico:

Nella fattispecie, sono inclusi in questo servizio:

- la fornitura di HW; include la fornitura dei dispositivi che realizzano la Storage Area Network, la rete di interconnessione interna, le unità di switching ed i firewall di protezione perimentrale; macchine server in configurazione cluster; n. 50 On Board Unit (OBU); n. 70 Tablet 7 e 10 pollici;
- l'acquisto di prodotti SW e personalizzazioni; include la fornitura del prodotto per modulo intelligence SISS, inclusi i servizi di configurazione, le licenze Tele Atlas, l'acquisto di licenze del/dei sistemi operativi;
- ogni altro software di base (ad es. DBMS) che il Fornitore riterrà utile per il funzionamento della soluzioni che intenderà proporre oltre che quanto necessario per tutte le funzioni di sicurezza ed integrità (ad es. anti-virus, ecc.).

Per approfondimenti si rimanda alle allegate schede di descrizione delle componenti:

- FPD Fornitura Prodotti HW e SW.

9.5.3.1 Dimensioni del Servizio

Per lo svolgimento del servizio sono previsti 43 GG.U. di attività.

9.5.3.2 Requisiti Hw e Sw

Tutte le licenze d'uso relative ai sistemi devono essere permanenti, irrevocabili e non esclusive; concesse a titolo definitivo e con durata perpetua.

Le licenze d'uso devono coprire l'intera configurazione e dimensionamento proposto.

L'offerta deve includere anche le licenze d'uso per gli ambienti di sviluppo e staging.

Deve essere inclusa inoltre la manutenzione delle licenze per l'intera durata del contratto.

Nel pieno rispetto della regole sancite in ambito di OpenPA, e di quanto già cennato in precedenza, le forniture di software di base potranno essere realizzate con l'utilizzo di prodotti Open Source.

9.5.4 Fornitura apparati non IT

La classe di Fornitura apparati non IT include le attività relative all'acquisto, la consegna, l'installazione ed il collaudo dei seguenti prodotti tecnologici da installare a bordo di automezzi di trasporto merci:

- un primo dispositivo, connesso alla OBU, consiste in un telecomando portatile che consente l'invio semplice e rapido di un allarme per richiesta di intervento, funzionante anche se il conducente si trova all'esterno del veicolo;
- per esigenze logicamente simili, si prevede anche un secondo dispositivo, consistente in un congegno per la segnalazione dello stato di uomo-a-terra, similmente a quelli già in uso in molte attività professionali come, ad esempio, il settore cantieristico.

I citati dispositivi saranno a disposizione del conducente che, solamente se lo riterrà necessario, sceglierà l'eventuale attivazione ed utilizzo secondo la esigenze che egli stesso ravviserà nel corso delle proprie attività.

- un terzo dispositivo è il ricevitore del segnale di posizionamento trasmesso da costellazioni satellitari per determinare la posizione del veicolo, velocità e direzione. Il ricevitore dovrà gestire la correzione degli eventuali errori indotti dai sistemi, qualora sussistano, per limitare la precisione d'uso nei sistemi civili; ad esso dovrà essere associato un quarto dispositivo (munito almeno di un odometro ed una bussola) per consentire la navigazione stimata.
- un quinto dispositivo consiste in una telecamera, installata a bordo, che riprende la strada di fronte al veicolo; la funzione della stessa è intuitiva, a vantaggio del conducente ma anche per offrire la possibilità di accedere ad informazioni utili da parte delle Forze dell'Ordine;
- un sesto e ultimo dispositivo consiste in un lettore di dispositivi a tecnologia RFID (Radio Frequency IDentification) che comunica con elementi (ad esempio, fascette e targhette) che possono essere applicate al carico trasportato;
- ultimo dispositivo che svolge il compito di sensore inerziale tale da rilevare il movimento del veicolo.

9.5.5 Fornitura Sala Crisi

La classe di Fornitura Sala Crisi include le attività relative all'acquisto, la consegna, l'installazione ed il collaudo di prodotti tecnologici, oltre che la realizzazione di opere di attrezzaggio dei locali.

La Sala Crisi sarà collocata in un idoneo ambiente da attrezzare e da collocare all'interno dell'Area Portuale di Gioia Tauro, in spazi idonei messi a disposizione dall'Autorità Portuale presso la palazzina della ex-sede della suddetta Autorità.

Sarà cura del Fornitore proporre e dettagliare l'intervento tecnologico, infrastrutturale, di arredo ed impiantistico che si intende proporre per i locali in argomento, tenendo conto del requisito minimo descritto nel presente capitolato.

9.5.6 Fornitura sala apparati e sistemi di energia

La classe di Fornitura Sala Apparati e Sistemi di Energia include le attività relative all'acquisto, la consegna, l'installazione ed il collaudo dei prodotti tecnologici, oltre che la realizzazione di alcune opere di attrezzaggio dei locali.

La Sala Apparati e la Sala Energia dovranno essere allestite presso i locali del Centro di Elaborazione Dati della Direzione Interregionale per la Campania e la Calabria dell'Agenzia delle Dogane e dei Monopoli e dei Monopoli, con sede in Napoli.

Sarà cura del concorrente proporre e dettagliare l'intervento tecnologico, infrastrutturale, di arredo ed impiantistico che si propone per i locali in argomento.

9.5.7 Servizi di gestione operativa

Il servizio di Gestione comprende l'insieme di attività, risorse e strumenti di supporto per consentire la corretta operatività dei sistemi di elaborazione.

E' richiesto al Fornitore di eseguire le attività sotto elencate, che sono da ritenersi non esaustive.

In particolare il servizio prevede le seguenti forniture:

- la gestione dei sistemi (GSI), che include:
  - attività di gestione operativa:
    - performance management;
    - job scheduling;
    - backup/restore;
    - accounting management;
    - capacity management;
  - security management:
    - progettazione del servizio di sicurezza, sulla base delle politiche concordate con il Committente;
    - organizzazione dei processi di erogazione del servizio;
    - preparazione documentazione di servizio;
    - attivazione, esercizio e gestione del servizio.
  - system & network management;
  - assistenza hardware:
    - interventi proattivi sugli apparati;
    - individuazione dei problemi e soluzioni;
    - gestione delle apparecchiature e guasti;
    - rispristino delle funzionalità.
  - assistenza su software di base;
    - preventiva, attraverso la pianificazione degli interventi pianificati;
    - adattativa, attraverso applicazioni patch, upgrade a nuove versioni.
- servizio di assistenza agli utenti (ASS), che include:
  - la gestione del front-level attraverso:
    - l'accoglimento e la registrazione delle richieste di assistenza;
    - la risoluzione dei problemi più ricorrenti, di non elevata complessità;
    - lo smistamento a strutture di assistenza specifiche la risoluzione di incidenti e problemi non risolvibili al primo livello;
    - il controllare dei processi di risoluzione attivati e verificarne gli esiti;
    - la rendicontare all'utente sullo stato dell'intervento;
    - l'analisi delle statistiche sugli interventi, al fine di identificare i fabbisogni e definire azioni di prevenzione di incidenti e problemi;
  - la gestione delle failure, garantendo:
    - il ripristino della situazione del sistema;
    - il recupero totale dei dati e delle transazioni.
- servizio di assistenza e supporto sistemistico specifico per modulo di intelligence (GSW);
- servizio di assistenza e supporto sistemistico specifico per OBU (GMR).

Per approfondimenti si rimanda alle allegate schede di descrizione delle componenti:

- GSW Gestione applicativi e Basi Dati;
- GSI Gestione sistemi;
- GMR Gestione e manutenzione reti;
- ASS Assistenza in remoto e in locale.

9.5.7.1 Dimensioni del Servizio

Il servizio di gestione operativa dovrà essere erogato per un periodo di 6 mesi successivo al rilascio in esercizio delle applicazioni collaudate.

Per questo, sono previsti 141 GG.UU. per il servizio GMR, 146 GG.UU. per il servizio GSI, 127 GG.UU. per il servizio GSW.

Per quanto, invece, concerne il servizio di assistenza agli utenti, ASS, è stata prevista la presenza di tre risorse per un totale di 476 GG.UU. a seguito del calcolo secondo la formula cd. Erlang B, impostata sui seguenti principali parametri:

- Livello di servizio pari al 98%

- tempo medio di risposta pari a 20 secondi
- stima della media delle chiamate in un'ora in numero di 10
- durata media della chiamata pari a 180 secondi.

9.6 Criteri generali di quantificazione dei servizi

Nella tabella principale di valutazione economica di cui al seguente paragrafo, sono indicati gli elementi che fanno parte della fornitura.

Per quanto concerne i servizi, si fornisce, altresì, il dimensionamento stimato, da intendersi come massimale, di Punti Funzione o Giorni Uomo previsti per l'intera fornitura.

Come già in più punti ribadito, si tratta di valori valutati al meglio delle conoscenze attuali, tenendo presente anche i contenuti di innovazione che contrassegnano questo progetto, per i quali sono state espresse quantificazioni in base a quanto già misurato in realizzazioni con caratteristiche similari, in analoghi segmenti tecnologici.

In nessun caso questi valori sono considerati, presi singolarmente, un obbligo ovvero un vincolo da parte della Committente ed il Fornitore, nella propria valutazione di offerta, dovrà tenere conto del prezzo a base d'asta come unico massimale vincolante.

9.7 Tabella di valutazione economica

Nei par. 10.1 e seguenti sono riportati i criteri di valutazione delle offerte che saranno presentate dal Fornitore.

Allo stesso modo, nel disciplinare di gara sono dettagliati, al capo 4, i contenuti dell'offerta economica che dovrà essere formulata nell'ambito complessivo dell'offerta.

Di seguito, a completamento e chiarimento dei paragrafi precedenti, si riporta comunque la tabella principale di valutazione economica, nella quale sono ribaditi – per una migliore comprensione e continuità di lettura - gli elementi che compongono l'offerta.

			Importo netto totale	***Importo con IVA totale***
Sezione 1 - Tariffe unitarie				
U.M.	Figura professionale		Tariffa unitaria	
G.U.	Analista di Sistemi Informativi			
	Analista Programmatore			
	Capo Progetto di Sistemi Informativi			
	Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche			
	Personale esecutivo			
	Progettista delle Telecomunicazioni			
	Progettista di Sistemi Informatici			
	Progettista per la sicurezza			
	Responsabile della Configurazione e del Centro Dati			

	Responsabile di Basi di Dati			
	Responsabile di Rete			
	Revisore di Sistemi informativi			
	Sistemista			
	Supervisore di un Centro di Assistenza			
	Tecnico di Collaudo e Integrazione di Sistemi			
Punto funzione per sviluppo applicazioni (PF)				

Sezione 2 - Prezzi complessivi delle attività oggetto di fornitura e prezzo globale offerto

	Servizio / U.M.	Quantità	Prezzo totale	
1	PGE/PAQ – Project Management			
	Giorni uomo	233		
2	PGE/PAQ - progettazione dettaglio / piano qualità			
	Giorni uomo	317		
3	SSW – sviluppo sistemi software delle componenti SiLS e SiSS			
	Punto funzione	4.296		
4	SSC – integrazione componenti applicative: On Board Unit			
	Giorni uomo	330		
5	SSC – integrazione componenti applicative: architettura SOA			
	Giorni Uomo	549		
6	FPD – Fornitura hw e ws di base			
	Giorni uomo	43		
7	fornitura di prodotto e configurazione Modulo Intelligence SiSS			
	Fornitura licenza e configurazione	a corpo		

	Servizio	Ris. MIN	GG. UU.	Durata	Prezzo totale	
8	ASS – Assistenza utenti	3	476	6 mesi		
9	GMR – Management Reti	1	141	6 mesi		
10	GSI – Gestione sistemi	1	146	6 mesi		
11	GSW – Gestione applicativi e DB	1	127	6 mesi		

Sezione 3 - Forniture hardware e software di base

	Fornitura/U.M.	Quantità	Prezzo totale	
12	fornitura di server completi di supporto di memoria, apparati attivi, software di base oltre che della Sala Apparati e Sala Energia			
	Prezzo totale per hw e sw di base	a corpo		

13 fornitura di OBU unità centrale, di comunicazione e dispositivi

Prezzo totale per 50 unità, dispositivi e tablet	a corpo		

Sezione 4 - Altre forniture e servizi

Fornitura/U.M.	Quantità	Prezzo totale	
14 Sala Crisi			
Prezzo totale	a corpo		
15 Sala Apparati e Sistemi di Energia			
Prezzo totale	a corpo		

	Prezzo totale offerta	
TOTALE GENERALE		

9.7.1 Approfondimenti del contenuto della tabella economica

Per quanto concerne altri elementi che possono essere di interesse ai fini della valutazione del Fornitore per l'elaborazione della propria offerta, si evidenzia quanto di seguito:

- il progetto ha una durata, alla data odierna, stimata in 18 mesi solari a decorrere dal 15/01/2014, data che il Committente può variare unilateralmente e che per lo stesso non rappresenta, comunque, alcun vincolo;
- per quanto riguarda le risorse da impiegare per i servizi GMR, GSI e GSW si ritiene opportuna la presenza continuativa per lo svolgimento dei compiti descritti di tre distinte Figure Professionali che, rispettivamente, abbiano un profilo adeguato alle esigenze di progetto. Si ritiene che la medesima risorsa possa difficilmente rispondere, con la propria esperienza e capacità, alle esigenze richieste alle tre diverse Figure Professionali. E' assoluto interesse della Committenza che il livello qualitativo delle stesse sia di livello adeguato agli obiettivi progettuali;

9.8 Criteri generali per la valutazione dello stato di avanzamento dei lavori

Gli stati di avanzamento dei lavori (SAL) dovranno portare puntuali riferimenti alle evidenze delle attività effettuate e alla documentazione di progetto a cui le attività si riferiscono.

I SAL saranno accettati in base alla verifica delle evidenze prodotte e per quanto riguarda la fornitura software o l'erogazione di servizi saranno subordinati ad apposite sessioni di test.

Al fine di consentire un costante monitoraggio dello stato di avanzamento del progetto, al Fornitore è richiesto quindi di illustrare delle possibili metriche di valutazione delle varie attività previste.

9.9 Altri obblighi del Fornitore

9.9.1 Rispetto delle normative vigenti

La produzione, la fornitura e l'installazione di tutti gli elementi del sistema, inteso come singolo ovvero nella propria complessità deve essere eseguita nel rispetto delle norme vigenti e in base alle prescrizioni definite nella offerta e nel Progetto di dettaglio.

Il Fornitore si impegna altresì ad espletare le pratiche relative al rilascio di tutta la documentazione, oltre a quella espressamente descritta nel presente documento, che dovesse essere oggettivamente necessaria per il funzionamento del sistema.

9.9.2 Custodia

Sarà sempre a carico del Fornitore l'onere di provvedere alla custodia e alla sorveglianza di tutto quanto concernente la fornitura, la posa in opera delle apparecchiature e le altre prestazioni occorrenti (hardware e software) per la realizzazione del sistema, tenendo sollevato il Committente da qualunque responsabilità in merito.

9.9.3 Esecuzione di prove, test, omologazioni

Il Fornitore dovrà provvedere a proprie spese all'esecuzione delle prove, test ed omologazioni sui materiali impiegati o da impiegare che il Committente, in caso di previsione normativa ovvero di contestazioni, disponga di far eseguire presso laboratori o istituti specializzati.

9.9.4 Varianti ed espansioni

Il Fornitore non potrà eseguire qualsivoglia variante che non sia a carattere migliorativo o a soluzione di difficoltà intervenute durante la realizzazione dei prodotti e dei sistemi oltre che all'erogazione dei servizi in relazione alle attività previste dal progetto senza la preventiva autorizzazione del Committente.

Le variazioni eventualmente richieste dal Committente saranno concordate con il Fornitore sulla base della determinazione ed approvazione dei nuovi prezzi non contemplati nel contratto.

9.9.5 Proprietà dei dati

Tutti i dati gestiti nell'ambito dell'erogazione del Servizio (inclusi i dati utente, i parametri di configurazione e di personalizzazione degli applicativi, i log di sistema, ecc.) sono proprietà del Committente.

Il Fornitore si impegna a gestire i dati secondo la normativa vigente, garantendo in ogni caso la massima riservatezza sui dati stessi.

Durante l'intera Fase di gestione, e comunque al termine della stessa, il Fornitore si impegna a fornire una copia dei dati in formato database completi di dizionario dati.

9.9.6 Esonero di responsabilità e trasferimento dei rischi

Il Fornitore risponde di tutti i danni causati, a qualsiasi titolo, nell'esecuzione del rapporto contrattuale:

- a persone o cose alle dipendenze e/o di proprietà dell'Impresa stessa;
- a terzi e/o cose di loro proprietà.

9.10 Penali

Nelle Fasi di Implementazione e di Gestione del progetto, le penali per ritardi nell'effettuazione di quanto descritto, relativamente alle diverse Fasi e specifiche attività del progetto, saranno applicate in base al seguente schema da ritenere prevalente laddove vi sia una analoga/equivalente previsione nelle schede in appendice (cd. "indicatori/misure di qualità").

Tipologia	Descrizione	Regola	Penale
Piprog	Piano di progetto contenente il dettaglio delle fasi e delle consegne (consegna documentazione)	Consegna deliverable, approvato dalla Committente, entro 60 giorni dalla stipula del Contratto.	1% dell'importo del Contratto per ogni giorno di ritardo
DefSOA	Definizione dell'architettura SOA(consegna documentazione)	Consegna deliverable, approvato dalla Committente, entro le date indicate nel Piano di Progetto per le singole componenti.	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
Anpre	Analisi preliminare dei requisiti Funzionali (consegna documentazione)	Consegna deliverable, approvato dalla Committente, entro le date indicate nel Piano di Progetto per le singole fasi di implementazione.	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
AnDefReq	Analisi di dettaglio e Definizione dei Requisiti Funzionali e Tecnici (consegna documentazione)	Consegna deliverable, approvato dalla Committente, entro le date indicate nel Piano di Progetto per le singole fasi di implementazione.	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
DefArch	Definizione dell'architettura Software (consegna documentazione)	Consegna deliverable, approvato dalla Committente, entro la data indicata nel Piano di Progetto	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
InSvil	Inizio operazioni di Sviluppo Software	Consegna deliverable, approvato dalla Committente, entro le date indicate nel Piano di Progetto per le singole fasi di implementazione.	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
TestFase	Fine Test con esito positivo della singola fase	Consegna deliverable di singola fase, approvato dalla Committente, entro le date indicate nel Piano di Progetto per le singole fasi	0,5‰ dell'importo del Contratto per ogni giorno di ritardo

		di implementazione.	
CollFase	Collaudo della singola fase	Collaudo con esito positivo della singola fase, entro le date indicate nel Piano di Progetto per le singole fasi di implementazione.	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
TestSys	Fine Test con esito positivo	Consegna deliverable finale, approvato dalla Committente, entro la data indicata nel Piano di Progetto.	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
CollSys	Collaudo del Sistema e passaggio in Esercizio	Collaudo con esito positivo e passaggio in Esercizio della Piattaforma. Entro la data indicata nel Piano di Progetto	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
ProgOBU	Progettazione delle OBU (consegna documentazione)	Consegna deliverable, approvato dalla Committente, entro la data indicata nel Piano di Progetto	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
CollOBU	Collaudo e consegna delle OBU	Collaudo con esito positivo e consegna delle apparecchiature. Entro la data indicata nel Piano di Progetto	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
ProdLic	Consegna dei prodotti a licenza	Installazione, configurazione e consegna deliverable dei prodotti a licenza entro una settimana dal collaudo positivo	0,5‰ dell'importo del Contratto per ogni giorno di ritardo
ModForm	Predisposizione dei moduli formativi	Consegna deliverable, approvato dalla Committente, entro la data indicata nel Piano di Progetto	0,5‰ dell'importo del Contratto per ogni giorno di ritardo

Nella fase di gestione del progetto le penali per incidenti e indisponibilità del sistema nonché per il servizio di help-desk saranno applicate in base al seguente schema; quelle sotto indicate saranno da ritenere prevalenti laddove vi sia una analoga/equivalente previsione nelle schede in appendice (cd. "indicatori/misure di qualità").:

Tipologia	Descrizione	Regola	Penale
IncBlo	Incidente bloccante (ovvero un evento che comporta un grave deterioramento delle funzionalità o dell'hardware tale da non permette agli utenti di proseguire nelle loro attività – applicabile anche al singolo utente)	97% dei guasti risolto entro 2 ore. La consuntivazione avverrà su base trimestrale.	0,5% dell'importo del Contratto per ogni punto percentuale di differenza
IncGra	Incidente Grave (evento che comporta un grave deterioramento delle funzionalità o dell'hardware, ma consente comunque di proseguire le operazioni)	98% dei guasti risolti entro 4 ore. La consuntivazione avverrà su base trimestrale.	0,3% dell'importo del Contratto per ogni punto percentuale di differenza

IncLie	Incidente Lieve (evento che non necessita di intervento urgente in quanto causa un degrado di prestazioni tollerabile per periodi limitati)	98% dei guasti risolti entro 4 ore. La consuntivazione avverrà su base trimestrale.	0,1% dell'importo del Contratto per ogni punto percentuale di differenza
RecFail	Recovery dei dati dopo failure di sistema	Ripristino dei messaggi e dati persi a seguito della failure entro 4 ore dal ripristino del sistema. La consuntivazione avverrà su base trimestrale.	0,1% dell'importo del Contratto per ogni ora aggiuntiva
DisComp	Disponibilità complessiva del servizio per segnalazione incidenti e problemi. La disponibilità sarà calcolata rispetto al numero di chiamate registrate nel periodo di riferimento (sono incluse nel conteggio anche le cosiddette chiamate abbandonate)	Giorni di accessibilità 7 giorni alla settimana x 24h al giorno. 98% di disponibilità calcolata in un trimestre. La consuntivazione avverrà su base trimestrale.	0,1% dell'importo del Contratto per ogni punto percentuale di differenza

Per incidente bloccante si intende qualsiasi incidente che invalidi la funzionalità anche del solo singolo utente, purché riconducibile a malfunzionamenti del Sistema.

10. CRITERI DI AGGIUDICAZIONE

L'appalto sarà aggiudicato con il criterio dell'offerta economicamente più vantaggiosa ai sensi dell'art. 83 del Decreto Legislativo n. 163/2006 e s.m.i., determinata in base ai seguenti elementi di valutazione applicati congiuntamente e di seguito descritti.

10.1 Contenuto dell'offerta del Fornitore

Si riprende, per comodità di trattazione, lo schema di contenuto dell'offerta che dovrà essere redatta dal Fornitore e già illustrata nel Disciplinare di Gara.

item	argomento	contenuto
1	Presentazione dell'offerente	1) Breve descrizione delle caratteristiche peculiari del Fornitore, con particolare riferimento, tra l'altro, a: • organizzazione aziendale • organico tecnico • struttura di assistenza • certificazioni possedute. 2) Elenco delle principali referenze di progettazione e di realizzazione di sistemi informativi evidenziando, tra l'altro: • progettazione e produzione di dispositivi di bordo similari alle OBU richieste; • sistemi di localizzazione di mezzi mobili; • sistemi informativi con architetture SOA; • sistemi informativi finalizzati alla Business Intelligence ed all'analisi semantica. 3) Elenco delle eventuali esperienze di progettazione e realizzazione di sistemi tecnologici e di sistemi informativi in ambito di • infrastrutture per la security portuale; • intelligence inerente il trasporto marittimo; • settore dell'autotrasporto; • altro, qualora attinente il presente progetto. *In relazione ai precedenti punti, in caso di RTI è richiesto che siano specificati i ruoli e le attività svolte da ciascuna impresa componente l'RTI.*
2	Obiettivi e analisi dei requisiti	4) Breve commento dell'analisi della situazione che identifichi, tra l'altro, il gap tra le descrizioni effettuate nel capitolato tecnico ed i riscontri effettuati, in termini di • obiettivi di progetto; • modalità di perseguimento; • criticità e inadeguatezze; • benefici attesi. 5) Breve presentazione della soluzione ai requisiti descritti, illustrata anche con uno schema di corrispondenza, nel

		capitolato tecnico. Deve essere colto l'obiettivo di inquadrare al meglio l'intervento del Fornitore e di far percepire il vantaggio competitivo che lo stesso offre rispetto al mercato di riferimento.
3	Sintesi della fornitura	6) Sintesi della fornitura di cui ai capitoli 6 e 7 del capitolato tecnico; si raccomanda il preciso elenco degli elementi di fornitura e di specificare, tra l'altro: • approccio metodologico e strumenti adottati per l'identificazione della soluzione • particolare riferimento alle motivazioni per la scelta dell'hardware e software di base per il centro elaborazione e memorizzazione dati • elenco e descrizione delle caratteristiche delle OBU e dei dispositivi collegati • elenco e descrizione delle integrazioni infrastrutturali (Sala Crisi, Sala Apparati, Sistemi d'Energia) • elenco e descrizione delle caratteristiche degli elementi di integrazione • elenco e descrizione delle caratteristiche di scalabilità e modularità • elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.
4	Architettura tecnico-funzionale del sistema	7) Presentazione delle specifiche relative all'architettura tecnica e funzionale della soluzione di cui ai capitoli 4 e 5 del capitolato tecnico; in particolare: • approccio metodologico e strumenti adottati per l'identificazione della soluzione • descrizione delle caratteristiche dell'infrastruttura tecnologica complessiva, con particolare riferimento alla infrastruttura di comunicazione e di collegamento con i sistemi oggetto di acquisizione e scambio dati • descrizione delle caratteristiche dell'architettura applicativa e delle soluzioni offerte, con particolare riferimento alle componenti centrali ed ai singoli moduli di elaborazione e ai singoli moduli client • descrizione delle funzionalità offerte, illustrate con uno schema di corrispondenza, rispetto a quanto indicato nel capitolato tecnico • descrizione delle caratteristiche di personalizzazione e delle caratteristiche di integrazione applicativa con i sistemi oggetto di acquisizione e scambio dati • elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.
5	Piano di Progetto	8) Presentazione di una sintesi del Piano di progetto, con descrizione delle caratteristiche delle attività di progetto con riferimento alle Fasi descritte nel capitolo 8 del capitolato tecnico. Il Piano dovrà essere accompagnato da un cronoprogramma che illustri le relazioni temporali e le dipendenze delle varie attività, anche con evidenza delle milestone relative, almeno, ai seguenti eventi: • Progettazione di dettaglio

		• Sviluppo e test • Collaudi • Avviamento • Attività per l'avvio della Fase di gestione • Attività continuative nella Fase di gestione • Termine della Fase di gestione Nel piano devono essere indicate le modalità e i momenti di raccordo, laddove possibile, con le risorse informatiche (infrastrutture di rete, servizi, applicazioni, basi di dati, ecc.) esistenti. Il Piano dovrà evidenziare le giornate uomo distribuite in relazione ai periodi di attività tra le milestone indicate, senza fornire indicazioni di carattere economico. 9) Presentazione di una sintesi del Piano di Qualità 10) Presentazione di una sintesi dei requisiti minimi di sicurezza e di osservanza alla normativa sulla privacy anche in relazione a quanto necessario per la sicurezza delle reti installate presso la Sala Apparati e la Sala Crisi
6	Dettaglio Fase di gestione	11) Descrizione delle caratteristiche del servizio di assistenza all'utenza; elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico 12) Descrizione delle caratteristiche dei Livelli di Servizio; elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.
7	Organizzazione di progetto	13) Indicazione dell'organizzazione di progetto e del gruppo di lavoro, con • definizione, ruolo e qualificazione delle figure professionali coinvolte • quantificazione (in giorni/uomo) delle attività ad esse associate • curriculum e l'associazione ai profili professionali di cui alle indicazioni contenute nel capitolato tecnico.

10.2 Tabelle dei costi da indicare nell'offerta economica

Di seguito, per comodità di trattazione, si fornisce lo schema delle tabelle da redigere in sede di offerta e relative ai costi per voci di spesa (sempre espresse in Euro); oltre alla Tabella Principale illustrata nel precedente capitolo, è richiesta la compilazione delle seguenti Tabelle di dettaglio

Tabella di dettaglio della voce 3, 4, 5 della tabella principale:
Costi di sviluppo e test software per componente/1

Voce di costo (escluse spese di installazione)	Importo netto totale	Importo con IVA totale
SOTTO SISTEMA SEA SIDE (SiSS)		
Soluzione architetturale e SOA governance		

Modulo Movimentazione		
Modulo Surveillance		
Service Portal		
Modulo Workflow		
Modulo Documentale		
Modulo Intelligence		
Modulo Gateway applicativo		
Modulo Orchestrator		
SOTTO SISTEMA LAND SIDE (SiLS)		
Sviluppo SW per OBU e connessione a dispositivi di bordo		
Sviluppo layer applicativo di comunicazione PNL – SiLS		
Sviluppo componente centrale SiLS		
Primo Client - Amministratore		
Secondo Client - Gestore tecnico		
Terzo Client – Utente Gestore operativo		
Quarto Client 4 - Utente conducente		
Quinto client - Utente Forze di Polizia		

Tabella di dettaglio delle voci 3, 4, 5 della tabella principale:
Costi di sviluppo e test software per componente/2

Voce di costo	Importo netto totale	Importo con IVA totale
Costo totale per installazione software oggetto di sviluppo		

Tabella di dettaglio della voce 12 della tabella principale:
Costi per software di base e altre licenze software/1

Voce di costo (escluse spese di installazione)	Importo netto unitario	Q.tà	Importo netto totale	Importo con IVA totale
Sistema Operativo (una riga per ogni singola licenza) ➔ *aggiungere le righe necessarie*				
Licenza Tele Atlas (comprensiva di tre mesi di copertura dopo il termine della Fase di gestione)				
➔ *aggiungere le righe necessarie*				

Tabella di dettaglio della voce 12 della tabella principale:
Costi per software di base e altre licenze software/2

Voce di costo	Importo netto totale	Importo con IVA totale
Costo totale per installazione software di base e altre licenze software		

Tabella di dettaglio della voce 12 della tabella principale:
Costi per hardware/2

Voce di costo	Importo netto totale	Importo con IVA totale
Costo totale per installazione hardware		

Tabella di dettaglio della voce 13 della tabella principale:
Costi per hardware/1

Voce di costo (escluse spese di installazione)	Importo netto unitario	Q.tà	Importo netto totale	Importo con IVA totale
On Board Unit (OBU) quale unità centrale e modulo di comunicazione e comprensiva di ricevitore satellitare, dispositivo navigazione stimata, dispositivo RFID per gestione carico, dispositivo RFID per attraversamento varchi (anche unificato al precedente), sensore inerziale, connettività centralina di bordo, connettività telecamere di bordo, antenne di comunicazione		50		
Dispositivi di bordo collegati alla OBU				
Telecomando portatile		50		
Congegno uomo-a-terra		50		
Telecamera installata a bordo con memoria estraibile		50		
Tablet “classe 7 pollici”		35		
Tablet “classe 10 pollici”		35		
➔ *aggiungere le righe necessarie*				

Tabella di dettaglio delle voci 14 e 15 della tabella principale:
Costi per integrazioni infrastrutturali/1

Voce di costo (escluse spese di installazione)	Importo netto unitario	Q.tà	Importo netto totale	Importo con IVA totale
SALA CRISI				
➔ *aggiungere le righe necessarie*				
SALA APPARATI				
➔ *aggiungere le righe necessarie*				
SISTEMI DI ENERGIA				
➔ *aggiungere le righe necessarie*				

Tabella di dettaglio delle voci 14 e 15 della tabella principale:
Costi per integrazioni infrastrutturali/2

Voce di costo	Importo netto totale	Importo con IVA totale
Costo totale per installazione Sala Crisi, Sala Apparati e Sistemi di Energia		

10.3 Tempi di realizzazione delle attività

Di seguito, per comodità di trattazione, si fornisce uno schema sommario della tempistica di progetto.

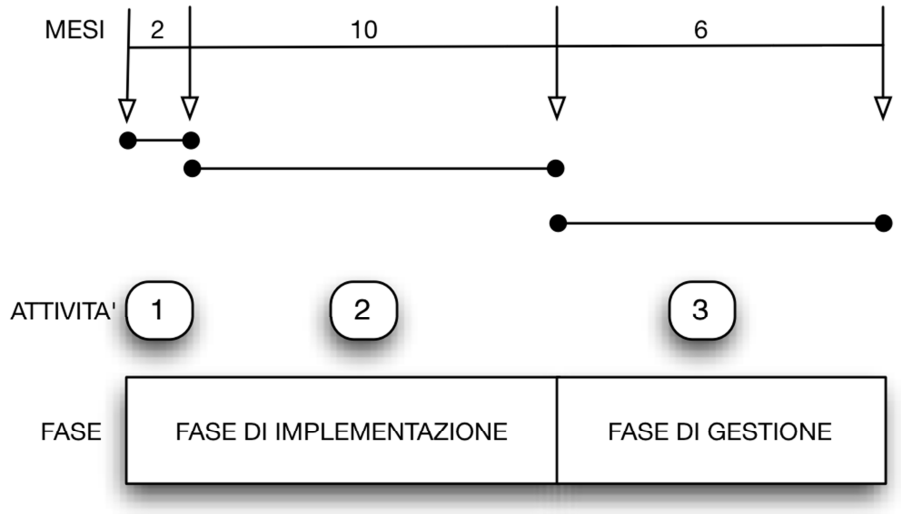

Figura 13 - Schema non standard dei tempi di realizzazione del progetto

In riferimento alla precedente figura, il dettaglio è costituito da

- attività 1; comprende la redazione del Piano di progetto e del Piano di qualità
- attività 2; comprende la fase di sviluppo e test fino alla dichiarazione del Fornitore di approntamento al collaudo. Si tratta di dieci mesi solari e continuativi.
- attività 3: ha inizio con l'avviamento e comprende la Fase di Gestione; la durata di questa attività corrisponde a sei mesi solari e continuativi.

10.4 Criteri di valutazione

Il punteggio massimo ottenibile corrisponde ai criteri seguenti

- offerta tecnica (elementi qualitativi) max 65 punti
- offerta economica (elementi quantitativi) max 35 punti
- totale offerta max 100 punti

Il punteggio totale (P_{TOT}) attribuito a ciascuna offerta è uguale a $P_T + P_E$, laddove

- P_T = somma dei punti attribuiti all'offerta tecnica (elementi qualitativi);
- P_E = punteggio attribuito offerta economica (elementi quantitativi).

La Commissione esaminerà e valuterà le soluzioni progettuali indicate nelle offerte tenendo conto dell'aderenza delle stesse alle esigenze espresse nel capitolato tecnico come requisito tecnico, prestazionale e funzionale.

Nel contempo, valuterà al meglio ogni aspetto, con particolare riferimento alle migliorie proposte dal Fornitore, che sia in grado di realizzare compiutamente le esigenze del

Committente esaltando l'investimento effettuato in termini di migliore rapporto tra prezzo e prestazioni.

10.4.1 Offerta tecnica (elementi di natura qualitativa)

La stessa sarà valutata con l'effettuazione del calcolo dell'offerta economicamente più vantaggiosa così come regolata dal D.P.R. n. 207/2010, allegato P, punto II, a), nel quale è descritto il metodo di calcolo

$$C(a) = \sum_n [Wi * V(a)i]$$

dove:

$C(a)$ = indice di valutazione dell'offerta (a)
n = numero totale dei requisiti
Wi = peso o punteggio attribuito al requisito (i)
$V(a)i$ = coefficiente della prestazione dell'offerta (a) rispetto al requisito (i)
$\sum_n$ = sommatoria

I coefficienti $V(a)i$ sono determinati attraverso la media dei coefficienti, variabili tra zero e uno, calcolati da ciascun Commissario mediante il "confronto a coppie", seguendo le linee guida riportate nell'allegato G del D.P.R. n. 207/2010. (cfr. D.P.R. n. 207/2010, allegato P, punto II, a), metodo 1.).

10.4.1.1 Griglia di valutazione dell'offerta tecnica

n.	item	argomento	contenuto	Punti max
1	1	Obiettivi e analisi dei requisiti	Breve commento dell'analisi della situazione che identifichi, tra l'altro, il gap tra le descrizioni effettuate nel capitolato tecnico ed i riscontri effettuati, in termini di obiettivi di progetto, modalità di perseguimento, criticità e inadeguatezze; benefici attesi.	1
2			Breve presentazione della soluzione ai requisiti descritti, illustrata anche con uno schema di corrispondenza, nel capitolato tecnico. Deve essere colto l'obiettivo di inquadrare al meglio l'intervento del Fornitore e di far percepire il vantaggio competitivo che lo stesso offre rispetto al mercato di riferimento.	2
	2	Sintesi della fornitura	Sintesi della fornitura di cui ai capitoli 6 e 7 del capitolato tecnico; si raccomanda il preciso elenco degli elementi di fornitura e di specificare, tra l'altro:	
3			approccio metodologico e strumenti adottati per l'identificazione della soluzione	1
4			particolare riferimento alle motivazioni per la scelta dell'hardware e software di base per il centro elaborazione e memorizzazione dati	3
5			elenco e descrizione delle caratteristiche delle OBU e dei dispositivi collegati	5
6			elenco e descrizione delle integrazioni infrastrutturali (Sala Crisi, Sala Apparati, Sistemi d'Energia)	3
7			elenco e descrizione delle caratteristiche degli elementi di integrazione	1

8			elenco e descrizione delle caratteristiche di scalabilità e modularità	2
9			elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.	2
	3	Architettura tecnico-funzionale del sistema	Presentazione delle specifiche relative all'architettura tecnica e funzionale della soluzione di cui ai capitoli 4 e 5; in particolare:	
10			approccio metodologico e strumenti adottati per l'identificazione della soluzione	1
11			descrizione delle caratteristiche dell'infrastruttura tecnologica complessiva, con particolare riferimento alla infrastruttura di comunicazione e di collegamento con i sistemi oggetto di acquisizione e scambio dati	1
			Sistema Sea-Side	
12			Soluzione architetturale e SOA governance	3
13			Modulo Movimentazione	1
14			Modulo Surveillance	2
15			Modulo Service Portal	1
16			Modulo Workflow	2
17			Modulo Documentale	1
18			Modulo Intelligence	9
19			Modulo Orchestrator	1
20			Modulo Gateway applicativo	1
			Sistema Land-Side	
21			Componente centrale SiLS e layer applicativo di comunicazione PLN/SiLS	2
22			Primo client SiLS	1
23			Secondo client SiLS	1
24			Terzo client SiLS	2
25			Quarto client SiLS	1
26			Quinto client SiLS	1
27			Descrizione delle funzionalità offerte, illustrate con uno schema di corrispondenza, rispetto a quanto indicato nel capitolato tecnico; descrizione delle caratteristiche dell'architettura applicativa e delle soluzioni offerte, con particolare riferimento alle componenti centrali ed ai singoli moduli di elaborazione e ai singoli moduli client; descrizione delle funzionalità offerte, illustrate con uno schema di corrispondenza, rispetto a quanto indicato nel capitolato tecnico	2
28			Descrizione delle caratteristiche di personalizzazione e delle caratteristiche di integrazione applicativa con i sistemi oggetto di acquisizione e scambio dati	1
29			Elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.	2
30	4	Piano di Progetto (incluso Piano di Qualità e di Sicurezza)	Presentazione di una sintesi del Piano di progetto, con descrizione delle caratteristiche delle attività di progetto con riferimento alle Fasi descritte nel capitolo 8 del capitolato tecnico.	1
31			Nel piano devono essere indicate le modalità e i momenti di raccordo, laddove possibile, con le risorse informatiche (infrastrutture di rete, servizi, applicazioni, basi di dati, ecc.) esistenti.	1
32			Presentazione di una sintesi del Piano di Qualità e presentazione di una sintesi dei requisiti minimi di sicurezza e di osservanza alla normativa sulla privacy, anche in relazione a quanto necessario per la sicurezza delle reti installate presso la Sala Apparati e la	1

			Sala Crisi.	
33	5	Dettaglio Fase di gestione	Descrizione delle caratteristiche del servizio di assistenza all'utenza; elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.	1
34			Descrizione delle caratteristiche dei Livelli di Servizio; elenco e descrizione delle caratteristiche degli eventuali elementi innovativi e migliorativi, rispetto a quanto indicato nel capitolato tecnico.	1
	6	Organizzazione di progetto	Indicazione dell'organizzazione di progetto e del gruppo di lavoro, con:	
35			definizione, ruolo e qualificazione delle figure professionali coinvolte	2
36			quantificazione (in giorni/uomo) delle attività ad esse associate	1
37			curriculum e l'associazione ai profili professionali di cui alle indicazioni contenute nel capitolato tecnico.	1

10.4.2 Offerta economica (elementi di natura quantitativa)

L'elemento dell'offerta economica è il PREZZO: il valore finale dichiarato dal Fornitore, dal quale si calcola il ribasso percentuale (di seguito valore R_a) rispetto all'importo a base di gara; il massimo dei punti ottenibili ai fini del calcolo del P_E è pari a 35;

La stessa sarà valutata con l'effettuazione del calcolo dell'offerta economicamente più vantaggiosa così come regolata dal D.P.R. n. 207/2010, allegato P, punto II, b), nel quale è descritto il metodo di calcolo

$$V(a)i = \frac{R_a}{R_{max}}$$

dove:

R_a = valore offerto dal Fornitore
R_{max} = valore dell'offerta più conveniente.

10.4.3 Interpretazione dei calcoli per le offerte

Ogni aspetto non esplicitato nei due precedenti paragrafi, relativamente al metodo di calcolo, all'attività dei Commissari ed ogni altro aspetto applicativo del metodo cd. aggregativo/compensatore è demandato a quanto previsto dal D.P.R. n. 207/2010, allegati P e G.

TABELLA DEGLI ACRONIMI

Acronimo	Descrizione
AIDA	Automazione Integrata Dogane Accise - Sistema informativo dell'Agenzia delle Dogane e dei Monopoli
AP	Autorità Portuale
AR	Analisi dei Rischi
ASIREG	Consorzio per lo Sviluppo Industriale della Provincia di Reggio Calabria
AUI	Archivio Unico Informatico
AUP	Agile Unified Process
BLG	Bremer Lagerhaus Gesellschaft – Operatore commerciale a Gioia Tauro
BPM/BPMN	Business Process Model/Business Process Model Notation
CA	Controllo Automatico
CCR	Centro Comune di Ricerca della Commissione Europea
CD	Controllo Documentale
CIFS	Common Internet File System
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
COTS	Commercial Off The Shelf
CS	Controllo Scanner
DPCM	Decreto del Presidente del Consiglio dei Ministri
EDA	Event Drive Architechture
ENS	Entry Summary Declaration
EORI	European Operator Registry Idenditification
ESB	Enterprise Service Bus
EUP	Enterprise Unified Process
EXS	Exit Summary Declaration
HACKPACK	Hazardous Assessment Computer Package
HS	Harmonized System
HTTPS	HyperText Transfer Protocol over Secure Socket
IAM	Identity Access Management
IATA	International Air Transport Association
ICT	Information and Communication Technology
IMAP	Internet Message Access Protocol
IMO	International Maritime Organization
ISO/ANSI	International Organization for Standardization / American National Standards Institute
ISPS	International Ship and Port Facility Security
J2EE	Java 2 Enterprise Edition

JRC	Joint Research Committee
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPR	License Plate Recognition
MAE	Ministero degli Affari Esteri
MASM	MAritime Security Management
MCT/BLG	Medcenter Container Terminal – Gestore del Terminal container a Gioia Tauro
MISE	Ministero dello Sviluppo Economico
MMA	Manifesto delle Merci in Arrivo
MMP	Manifesto delle Merci in Partenza
MRN	Movement Reference Number
NVR	Network Video Server
OCR	Optical Character Recognition
ODBC	Open DataBase Connectivity
OO	Object Oriented
OSINT	Open Source INTelligence
OWASP	Open Web Application Security Project
PLN	Piattaforma Logistica Nazionale
PMIS	Port Management Information System
PON	Programma Operativo Nazionale
RDBMS	Relational Data Base Management System
RFID	Radio Frequency IDentification
RUP	Rational Unified Process
SAN	Storage Area Network
SCORM	Shareable Content Object Reference Model
SiSS	Sistemi Sea-Side
SiLS	Sistemi Land-Side
SOA	Service Oriented Architecture
STAC	System Terminal Control Access
SW	Single Window
TC	Temporanea Custodia – Regime Doganale
TEU	Twenty-foot Equivalent Unit – Unità di misura per container
TVCC	Televisione a Circuito Chiuso
UML	Unified Modeling Language
UPS	Uninterruptible Power Supply
UVAC	Uffici Veterinari per gli Adempimenti degli obblighi Comunitari
VM	Visita Merce
VTS	Vessel Traffic Service

W3C	World Wide Web Consortium
XML	eXtensible Markup Language